

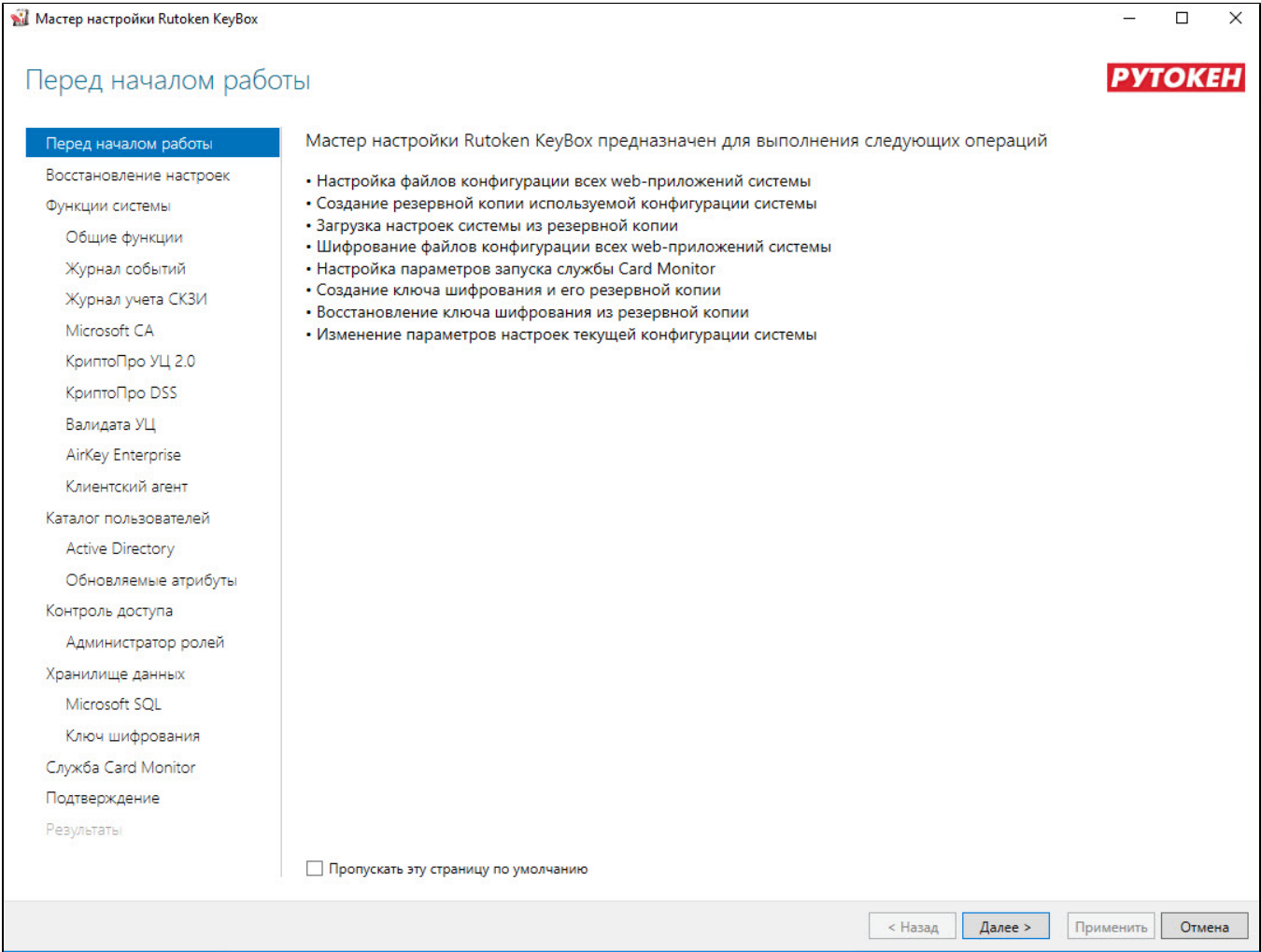
Настройка параметров системы

На этапе развертывания системы необходимо указать нужные значения в файлах конфигурации для каждого сервиса. Файлы конфигурации всех сервисов системы располагаются в корневом каталоге веб-приложений IIS (путь по умолчанию %SystemDrive%\inetpub\wwwroot).

Файлы конфигурации службы Card Monitor расположены в %ProgramFiles%\RutokenKeyBox\CardMonitor.

Настройка файлов конфигурации осуществляется при помощи **Мастера настройки RutokenKeyBox**. Мастер настройки запускается автоматически после завершения работы Мастера установки сервера RutokenKeyBox, если в последнем отмечена соответствующая опция.

Также Мастер настройки RutokenKeyBox может быть запущен в любой момент вручную (Пуск – Все программы – RutokenKeyBox Identity).



В таблице приведены разделы Мастера установки с описанием параметров, которые могут быть в них определены.

Разделы мастера настройки Рутокен KeyBox и их описание.

Раздел	Описание
Перед началом работы	Информация о назначении и возможностях мастера настройки RutokenKeyBox.
Восстановление настроек	Загрузка файла резервной копии конфигурации RutokenKeyBox.

<p>Функции системы:</p> <ul style="list-style-type: none"> Общие функции Журнал событий Журнал учета СКЗИ Microsoft CA КриптоПро УЦ 2.0 КриптоПро DSS Валидата УЦ AirCard Enterprise Клиентский агент 	<p>Общие функции: настройка внутренних параметров веб-приложений RutokenKeyBox.</p> <p>Консоль управления (Management Console)</p> <ul style="list-style-type: none"> Сводная информация о системе Журнал учета устройств и сертификатов <p>Журнал учета реализован для конфигураций системы с использованием хранилища данных Microsoft SQL и PostgreSQL.</p> <ul style="list-style-type: none"> Организационная структура Интеграция с Indeed Access Manager Интеграция с Secret Net Studio Интеграция со СМЭВ Сброс пароля пользователя в Active Directory Просмотр SO PIN устройства Публикация сертификатов в файловое хранилище <p>Публикация сертификатов не поддерживается для примонтированных сетевых дисков. Задайте путь к файловому хранилищу в формате:</p> <p>\\Имя рабочей станции\Имя сетевого каталога</p> <p>Сервис самообслуживания (Self Service)</p> <ul style="list-style-type: none"> Просмотр содержимого устройства Работа с TPM Virtual Smart Card Работа с Windows Hello for Business Загрузка файлов и ресурсов <hr/> <p>Журнал событий:</p> <ul style="list-style-type: none"> Переопределять атрибут имени пользователя для поиска в Журнале событий. Значение по умолчанию: CN (common name) Настройка подключения к единому журналу событий для нескольких серверов Rutoken KeyBox <hr/> <p>Журнал учета СКЗИ: настройка параметров ведения журнала учета СКЗИ.</p> <hr/> <p>Удостоверяющие центры: настройка параметров работы с центрами сертификации MS CA, КриптоПро УЦ 2.0 и Валидата УЦ.</p> <p>КриптоПро DSS: настройка интеграции с ПАК КриптоПро DSS.</p> <hr/> <p>AirCard Enterprise: настройка интеграции с сервером виртуальных смарт-карт Indeed AirCard Enterprise.</p> <hr/> <p>Клиентский агент: настройка параметров работы клиентского агента Rutoken KeyBox.</p>
<p>Каталог пользователей:</p> <ul style="list-style-type: none"> Active Directory КриптоПро УЦ 2.0 Active Directory + КриптоПро УЦ 2.0 	<p>Определение каталога пользователей системы. Параметры подключения отображаются в зависимости от выбранного каталога.</p>

<ul style="list-style-type: none"> • Соответствия атрибутов 	<p>Определение атрибутов, с которыми необходимо создать нового пользователя в Центре Регистрации КристоПро УЦ 2.0 с использованием RutokenKeyBox в момент выпуска устройства.</p> <p>Например: создать нового пользователя в ЦР КристоПро с теми значениями атрибутов, которые есть для существующего пользователя Active Directory.</p>
<ul style="list-style-type: none"> • Обновляемые атрибуты 	<p>Определение списка атрибутов пользователя при изменении которых требуется обновление сертификата на устройстве.</p> <p>В список отслеживаемых атрибутов пользователя в параметрах шаблонов сертификатов Microsoft CA и КристоПро УЦ 2.0 по умолчанию включены:</p> <ul style="list-style-type: none"> • Общее имя(CN) • E-mail • UPN-имя пользователя <p>Отслеживание изменений в атрибутах пользователей Active Directory доступно только для атрибутов из полей Субъект (Subject) и Дополнительное имя субъекта (Subject Alternative Name) сертификата.</p>
<p>Контроль доступа:</p> <ul style="list-style-type: none"> • Администратор ролей 	<p>Определение параметров доступа к сервисам Рутокен KeyBox.</p> <p>Определение учетной записи для первоначальной настройки привилегий пользователей в разделе Роли Консоли управления RutokenKeyBox.</p> <p>Указанная учетная запись должна иметь User Principal Name (UPN) и входить в выбранный каталог пользователей системы.</p>
<p>Хранилище данных:</p> <ul style="list-style-type: none"> • Active Directory, Microsoft SQL или PostgreSQL • Ключ шифрования 	<p>Определение хранилища данных системы, алгоритма шифрования данных. Создание резервной копии ключа шифрования и восстановление ключа из копии. Параметры подключения к хранилищу определяются в зависимости от выбранного типа.</p>

Служба Card Monitor	<p>Служба Card Monitor предназначена для выполнения операций по контролю за обращением устройств (USB-токенов и смарт-карт) и выполняет:</p> <ul style="list-style-type: none"> ○ Отзыв и изъятие (опционально) устройств пользователей, чьи учетные записи были удалены из каталога пользователей Рутокен KeyBox ○ Отзыв временных устройств с истекшим сроком действия ○ Выключение (опционально) устройств пользователей, чьи учетные записи Active Directory были отключены ○ Удаление учетных записей (опционально) из каталога пользователей Рутокен KeyBox, чьи учетные записи Active Directory были отключены ○ Установку и сброс статуса содержимого устройства (истекает/истекло) ○ Обновление содержимого устройств <p>Если обновление устройства проводилось через Агент RutokenKeyBox без автоматического одобрения сертификатов оператором УЦ.</p> <ul style="list-style-type: none"> ○ Регистрации события Длительное отсутствие связи с агентом в системный журнал ○ Рассылку почтовых уведомлений администраторам и пользователям системы: <ul style="list-style-type: none"> – Истечение срока действия сертификатов пользователей, хранящихся на устройстве – Одобрение/отклонение выпуска устройства – Одобрение/отклонение обновления сертификатов на устройстве – Одобрение/отклонение замены устройства – Изменение политики, действующей на пользователя <p>Для выполнения задач по регулярному запуску службы Card Monitor, учетная запись, указываемая в мастере настройки должна состоять в группе Администраторов (Administrators) на сервере RutokenKeyBox и иметь разрешение на Вход в качестве пакетного задания (Log on as a batch job).</p> <p>Для работы Card Monitor в разделе Роли потребуются создать сервисную роль, включить в нее учетную запись, от имени которой будет работать Card Monitor и определить для роли привилегии:</p> <ul style="list-style-type: none"> • Выключение устройства • Обновление устройства • Сброс PIN-кода • Блокировка устройства • Отзыв устройства • Очистка устройства • Отмена назначения устройства • Удаление устройства • Выключение устройства КристоПро DSS • Обновление устройства КристоПро DSS • Отзыв устройства КристоПро DSS • Удаление устройства КристоПро DSS • Удаление AirCard • Удаление записи из журнала учета <p>Если настроена интеграция с КристоПро DSS и AirCard Enterprise, то задайте привилегии для работы с данными устройствами.</p>
Подтверждение	<p>Сводная информация по настройкам всех разделов Мастера с возможностью создания резервной копии конфигурации Рутокен KeyBox.</p> <p>При первой установке Рутокен KeyBox настройте необходимые параметры и сохраните их копию (опция Сохранить резервную копию параметров конфигурации в разделе Подтверждение).</p> <p>Резервная копия настроек Рутокен KeyBox включает в себя все параметры, определенные при установке системы для всех сервисов, а также алгоритм и ключ шифрования данных. При развертывании новых серверов Рутокен KeyBox используйте файл резервной копии, указав его в разделе Восстановление настроек Мастера установки и настройки.</p> <p>Файл резервной копии содержит данные сервисных учетных записей (для работы с каталогом пользователей и хранилищем данных), алгоритм и ключ шифрования. Храните файл резервной копии в защищенном месте.</p>
Результаты	<p>Прогресс работы Мастера по записи указанных значений в файлы конфигурации сервисов Рутокен KeyBox.</p> <p>После завершения работы Мастера настройки RutokenKeyBox указанные значения для всех параметров будут записаны в файлы конфигурации всех приложений и зашифрованы. Шифрование осуществляется при помощи машинного ключа шифрования Microsoft .NET (NetFrameworkConfigurationKey). Алгоритм шифрования – RSA.</p>