Caliber PUBLIC SAFETY

Protecting Tomorrow–Today.™

Online RMS

Version 11.16.2

Product Change Notice

1 October 2024

REVISION HISTORY

Revised By	Revision Date	Version	Notes
B. Chapman	1 October 2024	1.0	Service Pack Available

TABLE OF CONTENTS

INTRODUCTION

This document provides an overview of the software changes delivered in the 11.16.2 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 11.16.2 release.

End Date	Milestone
24 SEPT 2024	11.16.2 Code Lock
01 OCT 2024	11.16.2 Service Pack Available

APPENDIX: 11.16.2 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 11.16.2 release. An ***** symbol - denotes a software resolution that was deployed prior to the 11.16.2 service pack installation date.

JIRA #	Client Ticket #	Summary	Type of Issue	RMS Module	Functional Documentation
IA-79991		IL IBR Create error message for location not having ZIP Code	Enhancement	State Submissions	The Online RMS Incident Based reporting for the state of Illinois (IL NIBRS) has been updated to include a validation to require the Zip Code be entered on the Incident Address. This validation is enforced on the Incident Approval and a Zip Code must be entered for the Incident prior to submittal for approval. This validation only applies to IL NIBRS and will not be enforced for other RMS clients that are not in the state of Illinois.
***IA-80016**		View Narrative is throwing an unexpected error IL57 McLean	Bug/Defect	Incidents	

JIRA #	Client Ticket #	Summary	Type of Issue	RMS Module	Functional Documentation
IA-80025		SOLR Indexing of People is causing Issues for some Schemas	Release Defects	Searching	The Online RMS SOLR searching for people has been updated to fix an issue with indexing on certain schemas where a person had a large number of collapsed records with miscellaneous IDs.
IA-79959		IL NIBRS Delete Submission File Invalid Schema	Bug/Defect	State Submissions	The Online RMS Incident Based Reporting for the state of Illinois (IL NIBRS) has been updated to correct an issue with the Incident Delete submission. This issue is IL NIBRS specific and has been corrected for IL NIBRS RMS Users. This issue did not impact other NIBRS clients and the fix has no impact on non Illinois Users.
IA-79960		Incident - saving header information resets current supp security level	Bug/Defect	Incidents	
IA-79982		Personnel - verify employee signature PIN against active users only	Bug/Defect	Property Mgmt	
IA-80009		Increase text size on evidence label	Bug/Defect	Property Mgmt	
IA-80018		McLean County - Intake Notifications	Enhancement	Admin	

JIRA #	Client Ticket #	Summary	Type of Issue	RMS Module	Functional Documentation
		Need to Make Offense as Part of Description			
IA-80022	444071	Court Paper Custom Fields Duplicating	Bug/Defect	Civil Process	
IA-80002		Auto match Configuration - McLean	Configuration	Interface	Additional auto-match criteria introduced for xml upload processing.
IA-80015		Online RMS- Install script for 11.16.2	DevTask	Admin	
IA-80030		CAD Spill Lat Long breaking incident mapping	Bug/Defect	RMS_CAD	The Online RMS CAD Interface has been updated to correct the latitude on the CAD transfer to the RMS Calls for service. In some cases the CAD was sending the latitude with a leading + before the latitude value, this was causing issues when the latitude, longitude is mapped using the RMS Mapping. This issue has been corrected in the CAD to RMS Interface and any existing data with the + in the latitude has been corrected.

--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.