СТАТЬЯ БАЗЫ ЗНАНИЙ

Как настроить роли и разрешения Policy Acknowledgement

2026 © Vitextra SIA. Все права защищены.

Отказ от ответственности

Для целей настоящего Заявления об отказе от ответственности:

- **Компания** (именуемая в данном Отказе от ответственности "Компания", "Мы", "Нас" или "Наш") относится к Vitextra SIA, LV-1009 Riga, Matise iela 61 - 25.
- **Документ** ссылается на статью Базы знаний.
- **Вы** означает физическое лицо, получающее доступ к Документу, или компанию, или другое юридическое лицо, от имени которого такое физическое лицо получает доступ к Документу или использует его, в зависимости от обстоятельств.
- **Веб-сайт** относится к Vitextra, доступному с https://vitextra.com

Отказ от ответственности

Информация, содержащаяся в Документе, предназначена только для общих информационных целей.

Компания не несет ответственности за ошибки или упущения в содержании Документа.

Ни в коем случае Компания не несет ответственности за какие-либо особые, прямые, косвенные, логически вытекающие или случайные убытки или любой ущерб вообще, будь то в результате действия договора, халатности или других правонарушений, возникающих в результате или в связи с использованием содержания Документа. Компания оставляет за собой право вносить дополнения, удаления или модификации в содержание Документа в любое время без предварительного уведомления.

Отказ от ответственности за ошибки и упущения

Информация, представленная в Документе, предназначена только для общего руководства по вопросам, представляющим интерес. Таким образом, ошибки могут возникать, даже если Компания принимает все меры предосторожности для обеспечения актуальности и точности содержания Документа. Кроме того, учитывая меняющийся характер законов, правил и подзаконных актов, могут возникнуть задержки, упущения или неточности в информации, содержащейся в Документе.

Компания не несет ответственности за какие-либо ошибки или упущения, а также за результаты, полученные в результате использования этой информации.

Отказ от добросовестного использования

Компания может использовать защищенные авторским правом материалы, которые владелец авторских прав явно не разрешил. Компания делает такие материалы доступными для критики, комментариев, новостных репортажей, преподавания, стипендий или исследований.

Компания считает, что это представляет собой "добросовестное использование" любого такого защищенного авторским правом материала, как это предусмотрено в разделе 107 закона США об авторском праве.

Если Вы хотите использовать защищенные авторским правом материалы из Документа в своих собственных целях, выходящих за рамки добросовестного использования, Вы должны получить разрешение от владельца авторских прав.

Отказ от ответственности "Используйте на Свой Страх и Риск"

Вся информация в Документе предоставляется "как есть", без каких-либо гарантий полноты, точности, своевременности или результатов, полученных в результате использования этой информации, и без каких-либо гарантий, явных или подразумеваемых, включая, но не ограничиваясь гарантиями производительности, товарной пригодности и пригодности для конкретного цель.

Компания не несет ответственности перед Вами или кем-либо еще за любое принятое решение или действие, основанное на информации, предоставленной Сервисом, или за любые косвенные, особые или аналогичные убытки, даже если она предупреждена о возможности таких убытков.

Свяжитесь с Нами

Если у вас есть какие-либо вопросы по поводу этого заявления об отказе от ответственности, Вы можете связаться с нами по электронной почте: support@vitextra.com .

Оглавление

Назначение ролей 4

Назначьте группы 4

Что меняется при применении разрешений 5

Разделяйте аудиторию, владение и разрешения 6

Используйте типичные проверки доступа 6

Поддерживайте доступ после организационных изменений 7

Проверьте и поддерживайте доступ 8

Роли продукта определяют доступные операции и представления Policy Acknowledgement. Policy Admin также применяет разрешения SharePoint для ролей к спискам центра политик. При проектировании доступа учитывайте оба уровня.

Назначение ролей

Роль	Основное использование в веб-частях
Администратор продукта	Настройка, параметры, роли и администрирование; доступ к управлению и отчётам.
Комплаенс-менеджер	Политики, кампании, отчёты и освобождения в рамках всего продукта.
Автор политик	Создание политик и управление политиками, владельцем которых является автор.
Аудитор	Отчётность и просмотр без действий по управлению политиками.
Сотрудник	Личные назначения и содержимое политик.

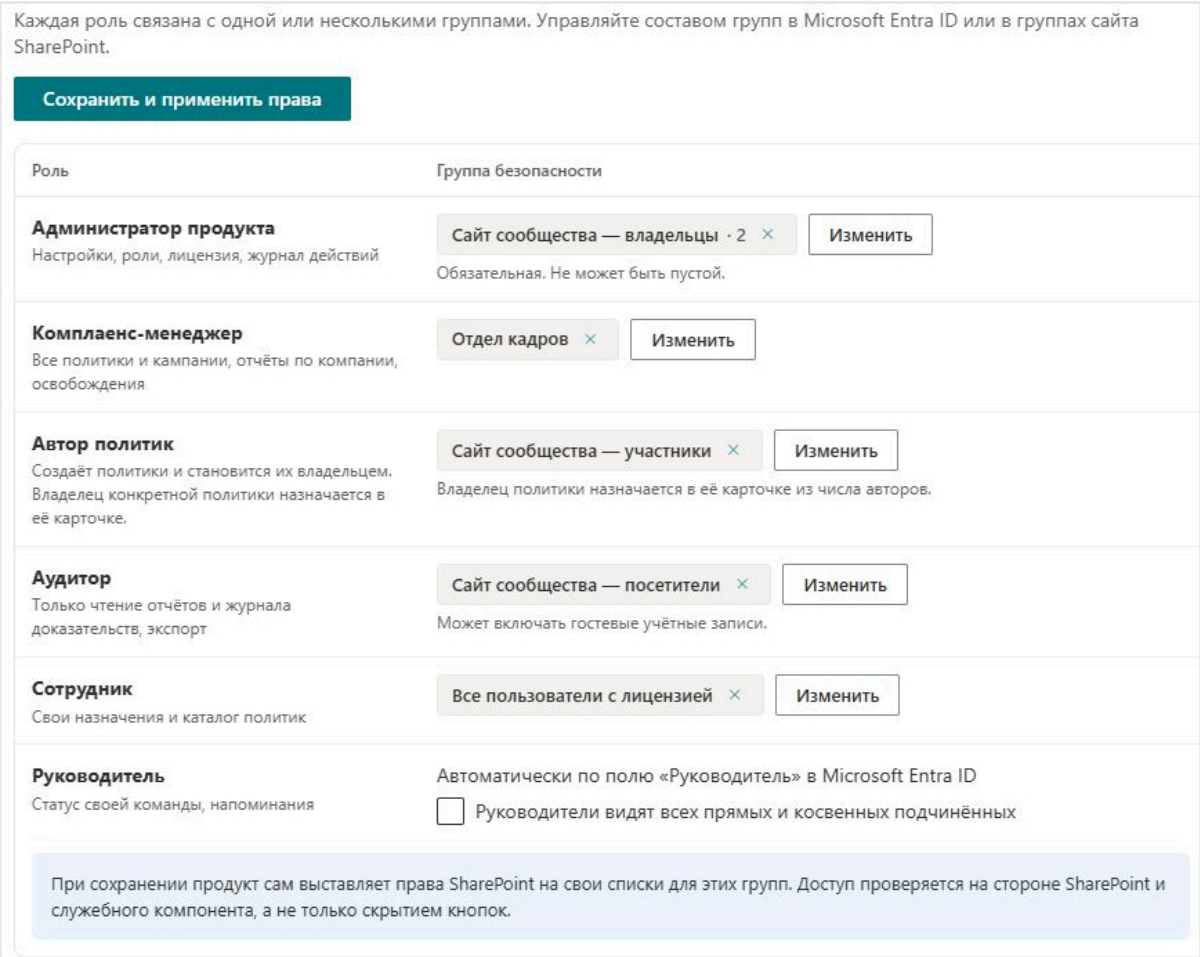
Область видимости руководителя определяется отношениями подчинённости и настройкой показа непосредственных подчинённых либо всей ветви. Это не шестая назначаемая роль в списке ролей. Владелец указан в каждой политике; представление автора фильтрует политики по этому владельцу.

Назначьте группы

1 Откройте Policy Admin как администратор продукта и выберите **Роли**.
2 Выберите группы безопасности Entra ID или группы SharePoint сайта центра политик для нужных ролей.
3 Оставьте хотя бы одну группу для роли **Администратор продукта**.
4 Проверьте состав сотрудников и параметр **Руководители видят всех прямых и косвенных подчинённых**.
5 Выберите **Сохранить и применить права** и дождитесь завершения синхронизации.

Используйте явно заданные группы сотрудников, если необходима точная граница

доступа. Хотя интерфейс предлагает вариант **Все пользователи с лицензией**, текущий механизм определения ролей считает его подходящим для текущего пользователя без проверки лицензии. Этот вариант не подтверждает, что доступ ограничен лицензированными учётными записями.



Роли продукта и назначенные группы

Что меняется при применении разрешений

Синхронизация предоставляет группам ролей доступ на чтение сайта, разрывает наследование разрешений списков продукта и применяет матрицу прав списков. Учётная запись, выполняющая синхронизацию, сохраняет полный доступ к этим спискам. Перед применением на существующем общем сайте оцените последствия.

В режиме Direct сотрудники получают права внесения изменений в назначения и записи подтверждений. В режиме Service матрица предоставляет сотрудникам только чтение этих двух списков. Права внесения изменений в вопросы сохраняются. Пользователь с несколькими ролями может получить совокупность разрешений своих групп.

Предупреждение

Фильтрация по владельцу политики и личным назначениям реализована в веб-частях. Матрица разрешений действует на уровне списка и не изолирует отдельные политики или записи сотрудников. Не представляйте эти фильтры как гарантию невозможности доступа к другим записям через SharePoint. Успешная синхронизация также не доказывает отзыв всех ранее существовавших или повышенных прав.

Разделяйте аудиторию, владение и разрешения

Эти понятия отвечают на разные вопросы. Аудитория кампании определяет получателей задачи. Владелец политики задаёт ответственность и отфильтрованное представление автора. Роль разрешает действия продукта, а разрешения SharePoint управляют доступом к сохранённым записям. Изменение одного не выполняет автоматически остальные задачи.

Например, назначение политики финансовому подразделению не делает записи исходных списков приватными для финансового подразделения. Передача карточки другому владельцу меняет ответственного автора, но не передаёт разрешения на уровне элемента. Скрытие страницы управления в навигации портала также не отзывает существующий доступ к спискам.

Проектируйте группы ролей по обязанностям, затем проверяйте их фактический доступ к данным. Если человек состоит в нескольких группах, проверяйте совокупное членство. Пользователь с ролью автора и административной группой может видеть или менять намного больше, чем тестовая учётная запись только автора. Удаление одного членства может оставить доступ через другую группу или повышенные права сайта.

Используйте типичные проверки доступа

Тестовая учётная запись	Проверка приложения	Дополнительная проверка доступа
Администратор	Открыть Policy Admin и проверить настроенные роли.	Подтвердить сохранение нужного администрирования после синхронизации.
Автор	Открыть свои политики и	Проверить фактические

Тестовая учётная запись	Проверка приложения	Дополнительная проверка доступа
	проверить нужные действия управления.	разрешения списка, не выводя изоляцию из фильтрованного представления.
Аудитор	Открыть нужный отчёт и скачать разрешённый экспорт.	Проверить, требуют ли действия с сохранением результата или аудита дополнительных прав записи.
Сотрудник	Открыть назначенную политику и отправить пилотное подтверждение.	Проверить источник и настроенный путь записи доказательств.
Руководитель	Загрузить ожидаемую команду.	Независимо проверить доступ к данным и поведение области отчёта.

Некоторые действия, которые выглядят как просмотр данных, также выполняют запись. Например, проверка целостности сохраняет результат, а экспорт отчёта записывает событие аудита после создания файла. Поэтому учётная запись только для чтения может получить полезный результат, а затем ошибку записи. Перед расширением роли исследуйте конкретную сбойную операцию.

Поддерживайте доступ после организационных изменений

При смене должности автора проверьте и членство в группах, и владение сопровождаемыми им политиками. При смене руководителей проверьте связи каталога и сохранённые поля руководителей в назначениях: перезагрузка страницы не переписывает исторические назначения. При смене режима записи проверьте сервис и повторно примените соответствующую матрицу разрешений.

Кратко фиксируйте, кто применил разрешения, какие группы предполагались и какие типичные тесты пройдены. Учётная запись синхронизации сохраняет полный

доступ, поэтому оценивайте её явно, не считая обозначение сервисного режима гарантией прав только для чтения у всех людей. Настройка всей ветви также не применяется текущим переключателем Team Compliance; возникающее ограничение отчётности описано в KB10530. Team Compliance: контроль команды и работа с просрочками.

Проверьте и поддерживайте доступ

Протестируйте отдельные учётные записи администратора, автора, пользователя отчётности и сотрудника. Проверьте нужные страницы и разрешения исходных списков. После изменения режима записи подтверждений повторно выполните **Сохранить и применить права** и изучите действующие права. Режимы записи и их ограничения описаны в KB10509. Хранение данных Policy Acknowledgement: режимы Direct и Service.