Caliber

PUBLIC SAFETY

Protecting Tomorrow–Today.™

Online RMS

Version 11.11.3

Product Change Notice

7 March 2023

REVISION HISTORY

Revised By	Revision Date	Version	Notes
B. Chapman	7 Mar 2023	1.0	Production release.

TABLE OF CONTENTS

INTRODUCTION

This document provides an overview of the software changes delivered in the 11.11.3 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 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 11.11.3 release.

End Date	Milestone
2 Feb 2023	11.11.3 Sprint 1 Starts
2 Mar 2023	11.11.3 Code Lock
7 Mar 2023	11.11.3 Release Available

APPENDIX: 11.11.3 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 11.11.3 release. An ***** symbol - denotes a software resolution that was deployed prior to the 11.11.3 service pack installation date.

JIRA #	Client Ticket #	Summary	Type of Issue	RMS Module	Functional Documentation
IA-76772	N/A	CORIS to Online RMS Automated Data Transfer Interface	Enhancement	Interface	Interface Update: Online RMS now offers a data exchange interface supporting the import/upload of Virginia Department of Corrections CORIS inmate demographic information and an associated mugshot image.
IA-77196*	N/A	GA NIBRS: Offender Religion value reported even though Offense Bias is None	Bug/Defect	Custom Forms	Configuration Update: Modification for Georgia NIBRS reporting.
IA-77276	426687	RMS- Online Reporting Form returns unable to save form upon submission	Bug/Defect	Custom Forms	Configuration Update: Modification to internal log file storage size.

JIRA #	Client Ticket #	Summary	Type of Issue	RMS Module	Functional Documentation
IA-77330	N/A	Remove Duplicated Table Joins	Bug/Defect	Admin	Software Update: Citation employee and gang relation query logic adjusted for better performance.
IA-77366*	N/A	GA NIBRS: Turn on XML, set custom field lengths and turn off flat file	Enhancement	State Submissions	Configuration Update: Modification for Georgia NIBRS reporting.
IA-77391	N/A	Online RMS-Install script for release 11.11.3	DevTask	Admin	Online RMS- Install script for release 11.11.3
IA-77402	N/A	CAPS eCite - XSLT Charge Code Mapping Adjustment	Bug/Defect	Interface	Software Update: The CAPS eCite XML translation has been adjusted to concatenate the eCite Charge Code with the ACD Code and map this unique combination to the RMS Charge Code.
IA-77404	427271	NDEx Interface connection update after software migration	Configuration	Interface	Configuration Update: Agency security file updated to submit to N-DEx.
IA-77414*	N/A	GA NIBRS: Victim Religion and other Bias related Victim custom fields reported even though Offense Bias is None	Bug/Defect	State Submissions	Configuration Update: Modification for Georgia NIBRS reporting.

JIRA #	Client Ticket #	Summary	Type of Issue	RMS Module	Functional Documentation
IA-77477	N/A	RMSDEx / LInX Extract - Restrict Supplemental Narratives	Enhancement	Interface	Interface Update: The incident extract now includes an option for only including the original report narrative(s).

--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.