KNOWLEDGE BASE ARTICLE

Troubleshooting Policy Hub Detection and Access

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

Record the symptom 4

Verify the hub connection 4

Check structure and permissions separately 4

Narrow the failure with a comparison matrix 5

Avoid broad changes while isolating the cause 6

Verify the repair 6

A hub-detection error and an access-denied message have different causes. Start by identifying whether the web part can locate the hub, whether the signed-in account can read its data and whether the application can resolve the required role. Recreating the hub is not the first diagnostic step.

Record the symptom

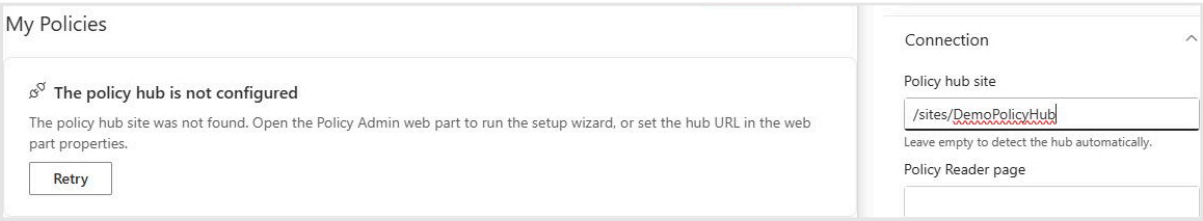
Note the page URL, web part, signed-in account, expected hub URL and exact message. Check whether the problem affects all users, one role or only one page. An administrator succeeding on a page does not prove that employees have the same list or source permissions.

If the interface explicitly reports an expired licence, route that issue to the administrator responsible for the product licence. Do not treat it as evidence that the policy lists have disappeared. Preserve the message before changing configuration.

Verify the hub connection

1 Edit the affected page and inspect **Policy hub site** in the web-part properties.
2 Compare it with the intended SharePoint hub site, not the URL of an individual policy or document.
3 Open the intended site directly with the affected account.
4 Ask an administrator to verify that the product settings list and the expected product lists exist there.
5 Save any corrected connection and reload the page before testing again.

The resolver considers the configured site, the current site and the default `/sites/VitextraPolicies` location. It uses the presence of the settings list to identify a hub and caches the resolved connection. A page can therefore point at a different available hub than the one you expected; compare actual data as well as the property value.



Checking the page connection to the intended hub

Check structure and permissions separately

The setup readiness check expects 11 product lists and libraries. The presence of all expected names does not establish that every permission and setting is correct. If

structure is incomplete, have an administrator inspect the existing hub and use the supported setup process to add missing components; do not delete existing records to make setup start again.

Next, verify the affected account's assigned product role and actual SharePoint access. Administrative and reporting web parts require the appropriate role, while the underlying lists and source documents have their own permissions. A visible page does not grant access to its data or documents.

Role resolution also depends on directory and group information. A failed group-membership lookup can leave the application without the expected role even when the administrator believes the user belongs to the group. Check the browser's reported errors and directory access before changing role assignments blindly.

Warning

Applying the product permission matrix changes permissions on product lists. Review the intended roles and preserve administrator access before selecting **Save and apply permissions**. Product roles and owner-based interface filtering are not a substitute for inspecting effective SharePoint permissions.

Narrow the failure with a comparison matrix

Compare the same operation across accounts and pages before changing permissions. This reveals whether the problem follows the person, the page connection or the underlying hub. Use a representative account rather than assuming an administrator's success demonstrates ordinary access.

Comparison	Likely area to inspect next
The same user works on another page connected to the intended hub	The failing page's connection and navigation properties.
An administrator works, but an employee fails on the same page	Role resolution, effective list rights and source access for the employee.
The site opens, but policy data does not load	Product lists, permissions and the resolved hub.
The card loads, but the document is denied	The source document's access rather than hub discovery alone.
Several roles fail after a configuration	The changed hub, role or permission

Comparison	Likely area to inspect next
change	settings and any partial synchronization.

These comparisons guide investigation; they are not proof of one cause. For example, a group lookup failure can look like missing role membership, while a page pointing to another valid hub can show different records without a hub-not-found message. Preserve the exact error and the actual resolved data context.

Avoid broad changes while isolating the cause

Do not create a replacement hub merely because one page fails. First establish whether the original data is still present and accessible to the responsible administrator. A second hub can split navigation and make employees appear to have different tasks on different pages.

Similarly, do not add everyone to an administrative group to test ordinary access. Such a test bypasses the condition you need to verify. Correct the identified connection or permission issue, reload the page and repeat the same operation with the original affected account.

If permission application failed partway through, inspect the affected lists rather than assuming the whole matrix was rolled back. The operation applies permissions across multiple lists. Record where the failure occurred, preserve administrator access and verify the completed configuration afterward. Use KB10500. How to Configure Policy Acknowledgement Roles and Permissions for a representative access test and KB10536. Troubleshooting Missing Policies, Employees and Assignments when access works but expected records remain absent.

Verify the repair

Reload the affected page with the affected account. Confirm that the expected policies appear and that a permitted action succeeds. Test the source document separately. If only one page fails, compare its hub and reader-page properties with a working page rather than changing tenant-wide access.

For escalation, provide the hub and page URLs, account, role, message, time and whether direct site access works. Include relevant error details without authentication tokens or sensitive employee records. See KB10496. Policy Acknowledgement: Quick Start Guide for the product's storage and connection model and KB10500. How to Configure Policy Acknowledgement Roles and Permissions for roles and permissions.