KNOWLEDGE BASE ARTICLE

How to Review and Export the Policy Audit Log

2026 © Vitextra SIA. All rights reserved.

Disclaimer

For the purposes of this Disclaimer:

- **Company** (referred to as either "the Company", "We", "Us" or "Our" in this Disclaimer) refers to Vitextra SIA, LV-1009 Riga, Matise iela 61 - 25.
- **Document** refers to the Knowledgebase Article.
- **You** means the individual accessing the Document, or the company, or other legal entity on behalf of which such individual is accessing or using the Document, as applicable.
- **Website** refers to Vitextra, accessible from https://vitextra.com

Disclaimer

The information contained in the Document is for general information purposes only.

The Company assumes no responsibility for errors or omissions in the contents of the Document.

In no event shall the Company be liable for any special, direct, indirect, consequential, or incidental damages or any damages whatsoever, whether in an action of contract, negligence, or other torts, arising out of or in connection with the use of the contents of the Document. The Company reserves the right to make additions, deletions, or modifications to the contents in the Document at any time without prior notice.

Errors and Omissions Disclaimer

The information given by the Document is for general guidance on matters of interest only. Therefore, errors can occur even if the Company takes every precaution to ensure that the Document's content is current and accurate. Plus, given the changing nature of laws, rules, and regulations, there may be delays, omissions, or inaccuracies in the information contained in the Document.

The Company is not responsible for any errors or omissions, or for the results obtained from the use of this information.

Fair Use Disclaimer

The Company may use copyrighted material that the copyright owner has not explicitly authorized. The Company is making such material available for criticism, comment, news reporting, teaching, scholarship, or research.

The Company believes this constitutes a "fair use" of any such copyrighted material as provided for in section 107 of the United States Copyright law.

If You wish to use copyrighted material from the Document for your own purposes that go beyond fair use, You must obtain permission from the copyright owner.

"Use at Your Own Risk" Disclaimer

All information in the Document is provided "as is", with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this information, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, merchantability and fitness for a particular purpose.

The Company will not be liable to You or anyone else for any decision made or action taken in reliance on the information given by the Service or for any consequential, special or similar damages, even if advised of the possibility of such damages.

Contact Us

If you have any questions about this Disclaimer, You can contact Us by email: support@vitextra.com.

Table of contents

Open the correct log 4

Interpret the events 4

Export the loaded entries 5

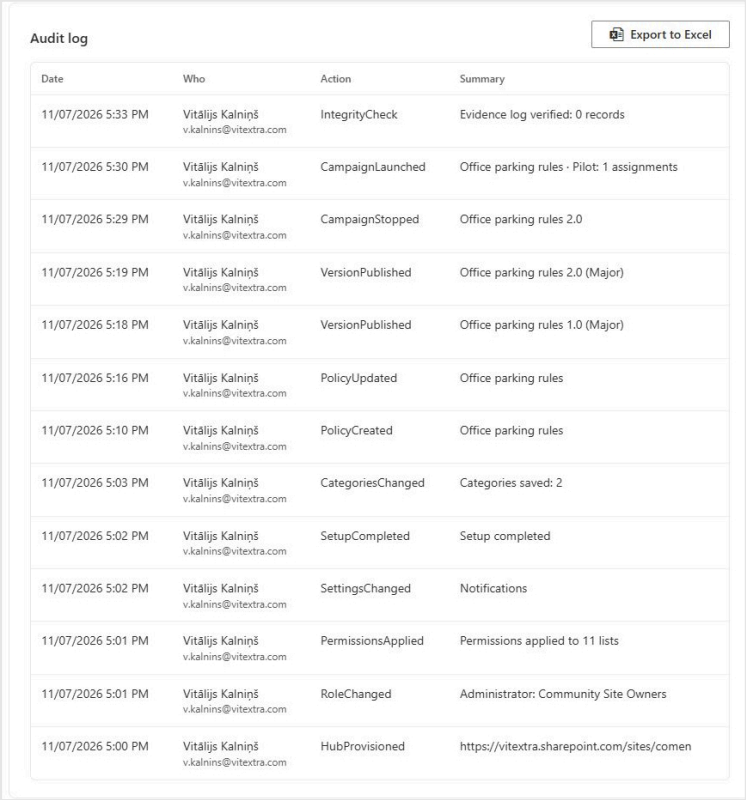
Build an investigation record 5

The audit log records selected administrative and operational actions in Policy Acknowledgement. It helps an administrator establish who launched a campaign, changed settings or published a version. Employee confirmations are stored separately in the acknowledgement log, so an audit export alone is not a complete evidence package.

Open the correct log

1 Open Policy Admin connected to the hub you want to investigate.
2 Sign in with an administrator account that can read the audit list.
3 Select **Audit log**.
4 Review the event time, actor, action and summary. Confirm that the policy, campaign or other identifier relates to your investigation.
5 Compare the event with the current policy or campaign record rather than assuming the summary describes its present state.

The tab loads the latest 500 entries in descending record-ID order. It has no paging control for retrieving the rest of the history. This is a display and export limit, not a statement that older records are automatically deleted from the underlying list.



Recent administrative events in the audit log

Interpret the events

Events cover operations such as policy creation and updates, version publication,

status changes, review confirmation, campaign launch and stop, reminders, role and permission changes, settings, categories, provisioning, integrity checks and report export. Action identifiers and stored summaries may remain in the language in which they were written; changing the interface language does not translate historical event data.

Read the timestamp together with the record identifier and actor. The interface uses the event timestamp, falling back to the item's creation time where necessary. An event indicates that the application attempted or recorded the associated operation; assess the underlying records when determining the final outcome.

Warning

Business updates and audit writes are separate operations. A policy or campaign change can succeed even if the subsequent audit write fails. Conversely, the absence of an event from the latest 500 entries does not prove that the action never happened. The tab is not a complete SharePoint security or change log.

Export the loaded entries

Select **Export to Excel** and save the workbook in an approved location. The file name follows `PolicyAuditLog_YYYY-MM-DD.xlsx`. The export includes the loaded events and adds the actor account and serialized details to the information visible in the table.

Inspect the details column for identifiers and context that do not fit into the summary. Treat these values as recorded application data, not a reconstructed history of every field change. Check the oldest exported event before describing the workbook as covering a requested period.

If the investigation needs events outside this window, ask the administrator responsible for the hub to retrieve the relevant underlying records using an approved method. There is no full-history export button in this tab. Preserve the original workbook and document any filters or extracts prepared from it.

Build an investigation record

Record the hub URL, export time, affected record identifiers, observed error and relevant event times. Compare campaign events with assignments, publication events with version history and employee confirmations with their receipts and acknowledgement records. A normal acknowledgement should not be considered

missing merely because it is absent from this administrative tab.

Avoid editing or deleting log entries to correct a business mistake. Correct the underlying configuration or workflow through its supported interface and retain the prior evidence. Restrict access to exports because actor accounts and details can contain employee information.

Tip

For employee receipt details, see KB10526. How to View Previous Policy Acknowledgements and Receipts. For the separate hash-chain check, see KB10533. How to Check the Integrity of the Acknowledgement Log. An audit export and an integrity result answer different questions and should be interpreted together with the underlying business records.