WISSENSDATENBANKARTIKEL

Datenspeicherung in Policy Acknowledgement: Direct und Service

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

Was der Hub speichert 4

Erfassungsmodi vergleichen 5

Moduswechsel konfigurieren und prüfen 6

Den Datensatz durch die Anwendung verfolgen 7

Die erforderlichen Prüfungen eines Moduswechsels trennen 7

Integrität als einen Teil des Schutzes interpretieren 8

Grenzen des Nachweisschutzes verstehen 8

Policy Acknowledgement speichert seine Arbeitsdaten auf einem SharePoint-Richtlinien-Hub. Der Erfassungsmodus bestimmt, wie normale Mitarbeiterbestätigungen geschrieben werden. Er verschiebt die Daten der Lösung nicht auf eine andere Speicherwebsite.

Was der Hub speichert

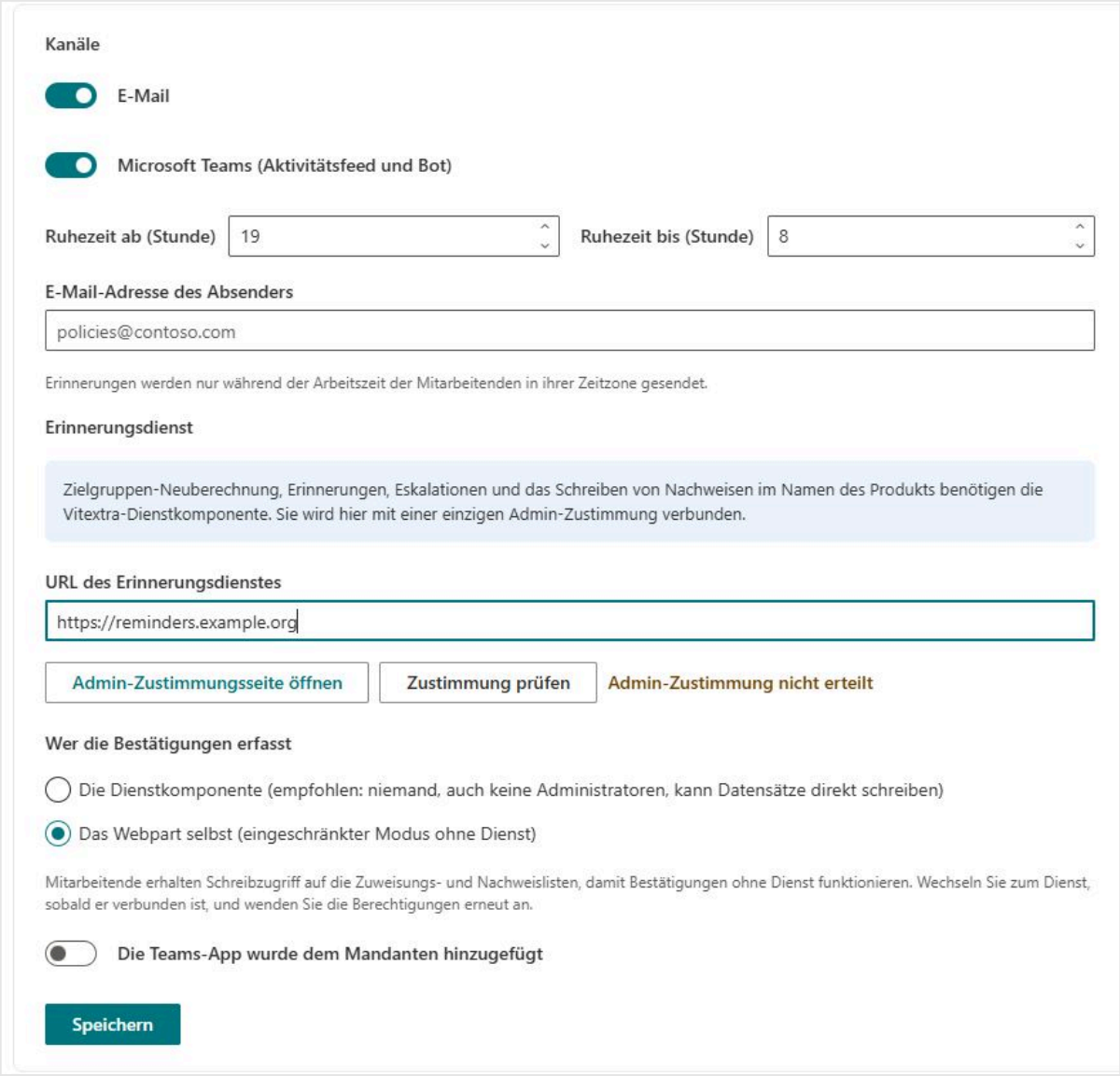
Liste oder Bibliothek	Zweck
`Policies`	Richtlinienkarten, aktuelle Version und Lesekontrollen.
`PolicyVersions`	Versionsmetadaten und Dokument-Snapshots, soweit unterstützt.
`PolicyCategories`	Kategorien und ihre Bestätigungstexte.
`PolicyCampaigns`	Zielgruppendefinitionen, Fristen und Erinnerungseinstellungen.
`PolicyAssignments`	Mitarbeiterzuweisungen und ihr aktueller Status.
`PolicyAcknowledgements`	Bestätigungen und weitere Nachweisereignisse mit verketteten Hashes.
`PolicyQuestions`	Mitarbeiterfragen, Begründungen und Antworten.
`PolicyNotificationLog`	Speicherung des Benachrichtigungsprotokolls.
`PolicyAuditLog`	Verwaltungs- und Workflowereignisse.
`PolicySettings`	Produkteinstellungen.
`PolicyRoleAssignments`	Zuordnungen zwischen Rollen und Gruppen.

Quelldokumente bleiben unter ihren konfigurierten URLs. Die Veröffentlichung eines Dokuments mit demselben Origin kann einen Snapshot in `PolicyVersions` speichern; externe Quellen erhalten weder einen solchen Snapshot noch einen Inhalts-Hash.

Erfassungsmodi vergleichen

Aspekt	Direct	Service
Schreiben normaler Bestätigungen	Das Webpart schreibt unter Verwendung der Mitarbeitersitzung in SharePoint.	Das Webpart sendet die Bestätigung an den angebundenen Dienst.
Mitarbeiterberechtigungen in der Rollenmatrix	Mitwirken bei Zuweisungen und Bestätigungen.	Lesezugriff auf diese beiden Listen.
Separater Dienst für diesen Schreibvorgang erforderlich	Nein.	Ja, mit funktionsfähigem Endpunkt und Zustimmung.
Automatische Erinnerungen und Zielgruppenaktualisierungen	Werden nicht durch den Modus Direct bereitgestellt.	Hängen von Implementierung und Betrieb des angebundenen Diensts ab.

Direct ist die Standardeinstellung. Die Auswahl von Service installiert den Dienst nicht und prüft nicht sein gesamtes Betriebsverhalten.



Auswahl des Erfassungsmodus für Kenntnisnahmen

Moduswechsel konfigurieren und prüfen

1 Öffnen Sie in Policy Admin **Benachrichtigungen**.
2 Geben Sie für den Modus Service **URL des Erinnerungsdienstes** ein, öffnen Sie die Administratorzustimmung und führen Sie **Zustimmung prüfen** aus.
3 Wählen Sie die gewünschte Option unter **Wer die Bestätigungen erfasst** und speichern Sie.
4 Öffnen Sie **Rollen** und wählen Sie **Speichern und Berechtigungen anwenden**.
5 Prüfen Sie die effektiven SharePoint-Berechtigungen und testen Sie eine Bestätigung mit einem separaten Mitarbeiterkonto.

Das Speichern einer Moduseinstellung wendet Berechtigungen nicht automatisch erneut an. Der Leser blockiert die normale Übermittlung, wenn im Modus Service eine URL oder bestätigte Zustimmung fehlt; ein späterer Dienstausfall wird als

Übermittlungsfehler gemeldet.

Den Datensatz durch die Anwendung verfolgen

Karte, Zuweisung und Bestätigung sind unterschiedliche Datensätze. Die Karte beschreibt die aktuelle Richtlinie; die Zuweisung identifiziert die Aufgabe einer Person für eine Version und Kampagne; die Bestätigung erfasst ein Nachweisereignis. Ein Beleg zeigt ausgewählte Nachweisfelder. Diese Datensätze stimmen nach erfolgreicher Übermittlung üblicherweise überein, sollten aber nicht als ein atomarer Gegenstand behandelt werden.

Beim direkten Weg liest die Anwendung den vorhergehenden Hash, hängt die Bestätigung an und aktualisiert die Zuweisung. Beim Dienstweg sendet sie die Nutzdaten an den konfigurierten Endpunkt und ruft den resultierenden Datensatz ab. Späteres Lesen oder Aktualisieren kann scheitern, obwohl ein früherer Schreibvorgang erfolgreich war. Deshalb sollte eine Untersuchung Zuweisungsverweis und Nachweisdatensatz vergleichen, bevor ein Mitarbeiter um einen erneuten Versuch gebeten wird.

Ein Wechsel des Aufzeichnungsmodus ändert den Weg gewöhnlicher Bestätigungen, nicht den Speicherort aller Richtliniendaten oder jeden administrativen Vorgang. Er schreibt auch frühere Ereignisse nicht in ein neues Nachweismodell um. Bewahren Sie die ursprünglichen Datensätze auf und prüfen Sie, wie wirksame Berechtigungen und Dienstverhalten der Bereitstellung die vorgesehenen Schutzanforderungen unterstützen.

Die erforderlichen Prüfungen eines Moduswechsels trennen

Prüfung	Was zu prüfen ist
Konfiguration	Gespeicherter Modus, Endpunkt und Zustimmungsstatus entsprechen der vorgesehenen Einrichtung.
Berechtigungen	Produktmatrix wurde erneut angewendet und tatsächliche Listenrechte wurden geprüft.
Mitarbeiterbestätigung	Ein repräsentativer Mitarbeiter kann übermitteln und den richtigen Beleg erhalten.
Zuweisungsabgleich	Die passende Zuweisung besitzt

Prüfung	Was zu prüfen ist
	erwarteten Status und Nachweisverweis.
Ausnahmeablauf	Ein berechtigter Bediener kann einen Testfall lösen, einschließlich des separaten Befreiungswegs, sofern verwendet.
Hintergrundarbeit	Der Dienstverantwortliche kann erforderliche geplante Aufgaben und Zustellverhalten nachweisen.

Führen Sie diese Prüfungen mit Konten durch, die Produktionsrollen repräsentieren. Tests nur als synchronisierender Administrator können dessen zusätzliche beibehaltene Vollzugriffsrechte verdecken. Ebenso belegt eine erfolgreiche Zustimmungsantwort nicht, dass sämtliche serverseitigen Schreib-, Planungs- und Zustellvorgänge funktionieren.

Integrität als einen Teil des Schutzes interpretieren

Eine Hashkette verknüpft Datensätze so, dass ein geänderter oder bestimmte fehlende Datensätze eine Abweichung erzeugen können. Sie liefert kein unabhängiges vertrauenswürdiges Inventar aller erwarteten Einträge. Die Erkennung eines entfernten Kettenendes oder einer vollständig ersetzten Kette kann andere Kontrollen oder aufbewahrte Nachweise erfordern. Der grüne Indikator bedeutet daher, dass die geladene Kette die implementierten Konsistenzprüfungen bestanden hat.

Verwenden Sie das Integritätsergebnis gemeinsam mit Berechtigungen, Quellen- und Versionsnachweisen sowie operativen Datensätzen. Ein passender Datensatzhash belegt weder die Anzeige einer archivierten Datei im Reader noch die Vollständigkeit aller erforderlichen Mitarbeiterereignisse oder das Textverständnis des Mitarbeiters. Sichern Sie bei Unstimmigkeiten Kennungen und Originaldaten vor Korrekturen; siehe KB10533. Die Integrität des Bestätigungsprotokolls prüfen und KB10538. Fehlgeschlagene Bestätigungen und fehlende Benachrichtigungen untersuchen.

Grenzen des Nachweisschutzes verstehen

Ein Nachweisereignis enthält Identitäts-, Richtlinien- und Versionsinformationen, einen Zeitstempel, Bestätigungstext, Lesekontrolldaten und Hashes. Die Anwendung prüft eine Kette von Datensatz-Hashes, um Unstimmigkeiten zu erkennen. Dies ist keine absolute Unveränderbarkeitsgarantie.

Warnung

Die Oberfläche beschreibt den Modus Service so, als verhindere er direkte Schreibzugriffe auch für Administratoren. Der aktuelle Code zur Berechtigungssynchronisierung behält jedoch Vollzugriff für das synchronisierende Konto bei. Erhöhte oder bestehende Berechtigungen müssen ebenfalls geprüft werden. Direct gewährt Mitarbeitern Mitwirkungsrechte, und die Matrix isoliert Datensätze nicht pro Mitarbeiter. Behaupten Sie nicht, sämtliche Nachweise seien technisch unveränderbar oder die Webpart-Filterung biete Sicherheit auf Datensatzebene.

Befreiungsereignisse werden derzeit auch im Modus Service direkt in SharePoint geschrieben. Dieser Weg kann für einen Compliance-Manager scheitern, der nur die dokumentierten Matrixberechtigungen besitzt. Siehe KB10507. Richtlinienfragen bearbeiten und Mitarbeiter befreien. Die separate Dienstimplementierung ist nicht Teil des Webpart-Projekts; ihre Anwendungsberechtigungen, Hintergrundverarbeitung und Schutzmechanismen müssen daher in der tatsächlichen Bereitstellung geprüft werden.