KNOWLEDGE BASE ARTICLE

Policy Acknowledgement Data Storage: Direct and Service Modes

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

What the hub stores 4

Compare recording modes 4

Configure and verify a mode change 6

Follow the record through the application 7

Separate the checks needed for a mode change 7

Interpret integrity as one part of protection 8

Understand the evidence boundary 8

Policy Acknowledgement stores its working data on a SharePoint policy hub. The recording mode determines how normal employee acknowledgements are written. It does not move the solution's data to a different storage site.

What the hub stores

List or library	Purpose
`Policies`	Policy cards, current version and reading controls.
`PolicyVersions`	Version metadata and document snapshots where supported.
`PolicyCategories`	Categories and their confirmation texts.
`PolicyCampaigns`	Audience definitions, deadlines and reminder settings.
`PolicyAssignments`	Employee assignments and their current status.
`PolicyAcknowledgements`	Confirmation and other evidence events with chained hashes.
`PolicyQuestions`	Employee questions, reasons and responses.
`PolicyNotificationLog`	Notification-log storage.
`PolicyAuditLog`	Administrative and workflow events.
`PolicySettings`	Product settings.
`PolicyRoleAssignments`	Role-to-group mappings.

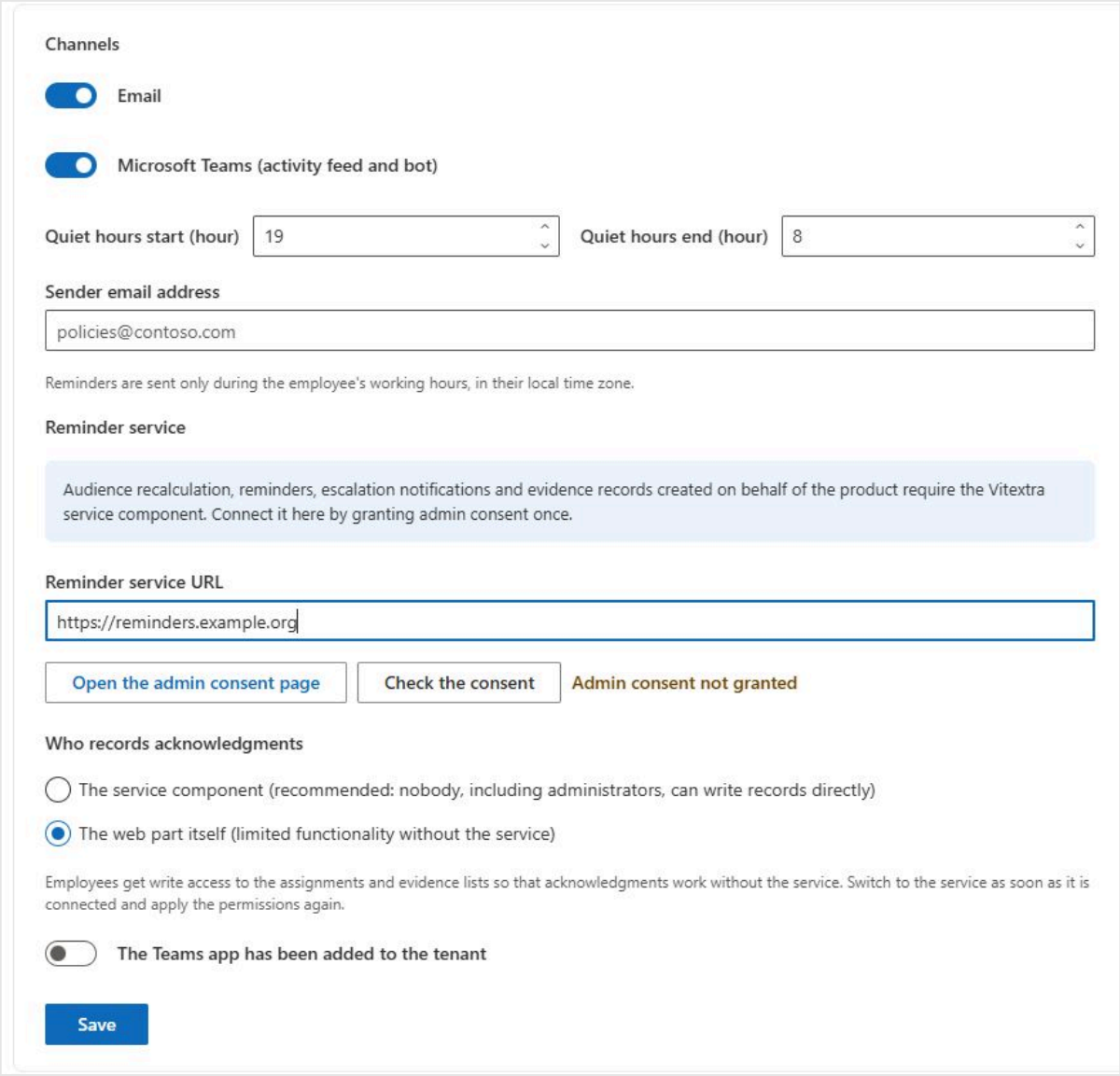
Source documents remain at their configured URLs. Publishing a same-origin document can save a snapshot in `PolicyVersions`; external sources do not receive such a snapshot or a content hash.

Compare recording modes

Aspect	Direct	Service
Normal acknowledgement	The web part writes to	The web part sends the

Aspect	Direct	Service
write	SharePoint using the employee's session.	acknowledgement to the connected service.
Employee permissions in the role matrix	Contribution on assignments and acknowledgements.	Read access on those two lists.
Separate service required for this write	No.	Yes, with a working endpoint and consent.
Automated reminders and audience updates	Not supplied by Direct mode.	Depend on the connected service's implementation and operation.

Direct mode is the default setting. Selecting Service does not install the service or verify all its operational behavior.



Choosing the acknowledgement recording mode

Configure and verify a mode change

1 Open **Notifications** in Policy Admin.
2 For Service mode, enter **Reminder service URL**, open administrator consent and run **Check the consent**.
3 Choose the required option under **Who records acknowledgments** and save.
4 Open **Roles** and select **Save and apply permissions**.
5 Inspect effective SharePoint permissions and test a confirmation using a separate employee account.

Saving a mode setting does not reapply permissions automatically. The reader blocks normal submission when Service mode lacks a URL or confirmed consent; a later service outage is reported as a submission error.

Follow the record through the application

The card, assignment and acknowledgement are different records. The card describes the current policy; the assignment identifies a person's work for a version and campaign; the acknowledgement records an evidence event. A receipt displays selected evidence fields. These records usually agree after a successful submission, but they should not be treated as one atomic object.

In the direct path, the application reads the preceding hash, appends the acknowledgement and updates the assignment. In the service path, it sends the payload to the configured endpoint and retrieves the resulting record. A later read or update can fail even if an earlier write succeeded. This is why investigation should compare the assignment reference and evidence record before asking an employee to retry.

Changing recording mode changes the path for ordinary acknowledgements, not the location of all policy data or every administrative operation. It also does not rewrite earlier events into a new evidence model. Keep the original records and inspect how the deployment's effective permissions and service behavior support the intended protection requirements.

Separate the checks needed for a mode change

Check	What to verify
Configuration	The saved mode, endpoint and consent status match the intended setup.
Permissions	The product matrix was reapplied and actual list rights were inspected.
Employee confirmation	A representative employee can submit and obtain the correct receipt.
Assignment reconciliation	The matching assignment has the expected status and evidence reference.
Exception workflow	An authorized operator can resolve a test case, including the separate exemption path where used.
Background work	The service owner can demonstrate the required scheduled jobs and delivery

Check	What to verify
	behavior.

Perform these checks with accounts that represent the production roles. Testing only as the synchronizing administrator can conceal the additional Full Control grant that account retains. Likewise, a successful consent response does not establish that all server-side writing, scheduling and delivery operations are healthy.

Interpret integrity as one part of protection

A hash chain links records so that a changed record or certain missing records can produce a mismatch. It does not supply an independent trusted inventory of everything that should exist. Removing the end of a chain or replacing an entire chain can require other controls or retained evidence to detect. The green indicator therefore means that the loaded chain passed the implemented consistency checks.

Use the integrity result together with permissions, source/version evidence and operational records. A matching record hash does not prove that the reader displayed an archived file, that every required employee event exists or that the employee understood the text. If you find an inconsistency, preserve identifiers and original data before making corrective changes; see KB10533. How to Check the Integrity of the Acknowledgement Log and KB10538. Troubleshooting Failed Acknowledgements and Missing Notifications.

Understand the evidence boundary

An evidence event includes identity, policy and version information, a timestamp, confirmation text, reading-control data and hashes. The application checks a chain of record hashes to detect inconsistencies. This is not an absolute immutability guarantee.

Warning

The interface describes Service mode as preventing direct writes even by administrators, but the current permission-sync code retains Full Control for the account performing synchronization. Elevated or existing grants also require inspection. Direct mode grants employees contribution rights, and the matrix does not isolate records per employee. Do not claim that all evidence is technically immutable or that web-part filtering provides record-level security.

Exemption events currently use a direct SharePoint write even in Service mode. That path can fail for a compliance manager with only the documented matrix permissions. See KB10507. How to Handle Policy Questions and Exempt Employees. The separate service implementation is not part of the web-part project, so its application permissions, background processing and protection controls must be verified in the actual deployment.