

eCASE Audit

Release Notes

v11.14.2.0

November 2025



OPEXUSTECH.COM

© AINS LLC, 2025



eCase Audit v11.14.2.0 Release Notes

Notice of Rights

Copyright © 2025, OPEXUS, LLC d/b/a OPEXUS. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the publisher: OPEXUS, LLC. For information on obtaining permission for reprints and excerpts, contact info@opexustech.com.

Additionally, all copyrights, confidential information, patents, design, rights and all other intellectual property rights of whatsoever nature contained herein are, and shall remain, the sole and exclusive property of the publisher.

Notice of Liability

The information in this publication is believed to be accurate and reliable. However, the information is distributed by the publisher (OPEXUS, LLC.) on an “As Is” basis without warranty for its use, or for any infringements of patents or other rights of third parties resulting from its use.

While every precaution has been taken in the preparation of this publication, neither the author (or authors) nor the publisher will have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused, directly or indirectly, by the information contained in this publication or by the computer software and hardware products described in it.

Notice of Trademarks

The publisher's company name, company logo, company patents, and company proprietary products are trademarks or registered trademarks of the publisher: OPEXUS, LLC. All other trademarks or registered trademarks are the property of their respective owners.

Non-Disclosure Statement

This document's contents are confidential and proprietary to OPEXUS, LLC. This document cannot be released publicly or outside the purchasing agency without prior written permission from OPEXUS, LLC.

Images in this manual are used as examples and may contain data and versioning that may not be consistent with your version of the application or information in your environment.

Additional Notice

Information in this documentation is subject to change without notice and does not represent a commitment on the part of OPEXUS, LLC.



Overview

Notwithstanding any of the foregoing, if this document was produced as a Deliverable or other work for hire under a contract on behalf of a U.S. Government end user, the terms and conditions of that contract shall apply in the event of a conflict.





Product Enhancements

1.1 Multi-Select Support for Adding Staff Roles

ID# 1325400

The Staff assignment workflow in Audit management has been enhanced to restore multi-selection capabilities.

Select an option

All ▾

✕

🔍

<input type="checkbox"/>	User Name	Full Name	Email	Office
<input checked="" type="checkbox"/>	1001			HQ - Headquar
<input type="checkbox"/>	AD			1234 - CP
<input checked="" type="checkbox"/>	Admin	Admin Admin	deployments@casepoint.in	1234 - CP

OK

Cancel

When adding staff, users can search within the User Lookup field after selecting a role. The search results now display selectable checkboxes that allow multiple users to be assigned to the selected role at once, improving efficiency in role management across teams.





Bug Fixes

ID	Description
1351633	Fixed an issue causing Audit Reports to fail during Production Export, ensuring accurate data retrieval and successful report generation.
1321413	Rectified the spell-check functionality within Audit Management, so they operate reliably during content editing.





Security Enhancements

ID	Description
1324866	Fixed a stored XSS vulnerability in Project Setup by sanitizing and escaping user comments, preventing malicious code execution and protecting users from unauthorized actions or data exposure.
1324866	Resolved a stored XSS issue in Estimated Staff Hours by ensuring proper sanitization of user inputs, preventing script execution on the Project Cost tab, and safeguarding user sessions and sensitive data.

