



Protecting Tomorrow–Today.™

Online RMS

Version 11.14.2

Product Change Notice

6 February 2024

REVISION HISTORY

Revised By	Revision Date	Version	Notes
B. Chapman	6 February 2024	1.0	Production release.

TABLE OF CONTENTS

Revision History 1

Introduction 3

Product Requirements..... 4

Release Milestones 5

Appendix: 11.14.2 Product Change Notice (PCN) – Detailed JIRA Listing. 6

 TABLE A: RELEASE ENHANCEMENTS AND PRODUCT SOFTWARE ISSUE RESOLUTIONS.....6

Appendix: Service Commitments..... 10

INTRODUCTION

This document provides an overview of the software changes delivered in the 11.14.2 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 11.14.2 release.

End Date	Milestone
30 JAN 2024	11.14.2 Code Lock
06 FEB 2024	11.14.2 Release Available

APPENDIX: 11.14.2 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 11.14.2 release. An * symbol - denotes a software resolution that was deployed prior to the 11.14.2 service pack installation date.

JIRA #	Client Ticket #	Summary	Type of Issue	RMS Module	Functional Documentation
IA-79117		Narrative Redaction - Adding a Narrative with no text causes an error on Arrests and Incidents	Bug/Defect	Incident Narrative	Software Update:
IA-79034	438874	Fleet Management - Sorting by Unit # on the \$ Cost of Ownership tab is slow for MSP	Enhancement	Fleet Mgmt	Software Update:
IA-79022	438586	Custom Forms and Fields - Show a warning when removing a Field if already in Designer	Bug/Defect	Custom Forms	Software Update:
IA-79021	437205	Agency Setup Spreadsheet Process - Only require	Enhancement	Admin	Software Update:

JIRA #	Client Ticket #	Summary	Type of Issue	RMS Module	Functional Documentation
		AGENCY_CODE on Agencies tab when updating remaining tab data			
IA-79000	438005	RMS- MSP requests the ability to disable Add Other Agency Officer from the Incident Report Summary	Enhancement	Incidents	Software Update: New Maint val : INCIDENT_ALLOW_ADD_OTHER_AGENCY_OFFICER Default value = 'Y'
IA-78999		Offense Details not displaying correctly between screens	Bug/Defect	Incidents	Software Update:
IA-78985	430859	IL NIBRS "unparsable number" error when submitting a Zero NIBRS report	Bug/Defect	State Submissions	Software Update:
IA-78945		NIBRS Code 40C is a Society Crime need to remove Victim Type I and L	Configuration	State Submissions	Software Update: The Online RMS Incident Based Reporting has been updated to correct an error in the configuration of victims for the NIBRS Offense code of 40C- Purchasing Prostitution. Previously the configuration allows Individuals and Victims to be entered as victims of the 40C, causing NIBRS submission errors. This has been corrected to

JIRA #	Client Ticket #	Summary	Type of Issue	RMS Module	Functional Documentation
					<p>only allow Society as the victim for 40C.</p> <p>This update is applied to all RMS clients for NIBRS reporting.</p>
IA-78928		NIEM Arrest XSLT - Additional Elements	Enhancement	Interface	Software Update:
IA-78911		Evidence - bad request 400 error when taking action on schedule disposition notification	Bug/Defect	Property Mgmt.	Software Update: SMTS, FBI Number and State ID added to NIEM Arrest XML export.
IA-78876		MS XML File Submission IEPD	Enhancement	State Submissions	Software Update: The Online RMS Incident Based Reporting for Mississippi (MS NIBRS) complies with the current MS NIBRS XML Specification 1.0. MS Agencies using the RMS Incident Based Reporting can submit XML generated files from the RMS to the state for submission.
IA-78592		Form Designer - Empty Rows	Bug/Defect	Custom Forms	Software Update:
IA-78425	434269	RMS - Evidence Created from Master Index Property will not print evidence label	Bug/Defect	Property Mgmt.	Software 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.