Online RMS

Version 11.10.2

Product Change Notice

4 October 2022

REVISION HISTORY

Revised By	Revision Date	Version	Notes
T. Thompson	4 Oct 2022	1.0	Production release.

TABLE OF CONTENTS

INTRODUCTION

This document provides an overview of the software changes delivered in the 11.10.2 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 and security, we recommend a computer, laptop, or tablet purchased within the last 3 years; running an industry common web browser that is actively supported and updated to the most recent web standards by the browser manufacturer and connecting to the internet by DSL, Cable, or cellular (4G or higher).

Your browser must support the TLS 1.2 security protocol or higher. Browsers running the TLS 1.0/1.1 security protocols have known security vulnerabilities and are no longer supported by Caliber Online RMS. Please make sure your web browser has TLS 1.2 or higher enabled.

IMPORTANT NOTICE FOR ONLINE RMS AGENCIES USING INTERNET EXPLORER (IE)

On August 17, 2021, Microsoft announced that Internet Explorer 11 will no longer work optimally with Microsoft 365 services. Microsoft ended support for the Internet Explorer 11 desktop application for certain versions of Windows 10 on June 15, 2022. Internet Explorer no longer supports new web standards used by modern applications. See Microsoft's website [announcement page](#) for more information.

Caliber strongly recommends that you use an industry popular web browser that is supported and updated to the most recent web standards. Caliber is unable to provide support and issue resolutions on web browsers that are not supported and maintained to the most recent web standards.

RELEASE MILESTONES

The following table contains the high-level release milestones for the Online RMS 11.10.2 release.

End Date	Milestone
23 Aug 2022	11.10.2 Sprint 1 Starts
20 Sep 2022	11.10.2 Code Lock
4 Oct 2022	11.10.2 Release Available

APPENDIX: 11.10.2 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 11.10.2 release. An ***** symbol - denotes a software resolution that was deployed prior to the 11.10.2 service pack installation date.

JIRA #	Client Ticket #	Summary	Type of Issue	RMS Module	Functional Documentation
IA-75633	417253	MICR Corrections for BIAS Codes	Configuration	State Submissions	Software Update - Michigan State MICR code table configuration updates.
IA-75757	N/A	MICR: Error 984 At least one Property Class must be (Dependent on Offense File Class)	Bug/Defect	State Submissions	Software Update - Michigan State MICR code table configuration updates.
IA-76226	N/A	MICR: v1.6 Configuration changes Part 2	Configuration	State Submissions	Software Update - Michigan State MICR code table configuration updates.
IA-76439*	421091	ODL - Fuel costs added to a vehicle in ODL is being auto added to Fluid costs	Bug/Defect	ODL	Software Update - Update logic when applying Fuel Costs entered from Officer Daily Log (ODL).

JIRA #	Client Ticket #	Summary	Type of Issue	RMS Module	Functional Documentation
IA-76441	N/A	Report Beam Crash - South Carolina - Officer Data	Enhancement	Interface	Interface Improvement - Logic update to translate the Officer badge number received from Report Beam Crash software to a matching Officer ID in Online RMS.
IA-76459*	421238	Administration/Agency/Agency Setting View Offense codes gives exception Error	Release Defects	Admin	Software Update - Improved the User interface display for admins viewing the Agency Local Offense configuration page.
A-76474*	421264	RMS - MDTA users cannot access Evidence navigating through Master Indices property no incident report assigned.	Release Defects	Property Mgmt	Software Update - Enhanced security for viewing Evidence Chain-of-Custody from the Master Property details page. A link to view evidence will appear for users based on the below business rules: 1) Evidence is checked out to the user OR 2) User is an evidence custodian and in the same evidence agency OR 3) User is an evidence custodian and the evidence is in the same ORG, where the ability to manage ORG evidence is set to yes. OR 4) Navigating to the Master Property page from an incident OR 5) The user is the creator of the evidence record.

JIRA #	Client Ticket #	Summary	Type of Issue	RMS Module	Functional Documentation
IA-76481	N/A	NIBRS Regenerate IBR values give an error message to contact support	Bug/Defect	State Submissions	Software Update - Improved the process for regenerating IBR values incident reports included in a dataset.
IA-76490	N/A	NIBRS: Incident should be reported but is Non reportable where occurrence date is prior to NIBRS_INCLUDE_ DATE and has never been reported before	Bug/Defect	State Submissions	Software Update - NIBRS submission improvement to manage situations where the incident report occurrence date is in the past before the RMS Include NIBRS date, but the report date is after the RMS include NIBRS date.
IA-76491	421478	MICR Offense 28000 does not allow property codes 03/05/24/28/37	Configuration	State Submissions	Software Update - Michigan State MICR code table configuration updates.
IA-76492	421478	MICR Pre-validation error submitted duplicate property	Bug/Defect	State Submissions	Software Update - Michigan State MICR Incident validation update.
IA-76550	421461	Update the property color code to the NCIC Code for Multicolor	Configuration	State Submissions	Software Configuration Update - Aligned the property color code of multicolored to the NCIC code of MUL/COL.
IA-76573	N/A	Online RMS-Install script for release 11.10.2	DevTask	Admin	Online RMS- Install script for release 11.10.2
IA-76593	N/A	IBR - Upgrade to remove Log4j Version1 references	Technical Upgrade	State Submissions	Security Update - deprecate references to Log4j.

JIRA #	Client Ticket #	Summary	Type of Issue	RMS Module	Functional Documentation
IA-76610*	421924	RMS- Error saving a sub form.	Bug/Defect	Custom Forms	Software Update - Improved validation warnings when user haven't completed all designated required fields on a sub form within a custom form.
IA-76621	N/A	CFS Export - Dispatch Date	Bug/Defect	Interface	Interface Improvement - Update to manage situations where dispatch date is not populated.
IA-76622	N/A	Report Beam Citation Interface - Address Matching	Configuration	Interface	Interface Improvement - Custom matching logic added improve matching on Street Number, Street Name, and State.

--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.