KNOWLEDGE BASE ARTICLE

How to Configure Policy Acknowledgement Roles and Permissions

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

Understand the roles 4

Assign groups 4

Understand what applying permissions changes 5

Separate audience, ownership and permission 6

Use a representative access test 6

Maintain access after organizational changes 7

Verify and maintain access 7

Product roles control which operations and views are available in Policy Acknowledgement. Policy Admin also applies role-based SharePoint permissions to the hub lists. Review both layers when designing access.

Understand the roles

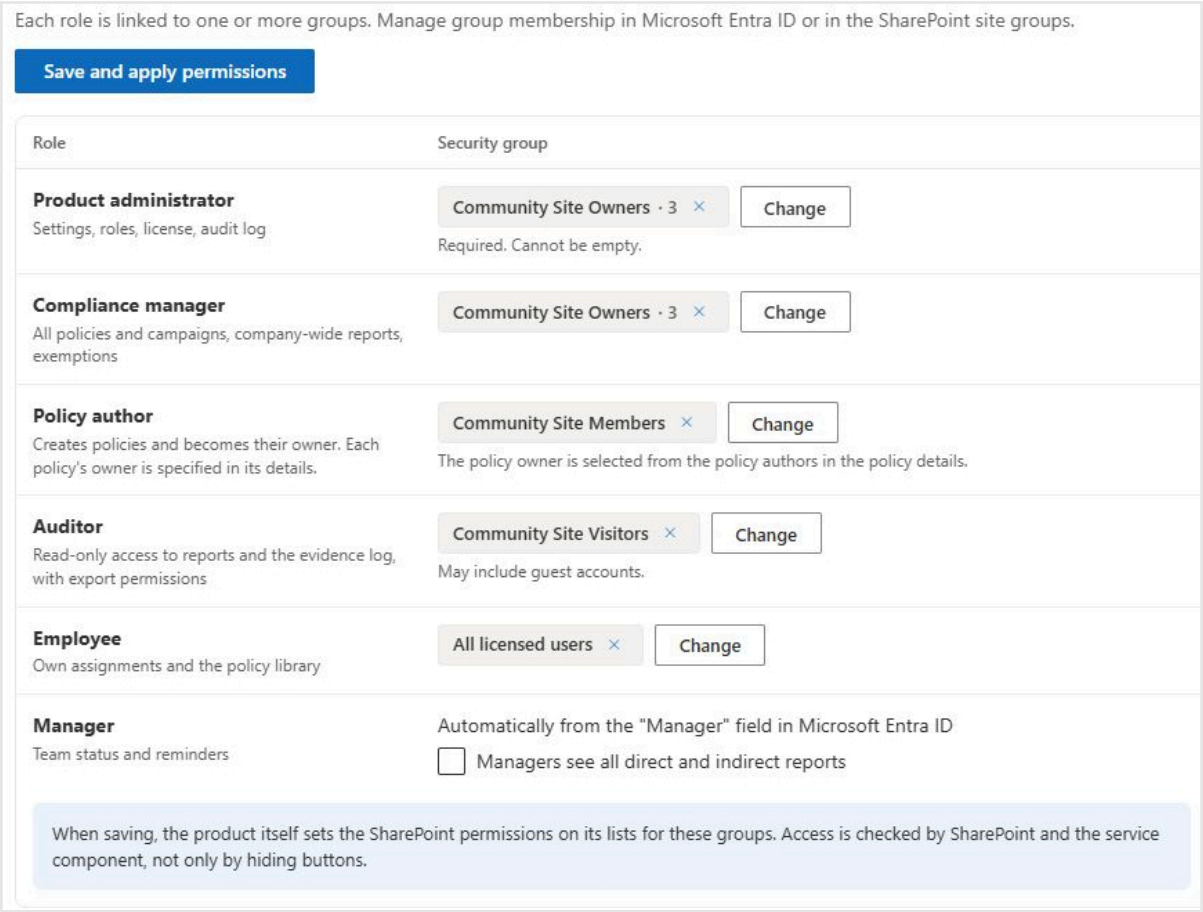
Role	Main use in the web parts
Product administrator	Setup, settings, roles and administration; management and reporting access.
Compliance manager	Policies, campaigns, reports and exemptions across the product.
Policy author	Creating policies and managing policies owned by that author.
Auditor	Reporting and inspection without policy-management actions.
Employee	Personal assignments and policy content.

Team-manager scope is derived from reporting relationships, with a setting for direct reports or the whole reporting branch. It is not a sixth role assignment in the Roles list. Ownership is stored on each policy; the author view filters policies by that owner.

Assign groups

1 Open Policy Admin as a product administrator and select **Roles**.
2 Select Entra ID security groups or SharePoint groups belonging to the hub site for the required roles.
3 Keep at least one group for **Product administrator**.
4 Review the employee population and **Managers see all direct and indirect reports**.
5 Select **Save and apply permissions** and wait for synchronization to finish.

Use explicit employee groups when a precise access boundary is required. Although the interface offers **All licensed users**, the current role resolver treats that option as matching the current user without a license check. It must not be used as proof that access is restricted to licensed accounts.



Product roles and assigned groups

Understand what applying permissions changes

Synchronization grants site read access for role groups, breaks permission inheritance on the product lists and applies the list permission matrix. The account performing synchronization retains Full Control on those lists. Review the impact before applying this to an existing shared site.

In Direct mode, employees receive contribution rights on assignments and acknowledgement records. In Service mode, the employee entries in that matrix are read-only for those two lists. Employees retain contribution rights on questions. A user with several roles can receive the combined permissions of their groups.

Warning

Policy-owner filtering and personal assignment filtering are implemented in the web parts. The permission matrix is list-level, not per-policy or per-employee isolation. Do not present these filters as a guarantee that users cannot access other records through SharePoint. A successful synchronization also does not prove that every pre-existing or elevated grant has been revoked.

Separate audience, ownership and permission

These concepts answer different questions. A campaign audience decides who should receive a task. The policy owner determines responsibility and the author-filtered management view. A role enables product actions, while SharePoint permissions govern access to the stored records. Changing one does not automatically accomplish the others.

For example, assigning a policy to the finance department does not make its underlying list records private to finance. Moving a card to another owner changes which author should manage it, but is not a per-item permission transfer. Hiding a management page in portal navigation also does not revoke a user's existing list access.

Design role groups around responsibilities, then review effective data access for those groups. Where a person belongs to several groups, test that combined membership. A user with an author role and an administrative group may see or change much more than an author-only test account. Removing one membership may leave access through another group or an elevated site permission.

Use a representative access test

Test account	Application check	Additional access check
Administrator	Open Policy Admin and inspect the configured roles.	Confirm that expected administration remains available after synchronization.
Author	Open owned policies and verify the intended management actions.	Inspect actual list permissions rather than inferring isolation from the filtered view.

Test account	Application check	Additional access check
Auditor	Open the relevant report and download an allowed export.	Check whether actions that save a result or audit event require additional write access.
Employee	Open an assigned policy and submit a pilot confirmation.	Verify source access and the configured evidence-writing path.
Manager	Load the expected reporting team.	Check the effective data access and the scope behavior independently.

Some apparently read-oriented actions also write data. For example, an integrity check saves its outcome, and a report export writes an audit event after generating the file. A read-only account can therefore see useful output and then encounter a write error. Investigate the specific failed operation before broadening its role.

Maintain access after organizational changes

When an author changes jobs, review both group membership and ownership of the policies they maintained. When managers change, inspect directory relationships and stored assignment manager fields; a page reload does not rewrite historical assignments. When the recording mode changes, review the service and reapply the corresponding permission matrix.

Keep a short record of who applied permissions, which groups were intended and which representative tests passed. The synchronizing account retains Full Control, so assess it explicitly rather than assuming that a service-mode label means all human accounts are read-only. The whole-branch setting is likewise not enforced by the current Team Compliance selector; see KB10530. Team Compliance: How to Monitor Your Team and Follow Up for the resulting reporting limitation.

Verify and maintain access

Test with separate administrator, author, reporting and employee accounts. Confirm both the intended pages and the underlying list permissions. After changing the acknowledgement recording mode, run **Save and apply permissions** again and inspect the effective rights. See KB10509. Policy Acknowledgement Data Storage: Direct and Service Modes for the recording modes and their limitations.