



Protecting Tomorrow–Today.™

Online RMS

Version 11.9.3

Product Change Notice

12 July 2022

REVISION HISTORY

Revised By	Revision Date	Version	Notes
T. Thompson	07 JUL 2022	1.0	Production release.

TABLE OF CONTENTS

Revision History	1
Introduction	3
Product Requirements.....	4
Release Milestones.....	5
Appendix: 11.9.3 Product Change Notice (PCN) – Detailed JIRA Listing ..	6
TABLE A: RELEASE ENHANCEMENTS AND PRODUCT SOFTWARE ISSUE RESOLUTIONS.....	6
Appendix: Service Commitments	8

INTRODUCTION

This document provides an overview of the software changes delivered in the 11.9.3 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 a modern industry 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 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 a modern 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 11.9.3 release.

End Date	Milestone
24 May 2022	11.9.3 Sprint 1 Starts
28 Jun 2022	11.9.3 Code Lock
12 Jul 2022	11.9.3 Release Available

APPENDIX: 11.9.3 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 11.9.3 release.

* - Denotes a software resolution that was occurred prior to the 11.9.3 service pack installation date.

JIRA #	Client Ticket #	Summary	Type of Issue	RMS Module	Functional Documentation
IA-75873	N/A	OK SIBRS: Duplicate property reported for the same NIBRS offense code	Bug/Defect	State Submissions	Software Update - OK State NIBRS Incident submission update.
IA-75875	N/A	OK SIBRS: Charges are not written in XML in some cases	Bug/Defect	State Submissions	Software Update - OK State NIBRS Incident submission update.
IA-75891	N/A	ETHOS - Accident Businesses – Unparseable Number Error	Bug/Defect	Interface	Interface Improvement - Enhanced to exclude business names.
IA-75905*	418490	Set GA NIBRS Flat Segments lengths to Federal NIBRS specifications.	Configuration	State Submissions	Software Update - GA State NIBRS Incident submission update.
IA-75952	N/A	Online RMS- Install script for release 11.9.3	DevTask	Admin	Online RMS- Install script for release 11.9.3

JIRA #	Client Ticket #	Summary	Type of Issue	RMS Module	Functional Documentation
IA-76045	N/A	EACC Interface - SSN	Bug/Defect	Criminal Complaint	Interface Improvement - Enhanced to ensure that SSNs with leading zeros are effectively managed via the interface.
IA-76046	N/A	Remove Hyperlink to Caliberpublicsafety.com on Online RMS login page.	Bug/Defect	Admin	Software Update - Removed the hyperlink for the Caliber logo on the Online RMS login page that routed users to Caliberpublicsafety.com.

--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.