Caliber

PUBLIC SAFETY

Protecting Tomorrow–Today.™

Online RMS

Version (11.7.3)

Product Change Notice

02 Nov 2021

REVISION HISTORY

Revised By	Revision Date	Version	Notes
T. Thompson	02 Nov 2021	1.0	Production release.

TABLE OF CONTENTS

INTRODUCTION

This document provides an overview of the software changes delivered in the 11.7.3 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 11.7.3 release.

End Date	Milestone
28 Sep 2021	11.7.3 Sprint 1 Starts
26 Oct 2021	11.7.3 Code Lock
02 Nov 2021	11.7.3 Release Available

APPENDIX: 11.7.3 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 11.7.3 release.

* - Denotes a software resolution was released prior to the 11.7.3 service pack installation date.

JIRA #	Client Ticket #	Summary	Type of Issue	RMS Module	Functional Documentation
IA-73466	399083	Upgrade Jasper Server	Engineering Enhancement	AdHoc Reporting	Improving Reporting - Upgraded Jasper Reporting Server to Version 7.9 in advance of the 11.8 Major Release in December. Version 7.9 includes many new features that give greater usability and flexibility to Admins when creating Ad Hoc Reports. 1. Overall UI Improvements – An updated look and feel for Repository, Schedule, and Management pages. 2. Distinct values - Easily remove Duplicate values in Reports. 3. Improved Schedule Workflow – Schedule directly from the Report Viewer. 4. Cryptography improvements - Import and export operations now allows administrators to specify an encryption key. 5. Performance Improvements – Significant improvements for filters and overall Jasper responsiveness.
IA-74239*	410238	NJ NIBRS Warnings Display for data set submissions	Bug/Defect	State Submissions	Software Update - New Jersey State NIBRS Incident submission update.

JIRA #	Client Ticket #	Summary	Type of Issue	RMS Module	Functional Documentation
IA-74276	N/A	Online RMS- Install script for release 11.7.3	DevTask	Admin	Online RMS- Install script for release 11.7.3
IA-74303	408749 408683 408650	NIBRS Resubmit Incident for NIBRS Corrections	Bug/Defect	State Submissions	Software Update - The Online RMS Incident Based Reporting process has been updated to determine if incident reports that are edit should be included in the open dataset for resubmission processing.
IA-74305	410645	NJ NIBRS Incident Location City State and Zip are required fields - Add Incident Warning to Notify Users if missing	Bug/Defect	State Submissions	Software Update - New Jersey State NIBRS Incident submission update.
IA-74335	N/A	ETHOS - Modify format for Date of Crash Date/Time	Bug/Defect	Interface	Interface Improvement - Update LexisNexis ETHOS eCrash Interface for Massachusetts.
IA-74339	410454	OK SIBRS Property value for 35A and 35B offenses	Bug/Defect	State Submissions	Software Configuration Update - Oklahoma State NIBRS Incident submission configuration to disallow drugs on 35B offenses and require value.
IA-74341	410454	OK SIBRS XSD Error Arrest Charge exceeds the size limit	Bug/Defect	State Submissions	Software Update - Oklahoma State NIBRS Incident submissions to handle charge code descriptions longer than allowed SIBRS limit.

JIRA #	Client Ticket #	Summary	Type of Issue	RMS Module	Functional Documentation
IA-74342	410454	OK SIBRS Victim Injury Reviewed	Bug/Defect	State Submissions	Software Update - Oklahoma State NIBRS Incident submission update.
IA-74353	N/A	OK SIBRS - 08 Circumstance Code Review	Bug/Defect	State Submissions	Software Update - Oklahoma State NIBRS Incident submission update.

--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.