

# Поведение

На этой вкладке выбираются настройки, определяющие действия с устройством в рамках политики использования устройств.

Поведение

☐ Добавлять устройство автоматически

☒ Разрешить сброс PIN-кода устройства

☒ Разрешить офлайновую разблокировку

☒ Проверять ответы на секретные вопросы

☒ Разрешить отмену обновления устройства

☐ Разрешить пользователю добавление устройства

☐ Разрешить пользователю назначение устройства

☒ Разрешить пользователю отзыв устройства

☒ Разрешить пользователю включение устройства

☒ Разрешить пользователю выключение устройства

☐ Разрешить пользователю очистку устройства

☐ Разрешить пользователю сброс PIN-кода устройства

☒ Разрешить пользователю обновление устройства

☐ Разрешить пользователю выбор необязательных сертификатов

☒ Пользователь должен задать ответы на секретные вопросы при первом входе в сервис самообслуживания

☐ Разрешить пользователю изменение ответов на секретные вопросы

☐ Включить отслеживание сертификатов

Сохранить

Для выбора настройки установите галочку рядом с ней.

Настройка	Описание	Значение по умолчанию
Добавлять устройство автоматически	Добавлять устройство в систему (если оно не было добавлено ранее) в момент выпуска или назначения устройства пользователю. Если опция выключена, то выпуск или назначение устройства, подключенного к компьютеру, но не добавленного в систему, запрещен.	Отключена
Разрешить сброс PIN-кода устройства	Разрешить администратору сбрасывать PIN-код пользователям устройств.	Включена
Разрешить офлайновую разблокировку	<p>Позволяет разблокировать устройство пользователя при помощи администратора системы в случае, когда соединение между рабочей станцией пользователя и сервером Rutoken KeyBox отсутствует.</p> <p>Необходимым условием разблокировки устройства является знание пользователем ответов на секретные вопросы. Проверку ответов на секретные вопросы при разблокировке устройства в случае необходимости можно отключить (опция <b>Проверять ответы на секретные вопросы</b>).</p>	Включена
Разрешить отмену обновления устройства	Позволяет администратору или оператору РутOKEN KeyBox отменить обновление содержимого устройства пользователя.	Включена
Разрешить пользователю добавление устройства	Разрешить пользователю выпуск устройства, не добавленного в систему. Устройство будет добавлено автоматически в процессе выпуска. Опция работает только если включена опция <b>Добавлять устройство автоматически</b> .	Отключена

Разрешить пользователю назначение устройства	Разрешить пользователю выпуск устройства, не назначенного на него администратором.	Отключена
Разрешить пользователю отзыв устройства	Разрешить пользователю отзыв своего устройства.	Включена
Разрешить пользователю включение устройства	Разрешить пользователю включение своего устройства (если оно было выключено ранее).	Включена
Разрешить пользователю выключение устройства	Разрешить пользователю выключение своего устройства (если оно была включено ранее).	Включена
Разрешить пользователю очистку устройства	Разрешить пользователю очистку содержимого своего устройства при его отзыве оператором с причинами <b>Изъятие устройства</b> и <b>Обновление устройства</b> . После очистки устройство останется назначенным пользователю.	Отключена
Разрешить пользователю сброс PIN-кода устройства	Разрешить пользователю сброс PIN-кода своего устройства.	Отключена
Разрешить пользователю обновление устройства	Разрешить пользователю обновлять сертификаты, хранящиеся на его устройстве, в случае, если их срок действия истек (или истекает).	Включена
Разрешить пользователю выбор необязательных сертификатов	Если опция включена, то при выпуске устройства в приложении <b>Сервис самообслуживания</b> (Self Service) пользователь сможет выбрать (среди необязательных сертификатов), те сертификаты, которые необходимо записать на устройство.  Если опция выключена, то сертификаты, отмеченные в политике выпуска устройств, как необязательные, записаны на устройство не будут.	Отключена
Разрешить пользователю выпуск AirKey карты	Если опция включена, то пользователи смогут самостоятельно выпускать карты AirKey в приложении <b>Сервис самообслуживания</b> (Self Service). Выпуск карт AirKey возможен только при настроенной интеграции с Indeed AirKey Enterprise.	Отключена
Разрешить пользователю выпуск устройства КристоПро DSS	Если опция включена, то пользователям разрешено самостоятельно выполнять запрос и выпуск устройств DSS.  Если опция выключена, то выпуск возможен только администратором или оператором.	Отключена
Разрешить пользователю удаление устройства КристоПро DSS	Если опция включена, то пользователям разрешено самостоятельно отзывать и удалять устройство DSS.  Если опция выключена, то отзыв и удаление возможно только администратором или оператором.	Отключена
Разрешить пользователю редактирование данных в форме проверки в СМЭВ	Если опция включена, то пользователям разрешено редактировать данные, полученные из Active Directory в форме проверки в СМЭВ.  Если опция выключена, то редактирование пользовательских данных в форме проверки в СМЭВ разрешено только администраторам или операторам.	Включена
Пользователь должен задать ответы на секретные вопросы при первом входе в сервис самообслуживания	Если опция включена, то после входа пользователя в приложение <b>Self Service</b> первый раз необходимо будет установить секретные вопросы и ответы на них. Вопросы в дальнейшем будут использоваться для аутентификации пользователя.  Если опция выключена, то форма установки секретных вопросов при входе в сервис самообслуживания отображаться не будет. Пользователь сможет установить секретные вопросы позднее в любой момент.	Включена
Разрешить пользователю изменение ответов на секретные вопросы	Если опция включена, то пользователям разрешено изменять ответы на секретные вопросы пользователя после их установки в приложении <b>Self Service</b> .  Если опция выключена, то пользователям будет недоступно изменение ответов на секретные вопросы после их установки в сервисе самообслуживания. Администраторы и операторы могут сбросить ответы на секретные вопросы для последующей их установки пользователями.	Отключена

<p><b>Включить отслеживание сертификатов</b></p>	<p>Если опция включена, то при выпуске устройства в Рутокен KeyBox выполнит поиск имеющихся на устройстве сертификатов и соответствующих им закрытых ключей. Поддерживается отслеживание сертификатов, выпущенных удостоверяющими центрами:</p> <ul style="list-style-type: none"> <li>○ Microsoft CA</li> <li>○ КриптоПро УЦ 2.0</li> <li>○ ViPNet УЦ 4</li> </ul> <p>При скором истечении срока действия таких сертификатов Рутокен KeyBox может рассылать соответствующие почтовые уведомления (<b>Отслеживаемые сертификаты истекают</b>) Администраторам и Пользователям системы. В Консоле управления и в приложении Self Service имеется возможность распечатать отслеживаемые сертификаты по стандартному шаблону печати сертификата, используемому в системе.</p>
--------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------