



Protecting Tomorrow–Today.™

Online RMS

Version 11.13.2

Product Change Notice

3 October 2023

REVISION HISTORY

Revised By	Revision Date	Version	Notes
B. Chapman	3 October 2023	1.0	Production release.

TABLE OF CONTENTS

Revision History	1
Introduction	3
Product Requirements.....	4
Release Milestones.....	5
Appendix: 11.13.2 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 11.13.2 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 11.13.2 release.

End Date	Milestone
28 Sep 2023	11.13.2 Code Lock
03 Oct 2023	11.13.2 Release Available

APPENDIX: 11.13.2 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 11.13.2 release. An * symbol - denotes a software resolution that was deployed prior to the 11.13.2 service pack installation date.

JIRA #	Client Ticket #	Summary	Type of Issue	RMS Module	Functional Documentation
IA-78605		PORT - Citation Import - Winona PD	PORT	Interface	Software Update: Citation Import
IA-78583		PORT - SAML - 'Content is not Allowed in Prologue' Error parsing IDP meta data URL	PORT	Security	Software Update: Modification to correct SAML issue
IA-78582		SAML - 'Content is not Allowed in Prologue' Error parsing IDP meta data URL	Bug/Defect	Security	Software Update: Modification to correct SAML issue
IA-78556		PORT - Incident Approval - Notify Prosecutor	PORT	Incidents	Software Update: Modification to update table value
IA-78553		Add XML format for RMS Jail Tracker Interface Web Services	Engineering Enhancement	Interface	Software Update: Interface update
IA-78539		Citation Import - Winona PD	Configuration	Interface	Software Update: Citation Import

JIRA #	Client Ticket #	Summary	Type of Issue	RMS Module	Functional Documentation
IA-78528		Citation Form Caching - Disable	Bug/Defect	Citations/Stops	Software Update: Modification to disable Citation Caching
IA-78527		Incident Approval - Notify Prosecutor	Bug/Defect	Incidents	Software Update: Modification to update table value
IA-78459		Charge Code table search not working past first page	Bug/Defect	Admin	Software Update: Modification to correct search
IA-78436	434194	RMS- Security Group cannot be added	Bug/Defect	Security	Software Update: Modification to correct security group addition
IA-78414		Warrant Upload - Process New Log Entries	Enhancement	Interface	Software Update: Modification for additional log entries
IA-78189	432675	NE NIBRS Additional Data Elements	Enhancement	State Submissions	Software Update: Modification to include additional NE NIBRS elements

--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.