WISSENSDATENBANKARTIKEL

Rollen und Berechtigungen in Policy Acknowledgement konfigurieren

2026 © Vitextra SIA. Alle Rechte vorbehalten.

Haftungsausschluss

Für die Zwecke dieses Haftungsausschlusses:

- **Das Unternehmen** (in diesem Haftungsausschluss entweder als „das Unternehmen“, „wir“, „uns“ oder „unser“ bezeichnet) bezieht sich auf Vitextra SIA, LV-1009 Riga, Matīsa iela 61 – 25.
- **Dokument** verweist auf den Wissensdatenbank-Artikel.
- **Sie** sind die Person, die auf das Dokument zugreift, bzw. das Unternehmen oder eine andere juristische Person, in deren Namen eine solche Person auf das Dokument zugreift oder es nutzt.
- **Die Website** verweist auf Vitextra, zugänglich über https://vitextra.com

Haftungsausschluss

Die in diesem Dokument enthaltenen Informationen dienen nur der allgemeinen Information.

Das Unternehmen übernimmt keine Verantwortung für Fehler oder Auslassungen im Inhalt des Dokuments.

In keinem Fall haftet das Unternehmen für besondere, direkte, indirekte oder zufällige Schäden oder für Schäden jeglicher Art, die sich aus der Nutzung des Inhalts des Dokuments ergeben, unabhängig davon, ob es sich um eine Klage aufgrund von Vertrag, Fahrlässigkeit oder anderen Delikten handelt. Das Unternehmen behält sich das Recht vor, den Inhalt des Dokuments jederzeit und ohne vorherige Ankündigung zu ergänzen, zu streichen oder zu ändern.

Haftungsausschluss für Fehler und Auslassungen

Die in dem Dokument enthaltenen Informationen dienen lediglich als allgemeine Orientierungshilfe zu Fragen von Interesse. Daher können Fehler auftreten, auch wenn das Unternehmen alle Vorsichtsmaßnahmen ergreift, um sicherzustellen, dass der Inhalt des Dokuments aktuell und korrekt ist. Außerdem kann es angesichts der sich ändernden Gesetze, Regeln und Vorschriften zu Verzögerungen, Auslassungen oder Ungenauigkeiten bei den in diesem Dokument enthaltenen Informationen kommen.

Das Unternehmen haftet nicht für etwaige Fehler oder Auslassungen oder für die Ergebnisse, die sich aus der Verwendung dieser Informationen ergeben.

Haftungsausschluss für faire Nutzung

Das Unternehmen darf urheberrechtlich geschütztes Material verwenden, das der Urheberrechtsinhaber nicht ausdrücklich genehmigt hat. Das Unternehmen stellt dieses Material für Kritik, Kommentare, Berichterstattung, Schulung, Wissenschaft oder Forschung zur Verfügung.

Das Unternehmen ist der Ansicht, dass dies eine „faire Nutzung“ von urheberrechtlich geschütztem Material im Sinne von Abschnitt 107 des US-Urheberrechtsgesetzes darstellt.

Wenn Sie urheberrechtlich geschütztes Material aus dem Dokument für Ihre eigenen Zwecke verwenden möchten, die über eine angemessene Nutzung hinausgehen, müssen Sie die Erlaubnis des Urheberrechtsinhabers einholen.

„Benutzung auf eigene Gefahr“ Haftungsausschluss

Alle Informationen in diesem Dokument werden im Ist-Zustand zur Verfügung gestellt, ohne Garantie auf Vollständigkeit, Genauigkeit, Aktualität oder auf die Ergebnisse, die sich aus der Verwendung dieser Informationen ergeben, und ohne jegliche ausdrückliche oder stillschweigende Garantie, einschließlich, aber nicht beschränkt auf Garantien für Leistung, Marktgängigkeit und Eignung für einen bestimmten Zweck.

Das Unternehmen haftet weder Ihnen noch anderen gegenüber für Entscheidungen oder Handlungen, die im Vertrauen auf die Informationen des Dienstes getroffen wurden, noch für Folgeschäden, besondere oder ähnliche Schäden, selbst wenn auf die Möglichkeit solcher Schäden hingewiesen wurde.

Kontaktieren Sie uns

Wenn Sie Fragen zu diesem Haftungsausschluss haben, können Sie uns per E-Mail kontaktieren: support@vitextra.com.

Inhaltsverzeichnis

Rollen verstehen 4

Gruppen zuweisen 4

Auswirkungen der Berechtigungsanwendung verstehen 5

Zielgruppe, Verantwortung und Berechtigung trennen 6

Einen repräsentativen Zugriffstest verwenden 6

Zugriff nach organisatorischen Änderungen pflegen 7

Zugriff prüfen und pflegen 8

Produktrollen steuern, welche Aktionen und Ansichten in Policy Acknowledgement verfügbar sind. Policy Admin wendet außerdem rollenbasierte SharePoint-Berechtigungen auf die Hublisten an. Berücksichtigen Sie bei der Zugriffsplanung beide Ebenen.

Rollen verstehen

Rolle	Hauptverwendung in den Webparts
Produktadministrator	Einrichtung, Einstellungen, Rollen und Administration sowie Verwaltungs- und Berichtszugriff.
Compliance-Manager	Richtlinien, Kampagnen, Berichte und Befreiungen im gesamten Produkt.
Richtlinienautor	Erstellen von Richtlinien und Verwalten der Richtlinien dieses Autors.
Auditor	Berichte und Prüfungen ohne Aktionen zur Richtlinienverwaltung.
Mitarbeitende	Persönliche Zuweisungen und Richtlinieninhalte.

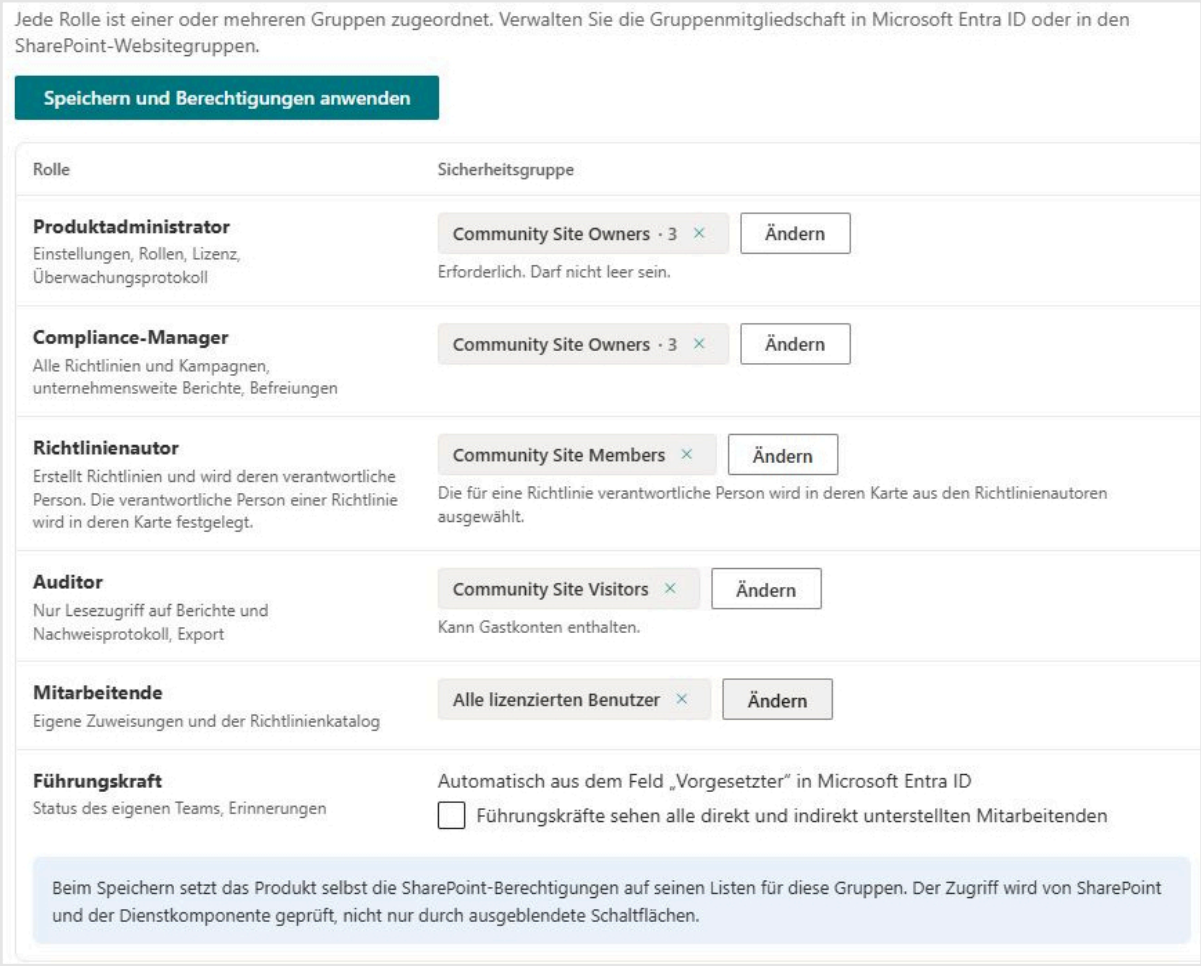
Der Sichtbereich einer Teamleitung ergibt sich aus den Berichtsbeziehungen und einer Einstellung für direkte Mitarbeiter oder den gesamten untergeordneten Bereich. Er ist keine sechste Rollenzuweisung in der Rollenliste. Der Verantwortliche wird in jeder Richtlinie gespeichert; die Autorenansicht filtert nach dieser Person.

Gruppen zuweisen

1 Öffnen Sie Policy Admin als Produktadministrator und wählen Sie **Rollen**.
2 Wählen Sie für die benötigten Rollen Entra ID-Sicherheitsgruppen oder SharePoint-Gruppen der Hubwebsite aus.
3 Behalten Sie mindestens eine Gruppe für **Produktadministrator** bei.
4 Prüfen Sie die Mitarbeitergruppe und **Führungskräfte sehen alle direkt und indirekt unterstellten Mitarbeitenden**.
5 Wählen Sie **Speichern und Berechtigungen anwenden** und warten Sie, bis die Synchronisierung abgeschlossen ist.

Verwenden Sie ausdrücklich ausgewählte Mitarbeitergruppen, wenn eine genaue Zugriffsgrenze erforderlich ist. Die Oberfläche bietet zwar **Alle lizenzierten Benutzer**

an, doch die aktuelle Rollenermittlung betrachtet diese Option ohne Lizenzprüfung als passend für den aktuellen Benutzer. Sie darf nicht als Nachweis verwendet werden, dass nur lizenzierte Konten Zugriff haben.



Produktrollen und zugewiesene Gruppen

Auswirkungen der Berechtigungsanwendung verstehen

Die Synchronisierung gewährt Rollengruppen Lesezugriff auf die Website, unterbricht die Berechtigungsvererbung auf den Produktlisten und wendet die Listenberechtigungsmatrix an. Das Konto, das die Synchronisierung ausführt, behält Vollzugriff auf diese Listen. Prüfen Sie die Auswirkungen, bevor Sie dies auf einer vorhandenen gemeinsam genutzten Website anwenden.

Im Modus Direct erhalten Mitarbeiter Mitwirkungsrechte für Zuweisungen und Bestätigungsdatensätze. Im Modus Service sehen die Mitarbeitereinträge der Matrix für diese beiden Listen nur Lesezugriff vor. Für Fragen behalten Mitarbeiter Mitwirkungsrechte. Ein Benutzer mit mehreren Rollen kann die kombinierten Berechtigungen seiner Gruppen erhalten.

Warnung

Die Filterung nach Richtlinienverantwortlichem und persönlichen Zuweisungen erfolgt in den Webparts. Die Berechtigungsmatrix arbeitet auf Listenebene und bietet keine Isolation pro Richtlinie oder Mitarbeiter. Stellen Sie diese Filter nicht als Garantie dar, dass Benutzer über SharePoint nicht auf andere Datensätze zugreifen können. Eine erfolgreiche Synchronisierung beweist auch nicht, dass sämtliche früheren oder erhöhten Berechtigungen entzogen wurden.

Zielgruppe, Verantwortung und Berechtigung trennen

Diese Konzepte beantworten unterschiedliche Fragen. Eine Kampagnenzielgruppe legt fest, wer eine Aufgabe erhalten soll. Der Richtlinienverantwortliche bestimmt Zuständigkeit und autorengefilterte Verwaltungsansicht. Eine Rolle ermöglicht Produktaktionen, während SharePoint-Berechtigungen den Zugriff auf gespeicherte Datensätze steuern. Eine Änderung an einem dieser Aspekte bewirkt nicht automatisch die anderen.

Die Zuweisung einer Richtlinie an die Finanzabteilung macht beispielsweise deren zugrunde liegende Listeneinträge nicht ausschließlich für diese Abteilung zugänglich. Die Übergabe einer Karte an einen anderen Verantwortlichen ändert den zuständigen Autor, ist jedoch keine Berechtigungsübertragung auf Elementebene. Auch das Ausblenden einer Verwaltungsseite in der Portalnavigation entzieht einem Benutzer nicht seinen bestehenden Listenzugriff.

Gestalten Sie Rollengruppen nach Zuständigkeiten und prüfen Sie anschließend deren wirksamen Datenzugriff. Gehört eine Person mehreren Gruppen an, testen Sie diese kombinierte Mitgliedschaft. Ein Benutzer mit Autorenrolle und administrativer Gruppe kann wesentlich mehr sehen oder ändern als ein reines Autorentestkonto. Das Entfernen einer Mitgliedschaft kann Zugriff über eine andere Gruppe oder erhöhte Websiteberechtigung bestehen lassen.

Einen repräsentativen Zugriffstest verwenden

Testkonto	Anwendungsprüfung	Zusätzliche Zugriffsprüfung
Administrator	Policy Admin öffnen und konfigurierte Rollen prüfen.	Sicherstellen, dass erwartete Verwaltung nach der Synchronisierung verfügbar bleibt.

Testkonto	Anwendungsprüfung	Zusätzliche Zugriffsprüfung
Autor	Eigene Richtlinien öffnen und vorgesehene Verwaltungsaktionen prüfen.	Tatsächliche Listenberechtigungen prüfen, statt Isolation aus der gefilterten Ansicht abzuleiten.
Auditor	Den relevanten Bericht öffnen und einen zulässigen Export herunterladen.	Prüfen, ob Aktionen mit Ergebnis- oder Überwachungsspeicherung zusätzliche Schreibrechte erfordern.
Mitarbeiter	Eine zugewiesene Richtlinie öffnen und eine Pilotbestätigung übermitteln.	Quellzugriff und konfigurierten Nachweisschreibweg prüfen.
Führungskraft	Das erwartete Berichtsteam laden.	Wirksamen Datenzugriff und Bereichsverhalten unabhängig prüfen.

Manche scheinbar lesenden Aktionen schreiben ebenfalls Daten. Eine Integritätsprüfung speichert beispielsweise ihr Ergebnis, und ein Berichtsexport schreibt nach der Dateierstellung ein Überwachungsereignis. Ein schreibgeschütztes Konto kann daher hilfreiche Ausgabe sehen und anschließend einen Schreibfehler erhalten. Untersuchen Sie den konkret fehlgeschlagenen Vorgang, bevor Sie seine Rolle erweitern.

Zugriff nach organisatorischen Änderungen pflegen

Wechselt ein Autor die Stelle, prüfen Sie sowohl Gruppenmitgliedschaft als auch Verantwortung für seine bisherigen Richtlinien. Bei Führungswechseln prüfen Sie Verzeichnisbeziehungen und gespeicherte Managerfelder von Zuweisungen; Neuladen einer Seite schreibt historische Zuweisungen nicht um. Bei Änderung des Aufzeichnungsmodus prüfen Sie den Dienst und wenden die entsprechende Berechtigungsmatrix erneut an.

Dokumentieren Sie kurz, wer Berechtigungen angewendet hat, welche Gruppen vorgesehen waren und welche repräsentativen Tests erfolgreich waren. Das

synchronisierende Konto behält Vollzugriff; bewerten Sie es daher ausdrücklich, statt aus der Bezeichnung Service-Modus zu schließen, alle menschlichen Konten seien schreibgeschützt. Auch die Einstellung für den gesamten Zweig wird von der aktuellen Team-Compliance-Auswahl nicht durchgesetzt; die daraus resultierende Berichtsgrenze beschreibt KB10530. Team Compliance: Ihr Team überwachen und Aufgaben nachverfolgen.

Zugriff prüfen und pflegen

Testen Sie mit getrennten Administrator-, Autoren-, Berichts- und Mitarbeiterkonten. Prüfen Sie sowohl die vorgesehenen Seiten als auch die zugrunde liegenden Listenberechtigungen. Führen Sie nach einer Änderung des Bestätigungserfassungsmodus **Speichern und Berechtigungen anwenden** erneut aus und prüfen Sie die effektiven Rechte. Die Erfassungsmodi und ihre Grenzen sind in KB10509. Datenspeicherung in Policy Acknowledgement: Direct und Service beschrieben.