



Indeed Certificate Manager 6.6.0

Руководство по установке и эксплуатации

Оглавление

1. Indeed Certificate Manager 6.6.0 Documentation	6
1.1 Общее описание	8
1.1.1 Задачи	9
1.1.2 Описание компонентов	11
1.1.3 Структурная схема	13
1.2 Установка и настройка	14
1.2.1 Системные требования	16
1.2.1.1 Серверные компоненты	17
1.2.1.2 Клиентские компоненты	20
1.2.1.3 Сетевое взаимодействие	21
1.2.1.4 Поддерживаемые устройства	25
1.2.2 Порядок установки	27
1.2.3 Настройка каталога пользователей	29
1.2.3.1 Каталог в Active Directory	30
1.2.3.2 Каталог в Центре Регистрации КриптоПро УЦ 2.0	35
1.2.3.3 Составной каталог в Active Directory и Центре Регистрации КриптоПро УЦ 2.0	37
1.2.4 Создание хранилища данных	38
1.2.4.1 Active Directory	39
1.2.4.2 Microsoft SQL	41
1.2.4.3 PostgreSQL	44
1.2.5 Настройка Центров Сертификации	50
1.2.5.1 Microsoft CA	51
1.2.5.1.1 Создание сервисной учетной записи для работы с Microsoft CA	52
1.2.5.1.2 Настройка шаблонов сертификатов	54
1.2.5.1.3 Добавление шаблонов сертификатов	58
1.2.5.1.4 Выпуск сертификата Агент регистрации (Enrollment Agent)	59
1.2.5.1.5 Подключение к центру сертификации Microsoft через IndeedCM MSCA Proxy	64
1.2.5.2 КриптоПро УЦ 2.0	66
1.2.5.2.1 Создание сервисной учетной записи для работы с КриптоПро УЦ 2.0	67
1.2.5.2.2 Создание шаблона сертификата для сервисной учетной записи	68
1.2.5.2.3 Выпуск сертификата агента подачи заявок сервисной учетной записи	69
1.2.5.2.4 Настройка аутентификации в web-сервисах Indeed CM по сертификатам	71
1.2.5.3 КриптоПро DSS 2.0	73
1.2.5.4 Валидата УЦ	76
1.2.5.4.1 Offline-режим работы	77
1.2.5.4.2 Online-режим работы	78
1.2.5.4.3 Настройка шаблонов сертификатов пользователей	81
1.2.6 Установка и настройка серверных компонентов	86
1.2.6.1 Установка сервера	87
1.2.6.2 Настройка параметров системы	90
1.2.6.3 Настройка клиентского агента	96
1.2.6.3.1 Создание сертификатов Агента	97
1.2.6.3.2 Настройка Indeed CM для работы с Агентами	100
1.2.6.3.3 Установка и настройка агентов на рабочих станциях	103

1.2.6.4 Единый журнал событий	108
1.2.6.4.1 Event Log Proxy	109
1.2.6.4.2 Indeed Log Server	110
1.2.6.4.3 Настройка Indeed CM на работу с единым журналом событий	115
1.2.7 Установка клиентских компонентов	118
1.2.7.1 Настройка разблокировки устройств	122
1.2.7.2 Настройка поддержки устройств Registry	126
1.2.8 Настройка браузеров	129
1.3 Руководство администратора	130
1.3.1 Конфигурация	131
1.3.1.1 Политики	132
1.3.1.1.1 Общие параметры	135
1.3.1.1.2 Настройки PKI	136
1.3.1.1.3 Indeed AM	166
1.3.1.1.4 Secret Net Studio	170
1.3.1.1.5 СМЭВ	172
1.3.1.1.6 Поведение	173
1.3.1.1.7 Выпуск	176
1.3.1.1.8 Аутентификация	182
1.3.1.1.9 Агенты (Политики)	184
1.3.1.1.10 Принтер смарт-карт	187
1.3.1.1.11 Уведомления	189
1.3.1.2 Назначения политик	208
1.3.1.3 Лицензии	211
1.3.1.4 Типы устройств	213
1.3.1.5 Организационная структура	220
1.3.1.6 Роли	223
1.3.1.7 Теги	226
1.3.1.8 Шаблоны печати	227
1.3.1.8.1 Настройка шаблона печати СКЗИ	229
1.3.1.9 Журналы учета (Конфигурация)	234
1.3.1.9.1 Справочники	235
1.3.1.9.2 Шаблоны журналов	237
1.3.1.10 Помощь и поддержка	242
1.3.2 Справочник по разделам консоли управления	243
1.3.2.1 Сводная информация	244
1.3.2.2 Пользователи	249
1.3.2.2.1 Карточка пользователя	252
1.3.2.3 Устройства	318
1.3.2.3.1 Добавление устройства	321
1.3.2.3.2 Выпуск устройства	323
1.3.2.3.3 Удаление устройства	324
1.3.2.3.4 Инициализация пустых устройств	326
1.3.2.3.5 Изменение тегов	329
1.3.2.3.6 Пакетное добавление устройств	331
1.3.2.4 Агенты	335
1.3.2.4.1 Профиль Агента	339
1.3.2.4.2 Назначение устройства в Агенте	342
1.3.2.4.3 Контроль за использованием устройств	344
1.3.2.4.4 Назначение задач	346
1.3.2.4.5 Мониторинг подключенных устройств	362

1.3.2.4.6 Журнал событий	365
1.3.2.5 СКЗИ	366
1.3.2.5.1 Операции с СКЗИ	369
1.3.2.5.2 Пакетный импорт СКЗИ	373
1.3.2.6 Журналы учета	376
1.3.2.7 Журнал	378
1.3.2.7.1 Список событий	383
1.4 Руководство пользователя	408
1.4.1 Сервис самообслуживания (Self Service)	409
1.4.1.1 Выпуск устройств в сервисе самообслуживания	412
1.4.1.1.1 Выпуск устройств Registry	420
1.4.1.1.2 Выпуск TPM Virtual Smart Card (VSC)	423
1.4.1.1.3 Выпуск Windows Hello for Business (WHfB)	426
1.4.1.2 Операции с устройствами AirKey	432
1.4.1.2.1 Выпуск устройств AirKey	433
1.4.1.2.2 Подключение устройства AirKey к рабочей станции	435
1.4.1.3 Изменение ответов на секретные вопросы	437
1.4.1.4 Обновление устройств	438
1.4.1.5 Выключение и включение устройств	440
1.4.1.6 Выключение устройств без выполнения входа в систему	442
1.4.1.7 Отзыв и очистка устройств	445
1.4.1.8 Сброс и изменение PIN-кода устройств	447
1.4.1.9 Просмотр содержимого устройства	449
1.4.1.10 Загрузка файлов и ресурсов	450
1.4.1.11 Клиентский агент Indeed CM	451
1.4.1.11.1 Сброс и разблокировка PIN-кода	452
1.4.1.11.2 Обновление содержимого устройства	453
1.4.1.12 Выгрузка сертификата DSS на рабочую станцию пользователя	455
1.4.2 Сервис удаленного самообслуживания (Remote Self Service)	457
1.5 Дополнительные инструкции	461
1.5.1 Indeed CM API	462
1.5.2 Indeed CM Client Browser Extension	468
1.5.3 Indeed CM Card Template Designer	469
1.5.3.1 Создание шаблона печати	470
1.5.3.2 Приложение 1	481
1.5.4 Миграция с Aladdin JaCarta Management System	483
1.5.4.1 Создание политики использования устройств	485
1.5.4.2 Настройка файла конфигурации утилиты миграции	486
1.5.4.3 Работа с утилитой IndeedCM.Migrate.JMS.exe	487
1.5.5 Миграция с SafeNet Authentication Manager	488
1.5.5.1 Настройка Indeed CM для работы с данными из SAM	489
1.5.5.1.1 Создание политик использования устройств	490
1.5.5.2 Настройка утилиты миграции IndeedCM.Migrate.SAM	491
1.5.5.2.1 Заполнение файла конфигурации IndeedCM.Migrate.SAM.exe.config	492
1.5.5.2.2 Заполнение файла конфигурации unity.config	495
1.5.5.2.3 Работа с утилитой IndeedCM.Migrate.SAM	497
1.5.6 Работа с ключевыми носителями	500
1.5.6.1 Устройства JaCarta	501
1.5.6.1.1 Работа с устройствами JaCarta при обновлении Indeed CM на версию 4.2.0 и выше	502

1.5.6.1.2 Особенности работы с ГОСТ-областью устройств JaCarta	504
1.5.6.1.3 Добавление различных моделей JaCarta	507
1.5.6.2 Добавление различных моделей eToken	509
1.5.6.3 Изменение иконок устройства	511
1.6 Сбор программных логов	513
1.6.1 Сбор логов серверных компонентов	514
1.6.2 Сбор логов клиентских компонентов	516
1.6.2.1 Ошибки сбора логов и способы их устранения	520
1.6.3 Сбор логов инсталлятора	522
1.7 Контакты	524

Indeed Certificate Manager 6.6.0 Documentation

Общее описание

Подготовка, установка и настройка Indeed CM

- [Системные требования](#)
- [Порядок установки](#)
- [Установка и настройка серверных компонентов](#)
- [Установка клиентских компонентов](#)
- [Настройка браузеров](#)
- [Конфигурация](#)

Администрирование Indeed CM

- [Руководство администратора](#)

Справочник администратора по разделам консоли управления Indeed CM

- [Сводная информация](#)
- [Пользователи](#)
- [Устройства](#)
- [Журнал](#)
- [Агенты](#)
- [СКЗИ](#)
- [Журнал учета](#)

Руководство пользователя Indeed CM

- [Руководство пользователя](#)

Сбор программных логов

Предыдущие версии

[Indeed Certificate Manager 6.5.2](#)

[Indeed Certificate Manager 6.4.1](#)

[Indeed Certificate Manager 6.3.2](#)

[Indeed Certificate Manager 6.2.5](#)

[Indeed Certificate Manager 6.1.1](#)

[Indeed Certificate Manager 6.0.0](#)

[Indeed Certificate Manager 5.9.0](#)

[Indeed Certificate Manager 5.8.2](#)

[Indeed Certificate Manager 5.7.0](#)

[Indeed Certificate Manager 5.6.2](#)

[Indeed Certificate Manager 5.5.2](#)

[Indeed Certificate Manager 5.4.1](#)

[Indeed Certificate Manager 5.3.0](#)

[Indeed Certificate Manager 5.2.1](#)

[Indeed Certificate Manager 5.1.2](#)

Общее описание

Indeed Certificate Manager – система, предназначенная для внедрения, управления и учета аппаратных средств аутентификации пользователей в масштабах предприятия. Indeed CM обеспечивает централизованное управление средствами аутентификации в течение всего жизненного цикла, ведет учет средств криптографической защиты информации и аудит их использования. Система также позволяет быстро и самостоятельно решать проблемы пользователей без обращения к администраторам, в том числе за пределами предприятия.

- [Задачи](#)
- [Описание компонентов](#)
- [Структурная схема](#)

Задачи

Сокращение издержек компании на рутинные операции обслуживания PKI

- Выпуск сертификатов. Indeed CM автоматически формирует список сертификатов для выпуска на основе механизма политик использования PKI. Все пользователи, подпадающие под действия одной политики получают идентичный набор настроек и сертификатов. Операции по созданию запросов на сертификаты, их выпуску и записи на ключевой носитель выполняется в автоматизированном режиме.
- Рядовым пользователям системы предоставляется удобный кабинет самообслуживания, выполненный в формате web-приложения. В этом кабинете пользователи, если им разрешено политикой, могут самостоятельно производить выпуск и обновление сертификатов, снижая нагрузку на департамент ИТ.
- Indeed CM отправляет почтовые уведомления администраторам и пользователям на заданные события системы. Например, администратор и/или пользователь получают уведомление о приближении окончания срока действия сертификата, что позволяет вовремя обновить сертификат и избежать простоев в работе.
- Indeed CM позволяет производить разблокировку заблокированного носителя без визита пользователя к администратору. Такая разблокировка может быть выполнена до или после входа пользователя в операционную систему, а также с или без явного участия администратора.
- Indeed CM предоставляет программный интерфейс (API) через который он интегрируется со сторонними системами. Такая интеграция расширяет возможности по автоматизации процессов использования сертификатов и ключевых носителей. Например, по событию из системы класса Identity Management Indeed CM может отозвать сертификат уволенного сотрудника.
- В состав Indeed CM входит электронный журнал учета средств криптографической защиты информации (СКЗИ), соответствующий приказу ФАПСИ 152. Используя этот журнал, сотрудники безопасности выполняют требования регуляторов в части учета средств криптографической защиты без применения бумажных носителей и ручного заполнения необходимых данных.
- Учет сертификатов, выданных сторонними организациями. Если в организации применяются сертификаты, выданные сторонними (не собственными) удостоверяющими центрами, Indeed CM позволяет занести информацию о таких сертификатах в базу решения и своевременно напомнить администратору и пользователю о скором истечении таких сертификатов. Это позволяет избежать простоев в работе с банками и торговыми площадками.

Повышение общего уровня информационной безопасности

- Централизованное применение политики PIN-кодов. При выпуске ключевого носителя на него записываются требования к PIN: сложность, частота смены, глубина истории и другие - набор параметров зависит от модели устройства. Политики хранятся и распространяются централизованно, администраторам не нужно прописывать политики для каждого отдельного носителя.
- Учет ключевых носителей. Каждое устройство - смарт-карта или USB-токен - закрепляется за ответственным сотрудником. Операции по выпуску или обновлению сертификатов на носителе могут выполнить администратор Indeed CM или сам пользователь - владелец устройства.
- Своевременный отзыв сертификатов уволенных сотрудников. Для того, чтобы оперативно прекращать доступ уволенных сотрудников к информационным ресурсам компании, Indeed CM включает специализированный сервис, который с заданной периодичностью проверяет каталог пользователей и отзывает сертификаты у пользователей, отмеченных как уволенные.
- Гибкая настройка прав на работу с системой. Indeed CM позволяет компаниям определить собственные роли безопасности с настраиваемым перечнем разрешенных операций. Это позволяет администраторам привести ролевую модель Indeed CM в соответствие с принятыми в компании бизнес-процессами.
- Контроль использования ключевых носителей на ПК пользователей. Indeed CM позволяет компаниям отслеживать, какие носители и кем подключаются к ПК организации. Администратор может жестко закрепить ключевой носитель за пользователем или конкретным ПК. Если система обнаружит несоответствие (например, носитель подключен в сессии нелегитимного пользователя или к неразрешенному ПК), ключевой носитель может быть заблокирован.

Описание компонентов

Indeed Certificate Manager состоит из серверных и клиентских компонентов. В качестве средства хранения данных и настроек решения используется Active Directory, база данных Microsoft SQL или PostgreSQL. Расширение схемы Active Directory не требуется.

Серверные компоненты

Indeed CM Server является серверным компонентом и включает в себя Web-приложения и вспомогательные утилиты.

Web-приложения:

- **Management Console** – Консоль управления для администраторов и операторов системы.
- **Self-Service** – Сервис самообслуживания (личный кабинет) пользователя.
- **Remote Self-Service** – Сервис удаленного обслуживания за пределами домена.
- **CredProvAPI** – Сервис online-разблокировки и выключения устройств.
- **ICMAPI** – Сервис API для управления жизненным циклом устройств (для интеграции со сторонними ПО).
- **MSCA Proxy** – Позволяет запрашивать и записывать на устройства при помощи Indeed CM сертификаты со всех УЦ, находящихся за пределами того домена, в котором развернут Indeed CM.
- **Event Log Proxy** – Позволяет записывать события со всех серверов Indeed CM в единый журнал событий Windows.
- **Indeed Log Server** – Позволяет записывать события со всех серверов Indeed CM в единый журнал событий Windows, базу данных Microsoft SQL или PostgreSQL, SysLog.
- **Indeed CM Agent** – Сервисы для удаленного выполнения задач (блокировки, сброса PIN-кода пользователя, обновления содержимого устройства, очистки или инициализации устройства при его отзыве, смены PIN-кода администратора) на устройствах пользователей.

Вспомогательные утилиты:

- **IndeedCM.Agent.Cert.Generator.exe** – Утилита для создания сертификатов клиентского агента.
- **IndeedCM.Persistence.AD.Cfg.exe** – Утилита для создания хранилища данных в Active Directory.
- **IndeedCM.Persistence.KeyGen.exe** – Утилита для создания ключа шифрования.
- **IndeedCM.CertEnroll.MsCA.exe** – Утилита для выпуска сертификата "Агент регистрации".
- **IndeedCM.CardMonitor.exe** – Служба мониторинга состояния устройств.
- **IndeedCM.Wizard.exe** – Мастер настройки Indeed CM.
- **Storage.sql** – Скрипт наполнения базы данных Microsoft SQL, используемой для хранения данных Indeed CM.
- **Storage-Postgre.sql** – Скрипт наполнения базы данных PostgreSQL, используемой для хранения данных Indeed CM.

Клиентские компоненты

Indeed CM Middleware – компонент, предоставляющий единый интерфейс остальным компонентам системы по управлению устройствами, подключенными к рабочей станции.

Indeed CM Client Tools:

- **Credential Provider** – компонент для разблокировки смарт-карт, используемых для аутентификации в операционной системе Windows, в offline- и online-режимах.
- **Indeed CM Unblock** – компонент для разблокировки смарт-карт, которые не используются для входа в операционную систему.

Indeed CM Agent – клиентский агент для удаленного выполнения задач (блокировки, сброса PIN-кода пользователя, обновления содержимого устройства, очистки или инициализации устройства при его отзыве, смены PIN-кода администратора) на устройствах пользователей.

Indeed CM Client Browser Extension – компонент для поддержки множественных сессий пользователей на терминальном сервере.

Структурная схема



Установка и настройка

В разделе описаны системные требования, порядок установки и настройки компонентов Indeed Certificate Manager.

Системные требования

- [Серверные компоненты](#)
- [Клиентские компоненты](#)
- [Сетевое взаимодействие](#)
- [Поддерживаемые устройства](#)

Порядок установки

Настройка каталога пользователей

- [Каталог в Active Directory](#)
- [Каталог в Центре Регистрации КриптоПро УЦ 2.0](#)
- [Составной каталог в Active Directory и Центре Регистрации КриптоПро УЦ 2.0](#)

Создание хранилища данных

- [Active Directory](#)
- [Microsoft SQL](#)
- [PostgreSQL](#)

Настройка Центров Сертификации

- Microsoft CA
 - Создание сервисной учетной записи для работы с Microsoft CA
 - Настройка шаблонов сертификатов
 - Добавление шаблонов сертификатов
 - Выпуск сертификата Агент регистрации (Enrollment Agent)
 - Утилитой IndeedCM.CertEnroll.MsCA
 - В Диспетчере сертификатов пользователя
 - Подключение к центру сертификации Microsoft через IndeedCM MSCA Proxy
- КриптоПро УЦ 2.0
 - Создание сервисной учетной записи для работы с КриптоПро УЦ 2.0
 - Создание шаблона сертификата для сервисной учетной записи
 - Выпуск сертификата агента подачи заявок сервисной учетной записи
 - Настройка аутентификации в web-сервисах Indeed CM по сертификатам
- КриптоПро DSS 2.0
- Валидата УЦ
 - Offline-режим работы
 - Online-режим работы
 - Настройка шаблонов сертификатов пользователей

Установка и настройка серверных компонентов

- Установка сервера
- Настройка параметров системы
- Настройка клиентского агента
 - Создание сертификатов Агента
 - Настройка Indeed CM для работы с Агентами
 - Установка и настройка агентов на рабочих станциях
- Единый журнал событий
 - Event Log Proxy
 - Indeed Log Server
 - Настройка Indeed CM на работу с единым журналом событий

Установка клиентских компонентов

- Настройка разблокировки устройств
- Настройка поддержки устройств Registry

Настройка браузеров

Системные требования

Перед тем, как приступить к установке Indeed Certificate Manager, необходимо удостовериться в том, что IT-инфраструктура компании соответствует минимальным требованиям к:

- [Серверным компонентам](#)
- [Клиентским компонентам](#)
- [Сетевому взаимодействию](#)
- [Поддерживаемым устройствам аутентификации](#)

Серверные компоненты

Аппаратные требования

- Не менее 8 ГБ оперативной памяти
- Не менее 50 ГБ свободного дискового пространства
- Аппаратные требования совпадают с требованиями, предъявляемыми к операционным системам, на которых функционирует ПО

Программные требования

Операционная система:

- Windows Server 2008 SP2 32/64bit (с обновлением KB980368)
- Windows Server 2008 R2 SP1
- Windows Server 2012/2012 R2
- Windows Server 2016
- Windows Server 2019



Языком программ, не поддерживающих Юникод должен быть русский, независимо от основного языка операционной системы.

Internet Information Services 7.0 и выше со следующими модулями:

- Статическое содержимое (Static Content)
- Перенаправление HTTP (HTTP Redirection)
- ASP.NET
- Расширяемость .NET (.NET Extensibility)
- Расширения ISAPI (ISAPI Extensions)
- Фильтры ISAPI (ISAPI Filters)
- Обычная проверка подлинности (Basic Authentication)
- Windows-проверка подлинности (Windows Authentication)
- Консоль управления службами IIS (IIS Management Console)



Используйте скрипт PowerShell из дистрибутива (**IIS.Setup.Scripts**) для быстрой установки Internet Information Services с требуемыми модулями.
При развертывании сервера Indeed CM необходимо выполнить установку Microsoft .NET Framework 4.5 после установки и настройки компонента IIS.

Дополнительные компоненты Microsoft:

- Microsoft .NET Framework 4.5 и выше

Компоненты КриптоПро:

- КриптоПро CSP 4.0R4 и выше (в случае использования с Microsoft Enterprise CA, настроенного на выпуск сертификатов по алгоритмам ГОСТ Р34.10-2001/2012, КриптоПро УЦ 2.0, Валидата УЦ)
- КриптоПро CSP 5.0 и выше (в случае использования с КриптоПро DSS 2.0)



В случае использования TLS-соединения между сервером Indeed CM и Центрами Регистрации КриптоПро, и Валидата УЦ, защищенного в соответствии с Государственными Стандартами РФ, необходимо наличие серверной лицензии КриптоПро CSP.

Требования к окружению

Каталог пользователей:

- Active Directory
- Центр Регистрации КриптоПро УЦ 2.0

Центр сертификации:

- Центр сертификации предприятия Microsoft (Microsoft Enterprise CA), в том числе настроенного на выпуск сертификатов с использованием КриптоПро CSP:
 - на базе Windows Server 2003 и 2008 начиная с редакции Enterprise
 - на базе Windows Server 2012/2012 R2 всех редакций
 - на базе Windows Server 2016 всех редакций
 - на базе Windows Server 2019 всех редакций
- КриптоПро УЦ 2.0
- Валидата УЦ версии 3.1, 4.0

Хранилище данных:

- Active Directory без расширения схемы
- Microsoft SQL Server 2012 SP2 и выше всех редакций
- PostgreSQL, PostgreSQL Pro версии 10 и выше

Поддерживаемые поставщики службы криптографии (CSP):

RSA

- CSP производителя устройства (Рутокен, eToken и т.д.)
- Microsoft Base Smart Card Cryptographic Service Provider (если CSP не предоставляется производителем устройства)

 Поддерживается в том числе и в связке с УЦ КриптоПро 2.0.

ГОСТ Р34.10-2001/2012

- КриптоПро CSP 3.6R4 и выше
- Аппаратная криптография Рутокен ECP 2.0, Рутокен ECP 3.0 NFC, Рутокен 2151, JaCarta ГОСТ, JaCarta-2 ГОСТ, ESMART Token ГОСТ, MS_KEY К-"Ангара"

 Поддерживается в том числе и в связке с Microsoft Enterprise CA.

Клиентские компоненты

Аппаратные требования

- Не менее 300 МБ свободного дискового пространства
- Аппаратные требования совпадают с требованиями, предъявляемыми к операционным системам, на которых функционирует ПО

Программные требования

Операционная система:

- Windows Vista SP2 32/64bit
- Windows 7 SP1 32/64bit
- Windows 8/8.1 32/64bit
- Windows 10 32/64bit
- Windows 11 32/64bit
- Windows Server 2008 SP2 32/64bit (с обновлением KB980368)
- Windows Server 2008 R2 SP1
- Windows Server 2012/2012 R2
- Windows Server 2016
- Windows Server 2019

Требования к окружению:

- Установленные драйверы (PKI-менеджеры) используемых смарт-карт
- Internet Explorer 10 и выше
- Mozilla Firefox 52.4 и выше
- Google Chrome 64.0 и выше
- Microsoft Edge 41.16299 и выше
- КриптоПро CSP 3.6R4 и выше (в случае использования с КриптоПро УЦ)
- КриптоПро CSP 4.0R4 и выше (в случае использования с Валидата УЦ)

Сетевое взаимодействие

Сервер Indeed CM

Веб-приложения, HTTP, HTTPS

- 80 (TCP), входящие и исходящие подключения
- 443 (TCP), входящие и исходящие подключения
- 3001/3002 (TCP), входящие и исходящие подключения для Indeed AirKey Enterprise
- 3003 (TCP), входящие и исходящие подключения для Клиентского агента (Indeed CM Agent)

Почтовые уведомления, SMTP сервер

- 25 (TCP), исходящие подключения
- 465 (TCP), исходящие подключения
- 587 (TCP), исходящие подключения

Active Directory, входящие и исходящие подключения

- 53 (TCP/UDP), исходящие подключения – DNS
- 135 (TCP) – RPC
- 389 (TCP/UDP) – LDAP
- 636 (TCP) – LDAPS
- 3268 (TCP) – LDAP Global Catalog
- 3269 (TCP) – LDAP Global Catalog SSL
- 88 (TCP/UDP) – Kerberos
- 464 (TCP/UDP) – Kerberos Password Change

Microsoft SQL Server, входящие и исходящие

- 135 (TCP) – Transact-SQL debugger
- 1433 (TCP) – SQL Server default instance
- 1434 (UDP) – SQL Server Browser service
- 4022 (TCP) – Service Broker

PostgreSQL, входящие и исходящие

- 5432 (TCP/UDP) – PostgreSQL default port

Microsoft Enterprise CA, входящие и исходящие

- 135 (TCP) – RPC
- 389 (TCP/UDP) – LDAP
- 636 (TCP) – LDAPS
- Случайный DCOM/RPC (TCP) порт верхнего диапазона:
 - 1024 - 5000 для MS CA на базе Windows 2003 и более ранних версий
 - 49152 - 65535 для MS CA на базе Windows 2008 и более новых версий

 Microsoft CA реализован с помощью технологии DCOM. По умолчанию приложения DCOM используют случайные номера TCP портов верхнего диапазона. Также существует возможность настроить удостоверяющий центр на использование жестко заданного TCP порта.

КриптоПро УЦ 2.0, входящие и исходящие

- 443 (TCP) – Центр Регистрации КриптоПро УЦ 2.0

КриптоПро DSS 2.0, входящие и исходящие

- 443 (TCP) – Центр идентификации КриптоПро DSS

Валидата УЦ, входящие и исходящие

- 13434 (TCP) – Порт по умолчанию для RPC сервера Центра Регистрации Валидата УЦ. (в случае онлайн-режима работы)

Indeed Access Manager

- 80 (TCP), входящие и исходящие подключения
- 443 (TCP), входящие и исходящие подключения

Secret Net Studio, входящие и исходящие

- 135 (TCP) – RPC
- 443 (TCP) – Сервер безопасности
- 389 (TCP/UDP) – LDAP
- 636 (TCP) – LDAPS
- 5355 (TCP/UDP) – Link-Local Multicast Name Resolution (LLMNR)
- 50000/50001 (TCP) - Secret Net LDS
- 50002/50003 (TCP) - Secret Net-GC LDS

Клиентские рабочие станции

DNS

- 53 (TCP/UDP), исходящие подключения

Веб-приложения, HTTP, HTTPS

- 80 (TCP), входящие и исходящие подключения
- 443 (TCP), входящие и исходящие подключения
- 3001/3002 (TCP), входящие и исходящие подключения для Indeed AirKey Enterprise
- 3003 (TCP), входящие и исходящие подключения для Клиентского агента (Indeed CM Agent)

Схема сетевого взаимодействия

Поддерживаемые устройства

Перечень поддерживаемых устройств аутентификации и электронной подписи (USB-токенов и смарт-карт):

Производитель	Модель
Компания «Актив»	Рутокен S Рутокен Lite и Lite SC Рутокен ЭЦП PKI и ЭЦП PKI SC Рутокен ЭЦП 2.0 и ЭЦП 2.0 SC Рутокен 2151 и 2151 SC Рутокен ЭЦП 3.0 NFC и ЭЦП 3.0 NFC SC
Компания Индид	Сетевая смарт-карта AirKey
Аладдин Р.Д.	JaCarta PKI JaCarta PKI/Flash JaCarta PKI/BIO JaCarta PKI/ГОСТ JaCarta PKI/ГОСТ/Flash JaCarta-2 PKI/ГОСТ JaCarta-2 PKI/ГОСТ/Flash JaCarta-2 SE
ACS	ACOS5-64
Avest	Avest Key 256A
Bit4id	ID-One Cosmo
CRYPTAS	TicTok V2/V3
Cryptovision	ePasslet Suite v3.0, JCOP V3.0
Feitian	ePass2003 (A1+, A2) BioPass2003
HID	Crescendo C1150 Series Crescendo C1300 Series Crescendo C2300 Series

ISBC	ESMART Token 64K и ESMART Token SC 64K ESMART Token ГОСТ и ESMART Token SC ГОСТ MS_KEY К-"Ангара"
Kaztoken	Kaztoken, Kaztoken SC
Microsoft	Реестр Локального компьютера Реестр Пользователя TPM Virtual Smart Card (Microsoft VSC) - виртуальная смарт-карта на базе Trusted Platform Module v.2.0 Windows Hello for Business (WHfB)
RSA	RSA SecurID 800
Thales Group (Ex SafeNet and Gemalto)	SafeNet eToken PRO 32k SafeNet eToken PRO 64k eToken PRO Java 72K OS755 SafeNet eToken 5105 SafeNet eToken 5110 IDCore30B eToken 1.7.7 IDPrime MD 830 IDPrime MD 840 IDPrime MD 3810 IDPrime MD 3811
Yubico	YubiKey 5 Series

Порядок установки

Порядок установки и настройки Indeed Certificate Manager зависит от окружения, в котором планируется эксплуатировать систему. Данные системы Indeed CM могут храниться в Active Directory, в базе данных Microsoft SQL или PostgreSQL. Пользователи системы могут быть расположены в Active Directory и Центрах Регистрации КриптоПро УЦ 2.0. Для управления жизненным циклом персональных сертификатов пользователей Indeed CM может быть интегрирован с Microsoft Enterprise CA, КриптоПро УЦ 2.0 (в том числе, предоставляемых, как [услуги УЦ](#) компанией ООО "КРИПТО-ПРО"), КриптоПро DSS (в том числе, предоставляемых, как [услуги СЭП](#) компанией ООО "КРИПТО-ПРО") и Валидата УЦ.



Поддержка хранилища данных системы в Active Directory будет прекращена в версии 7.0.0.

Ведение [Журнала учета устройств и сертификатов](#) реализовано для конфигураций системы с использованием Хранилища данных в **Microsoft SQL** или **PostgreSQL**.

Сводная таблица конфигураций с переходами на предварительную настройку инфраструктуры, установку и настройку требуемых компонентов Indeed CM.

Предварительные настройки инфраструктуры		
Каталог пользователей	Хранилище данных	Удостоверяющий центр

Настройка каталога пользователей Active Directory	Создание хранилища данных в Active Directory	1. Создание сервисной учетной записи для работы с Microsoft CA 2. Настройка шаблонов сертификатов 3. Добавление шаблонов сертификатов 4. Выпуск сертификата Агент регистрации (Enrollment Agent) сервисной учетной записи Если Центр сертификации, располагается за пределами домена, в котором развернут сервер Indeed CM, то перейдите к инструкции по настройке интеграции с Microsoft CA через компонент Indeed CM MSCA Proxy.
Настройка каталога пользователей КристоПро УЦ 2.0	Создание и настройка хранилища данных в Microsoft SQL	1. Создание сервисной группы пользователей 2. Создание сервисной учетной записи для работы с КристоПро УЦ 2.0 3. Создание шаблона сертификата для сервисной учетной записи 4. Выпуск сертификата агента подачи заявок сервисной учетной записи Если каталог пользователей расположен только в Центре Регистрации КристоПро УЦ 2.0, то выполните настройку аутентификации в web-сервисах Indeed CM по сертификатам.
1. Настройка каталога пользователей Active Directory 2. Настройка каталога пользователей КристоПро УЦ 2.0	Создание и настройка хранилища данных в PostgreSQL	Настройка интеграции с КристоПро DSS 1. Выбор режима работы с УЦ: • Настройка Offline-режима работы • Настройка Online-режима работы 2. Настройка шаблонов сертификатов
Порядок установки и настройки		
1. Установка роли Internet Information Services (IIS) 2. Установка и настройка серверных компонентов 3. Установка клиентских компонентов 4. Настройка браузеров на рабочих станциях администраторов\операторов и пользователей системы 5. Установка и настройка Клиентского Агента (дополнительный компонент системы)		

Настройка каталога пользователей

В разделе описаны необходимые настройки каталогов пользователей для работы с Indeed Certificate Manager.

- [Каталог в Active Directory](#)
- [Каталог в Центре Регистрации КриптоПро УЦ 2.0](#)
- [Составной каталог в Active Directory и Центре Регистрации КриптоПро УЦ 2.0](#)

Каталог в Active Directory

Создание сервисной учетной записи для работы с каталогом пользователей Active Directory и хранилищем данных системы

Для полноценной работы системы Indeed Certificate Manager необходимо наличие определенных прав доступа к объектам Active Directory. В соответствии с принятой в вашей компании политикой безопасности, вы можете распределить привилегии между несколькими сервисными учетными записями, либо создать сервисную учетную запись с максимальным набором прав на управление системой.

Создайте сервисную учетную запись (например, **servicecm**), от имени которой будут выполняться операции сохранения и чтения данных в хранилище Active Directory.

Настройка каталога пользователей в Active Directory

Выдайте созданной сервисной учетной записи (**servicecm**) необходимые права для работы с объектом (доменом, контейнером, подразделением), в котором будут располагаться пользователи Indeed Certificate Manager. Эта учетная запись будет использоваться для чтения и записи атрибутов пользователей.

Для этого выполните следующее:

1. Откройте свойство **Безопасность** (Security) объекта (домена, контейнера или подразделения), в котором содержатся пользователи системы Indeed CM.
2. Нажмите **Дополнительно** (Advanced). Нажмите кнопку **Добавить** (Add). Щелкните **Выбрать субъект** (Select a principal).
3. В текстовом поле **Введите имена выбираемых объектов** (Enter the object name to select) введите имя сервисной учетной записи (**servicest**) и нажмите **ОК**.
4. В поле со списком **Применяется к** (Applies to) выберите **Дочерние объекты: Пользователь** (Descendant User objects).
5. В списке **Разрешений** (Permissions) поставьте разрешение напротив:
 - **Список содержимого** (List contents).
 - **Прочитать все свойства** (Read all properties).

 По умолчанию разрешение на чтение всех свойств пользователя имеется у всех учетных записей домена.

- **Сброс пароля** (Reset password) - Требуется для возможности **Сброса пароля пользователя** через интерфейс системы.
6. В списке **Свойств** (Properties) отметьте пункты:
 - **Запись: pwdLastSet** (Write pwdLastSet) - Также требуется для возможности сброса пароля пользователя.
 - **Запись: thumbnailPhoto** (Write thumbnailPhoto) или **Запись: jpegPhoto** (Write jpegPhoto) - Требуется для возможности **Загрузки фотографии пользователю** в Active Directory через интерфейс системы.
 - **Запись: userAccountControl** (Write userAccountControl) - Необходима для работы опции **Требовать логон по смарт-карте**.
 - **Запись: userCertificate** (Write userCertificate) - Требуется для возможности **Публиковать сертификат КристоПро 2.0** в профиль пользователя Active Directory.
 7. Нажмите **ОК** и затем **Применить** (Apply).

 Установите одинаковый набор прав сервисной учетной записи для каждого объекта (домена, контейнера или подразделения), в котором располагаются пользователи Indeed CM.

Если в домене чтение всех свойств пользователя запрещено политиками безопасности, то выдайте сервисной учетной записи права на чтение только необходимых атрибутов пользователей, описанных ниже в таблице **и атрибутов объекта** (домена, контейнера или подразделения), в котором располагаются пользователи Indeed CM.

1. В оснастке **Редактирование ADSI** (ADSI edit) откройте свойство **Безопасность** (Security) объекта (домена, контейнера или подразделения), в котором содержатся пользователи системы Indeed CM.
2. Для области применения **Этот объект и все дочерние объекты** (This object and all descendant objects).
 - В списке **Разрешений** (Permissions) отметьте **Список содержимого** (List contents).
 - В списке **Свойств** (Properties) отметьте пункты:
 - **Чтение: canonicalName** (Read canonicalName)
 - **Чтение: Distinguished Name** (Read Distinguished Name)
 - **Чтение: objectClass** (Read objectClass)
 - **Чтение: objectGuid** (Read objectGuid)
 - **Чтение: showInAdvancedViewOnly** (Read showInAdvancedViewOnly)
3. Для области применения **Дочерние объекты: Пользователь** (Descendant user objects).
 - В списке **Разрешений** (Permissions) отметьте **Список содержимого** (List contents).
 - В списке **Свойств** (Properties) выберите чтение/запись следующих наборов свойств и атрибутов, соответствующих таблице:
 - **Чтение: личные сведения** (Read personal Information)
 - **Чтение: общие сведения** (Read general Information)
 - **Чтение: ограничения учетной записи** (Read account restrictions)
 - **Чтение: открытые сведения** (Read public Information)
 - **Запись: pwdLastSet** (Write pwdLastSet)
 - **Запись: thumbnailPhoto** (Write thumbnailPhoto) или **Запись: jpegPhoto** (Write jpegPhoto)
 - **Запись: userAccountControl** (Write userAccountControl)
 - **Запись: userCertificate** (Write userCertificate)



Приведены отображаемые имена **LDAP** (LDAP Display Name).

Предоставление прав доступа к набору свойств значительно улучшает производительность и упрощает управление безопасностью (см. [Наборы свойств Active Directory](#)).

Атрибуты, используемые Indeed CM при работе с каталогом пользователей.

Атрибут (LDAP Display Name)	Common Name	Комментарий

c	Country/Region или Country /Region Abbreviation	Входит в набор свойств «Личные сведения» (Personal Information).
canonicalName	Canonical Name	Входит в набор свойств «Открытые сведения» (Public Information).
cn	Common Name	Входит в набор свойств «Открытые сведения» (Public Information).
company	Company	Входит в набор свойств «Открытые сведения» (Public Information).
department	Department	Входит в набор свойств «Открытые сведения» (Public Information).
distinguishedName	Distinguished Name	Входит в набор свойств «Открытые сведения» (Public Information).
givenName	Given Name	Входит в набор свойств «Открытые сведения» (Public Information).
l	Locality Name	Входит в набор свойств «Личные сведения» (Personal Information).
mail	E-mail Addresses	Входит в набор свойств «Открытые сведения» (Public Information).
manager	Manager	Входит в набор свойств «Открытые сведения» (Public Information).
objectClass	Object Class	Входит в набор свойств «Открытые сведения» (Public Information).
objectGUID	Object GUID	Входит в набор свойств «Открытые сведения» (Public Information).
objectSid	Object Sid	Входит в набор свойств «Общие сведения» (General Information).
otherMailbox	Other Mailbox	Входит в набор свойств «Открытые сведения» (Public Information).
proxyAddresses	Proxy Addresses	Входит в набор свойств «Открытые сведения» (Public Information).
pwdLastSet	Pwd Last Set	Входит в набор свойств «Ограничения учетной записи» (Account Restrictions).
sAMAccountName	SAM Account Name	Входит в набор свойств «Общие сведения» (General Information).
sn	Surname	Входит в набор свойств «Открытые сведения» (Public Information).
st	State or Province Name	Входит в набор свойств «Личные сведения» (Personal Information).
streetAddress	Address (или Street)	Входит в набор свойств «Личные сведения» (Personal Information).

telephoneNumber	Telephone Number	Входит в набор свойств «Личные сведения» (Personal Information).
thumbnailPhoto или jpegPhoto	Picture	Входит в набор свойств «Личные сведения» (Personal Information).
userAccountControl	User Account Control	Входит в набор свойств «Ограничения учетной записи» (Account Restrictions).
userCertificate	User Certificate	Входит в набор свойств «Личные сведения» (Personal Information).
userPrincipalName	User Principal Name	Входит в набор свойств «Открытые сведения» (Public Information).

Каталог в Центре Регистрации КриптоПро УЦ 2.0

Создание сервисной группы пользователей в Центре Регистрации КриптоПро

Для взаимодействия системы Indeed Certificate Manager с КриптоПро УЦ 2.0 необходимо наличие сервисной учетной записи, от имени которой Indeed CM будет обращаться к УЦ для запроса сертификатов пользователей. Вы можете использовать любую имеющуюся в Центре Регистрации учетную запись в качестве сервисной, поместив ее в предварительно созданную и наделенную необходимыми полномочиями сервисную группу системы Indeed CM.

Для создания такой группы и сервисной учетной записи выполните следующие действия:

1. Создайте группу безопасности с произвольным именем, например, **Indeed CM Service Users** в Консоли управления ЦР.
2. Откройте свойства папки, в которой будут располагаться пользователи Indeed CM, и перейдите на вкладку **Безопасность**.
3. Добавьте созданную группу **Indeed CM Service Users**.
4. Выдайте группе **Indeed CM Service Users** следующие разрешения:

Разрешения: Папок

- Чтение свойств (необходимо выдать и для корневой папки «Центр Регистрации» с наследованием для чтения списка пользователей)
- Запись свойств (необходимо выдать и для корневой папки «Центр Регистрации» с наследованием для публикации списка отозванных сертификатов)
- Запрос регистрации
- Одобрение регистрации

Разрешения: Пользователей

- Чтение свойств
- Запрос переименования
- Запрос сертификата
- Запрос аннулирования
- Запрос приостановления
- Запрос возобновления
- Одобрение переименования
- Одобрение сертификата (необходимо выдать и для корневой папки «Центр Регистрации» с наследованием)
- Одобрение аннулирования
- Одобрение приостановления
- Одобрение возобновления

Разрешения: Шаблонов

- Запрос сертификата
- Одобрение сертификата (необходимо выдать и для корневой папки «Центр Регистрации» с наследованием)

Составной каталог в Active Directory и Центре Регистрации КriptoПро УЦ 2.0

Для работы Indeed Certificate Manager с составным каталогом пользователей в Active Directory и КriptoПро УЦ 2.0 необходимо выполнить:

- [Настройку каталога пользователей в Active Directory](#)
- [Настройку каталога пользователей в Центре Регистрации КriptoПро УЦ 2.0](#)

Создание хранилища данных

В разделе описаны методы создания хранилищ данных Indeed Certificate Manager:



Поддержка хранилища данных системы в Active Directory будет прекращена в версии 7.0.0.

- [Active Directory](#)
- [Microsoft SQL](#)
- [PostgreSQL](#)

Active Directory

Хранилище данных Indeed Certificate Manager создается при помощи утилиты **IndeedCM.PersistenceAD.Cfg.exe** (располагается в каталоге Misc дистрибутива сервера).



Для продуктовых инсталляций не рекомендуется использование хранилища данных системы в Active Directory. Поддержка хранилища данных системы в Active Directory будет прекращена в версии 7.0.0.

В общем случае, для создания хранилища при помощи утилиты IndeedCM.Persistence.AD.Cfg.exe в корне домена необходимо наличие прав Администратора Домена (Domain Admins), либо администратор домена может создать вручную **Подразделение** (Organizational Unit) с произвольным именем и предоставить полный доступ на управление этим подразделением и всеми его дочерними объектами сервисной учетной записи (**servicem**), от имени которой будет запущена утилита IndeedCM.Persistence.AD.Cfg.exe.

Для создания хранилища данных запустите утилиту **IndeedCM.Persistence.AD.Cfg.exe** с параметром **/create <LDAP Path> <container name> <subcontainer name>**, где:

- **LDAP Path** – путь к контейнеру или корню домена, в котором необходимо создать хранилище.
- **container name** – имя контейнера, в котором будут храниться все данные системы.
- **subcontainer name** – имя подконтейнера.

Пример:

```
IndeedCM.Persistence.AD.Cfg.exe /create LDAP://OU=MSK Office,DC=demo,DC=local" "Indeed Identity" "Indeed CM"
```

Пример запуска и выполнения команды для создания хранилища данных в подразделении *MSK Office*, домена *demo.local* с именем контейнера *Indeed Identity* и именем подконтейнера *Indeed CM*.

```
C:\Windows\system32\cmd.exe

C:\Misc>IndeedCM.Persistence.AD.Cfg.exe /create LDAP://OU=MSK Office,DC=demo,DC=local" "Indeed Identity" "Indeed CM"
Storage has been created successfully.

C:\Misc>
```

Выдайте сервисной учетной записи (**servicest**) **Полные права** (Full Control) на **Этот объект и все дочерние объекты** (This object and all descendant objects) для созданного контейнера Indeed Identity.

Для этого выполните следующее:

1. Откройте свойство **Безопасность** (Security) контейнера Indeed Identity.
2. Нажмите **Добавить** (Add) и укажите сервисную учетную запись (servicest).
3. Нажмите **Дополнительно** (Advanced), выберите сервисную учетную запись и нажмите **Изменить** (Edit).
4. Выберите область применения **Этот объект и все дочерние объекты** (This object and all descendant objects).
5. Установите разрешение **Полный доступ** (Full control) в списке **Разрешений** (Permissions).
6. Нажмите **ОК** и затем **Применить** (Apply).

Microsoft SQL

Хранилище данных Indeed Certificate Manager представляет собой базу данных. База данных создается вручную, а для ее наполнения используются скрипт **Storage.sql**, входящий в состав дистрибутива Indeed CM (скрипт располагается в каталоге \IndeedCM.Server\Misc).

1. Создайте базу данных в среде SQL Management Studio с произвольным именем:
 - В окне **Обозреватель объектов** (Object Explorer) нажмите правой кнопкой мыши по вкладке **Базы данных** (Databases).
 - Выберите **Создать базу данных...** (New Database...).
 - Укажите **Имя базы данных:** (Database name:) например, **IndeedCM** и нажмите **OK**.

Создание базы данных

Выбор страницы

- Общие
- Параметры
- Файловые группы

Соединение

Сервер: INDEEDCMRU\SQLEXPRESS

Соединение: DEMO\adm

[Просмотреть свойства соединения](#)

Ход выполнения

Готово

Имя базы данных: IndeedCM

Владелец: <по умолчанию>

☒ Использовать полнотекстовое индексирование

Файлы базы данных:

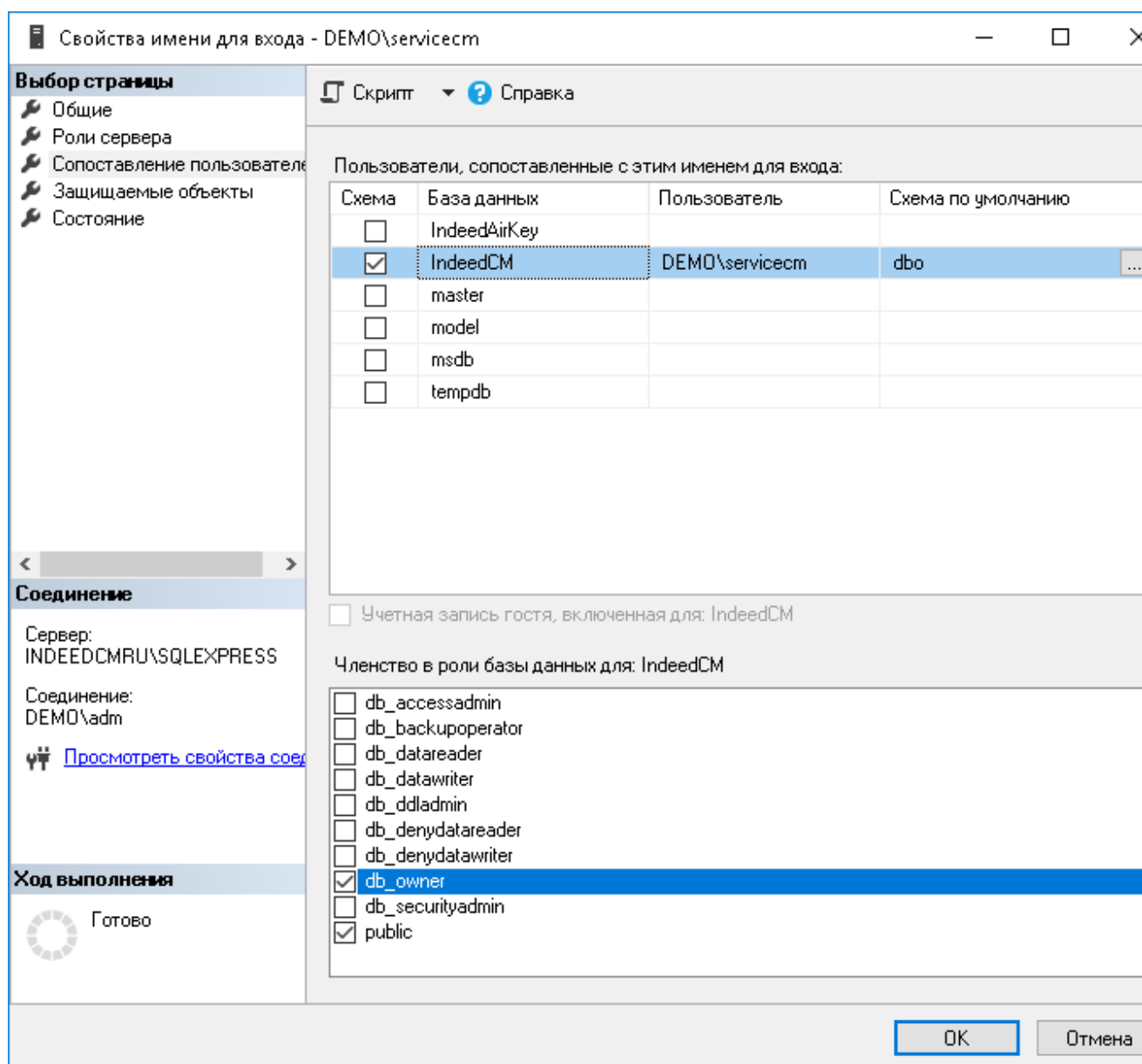
Логическое имя	Тип файла	Файловая группа	Начальный размер (МБ)	Автоувеличение
IndeedCM	Данные ...	PRIMARY	8	С шагом по 8
IndeedCM_log	ЖУРНАЛ	Неприменимо	8	С шагом по 8

Добавить Удалить

OK Отмена

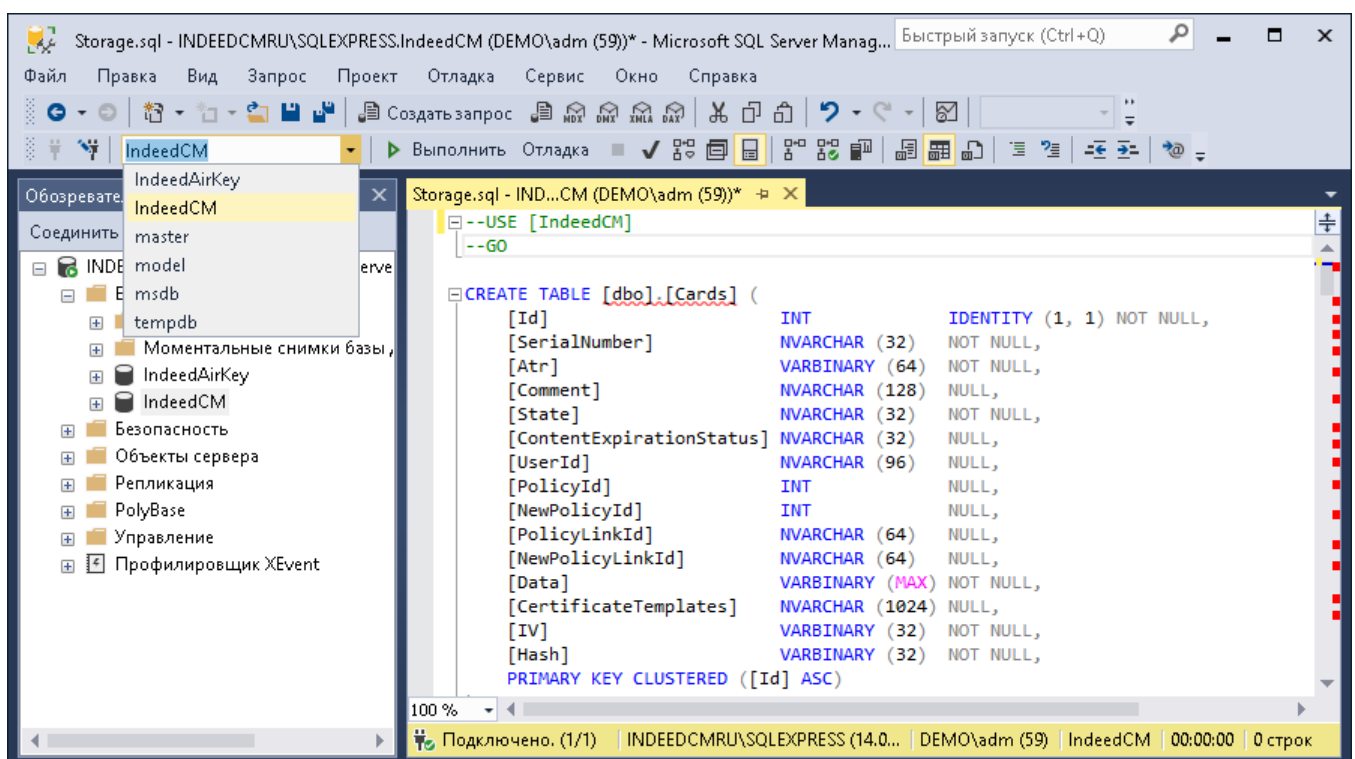
2. Используйте локальную учетную запись SQL или учетную запись Active Directory (например, **servicecm**) и наделите её необходимыми правами для работы с созданной базой данных. Данная учетная запись будет использоваться для выполнения операций чтения и записи в базу данных. Настройка подключения к базе с использованием указанной учетной записи производится в Мастере настройки Indeed CM.

- Определите **Имя для входа** (Logins) для созданной базы (например, **servicecm**).
- Нажмите **Безопасность** (Security) > **Имя для входа** (Logins), из списка выберите учетную запись.
- Перейдите на вкладку **Сопоставление пользователей** (User Mapping).
- Выдайте права на работу с базой для выбранного имени входа, укажите разрешения: **db_owner** и **public** и нажмите **OK**.



3. Выберите в **Обозревателе объектов** (Object Explorer) созданную базу данных (**IndeedCM**) и выполните скрипт **Storage.sql**:

- Выберите меню **Файл** (File) > **Открыть** (Open) > **Файл...** (File...), укажите путь к файлу **Storage.sql** (располагается в каталоге `..\IndeedCM.Server\Misc`) и нажмите **Открыть** (Open).
- До запуска скрипта раскомментируйте: `--USE [<database name>]--GO` и укажите название базы данных, для которой применяется скрипт (**IndeedCM**): `--USE [Indeed CM]--GO`. Или выберите необходимую базу данных в выпадающем меню.
- Нажмите **Выполнить** (Execute).

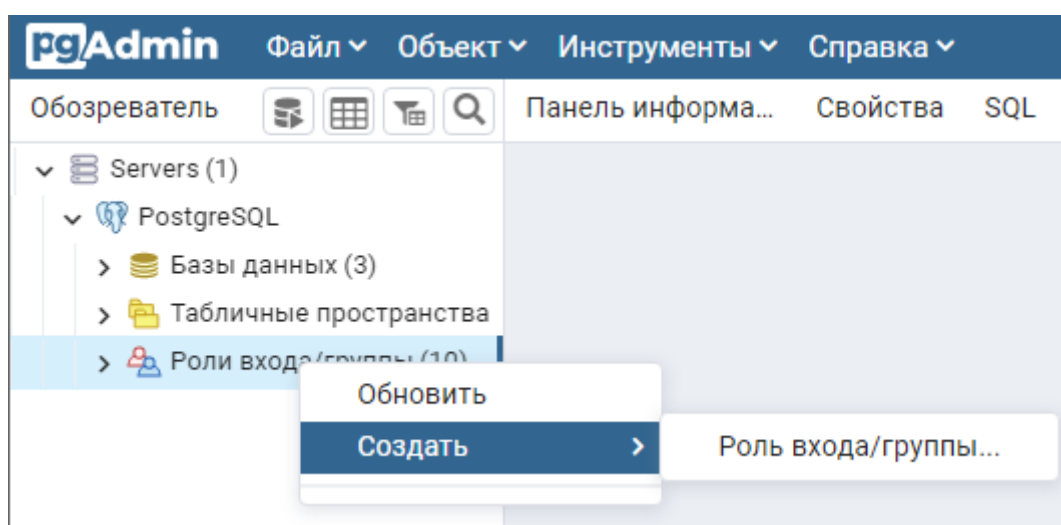


PostgreSQL

Создание сервисной учётной записи

Хранилище данных Indeed Certificate Manager представляет собой базу данных. Для работы системы с базой данных необходимо создать сервисную учётную запись и выдать права для работы с ней.

1. Откройте **pgAdmin**, укажите мастер пароль и подключитесь к серверу.
2. В разделе **Обозреватель** (Browser) Правой кнопкой мыши нажмите по пункту меню **Роли входа/группы** (Login/Group Roles).
3. Выберите **Создать** > **Роль входа/группы** (Create > Login/Group Role....)

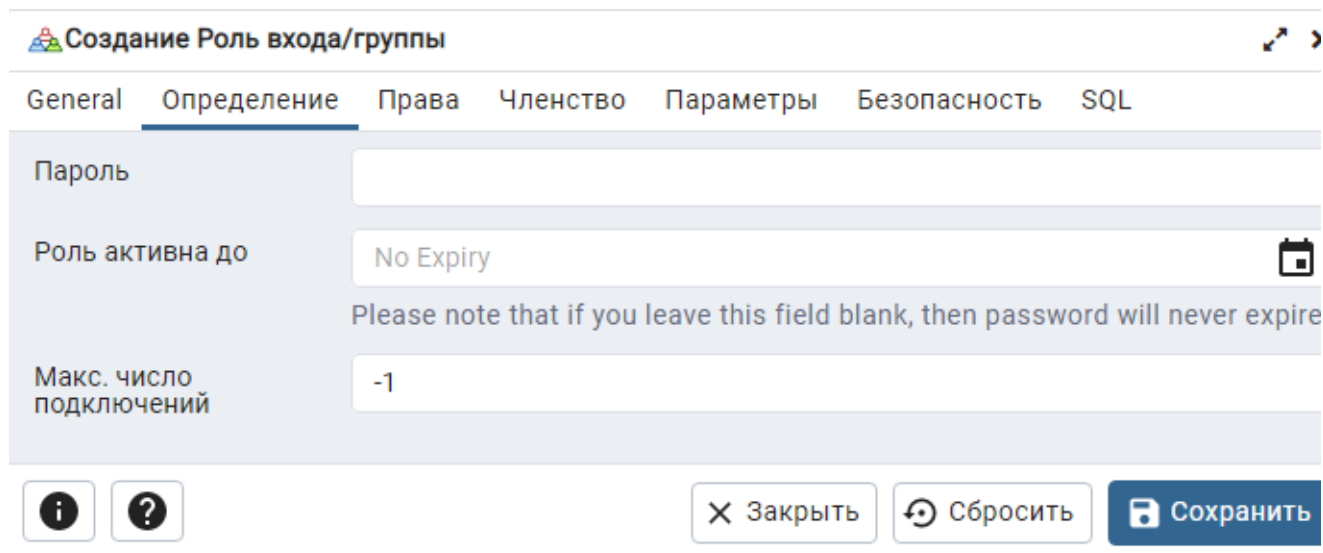


4. На вкладке **Общие** (General), в поле **Имя** (Name), укажите произвольное имя пользователя, например **servicepg**.

A screenshot of the 'Создание Роль входа/группы' (Create Login/Group Role) dialog box in pgAdmin. The 'General' tab is active. It contains a text input field for 'Имя' (Name) with the value 'servicepg' and a larger text area for 'Комментарии' (Comments). At the bottom, there are three buttons: 'Закрыть' (Close), 'Сбросить' (Reset), and 'Сохранить' (Save).

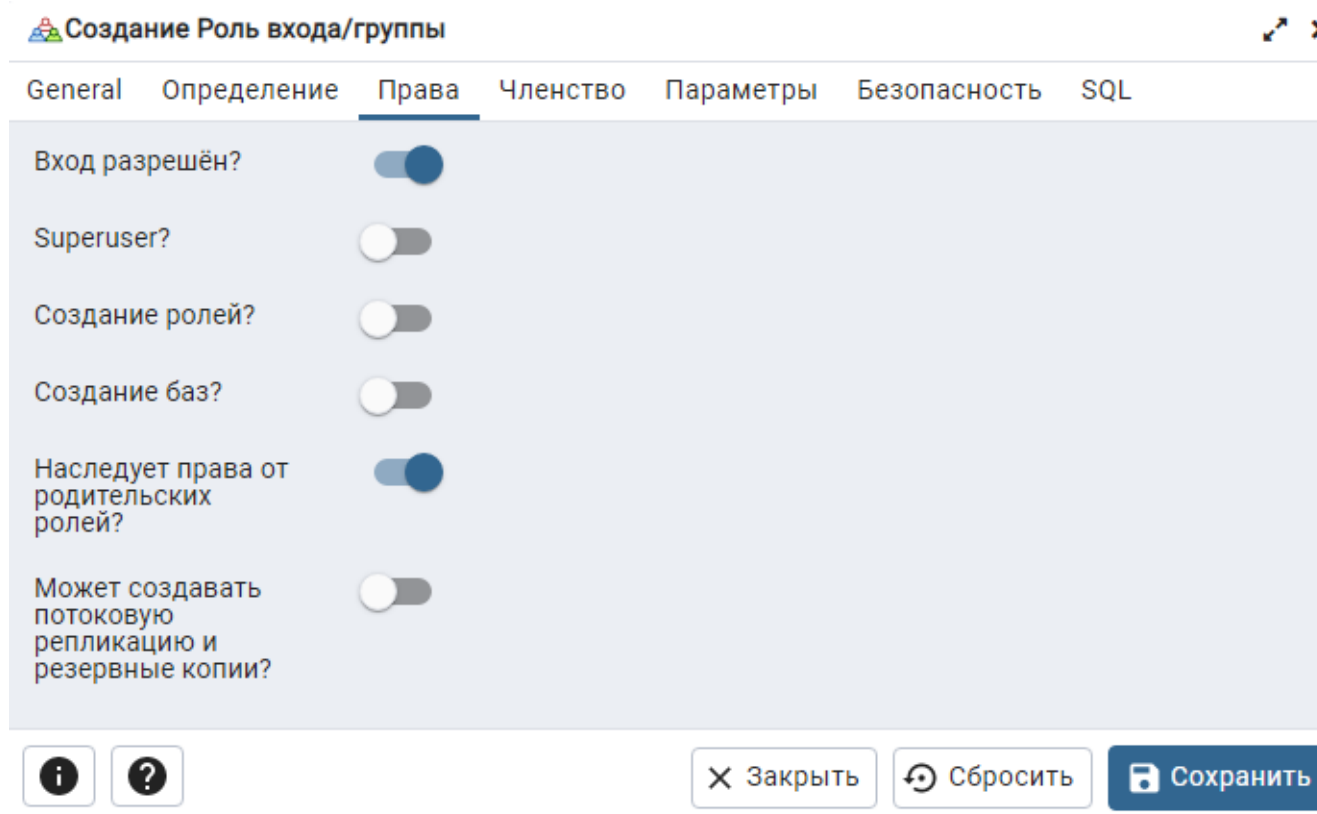
5. На вкладке **Определение** (Definition), в поле **Пароль** (Password), укажите пароль пользователя. В поле **Роль активна до** (Account Expires) должно быть указано значение **No Expiry**.

 При создании сервисной учётной записи требуется отключить срок действия пароля.



The screenshot shows the 'Definition' tab of the 'Create Role/Group' window. It contains three input fields: 'Password' (empty), 'Role active until' (set to 'No Expiry' with a calendar icon), and 'Max. number of connections' (set to '-1'). A note below the second field states: 'Please note that if you leave this field blank, then password will never expire'. At the bottom are buttons for 'Close' (Заккрыть), 'Reset' (Сбросить), and 'Save' (Сохранить).

6. На вкладке **Права** (Privileges) включите параметр **Вход разрешён?** (Can Login?).



The screenshot shows the 'Privileges' tab of the 'Create Role/Group' window. It features a list of toggle switches: 'Can login?' (Вход разрешён?) is turned on, 'Superuser?' is off, 'Create roles?' (Создание ролей?) is off, 'Create databases?' (Создание баз?) is off, 'Inherits privileges from parent roles?' (Наследует права от родительских ролей?) is on, and 'Can create streaming replication and backup?' (Может создавать потоковую репликацию и резервные копии?) is off. At the bottom are buttons for 'Close' (Заккрыть), 'Reset' (Сбросить), and 'Save' (Сохранить).

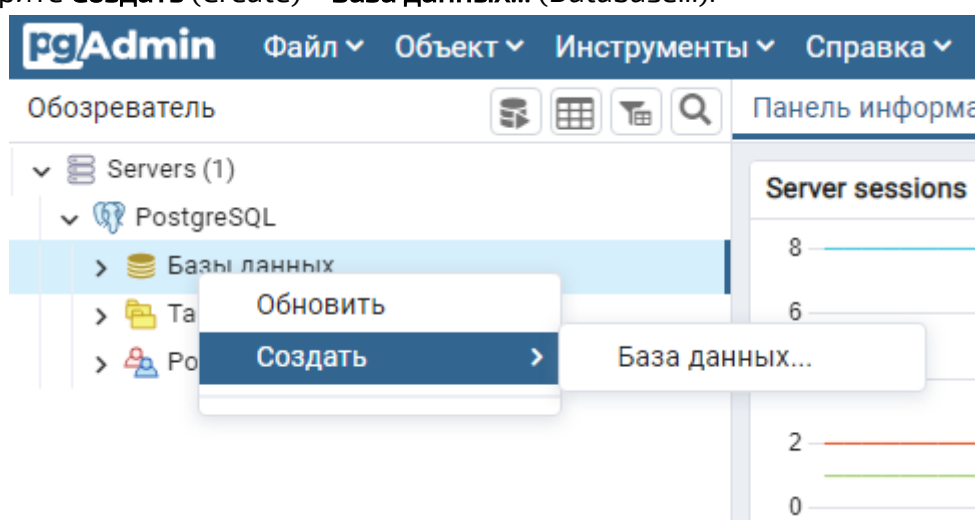
7. Оставьте остальные значения по умолчанию и нажмите **Сохранить** (Save).

Создание базы данных

База данных создаётся вручную, а для её наполнения используются скрипт **Storage-Postgre.sql**, входящий в состав дистрибутива Indeed CM (скрипт располагается в каталоге \IndeedCM.Server\Misc).

1. Создайте базу данных в среде **pgAdmin** с произвольным именем:

- В окне **Обозреватель** (Browser) нажмите правой кнопкой мыши по пункту **Базы данных** (Databases).
- Выберите **Создать** (Create) > **База данных...** (Database...).



- На вкладке **Общие** (General) укажите название базы данных в поле **База данных** (Database), например, **IndeedStorage**, выберите пользователя созданного на первом этапе (**servicepg**) из списка **Владелец** (Owner) и нажмите **Сохранить** (Save).

Создание База данных

General Определение Безопасность Параметры Дополнительно SQL

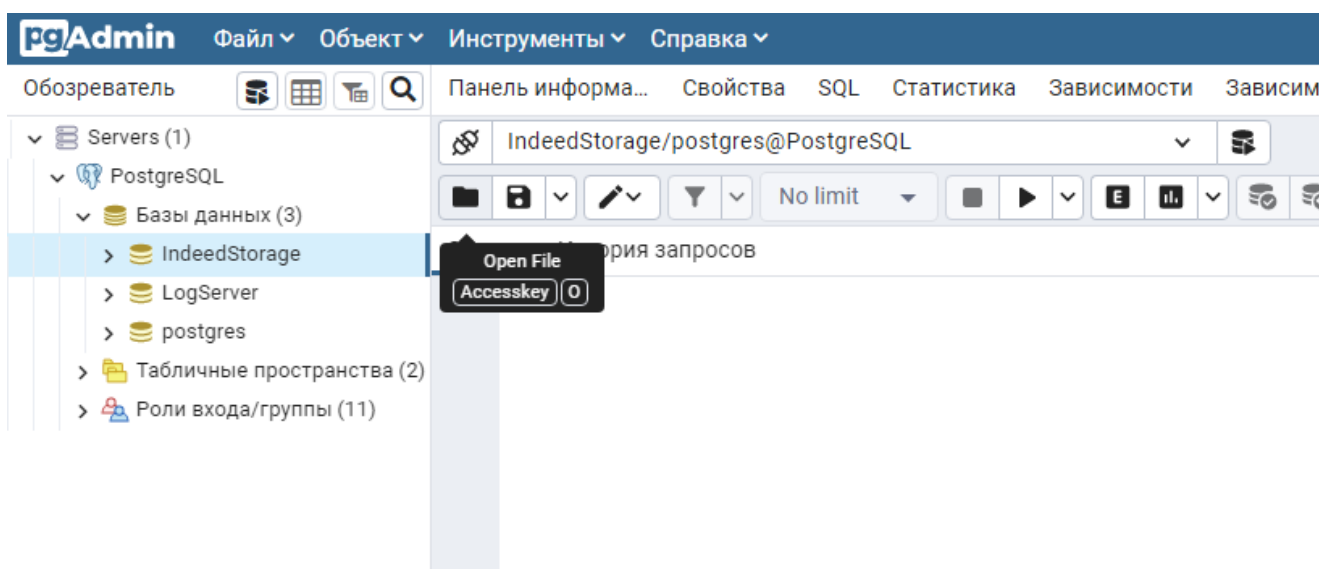
База данных: IndeedStorage

Владелец: servicepg

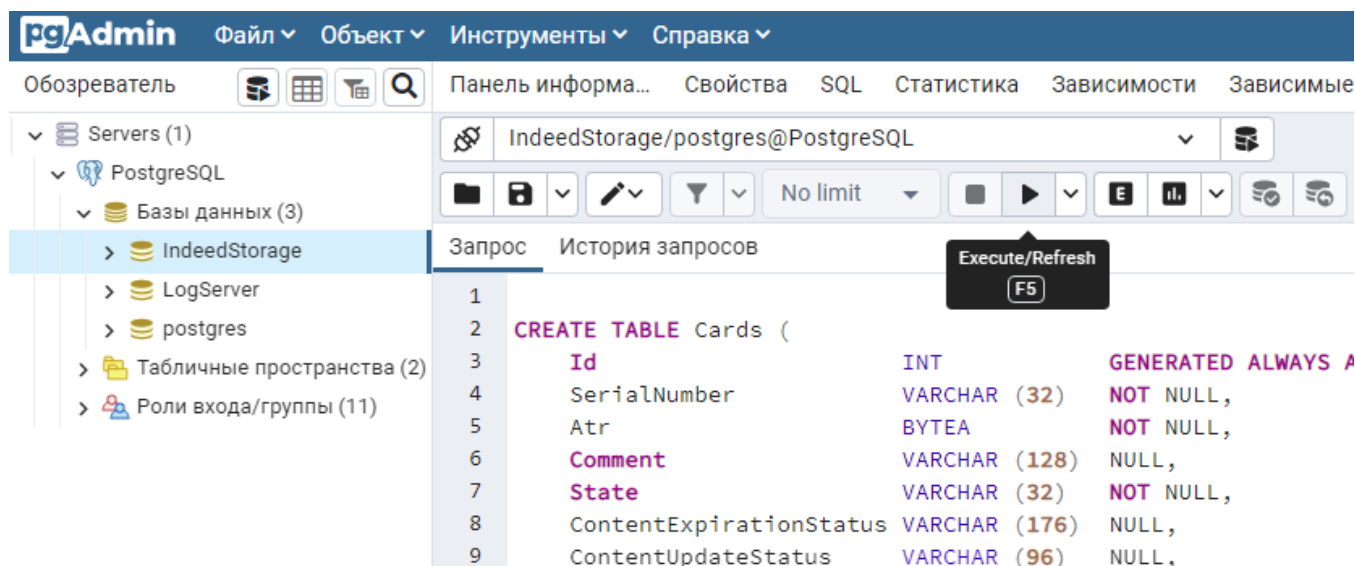
Комментарий:

2. Выберите в **Обозревателе** (Browser) созданную базу данных (**IndeedStorage**) и выполните скрипт **Storage-Postgre.sql**:

- Выберите меню **Инструменты** (Tools) > **Запросник** (Query Tool).
- В меню Запросника нажмите на значок  для открытия файла скрипта и укажите путь к файлу **Storage-Postgre.sql** (располагается в каталоге \IndeedCM.Server\Misc) и нажмите **Выбрать** (Select).

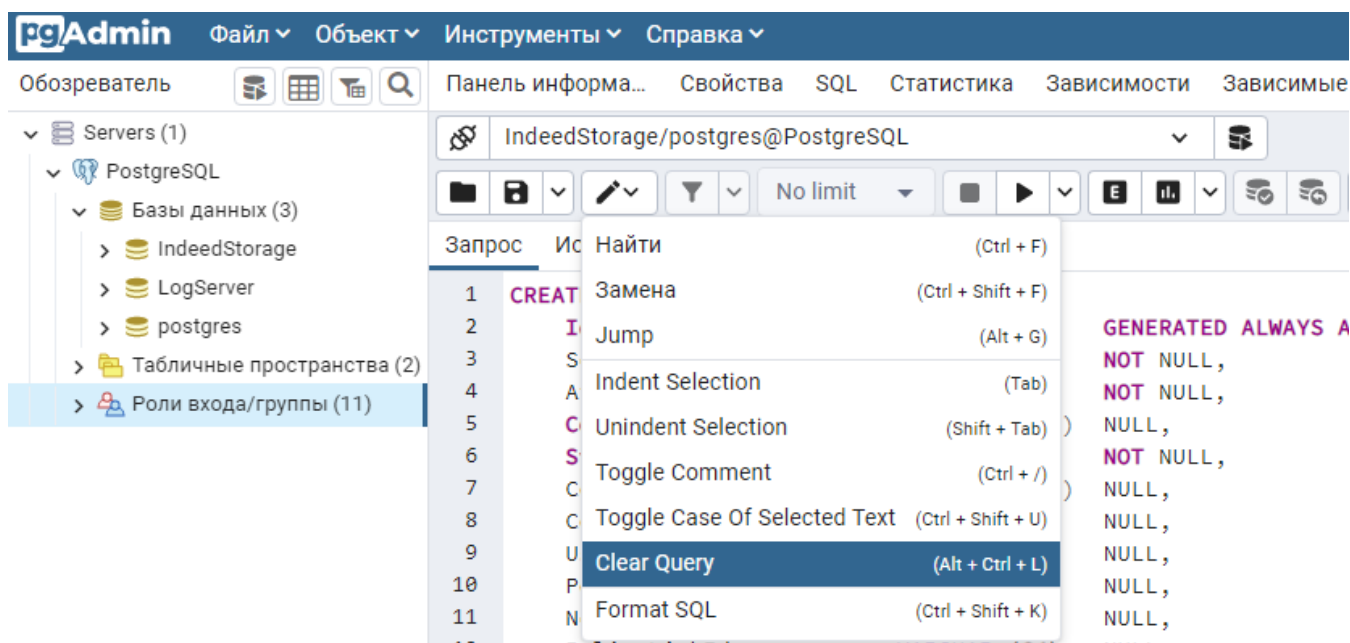


- В меню Запросника нажмите на кнопку **Выполнить** (Execute/Refresh) .



3. Предоставление привилегий сервисной учётной записи на таблицы базы данных

- Нажмите в меню **Запросника** (Query Tool) на кнопку  затем выберите **Clear Query**, чтобы очистить поле запроса к базе данных.



- Введите текст запроса, указав в запросе имя учётной записи:

```
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA public TO "имя сервисной учётной записи";
```

Пример:

```
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA public TO servicepg;
```

- В меню Запросника нажмите на кнопку **Выполнить** (Execute/Refresh) ► .

Настройка удалённого подключения к БД

Откройте конфигурационный файл PostgreSQL "pg_hba.conf"

i **Расположение файла pg_hba.conf**

Для Windows C:\Program Files\PostgreSQL\< >\data

Для *nix /etc/postgresql/< >/main

Добавьте строку следующего формата:

```
CONNECTIONTYPE DATABASE USER ADDRESS METHOD
```

Где:

- **CONNECTIONTYPE** - Тип подключения. Указывается "host" - будет использоваться подключение по TCP/IP.
- **DATABASE** - Имя базы данных, для которой предоставляется доступ.
- **USER** - Имя пользователя, для которого будет доступно подключение.
- **ADDRESS** - IP-адрес удалённого сервера Indeed Certificate Manager.
- **METHOD** - Метод аутентификации пользователя.

Пример:

```
host IndeedStorage servicepg 192.200.1.0/24 md5
```

Настройка Центров Сертификации

В разделе описаны основные настройки центров сертификации для работы с Indeed Certificate Manager.

Microsoft CA

- [Создание сервисной учетной записи для работы с Microsoft CA](#)
- [Настройка шаблонов сертификатов](#)
- [Добавление шаблонов сертификатов](#)
- [Выпуск сертификата Агент регистрации \(Enrollment Agent\)](#)
 - [Утилитой IndeedCM.CertEnroll.MsCA](#)
 - [В Диспетчере сертификатов пользователя](#)
- [Подключение к центру сертификации Microsoft через IndeedCM MSCA Proxy](#)

КриптоПро УЦ 2.0

- [Создание сервисной учетной записи для работы с КриптоПро УЦ 2.0](#)
- [Создание шаблона сертификата для сервисной учетной записи](#)
- [Выпуск сертификата агента подачи заявок сервисной учетной записи](#)
- [Настройка аутентификации в web-сервисах Indeed CM по сертификатам](#)

КриптоПро DSS 2.0

Валидата УЦ

- [Offline-режим работы](#)
- [Online-режим работы](#)
- [Настройка шаблонов сертификатов пользователей](#)

Microsoft CA

Для настройки работы Indeed Certificate Manager с Microsoft Enterprise CA выполните следующие действия:

1. [Создайте сервисную учетную запись для работы с Microsoft CA](#)
2. [Выполните настройку шаблонов сертификатов](#)
3. [Добавьте подготовленные шаблоны сертификатов в список выдаваемых](#)
4. [Выпустите сертификат Агента регистрации \(Enrollment Agent\) сервисной учетной записи](#)

Если центры сертификации Microsoft, располагаются за пределами домена, в котором развернут сервер Indeed CM, то перейдите к инструкции [по подключению к центру сертификации Microsoft через компонент IndeedCM MSCA Proxy](#).

Создание сервисной учетной записи для работы с Microsoft CA

Для работы с Microsoft CA необходимо создать сервисную учетную запись, от имени которой Indeed CM будет запрашивать сертификаты пользователей в центре сертификации.

Выполните следующие действия:

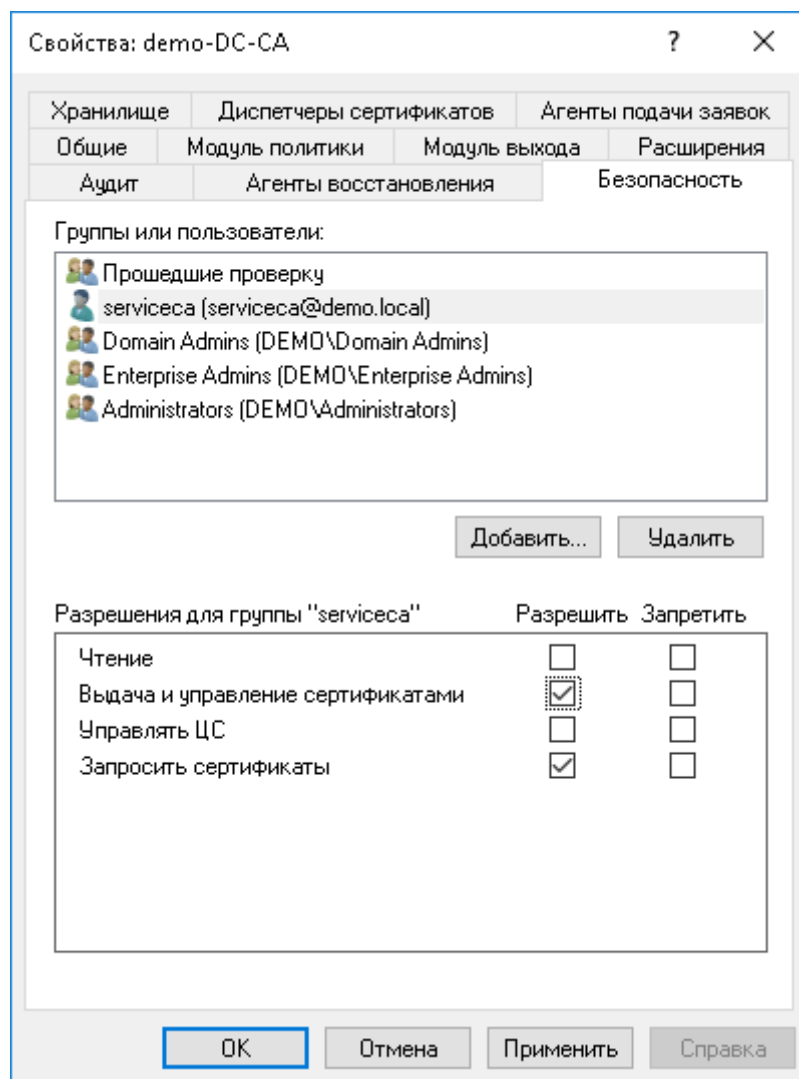
1. Создайте учетную запись пользователя в Active Directory (например, **serviceca**).
2. Откройте оснастку **Центр сертификации** (Certification Authority), выберите центр сертификации и перейдите в его **Свойства** (Properties).
3. На вкладке **Безопасность** (Security) нажмите **Добавить** (Add) и укажите имя созданной учетной записи.
4. Задайте разрешение **Выдача и управление сертификатами** (Issue and Manage Certificates). Разрешение **Запросить сертификаты** задано по умолчанию.
5. Нажмите **ОК**, чтобы сохранить настройки.



Включите разрешение **Управлять ЦС**, чтобы иметь возможность **Публиковать список отозванных сертификатов** при настройке шаблонов сертификатов для ЦС.



Если вы планируете использовать Indeed CM с несколькими центрами сертификации (ЦС), сервисная учетная запись должна иметь одинаковый набор привилегий для всех ЦС.



Настройка шаблонов сертификатов

Для работы с Indeed Certificate Manager обязательно необходим шаблон сертификата **Агент регистрации** (Enrollment Agent). Сертификат **Агент регистрации** (Enrollment Agent), выданный на имя сервисной учетной записи (**serviceca**) необходим для подписи запроса на сертификат от имени других пользователей по всем остальным шаблонам сертификатов, которые будут использоваться системой Indeed CM.

Ниже описан процесс настройки шаблона сертификата пользователя на примере шаблона **Вход со смарт-картой** (Smartcard Logon), который будет использоваться для выпуска сертификатов, предназначенных для входа в операционную систему по смарт-карте.

1. Откройте консоль управления **Центр сертификации** (Certification Authority).
2. Перейдите в раздел **Шаблоны сертификатов** (Certificate Templates), щелкните правой кнопкой мыши выберите **Управление** (Manage).
3. Щелкните правой кнопкой мыши по шаблону **Вход со смарт-картой** (Smartcard Logon) и выберите **Скопировать шаблон** (Duplicate Template).
4. Перейдите на вкладку **Общие** (General) и в поле **Отображаемое имя шаблона** (Template display name) введите **Indeed Smart Card Logon**. Измените **Период действия** (Validity period) и **Период обновления** (Renewal period) в соответствии с потребностями вашей организации.
5. На вкладке **Шифрование** (Cryptography) в поле **Минимальный размер ключа** (Minimum key size) укажите необходимую длину ключа.

✔ Опция доступна для Microsoft CA 2008/2008R2 и выше. В предыдущих версиях настройка осуществляется на вкладке **Обработка запроса** (Request Handling).

⚠ Обратите внимание на размер ключей шифрования указанный в свойствах шаблонов сертификатов, которые планируется использовать. Чтобы снизить риск несанкционированного доступа к конфиденциальной информации компания Майкрософт выпустила несвязанное с безопасностью обновление ([KB 2661254](#)) для всех поддерживаемых версий Microsoft Windows. Это обновление блокирует криптографические ключи меньше 1024 бит. Обновление не относится к Windows 8 (и выше) или Windows Server 2012 (и выше), т.к. эти операционные системы уже могут блокировать использование ключей RSA меньше 1024 бит.

6. На вкладке **Требования выдачи** (Issuance Requirements):

- Установите опцию **Одобрения диспетчера сертификатов ЦС** (CA certificate manager approval).
- Установите флажок **Указанного числа авторизованных подписей** (This number of authorised signatures) и укажите число подписей, равное **1** (значение по умолчанию).
- Выберите **Политики применения** (Application Policy) из списка **В подписи требуется указать тип политики** (Policy type required in signature).
- Выберите **Агент запроса сертификата** (Certificate Request Agent) из списка **Политика применения** (Application Policy).
- Выберите параметр **Тех же условий, что и для регистрации** (Same criteria as for enrollment) в разделе **Требовать для повторной регистрации** (Require the following for reenrollment).

The screenshot shows the 'Indeed Smart Card Logon' properties dialog box with the 'Issuance Requirements' tab selected. The dialog has a title bar with a question mark and a close button. Below the title bar is a tabbed interface with four tabs: 'Устаревшие шаблоны', 'Расширения', 'Безопасность', and 'Сервер'. The 'Безопасность' tab is active, showing sub-tabs: 'Общие', 'Совместимость', and 'Обработка запроса'. The 'Обработка запроса' sub-tab is selected, displaying the 'Требования выдачи' section.

Требования выдачи

Требовать для регистрации:

- ☒ Одобрения диспетчера сертификатов ЦС
- ☒ Указанного числа авторизованных подписей:

Автоматическая регистрация не разрешена (если требуется более одной подписи).

В подписи требуется указать тип политики:

Политика применения:

Политика применения:

Политики выдачи:

Требовать для повторной регистрации:

- ☒ Тех же условий, что и для регистрации
- ☐ Подтвердить существующий сертификат
- ☐ Разрешить обновление на основе ключей (*)

Требует предоставлять данные о субъекте в запросе сертификата.

* Элемент управления отключен из-за [параметров совместимости](#).

Buttons at the bottom:

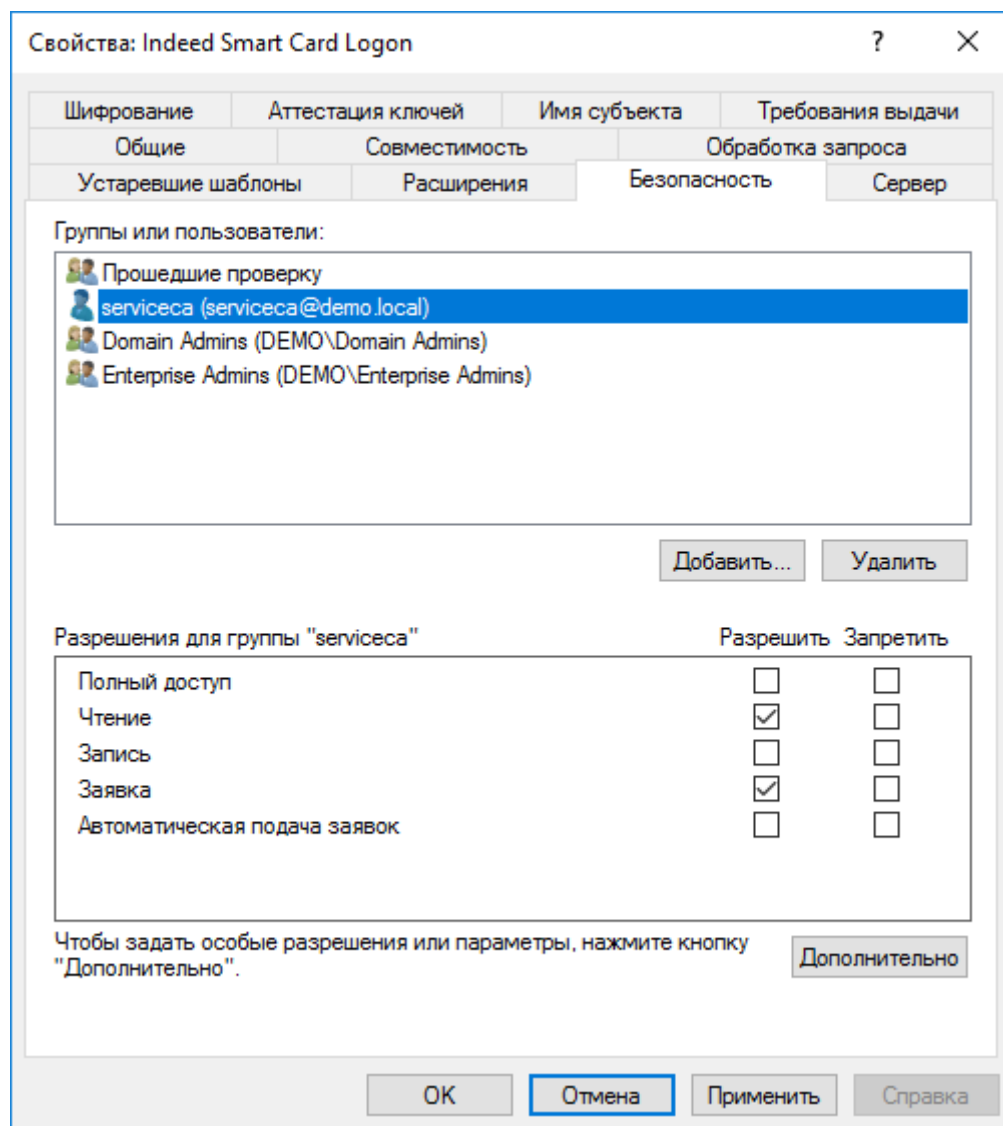
7. На вкладке **Имя субъекта** (Subject Name) нажмите **Строится на основе данных Active Directory** (Build from this Active Directory information).

- Выберите **Полное различающееся имя** (Fully distinguished name) из списка **Формат имени субъекта** (Subject name format).
- Установите флажок **Имя субъекта-пользователя (UPN)** (User principal name (UPN)).
- Снимите флажки с опций **Включить имя электронной почты в имя субъекта** (Include e-mail name in subject name) и **Имя электронной почты** (E-mail name), если требуется выпуск сертификатов по данному шаблону пользователям, у которых не указан E-mail в Active Directory.

The screenshot shows the 'Свойства: Indeed Smart Card Logon' (Properties: Indeed Smart Card Logon) dialog box. The 'Имя субъекта' (Subject Name) tab is selected. The 'Предоставляется в запросе' (Provided in request) section has the 'Строится на основе данных Active Directory' (Build from this Active Directory information) radio button selected. Below this, the 'Формат имени субъекта:' (Subject name format:) dropdown menu is set to 'Полное различающееся имя' (Fully distinguished name). The 'Включить имя электронной почты в имя субъекта' (Include e-mail name in subject name) checkbox is unchecked. The 'Включить эту информацию в альтернативное имя субъекта:' (Include this information in alternative subject name:) section has the 'Имя субъекта-пользователя (UPN)' (User principal name (UPN)) checkbox checked, while 'Имя электронной почты' (E-mail name), 'DNS-имя' (DNS name), and 'Имя субъекта-службы (SPN)' (Service principal name (SPN)) are unchecked. A note at the bottom states: '* Элемент управления отключен из-за параметров совместимости.' (The control is disabled due to compatibility parameters.). The dialog box has standard buttons: 'ОК', 'Отмена' (highlighted), 'Применить', and 'Справка'.

8. На вкладке **Безопасность** (Security) нажмите кнопку **Добавить...** (Add...).
- В поле **Введите имена выбираемых объектов** (Enter the object names to select) введите имя сервисной учетной записи (**serviceca**) и нажмите **ОК**.
 - В разделе **Разрешения для группы** (Permissions for) установите флажок **Разрешить** (Allow) для привилегий **Чтение** (Read) и **Заявка** (Enroll).

! **Обязательно** выдайте аналогичные разрешения сервисной учетной записи для шаблона **Агент регистрации** (Enrollement Agent) и для всех шаблонов сертификатов, которые будут использоваться Indeed CM.



9. Сохраните настройки шаблона, нажав **ОК**.

Добавление шаблонов сертификатов

1. Откройте консоль управления **Центр сертификации** (Certification Authority) и дважды щелкните имя ЦС.
2. Кликните правой кнопкой мыши на контейнере **Шаблоны сертификатов** (Certificate Templates).
3. Выберите команду **Создать** (New), а затем пункт **Выдаваемый шаблон сертификата** (Certificate Template to Issue).
4. Обязательно выберите шаблон сертификата **Агент регистрации** (Enrollment Agent), а также все остальные шаблоны сертификатов (например, **Indeed Smart Card Logon**), которые будут использоваться системой Indeed CM.
5. Для сохранения нажмите кнопку **ОК**.

Выпуск сертификата Агент регистрации (Enrollment Agent)

Наличие в системе Indeed Certificate Manager сервисного пользователя (**serviceca**), обладающего сертификатом **Агент регистрации** (Enrollment Agent) необходимо для того, чтобы от имени данного пользователя системой запрашивались и подписывались запросы на сертификаты для всех остальных пользователей.

Сертификат может быть создан двумя способами:

1. [Утилитой IndeedCM.CertEnroll.MsCA](#) (располагается в каталоге IndeedCM. Server\Misc дистрибутива).
2. [Используя Диспетчер сертификатов пользователя](#) (Certificates - Current User) (certmgr.msc).

Утилитой IndeedCM.CertEnroll.MsCA

Для выпуска сертификата с назначением Enrollment Agent запустите от имени учетной записи с правами локального администратора на сервере Indeed Certificate Manager утилиту **IndeedCM.CertEnroll.MsCA.exe** с параметром **/e <service username> <Password>** где:

- **<service username>** – имя сервисной учетной записи для работы с центрами сертификации (**serviceca**).
- **<Password>** – пароль сервисной учетной записи.

Пример:

```
IndeedCM.CertEnroll.MsCA.exe /e serviceca p@ssw0rd
```

Результат работы утилиты:

```
CA: msca.demo.local\Indeed-Demo-CA  
Certificate has been enrolled successfully.
```

Если запрос на сертификат должен быть одобрен оператором УЦ, то утилита предложит принять запрос и продолжить работу, указав при этом порядковый номер запроса и имя ключевого контейнера:

```
CA: msca.demo.local\Indeed-Demo-CA  
Certificate request is pending.  
Request id: 27  
Container name: Ir-EnrollmentAgent-175d9490-7481-4a29-b567-503d39747354  
Please accept request and then install certificate.
```

После одобрения запроса оператором необходимо выполнить команду для установки сертификата в хранилище.

Для этого запустите утилиту **IndeedCM.CertEnroll.MsCA.exe** с параметром **/i <service username> <password> <requestId> <containerName>**, где:

- **service username** – имя сервисной учетной записи для работы с центрами сертификации (**serviceca**)
- **password** – пароль сервисной учетной записи
- **requestId** – порядковый номер запроса на сертификат
- **containerName** – имя ключевого контейнера

Пример:

```
IndeedCM.CertEnroll.MsCA.exe /i serviceca p@ssw0rd 27 lr-EnrollmentAgent-175d9490-7481-4a29-b567-503d39747354
```

Результат работы утилиты:

```
CA: msca.demo.local\Indeed-Demo-CA  
Certificate has been installed successfully.
```

В результате работы утилиты в хранилище сертификатов компьютера, на котором установлен сервер Indeed CM, появится сертификат с назначением **Агент запроса сертификатов** (Enrollment Agent) с экспортируемым закрытым ключом и настроенными правами на управление закрытым ключом для учетной записи сервисного пользователя.

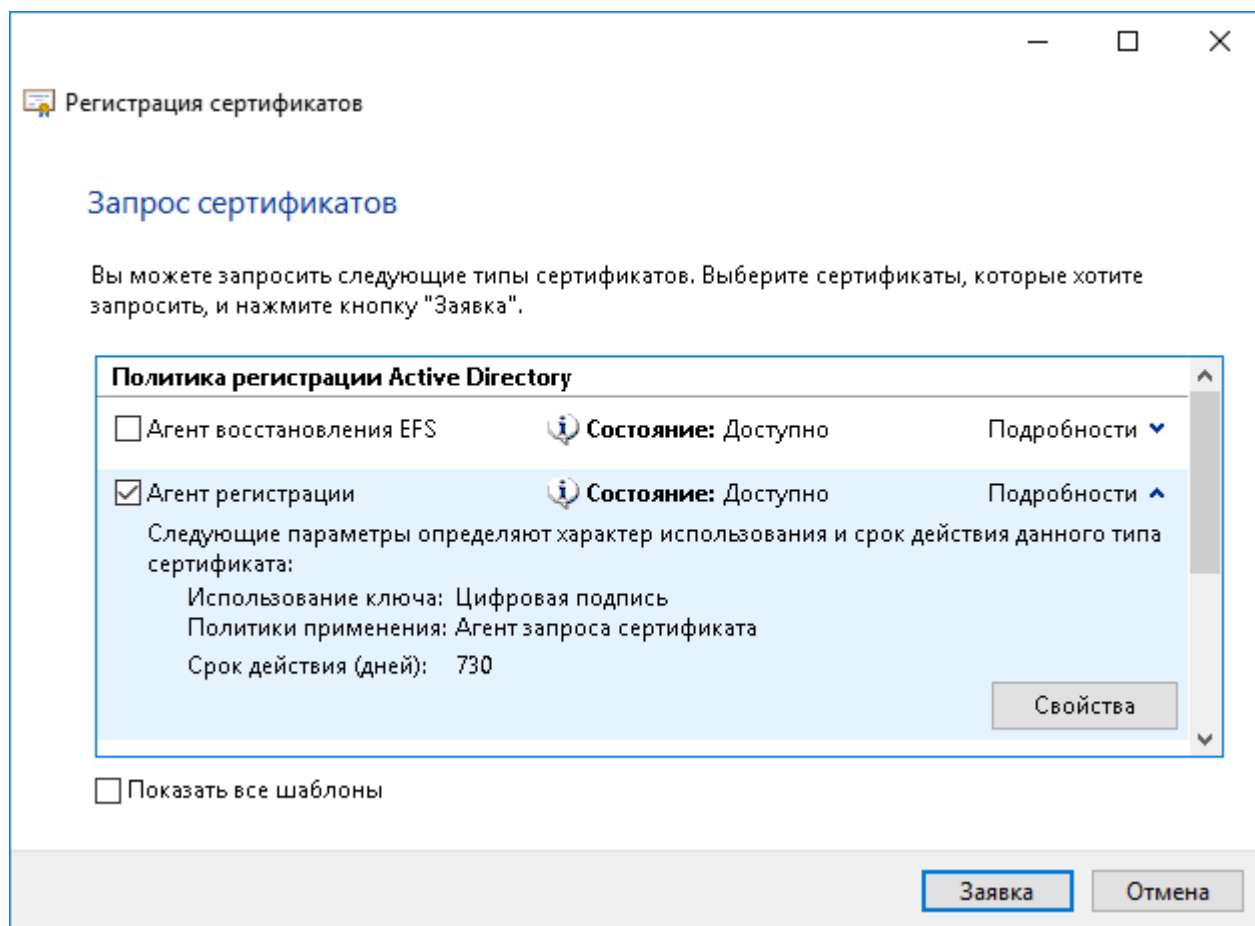
В случае необходимости можно указать имя шаблона сертификата (параметр **/t**) и центр сертификации (параметр **/c**) к которому следует обратиться (если развернуто несколько центров сертификации). Имя шаблона по умолчанию – **Агент регистрации** (Enrollment Agent). Поддерживаются шаблоны с любыми именами, имеющие **Улучшенный ключ** (Extended Key Usage) **Агент запроса сертификата** (Certificate Request Agent). Имя шаблона сертификата указывается без пробелов.

Пример:

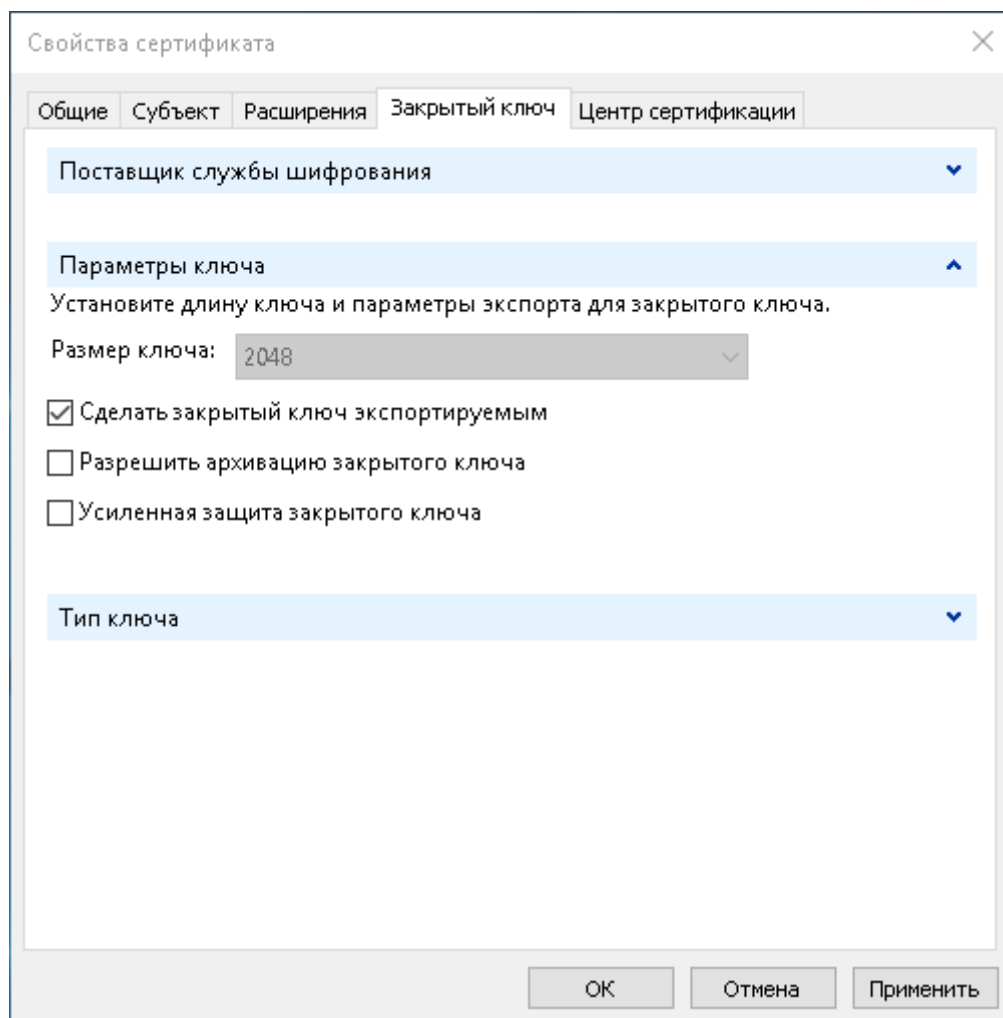
```
IndeedCM.CertEnroll.MsCA.exe /e serviceca p@ssw0rd /t="IndeedEnrollmentAgent" /c="msca.demo.local\Indeed-Demo-CA"
```

В Диспетчере сертификатов пользователя

1. Выполните вход на сервер Indeed CM под сервисной учетной записью (**serviceca**) и откройте оснастку **Сертификаты** (Certificates) пользователя (certmgr.msc).
2. Запустите мастер выпуска нового сертификата.
3. Выберите тип сертификата **Агент регистрации** (Enrollment Agent), разверните окно подробной информации и нажмите кнопку **Свойства** (Properties).



4. Перейдите на вкладку **Закрытый ключ** (Private key), разверните меню **Параметры ключа** (Key options) и включите опцию **Сделать закрытый ключ экспортируемым** (Make private key exportable).



5. Переместите выпущенный сертификат и его закрытый ключ **в хранилище сертификатов компьютера**, на котором развернут сервер Indeed CM.

6. Выдайте сервисному пользователю (**serviceca**) права на чтение закрытого ключа сертификата **Агент регистрации** (Enrollment Agent).

- Для этого в оснастке **Сертификаты** (Certificates) компьютера кликните правой кнопкой мыши на сертификате.
- Выберите **Все задачи** (All tasks) > **Управление закрытыми ключами...** (Manage Private Keys...).
- Нажмите **Добавить** (Add), укажите сервисную учетную запись (**serviceca**).
- Выставите право **Полный доступ** (Full control).
- Нажмите **Применить** (Apply).

Подключение к центру сертификации Microsoft через IndeedCM MSCA Proxy

Indeed Certificate Manager может взаимодействовать с центрами сертификации Microsoft, расположенными за пределами домена, в котором находится сервер Indeed CM.

Например, в конфигурации, когда у одной организации есть несколько независимых доменов с самостоятельными центрами сертификации в каждом, а Indeed CM развернут только в одном из этих доменов. При этом учетные записи пользователей в этих доменах одинаковы.

Использование компонента **IndeedCM.MSCA.Proxy** позволит запрашивать и записывать на устройства при помощи Indeed CM сертификаты со всех УЦ, находящихся за пределами того домена, в котором развернут Indeed CM. В такой схеме в политику использования устройств Indeed CM добавляется адрес MSCA Proxy, который развернут во внешнем домене с каталогом пользователей и центром сертификации. При выпуске устройства Indeed CM обращается к MSCA Proxy, а тот, используя сертификат Агента Регистрации (располагается в хранилище рабочей станции с установленным компонентом IndeedCM.MSCA.Proxy) передает запрос на целевой центр сертификации.

Для установки и настройки приложения MSCA Proxy выполните следующие действия:

1. Создайте во внешнем домене сервисную учетную запись для работы с центром сертификации Microsoft (см. [Создание сервисной учетной записи для работы с Microsoft CA](#)).
2. Настройте для сервисной учетной записи из п.1 шаблон Агент регистрации (см. [Настройка шаблонов сертификатов](#)) и выпустите для этой учетной записи сертификат по этому шаблону (см. [Выпуск сертификата Агент регистрации \(Enrollment Agent\)](#)).

 Сертификат **Агент регистрации** должен располагаться в **хранилище сертификатов рабочей станции (Local computer)**, на которой установлен компонент IndeedCM.MSCA.Proxy.

3. Установите компонент **IndeedCM.MSCA.Proxy.msi** из дистрибутива (распологающемся в каталоге IndeedCM.Server) на рабочей станции в домене с внешним УЦ.

 Системные требования для установки компонента совпадают с требованиями для установки сервера Indeed CM.

4. Перейдите в каталог **C:\inetpub\wwwroot\mscaproxy** и откройте в редакторе Блокнот, запущенном от имени администратора, файл **Web.config**.

5. Укажите в секции **caProxySettings**:

- Имя центра сертификации в параметре **ca**.
- Данные учетной записи (логин и пароль), обладающей сертификатом **Агент регистрации** в параметрах **userName** и **password** соответственно.
- **Отпечаток** (Thumbprint) сертификата **Агент регистрации** в параметре **enrollmentAgentCertificateThumbprint**.

Пример заполненной секции:

```
<caProxySettings ca="servercm.external.com\EXTERNAL-CA" userName="EXTERNAL\service" password="p@ssw0rd" enrollmentAgentCertificateThumbprint="dbd1859d27395860843643ebe17e2ee3fc463aba"/>
```

6. В секции **authorization** в параметре **allow users** также укажите сервисную учетную запись для работы с центром сертификации.

Пример заполненной секции:

```
<authorization>
  <deny users="?" />
  <allow users="EXTERNAL\service" />
  <deny users="*" />
</authorization>
```

7. **Сохраните** изменения в файле.

КриптоПро УЦ 2.0

В разделе описаны основные шаги, которые необходимо выполнить для настройки работы Indeed Certificate Manager с КриптоПро УЦ 2.0:

1. [Создайте сервисную группы пользователей в Центре Регистрации](#)
2. [Создайте сервисную учетную запись для работы с КриптоПро УЦ 2.0](#)
3. [Настройте шаблон сертификата агента подачи заявок](#)
4. [Выпустите сертификат агента подачи заявок сервисной учетной записи](#)

Если каталог пользователей расположен только в Центре Регистрации КриптоПро УЦ 2.0, то выполните [Настройку аутентификации в web-сервисах Indeed CM по сертификатам](#).

Создание сервисной учетной записи для работы с КриптоПро УЦ 2.0

Описанный ниже вариант создания сервисной учетной записи является рекомендуемым, но не единственным. Вы можете создать учетную запись пользователя и выпустить сертификат непосредственно в Центре Регистрации и затем экспортировать его для установки на сервер Indeed Certificate Manager.

1. Запустите от имени администратора браузер Internet Explorer на сервере Indeed CM и откройте корневую страницу КриптоПро УЦ 2.0 (<https://<имя сервера УЦ>/UI/>).
2. Подайте заявку на регистрацию сервисной учетной записи:
 - Укажите в заявке **имя** сервисной учетной записи и **e-mail**
 - Запомните или запишите выданный ЦР идентификатор и временный пароль
 - Укажите дополнительную информацию, если необходимо или пропустите этот шаг
 - Завершите регистрацию
3. **Одобрите запрос** на регистрацию нового пользователя (см. п.2) в **Консоли управления ЦР**.
4. Добавьте созданного пользователя в группу безопасности **Indeed CM Service Users**.

Создание шаблона сертификата для сервисной учетной записи

Для сервисной учетной записи системы Indeed Certificate Manager необходимо создать шаблон сертификата, на основе которого впоследствии будет выпущен сертификат агента подачи заявок. Для этого выполните:

1. Откройте узел **Шаблоны сертификатов** в утилите **Диспетчер УЦ**.
2. Создайте шаблон сертификата **Indeed CM Service User** на основе шаблона **Пользователь**:
 - Укажите **Срок действия** сертификата.
 - В разделе **Параметры создания ключа** выберите **Ключ принадлежит: Компьютеру** и включите опцию **Разрешить экспорт ключа**.
 - В разделе **Настройка расширений сертификата** выберите **Улучшенный ключ (2.5.29.37)** и нажмите **Изменить...**
 - В появившемся окне **Настройки расширения** снова нажмите **Изменить...**
 - Поставьте отметку напротив пункта **Агент запроса сертификата** и два раза нажмите **ОК**.
3. **Примените** изменения в шаблоне.
4. Щелкните правой кнопкой мыши по корневому узлу **Роли УЦ** и нажмите кнопку **Обновить**.

Выпуск сертификата агента подачи заявок сервисной учетной записи

Для выпуска сертификата агента подачи заявок сервисной учетной записи необходимо выполнить:

1. С рабочей станции, на которой установлен сервер Indeed Certificate Manager, выполните вход в личный кабинет пользователя КriptoПро УЦ по идентификатору и временному паролю сервисной учетной записи.
2. Создайте запрос на сертификат, указав шаблон **Indeed CM Service User** и криптопровайдер **Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider**.

 Поддерживаются и крипто-провайдеры RSA.

3. Дождитесь одобрения запроса Оператором Центра Регистрации.
4. Перейдите в раздел **Запросы > Изготовление** личного кабинета пользователя КriptoПро.
5. Загрузите и сохраните изготовленный сертификат.

 Если предполагается использовать несколько серверов Indeed CM с общим хранилищем данных совместно с КriptoПро УЦ, то сертификат сервисного пользователя **должен быть выпущен с экспортируемым закрытым ключом**. Этот сертификат и его контейнер закрытого ключа необходимо будет переносить на каждый сервер Indeed CM.

6. Установите сертификат в контейнер локального хранилища рабочей станции.
7. Выдайте системе Indeed CM **права на чтение закрытого ключа сертификата сервисной учетной записи**, который был установлен на предыдущем шаге.

- В оснастке **Сертификаты** (Certificates) компьютера, на котором установлен сервер Indeed CM.
- Кликните правой кнопкой мыши на сертификате, выберите **Все задачи** (All tasks) > **Управление закрытыми ключами...** (Manage Private Keys...).
- Нажмите **Добавить** (Add), укажите локальную группу **IIS_IUSRS** (если используется IIS 7.0) или локальную учетную запись **IIS AppPool\IndeedCM** (если используется IIS 7.5 и более поздние версии).
- Выставьте права **Полный доступ** (Full Control) и **Чтение** (Read).
- Нажмите **Применить** (Apply).



Если в конфигурации системы используется Агент Indeed CM, то также необходимо выдать права на **Полный доступ** (Full Control) и **Чтение** (Read) для учетной записи **IIS AppPool\IndeedCM Agent** (если используется IIS 7.5 и более поздние версии).

8. Установите в хранилище **Локального компьютера** (Local computer), на котором установлен сервер Indeed CM в список **Доверенных Корневых Центров Сертификации** (Trusted Root Certification Authorities) сертификат корневого центра сертификации КриптоПро УЦ 2.0.

9. Установите список отозванных сертификатов (CRL) центра сертификации КриптоПро УЦ 2.0 в хранилище **Локального компьютера** (Local Computer), на котором установлен сервер Indeed CM в **Промежуточные Центры Сертификации** (Intermediate Certification Authorities).

Настройка аутентификации в web-сервисах Indeed CM по сертификатам

Для настройки аутентификации в web-сервисах Indeed Certificate Manager по сертификатам создайте сертификат аутентификации сервера КриптоПро УЦ 2.0:

1. Зарегистрируйте нового пользователя КриптоПро УЦ, указав в качестве имени пользователя полное имя рабочей станции, на которой установлен сервер Indeed CM.
2. С рабочей станции, на которой установлен сервер Indeed CM, выполните вход в личный кабинет пользователя Крипто Про УЦ по идентификатору и временному паролю учетной записи сервера, созданной в п.1.
3. Создайте запрос на сертификат, указав шаблон **Веб-сервер**, криптопровайдер **Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider**, использование ключа – **Подпись**.
4. Дождитесь одобрения запроса оператором Центра Регистрации.
5. Перейдите в раздел **Запросы > Изготовление** личного кабинета пользователя КриптоПро.
6. Загрузите и сохраните изготовленный сертификат.
7. Установите полученный сертификат в личное хранилище компьютера используя КриптоПро CSP (**Сервис > Установить личный сертификат...**).
8. Укажите путь к файлу сертификата. Убедитесь в том, что выбран сертификат той рабочей станции, имя которой было указано в п.1.
9. Укажите, что введенное имя задает ключевой контейнер **компьютера** и отметьте опцию **Найти контейнер автоматически**. После этого в качестве хранилища контейнера определится **Реестр**, нажмите **Далее** и завершите установку сертификата.
10. Выдайте системе Indeed CM **права на чтение закрытого ключа сертификата сервисной учетной записи**, который был установлен на предыдущем шаге.
 - Запустите оснастку **Сертификаты** (Certificates) для локального компьютера на сервере Indeed CM.
 - Перейдите в раздел **Личные** (Personal) > **Сертификаты** (Certificates).
 - Кликните правой кнопкой мыши на сертификате, установленному при помощи КриптоПро CSP, выберите **Все задачи** (All tasks) > **Управление закрытыми ключами...** (Manage Private Keys...).
 - Нажмите **Добавить** (Add), укажите локальную группу **IIS_IUSRS** (если используется IIS 7.0) или локальную учетную запись **IIS AppPool\IndeedCM** (если используется IIS 7.5 и более поздние версии).
 - Выставите права **Полный доступ** (Full Control).
 - Нажмите **Применить** (Apply).

 Если в конфигурации системы используется Агент Indeed CM, то также необходимо выдать права на **Полный доступ** (Full Control) и **Чтение** (Read) для учетной записи IIS AppPool\IndeedCM Agent (если используется IIS 7.5 и более поздние версии).

КриптоПро DSS 2.0

ПАК "КриптоПро DSS" версии 2.0 предназначен для защищенного хранения закрытых ключей пользователей, а также для удаленного выполнения операций по созданию электронной подписи. Интеграция с Indeed Certificate Manager позволяет осуществлять выпуск и централизованный учёт средств облачной аутентификации. Для работы с электронной подписью не требуется устройство (USB-токен или смарт-карта), ключи генерируются и хранятся в хранилище КриптоПро DSS, для доступа и использования электронной подписи применяется облачный криптопровайдер КриптоПро Cloud CSP.

Предварительные условия

Для интеграции Indeed Certificate Manager с КриптоПро DSS в окружении компании должны быть развернуты:

- Сервер Indeed CM версии 5.1 и выше.
- ПАК "КриптоПро УЦ" 2.0
- ПАК "КриптоПро DSS" 2.0
- ПАКМ "КриптоПро HSM"
- КриптоПро CSP 5.0
- Настроенная интеграция КриптоПро УЦ 2.0 с КриптоПро DSS

 Интеграция УЦ и DSS необходима для управления пользователями и их сертификатами в удостоверяющем центре. КриптоПро DSS выступает в роли привилегированного пользователя по отношению к КриптоПро УЦ 2.0. Создание и обновление пользователей, запрос сертификатов и прочие действия на УЦ в этом случае выполняются от имени **Оператора DSS**. Подробная инструкция по интеграции входит комплект поставки ПАК "КриптоПро DSS".

Настройка интеграции

Для работы с КриптоПро DSS используется учётная запись **Оператор DSS**, сертификат которой должен храниться на сервере Indeed CM. Для установки сертификата Оператора DSS выполните следующие действия:

1. Добавьте сертификат **Оператора DSS** в **локальное хранилище компьютера** (Local Computer) на сервере Indeed CM.
2. Добавьте корневой сертификат КристоПро УЦ 2.0 и корневой сертификат DSS в **Доверенные корневые центры сертификации** (Trusted Root Certification Authorities) на сервере Indeed CM.
3. Выдайте системе Indeed CM **права на чтение закрытого ключа сертификата Оператора DSS**.
 - В оснастке **Сертификаты** (Certificates) компьютера, на котором установлен сервер Indeed CM.
 - Кликните правой кнопкой мыши на сертификате, выберите **Все задачи** (All tasks) > **Управление закрытыми ключами...** (Manage Private Keys...).
 - Нажмите **Добавить** (Add), укажите локальную группу **IIS_IUSRS** (если используется IIS 7.0) или локальную учетную запись **IIS AppPool\IndeedCM** (если используется IIS 7.5 и более поздние версии).
 - Выставьте права **Полный доступ** (FullControl).
 - Нажмите **Применить** (Apply).

Выдайте права на папку с пользователями в КристоПро УЦ 2.0 для учётной записи **Оператор DSS**:

1. Создайте группу безопасности, например **DSS Operators** и включите в неё учётную запись **Оператор DSS**.
2. Откройте свойства папки, в которой будут располагаться пользователи DSS, перейдите на вкладку безопасность и добавьте созданную группу **DSS Operators**.
3. Выдайте группе разрешения согласно таблице.

Набор прав для сервисной группы пользователей DSS Operators.

Наименование разрешения	Тип объекта	Комментарий
Чтение свойств	Папка, Пользователь	Чтение свойств объекта. Если у субъекта нет права чтения свойств объекта, то объект не виден субъекту.
Запрос регистрации	Папка	Создание запроса на регистрацию пользователя
Запрос сертификата	Пользователь, шаблон	Создание запроса сертификата для пользователя

Запрос аннулирования	Пользователь	Создание запроса на аннулирование сертификата пользователя
Запрос приостановления	Пользователь	Создание запроса на приостановление сертификата пользователя
Запрос возобновления	Пользователь	Создание запроса на возобновление сертификата пользователя
Одобрение регистрации	Папка	Одобрение запроса на регистрацию пользователя
Одобрение сертификата	Пользователь, шаблон	Одобрение запроса сертификата для пользователю
Одобрение аннулирования	Пользователь	Одобрение запроса на аннулирование сертификата пользователя
Одобрение приостановления	Пользователь	Одобрение запроса на приостановление сертификата пользователя
Одобрение возобновления	Пользователь	Одобрение запроса на возобновление сертификата пользователя
Передача запросов	Пользователь	Передача запросов, подписанных пользователем-получателем услуги, а не подписью пользователя, передающего или одобряющего запрос.
Запрос переименования	Пользователь	Создание запроса на изменение данных пользователя.
Одобрение переименования	Пользователь	Одобрение запроса на изменение данных пользователя.

Валидата УЦ

В разделе описаны основные шаги, которые необходимо выполнить для настройки работы Indeed Certificate Manager с Валидата УЦ:

1. Выберите режим работы с Валидата УЦ и выполните его настройку:
 - [Настройка Offline-режима работы](#)
 - [Настройка Online-режима работы](#)
2. [Настройте шаблоны сертификатов пользователей](#)

Offline-режим работы

Для работы Indeed Certificate Manager с Валидата УЦ в offline-режиме необходимо предоставить доступ на чтение и запись к каталогу для обмена файлами с Центром Регистрации Валидата УЦ. Данный каталог должен содержать следующее:

1. Корневой и промежуточные сертификаты Валидата УЦ.
2. Актуальный файл Списка Отозванных Сертификатов (COC).
3. Два подкаталога:
 - Подкаталог для входящих незащищённых запросов пользователей (в формате PKCS#10).

 Обработка запросов в формате PKCS#10 может быть выполнена исключительно в ручном режиме на АРМ Администратора ЦР.

- Подкаталог сертификатов для выдачи конечным пользователям.

Online-режим работы

Для работы Indeed Certificate Manager с Валидата УЦ в online-режиме необходимо предоставить доступ на чтение и запись к каталогу для обмена файлами с Центром Сертификации Валидата и настроить подключение к АРМ Администратора Центра Регистрации Валидата УЦ с помощью сертификата Оператора ЦР.

Выпуск сертификата Оператора Центра Регистрации

В Online-режиме работы с Валидатой УЦ Indeed CM заменяет собой АРМ Оператора ЦР Валидата. Для работы в данном режиме необходимо **Разрешить удаленное подключение к сервису** в настройках Центра Регистрации и подготовить сертификат Оператора ЦР.

 Сертификат Оператора ЦР используется как при подключении к сервису ЦР для выполнения аутентификации по протоколу TLS, так и для подписания XML шаблона на получение или отзыв сертификата ключа проверки ЭП пользователя и должен содержать OID Оператор Центра Регистрации (1.3.6.1.4.1.10244.6.1) и OID Проверка подлинности TLS клиента (1.3.6.1.5.5.7.3.2).

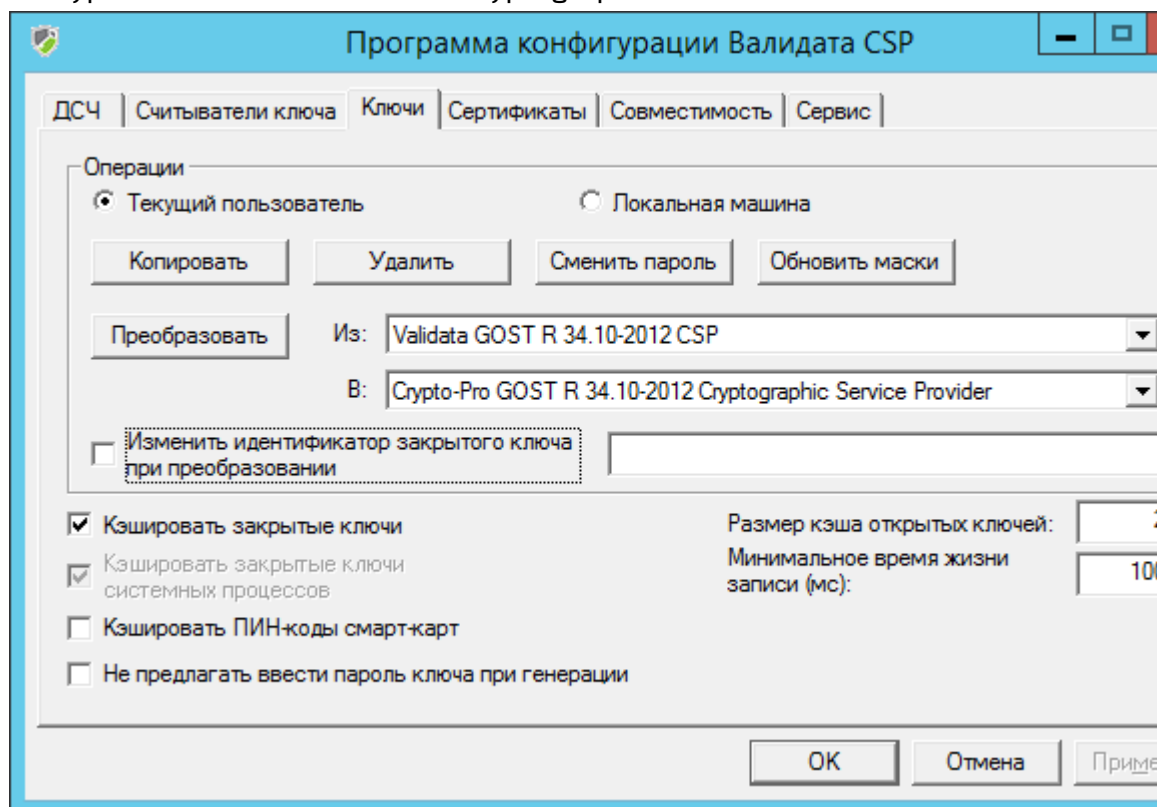
Сертификат **Оператора ЦР** можно выпустить с использованием Валидата CSP или с помощью Крипто Про CSP.

Ниже описан процесс выпуска сертификата Оператора ЦР в Центре Регистрации Валидата УЦ с использованием Валидата CSP:

1. Для создания шаблона сертификата выберите пункт меню **Центр Регистрации - Сформировать запрос на сертификат абонента** из основного меню АРМ Администратора ЦР.
2. В появившемся окне выберите шаблон, если он был подготовлен ранее, и нажмите **Далее**.
3. Заполните атрибуты сертификата для построения **Имени Владельца сертификата**, установите опцию **Разрешить генерацию ключа шифрования**, если требуется и нажмите **Далее**.
4. Выберите область применения ключа: **Оператор ЦР** и **Проверка подлинности TLS клиента** и нажмите **Далее**.
5. Выберите регламент сертификата и нажмите **Далее**.
6. Выберите дополнения для сертификата и нажмите **Далее**.
7. Задайте атрибуты **альтернативного имени Владельца сертификата**, если это требуется и нажмите **Готово**.

Если сертификат был выпущен с помощью Валидата CSP, то необходимо преобразовать его закрытый ключ из **Validata GOST R 34.10-2012 CSP** в **Crypto-Pro GOST R 34.10-2012 CSP**:

1. Запустите, от имени администратора, приложение **Validata CSP**.
2. Перейдите на вкладку Ключи. В поле **Преобразовать** выберите соответствующие поля
 - **Из:** Validata GOST R 34.10-2012 CSP
 - **В:** Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider:



3. Следуя подсказкам мастера преобразуйте закрытый ключ сертификата **Оператора ЦР** в **Crypto-Pro GOST R 34.10-2012 CSP**.
4. Установите преобразованный ключ и сертификат Оператора ЦР в контейнер локального хранилища рабочей станции (сервера Indeed CM).

5. Выдайте системе Indeed CM **права на чтение закрытого ключа сертификата**

Оператора, который был установлен на предыдущем шаге:

- В оснастке **Сертификаты** (Certificates) компьютера, на котором установлен сервер Indeed CM.
- Кликните правой кнопкой мыши на сертификате, выберите **Все задачи** (All tasks) > **Управление закрытыми ключами...** (Manage Private Keys...).
- Нажмите **Добавить** (Add), укажите локальную группу **IIS_IUSRS** (если используется IIS 7.0) или локальную учетную запись **IIS AppPool\IndeedCM** (если используется IIS 7.5 и более поздние версии).
- Выставите права **Полный доступ** (Full Control) и **Чтение** (Read).
- Нажмите **Применить** (Apply).



Если в конфигурации системы используется Агент Indeed CM, то также необходимо выдать права на **Полный доступ** (Full Control) и **Чтение** (Read) для учетной записи **IIS AppPool\IndeedCM Agent** (если используется IIS 7.5 и более поздние версии).

6. Установите сертификат корневого центра сертификации Валидата УЦ в хранилище **Локального компьютера** (Local computer), на котором установлен сервер Indeed CM в список **Доверенных Корневых Центров Сертификации** (Trusted Root Certification Authorities).
7. Установите сертификат промежуточного центра сертификации и список отозванных сертификатов (CRL) Валидата УЦ в хранилище **Локального компьютера** (Local Computer), на котором установлен сервер Indeed CM в **Промежуточные Центры Сертификации** (Intermediate Certification Authorities).

Настройка шаблонов сертификатов пользователей

Для работы с Indeed Certificate Manager необходимо предварительно подготовить шаблоны сертификатов в Центре Регистрации Валидата УЦ в формате XML, которые будут использоваться для выпуска сертификатов конечным пользователям.

Ниже описан процесс настройки шаблона сертификата пользователя в Центре Регистрации Валидата УЦ:

1. Для создания шаблона сертификата выберите пункт меню **Центр Регистрации - Создать новый шаблон сертификата** из основного меню АРМ Оператора или Администратора ЦР.
2. В появившемся окне укажите **Наименование шаблона** и нажмите **Далее**.
3. Заполните атрибуты сертификата для построения **Имени Владельца сертификата**, установите опцию **Разрешить генерацию ключа шифрования**, если требуется и нажмите **Далее**:



Поддерживаемые атрибуты для построения X.500-имени пользователя:

- Должность (Т)
- ОГРН (OGRN)
- ОГРНИП (ORGNIP)
- СНИЛС (SNILS)
- ИНН (INN)
- ИНН юридического лица (INNLE)
- Фамилия (SN)
- Приобретенное имя (GN)
- Общее имя (CN)
- Организация (O)
- Название улицы, номер дома (street)
- Населенный пункт (L)
- Город, область (ST)
- Страна (C)
- Почтовый адрес RFC822 (Email)
- Подразделение (OU)

Использование опции **Разрешить генерацию ключа шифрования** позволяет создать ключ шифрования для сертификата. В случае если эта опция не выбрана, то пользователю, для которого создается сертификат, будет запрещено иметь ключ шифрования.

Создание нового шаблона сертификата

Имя Владельца сертификата

Заполните атрибуты сертификата

Параметр	Значение
Должность (T)	title
Неструктурированное имя (unstructuredName)	
Неструктурированный адрес (unstructuredAddress)	
ОГРН (OGRN)	1234567890123
ОГРНИП (OGRNIP)	123456789012345
СНИЛС (SNILS)	12345678901
ИНН (INN)	123456789012
Фамилия (SN)	surName
Приобретенное имя (GN)	givenName
Общее имя (CN)	commonName
Общее имя (CN)	
Организация (O)	organizationName
Название улицы, номер дома (street)	streetAddress
Населённый пункт (L)	localityName
Город, Область (ST)	stateOrProvidenceName
Страна (C)	RU
Почтовый адрес RFC822 (Email)	user Email
Доменное имя (DC)	
Подразделение (OU)	organizationUnitName
Подразделение (OU)	
Подразделение (OU)	
Подразделение (OU)	

☒ Разрешить генерацию ключа шифрования
 ☐ Использовать только для шифрования

< Назад

Далее >

Отмена

4. Выберите область применения ключа и нажмите **Далее**.
5. Выберите регламент для сертификата и нажмите **Далее**.
6. Выберите дополнения для сертификата и нажмите **Далее**.
7. Задайте альтернативное имя Владельца сертификата и нажмите **Готово**.



Поддерживаемые атрибуты для построения альтернативного имени владельца сертификата:

- email
- Описание
- Microsoft Имя участника-пользователя (User Principal Name)

Создание нового шаблона сертификата

✕

Задание альтернативного имени Владельца сертификата

Заполните дополнительные сведения о Владельце сертификата

Параметр	Значение
email	user Email
DNS	
URL	
IP адрес	
Организация	
Зарегистрированный Адрес	
Фамилия	
Должность	
Номер телефона	
Описание	
Номер Расчетного Счета	
Банковский Идентификационный Код	
Почтовый Адрес	
Адрес Exchange	
Адрес Notes	
Паспортная информация	
Microsoft Имя участника-пользователя	UserPrincipalName
ИНН	
ОГРН	
ОГРНИП	
СНИЛС	

< Назад

Готово

Отмена

- Для того, чтобы использовать созданный шаблон в Indeed CM, необходимо в текстовом редакторе очистить значения заполненных атрибутов и перекодировать его в UTF-8 при сохранении.

Пример отредактированного шаблона:

```
<?xml version="1.0" encoding="UTF-8" ?>
<pkiUser>
  <templateName>Квалифицированный сертификат</templateName>
  <templateSubject>
    <INN></INN>
    <INNLE></INNLE>
    <OGRNIP></OGRNIP>
    <OGRN></OGRN>
    <SNILS></SNILS>
    <T></T>
    <SN></SN>
    <GN></GN>
    <Email></Email>
    <CN></CN>
    <OU></OU>
    <O></O>
    <street></street>
    <L></L>
    <ST></ST>
    <C></C>
  </templateSubject>
  <subjectAltName>
    <UPN></UPN>
    <emailAddress></emailAddress>
    <description>СЗ $docNumber от $docDate</description>
  </subjectAltName>
  <ExtKeyUsage>1.3.6.1.5.5.7.3.2</ExtKeyUsage>
  <ExtKeyUsage>1.3.6.1.5.5.7.3.4</ExtKeyUsage>
  <Policy>
    <OID>1.2.643.100.113.1</OID>
    <UserNotice>Класс средства ЭП КС1</UserNotice>
    <Org>Минкомсвязь России</Org>
  </Policy>
  <Policy>
    <OID>1.2.643.100.113.2</OID>
    <UserNotice>Класс средства ЭП КС2</UserNotice>
    <Org>Минкомсвязь России</Org>
  </Policy>
  <Extension>
    <OID>1.2.643.100.111</OID>
    <Type>ASN1_UTF8STRING</Type>
    <Value></Value>
  </Extension>
  <Encipherment>yes</Encipherment>
  <IdentificationKind>0</IdentificationKind>
</pkiUser>
```


Установка и настройка серверных компонентов

Для установки и настройки сервера Indeed Certificate Manager выполните следующие действия:

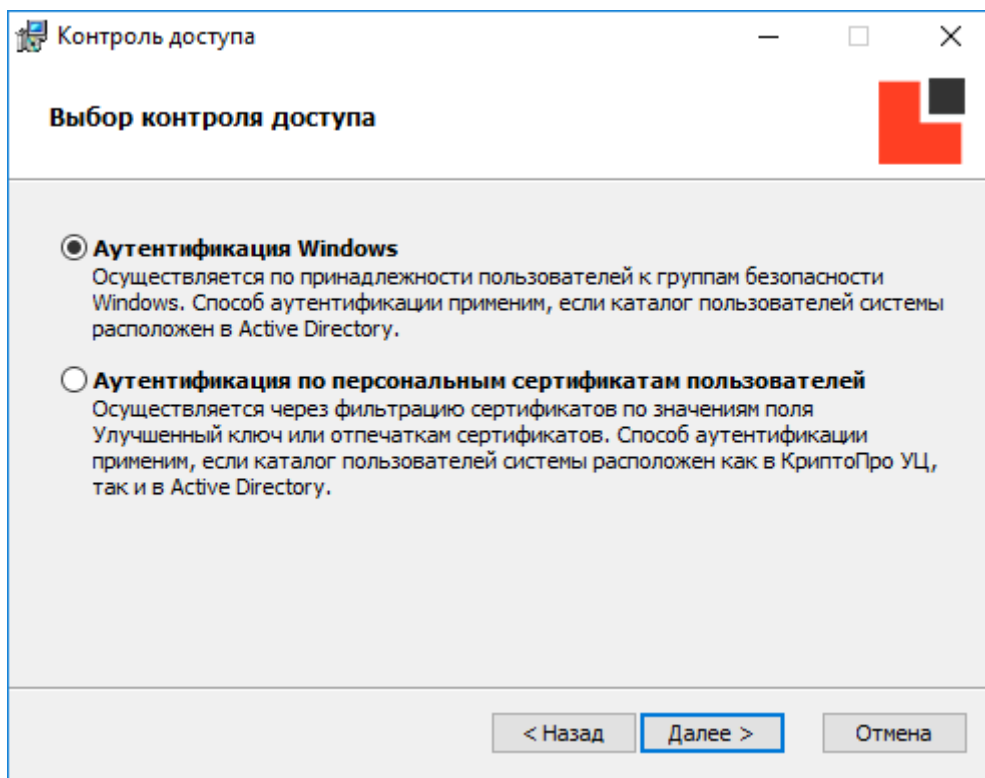
- [Выполните установку сервера](#)
- [Настройте параметры системы](#)

Если используется конфигурация с [клиентским агентом](#) (дополнительный компонент системы), то выполните его установку и настройку.

Если используется конфигурация с несколькими серверами Indeed CM, то имеется возможность настроить [Единый журнал событий](#) для всех серверов.

Установка сервера

Запустите файл **IndeedCM.Server.msi** из дистрибутива Indeed Certificate Manager (каталог **IndeedCM.Server**) и выполните установку, следуя указаниям мастера. В процессе установки будет предложено выбрать способ контроля доступа для всех приложений системы.



Система Indeed CM состоит из набора сервисов:

- **Консоль управления** (Management Console) – веб-приложение **icm**.
- **Сервис самообслуживания** (Self Service) – веб-приложение **icmservice**.
- **Консоль самообслуживания за пределами домена** (Remote Self Service) – веб-приложение **icmremote**.
- **Сервис разблокировки смарт-карт** – веб-приложение **credprovapi**.
- **Сервис API** – веб-приложение **icmapapi**.
- **Сервис отслеживания состояния карт** – **Служба Card Monitor**, не имеет веб-приложения.
- **Сервисы клиентского агента:**
 - **Сервис регистрации агентов** – веб-приложение **agentregistrationapi**.
 - **Сервис для удаленного выполнения задач** – веб-приложение **agentserviceapi**.

 Каждый сервис имеет собственные файлы конфигурации и настройки доступа.

При выборе **Аутентификации Windows** будут заданы следующие параметры контроля доступа:

- **Проверка подлинности (Authentication):**
 - **Проверка подлинности Windows (Windows Authentication)** для приложений icm, icmap, icmservice. Остальные способы отключены.
 - **Анонимная проверка подлинности (Anonymous Authentication)** для приложения credprovapi, agentregistrationapi, agentseviceapi.
 - **Анонимная проверка подлинности (Anonymous Authentication) и Проверка подлинности с помощью форм (Forms Authentication)** для приложения icmremote.
- **Параметры SSL (SSL Settings):**
 - **Требовать SSL (Require SSL)** для всех приложений.
 - **Сертификаты клиента (Client certificates):**
 - **Игнорировать (Ignore)** для приложений icm, icmap, icmremote, icmservice, credprovapi, agentregistrationapi.
 - **Требовать (Require)** для приложения agentseviceapi.

При выборе **Аутентификации по персональным сертификатам пользователей** будут заданы следующие параметры контроля доступа:

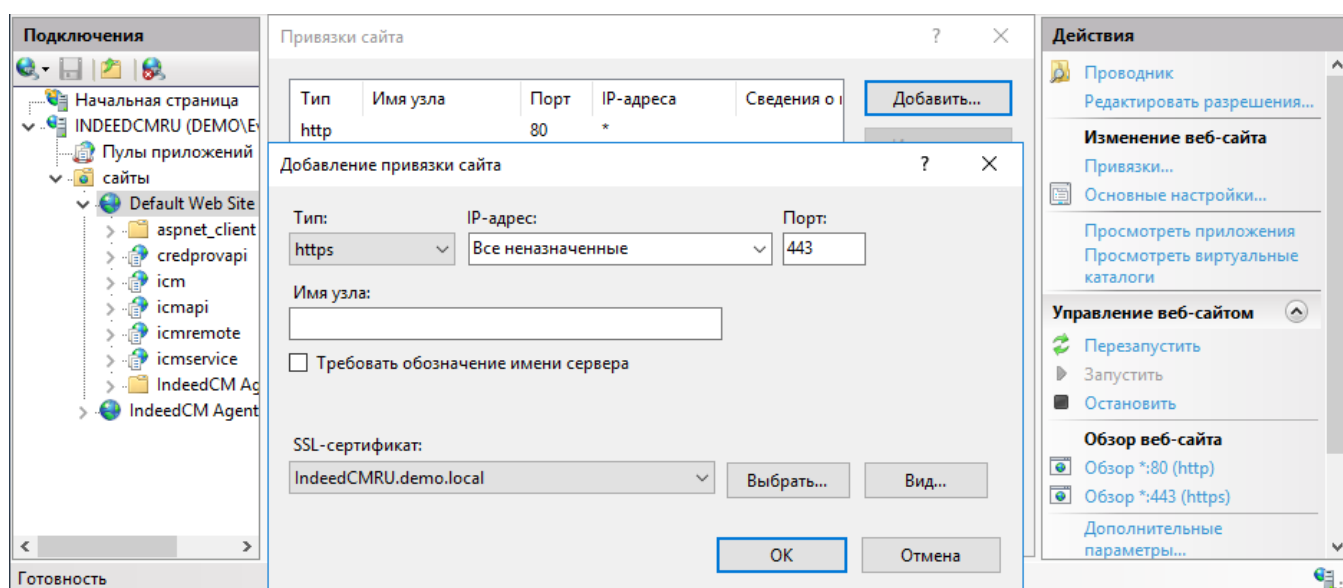
- **Проверка подлинности (Authentication):**
 - **Анонимная проверка подлинности (Anonymous Authentication)** для приложений icm, icmap, icmservice, credprovapi, agentregistrationapi, agentseviceapi. Остальные способы отключены.
 - **Анонимная проверка подлинности (Anonymous Authentication) и Проверка подлинности с помощью форм (Forms Authentication)** для приложения icmremote.
- **Параметры SSL (SSL Settings):**
 - **Требовать SSL (Require SSL)** для всех приложений.
 - **Сертификаты клиента (Client certificates):**
 - **Игнорировать (Ignore)** для приложений credprovapi, icmremote, agentregistrationapi.
 - **Требовать (Require)** для приложений icm, icmap, icmservice, agentseviceapi.

❗ Если каталог пользователей расположен в Active Directory, то сертификаты, используемые для аутентификации должны содержать **User Principal Name**. Без включенного в сертификат **UPN** вход в web-приложения Indeed CM будет невозможен.

После установки системы **Параметры SSL** для каждого приложения можно изменить вручную в **Диспетчере служб IIS** (IIS Manager).

Для настройки защищенного соединения для веб-приложений Indeed CM, необходимо выпустить SSL/TLS-сертификат и **Привязать** (Bindings) его в **Диспетчере служб IIS** (IIS Manager) для сайта **Default Web Site**:

- Запустите **Диспетчер служб IIS** (Internet Information Services (IIS) Manager).
- Выберите сайт **Default Web Site** и перейдите в раздел **Привязки...** (Bindings...).
- Нажмите **Добавить...** (Add...), выберите **Тип:** (Type:) **https** и **Порт:** (Port:) **443**.
- Выберите **SSL-сертификат:** (SSL certificate:) и нажмите **OK**.



❗ **Улучшенный ключ** (Enhanced Key Usage) сертификата должен содержать значение **Проверка подлинности сервера** (Server Authentication).
Общее имя (Common name) сервера Indeed CM (FQDN) в поле **Субъект** (Subject).
DNS-имя (DNS Name) сервера Indeed CM в поле **Дополнительное имя субъекта** (Subject Alternative Name). Например: *indeedcmru.demo.local* (или соответствующую запись с подстановочными знаками, например: **.demo.local*).

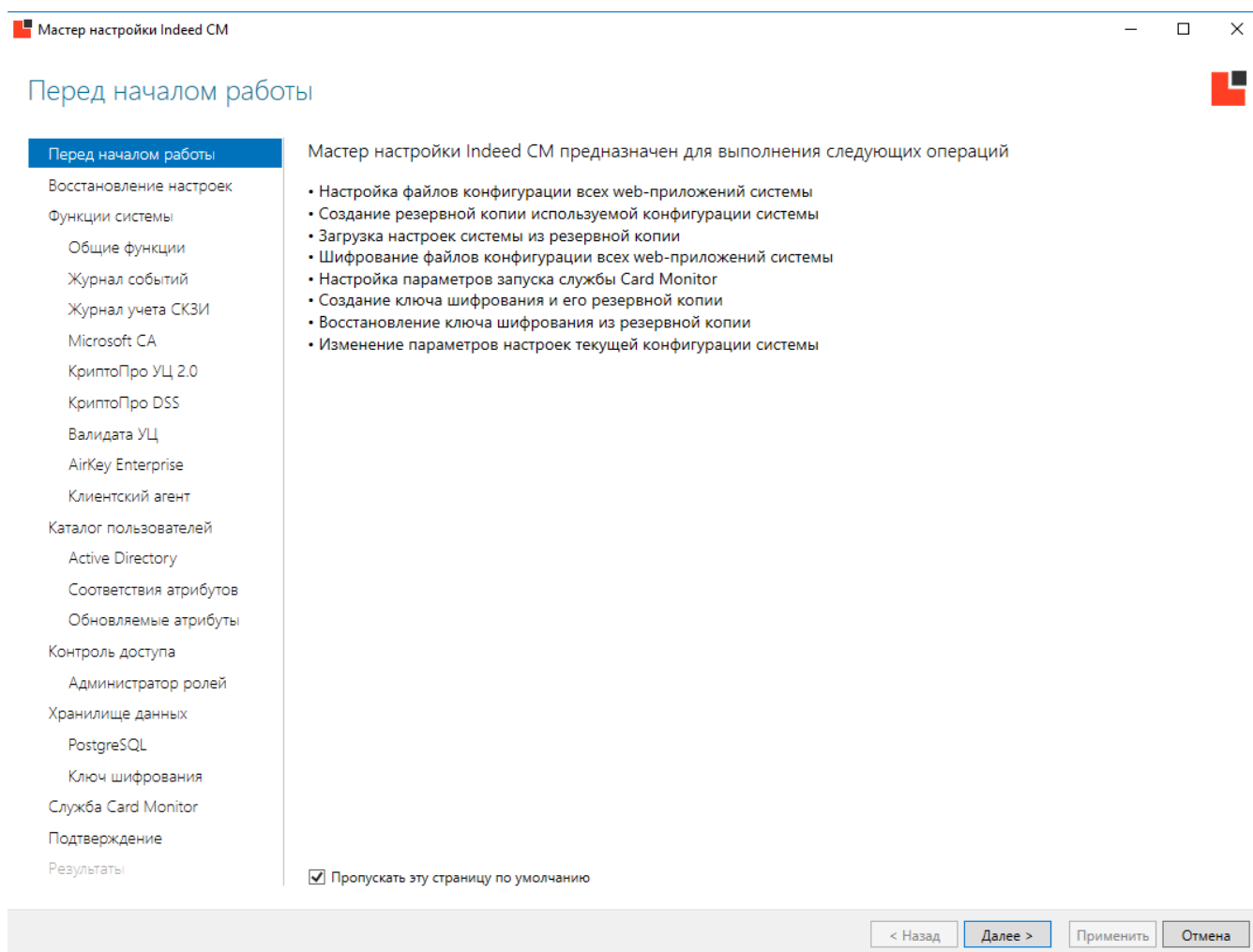
Настройка параметров системы

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).

i Файлы конфигурации службы Card Monitor расположены в %ProgramFiles%\Indeed CM\CardMonitor.

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

Также Мастер настройки Indeed CM может быть запущен в любой момент вручную (*Пуск – Все программы – Indeed*).



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

Разделы мастера настройки Indeed CM и их описание.

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

Функции системы: • Общие функции • Журнал событий • Журнал учета СКЗИ • Microsoft CA • КриптоПро УЦ 2.0 • КриптоПро DSS • Валидата УЦ • AirKey Enterprise • Клиентский агент	Общие функции: настройка внутренних параметров web-приложений Indeed CM. Консоль управления (Management Console) • Сводная информация о системе • Журнал учета устройств и сертификатов  Журнал учета реализован для конфигураций системы с использованием хранилища данных Microsoft SQL и PostgreSQL. • 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  Публикация сертификатов не поддерживается для примонтированных сетевых дисков. Задайте путь к файловому хранилищу в формате: \\Имя рабочей станции\Имя сетевого каталога Сервис самообслуживания (Self Service) • Просмотр содержимого устройства • Работа с TPM Virtual Smart Card • Работа с Windows Hello for Business • Загрузка файлов и ресурсов Журнал событий: • Переопределять атрибут имени пользователя для поиска в Журнале событий. Значение по умолчанию: CN (common name) • Настройка подключения к единому журналу событий для нескольких серверов Indeed CM Журнал учета СКЗИ: настройка параметров ведения журнала учета СКЗИ. Удостоверяющие центры: настройка параметров работы с центрами сертификации MS CA, КриптоПро УЦ 2.0 и Валидата УЦ. КриптоПро DSS: настройка интеграции с ПАК КриптоПро DSS. AirKey Enterprise: настройка интеграции с сервером виртуальных смарт-карт Indeed AirKey Enterprise. Клиентский агент: настройка параметров работы клиентского агента Indeed CM.

Каталог пользователей: • Active Directory • КристоПро УЦ 2.0 • Active Directory + КристоПро УЦ 2.0	Определение каталога пользователей системы. Параметры подключения отображаются в зависимости от выбранного каталога.
• Соответствия атрибутов	Определение атрибутов, с которыми необходимо создать нового пользователя в Центре Регистрации КристоПро УЦ 2.0 с использованием Indeed CM в момент выпуска устройства. Например: создать нового пользователя в ЦР КристоПро с теми значениями атрибутов, которые есть для существующего пользователя Active Directory.
• Обновляемые атрибуты	Определение списка атрибутов пользователя при изменении которых требуется обновление сертификата на устройстве. В список отслеживаемых атрибутов пользователя в параметрах шаблонов сертификатов Microsoft CA и КристоПро УЦ 2.0 по умолчанию включены: • Общее имя(CN) • E-mail • UPN-имя пользователя  Отслеживание изменений в атрибутах пользователей Active Directory доступно только для атрибутов из полей Субъект (Subject) и Дополнительное имя субъекта (Subject Alternative Name) сертификата.
Контроль доступа: • Администратор ролей	Определение параметров доступа к сервисам Indeed CM. Определение учетной записи для первоначальной настройки привилегий пользователей в разделе Роли Консоли управления Indeed Certificate Manager.  Указанная учетная запись должна иметь User Principal Name (UPN) и входить в выбранный каталог пользователей системы.
Хранилище данных: • Active Directory, Microsoft SQL или PostgreSQL • Ключ шифрования	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.
Служба Card	

Служба Card Monitor предназначена для выполнения операций по контролю за обращением устройств (USB-токенов и смарт-карт) и выполняет:

- Отзыв и изъятие (опционально) устройств пользователей, чьи учетные записи были удалены из каталога пользователей Indeed CM
- 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 Indeed CM, чьи учетные записи Active Directory были отключены
- Установку и сброс статуса содержимого устройства (истекает/истекло)
- Обновление содержимого устройств



Если обновление устройства проводилось через Агент Indeed CM без автоматического одобрения сертификатов оператором УЦ.

- Регистрации события Длительное отсутствие связи с агентом в системный журнал
- Рассылку почтовых уведомлений администраторам и пользователям системы:
 - 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



Для выполнения задач по регулярному запуску службы Card Monitor, учетная запись, указываемая в мастере настройки должна состоять в группе **Администраторов** (Administrators) на сервере Indeed CM и иметь разрешение на **Вход в качестве пакетного задания** (Log on as a batch job).

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:

- Выключение устройства
- Обновление 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 AirKey
- Удаление записи из журнала учета

	 Если настроена интеграция с КриптоПро DSS и AirKey Enterprise, то задайте привилегии для работы с данными устройствами.
Подтверждение	Сводная информация по настройкам всех разделов Мастера с возможностью создания резервной копии конфигурации Indeed CM. При первой установке Indeed CM настройте необходимые параметры и сохраните их копию (опция Сохранить резервную копию параметров конфигурации в разделе Подтверждение). Резервная копия настроек Indeed CM включает в себя все параметры, определенные при установке системы для всех сервисов, а также алгоритм и ключ шифрования данных. При развертывании новых серверов Indeed CM используйте файл резервной копии, указав его в разделе Восстановление настроек Мастера установки и настройки.  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.
Результаты	Прогресс работы Мастера по записи указанных значений в файлы конфигурации сервисов Indeed CM. После завершения работы Мастера настройки Indeed CM 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.

Настройка клиентского агента



Клиентский Агент Indeed CM является дополнительным компонентом системы, его установка и настройка выполняется после развертывания и настройки Indeed Certificate Manager.

Данный компонент предназначен для удаленного управления, мониторинга состояния и контроля за использованием персональных устройств аутентификации пользователей (USB-токенов, смарт-карт). В автоматическом режиме при помощи агента на рабочих станциях пользователей выполняются операции блокировки и разблокировки, очистки и смены PIN-кода администратора устройства, мониторинг устройств (смарт-карт, USB-токенов) с фиксацией информации о наличии в системе заблокированных устройств, подключении незарегистрированных устройств и попытках ввода неверных PIN-кодов. При нарушении установленных администратором правил использования устройства (например, подключение к рабочей станции другого сотрудника), устройство или сессия пользователя в операционной системе могут быть заблокированы. Компонент устанавливается совместно с Indeed CM Middleware на рабочие станции, к которым подключаются устройства, выпущенные при помощи Indeed CM.

Порядок установки и настройки:

1. [Создание сертификатов Агента](#)
2. [Настройка Indeed CM для работы с Агентами](#)
3. [Установка и настройка агентов на рабочих станциях](#)

Создание сертификатов Агента

Для работы Агентов требуются сертификаты:

- **Indeed CM Agent CA** – корневой сертификат Агента Indeed CM. Используется для выдачи сертификатов рабочим станциям пользователей, на которых будут устанавливаться Агенты.
- **Indeed CM Agent SSL** – сертификат проверки подлинности, подписан корневым сертификатом. Необходим для установления двухстороннего защищенного соединения между сервером и рабочей станцией с установленным Агентом. Сертификат выдается на имя рабочей станции, на которой развернут сервер Indeed CM.
- **Сертификат рабочей станции** – выдается автоматически при регистрации Агента. Обращаясь к серверу клиентский компьютер предоставляет свой сертификат, сервер Indeed CM проверяет подлинность сертификата после чего начинает доверять Агенту, установленному на рабочей станции пользователя, и готов передавать на него задачи.

Сертификаты Агента создаются при помощи утилиты **IndeedCM.Agent.Cert.Generator.exe**, входящей в состав дистрибутива Indeed CM (располагается в `IndeedCM\Server\Misc\AgentCertGenerator`).

1. Запустите в командной строке, запущенной от имени администратора, на сервере Indeed CM утилиту с параметрами: **IndeedCM.Agent.Cert.Generator.exe /root /csn /installToStore**. Дождитесь завершения работы утилиты.



Параметр **/csn** запускает процедуру выпуска сертификатов на DNS-имя рабочей станции, на которой запускается утилита. Для создания сертификатов для рабочей станции с другим именем запустите утилиту с параметром **/sn <DNS-имя рабочей станции>**.

Параметр **/installToStore** публикует выпущенные утилитой сертификаты в хранилища сертификатов сервера:

- Сертификат **Indeed CM Agent CA** в **Доверенные корневые центры сертификации** (Trusted Root Certification Authorities)
- Сертификат **Indeed CM Agent SSL** в хранилище личных сертификатов рабочей станции, на которой установлен сервер Indeed CM.

2. В каталоге с утилитой появятся файл **Indeed CM Agent CA.key**, содержащий отпечаток сертификата Indeed CM Agent CA и значение ключа сертификата.
3. Поместите сертификат **Indeed CM Agent CA** в **Доверенные корневые центры сертификации** (Trusted Root Certification Authorities) на всех рабочих станциях пользователей.

 Для распространения сертификата на рабочие станции пользователей удобно использовать механизм групповых политик Active Directory.

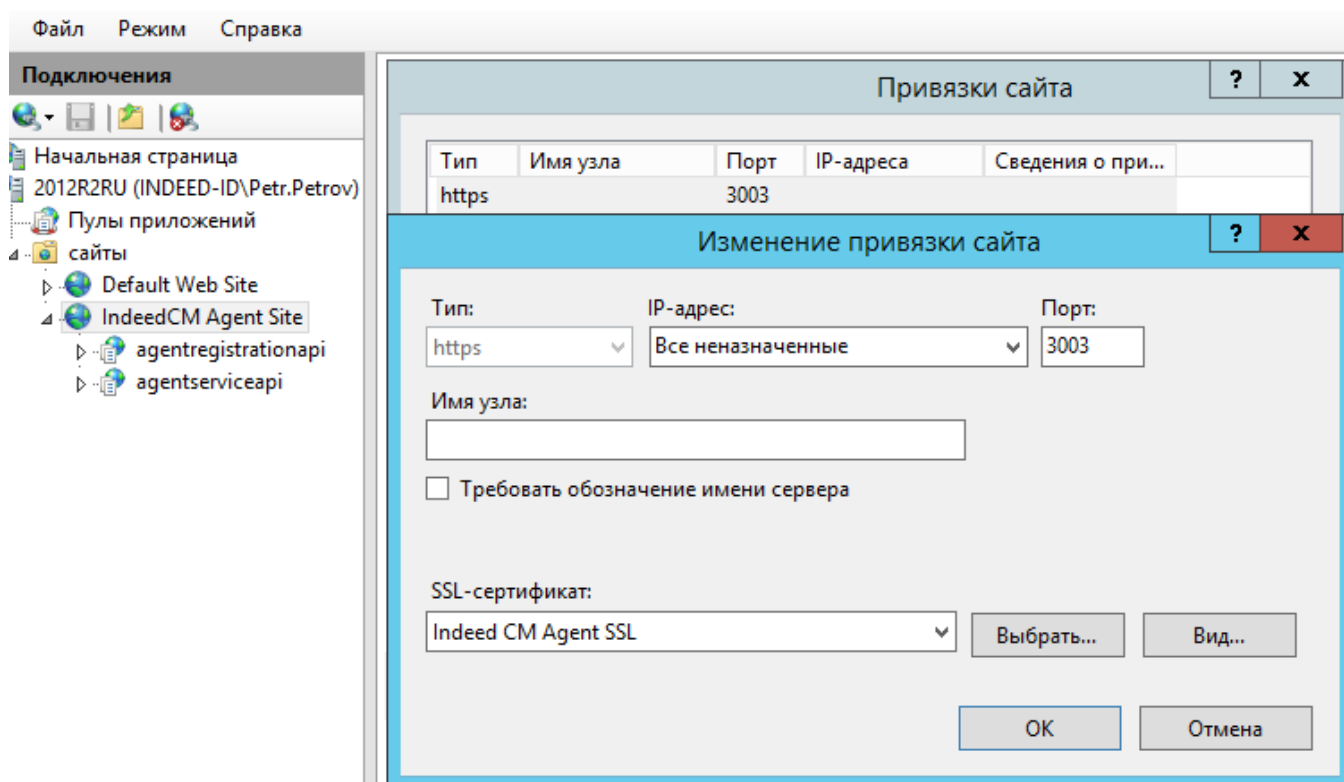
4. Настройте защищенное соединение с сайтом Агентов. Для этого:

- Перейдите в **Диспетчер служб IIS** (Internet Information Services (IIS) Manager).
- Выберите сайт **IndeedCM Agent Site** и перейдите в раздел **Привязки...** (Bindings...).
- Выберите привязку по порту **3003**.
- Нажмите **Изменить...** (Edit...).

 Порт **3003** устанавливается по умолчанию. Если вы используете другой порт, то создайте и настройте новую привязку для него. Убедитесь в том, что порт открыт для входящих подключений в брандмауэре.

- Укажите в качестве **SSL-сертификата** сертификат **Indeed CM Agent SSL** и нажмите **ОК**.

5. Пример настройки привязки для сайта IndeedCM Agent Site.



6. Если в вашем окружении используется несколько серверов Indeed CM с Агентами, то для каждого сервера потребуется свой SSL-сертификат Агента (корневой сертификат на всех серверах один и тот же). Для создания SSL-сертификата дополнительного сервера перенесите на него каталог с утилитой **IndeedCM.Agent.Cert.Generator.exe** и файл ключа корневого сертификата **Indeed CM Agent CA.key**, затем выполните команду:

```
IndeedCM.Agent.Cert.Generator.exe /ssl /csn /rootKey <путь к каталогу с ключом корневого сертификата> /installToStore
```

Пример:

```
IndeedCM.Agent.Cert.Generator.exe /ssl /csn /rootKey "C:\AgentCertGenerator\Indeed CM Agent CA.key" /installToStore
```

Настройка Indeed CM для работы с Агентами

Для того, чтобы Indeed Certificate Manager смог назначать задачи на Агенты, включите опцию **Разрешить использование клиентских агентов** в Мастере настройки Indeed CM и выполните настройку сервиса агентов:

Мастер настройки Indeed CM

Клиентский агент

Перед началом работы
Восстановление настроек
Функции системы
Общие функции
Журнал событий
Журнал учета СКЗИ
Microsoft CA
КриптоПро УЦ 2.0
КриптоПро DSS
Валидата УЦ
AirKey Enterprise
Клиентский агент
Каталог пользователей
Active Directory
Соответствия атрибутов
Обновляемые атрибуты
Контроль доступа
Администратор ролей
Хранилище данных
Active Directory
Ключ шифрования
Служба Card Monitor
Подтверждение
Результаты

Настройки клиентского агента

☒ Разрешить использование клиентских агентов

Идентификатор агента в домене: Не задано

Идентификатор агента вне домена: Не задано

☐ Автоматическая регистрация агентов

[Загрузить сертификат агента:](#) сертификат **не** предоставлен
(Сертификат генерируется утилитой Agent.Cert.Generator)

Уровень журналирования событий агентом: Все

Периодичность получения данных с сервера (сек.)
30

Интервал повторного выполнения отмененной пользователем задачи (сек.)
60

Имя заголовка https-запроса сертификата
X-IndeedCM-ClientCert

Имя заголовка используется балансировщиком нагрузки для передачи сертификата агента

☐ Передавать в заголовках https-запросов только поле 'Субъект' сертификата агента
Если опция выключена, в запросе передается полностью сертификат агента

< Назад Далее > Применить Отмена

1. Укажите стратегию генерации **Идентификатора агента для доменных/вне доменных компьютеров** для регистрации в системе:

- **Не задано** (значение по умолчанию)
- **Использовать машинный GUID** ('MachineGuid' рабочей станции)
- **Генерировать новый GUID** (если имеется вероятность использования одного значения 'MachineGuid' несколькими рабочими станциями)
- **Использовать доменный SID компьютера**
- **Использовать SID компьютера** (в случае использования агента на рабочих станциях, находящихся вне домена)



При указании стратегии **Использовать машинный GUID**, идентификатору агента присваивается строковое значение 'MachineGuid' из ветки реестра [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography] рабочей станции.



При смене **Стратегии генерации идентификатора агента** необходимо:

- Удалить все агенты на клиентских рабочих станциях (**Indeed CM - Agent**)
- Удалить все агенты в разделе **Агенты** Консоли управления
- После изменения параметра в Мастере настройки Indeed CM, необходимо **Настроить Агентов на рабочих станциях пользователя**

2. Для регистрации агентов без подтверждения со стороны администратора включите опцию **Автоматическая регистрация Агентов**.



Управление агентами осуществляется в разделе **Агенты** Консоли управления Indeed Certificate Manager. После установки и настройки Агента на рабочей станции при включении данной опции он появится в разделе со статусом **Зарегистрирован**.

3. **Загрузите сертификат агента** - файл **Indeed CM Agent CA.key**, содержащий отпечаток сертификата Indeed CM Agent CA и значение ключа сертификата.

4. Выберите **Уровень журналирования событий агентом**:

- Все (значение по умолчанию)
- Только ошибки
- Только предупреждения и ошибки

5. Укажите **Периодичность получения данных с сервера** и **Интервал повторного выполнения отмененной пользователем задачи**.

6. Если система используется с балансировщиком нагрузки, то имеется возможность изменить **Имя заголовка https-запроса сертификата**. Для передачи только значения поля '**Субъект**' сертификата агента в заголовках https-запросов включите соответствующую опцию.
7. Примените изменения в Мастере настройки, перейдите в пункт **Подтверждение** и **Сохраните резервную копию параметров конфигурации** Indeed CM.

Установка и настройка агентов на рабочих станциях

Установка клиентских агентов

Клиентский агент устанавливается на рабочие станции пользователей.

Запустите файл **IndeedCM.Agent.msi** из дистрибутива Indeed CM (каталог **IndeedCM.Client**) и выполните установку, следуя указаниям мастера. После установки агент запустится автоматически.

Необходимые для связи с сервером Indeed Certificate Manager настройки задаются через групповые политики или реестр Windows.

Настройка параметров работы агента через групповые политики

Для добавления административных шаблонов Indeed-Id выполните следующие действия:

1. Скопируйте содержимое каталога **IndeedCM.Client\Misc** в центральное хранилище ADMX-файлов контроллера домена C:
\Windows\SYSTEM32\policies\PolicyDefinitions.

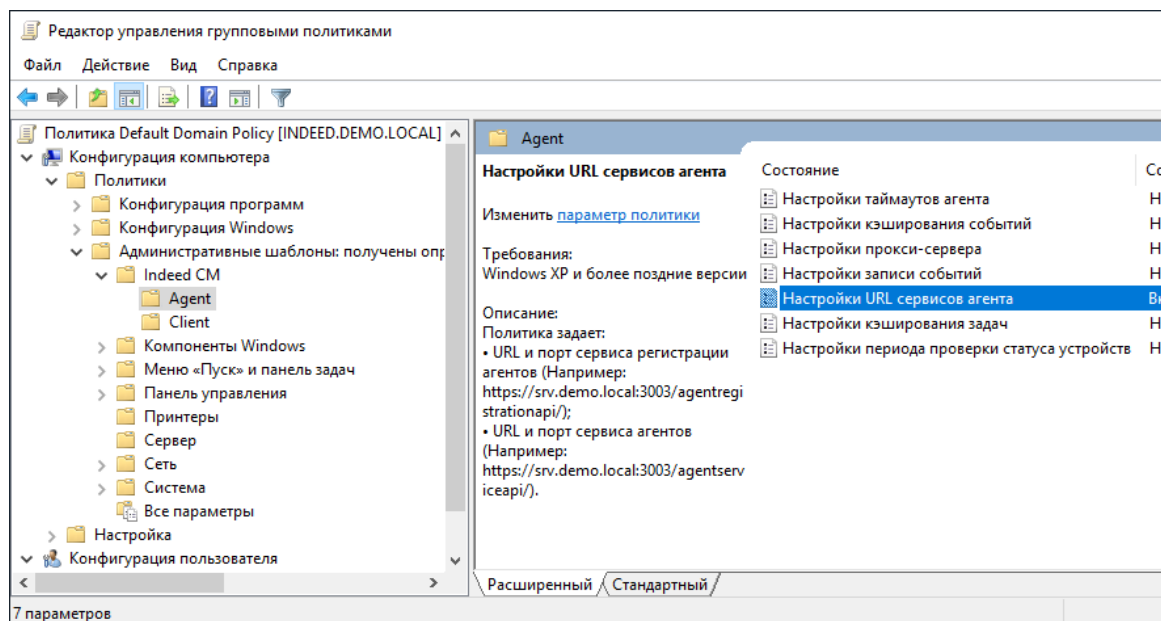
 При использовании локального хранилища ADMX-файлов поместите шаблоны Indeed-Id в **C:\Windows\PolicyDefinitions**.

2. Откройте консоль **Управление групповой политикой** (Group Policy Management).
3. В дереве окна консоли создайте новый объект групповой политики или выберите существующий.
4. Вызовите контекстное меню и выберите пункт **Изменить** (Edit).
5. В открывшемся **Редакторе управления групповыми политиками** (Group Policy Management Editor) выберите **Конфигурация компьютера** (Computer Configuration) > **Политики** (Policies) > **Административные шаблоны** (Administrative Templates) > **Indeed CM > Agent**.
6. Включите политику **Настройка URL сервисов агентов** (Agent's URL Settings) и укажите её значения:
 - в параметре **URL сервиса регистрации агентов** (Agents registration service URL) укажите web-адрес и порт подключения к приложению **agentregistrationapi**, размещенного на сервере Indeed CM.
 - в параметре **URL сервиса агентов** (Agents service URL) укажите web-адрес и порт сервиса **agentserviceapi**.

Пример:

URL сервиса регистрации агентов: <https://srv.demo.local:3003/agentregistrationapi/>

URL сервиса агентов: <https://srv.demo.local:3003/agentserviceapi/>



7. Свяжите этот объект политики с группой, членами которой являются рабочие станции пользователей системы Indeed CM.

8. Нажмите **Применить** (Apply) и выполните обновление политик.



Обновление политик происходит при перезагрузке рабочей станции с установленным клиентским агентом. Для принудительного обновления групповых политик без перезагрузки выполните команду **gpupdate /force**.

В случае необходимости настройте дополнительные политики, определяющие работу Агентов:

Настройки таймаутов агентов (Agent's timeouts settings)

Политика задает:

- Таймаут запросов к сервисам агента (по умолчанию: 30 сек.)
- Периодичность запроса проверки статуса агента (по умолчанию: 300 сек.)

- Периодичность запроса на обновление настроек, привязок, задач и сессий (по умолчанию: 30 сек.)
- Таймаут запроса отключения агента от сервера (по умолчанию: 3 сек.)

Настройки кэширования событий (Events caching settings)

Политика задает настройки кэширования событий:

- Период в минутах, в течение которого агент будет пытаться отправить события из кэша на сервер (по умолчанию: 10 мин.)
- Количество событий, передаваемых за один раз из кэша рабочей станции пользователя на сервер (по умолчанию: 500 событий)

Настройки прокси-сервера (Proxy server settings)

Политика определяет использование прокси-сервера при подключении к серверу Indeed CM.

Если политика не задана или отключена, прокси-сервер использоваться не будет. В параметре "Прокси-сервер" задается адрес прокси-сервера.

Настройки записи событий (Event log settings)

Политика задает уровень записи событий в серверный журнал:

- Все (по умолчанию)
- Только ошибки
- Только ошибки и предупреждения

Настройки кэширования задач (Tasks caching settings)

Политика задает:

- Периодичность обновления кэша задач и отправки статуса выполнения задачи на сервер, если сразу не удалось сообщить статус серверу (по умолчанию: 60 сек)
- Таймаут, при котором задачи будут удалены из кэша при очередном обновлении кэша (по умолчанию: 300 сек.)
- Таймаут, после которого можно будет повторно выполнить отмененную пользователем задачу (по умолчанию: 60 сек.)

Настройки периода проверки статуса устройств (Smart card status update settings)

Политика задает периодичность проверки статуса устройств (по умолчанию: 30 сек.):

- Блокировка PIN-кода пользователя\администратора
- Попытки ввода неверного PIN-кода пользователя\администратора

Настройка параметров работы агента через реестр

Создайте файл реестра (.reg) со следующим содержанием:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\IndeedCM\Agent]
"AgentRegistrationServiceUrl"=""
"AgentServiceUrl"=""
"ProxyEnable"=""
"ProxyServer"=""
```



Для 32-разрядных ОС параметры настраиваются в ветке:

[HKEY_LOCAL_MACHINE\SOFTWARE\IndeedCM\Agent]

В параметре **AgentRegistrationServiceUrl** укажите ссылку и порт подключения к приложению **agentregistrationapi**.

В параметре **AgentServiceUrl** укажите web-адрес и порт подключения к приложению **agentserviceapi**.

Если на рабочих станциях где установлен клиентский агент используется прокси, то укажите параметры **ProxyEnable** и **ProxyServer** (URL прокси-сервера).

Возможные значения параметров:

1. "ProxyEnable"=dword:00000000 - прокси не используется.
2. "ProxyEnable"=dword:00000001 и "ProxyServer"= "" - используются настройки прокси по умолчанию.
3. "ProxyEnable"=dword:00000001 и "ProxyServer"="<URL прокси-сервера>" - используется прокси-сервер, указанный в настройке.

Ниже приведен пример содержимого .reg-файла для подключения к серверу Indeed CM с именем *srv.demo.local* по протоколу *https* и порту *3003* с использованием прокси-сервера *https://192.168.10.10:443*.

Пример:

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\IndeedCM\Agent]
"AgentRegistrationServiceUrl"="https://srv.demo.local:3003/agentregistrationapi/"
"AgentServiceUrl"="https://srv.demo.local:3003/agentserviceapi/"
"ProxyEnable"=dword:00000001
"ProxyServer"="https://192.168.10.10:443"
```



Распространите файл реестра и внесите изменения на рабочие станции пользователей. Для применения внесенных изменений перезагрузите рабочую станцию с установленным Агентом Indeed CM или перезапустите службу **Indeed CM Agent Service**.

Единый журнал событий

Единый журнал событий используется в конфигурации системы с несколькими серверами Indeed Certificate Manager и предназначен для записи событий со всех серверов в общий журнал. Единый журнал может быть настроен с помощью приложений **Indeed CM Event Log Proxy** или **Indeed Log Server**.

- [Event Log Proxy](#)
- [Indeed Log Server](#)
- [Настройка Indeed CM на работу с единым журналом событий](#)

Event Log Proxy

Компонент **Indeed CM Event Log Proxy** позволяет записывать события со всех серверов Indeed Certificate Manager в единый журнал Windows Event Log.

 Компонент устанавливается на одном из серверов Indeed CM или на отдельной рабочей станции (в домене или вне его). Системные требования для установки компонента совпадают с требованиями к серверу Indeed CM.

Для установки и настройки Indeed CM Event Log Proxy выполните следующие действия:

1. Выполните вход на рабочую станцию с правами локального администратора.
2. Запустите **IndeedCM.EventLog.Proxy.msi** из дистрибутива (располагающемся в каталоге `IndeedCM.Server`) и выполните его установку следуя указаниям Мастера.
3. Откройте файл конфигурации сервиса `eventLogProxy`: **C:\inetpub\wwwroot\eventlogproxy\Web.config** в редакторе Блокнот, запущенном от имени администратора.
4. В секции **authorization** укажите имя учетной записи для доступа к сервису. В качестве учетной записи используйте сервисную учетную запись Indeed CM для работы с Active Directory (**servicecm**).
Во внедоменной конфигурации используйте локальную учетную запись пользователя (например, `SERVERNAME\Администратор`).

Пример заполненной секции:

```
<authorization>
  <deny users="?" />
  <allow users="DEMO\servicecm"/>
  <deny users="*" />
</authorization>
```

5. Сохраните изменения и закройте файл конфигурации.

Indeed Log Server

Компонент **Indeed Log Server** позволяет записывать события со всех серверов Indeed Certificate Manager в единый журнал Windows Event Log, SysLog, СУБД Microsoft SQL Server или PostgreSQL.

 Компонент устанавливается на одном из серверов Indeed CM или на отдельной рабочей станции (в домене или вне его). Системные требования для установки компонента совпадают с требованиями к серверу Indeed CM.

Установка Indeed Log Server

1. Выполните вход на рабочую станцию с правами локального администратора.
2. Запустите **Indeed.LogServer.msi** из дистрибутива (каталог **Indeed.Log.Server**) и выполните его установку следуя указаниям Мастера.
 - Из каталога **Indeed.Log.Server** скопируйте файл **cmSchema.config** в каталог **C:\inetpub\wwwroot\ls**.
 - Из каталога **Indeed.Log.Server\targetConfigs** файлы **cmEventLogTarget.config** и **cmSqlTarget.config** в каталог **C:\inetpub\wwwroot\ls\targetConfigs**.

Настройка чтения и записи событий в Windows Event Log

1. Перейдите в каталог **C:\inetpub\wwwroot\ls** и отредактируйте файл **clientApps.config** следующим образом:

- В секции **Applications** добавьте:

```
<Application Id="cm" SchemaId="cmSchema">
  <ReadTargetId>cmEventLogTarget</ReadTargetId>
  <WriteTargets>
    <TargetId>cmEventLogTarget</TargetId>
  </WriteTargets>
  <AccessControl>
    <!--<CertificateAccessControl CertificateThumbprint="001122...AA11" Rights="
Read" />-->
  </AccessControl>
</Application>
```

- В секции **Targets** добавьте новый элемент:

```
<Targets>
...
  <Target Id="cmEventLogTarget" Type="eventlog"/>
</Targets>
```

2. Сохраните изменения и закройте файл конфигурации.

Настройка чтения и записи событий в СУБД MS SQL

База для хранения данных Indeed Log Server создается вручную, а её наполнение происходит автоматически.

1. Создайте базу данных в среде SQL Management Studio с произвольным именем:

- В окне **Обозреватель объектов** (Object Explorer) нажмите правой кнопкой мыши по вкладке **Базы данных** (Databases).
- Выберите **Создать базу данных...** (New Database...).
- Укажите **Имя базы данных:** (Database name:) например, **LogServer**.
- В поле **Владелец:** (Owner:) определите владельца создаваемой базы.

 Создайте (например, **servicesql**) или выберите любую внутреннюю учетную запись SQL, или учетную запись Active Directory (например, сервисную учетную запись для работы Indeed CM: **servicecm**). Указанная учетная запись после создания базы будет обладать правами **db_owner, public** и будет использоваться системой для выполнения операций записи/чтения в базу данных.

- Сохраните созданную базу данных нажав **OK**.

Создание базы данных

Выбор страницы

- Общие
- Параметры
- Файловые группы

Соединение

Сервер:
DC\SQLEXPRESS

Соединение:
sa

[Просмотреть свойства соеди...](#)

Ход выполнения

Готово

Скрипт Справка

Имя базы данных: LogServer

Владелец: servicesql

☒ Использовать полнотекстовое индексирование

Файлы базы данных:

Логическое имя	Тип файла	Файловая группа	Начальный размер (МБ)	Автоувелич...
LogServer	Данные ...	PRIMARY	8	С шагом п...
LogServer_log	ЖУРНАЛ	Неприменимо	8	С шагом п...

Добавить Удалить

OK Отмен

2. Перейдите в каталог **C:\inetpub\wwwroot\ls\targetConfigs** и отредактируйте файл **cmSqlTarget.config** в соответствии с настройками ниже:

<Settings> ... </Settings>:

- **Data Source** - имя сервера Microsoft SQL Server или именованного экземпляра Microsoft SQL Server
- **Database** - имя базы данных (ILS)
- **User Id** - сервисная учётная запись для работы с базами данных Indeed CM
- **Password** - пароль сервисной учётной записи

```
<Settings>
  <ConnectionString>Data Source=MSSQL\SQLEXPRESS;Database=LogServer;User
Id=servicesql;Password=P@sswOrd</ConnectionString>
</Settings>
```



В случае использования именованного экземпляра Microsoft SQL Server значение параметра **Server** необходимо задавать в формате **<имя сервера>\<имя экземпляра>**.

```
<Settings>
  <ConnectionString>Server=sql\Named instance; ... </ConnectionString>
</Settings>
```

3. Отредактируйте **C:\inetpub\wwwroot\ls\clientApps.config** для работы с файлом **cmSqlTarget.config**:

- В секции **Application** добавьте:

```
<Application Id="cm" SchemaId="cmSchema">
  <ReadTargetId>cmSqlTarget</ReadTargetId>
  <WriteTargets>
    <TargetId>cmSqlTarget</TargetId>
  </WriteTargets>
  <AccessControl>
    <!--<CertificateAccessControl CertificateThumbprint="001122...AA11" Rights="
Read" />-->
  </AccessControl>
</Application>
```

- В секции **Targets** добавьте новый элемент:

```
<Targets>
  ...
  <Target Id="cmSqlTarget" Type="mssql"/>
</Targets>
```

4. Сохраните изменения и закройте файл конфигурации.

Настройка Indeed CM на работу с единым журналом событий



Локальные события, записанные ранее на серверах Indeed Certificate Manager будут недоступны в разделе **Журнал** при переходе на единый журнал для всех серверов. Такие события останутся в журнале Windows **IndeedCM/Operational** на каждом сервере Indeed CM.

После настройки всех серверов Indeed CM на работу с единым журналом событий все события со всех серверов Indeed CM будут записываться в него.

Для настройки сервера Indeed CM на работу с единым журналом выполните следующие действия:

1. Выполните вход на сервер Indeed CM с правами локального администратора.
2. Запустите **Мастер настройки Indeed CM** (Пуск – Все программы – Indeed).
3. Перейдите в раздел **Журнал событий**.

- Нажмите **Включить Indeed CM Event Log Proxy**, если для единого журнала событий используется приложение **Event Log Proxy** и укажите:
 - URL подключения к Event Log Proxy – URL сервиса Event Log Proxy.

https://<FQDN сервера>/eventlogproxy

- **Имя сервисной учетной записи** – имя пользователя для подключение к сервису **eventlogproxy** (из секции **<authorization>** файла **Web.config** приложения **eventlogproxy**).

☒ **Использовать локальный журнал Windows**

☒ **Включить Indeed CM Event Log Proxy**

Используется в конфигурации системы с несколькими серверами Indeed CM. При включении опции все серверы используют единый журнал Windows. Для использования единого журнала установите и настройте приложение Indeed CM Event Log Proxy.

URL подключения к Event Log Proxy

https://indeedcmru.demo.local/eventlogproxy

Например: **https://server.demo.local/eventlogproxy**

Имя сервисной учетной записи

DEMO\servicecm

Укажите учетную запись, обладающую правами на доступ к единому журналу событий

☐ **Использовать Indeed Log Server**

Используется в конфигурации системы с несколькими серверами Indeed CM. При включении опции события записываются в единый журнал Windows, SysLog, базу данных Microsoft SQL или PostgreSQL. Для использования единого журнала установите и настройте приложение Indeed Log Server.

URL подключения к Indeed Log Server

https://indeedcmru.demo.local/lis/api

Например: **https://server.demo.local/lis/api**

- Выберите **Использовать Indeed Log Server**, если единый журнал событий настроен через приложение **Indeed Log Server** и укажите:
 - URL подключения к Indeed Log Server – URL сервиса Indeed Log Server.

https://<FQDN сервера>/lis/api

4. Перейдите в раздел **Подтверждение** и нажмите **Применить**.
5. Выполните настройку на работу с единым журналом событий, повторив пункты 2-4 на каждом сервере Indeed CM.
6. Перейдите в консоль управления Indeed CM в браузере и выполните поиск в разделе **Журнал**.
Ожидаемый результат: отсутствие каких-либо ошибок.

❗ Поиск в Журнале может не дать результатов, если журнал на удаленном сервере не содержит никаких событий. Выполните на сервере Indeed CM, настроенном на работу с единым журналом любое действие, результат которого записывается в журнал (выключение устройства, добавление или изменение комментария и т.п.) и повторите поиск событий.

Установка клиентских компонентов

Установка Indeed CM Middleware

Компоненты Indeed CM Middleware устанавливаются на рабочих местах операторов Indeed Certificate Manager и на рабочих станциях пользователей. В зависимости от типа устройств, используемых в организации, на рабочую станцию оператора и пользователя устанавливаются те или иные компоненты Middleware. Например, для работы с устройствами **Рутокен** необходимо установить компонент **IndeedCM.Rutoken.Middleware**, а для устройств **eToken** (Thales) – **IndeedCM.eToken.Middleware**.

Запустите файл **IndeedCM.Middleware.msi** из дистрибутива Indeed CM (каталог IndeedCM.Client) и выполните установку, следуя указаниям мастера.

 На всех рабочих станциях пользователей должны быть установлены драйвера и сервисные утилиты, тех устройств и считывателей, которые будут использоваться с системой Indeed CM. Это ПО не входит в комплект поставки Indeed CM.

Таблица соответствия производителей, типов устройств и клиентских Middleware:

Производитель	Модели устройств	Middleware
Компания «Актив»	Рутокен S	IndeedCM.Rutoken.Middleware
	Рутокен Lite и Lite SC	
	Рутокен ЭЦП PKI и ЭЦП PKI SC	
	Рутокен ЭЦП 2.0 и ЭЦП 2.0 SC	
	Рутокен 2151 и 2151 SC	
	Рутокен ЭЦП 3.0 NFC и ЭЦП 3.0 NFC SC	
Компания Индид	Сетевая смарт-карта AirKey	IndeedCM.AirKey.Middleware

Аладдин Р.Д.	JaCarta PKI	IndeedCM.JaCarta.Middleware
	JaCarta PKI/Flash	
	JaCarta PKI/BIO	
	JaCarta PKI/ГОСТ	
	JaCarta PKI/ГОСТ/Flash	
	JaCarta-2 PKI/ГОСТ	
	JaCarta-2 PKI/ГОСТ /Flash	
	JaCarta-2 SE	
ACS	ACOS5-64	IndeedCM.ACOS.Middleware
Avest	Avest Key 256A	IndeedCM.Avest.Middleware
Bit4id	ID-One Cosmo	IndeedCM.Bit4Id.Middleware
CRYPTAS	TicTok V2/V3	IndeedCM.TicTok.Middleware
Cryptovision	ePasslet Suite v3.0, JCOP V3.0	IndeedCM.Cryptovision.Middleware
Feitian	ePass2003 (A1+, A2)	IndeedCM.ePass.Middleware
	BioPass2003	
HID	Crescendo C1150 Series	IndeedCM.HID.Middleware
	Crescendo C1300 Series	
	Crescendo C2300 Series	
ISBC	ESMART Token 64K и ESMART Token SC 64K	IndeedCM.ESMART.Middleware
	ESMART Token ГОСТ и ESMART Token SC ГОСТ	
	MS_KEY K-"Ангара"	
Kaztoken	Kaztoken, Kaztoken SC	IndeedCM.Kaztoken.Middleware
Microsoft	Реестр Локального компьютера	IndeedCM.Registry.Middleware
	Реестр Пользователя	

 Для возможности выпуска устройств **Registry** с записью сертификатов в локальное хранилище компьютера и/или пользователя через **Сервис самообслуживания** (Self Service) **включите поддержку данных устройств через групповую политику.**

	TPM Virtual Smart Card (Microsoft VSC) - виртуальная смарт-карта на базе Trusted Platform Module v.2.0	IndeedCM.TPM.Middleware
	Windows Hello for Business (WHfB)	IndeedCM.WHfB.Middleware
RSA	RSA SecurID 800	IndeedCM.RSA.Middleware
Thales Group (Ex SafeNet and Gemalto)	SafeNet eToken PRO 32k SafeNet eToken PRO 64k eToken PRO Java 72K OS755 SafeNet eToken 5105 SafeNet eToken 5110 IDCore30B eToken 1.7.7	IndeedCM.eToken.Middleware
	IDPrime MD 830 IDPrime MD 840 IDPrime MD 3810 IDPrime MD 3811	IndeedCM.Gemalto.Middleware
Yubico	YubiKey 5 Series	IndeedCM.YubiKey.Middleware

Установка Indeed CM Client Tools

Компонент Indeed CM Client Tools требуется для разблокировки смарт-карт, используемых для аутентификации в операционной системе Windows, в offline- и online-режимах и для разблокировки смарт-карт, которые не используются для входа в операционную систему. Данный компонент устанавливается на рабочие станции пользователей.

Запустите файл **IndeedCM.Client.Tools.msi** из дистрибутива Indeed CM (каталог IndeedCM.Client) и выполните установку, следуя указаниям мастера.



Для online-режима разблокировки необходимо выполнить [настройку разблокировки устройств](#).

Установка Indeed CM Agent

Indeed CM Agent является дополнительным компонентом системы, его установка и настройка выполняется после развертывания и настройки Indeed Certificate Manager. Данный компонент предназначен для удаленного управления, мониторинга состояния и контроля за использованием персональных устройств аутентификации пользователей (USB-токенов, смарт-карт). В автоматическом режиме при помощи агента на рабочих станциях пользователей выполняются операции блокировки и разблокировки, очистки и смены PIN-кода администратора устройства; мониторинг состояния устройств с фиксированием информации в журнал о наличии в системе заблокированных устройств, подключении незарегистрированных устройств, попытках ввода неверных PIN-кодов. Компонент устанавливается **совместно с Indeed CM Middleware** на рабочие станции, к которым подключаются устройства, выпущенные при помощи Indeed CM.

Запустите файл **IndeedCM.Agent.msi** из дистрибутива Indeed CM (каталог IndeedCM.Client) и выполните установку, следуя указаниям мастера. После установки Агент запустится автоматически.



На всех рабочих станциях пользователей должны быть установлены Indeed CM Middleware, драйвера и сервисные утилиты, тех устройств и считывателей, которые будут использоваться с системой Indeed CM.

Необходимые для связи с сервером Indeed CM настройки и другие параметры Агента **задаются через групповые политики или реестр Windows**.

Настройка разблокировки устройств

Разблокировка устройств реализована в двух режимах:

1. **Online режим** подразумевает, что рабочая станция пользователя, к которой подключено заблокированное устройство, имеет соединение с сервером Indeed CM. Соединение с сервером необходимо для проведения аутентификации пользователя при помощи ответов на секретные вопросы. Для связи рабочих станций пользователей с сервером Indeed CM при online-разблокировке рекомендуется использовать защищенное соединение (https).
2. Разблокировка в **Offline режиме** осуществляется оператором Indeed CM по принципу аутентификации вида запрос-ответ (англ. challenge-response authentication mechanism).
При исчерпании заданного числа попыток ввода PIN-кода, пользователь получает сообщение о том, что его устройство заблокировано. Вместе с сообщением пользователь получает уникальный 16-ти символьный код-запрос. Пользователю необходимо связаться с оператором системы (например, по телефону) и подтвердить свою личность.

Настройка разблокировки устройств через групповые политики

Для включения возможности **online**-разблокировки устройств настройте соответствующую групповую политику. Эта политика должна распространяться на **рабочие станции пользователей** Indeed CM.

Для добавления административных шаблонов Indeed-Id выполните следующие действия:

1. Скопируйте содержимое каталога **IndeedCM.Client\Misc** в центральное хранилище ADMX-файлов контроллера домена C:
\Windows\SYVOL\domain\Policies\PolicyDefinitions.



При использовании локального хранилища ADMX-файлов поместите шаблоны Indeed-Id в **C:\Windows\PolicyDefinitions.**

2. Откройте консоль **Управление групповой политикой** (Group Policy Management).
3. В дереве окна консоли создайте новый объект групповой политики, или выберите существующий.
4. Вызовите контекстное меню и выберите пункт **Изменить** (Edit).

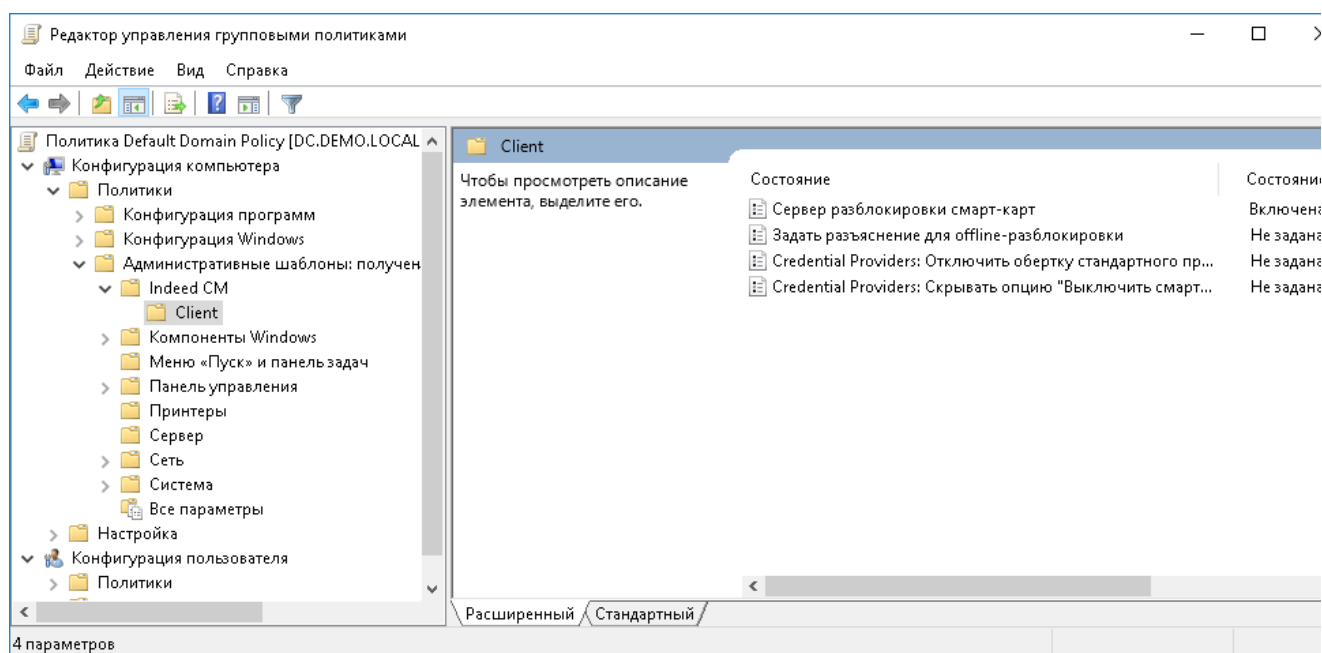
5. В открывшемся **Редакторе управления групповыми политиками** (Group Policy Management Editor) выберите **Конфигурация компьютера** (Computer Configuration) > **Политики** (Policies) > **Административные шаблоны** (Administrative Templates) > **Indeed CM > Client**.

6. Включите политику **Сервер разблокировки смарт-карт** (Smart card unlocking server) и укажите её значения:

- в параметре **URL сервиса** (Service URL) укажите ссылку на компонент **credprovapi**, размещенный на сервере Indeed CM.

https://<FQDN сервера Indeed CM>/credprovapi

- в параметре **Проверять сертификат сервера** (Verify server certificate) установите значение **Да**, если необходимо проводить проверку подлинности сертификата сервера. Установите **Нет** (значение по умолчанию), если проверку подлинности проводить не требуется.



7. Свяжите этот объект политики с группой, членами которой являются рабочие станции пользователей системы Indeed CM.

8. Нажмите **Применить** (Apply) и выполните обновление политик.

В случае необходимости настройте дополнительные политики, определяющие работу сервиса разблокировки:

Задать разъяснения для offline-разблокировки (Set explanations for offline unlocking)

Политика применяется к рабочим станциям пользователей. Если политика **выключена или не определена**, то при offline-разблокировке устройства текст разъяснения в Credential Provider не отображается.

Если политика **включена** то, при offline-разблокировке устройства в Credential Provider будет отображаться указанный в политике текст разъяснения. Например, контактный телефон администратора Indeed CM.

Credential Providers: Отключить обертку стандартного провайдера смарт-карт (Credential Providers: Disable smart card standard provider wrapping)

Политика применяется к рабочим станциям пользователей. Если политика **выключена или не определена**, пользователь имеет возможность выполнить разблокировку смарт-карты в стандартном интерфейсе входа в ОС Windows по смарт-карте.

Если политика **включена**, то отдельная опция для разблокировки смарт-карты будет отображаться на экране входа в ОС. Такая настройка может быть использована в ситуации, когда на рабочей станции установлено стороннее ПО, запрещающее разблокировку карты через стандартный Credential Provider.

Credential Providers: Скрывать опцию "Выключить смарт-карту" (Credential Providers: Hide the "Disable the smart card" option)

Политика применяется к рабочим станциям пользователей. Если политика **выключена или не определена**, пользователь имеет возможность выполнить выключение смарт-карты в интерфейсе входа в ОС Windows.

Если политика **включена**, то опция для выключения смарт-карты не будет отображаться на экране входа в ОС.

Настройка разблокировки устройств вне домена Windows

В случае, когда сервер Indeed CM и рабочие станции пользователей находятся вне домена Windows, путь к приложению **credprovapi** необходимо прописать в реестре каждой клиентской рабочей станции. Для этого создайте файл реестра (.reg) со следующим содержанием:

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\IndeedCM\Client]

"CredProvAPIURL"=""

"AdminDetails"=""

"DisableServerCertificateChecking"=dword:00000000

"DisableSuspendCP"=dword:00000000

"DisableWrapperCP"=dword:00000000

В параметре **CredProvAPIURL** задайте адрес приложения credprovapi на сервере Indeed CM.

В параметре **AdminDetails** задайте текст разъяснения для пользователя.

В параметре **DisableServerCertificateChecking** установите значение **0** (значение по умолчанию), если необходимо проводить проверку подлинности сертификата сервера Indeed CM. Установите **1** (dword:00000001), если проверку подлинности проводить не требуется.

В параметре **DisableSuspendCP** установите значение **0** (значение по умолчанию), если в интерфейсе ОС необходимо отображать кнопку "Выключение смарт-карты" или значение **1** (dword:00000001), если кнопку "Выключение смарт-карты" отображать не требуется.

В параметре **DisableWrapperCP** установите значение **0** (значение по умолчанию), если необходимо выполнять разблокировку смарт-карты с использованием стандартного Credential Provider. Установите значение **1** (dword:00000001), если необходимо использовать отдельный Credential Provider.

Ниже приведен пример .reg-файла для сервера Indeed CM с именем машины *certificatemanagerSRV*, включенной проверкой подлинности сертификата сервера, отключенным отображением кнопки "Выключить смарт-карту" и включенной опцией разблокировки смарт-карты в отдельном Credential Provider на экране входа в ОС:

Пример:

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\IndeedCM\Client]

"CredProvAPIURL"="https://certificatemanagerSRV/credprovapi"

"AdminDetails"="Свяжитесь с администратором по внутреннему номеру 1607"

"DisableServerCertificateChecking"=dword:00000000

"DisableSuspendCP"=dword:00000001

"DisableWrapperCP"=dword:00000001

Настройка поддержки устройств Registry

Настройка поддержки устройств Registry через групповые политики

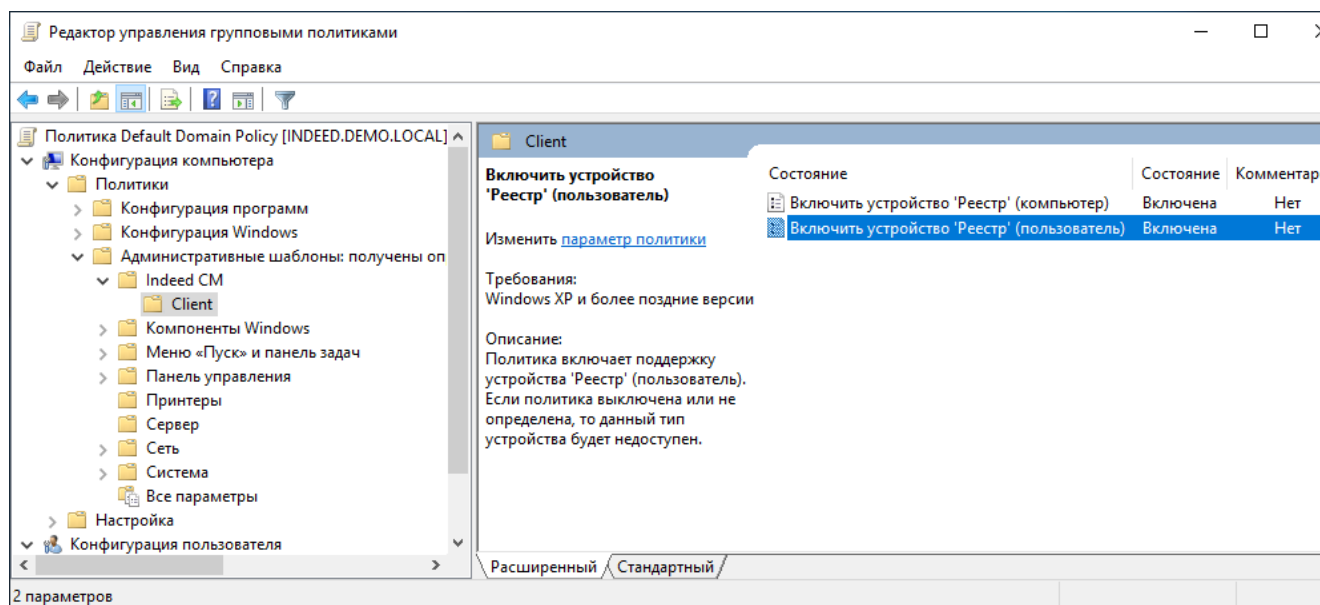
Для включения возможности выпуска устройств Registry с записью сертификатов в локальное хранилище компьютера и/или пользователя через [Сервис самообслуживания](#) (Self Service) настройте соответствующую групповую политику. Эта политика должна распространяться на **рабочие станции пользователей** Indeed CM.

Для добавления административных шаблонов Indeed-Id выполните следующие действия:

1. Скопируйте содержимое каталога **IndeedCM.Client\Misc** в центральное хранилище ADMX-файлов контроллера домена C:
\Windows\SYSVOL\domain\Policies\PolicyDefinitions.

 При использовании локального хранилища ADMX-файлов поместите шаблоны Indeed-Id в **C:\Windows\PolicyDefinitions.**

2. Откройте консоль **Управление групповой политикой** (Group Policy Management).
3. В дереве окна консоли создайте новый объект групповой политики, или выберите существующий.
4. Вызовите контекстное меню и выберите пункт **Изменить** (Edit).
5. В открывшемся **Редакторе управления групповыми политиками** (Group Policy Management Editor) выберите **Конфигурация компьютера** (Computer Configuration) > **Политики** (Policies) > **Административные шаблоны** (Administrative Templates) > **Indeed CM > Client.**
6. Включите политики:
 - **Включить устройство 'Реестр' (компьютер)** (Enable 'Registry' card (Machine)), если требуется выпуск сертификатов в локальное хранилище рабочей станции
 - **Включить устройство 'Реестр' (пользователь)** (Enable 'Registry' card (User)), если требуется выпуск сертификатов в хранилище пользователя



7. Свяжите данный объект политики с группой, членами которой являются рабочие станции пользователей системы Indeed CM.

8. Нажмите **Применить** (Apply) и выполните обновление политик.

Настройка поддержки устройств Registry через реестр

В случае, когда сервер Indeed CM и рабочие станции пользователей находятся вне домена Windows, возможность выпуска устройств Registry необходимо задать в реестре каждой клиентской рабочей станции. Для этого создайте файл реестра (.reg) со следующим содержанием:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\IndeedCM\Client]
"MachineRegistryCardEnabled"=dword:00000000
"UserRegistryCardEnabled"=dword:00000000
```

В параметре **MachineRegistryCardEnabled** установите значение **1** (dword:00000001), если требуется выпуск сертификатов в локальное хранилище рабочей станции.

В параметре **UserRegistryCardEnabled** установите значение **1** (dword:00000001), если требуется выпуск сертификатов в хранилище пользователя рабочей станции.

Ниже приведен пример содержимого .reg-файла с включенной возможностью выпуска устройств Registry компьютера и пользователя:

Пример:

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\IndeedCM\Client]

"MachineRegistryCardEnabled"=dword:00000001

"UserRegistryCardEnabled"=dword:00000001

Настройка браузеров

Выполните настройку браузера, через который будет осуществляться доступ в приложения Indeed Certificate Manager на рабочих станциях Администраторов, Операторов и Пользователей системы.

Internet Explorer, Google Chrome и Microsoft Edge (Chromium)

1. Для работы Google Chrome и Microsoft Edge (Chromium) используются настройки Internet Explorer.
2. Выберите **Свойства браузера** (Internet Options), перейдите на вкладку **Безопасность** (Security), выберите зону **Местная интрасеть** (Local Intranet), нажмите **Сайты (Sites) > Дополнительно** (Advanced).
3. Добавьте узлы:
 - адрес сервера Indeed CM (например, **https://server.demo.local**)
 - адрес для работы через WebSocket **wss://localhost**

Mozilla Firefox

1. Откройте новую вкладку и перейдите по адресу **about:config**.
2. Измените значение параметра *security.enterprise_roots.enabled* на **true** чтобы браузер работал с хранилищем сертификатов рабочей станции, а не браузера.
3. Для работы с использованием протокола TLS 1.2 и проверки подлинности NTLM измените значение параметра *network.http.spdy.enabled.http2* на **false**.

Microsoft Edge (HTML)

1. Выполните настройку аналогичную, как для браузеров Internet Explorer и Google Chrome.
2. Откройте новую вкладку и перейдите по адресу **about:flags**.
3. Включите опцию **Разрешить замыкание на себя для localhost** (Allow localhost loopback).
4. В командной строке, запущенной от имени администратора, выполните команду:

```
CheckNetIsolation LoopbackExempt -a -n="Microsoft.MicrosoftEdge_8wekyb3d8bbwe"
```

Руководство администратора

Взаимодействие операторов и администраторов с Indeed Certificate Manager осуществляется через веб-интерфейс при помощи web-приложения **Консоль управления** (Management Console). Аутентификация в приложение осуществляется в соответствии с выбранной на этапе развертывания системы конфигурацией.

Приложение доступно по адресу **<https://<FQDN сервера Indeed CM>/icm>**

Прежде, чем начать работу в Indeed Certificate Manager, необходимо выполнить следующие действия:

- [настроить привилегии пользователей](#)
- [добавить файл лицензии в систему](#)
- [добавить необходимые типы устройств](#)
- [выполнить настройку политик использования устройств](#)
- [назначить созданные политики на пользователей системы](#)

Процесс предоставления привилегий пользователям, добавления лицензий и типов карт, а также установки необходимых настроек описан в разделе [Конфигурация](#) Консоли управления.

Конфигурация

В данном разделе администраторами Indeed Certificate Manager задаются основные параметры системы:

- [Политики](#)
- [Назначения политик](#)
- [Лицензии](#)
- [Типы устройств](#)
- [Организационная структура](#)
- [Роли](#)
- [Теги](#)
- [Шаблоны печати](#)
- [Журналы учета \(Конфигурация\)](#)
- [Помощь и поддержка](#)

Политики

Создание и редактирование политик использования устройств осуществляется в меню **Политики** в Консоли управления Indeed Certificate Manager.

1. Для создания политики перейдите в меню **Политики** и нажмите **Создать политику**.

 [Создать политику](#)

Создать политику

Имя

Копировать из

Не задано 

СоздатьОтмена

2. Укажите:

- **Имя** – отображаемое имя политики
- **Копировать из** – создание новой политики через копирование параметров ранее созданной

3. Нажмите **Создать**. После создания политики осуществится автоматический переход к её параметрам.

Для удаления политики выберите её в списке и нажмите . Подтвердите действие нажатием кнопки **Удалить**.

 Политику можно удалить только в том случае, если она не используется (т.е. в Indeed CM нет ни одного устройства, выпущенного с применением этой политики).

Названия и описания параметров политик использования устройств.

Группа политик	Описание
Общие	Сведения об имени и области действия политики.

Настройки PKI Microsoft - Удостоверяющие центры - Шаблоны КриптоПро 2.0 - Удостоверяющие центры - Шаблоны Валидата - Удостоверяющие центры - Шаблоны КриптоПро DSS - Серверы - Шаблоны Общие сертификаты Организации	Настройки центров сертификации, шаблонов, параметров использования сертификатов, параметров доступа в операционную систему. Раздел для загрузки файлов PFX, содержимое которых должно записываться на устройства средствами Indeed CM. Параметры организаций пользователей.
Indeed AM	Параметры интеграции с продуктами Indeed Access Manager и Indeed AM Enterprise Single Sign-On.
Secret Net Studio	Параметры интеграции с Secret Net Studio.
СМЭВ	Параметры интеграции с системой межведомственного электронного взаимодействия (СМЭВ) через КриптоПро Шлюз УЦ-СМЭВ.
Поведение	Параметры обращения с устройствами.
Выпуск Инициализация устройства	Настройки выпуска устройств и параметры инициализации.
Аутентификация Секретные вопросы	Параметры аутентификации, создание и изменение секретных вопросов.
Агенты - Контроль - Сообщения пользователю	Параметры Агента Indeed CM.

Принтер смарт-карт • Шаблон устройства	Настройки выпуска и печати на смарт-картах.
Уведомления • Группы получателей • Уведомления администратора • Уведомления пользователя • Шаблоны администратора • Шаблоны пользователя	Настройки почтовых уведомлений о событиях системы. Настройки шаблонов почтовых уведомлений.

Общие параметры

В этом разделе отображается имя политики, которое можно изменить в случае необходимости. Для применения изменений нажмите **Сохранить**.

Настройки PKI

На вкладке **Настройки PKI** настраиваются параметры входа в операционную систему:

- **Импортировать сертификаты УЦ**

Определяет необходимость записи корневого сертификата удостоверяющего центра (или цепочки сертификатов) на устройство в момент выпуска. Такие сертификаты не удаляются с устройства при его изъятии из Indeed Certificate Manager. Если опция включена, то корневые сертификаты или цепочки сертификатов будут записаны на устройство.

 Запись корневого сертификата или цепочки сертификатов может не поддерживаться устройством.

- **Требовать логон по смарт-карте**

Если опция включена, то в параметрах учетной записи пользователя в Active Directory при выпуске устройства будет применена настройка **Для интерактивного входа в сеть нужна смарт-карта** (Smart card is required for interactive logon).

 Сервисная учетная запись для работы с каталогом пользователей (**servicecm**) должна обладать правами на **Запись: userAccountControl** (Write userAccountControl) в Active Directory (см. раздел [Настройка каталога пользователей в Active Directory](#)).

Включение опции в профиле пользователя Active Directory приведет к тому, что его доменный пароль будет изменен на случайный и срок действия этого пароля будет неограничен (см. описание в статье Microsoft [Общее представление об учетных записях пользователей](#)).

Задайте необходимые параметры и нажмите **Сохранить**.

Раздел состоит из следующих пунктов:

- **Microsoft**
 - Удостоверяющие центры
 - Шаблоны

- **КриптоПро 2.0**
 - Удостоверяющие центры
 - Шаблоны
- **Валидата**
 - Удостоверяющие центры
 - Шаблоны
- **КриптоПро DSS**
 - Серверы
 - Шаблоны
- **Общие сертификаты**
- **Организации**

Microsoft

- ✔ Раздел доступен для настройки при активированной опции [Включить интеграцию с Microsoft CA Enterprise](#) в разделе **Microsoft CA** Мастера настройки Indeed CM.

В разделе **Удостоверяющие центры** задаются Microsoft CA, с которыми будет работать Indeed Certificate Manager.

- ℹ Indeed CM поддерживает работу с множеством удостоверяющих центров организации. Вы можете добавить несколько УЦ для одной политики или создать несколько политик, указав для каждой свой удостоверяющий центр.

1. Чтобы добавить удостоверяющий центр, нажмите **Добавить УЦ**.
Удостоверяющие центры

 **Добавить УЦ**

Добавить удостоверяющий центр

Адрес

Укажите учетные данные пользователя для подключения к УЦ

Имя пользователя

Пароль

Сертификат агента регистрации

☐ Выпускать сертификаты для пользователей из внешнего сопоставленного каталога

Добавить **Отмена**

2. Задайте адрес удостоверяющего центра (если он не определился автоматически).
3. Укажите данные сервисной учетной записи (например, **serviceca**), обладающей сертификатом **Агент регистрации** (Enrollment Agent).

 Наличие пользователя с сертификатом **Агент регистрации** (Enrollment Agent) является обязательным условием для работы Indeed CM с УЦ. От имени этого пользователя будет выполняться запрос к указанному удостоверяющему центру на выдачу сертификатов пользователям Indeed CM. Учетные данные этого пользователя могут быть изменены после добавления удостоверяющего центра в Indeed CM (см. раздел [Microsoft CA](#) в Настройке Центров Сертификации для работы с Indeed CM).

4. Нажмите **Добавить**.

Для изменения учетных данных пользователя, обладающего сертификатом **Агент регистрации** (Enrollment Agent), выберите нужный удостоверяющий центр и нажмите   справа от имени пользователя. Для удаления удостоверяющего центра нажмите .

Для добавления удостоверяющего центра, расположенного за пределами домена в котором находятся пользователи Indeed CM (например, в другом независимом домене, который также принадлежит вашей организации) выполните следующие действия:

1. Нажмите **Добавить УЦ**.
2. В поле **Адрес** укажите URL-адрес приложения Indeed CM MSCA Proxy.

 См. раздел [Подключение к центру сертификации Microsoft через IndeedCM MSCA Proxy](#).

В случае развертывания Indeed CM в лесу доменов использование MSCA Proxy не обязательно. В этом случае в поле **Адрес** следует указать имя удостоверяющего центра.

3. Укажите учетную запись пользователя (в формате ДОМЕН\ИМЯ), обладающего сертификатом **Агент регистрации** (Enrollment Agent) на УЦ, расположенном вне домена с каталогом пользователей Indeed CM и её пароль.
4. Включите опцию **Выпускать сертификаты для пользователей из внешнего сопоставленного каталога**.
5. В поле **Путь (LDAP)** укажите путь к каталогу пользователей Indeed CM внешнего домена.

Пример:

Indeed CM развернут в домене *demo.local* и сертификаты пользователям этого домена выпускаются развернутым в этом домене УЦ. При добавлении УЦ, развернутого в домене *external.com*, следует указать путь к каталогу пользователей в этом домене, где у пользователей системы Indeed CM есть еще одна доменная учетная запись и на имя которой добавляемый УЦ будет выпускать сертификаты.

Таким образом, для одного сотрудника, имеющего учетные записи в независимых доменах, система позволит записать на одно устройство несколько сертификатов, выданных удостоверяющими центрами, расположенными в независимых доменах.

 Выпуск сертификатов для пользователей внешнего каталога будет успешен только при совпадении атрибута соответствия с основным каталогом пользователей.

Например: адрес электронной почты, указанный в свойствах учетной записи пользователя в домене *demo.local* должен совпадать с адресом электронной почты, указанным в свойствах учетной записи пользователя в домене *external.com*.

6. В поле **Имя пользователя** укажите в формате ДОМЕН\ИМЯ учетную запись, обладающую правами на чтение всех свойств пользователей во внешнем домене. Для этого можно использовать учетную запись, указанную в п.3.

 Для настройки разрешения на чтение только необходимого набора свойств обратитесь к разделу [Настройка каталога пользователей в Active Directory](#).

7. В поле **Атрибут сопоставления каталогов** укажите атрибут (Общее имя (CN), E-mail или Логин (sAMAccountName)), по которому Indeed CM будет определять уникальность пользователя, для которого созданы учетные записи в каждом домене. Пример настроек для внешнего Microsoft CA с опцией выпуска сертификатов для пользователей сопоставленного каталога.

Добавить удостоверяющий центр

Адрес

https://servercm.external.com/mscaproxy

Укажите учетные данные пользователя для подключения к УЦ

Имя пользователя

EXTERNAL\Service

Пароль

.....

Сертификат агента регистрации

Service ▼

☒ Выпускать сертификаты для пользователей из внешнего сопоставленного каталога

Путь (LDAP)

LDAP://EXTERNAL.COM/DC=EXTERNAL,DC=COM

Имя пользователя

EXTERNAL\Service

Пароль

.....

Атрибут сопоставления каталогов

Общее имя ▼

Добавить

Отмена

В разделе **Шаблоны** задаются шаблоны, в соответствии с которыми будут выпускаться сертификаты пользователям.

⚠ Прежде, чем приступить к созданию шаблонов сертификатов в Indeed CM, убедитесь в том, что необходимые шаблоны настроены и добавлены в центр сертификации Microsoft CA. См. разделы [Настройка шаблонов сертификатов](#) и [Добавление шаблонов сертификатов](#).

- Для создания шаблона сертификата нажмите **Создать шаблон сертификата**.
- Задайте необходимые [Параметры шаблона сертификата](#).
- Нажмите **Создать**.

Шаблоны сертификатов

[+ Создать шаблон сертификата](#)

Имя	УЦ	Шаблон сертификата УЦ Microsoft	
Вход по смарт-карте	demo-DC-CA	Indeed Smart Card Logon	
Пользователь со смарт-картой	demo-DC-CA	Indeed Smart Card User	

 Indeed CM позволяет создать множество разных шаблонов сертификатов для одной политики (при условии, что эти шаблоны не повторяются). Просмотреть список созданных шаблонов можно в разделе **Шаблоны** выбранной политики.

Для редактирования шаблона выберите его и нажмите . Для удаления шаблона из политики нажмите .

КриптоПро 2.0

- ✓ Раздел содержит параметры работы с удостоверяющими центрами КриптоПро 2.0 и доступен для настройки при активированной опции [Включить интеграцию с КриптоПро УЦ 2.0](#) в разделе **КриптоПро УЦ 2.0** Мастера настройки Indeed CM.

В разделе **Удостоверяющие центры** задаются УЦ КриптоПро версии 2.0, с которыми будет работать Indeed Certificate Manager.

1. Нажмите **Добавить УЦ**, чтобы добавить удостоверяющий центр:

Удостоверяющие центры

[+ Добавить УЦ](#)

Добавить удостоверяющий центр

URL-адрес веб-службы ЦР

Имя ЦС

URL-адрес прокси-сервера

Выберите сертификат, который будет использоваться для подключения к УЦ КриптоПро

Клиентский сертификат

- ☒ Устанавливать привязку между пользователем УЦ и пользователем каталога
 - ☒ Устанавливать привязку автоматически
 - ☒ Создавать пользователя УЦ, если он не существует

Папка: [Центр Регистрации/Пользователи](#)

- ☒ Обновлять учетные данные пользователя УЦ

2. Введите **URL-адрес веб-службы Центра Регистрации**, в полном или сокращенном виде:

```
https://<host_name>/ra/RegAuthLegacyService.svc  
https://<host_name>/ra
```

Если для соединения с удостоверяющим центром используется прокси-сервер, укажите его параметры (имя сервера и порт) в поле **URL-адрес прокси-сервера**.

Пример:

```
http://proxy.company.com:8080
```

Если на рабочей станции развернута только одна роль Центра Сертификации (ЦС), то поле **Имя ЦС** можно оставить пустым (имя будет определено автоматически), если ролей ЦС несколько, задайте имя того ЦС, к которому необходимо подключиться.

3. Укажите имя пользователя, обладающего сертификатом **Indeed CM Service User** (см. раздел [Создание сервисной учетной записи для работы с КриптоПро УЦ 2.0](#)).

4. Установите связь между пользователями удостоверяющего центра КриптоПро и пользователями каталога, если это требуется (опция **Устанавливать привязку между пользователем УЦ и пользователем каталога**). Устанавливать связь между пользователями каталога и пользователями УЦ необходимо, если каталог пользователей системы Indeed CM не является каталогом пользователей УЦ. Такая ситуация может быть в следующих сценариях использования:

- Indeed CM работает с пользователями домена Windows, запрашивая для них сертификаты КриптоПро УЦ, который имеет свой каталог пользователей, не связанный с Active Directory.
- Indeed CM работает с пользователями КриптоПро УЦ, но таким пользователям необходимо кроме сертификатов «своего» УЦ выдавать еще и сертификаты одного или нескольких других удостоверяющих центров.

Indeed CM позволяет определять следующие параметры работы с УЦ, если опция **Устанавливать привязку между пользователем УЦ и пользователем каталога** включена:

- **Устанавливать привязку автоматически** (если каталог УЦ содержит пользователя, для которого будет выпущено устройство).
- **Создавать пользователя УЦ, если он не существует** (если каталог УЦ не содержит пользователя, для которого будет выпущено устройство с сертификатом). По умолчанию пользователи будут создаваться в корневом каталоге Центра Регистрации (папка "Центр Регистрации"). Для создания пользователей во вложенных папках укажите имя папки.

Indeed CM может обновлять данные ранее созданных пользователей КристоПро УЦ 2.0 при выпуске или обновлении устройства. Например, изменять email, если он изменился в профиле пользователя в Active Directory. Включите опцию **Обновлять учетные данные пользователя УЦ**, если обновление данных необходимо.

 Для обновления данных должна быть установлена привязка пользователя Active Directory к пользователю Центра Регистрации. Если привязка не установлена, то в каталоге ЦР будет создан новый пользователь.

5. Нажмите **Добавить**.

Indeed CM поддерживает работу с множеством удостоверяющих центров организации. Вы можете добавить несколько УЦ для одной политики или создать несколько политик, указав для каждой свой удостоверяющий центр.

В разделе **Шаблоны** задаются шаблоны, в соответствии с которыми будут выпускаться сертификаты пользователям.

- Для создания шаблона нажмите **Создать шаблон сертификата**.
- Задайте необходимые [Параметры шаблона сертификата](#).
- Нажмите **Создать**.

Для редактирования шаблона выберите его и нажмите . Для удаления шаблона из политики нажмите .

Валидата

- ✔ Раздел содержит параметры работы с удостоверяющими центрами Валидата и доступен для настройки при активированной опции [Включить интеграцию с Валидата УЦ](#) в разделе **Валидата УЦ** Мастера настройки Indeed CM.

В разделе **Удостоверяющие центры** задаются Валидата УЦ, с которыми будет работать Indeed Certificate Manager в online- и/или offline-режимах.

- ℹ Indeed CM поддерживает работу с множеством удостоверяющих центров организации. Вы можете добавить несколько УЦ для одной политики или создать несколько политик, указав для каждой свой удостоверяющий центр.

Online-режим работы

- ⚠ В Online-режиме Indeed CM заменяет собой АРМ Оператора ЦР Валидата. Для работы в данном режиме необходимо **Разрешить удаленное подключение к сервису** в настройках Центра Регистрации.

1. Нажмите **Добавить УЦ**, чтобы добавить удостоверяющий центр:

Удостоверяющие центры

+ Добавить УЦ

Добавить удостоверяющий центр

Адрес сервера ЦР

ncacn_ip_tcp:192.168.0.15[13434]

Выберите сертификат, который будет использоваться для подключения к ЦР Валидата

Клиентский сертификат

Operator VD

Каталог для обмена файлами с ЦР/ЦС

\\Validatara\PKI

Укажите учетные данные пользователя для подключения к каталогу

Имя пользователя

Validatara\Operator VD

Пароль

.....

Подкаталог для запросов

requests

Подкаталог для сертификатов

certificates

Добавить

Отмена

2. В поле **Адрес сервера ЦР** укажите адрес и порт RPC сервера Центра Регистрации:

ncacn_ip_tcp:<ip>[<port>]

3. Выберите **Клиентский сертификат** - сертификат Оператора Центра Регистрации.

 Данный сертификат используется как при подключении к сервису ЦР для выполнения аутентификации по протоколу TLS, так и для подписания XML шаблона на получение или отзыв сертификата ключа проверки ЭП пользователя и должен содержать OID Оператор Центра Регистрации (1.3.6.1.4.1.10244.6.1) и OID Проверка подлинности TLS клиента (1.3.6.1.5.5.7.3.2).

4. Укажите **Каталог для обмена файлами с ЦР/ЦС** - каталог для обмена файлами Indeed CM с Центром Регистрации.

 В каталоге должны присутствовать цепочка сертификатов Валидата УЦ и актуальный список отозванных сертификатов X.509 (CRL или СОС).

5. В полях **Имя пользователя** и **Пароль** укажите учетные данные пользователя для подключения к выбранному каталогу.

- Укажите **Подкаталог для запросов** - подкаталог запросов для Центра Сертификации, обработанных Оператором ЦР (в формате CMS/PKCS#7).
- Укажите **Подкаталог для сертификатов** - подкаталог сертификатов, обработанных Центром Сертификации (в формате CMS/PKCS#7).

6. Нажмите **Добавить**.

Offline-режим работы

1. Нажмите **Добавить УЦ**, чтобы добавить удостоверяющий центр:

 **Добавить УЦ**

Добавить удостоверяющий центр

Адрес сервера ЦР

Выберите сертификат, который будет использоваться для подключения к ЦР Валидата

Клиентский сертификат

Каталог для обмена файлами с ЦР/ЦС

Укажите учетные данные пользователя для подключения к каталогу

Имя пользователя

Пароль

Подкаталог для запросов

Подкаталог для сертификатов

Добавить **Отмена**

2. Укажите **Каталог для обмена файлами с ЦР/ЦС** - каталог для обмена файлами Indeed CM с Центром Регистрации.



В каталоге должны присутствовать цепочка сертификатов Валидата УЦ и актуальный список отозванных сертификатов X.509 (CRL или СОС).

3. В полях **Имя пользователя** и **Пароль** укажите учетные данные пользователя для подключения к выбранному каталогу.

- Укажите **Подкаталог для запросов** - подкаталог для входящих незащищённых запросов пользователей (в формате PKCS#10).

 Обработка запросов в формате PKCS#10 может быть выполнена исключительно в ручном режиме на АРМ Администратора ЦР.

- Укажите **Подкаталог для сертификатов** - подкаталог сертификатов для выдачи конечным пользователям.

4. Нажмите **Добавить**.

В разделе **Шаблоны** задаются шаблоны, в соответствии с которыми будут выпускаться сертификаты пользователям.

- Для создания шаблона нажмите **Создать шаблон сертификата**.
- Загрузите **Подготовленный XML шаблон сертификата**.
- Задайте необходимые **Параметры шаблона сертификата**.
- Нажмите **Создать**.

Для редактирования шаблона выберите его и нажмите . Для удаления шаблона из политики нажмите .

КриптоПро DSS



Раздел содержит параметры работы с ПАК "КриптоПро DSS" и доступен для настройки при активированной опции [Включить интеграцию с КриптоПро DSS](#) в разделе **КриптоПро DSS** Мастера настройки Indeed CM.

В разделе **Серверы** задаются серверы DSS, с которыми будет работать Indeed Certificate Manager.

1. Нажмите **Добавить сервер**, чтобы добавить удостоверяющий центр.

 Добавить сервер

Добавить сервер

Имя

КриптоПро DSS

URL-адрес веб-службы СЭП

https://stenddss.cryptopro.ru/dss

URL-адрес веб-службы ЦИ

https://stenddss.cryptopro.ru:4430/idp

URL-адрес прокси-сервера

Идентификатор клиента OAuth

indeed

Адрес возврата

Пожалуйста, выберите сертификат, который будет использоваться для подключения к КриптоПро DSS

Клиентский сертификат

Оператор DSS



- ☒ Устанавливать привязку между пользователем DSS и пользователем каталога
 - ☒ Устанавливать привязку автоматически
 - ☒ Создавать пользователя DSS, если он не существует
 - ☒ Обновлять учетные данные пользователя DSS

Добавить

Отмена

2. Укажите параметры подключения:

- **Имя** - произвольное имя добавляемого сервера.
- **URL-адрес веб-службы СЭП** - адрес службы электронной подписи DSS.
- **URL-адрес веб-службы ЦИ** - адрес центра идентификации DSS.
- **URL-адрес прокси-сервера** - если для соединения с сервером DSS используется прокси сервер, укажите его параметры (имя сервера и порт).

Пример:

`https://proxy.company.com:8080`

- **Идентификатор клиента OAuth** - клиентский идентификатор (client_id) для взаимодействия через API.
- **Адрес возврата** - укажите адрес возврата (redirect_uri), если он отличается от дефолтного значения.
- **Клиентский сертификат** - сертификат оператора DSS.

3. Задайте опции:

- **Устанавливать привязку между пользователем DSS и пользователем каталога** - если опция включена, то при выпуске устройства пользователь каталога будет связан с пользователем DSS.
 - **Устанавливать привязку автоматически** - если опция включена, то пользователь каталога будет автоматически привязан к пользователю DSS.
 - **Создавать пользователя DSS, если он не существует** - если опция включена, то будет создан пользователь.
 - **Обновлять учётные данные пользователя DSS** - если опция включена, то при обновлении или выпуске устройства будут обновлены данные пользователя DSS.

4. Заполните поля и нажмите **Добавить**.

В разделе **Шаблоны** задаются шаблоны, в соответствии с которыми будут выпускаться сертификаты пользователям.

- Для создания шаблона нажмите **Создать шаблон сертификата**.
- Задайте необходимые **Параметры шаблона сертификата**.
- Нажмите **Создать**.

Для редактирования шаблона выберите его и нажмите . Для удаления шаблона из политики нажмите .

Параметры шаблонов сертификатов

В разделе приведено описание настроек шаблонов сертификатов всех поддерживаемых в Indeed CM удостоверяющих центров.

Настройки шаблонов сертификатов в Indeed Certificate Manager.

Параметр	Описание	MSCA	КП2.0	Валидата (Online-/Offline-режим)	DSS
Имя	Имя шаблона сертификата.	+	+	+	+
Сервер	Имя сервера DSS.	-	-	-	+
УЦ	Имя удостоверяющего центра.	+	+	+	+
Шаблон сертификата УЦ	Загружается из выбранного удостоверяющего центра.	+	+	+	+
Префикс имени ключа	Если префикс не задан, то имя контейнера, содержащего ключевую пару, будет сформировано случайным образом. Если указан префикс, то он добавится перед именем контейнера. Значение префикса отображается в Indeed CM (имя контейнера в разделе СКЗИ) и в стороннем ПО для работы с контейнерами закрытого ключа (КриптоПро CSP, клиенты устройств и пр.). Имя контейнера с префиксом может не поддерживаться устройством.	+	+	+	-

Включить в имя субъекта	Укажите атрибуты для формирования имени субъекта (Subject) сертификата: • Полное различающееся имя (значение по умолчанию) • Общее имя(CN) • Имя • Фамилия • Инициалы • E-mail • Должность • Подразделение • Организация • Адрес • Город • Область • Страна  Для формирования имени субъекта (Subject) и альтернативного имени субъекта (Subject Alternative Name) сертификата из списка атрибутов в свойствах шаблона Microsoft CA на вкладке Имя субъекта (Subject Name) укажите Предоставляется в запросе (Supply in the request).	+	-	-	-
Включить в альтернативное имя субъекта	Укажите атрибуты для формирования альтернативного имени субъекта (Subject Alternative Name) сертификата: • E-mail • Дополнительные e-mail адреса • UPN-имя пользователя  Атрибут пользователя Active Directory, из которого вычитываются дополнительные e-mail адреса, указывается в разделе Microsoft CA Мастера настройки Indeed CM. Атрибут по умолчанию: proxyAddresses.	+	-	-	-

Выпускать сертификат на указанного пользователя	Если опция включена, то в свойствах шаблона отобразится поле поиска пользователя в каталоге ЦР КриптоПро УЦ, на которого будут выпускаться сертификаты.  Опция доступна при включении Разрешить выпуск сертификатов на имя общей учетной записи в разделе КриптоПро УЦ 2.0 Мастера настройки Indeed CM. Изменить значение опции при редактировании шаблона нельзя.	-	+	-	-
Использовать аппаратную криптографию, если поддерживается	Если опция включена, то при выпуске сертификата ключевая пара будет создаваться с использованием криптографических алгоритмов, поддерживаемых устройством. Если устройство не поддерживает аппаратную криптографию, то будет использоваться КриптоПро CSP, установленный на рабочей станции, к которой подключено устройство. Изменить значение опции при редактировании шаблона нельзя.	-	+	+	-
Создать резервную копию ключа	Если опция включена, то в этом случае при генерации ключевой пары на смарт-карте будет применена опция её архивации. Это значит, что ключевая пара будет сгенерирована на смарт-карте и ее копия (открытый и закрытый ключи) будут отправлены на сервер Indeed CM и затем в хранилище системы. Архивация ключевой пары возможна только один раз. Если опция выключена, то ключевая пара сразу генерируется на устройстве.	+	+	+	-
Записывать копию ключа при временной замене устройства	Если опция включена, то копии сертификатов и закрытых ключей будут записаны на временное устройство при замене, как и в случае с постоянной заменой. Если опция отключена, то копии сертификатов и закрытых ключей не будут записаны на временное устройство при замене.	+	+	+	-
Использовать ключи повторно	Если опция включена, то при обновлении сертификатов, записанных на устройство, существующий ключ шифрования будет использован повторно.	+	-	-	-

Импортировать сертификат, если существует	Если опция включена, то система будет искать существующие сертификаты на устройстве (для указанного пользователя, УЦ и шаблона) и использовать их, не создавая новых ключей. Импорт сертификата невозможен, если устройство будет инициализировано перед выпуском.	+	+	+	+
Не удалять сертификат при обновлении /очистке устройства	Если опция включена, то при обновлении или очистке устройства истекающий/истекший сертификат не будет удален с устройства и отозван на УЦ. В процессе обновления будет запрошен новый сертификат с новым закрытым ключом и записан на устройство.  Для шаблона сертификата MSCA: Если включена опция Использовать ключи повторно, то при обновлении устройства истекающий/истекший сертификат будет удален с устройства. На устройство будет запрошен и записан новый сертификат со старым закрытым ключом. Истекающий/истекший сертификат будет удален, если устройство изъято с инициализацией.	+	+	+	-
Отзывать сертификат при отзыве или выключении устройства	Если опция включена, то сертификаты пользователя будут отозваны при выключении или отзыве устройства. Если опция выключена, то при выключении или отзыве устройства сертификаты не будут отозваны.	+	+	+	+
Устанавливать сертификат в локальное хранилище	Если опция включена, то при выпуске (обновлении) устройства через Self Service записанные на него сертификаты добавятся в локальное хранилище пользователя на рабочей станции.	+	+	+	-

Публиковать сертификат в каталоге пользователей	Если опция включена, то выпущенный сертификат опубликуется в профиле пользователя в Active Directory на вкладке Опубликованные сертификаты (Published Certificates). Сертификат удалится из профиля при включении опции Удалять опубликованный сертификат при отзыве устройства.  Необходимо наличие прав на Запись: userCertificate (Write userCertificate) для сервисной учетной записи для работы с каталогом пользователей Active Directory.				
Публиковать сертификат в ЕСИА	Если опция включена, то выпущенный квалифицированный сертификат будет зарегистрирован в Единой системе идентификации и аутентификации (ЕСИА).  Опция доступна при включении Интеграция со СМЭВ в разделе Общие функции Мастера настройки Indeed CM.				
Публиковать сертификат в файловое хранилище	Если опция включена, то выпущенный сертификат будет помещен в сетевое хранилище (папку). При отзыве устройства сертификаты из хранилища не удаляются.  Опция доступна при включении Публикация сертификатов в файловое хранилище в разделе Общие функции Мастера настройки Indeed CM.				

Публиковать сертификат в ЦФТ	Если опция включена, то выпущенный сертификат будет помещен в базу приложений ЦФТ. При отзыве устройства сертификаты из базы приложений ЦФТ не удаляются.  Опция доступна при включении Публиковать сертификаты пользователей КриптоПро УЦ 2.0 в базе приложений ЦФТ в разделе КриптоПро УЦ 2.0 Мастера настройки Indeed CM.	-	+	-	-
Публиковать список отозванных сертификатов	Если опция включена, то при выключении, включении и отзыве устройств будет выполняться внеочередная публикация списка отозванных сертификатов (CRL).	+	+	-	-
Использовать комментарий устройства в качестве комментария пользователя к запросу на сертификат	Если опция включена, то в поле "Заметки пользователя" запроса сертификата будет добавлен текст комментария устройства.	-	+	-	-
Автоматически одобрять запрос на сертификат	Если опция включена, то запросы на сертификат будут автоматически одобрены. Если опция выключена, то для завершения выпуска потребуется дождаться одобрения запроса на УЦ или отменить выпуск, если запрос будет отклонен.	+	+	-	+
Автоматически одобрять подписанный запрос на обновление сертификата	Если опция включена, то запрос на обновление сертификата будет одобрен автоматически. Если опция выключена, то для обновления сертификата потребуется дождаться одобрения запроса на УЦ.	+	+	-	-

Отслеживаемые атрибуты пользователя	Укажите атрибуты пользователя при изменении которых необходимо обновление сертификата: - Общее имя(CN) - E-mail - UPN-имя пользователя  Изменение E-mail приводит к обновлению сертификата в случае, если этот атрибут включен в свойствах шаблона сертификата в Microsoft CA на вкладке Имя субъекта (Subject Name) опции Включить имя электронной почты в имя субъекта (Include e-mail name in subject name) и Имя электронной почты (E-mail name).  Дополнительный список отслеживаемых атрибутов пользователей задается в разделе Обновляемые атрибуты Мастера настройки Indeed CM.				
Шаблон печати запроса на сертификат	Если параметр: Не задано, то используется стандартный шаблон печати запроса на сертификат. Если в систему добавлены Шаблоны печати запроса сертификата, то выберите шаблон из выпадающего меню.				
Шаблон печати сертификата	Если параметр: Не задано, то используется стандартный шаблон печати сертификата. Если в систему добавлены Шаблоны печати сертификата, то выберите шаблон из выпадающего меню.				
Шаблон печати запроса на отзыв сертификата	Если параметр: Не задано, то используется стандартный шаблон печати запроса на отзыв сертификата. Если в систему добавлены Шаблоны печати запроса на отзыв сертификата, то выберите шаблон из выпадающего меню.				
Использовать по умолчанию	Если опция включена, то сертификат отмечается как используемый по умолчанию для входа в операционную систему Windows XP.				
Период обновления (дней)	Период времени, в течение которого сертификат и закрытый ключ можно обновить. Значение по умолчанию – 30 дней.				

Необязательный сертификат	Если опция включена, то при выпуске устройства появится возможность выбора сертификатов для записи из числа отмеченных, как необязательные. Если опция выключена, то сертификат считается обязательным для записи на устройство.				

Общие сертификаты

Общие сертификаты используются в сценарии, когда уже выпущенный вне системы Indeed Certificate Manager сертификат и закрытый ключ необходимо записать на устройства множества пользователей средствами Indeed CM.

Особенности работы системы с общими сертификатами:

- Поддерживаются сертификаты с ключами RSA и ГОСТ.
- Для записи ГОСТ-сертификатов требуется наличие КриптоПро CSP на сервере Indeed CM и рабочей станции, к которой подключено устройство.
- Общие сертификаты не могут быть приостановлены и отозваны, обновление возможно через удаление старого PFX и добавление нового.
- Общие сертификаты не публикуются в Active Directory, файловое хранилище и базу приложений ЦФТ, не помещаются средствами Indeed CM в хранилище сертификатов пользователя.
- Отправка почтовых уведомлений для события **Общие сертификаты истекают** задает ся в пункте [Уведомления администратора](#). Рассылка происходит при достижении 10% до окончания срока действия сертификата. Для истекших сертификатов уведомления перестают отправляться.



Уведомление доступно только для администраторов, так как оно привязано к политике выпуска устройств, а не к самому устройству.

Для добавления общего сертификата в политику использования устройств выберите файл PFX, укажите пароль для доступа к содержимому файла и нажмите **Добавить**. При включении опции **Необязательный сертификат** общий сертификат будет предлагаться к выбору для записи на устройство при его выпуске или обновлении. При отключенной опции сертификат будет записан на устройство без предоставления возможности выбора.

Организации

- ✔ Настройка доступна при включении опции [Использовать настраиваемый перечень организаций пользователя для выпуска сертификатов](#) в разделе КристоПро УЦ 2.0 Мастера настройки Indeed CM.

При создании пользователя в Центре Регистрации КристоПро УЦ 2.0 Indeed Certificate Manager использует данные из профиля пользователя Active Directory. Если в Active Directory отсутствует полная информация об организации пользователя (например: ОГРН, ИНН, полный адрес), то она может быть загружена из шаблона организации, настраиваемого в политике использования устройств Indeed CM.

Нажмите **Добавить организацию**, заполните необходимые поля и нажмите **Добавить**.

Организации

[+ Добавить организацию](#)

Добавить организацию

Имя	
Общее имя	
Страна	
Область	
Город	
Адрес	
ОГРН	
ИНН	

Добавленные организации будут доступны администратору или оператору Indeed CM при выпуске карты пользователю, которого еще нет в каталоге Центра Регистрации КriptoПро УЦ 2.0. После выпуска устройства в каталоге ЦР будет создан пользователь, профиль которого будет заполнен данными из Active Directory (Общее имя, Фамилия, Имя, Отчество, Email) и данными организации, выбранной из списка. При изменении данных в шаблоне организации данные в каталоге Центра Регистрации будут обновлены при следующем выпуске устройства. Для ранее созданных в каталоге ЦР пользователей данные по организации обновятся после обновления содержимого устройства.

Indeed AM



Настройка доступна при включении опции [Интеграция с Indeed Access Manager](#) в разделе **Общие функции** Мастера настройки Indeed CM.

Indeed Certificate Manager может быть интегрирован с продуктами компании Индид – Indeed Access Manager и Indeed AM Enterprise Single Sign-On. Интеграция позволит объединить операции выпуска устройства, запроса сертификата, записи сертификата и регистрации аутентификатора в единый процесс.

Выпущенное подобным образом устройство может быть использовано пользователем как для аутентификации в домене и SSO-приложениях, так и для цифровой подписи или доступа к ресурсам, требующих наличие персональных сертификатов. Интеграция между системами возможна на любом этапе, независимо от того, какой из продуктов был развернут раньше.

Настройка интеграции систем Indeed CM и Indeed AM состоит из двух этапов:

- Установка и настройка необходимого ПО
- Конфигурирование параметров интеграции

На первом этапе необходимо выполнить установку следующих компонентов:

- **Indeed Administration Tools** (или Indeed Admin Pack) на каждый сервер Indeed CM
- **Indeed Extended Security Provider** на каждый сервер Indeed AM
- **Indeed SmartCard + PIN Provider** на каждый сервер Indeed AM



Indeed Administration Tools поставляется в дистрибутиве системы Indeed Access Manager.

Indeed Extended Security Provider и **Indeed SmartCard + PIN Provider** поставляется по запросу [службой технической поддержки компании Indeed Identity](#).

А также выполнить настройку Extended Security Provider:

- Создать группу безопасности Indeed-ID Enrollment Admins согласно Руководству по установке и эксплуатации Indeed Extended Security Provider.
- Добавить сервисную учетную запись (**'servicecm'**) в группы безопасности Indeed-ID User Admins и Indeed-ID Enrollment Admins.

На втором этапе необходимо задать параметры интеграции в политике использования устройств в Indeed Certificate Manager. Перейдите в раздел **Indeed AM** в конфигурации выбранной политики и определите параметры работы с Indeed AM.

Параметры интеграции с Indeed AM.

Параметр	Описание
Включить интеграцию с Indeed AM	Если опция включена, то при выпуске устройства в системе Indeed CM будет выпускаться и аутентификатор «Смарт-карта или USB-ключ + PIN» в системе Indeed AM.
Использовать прокси-сервер Indeed AM	Если опция включена, то Indeed CM будет обращаться к прокси-серверу Indeed AM, который направит запрос на серверы Indeed AM. Использование прокси-сервера необходимо, если серверы Indeed CM располагаются за пределами домена, в котором установлена система Indeed AM.
URL-адрес прокси-сервера	Адрес, по которому доступен Indeed AM Proxy Server.
Имя пользователя Пароль	Учетные данные пользователя (логин и доменный пароль), входящего в группы безопасности Indeed-ID User Admins и Indeed-ID Enrollment Admins.
Разрешить использование Indeed AM Windows Logon	Если опция включена, то при выпуске устройства в Indeed CM пользователю будет разрешено использование технологии Indeed для аутентификации в домене при помощи компонента Indeed AM Windows Logon.
Разрешить использование Indeed AM Enterprise Single Sign-On	Если опция включена, то при выпуске устройства в Indeed CM пользователю будет разрешено использование технологии Indeed для аутентификации в приложениях при помощи компонента Indeed AM Enterprise SSO Agent.
Генерировать случайный пароль учетной записи Windows	Если опция включена, то при выпуске устройства в Indeed CM для пользователя будет установлена опция генерации случайного доменного пароля. В этом случае при истечении срока действия пароля новый пароль будет сгенерирован случайным образом и будет известен только системе Indeed AM.

Разрешения на использование Indeed AM Windows Logon, Indeed AM Enterprise Single Sign-On и генерацию случайного пароля будут выключены в случае удаления последнего зарегистрированного аутентификатора пользователя.

Например:

Если у пользователя не было ни одного аутентификатора в системе Indeed AM и ни одного устройства в системе Indeed CM, то после выпуска устройства с настроенными параметрами интеграции у пользователя появится один аутентификатор («Смарт-карта или USB-ключ + PIN») в системе Indeed AM и одно устройство (например, eToken) в системе Indeed CM.

В случае удаления устройства в Indeed CM, удалится и аутентификатор в Indeed AM, а если других обученных аутентификаторов нет, отключатся и разрешения на использование Indeed AM Windows Logon, Indeed AM Enterprise Single Sign-On и генерация случайного пароля (если хотя бы одна из этих опций была активна на момент отзыва).

Secret Net Studio



Настройка доступна при включении опции **Интеграция с Secret Net Studio** в разделе **Общие функции** Мастера настройки Indeed CM.

Indeed Certificate Manager может быть интегрирован с продуктом компании "Код безопасности" - Secret Net Studio (SNS) версий 8.4, 8.5 и 8.6.

Интеграция позволяет:

- при выпуске/замене в Indeed CM устройства добавлять его в базу данных SNS
- при отзыве у пользователя в Indeed CM удалять устройство из БД SNS



- Для уже выпущенных устройств в Indeed CM интеграция устанавливается через операцию обновления.
- При замене в Indeed CM, если заменяемое устройство уже добавлено в БД SNS.
- Запись создается только для известных SNS устройств.

Для интеграции Indeed CM с Secret Net Studio потребуется:

1. Установить "SNS клиент" версии **8.4.2863** с патчем **8_4_2863_106_Inc85078_Build80**, **8.5.5329** с патчем **8_5_5329_64_Inc85077_Build43** или **8.6.8330.0** с базовой функциональностью на сервер Indeed CM (требуется для подключения к БД SNS).
2. Установить "SNS клиент" версии **8.4.2863** с патчем **8_4_2863_106_Inc85078_Build80**, **8.5.5329** с патчем **8_5_5329_64_Inc85077_Build43** или **8.6.8330.0** на клиентские рабочие станции, с которых будут выпускаться устройства.



Патчи **8_4_2863_106_Inc85078_Build80** и **8_5_5329_64_Inc85077_Build43** предоставляются по запросу [службой технической поддержки компании "Код безопасности"](#).

3. **Включить интеграцию с Secret Net Studio** в политике, указав учетную запись, входящую в группу администраторов безопасности SNS.

Secret Net Studio

☒ Включить интеграцию с Secret Net Studio

Укажите учетные данные администратора безопасности

Имя пользователя

Administrator_SNS

Пароль

.....

☐ Включить режим хранения пароля пользователя

Сохранить



Если опция **Включить режим хранения пароля пользователя** задана, то при выпуске устройства в Indeed CM на него будет записан идентификатор SNS с включенным режимом хранения доменного пароля пользователя.

СМЭВ

- ✔ Настройка доступна при включении опции **Интеграция со СМЭВ** в разделе **Общие функции** Мастера настройки Indeed CM.

Indeed Certificate Manager может быть интегрирован с системой межведомственного электронного взаимодействия (СМЭВ) через КриптоПро Шлюз УЦ-СМЭВ версии 1.0.7374.2300 и выше. Интеграция позволит объединить операции выпуска /обновления устройства, проверки данных пользователя в СМЭВ, запроса сертификата, регистрации сертификата в единой системе идентификации и аутентификации (ЕСИА) и записи его на устройство в единый процесс.

Для настройки интеграции выполните следующие действия:

1. **Включите интеграцию со СМЭВ.**
2. Укажите **URL-адрес шлюза КриптоПро СМЭВ.**
3. Выберите **Сертификат оператора шлюза СМЭВ.**

СМЭВ

☒ Включить интеграцию со СМЭВ

URL-адрес шлюза КриптоПро СМЭВ

Сертификат оператора шлюза СМЭВ

Сохранить

- ⚠ Сертификат оператора шлюза КриптоПро и его контейнер закрытого ключа должен быть установлен в локальное хранилище сертификатов сервера Indeed CM.

4. Нажмите **Сохранить**.

Поведение

В данном разделе задаются настройки, определяющие доступные операции для администраторов\операторов в консоли управления и для пользователей в сервисе самообслуживания в рамках политики использования устройств.

Опция	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	Позволяет разблокировать устройство пользователя при помощи администратора системы в случае, когда соединение между рабочей станцией пользователя и сервером Indeed CM отсутствует. 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 Проверять ответы на секретные вопросы).	Включена
Разрешить отмену обновления устройства	Позволяет администратору или оператору Indeed CM 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 Добавлять устройство автоматически .	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 Изъятие устройства и Обновление устройства . 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 Сервис самообслуживания (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 Сервис самообслуживания (Self Service). Выпуск карт AirKey возможен только при настроенной интеграции с Indeed AirKey Enterprise (см. установка и настройка 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 отзываться 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 Self Service 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 Self Service. 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
Включить отслеживание сертификатов	Если опция включена, то при выпуске устройства Indeed CM выполнит поиск имеющихся на устройстве сертификатов и соответствующих им закрытых ключей. Поддерживается отслеживание сертификатов, выпущенных удостоверяющими центрами: ○ Microsoft CA ○ КriptoПро УЦ 2.0 ○ ViPNet УЦ 4 ○ Валидата УЦ При скором истечении срока действия таких сертификатов Indeed CM может рассылать соответствующие почтовые уведомления (Отслеживаемые сертификаты истекают) Администраторам и Пользователям системы. В Консоли управления и в приложении Self Service имеется возможность распечатать отслеживаемые сертификаты по стандартному шаблону печати сертификата, используемому в системе.	Отключена

Выпуск

В данном разделе задаются параметры выпуска устройства и параметры его инициализации.

Настройки выпуска устройства.

Опция	Описание
Максимальное количество устройств у пользователя	Число, ограничивающее количество устройств у пользователя. Значение по умолчанию – 1.
Инициализировать устройство	Если опция включена, устройство будет инициализировано перед выпуском. В результате инициализации все данные, хранящиеся на устройстве, будут удалены. В процессе выпуска устройства имеется возможность отключить или включить данную опцию для конкретного устройства.
Установить случайный PIN-код пользователя	Если опция включена, то в процессе выпуска устройства будет установлен случайный PIN-код пользователя. При включении опции становятся доступными для редактирования Параметры генерации PIN-кода пользователя: ○ Использовать только цифры ○ Длина (от 4 до 31 символа) ○ Отображать установленный PIN-код администратору ○ Отображать установленный PIN-код пользователю  Длина случайного PIN-кода зависит от настройки Минимальная длина PIN-кода пользователя на вкладке Инициализация устройства. Формируемый случайный PIN-код соответствует следующим правилам: ○ Содержит латинские строчные буквы ○ Содержит латинские прописные буквы ○ Содержит цифры ○ Содержит специальные символы ○ Повторы любых символов запрещены Случайный PIN-код пользователя может быть сообщен сотруднику, выпускающему карту. Случайный PIN-код пользователя может быть сообщен пользователю или его руководителю посредством почтового уведомления (см. раздел Уведомления).  Если в разделах Выпуск и Инициализация устройства будут указаны разные значения длины PIN-кода пользователя, то в процессе выпуска устройства будет использовано большее из них.

Пользователь должен поменять PIN-код при первом входе	Если опция включена, то пользователю будет необходимо изменить PIN-код устройства при первом его подключении к рабочей станции.  Опция поддерживается только устройствами eToken, IDPrime и Рутокен ЭЦП 3.0 NFC.
Блокировать устройство	Если опция включена, то устройство будет заблокировано после выпуска. Перед использованием устройства, пользователь должен будет его разблокировать любым доступным способом (в режиме online или offline) и установить новый PIN-код.  Данная опция и опции Устанавливать случайный PIN-код пользователя и Пользователь должен поменять PIN-код при первом входе взаимоисключаемы.
Генерировать имя устройства автоматически	Если опция включена, то в качестве имени устройства может быть использовано одно из следующих значений из свойств пользователя: ○ Общее имя (CN) ○ Логин ○ Фамилия ○ E-mail ○ Подразделение ○ Заданная строка Выбранное значение будет автоматически подставлено в имя устройства в окне выпуска. При включенной опции Разрешить редактирование имени устройства подставленное имя может быть изменено сотрудником или пользователем перед выпуском устройства.
Требовать указания комментария к устройству	Если опция включена, то при выпуске устройства в Консоле управления Администратор или Оператор системы должен задать Комментарий к устройству.
Требовать указания тегов к устройству	Если опция включена, то при выпуске устройства в Консоле управления Администратор или Оператор системы должен задать Теги для устройства.
Отображать установленный пароль пользователя КристоПро DSS администратору	Если опция включена, то при создании пользователя КристоПро DSS и выпуске ему сертификата пароль будет отображен администратору в личной карточке пользователя.
Отображать установленный пароль пользователя КристоПро DSS пользователю	Если опция включена, то при создании пользователя КристоПро DSS и выпуске ему сертификата пароль будет отображен пользователю в кабинете самообслуживания.

Инициализация устройства

Параметры инициализации, задаваемые в интерфейсе Indeed Certificate Manager (требования к длине и сложности пароля, количество попыток ввода до блокировки и т.д.) будут сохранены на устройстве до следующей инициализации.

Для настройки инициализации нажмите **Добавить параметры инициализации** и выберите тип устройства.

Инициализация устройства

 Добавить параметры инициализации

Добавить параметры инициализации

Тип устройства

Rutoken ECP



ОК

Отмена

После нажатия на **ОК** произойдет переход к списку доступных для изменения параметров инициализации выбранного типа устройств. Установите параметры инициализации и нажмите **Добавить** для сохранения.

Добавить параметры инициализации

Тип устройства

Rutoken ECP

Оставьте поле 'PIN-код пользователя' пустым, если хотите использовать значение, установленное производителем устройства

PIN-код пользователя

Минимальная длина PIN-кода

6

Максимальное количество попыток ввода PIN-кода

10

Максимальное количество попыток ввода PIN-кода администратора

3

Пользователь
Администратор
Пользователь и Администратор

Добавить

Отмена



Набор параметров инициализации зависит от типа устройства.

Для редактирования параметров нажмите . Для удаления нажмите .

[+ Добавить параметры инициализации](#)

Тип устройства

eToken PRO Java 72K	 
JaCarta	 
Rutoken ECP	 

 В случае отсутствия в политике параметров инициализации для любого выпускаемого устройства при включении инициализации будут установлены значения по умолчанию из раздела [Типы устройств](#).

Разрешенные устройства

По умолчанию выпуск разрешен на всех добавленных в Indeed Certificate Manager типах устройств. Для настройки политики на выпуск устройств определенного типа нажмите **Добавить тип устройства**.

Разрешенные устройства

Разрешен выпуск всех типов устройств

[+ Добавить тип устройства](#)

Добавить тип устройства

Имя

Rutoken ECP



Добавить

Отмена

Количество типов устройств, разрешенных для выпуска, неограничено. Для удаления типа устройства из списка разрешенных нажмите **✕**.

Разрешенные устройства

[+ Добавить тип устройства](#)

Имя

Rutoken ECP



Rutoken S



Операции для уже выпущенных в рамках политики устройств, которых нет в списке разрешенных остаются доступными, включая выпуск новых сертификатов через обновление содержимого устройства.

Аутентификация

Аутентификация пользователей по секретным вопросам осуществляется при [самостоятельной разблокировке](#) устройства пользователем, [выключении устройства](#) без выполнения входа в ОС, при доступе в [Удаленный личный кабинет пользователя](#) (Remote Self Service), и при выполнении задачи по [сбросу PIN-кода пользователя](#) на клиентском агенте.

В этом разделе задаются параметры аутентификации пользователей: количество секретных вопросов (значение по умолчанию – 1) и максимальное количество попыток аутентификации по секретным вопросам до блокировки пользователя (значение по умолчанию – 3).

Аутентификация

Количество вопросов при аутентификации

Максимальное количество попыток аутентификации

Сохранить

На вкладке **Секретные вопросы** задаются параметры секретных вопросов: список вопросов и минимальное количество символов для ответа на каждый вопрос.



Если список секретных вопросов не задан, то у пользователя не будет возможности указать ответы на секретные вопросы в **Сервисе самообслуживания** (Self Service).

Чтобы задать секретный вопрос, нажмите **Создать секретный вопрос**, введите вопрос и задайте минимальную длину ответа (значение по умолчанию – 3 символа). Нажмите кнопку **Создать** для сохранения параметров.

Секретные вопросы

[+ Создать секретный вопрос](#)

Создать секретный вопрос

Вопрос

Минимальная длина ответа

3

Создать

Отмена

Созданные вопросы в случае необходимости могут быть изменены или удалены. Чтобы изменить вопрос, нажмите  напротив нужного вопроса. Для удаления вопроса нажмите .

 Секретный вопрос может быть удален только в том случае, если его не использует ни один из пользователей системы.

Секретные вопросы

[+ Создать секретный вопрос](#)

Вопрос	Минимальная длина ответа	
Как называется наша компания?	3	 
Девичья фамилия матери?	3	 

Агенты (Политики)

В разделе задаются основные параметры Агента Indeed Certificate Manager:

- [Контроль за использованием устройств](#)
- [Сообщения пользователю после успешного выполнения задач](#)

Контроль

Контроль за использованием устройств осуществляется при помощи клиентского Агента Indeed CM, устанавливаемого на рабочие станции пользователей. В разделе задаются действия и тексты сообщений (опционально), которые будут выполняться при нарушении правил использования устройств.

Настройки контроля использования устройства.

Опция	Описание
Сообщение при нарушении условий привязки устройства к агенту	Сообщение, которое будет отображено пользователю Агентом Indeed CM при подключении устройства к неразрешенной администратором рабочей станции. Если значение не задано, то сообщение не будет отображаться.
Действие, выполняемое при нарушении условий привязки устройства к агенту	Действие, которое будет выполнено Агентом Indeed CM при подключении устройства к неразрешенной администратором рабочей станции. Возможные варианты: ○ Запись события ○ Блокировка пользовательской сессии ○ Блокировка устройства ○ Блокировка пользовательской сессии и устройства
Включить проверку привязки устройства к пользователю	Если опция включена, то Агент Indeed CM при подключении устройства к рабочей станции будет проверять его принадлежность к пользователю, под которым было выполнено подключение.
Сообщение при нарушении условий привязки устройства к пользователю	Сообщение, которое будет отображено пользователю Агентом Indeed CM при подключении устройства к рабочей станции с сессией другого пользователя. Если значение не задано, то сообщение не будет отображаться.
Действие, выполняемое при нарушении условий привязки устройства к пользователю	Действие, которое будет выполнено Агентом Indeed CM при подключении устройства к рабочей станции с сессией другого пользователя. Возможные варианты: ○ Запись события ○ Блокировка пользовательской сессии ○ Блокировка устройства ○ Блокировка пользовательской сессии и устройства
Таймаут до блокировки пользовательской сессии (сек.)	Период времени, по истечении которого сессия пользователя будет заблокирована, если блокировка выбрана как действие, которое должен выполнять Агент Indeed CM при нарушении правил использования устройства пользователем. Возможный интервал от 0 до 5 секунд.

Сообщения пользователю

Агент Indeed Certificate Manager может уведомлять пользователей об успешном выполнении следующих операций с их устройствами:

- Блокировки PIN-кода пользователя
- Смены PIN-кода администратора на устройстве
- Отзыва устройства с инициализацией

По умолчанию сообщения не заданы и не выводятся пользователю. Для включения сообщений введите текст сообщений.

Сообщения пользователю после успешного выполнения задач

Сообщения отображаются только внутри сессии пользователя в операционной системе. В сообщениях допустимо использовать следующие атрибуты:

- {sn} – вывод серийного номера устройства
- {atr} – вывод значения ATR устройства
- {model} – вывод модели устройства
- {label} – вывод метки устройства

Пример: Устройство {model} ({label}) {sn} было заблокировано.

Если параметр не задан, то сообщение отображаться не будет.

Блокировка PIN-кода пользователя

Устройство {model} ({label}): {sn} было заблокировано администратором.

Смена PIN-кода администратора на устройстве

PIN-код администратора на устройстве {model} ({label}): {sn} был изменен.

Отзыв устройства с инициализацией

Администратор выполнил инициализацию устройства {model} ({label}): {sn}.

Сохранить

Принтер смарт-карт

Интеграция Indeed Certificate Manager с принтером EDIsecure XID 8300 позволяет выполнять следующие сценарии:

- выпускать смарт-карты пользователям используя считыватели принтера (контактный и бесконтактный) без печати
- выпускать смарт-карты пользователям используя считыватели принтера (контактный и бесконтактный) с печатью на карте изображения или текста
- печатать на смарт-картах изображение или текст без выпуска карты пользователям

Принтер смарт-карт

☐ Включить поддержку принтера смарт-карт

☐ Читать RFID-метку устройства

☐ Включить печать устройства

Сохранить

Опция **Включить поддержку принтера смарт-карт** позволяет при выпуске выбирать считыватель, к которому подключена карта: считыватель, подключенный к рабочей станции или считыватель принтера. При включении опции становятся доступны опции выпуска устройства с использованием принтера:

- **Читать RFID-метку устройства**

Если опция включена, то Indeed CM прочитает метку устройства и сохранит её в свою базу данных связав с пользователем, для которого выпускается устройство. При отзыве устройства значение метки останется в хранилище Indeed CM до тех пор, пока устройство находится в системе. При выпуске устройства другому пользователю, значение метки закрепляется за ним.

- **Включить печать устройства**

Если опция включена, то при выпуске устройства через принтер будет происходить печать изображения/текста на нем в соответствии с загруженным шаблоном печати.

На вкладке **Шаблон устройства** задается шаблон печати данных при выпуске смарт-карты в текущей политике. Шаблон представляет собой xml-файл, содержащий данные о том, что необходимо выводить на печать.

Для загрузки шаблона нажмите **Загрузить шаблон устройства**, укажите файл шаблона и нажмите кнопку **Загрузить**. После загрузки шаблона его статус в политике ("не загружен") изменится на имя, указанное в файле шаблона.

Шаблон устройства

Не загружен

 [Загрузить шаблон устройства](#)

Загрузить шаблон устройства

Файл шаблона устройства



Загрузить

Отмена



Файл шаблона печати можно получить обратившись в [службу технической поддержки компании Indeed Identity](#).

Уведомления

В разделе задаются настройки почтовых уведомлений о событиях Indeed Certificate Manager.

Задайте настройки почтового сервера, определите получателей (администраторы или обычные пользователи) и настройте для них шаблоны почтовых уведомлений:

- [Группы получателей](#)
- [Уведомления администратора](#)
- [Уведомления пользователя](#)
- [Шаблоны администратора](#)
- [Шаблоны пользователя](#)

Настройка почтового сервера

Уведомления

Почтовый сервер

Порт

☒ Использовать SSL

Оставьте поля 'Имя пользователя' и 'Пароль' пустыми, если аутентификация на почтовом сервере не требуется

Имя пользователя

Пароль

E-mail адрес, который пользователи будут видеть в поле 'От' нотификации. Некоторые почтовые серверы и клиенты могут игнорировать этот параметр (например, gmail)

E-mail отправителя

☒ [Отправить тестовое сообщение](#)

☒ Включить уведомления администратора

☒ Включить уведомления пользователя

Сохранить

Воспользуйтесь функцией отправки тестового сообщения для проверки заданных настроек почтового сервера. Для этого укажите необходимые настройки почтового сервера, нажмите **Сохранить**, а затем **Отправить тестовое сообщение**.

✉ Отправить тестовое сообщение

Отправить тестовое сообщение

Получатель

admin@company.com x

Отправить

Заккрыть

Укажите адрес электронной почты получателя и нажмите **Отправить**. Если настройки указаны верно, сообщение будет отправлено.

✉ Отправить тестовое сообщение

Отправить тестовое сообщение

Тестовое сообщение успешно отправлено

Получатель

admin@company.com

Отправить

Заккрыть

Нажмите кнопку **Заккрыть**, если тестовое сообщение отправить не удалось. Измените настройки почтового сервера, нажмите **Отправить** и повторите попытку.

Если опция **Включить уведомления пользователя** задана, то в Консоли управления при просмотре содержимого устройства пользователя, Администратор или Оператор системы имеет возможность отправить печатную форму **Сертификата**, **Запроса на сертификат** или **Запроса на отзыв сертификата** в формате PDF на e-mail пользователю.

▼

Rutoken S, 0755398982

Evgeniy Belov

Выпущено

Сбросить PIN-код

Разблокировать

Выключить

Отозвать

Заменить

Заменить на AirKey

Обновить

Заблокировать

Сменить PIN-код администратора

Комментарий

Политика

Базовая политика

PIN-код администратора

Теги

Сертификаты

Шаблон	УЦ	Действителен до	Состояние	
Вход по смарт-карте	demo-DC-CA	11.11.2020 16:16	Действительный	Сертификат Запрос на сертификат

⊕ Выпустить устройство

⊕ Выпустить AirKey

⊕ Назначить устройство

Группы получателей

В пункте настраиваются группы получателей уведомлений администраторов.

Например:

Это могут быть специалисты по информационной безопасности и защите информации вашей компании.

Для того чтобы установить группу получателей нажмите **Создать группу**, укажите имя группы, введите адреса получателей и нажмите **Создать**.

Группы получателей

[+ Создать группу](#)

Создать группу

Имя

ОИБ

Получатели

✕ oib@company.com

[+ Добавить](#)

Создать

Отмена

Созданные группы получателей в случае необходимости могут быть изменены или удалены. Для изменения группы выберите ее в списке и нажмите . Для удаления группы нажмите .

Группы получателей

[+ Создать группу](#)

Имя	Получатели	
ОИБ	oib@company.com, admin@company.com	 
ОЗИ	ozi@company.com	 

 Группа получателей может быть удалена только в том случае, если она не используется для рассылки уведомлений.

Уведомления администратора

1. Для создания уведомления нажмите **Создать уведомление**.

2. Выберите **Событие** из списка.

- Атрибуты пользователя были изменены
- Аутентификация
- Блокировка пользователя
- Ввод неверного PIN-кода администратора на устройстве
- Ввод неверного PIN-кода пользователя на устройстве
- Включение устройства
- Включение устройства КристоПро DSS
- Выключение устройства
- Выключение устройства КристоПро DSS
- Выпуск сертификата (Событие доступно для каждого добавленного шаблона сертификата в политику)
- Выпуск сертификата КристоПро DSS (Событие доступно для каждого добавленного шаблона сертификата DSS в политику)
- Выпуск устройства
- Выпуск устройства КристоПро DSS
- Выпуск устройства КристоПро DSS ожидает решения
- Выпуск устройства ожидает решения
- Добавление AirKey к компьютеру
- Добавление СКЗИ
- Задача выполнена
- Замена устройства
- Замена устройства ожидает решения
- Изменение PIN-кода
- Изменение ответов на секретные вопросы
- Изменение политики
- Назначение СКЗИ
- Назначение устройства
- Нарушение условий привязки устройства к агенту
- Нарушение условий привязки устройства к пользователю
- Обнаружена блокировка PIN-кода администратора на устройстве
- Обнаружена блокировка PIN-кода пользователя на устройстве
- Обновление СКЗИ
- Обновление устройства
- Обновление устройства КристоПро DSS
- Обновление устройства КристоПро DSS ожидает решения
- Обновление устройства ожидает решения
- Общие сертификаты истекают

- Одобрение выпуска устройства
- Одобрение выпуска устройства КристоПро DSS
- Одобрение замены устройства
- Одобрение обновления устройства
- Одобрение обновления устройства КристоПро DSS
- Отзыв устройства
- Отзыв устройства КристоПро DSS
- Отклонение выпуска устройства
- Отклонение выпуска устройства КристоПро DSS
- Отклонение замены устройства
- Отклонение обновления устройства
- Отклонение обновления устройства КристоПро DSS
- Отмена назначения устройства
- Отмена обновления устройства
- Отмена обновления устройства КристоПро DSS
- Отслеживаемые сертификаты истекают
- Очистка устройства
- Политика была обновлена
- Политика пользователя была изменена
- Политика пользователя устройства КристоПро DSS была изменена
- Политика устройства КристоПро DSS была обновлена
- Разблокировка пользователя
- Разблокировка устройства
- Сброс PIN-кода
- Сброс ответов на секретные вопросы
- Сброс пароля пользователя
- Содержимое устройства истекает
- Содержимое устройства КристоПро DSS истекает
- Создание кода подключения AirKey к компьютеру
- Удаление AirKey от компьютера
- Удаление устройства КристоПро DSS
- Уничтожение/изъятие СКЗИ

3. Укажите **Тип события**, о котором необходимо извещать администратора:

- Информация
- Ошибка
- Предупреждение

4. Выберите **Группу получателей**. В качестве адресатов могут быть выбраны:

- Приложение - группа созданная в разделе [Группы получателей](#)
- Каталог пользователей - группа безопасности Active Directory

5. Укажите **Период отправки (дней)** - количество дней, через которое уведомление будет отправлено повторно.

- Атрибуты пользователя были изменены
- Общие сертификаты истекают
- Одобрение выпуска устройства
- Одобрение выпуска устройства КристоПро DSS
- Одобрение замена устройства
- Одобрение обновления устройства
- Одобрение обновления устройства КристоПро DSS
- Отклонение выпуска устройства
- Отклонение выпуска устройства КристоПро DSS
- Отклонение замены устройства
- Отклонение обновления устройства
- Отклонение обновления устройства КристоПро DSS
- Отслеживаемые сертификаты истекают
- Политика была обновлена
- Политика пользователя была изменена
- Политика пользователя устройства КристоПро DSS была изменена
- Политика устройства КристоПро DSS была обновлена
- Содержимое устройства истекает
- Содержимое устройства КристоПро DSS истекает

6. Нажмите **Создать**.

Уведомления администратора

[+ Создать уведомление](#)

Создать уведомление

Событие

Одобрение выпуска устройства

Типы событий

☒ Информация

☐ Ошибка

☐ Предупреждение

Группа получателей

☒ Приложение

☐ Каталог пользователей

ОИБ

Период отправки (дней)

0

Создать

Отмена

Созданные уведомления в случае необходимости могут быть изменены или удалены. Для изменения уведомления выберите его в списке и нажмите . Для удаления уведомления нажмите .

Уведомления администратора

[+ Создать уведомление](#)

Событие	Тип события	Группа получателей	
Одобрение выпуска устройства	Информация	ОИБ	
Выпуск устройства	Информация, Ошибка	ОИБ	
Блокировка пользователя	Предупреждение	ОИБ	

Уведомления пользователя

В этом пункте настраивается перечень событий системы, о которых необходимо извещать пользователей.



Уведомления о событиях системы отправляются только тем пользователям, у которых в свойствах учетной записи Active Directory указан адрес электронной почты.

1. Для создания уведомления нажмите **Создать уведомление**.
2. Выберите **Событие** из списка, о котором необходимо извещать пользователя.
 - Атрибуты пользователя были изменены
 - Аутентификация
 - Блокировка пользователя
 - Включение устройства
 - Включение устройства КристоПро DSS
 - Выключение устройства
 - Выключение устройства КристоПро DSS
 - Выпуск сертификата (Событие доступно для каждого добавленного шаблона сертификата в политику)
 - Выпуск сертификата КристоПро DSS (Событие доступно для каждого добавленного шаблона сертификата DSS в политику)
 - Выпуск устройства
 - Выпуск устройства КристоПро DSS
 - Выпуск устройства КристоПро DSS ожидает решения
 - Выпуск устройства ожидает решения
 - Добавление AirKey к компьютеру
 - Добавление СКЗИ
 - Замена устройства
 - Замена устройства ожидает решения
 - Изменение PIN-кода
 - Изменение ответов на секретные вопросы
 - Назначение СКЗИ
 - Назначение устройства
 - Обновление СКЗИ
 - Обновление устройства
 - Обновление устройства КристоПро DSS
 - Обновление устройства КристоПро DSS ожидает решения
 - Обновление устройства ожидает решения
 - Одобрение выпуска устройства

- Одобрение выпуска устройства КристоПро DSS
- Одобрение замены устройства
- Одобрение обновления устройства
- Одобрение обновления устройства КристоПро DSS
- Отзыв устройства
- Отзыв устройства КристоПро DSS
- Отклонение выпуска устройства
- Отклонение выпуска устройства КристоПро DSS
- Отклонение замены устройства
- Отклонение обновления устройства
- Отклонение обновления устройства КристоПро DSS
- Отмена назначения устройства
- Отмена обновления устройства
- Отмена обновления устройства КристоПро DSS
- Отслеживаемые сертификаты истекают
- Очистка устройства
- Политика была обновлена
- Политика пользователя была изменена
- Политика пользователя устройства КристоПро DSS была изменена
- Политика устройства КристоПро DSS была обновлена
- Разблокировка пользователя
- Разблокировка устройства
- Сброс PIN-кода
- Сброс ответов на секретные вопросы
- Сброс пароля пользователя
- Содержимое устройства истекает
- Содержимое устройства КристоПро DSS истекает
- Создание кода подключения AirKey к компьютеру
- Удаление AirKey от компьютера
- Удаление устройства КристоПро DSS
- Уничтожение/изъятие СКЗИ
- Установка PIN-кода
- Установка пароля пользователя КристоПро DSS

3. Укажите **Тип события**:

- Информация
- Ошибка
- Предупреждение

4. Укажите **Период отправки (дней)** - количество дней, через которое уведомление будет отправлено повторно.

- Атрибуты пользователя были изменены
- Общие сертификаты истекают
- Одобрение выпуска устройства
- Одобрение выпуска устройства КристоПро DSS
- Одобрение замена устройства
- Одобрение обновления устройства
- Одобрение обновления устройства КристоПро DSS
- Отклонение выпуска устройства
- Отклонение выпуска устройства КристоПро DSS
- Отклонение замены устройства
- Отклонение обновления устройства
- Отклонение обновления устройства КристоПро DSS
- Отслеживаемые сертификаты истекают
- Политика была обновлена
- Политика пользователя была изменена
- Политика пользователя устройства КристоПро DSS была изменена
- Политика устройства КристоПро DSS была обновлена
- Содержимое устройства истекает
- Содержимое устройства КристоПро DSS истекает

5. Если необходимо, включите опцию **Отправлять копию менеджеру** (руководителю) в выбранном событии пользователя.



Доступно только для пользователей, расположенных в Active Directory. Адрес электронной почты руководителя (менеджера) задается на вкладке **Организация** (Organization) свойств пользователя Active Directory в разделе **Руководитель** (Manager).

6. Нажмите **Создать**.

Уведомления пользователя

[+ Создать уведомление](#)

Создать уведомление

Событие

Одобрение выпуска устройства 

Типы событий

☒ Информация

☐ Ошибка

☐ Предупреждение

Период отправки (дней)

2

☐ Отправлять копию менеджеру

Создать

Отмена

Для изменения уведомления выберите его в списке и нажмите . Для удаления уведомления нажмите .

Шаблоны администратора

В этом пункте настраиваются шаблоны почтовых уведомлений о событиях системы, которые будут рассылаться администраторам Indeed Certificate Manager. В базовом варианте почтовое уведомление содержит следующую информацию:

Тема. Формируется исходя из названия события, например, «Выпуск устройства».

Текст сообщения. Формируется исходя из названия сообщения и его типа, может содержать информацию об инициаторе, пользователе, сертификатах и устройствах.

Шаблоны администратора

Событие и тип события

Выпуск устройства ожидает решения

Информация

Тема

Выпуск устройства

Текст сообщения

B *I* U ~~X~~





Формат... Шрифт Ра...    Источник

Выпуск устройства ожидает решения.
Пользователь: {1}
Политика: {2}
Устройство: {3}:{4}
Сертификаты: {5}
Общие сертификаты: {6}
Отслеживаемые сертификаты: {7}
Инициатор: {0}

body

Сохранить Сбросить

Для каждого уведомления в одной политике использования устройств настраивается только один шаблон. На основе базового шаблона, Indeed CM сформирует и отправит электронное письмо следующего содержания:

Тема: Выпуск устройства
Текст сообщения: Выпуск устройства ожидает решения.
Пользователь: Евгений Белов
Политика: Базовая политика
Устройство: Rutoken S:0755398982
Сертификаты: Вход по смарт-карте, Квалифицированный пользователь
Общие сертификаты: Сертификат для VPN
Отслеживаемые сертификаты: Пользователь VIPNet
Инициатор: DEMO\Administrator

Базовый шаблон может быть изменен. Система позволяет использовать HTML-теги для форматирования текста сообщения. Пример персонализированного шаблона почтового уведомления:

Шаблоны администратора

Событие и тип события

Выпуск устройства ожидает решения

Информация

Тема

Выпуск устройства пользователя ожидает решения

Текст сообщения

B **I** **U** **I_x**

Обычное Шрифт Ра... Источник

Пользователь {1} направил запрос на выпуск смарт-карты {3}:{4} для использования в корпоративной сети предприятия согласно политике {2}.

На карту будут записаны следующие сертификаты: {5}.

Для выпуска устройства пользователю необходимо одобрить запросы на запрашиваемые сертификаты.

body p

Сохранить Сбросить

Текст почтового уведомления, созданного на основе изменённого базового шаблона, будет таким:

Тема: Выпуск устройства пользователя ожидает решения

Пользователь **Евгений Белов** направил запрос на выпуск смарт-карты **Rutoken S: 0755398982** для использования в корпоративной сети предприятия согласно политике **Базовая политика**.

На карту будут записаны следующие сертификаты: **Вход по смарт-карте, Квалифицированный пользователь**.

Для выпуска устройства пользователю необходимо одобрить запросы на запрашиваемые сертификаты.

Шаблоны пользователя

В данном пункте настраиваются шаблоны почтовых уведомлений о событиях Indeed Certificate Manager, которые будут рассылаться пользователям. Для каждого уведомления в одной политике использования устройств настраивается один шаблон. В базовом варианте почтовое уведомление содержит следующую информацию:

Тема. Формируется исходя из названия события, например, «Установка PIN-кода».

Текст сообщения. Формируется исходя из названия сообщения и его типа, может содержать информацию об инициаторе, пользователе и устройствах.

Шаблоны пользователя

Событие и тип события

Установка PIN-кода

Информация

Тема

Установка PIN-кода

Текст сообщения

B **I** **U** **I_x**                        

Например:

Текст письма может быть дополнен сообщением о конфиденциальности, содержащейся в нем информации, либо дополнен указаниями к действиям, которые должны предпринять сотрудники, получившее письмо.

Назначения политик

Политики использования устройств начнут действовать на пользователей после определения области действия. Политика может распространяться на следующие объекты:

Active Directory:

- **Домен** (Domain)
- **Контейнер** (Container)
- **Подразделение** (Organizational Unit)

 Действие политики может распространяться как на весь объект (домен, контейнер или подразделение), так и на отдельные группы пользователей, входящие в него.

КриптоПро УЦ 2.0:

- Часть существующей в Центре Регистрации структуры контейнеров (папок) или на весь ЦР

Организационная структура Indeed CM, в узлы которой могут входить:

- **Домен** (Domain), **Контейнер** (Container), **Подразделение** (Organization Unit), пользователи или группы безопасности Active Directory
- Часть существующей в **Центре Регистрации** структуры контейнеров (папок) или на весь ЦР. Пользователи или группы безопасности ЦР

 Политики, действующие на каталог пользователей Active Directory или каталог Центра Регистрации КриптоПро УЦ 2.0 имеют приоритет над политиками, действующими на Организационную структуру Indeed CM.

Для назначения политики на объект нажмите **Создать назначение политики**, выберете политику из списка и задайте следующие параметры:

 [Создать назначение политики](#)

Создать назначение политики

Политика

Базовая политика

Контейнер

Выберите контейнер

 [Выбрать](#)

Группа

Выберите группу

 [Выбрать](#)

Приоритет

0

Роли

 [Добавить роль](#)

Создать

Отмена

- **Контейнер** – область действия политики. Контейнером может быть подразделение Active Directory, папка Центра Регистрации КриптоПро УЦ 2.0 или узел организационной структуры Indeed CM.
- **Группа** – дополнительный фильтр для распространения политики. Например, на один контейнер с пользователями организации может быть назначено несколько политик, которые будут распространяться на пользователей, входящих в определенные группы Active Directory.
- **Приоритет** – значение, определяющее применение той или иной политики к пользователю. Если пользователь попадает под область действия нескольких политик выпуска устройств одного типа (политики Active Directory, ЦР КриптоПро УЦ или Организационной структуры), например, состоит в двух группах, расположенных в одном OU, то действовать на пользователя будет политика с большим приоритетом.
- **Роли** – если в разделе **Роли** есть хотя бы одна локальная роль, то ее можно будет добавить в создаваемое назначение политики и задать пользователей роли.

Нажмите **Создать** для сохранения назначения политики. Для изменения назначения политики нажмите . Для удаления назначения нажмите .

Назначения политик

[+ Создать назначение политики](#)

Политика	Контейнер	Группа	Приоритет	
Базовая политика	Тестовая компания	demo.local/Users/Domain Users	0	 

Лицензии

Для добавления новой лицензии нажмите **Добавить лицензию**, укажите файл лицензии и нажмите кнопку **Добавить**.

Лицензии

Идентификатор системы	8008-01ef-f4f9-648f-3fc1	
Количество лицензий	0	
Используется лицензий	0	

 [Добавить лицензию](#)

Добавить лицензию

Файл лицензии

General.lic



Добавить

Отмена

Чтобы удалить лицензию из системы, выберите её в списке и нажмите кнопку  .
Подтвердите действие нажатием на кнопку **Удалить**.

Лицензии

Идентификатор системы	8008-01ef-f4f9-648f-3fc1	
Количество лицензий	50	
Используется лицензий	1	

 [Добавить лицензию](#)

Организация	Срок действия	Количество пользователей	Тип	
Indeed-ID	01.01.2020 - 01.01.2025	50	General	

Удалить лицензию

Вы уверены, что хотите удалить лицензию?

Удалить

Отмена

Типы устройств

Indeed Certificate Manager поддерживает работу с USB-токенами, смарт-картами и комбинированными устройствами. Количество поддерживаемых устройств аутентификации и типов постоянно увеличивается. Если в вашей организации появились устройства нового типа, или наоборот, устройства одного типа перестали использоваться, потребуется внести соответствующие изменения в Indeed CM.

Добавление типов устройств

Для добавления типа устройства нажмите **Добавить тип устройства**, укажите файл типа устройства и нажмите **Добавить**. Если необходимо заменить имеющийся в системе файл типа устройства, отметьте опцию **Заменить существующий**.

Типы устройств

[+ Добавить тип устройства](#)

Добавить тип устройства

Файл типа устройства



☐ Заменить существующий

Добавить

Отмена



Файлы для устройств различных типов поставляется вместе с дистрибутивом и располагаются в каталоге \Misc\CardTypes дистрибутива Indeed CM Server.

Типы устройств и файлов соответствующих их типам представлены в таблице:

Производитель	Модель устройства	Файл типа устройства
Компания «Актив»	Рутокен S	RutokenS.xml
	Рутокен Lite	RutokenLite.xml
	Рутокен Lite SC	RutokenLiteSC.xml

	Рутокен ЭЦП PKI	RutokenECP.xml
	Рутокен ЭЦП 2.0	
	Рутокен ЭЦП 3.0 NFC	
	Рутокен ЭЦП PKI SC	RutokenECPSC.xml
	Рутокен ЭЦП 2.0 SC	
	Рутокен ЭЦП 3.0 NFC SC	RutokenECPNFCSC.xml
	Рутокен 2151	Rutoken2151.xml
	Рутокен 2151 SC	Rutoken2151SC.xml
Компания Индид	AirKey	AirKey.xml
Аладдин Р.Д.	JaCarta PKI	JaCarta.xml
	JaCarta PKI/Flash	
	JaCarta PKI/BIO	
	JaCarta PKI/ГОСТ	
	JaCarta PKI/ГОСТ/Flash	
	JaCarta-2 PKI/ГОСТ	
	JaCarta-2 PKI/ГОСТ/Flash	
	JaCarta-2 SE	
ACS	ACOS5-64	Acos5-64.xml
Avest	Avest Key 256A	AvestKey-256-A.xml
Bit4id	ID-One Cosmo	Bit4Id.xml
CRYPTAS	TicTok V2	TicTok_v2.xml
	TicTok V3	TicTok_v3.xml
Cryptovision	ePasslet Suite v3.0, JCOP V3.0	cv-ePassletSuite3.0-JCOP3.0.xml
Feitian	ePass2003 (A1+, A2)	ePass2003.xml
	BioPass2003	
HID	Crescendo C1150 Series	CrescendoC1150.xml
	Crescendo C1300 Series	CrescendoC1300.xml
	Crescendo C2300 Series	CrescendoC2300.xml
ISBC	ESMART Token 64K и ESMART Token SC 64K	EsmartToken64K.xml

	ESMART Token ГОСТ	EsmartTokenGOST.xml
	ESMART Token SC ГОСТ	EsmartTokenGOST-D.xml
Kaztoken	Kaztoken	Kaztoken.xml
	Kaztoken SC	KaztokenSC.xml
Microsoft	Реестр Локального компьютера	Registry.xml
	Реестр Пользователя	
	TPM Virtual Smart Card (Microsoft VSC) - виртуальная смарт-карта на базе Trusted Platform Module v.2.0	Tpm.xml
	Windows Hello for Business (WHfB)	Whfb.xml
RSA	RSA SecurID 800	RSASecurID.xml
Thales Group	SafeNet eToken PRO 32k	eTokenPro32K.xml
	SafeNet eToken PRO 64k	eTokenPro4.2B.xml
	eToken PRO Java 72K OS755	eTokenProJava72K.xml
	SafeNet eToken 5105	
	SafeNet eToken 5110	
	IDCore30B eToken 1.7.7	
	IDPrime MD 830	IDPrimeMD.xml
	IDPrime MD 840	
	IDPrime MD 3810	
	IDPrime MD 3811	
Yubico	YubiKey 5 Series	YubiKey5.xml

После добавления типа карты в системе отобразится его имя.

Типы устройств

[+ Добавить тип устройства](#)

Имя	
AirKey	 
ESMART Token GOST	 
eToken PRO Java 72K (JC1.0b)	 
JaCarta	 
Rutoken ECP	 

Редактирование типов устройств

Файл типа устройства по умолчанию содержит предустановленные значения PIN-кодов администратора и пользователя (в том числе и для ГОСТ-области). Эти значения могут быть изменены во время и после добавления типа устройства в Indeed CM. Для

редактирования типа устройства выберите нужный тип в списке и нажмите  , для просмотра PIN-кодов нажмите .

Редактировать тип устройства

Имя

PIN-код администратора



PIN-код пользователя



PIN-код администратора (ГОСТ)



PIN-код пользователя (ГОСТ)



- ☒ Инициализировать устройство при добавлении
- ☒ Устанавливать неслучайный PIN-код администратора



- ☒ Устанавливать неслучайный PIN-код администратора (ГОСТ)



Наличие ГОСТ-области зависит от производителя и модели устройства.

При редактировании устройства доступны следующие опции:

- **Инициализировать устройство при добавлении** – Indeed CM позволяет выполнять инициализацию устройства в процессе добавления. При этом:
 - Добавляемое устройство будет очищено.
 - В качестве имени устройства будет задано значение **Empty**.
 - PIN-код администратора будет изменен на случайный (известный только Indeed CM) или указанный в опции **Установить неслучайный PIN-код администратора**.
 - Количество попыток ввода PIN-кода администратора до блокировки будет равно **3**.
 - PIN-код пользователя, его минимальная длина и количество попыток ввода до блокировки будут изменены на указанные в файле типа устройства.



Для устройств eToken поддерживается инициализация с любым состоянием и значением PIN-кода администратора.

- **Устанавливать неслучайный PIN-код администратора** – если опция выключена, то при добавлении устройства установится случайный и известный только Indeed CM PIN-код. Если опция включена, то при добавлении устройства будет установлен указанный PIN-код.
- **Устанавливать неслучайный PIN-код администратора (ГОСТ)** – если опция выключена, то при добавлении устройства установится случайный и известный только Indeed CM PIN-код ГОСТ-области. Если опция включена, то при добавлении устройства будет установлен указанный PIN-код для ГОСТ-области.

Для сохранения внесенных изменений нажмите **Сохранить**.

Удаление типов устройств

Для удаления типа устройства, выберите его в списке, нажмите **✕** и подтвердите действие, нажав **Удалить**.

Типы устройств

[+ Добавить тип устройства](#)

Имя

AirKey



Удалить тип устройства

Вы уверены, что хотите удалить тип устройства?

Удалить

Отмена



Внимание

Удалить **Тип устройства** можно только в том случае, если в Indeed CM нет ни одного устройства этого типа.

Организационная структура



Раздел доступен при включенной опции **Организационная структура** в разделе **Общие функции** Мастера настройки Indeed CM и предоставленных привилегиях на **Просмотр организационной структуры** и **Изменение организационной структуры** членам Роли.

Устройства в Indeed Certificate Manager выпускаются пользователям по заданным правилам. Правила использования устройств, такие как необходимость инициализации, настройки выдачи, параметры аутентификации пользователей и т.д. задаются в политиках использования устройств, которые распространяются на указанную область. Область распространения политики – объект каталога пользователей. Например, подразделение домена Active Directory или папка в Центре Регистрации КриптоПро УЦ.

Организационная структура позволяет объединить разрозненные объекты каталога пользователей под действие одной политики использования устройств. Для добавления нового узла нажмите **Добавить** и введите его имя. Для удаления созданного узла выберите его и нажмите **Удалить**. Для переименования узла щелкните по нему два раза левой кнопкой мыши или нажмите F2.

Организационная структура

Имя

Q

▲

ООО Тестовая компания

Бухгалтерия

Кадры

Юристы

▲

Филиал в Воронеже

Менеджеры

Производство

Филиал в Самаре

+

Добавить

-

Удалить

Политики

☐

Общее имя(CN)

Контейнер

-

+

Добавить

-

Удалить

Добавить узел организационной структуры

Имя

Добавить

Отмена

Для добавления объектов в узел нажмите **Добавить** в правой части окна редактирования организационной структуры. При создании структуры используются объекты каталога пользователей: контейнеры, подразделения и группы Active Directory, папки Центра Регистрации КриптоПро УЦ.

Ниже на рисунке приведен пример структуры организации, в узел которой добавлена группа пользователей Active Directory. Для добавления объекта в узел нажмите **Добавить**, укажите его тип и имя. Для удаления объекта выберите его и нажмите **Удалить**.

Имя

Поиск

ООО Тестовая компания

Бухгалтерия

Кадры

Юристы

Филиал в Воронеже

Менеджеры

Производство

Филиал в Самаре

Добавить

Удалить

Политики

☐

Общее имя(CN)

Контейнер

☐

 Бухгалтеры головного офиса

indeed-id.local

Добавить

Удалить

Добавить объекты каталога

☐ Контейнер

☒ Группа

☐ Пользователь

indeed-id.local

Общее имя(CN)

Поиск

Добавить

Отмена

Назначенная на узел политика отображается в правой части окна:

- ООО Тестовая компания
 - Бухгалтерия
 - Кадры
 - Юристы
- Филиал в Воронеже
 - Менеджеры
 - Производство
- Филиал в Самаре

Политики Базовая политика

	Общее имя(CN)	Контейнер
☐	Бухгалтеры головного офиса	indeed-id.local

Роли

В данном разделе настраиваются полномочия администраторов и операторов доступные в Консоли управления Indeed Certificate Manager.

✔ Для первоначальной настройки привилегий используйте учетную запись, указанную при настройке параметров системы в разделе [Администратор ролей](#) Мастера настройки Indeed CM.

Роли могут быть **глобальными** (распространяться на все политики использования устройств) и **локальными** (распространяться только на указанные политики). Добавление локальных ролей в политики осуществляется в разделе **Назначения политик**. Предусмотренными являются глобальные роли **Администраторов** и **Операторов**.

Роли

[+ Создать роль](#)

Имя	Состав роли
 Администраторы	 
 Операторы	 

Для членов роли задается набор разрешенных и запрещенных действий. По умолчанию предустановленная роль администраторов имеет максимальные полномочия, а операторы ограничены в правах на конфигурирование системы. Для изменения роли нажмите . Пользователи включаются в состав роли персонально или через членство в группах Active Directory.

Состав глобальных ролей формируется при их создании или редактировании. Состав локальных ролей задается при добавлении роли в политику в разделе **Назначения политик**.

Для добавления пользователей в глобальную роль и настройки привилегий:

1. Нажмите **Добавить**.
 - Выберите **Группу безопасности** Active Directory.
 - Укажите **Общее имя** (CN) или **Логин** (sAMAccountName) пользователя.

2. Нажмите **Добавить**:

Администраторы

Редактировать роль

Имя

Администраторы

Тип

☐ Локальная

☒ Глобальная

Состав роли

-

+ Добавить

☒ Группа

☐ Пользователь

demo.local

Domain

Q

☐	Общее имя(CN)	Контейнер
☐	Domain Computers	demo.local/Users
☐	Domain Controllers	demo.local/Users
☒	Domain Admins	demo.local/Users
☐	Domain Users	demo.local/Users
☐	Domain Guests	demo.local/Users

Добавить

Отмена

3. Задайте **Привилегии** для членов роли:

Редактировать роль

Имя

Администраторы

Тип

☐ Локальная ☒ Глобальная

Состав роли

 Domain Admins

demo.local/Users

✕

[+ Добавить](#)

Привилегии

Привилегия	Разрешить	Запретить
▼ Пользователь	☒	☐
Поиск пользователей	☒	☐
Просмотр пользователя	☒	☐
Разблокировка пользователя	☒	☐
Сброс ответов на секретные вопросы	☒	☐
Загрузка фото	☒	☐
Сброс пароля пользователя	☒	☐
Назначение пользователя УЦ	☒	☐
► Конфигурация	☒	☐
► Журнал событий	☒	☐
► Устройство	☒	☐
► Агенты	☒	☐

Сохранить

Отмена

4. Нажмите **Сохранить** для применения внесенных изменений.

 Тип роли (глобальная или локальная) нельзя изменить после создания роли.
Состав и набор привилегий доступны для изменения при редактировании роли.

Теги

Теги необходимы для более гибкого учета устройств (USB-токенов, смарт-карт) в организации.

Для создания тега нажмите **Создать тег**, укажите **Имя** и нажмите **Создать**:

Теги

+ Создать тег

Создать тег

Имя

Создать

Отмена

Созданные теги возможно назначить на устройство:

- [При пакетном добавлении устройств](#)
- [При выпуске устройства](#)
- [При просмотре содержимого устройства](#)
- [При изменении тегов на вкладке **Устройства**](#)
- [В карточке пользователя](#)

Поиск устройств по заданным тегам осуществляется на вкладке [Устройства > Расширенный поиск](#).

Шаблоны печати

Шаблоны печати предназначены для заполнения и печати документов СКЗИ, запроса на сертификат, самого сертификата и документов пользователя.

Для создания шаблона нажмите **Добавить шаблон печати**:

Шаблоны печати

[+ Добавить шаблон печати](#)

Добавить шаблон печати

Имя

Тип

Дистрибутив 

Файл шаблона печати



Укажите произвольное **Имя** и выберите **Тип**:

СКЗИ:

- Дистрибутив
- Лицензия
- Документация
- Ключевой документ
- Ключевой носитель
- Пользовательский

Сертификат:

- Запрос на сертификат
- Сертификат
- Запрос на отзыв сертификата

Пользователь:

- Пользовательский документ

Загрузите **Файл шаблона печати** и нажмите **Добавить**.

 Для типов объектов СКЗИ поддерживаются шаблоны в формате RTF. Создание шаблона печати описано в разделе [Настройка шаблона печати СКЗИ](#).

Для типов объектов сертификат и пользователь поддерживаются шаблоны в формате XSL. Загруженные шаблоны печати **Запроса на сертификат**, **Сертификата** и **Запроса на отзыв сертификата** задаются в [Параметрах шаблонов сертификатов](#).

Шаблоны печати

[+ Добавить шаблон печати](#)

Имя	Тип	
Ключевой документ	Ключевой документ	
Запрос MSCA	Запрос на сертификат	
Шаблон для сертификатов MSCA	Сертификат	

Для редактирования добавленного шаблона нажмите  , для удаления нажмите  .

Настройка шаблона печати СКЗИ

Подстановка необходимых атрибутов в поля документа для автоматического заполнения, осуществляется с помощью **Закладок** (Bookmark) заданных в Microsoft Word.

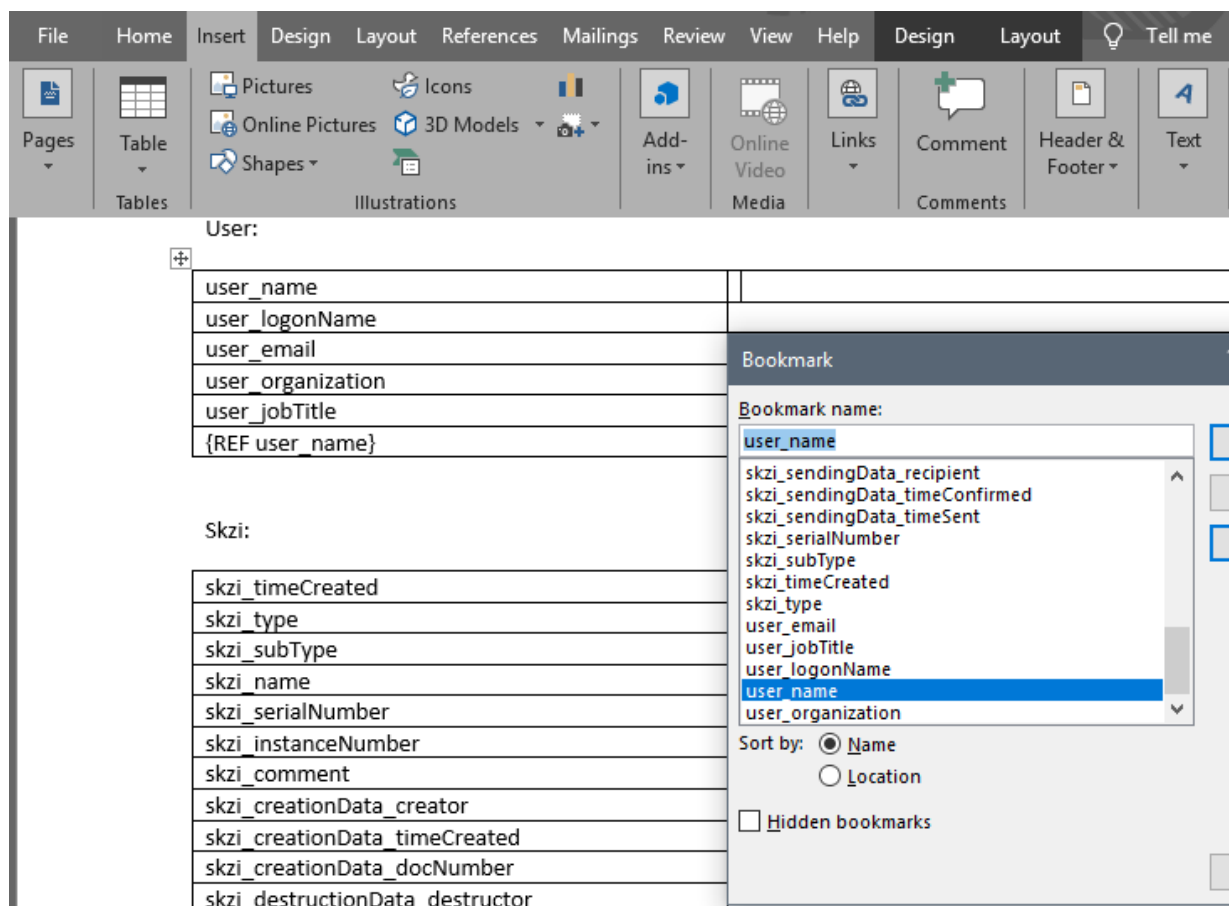
❗ Поддерживаются шаблоны в формате RTF (заполненный данными шаблон также будет доступен в формате RTF).

✅ Для настройки шаблона печати воспользуйтесь демонстрационным шаблоном (прикрепленным к статье), в котором перечислены все атрибуты доступные для подстановки. В левом столбце указаны имена атрибутов, в правом подставлены **Закладки** (Bookmarks) для данных атрибутов.

Пример настройки шаблона печати:

1. Откройте в Microsoft Word шаблон печати (например, "Акт установки СКЗИ"), в который необходимо добавить поля для автоматического заполнения из журнала СКЗИ.
2. Переведите курсор в заполняемое поле и нажмите **Вставка > Закладка** (Insert > Bookmark).

3. Выберите необходимый атрибут для подстановки (например, user_name).



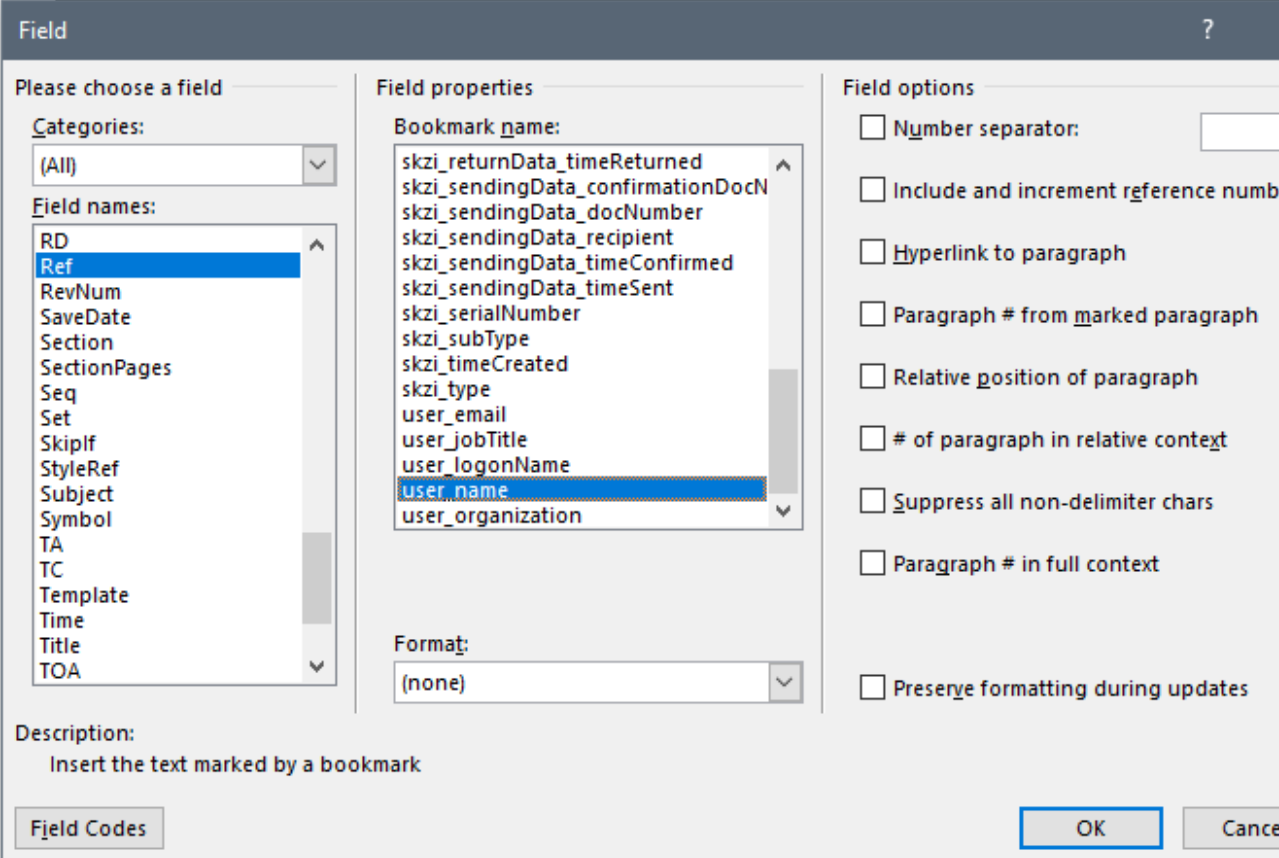
4. В поле **Имя закладки:** (Bookmark name:) укажите требуемый атрибут (user_name) и нажмите **Добавить** (Add).

5. Повторите аналогичные действия для остальных полей.

6. Для повторного использования одного значения в рамках документа необходимо применить ссылку на закладку (Bookmark):

- Нажмите Ctrl+F9 в требуемом поле
- Нажмите правой кнопкой мыши по {} и выберите **Изменить поле...** (Edit Field...)

user_name	
user_logonName	
user_email	
user_organization	
user_jobTitle	
{REF user_name}	{ }



Field

Please choose a field

Categories: (All)

Field names:

- RD
- Ref**
- RevNum
- SaveDate
- Section
- SectionPages
- Seq
- Set
- SkipIf
- StyleRef
- Subject
- Symbol
- TA
- TC
- Template
- Time
- Title
- TOA

Field properties

Bookmark name:

- skzi_returnData_timeReturned
- skzi_sendingData_confirmationDocN
- skzi_sendingData_docNumber
- skzi_sendingData_recipient
- skzi_sendingData_timeConfirmed
- skzi_sendingData_timeSent
- skzi_serialNumber
- skzi_subType
- skzi_timeCreated
- skzi_type
- user_email
- user_jobTitle
- user_logonName
- user_name**
- user_organization

Format: (none)

Field options

- ☐ Number separator:
- ☐ Include and increment reference numb
- ☐ Hyperlink to paragraph
- ☐ Paragraph # from marked paragraph
- ☐ Relative position of paragraph
- ☐ # of paragraph in relative context
- ☐ Suppress all non-delimiter chars
- ☐ Paragraph # in full context
- ☐ Preserve formatting during updates

Description: Insert the text marked by a bookmark

Field Codes OK Cancel

- В **Поля:** (Field names:) укажите значение **Ref**, в **Имя закладки:** (Bookmark name:) выберите требуемую закладку (user_name) и нажмите **OK**.



Перед печатью заполненного документа необходимо повторно обновить все поля (**Ctrl+A + F9**) для подстановки значений, на которые указаны ссылки на **Закладки** {Ref Bookmark name:}.



Печать сводных данных (по нескольким СКЗИ или пользователям) не предусмотрена.

Создание дополнительных полей

Если в журнале учета СКЗИ вашей организации присутствуют поля, которые необходимо заполнить, но в списке атрибутов Indeed CM нет соответствующего, то имеется возможность создавать дополнительные поля.

 Дополнительные поля задаются в **Мастере настройки Indeed CM** в разделе **Журнал учета СКЗИ** и после создания будут доступны при **редактировании СКЗИ**.

1. Запустите **Мастер настройки Indeed CM** на сервере.
2. Перейдите в раздел **Журнал учета СКЗИ**.
3. Нажмите **Добавить** и укажите:
 - **ID** (значение, которое необходимо будет указать в **Имя закладки: (Bookmark name:)**). Допустимы латинские имена

 При добавлении дополнительных полей в документ необходимо указать Имя закладки формата **skzi_<id>**. Например, для создаваемого поля **demo** **Имя закладки: (Bookmark name:)** будет **skzi_demo**, для **customField1**: **skzi_customField1**.

- **Атрибут** (Отображаемое имя поля в журнале СКЗИ)

Журнал учета СКЗИ

☒ Вести журнал учета СКЗИ

Укажите имена дополнительных атрибутов, которые будут использоваться при ведении учета СКЗИ в вашей организации

ID	Атрибут	Добавить
customField1	Номер кабинета	Изменить
customField2	АРМ	Удалить
customField3	Формуляр	

Indeed CM позволяет создавать дополнительные атрибуты при ведении учета средств криптографической защиты информации в организации. Такими атрибутами могут быть: Номер АРМ, Номер кабинета, Формуляр и т.д..

Журнал учета СКЗИ

ID

demo

Атрибут

Адрес: Улица

Добавить

Отмена

4. Для сохранения нажмите **Добавить**.

5. Перейдите в раздел **Подтверждение** и нажмите **Применить**.

Файл

Изменено

Microsoft Word 97 документ demo_template.rtf

сен 03, 2020 by Mikhail Yakovlev

Журналы учета (Конфигурация)

В данном разделе настраиваются:

- [Справочники](#)
- [Шаблоны журналов](#)

Справочники

Под **Справочником** понимается перечень значений, которые могут быть указаны при заполнении поля в одном или нескольких **Журналах учета**.

Для создания справочника нажмите **Создать справочник**, укажите его **Имя**, добавьте в него **Значения** и нажмите **Создать**:

Справочники

+ Создать справочник

Создать справочник

Имя

Должность

Значения

CFO



СТО



QA Engineer



CEO



Product Manager



+ Добавить

Значение

Support Engineer

Добавить

Отмена

Создать

Отмена

Для редактирования созданного Справочника и его значений нажмите , для удаления - .



Удалить используемый **Справочник** или используемое **Значение** невозможно.

Имя

Должность

Редактировать справочник

Имя

Должность

Значения

CFO	 
CTO	 
QA Engineer	 

Значение

QA Engineer

Сохранить

Отмена

CEO	 
Product Manager	 
Support Engineer	 

 Добавить

Сохранить

Отмена

Нажмите **Сохранить** для применения внесенных изменений.

Шаблоны журналов

Под журналом учёта в Indeed Certificate Manager понимается набор полей, содержащих данные об устройствах и сертификатах, их владельцах и системах, в которых эти устройства/сертификаты используются.

Для создания шаблона журнала учета:

1. Нажмите **Создать шаблон журнала**
2. Укажите его **Имя**
3. Выберите **Тип объектов**:
 - Устройство
 - Сертификат
 - Пользовательский
4. Выберите **Политики**:

[+ Создать шаблон журнала](#)

Создать шаблон журнала

Имя

Устройства

Тип объектов

Устройство ▼

Политики

- ▼

Поля

Имя	Способ заполнения	Тип	Уникальное	Обязательное	Поиск

[+ Добавить поле](#) [+ Добавить типовые поля](#)

Создать

Отмена

5. **Добавьте поля** или выберите **Добавить типовые поля** для типов объектов **Устройство** и **Сертификат**:

✓ Поле представляет собой колонку журнала, в которой содержится информация, относящаяся к устройству/сертификату.

⚠ Для **Типа объектов: Устройство** **Обязательным** и **Уникальным** полем является **Серийный номер устройства**.

Для **Типа объектов: Сертификаты** обязательными полями являются **Серийный номер сертификата** и **Серийный номер устройства**. Данные поля не являются уникальными, так как на одном устройстве могут быть записаны несколько сертификатов или на разных устройствах может быть записан **Общий сертификат**.

- a. Укажите **Имя** создаваемого поля
- b. Выберите **Способ заполнения**:
 - **Вручную**
 - **Автоматически** (выберите **Выражение** из выпадающего списка подходящие для выбранного типа журнала)
 - **Справочник** (выберите созданный **Справочник** из выпадающего меню)
- c. Выберите **Тип значения**:
 - **Текст**
 - **Дата**
- d. Задайте параметры поля:
 - **Уникальное** (Если в данном поле присутствуют уникальные значения)
 - **Обязательное** (Обязательное к заполнению поле при редактировании)
 - **Поиск** (Поиск по данному полю на вкладке **Журналы учета**)
- e. Нажмите **Добавить**

⚠ При редактировании уже добавленного поля доступно только изменение его **Имени** и набора параметров: **Уникальное**, **Обязательное**, **Поиск**.

+

Добавить поле

+

Добавить типовые поля

Имя

Модель

Способ заполнения

Автоматически

Выражение

Модель устройства

Тип значения

Текст

☐ Уникальное

☐ Обязательное

☒ Поиск

Добавить

Отмена

 Автоматическое заполнение **Модели устройства** доступно только для устройств **JaCarta** и **eToken**, если в типах данных карт добавлено разделение по различным моделям. Для остальных моделей устройств необходимо использовать выражение **Тип устройства**.

6. Нажмите **Создать** для сохранения шаблона.

Для редактирования шаблона журнала выберите  , если необходимо удалить шаблон нажмите  .



Редактировать шаблон журнала

Имя

Тип объектов

Политики

Поля

Имя	Способ заполнения	Тип	Уникальное	Обязательное	Поиск	
Серийный номер устройства	Автоматически : Серийный номер устройства	Текст	✓	✓	✓	
Тип устройства	Автоматически : Тип устройства	Текст		✓	✓	
Имя пользователя устройства	Автоматически : Имя пользователя устройства	Текст		✓	✓	
Комментарий устройства	Автоматически: Комментарий устройства	Текст			✓	
Модель устройства	Автоматически : Модель устройства	Текст				

[+ Добавить поле](#)

При редактировании созданного шаблона имеется возможность:

- Изменить **Имя** шаблона
- Изменить **Политики**
- **Добавить**, **Удалить** поля или **Отредактировать** уже добавленные поля

 При удалении поля в шаблоне, оно будет удалено для всех записей в [Журнале учета](#).

Помощь и поддержка

В данном разделе отображается информация о конфигурации Indeed Certificate Manager и ссылки на порталы технической поддержки:

- Версия сервера
- Тип каталога пользователей
- Тип хранилища данных
- Тип журнала событий

Ссылки на порталы технической поддержки:

- Портал технической поддержки
- Документация
- База знаний

Справочник по разделам консоли управления

Сводная информация

Пользователи

- [Карточка пользователя](#)

Устройства

- [Добавление устройства](#)
- [Выпуск устройства](#)
- [Удаление устройства](#)
- [Инициализация пустых устройств](#)
- [Изменение тегов](#)
- [Пакетное добавление устройств](#)

Агенты

- [Профиль Агента](#)
- [Назначение устройства в Агенте](#)
- [Контроль за использованием устройств](#)
- [Назначение задач](#)
- [Мониторинг подключенных устройств](#)
- [Журнал событий](#)

СКЗИ

- [Операции с СКЗИ](#)
- [Пакетный импорт СКЗИ](#)

Журналы учета

Журнал

- [Список событий](#)

Сводная информация



Раздел доступен при включенной опции [Сводная информация о системе](#) в разделе **Общие функции** Мастера настройки Indeed CM и предоставленной привилегии [Просмотр сводной информации](#) членам Роли.

В разделе отображается сводная информация о Indeed CM с возможностью перехода в соответствующие разделы системы:

Лицензии ⚠

Тип	Количество	Используется	Осталось
General	50	46	4
AirKey	50	16	34
CryptoPro DSS	50	4	46

Агенты

Общее	Агенты	Задачи
Зарегистрировано 18	Активные 17	В ожидании 4
В ожидании 1	С устройствами 17	Выполняются 0

Устройства

Общее	С истекающими сертификатами	С истекшими сертификатами	Требуют обновления
Выпущено 64	Управляемые 9	7	Сертификаты 9
Назначено 11	Общие 8	1	Смена политики 8
В ожидании 7	Отслеживаемые 3	0	Данные коннекторов 12
Выключено 6			

Сервисные сертификаты ⚠

Издатель	Субъект	Действителен до	Состояние
demo-DC-CA	serviceca	26.06.2020 13:29	Истекает
Indeed Demo CA	servicecp	27.03.2023 9:47	Действительный
Sub-TESTCA20-2012-CA	Operator	21.02.2020 14:28	Истек

Пользователи

Заблокированы	4
Не заданы секретные вопросы	12

Лицензии

- Тип лицензий
- Общее количество
- Количество используемых лицензий
- Количество оставшихся лицензий

Лицензии ⚠			
Тип	Количество	Используется	Осталось
General	50	46	4
AirKey	50	16	34
CryptoPro DSS	50	4	46



Иконка предупреждения ⚠ появляется в случаях:

- Не добавлены лицензии в систему.
- Осталось 10% от общего количества лицензий.
- Все лицензии использованы.

Агенты



Поле отображается если выполнена **Настройка клиентского агента Indeed CM**.

Количество агентов по их статусу:

- **Зарегистрирован**
- **Ожидает регистрации**

По доступности связи с сервером Indeed CM:

- **Активные** - агенты, которые обращались к серверу в Indeed CM за последние 5 минут.
- **С устройствами** - в сессиях агентов имеется хоть одно устройство.

Количество назначенных задач на агенты по статусу их выполнения:

- **В ожидании** - задача ожидает выполнения (включения рабочей станции с Агентом, подключения устройства к рабочей станции или завершения выполнения предыдущей задачи).
- **Выполняются** - агент приступил к выполнению задачи.

Агенты					
Общее		Агенты		Задачи	
Зарегистрировано	18	Активные	17	В ожидании	4
В ожидании	1	С устройствами	17	Выполняются	0

Устройства

Устройства по состояниям:

- **Выпущено**
- **Назначено**
- **В ожидании**
- **Выключено**

Количество устройств по статусу содержимого (с истекающими и с истекшими сертификатами):

- **Управляемые** - сертификаты, выпущенные через Indeed CM.
- **Общие** - сертификаты, добавленные в политику использования устройств в .pfx формате и записанные на устройство.
- **Отслеживаемые** - сертификаты, выпущенные и записанные на устройство вне Indeed CM.

Устройства, требующие обновления:

- **Сертификаты** - в политике использования устройств изменился набор **Обязательных** шаблонов сертификатов.
- **Смена политики** - на пользователя, на которого было выпущено устройство, была назначена новая политика использования устройств.
- **Данные коннекторов** - после выпуска устройства в действующей политике была включена\выключена [интеграция с Indeed Access Manager](#) и\или [интеграция с Secret Net Studio](#).

Устройства					
Общее		С истекающими сертификатами		С истекшими сертификатами	
Выпущено	64	Управляемые	9		7
Назначено	11	Общие	8		1
В ожидании	7	Отслеживаемые	3	0	
Выключено	6				
				Требуют обновления	
				Сертификаты	9
				Смена политики	8
				Данные коннекторов	12

Сервисные сертификаты

Сертификаты, выданные для сервисных учетных записей при настройке интеграции с Удостоверяющими Центрами: Microsoft CA, КриптоПро УЦ 2.0.



Иконка предупреждения  отображается в случаях, если хотя бы один из сервисных сертификатов истекает (10% от срока действия) или истёк.

Сервисные сертификаты 			
Издатель	Субъект	Действителен до	Состояние
demo-DC-CA	serviceca	26.06.2020 13:29	Истекает
Indeed Demo CA	servicecp	27.03.2023 9:47	Действительный
Sub-TESTCA20-2012-CA	Operator	21.02.2020 14:28	Истек

Пользователи

Отображение количества пользователей по состоянию в базе Indeed CM с возможностью перехода в раздел расширенного поиска пользователей:

- **Заблокированы** - пользователи, которые исчерпали попытки ответов на секретные вопросы при выполнении [Online-разблокировки устройства](#) или выполнении входа в сервис [Дистанционного самообслуживания](#) (Remote Self Service).
- **Не заданы секретные вопросы** - пользователи, у которых не заданы ответы на секретные вопросы.

Пользователи	
Заблокированы	4
Не заданы секретные вопросы	12

Пользователи

Раздел **Пользователи** открывается автоматически при переходе на страницу Консоли управления (Management Console). Для выполнения действия с устройством, имеющего отношение к пользователю системы, необходимо выполнить поиск нужного пользователя среди всех пользователей каталога.

Простой поиск пользователей

Выполняется по заданным в строке символам: логина (sAMAccountName), общего имени (Common name), имени, фамилии и адресу электронной почты. Для поиска всех пользователей каталога введите символ *. Результаты поиска выводятся после нажатия

кнопки  или клавиши **Enter** в виде таблицы с полями:

- Общее имя(CN)
- Имя и фамилия
- E-mail
- Контейнер
- Устройства

Поиск пользователя

Пользователь

Расширенный



Общее имя(CN)	Имя и фамилия	E-mail	Контейнер	Устройства	
Evgeniy Belov	Evgeniy Belov	evgeniy.belov@demo.com	demo.local/Users	Rutoken ECP, 0894130607 Registry, 62950d0309864edbe50d657ee07b5473 WHfB, aa3190947c8f4f778c7eb53112f088e5	

Переход к просмотру свойств пользователя (**Карточке пользователя**) осуществляется по щелчку на **Общее имя** (CN) пользователя в результатах поиска.

Расширенный поиск пользователей

Расширенный поиск может выполняться по нескольким параметрам: логину (sAMAccountName), общему имени (Common name), имени, фамилии и контейнеру. Поиск может осуществляться как по одному параметру (например, фамилии) так и по нескольким (например, все пользователи с фамилией, начинающейся на "В", находящиеся в указанном контейнере или подразделении).

Поиск пользователя

Пользователь

Расширенный

Общее имя(CN)

Общее имя(CN)

Контейнер

Имя контейнера

Логин

Логин

Имя

Имя

Фамилия

В

☐ Заблокирован в Indeed CM

☐ Не заданы секретные вопросы

☐ Отображать отключенные учетные записи

Общее имя(CN)

Имя и фамилия

E-mail

Контейнер

Устройства

Evgeniy Belov

Evgeniy Belov

evgeniy.belov@demo.com

demo.local/Users

Rutoken ECP, 0894130607
Registry, 62950d0309864edbe50d657ee07b5473
WHfB, aa3190947c8f4f778c7eb53112f088e5

Anna Berezova

Anna Berezova

anna.berezova@demo.com

demo.local/Users

При включенной опции **Отображать отключенные учетные записи** в результатах поиска будут отображены активные и отключенные учетные записи пользователей Active Directory.

При включенных опциях **Заблокирован в Indeed CM** и **Не заданы секретные вопросы** будет выполнен поиск пользователей по состоянию в базе Indeed CM:

- Заблокированные - это пользователи, которые исчерпали попытки ответов на секретные вопросы.
- Пользователи, у которых не заданы ответы на секретные вопросы.

Пользователь

Расширенный

Общее имя(CN)

Общее имя(CN)

Контейнер

Имя контейнера

Логин

Логин

Имя

Имя

Фамилия

Фамилия

☒ Заблокирован в Indeed CM
 ☒ Не заданы секретные вопросы
 ☐ Отображать отключенные учетные записи

Общее имя(CN)	Имя и фамилия	E-mail	Контейнер	Устройства	
Maria Ivanova	Maria Ivanova	maria.ivanova@demo.com	demo.local/Users	eToken PRO Java 72K, 01cec45d AirKey, aad4aafef4db414f	
Evgeniy Belov	Evgeniy Belov	evgeniy.belov@demo.com	demo.local/Users	Rutoken ECP, 0894130607 WHfB, aa11e3e97f1b4a4cbd70b81c1b162866 Registry, 62950d0309864edbe50d657ee07b5473	

Результаты поиска пользователей могут быть сохранены в виде файла. Для создания файла с результатами поиска нажмите и выберите формат (PDF или CSV). Сохраните полученный файл.

Карточка пользователя

В карточке пользователя содержится общая информация о пользователе: данные из профиля Active Directory (в случае использования Active Directory в качестве каталога пользователей Indeed Certificate Manager), сведения по устройствам, средствам криптографической защиты информации (СКЗИ) и последние события пользователя. Если устройств у пользователя нет, оператор системы сможет их ему назначить или выпустить.

Доступные операции:

- [Загрузка фотографии](#)
- [Связь пользователя AD с пользователями Центра Регистрации КриптоПро УЦ 2.0 и КриптоПро DSS](#)
- [Разблокировка пользователя](#)
- [Сброс ответов на секретные вопросы](#)
- [Сброс пароля пользователя](#)
- [Выпуск устройств](#)
- [Назначение устройства](#)
- [Сброс PIN-кода устройства](#)
- [Разблокировка устройства](#)
- [Выключение и включение устройства](#)
- [Отзыв устройства](#)
- [Изъятие устройства](#)
- [Замена устройства](#)
- [Обновление устройства](#)
- [Выпуск устройства с печатью](#)
- [Массовый выпуск смарт-карт](#)
- [Назначенные СКЗИ](#)
- [События пользователя](#)



Белов Евгений Александрович

Логин DEMO\Evgeniy.Belov
Путь demo.local/Indeed CM RU/Белов Евгений Александрович
Политика Базовая политика
E-mail evgeniy.belov@demo.com
Телефон +7 (905) 288-58-23

[Загрузить фотографию](#) [Пользователь КриптоПро 2.0](#) [Пользователь КриптоПро DSS](#) [Сбросить ответы на секретные вопросы](#)
[Сбросить пароль пользователя](#)

Назначенные устройства

▼ **Rutoken S, 0755398982** Evgeniy Belov Выпущено

[Сбросить PIN-код](#) [Разблокировать](#) [Выключить](#) [Отозвать](#) [Заменить](#) [Заменить на AirKey](#) [Обновить](#)

[Заблокировать](#) [Сменить PIN-код администратора](#)

Комментарий

Политика [Базовая политика](#)

PIN-код администратора

Теги

Сертификаты

Шаблон	УЦ	Действителен до	Состояние	
Вход по смарт-карте	demo-DC-CA	11.11.2020 16:16	Действительный	

> **eToken PRO Java 72K (JC1.0b) (SafeNet eToken 5110), 024084ab** Назначено

[Выпустить устройство](#) [Выпустить AirKey](#) [Назначить устройство](#) [Выпустить устройство КриптоПро DSS](#)

Назначенные СКЗИ

Нет назначенных СКЗИ

[Добавить СКЗИ](#) [Редактировать СКЗИ](#) [Уничтожить/изъять СКЗИ](#)

Последние события

	Время	Событие	Сервис	Тип устройства	Серийный номер	Инициатор
▶	12.11.2019 17:35:26	Назначение устройства	Консоль управления	eToken PRO Java 72K (JC1.0b)	024084ab	DEMO\Ad
▶	12.11.2019 17:33:07	Отвязка устройства	Консоль управления	AirKey	1f67c0aa16514a25	DEMO\Ad
▶	12.11.2019 17:33:06	Очистка устройства	Консоль управления	AirKey	1f67c0aa16514a25	DEMO\Ad
▶	12.11.2019 17:33:06	Отзыв устройства	Консоль управления	AirKey	1f67c0aa16514a25	DEMO\Ad
▶	12.11.2019 17:32:52	Выпуск устройства	Консоль управления	AirKey	1f67c0aa16514a25	DEMO\Ad

[Просмотреть все](#)

Загрузка фотографии

Если профиль пользователя в Active Directory содержит фотографию, то она будет отображена в карточке пользователя. Для загрузки фотографии вручную нажмите **Загрузить фотографию**.



- Фотография пользователя может быть записана в атрибуты **thumbnailPhoto** или **jpegPhoto**. Выбор атрибута осуществляется в разделе **Каталог пользователей > Active Directory > Расширенные настройки** Мастера настройки Indeed CM.
- Сервисная учетная запись для работы с каталогом пользователей в Active Directory (**servicecm**) должна обладать правами на запись для выбранного атрибута (см. раздел **Настройка каталога пользователей в Active Directory**).
- Размер загружаемой фотографии не должен превышать 100Кб.

Связь пользователя AD с пользователями Центра Регистрации КriptoПро УЦ 2.0 и КriptoПро DSS

Если в используемой вами конфигурации каталог пользователей Indeed Certificate Manager не совпадает с каталогом пользователей удостоверяющего центра (например, пользователям Active Directory необходимо выпускать сертификаты КriptoПро УЦ 2.0), то для выпуска устройства необходимо установить связь с каталогом нужного удостоверяющего центра.

Необходимость привязки пользователя к каталогу удостоверяющего центра определяется опцией [Устанавливать привязку между пользователем УЦ и пользователем каталога](#) в разделе КriptoПро 2.0 политики использования устройств. Один и тот же пользователь Active Directory может быть связан с каталогами различных УЦ.

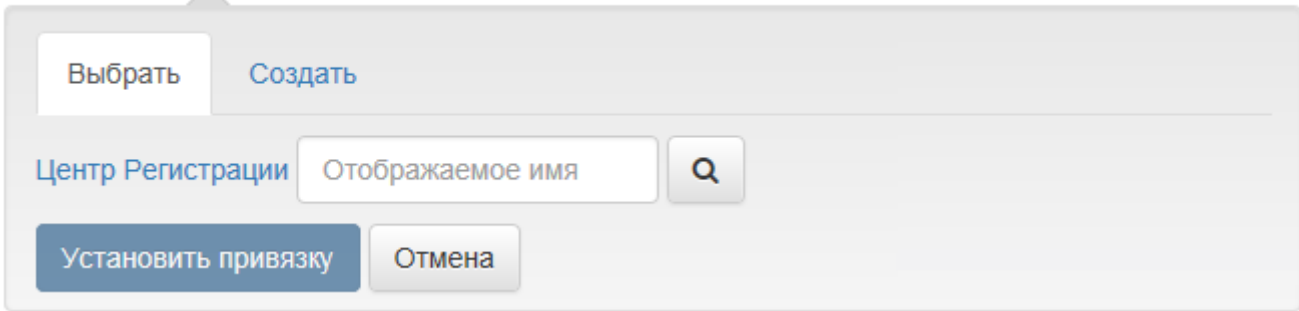
Пользователь Indeed CM (не важно, в каком каталоге он расположен: Active Directory или КriptoПро 2.0) может быть связан с любым пользователем удостоверяющего центра КriptoПро 2.0. Если каталог УЦ, с которым необходимо установить связь, не содержит пользователей, то при помощи Indeed CM их можно создать.

Связать пользователя Active Directory с пользователем КriptoПро УЦ 2.0 можно автоматически (см. опцию [Устанавливать привязку автоматически](#)) и в ручном режиме.

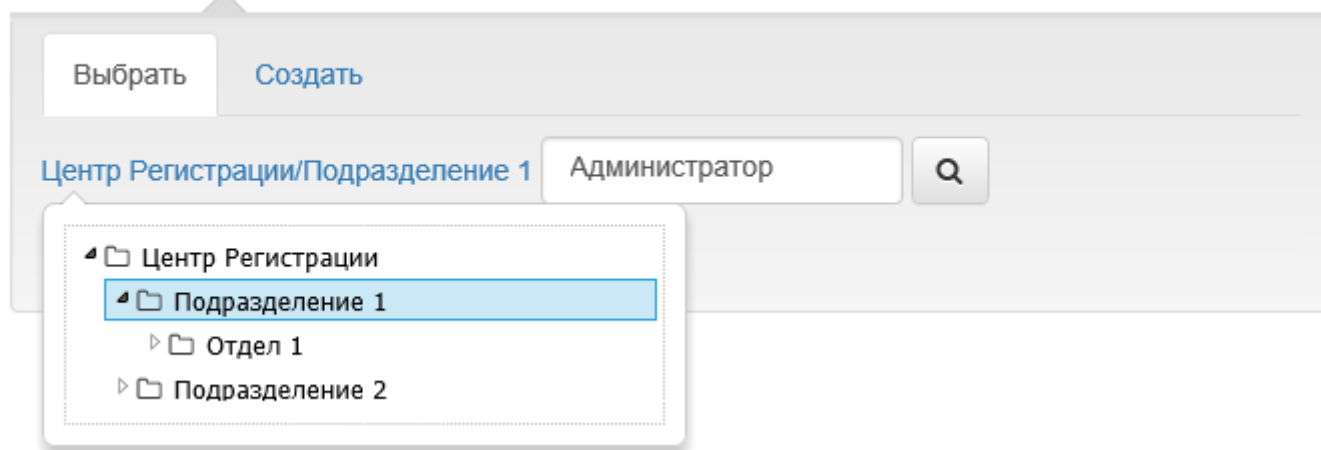
Для установки связи вручную:

1. Перейдите в карточку пользователя.
2. Нажмите **Пользователь КriptoПро 2.0:**

 Пользователь КriptoПро 2.0

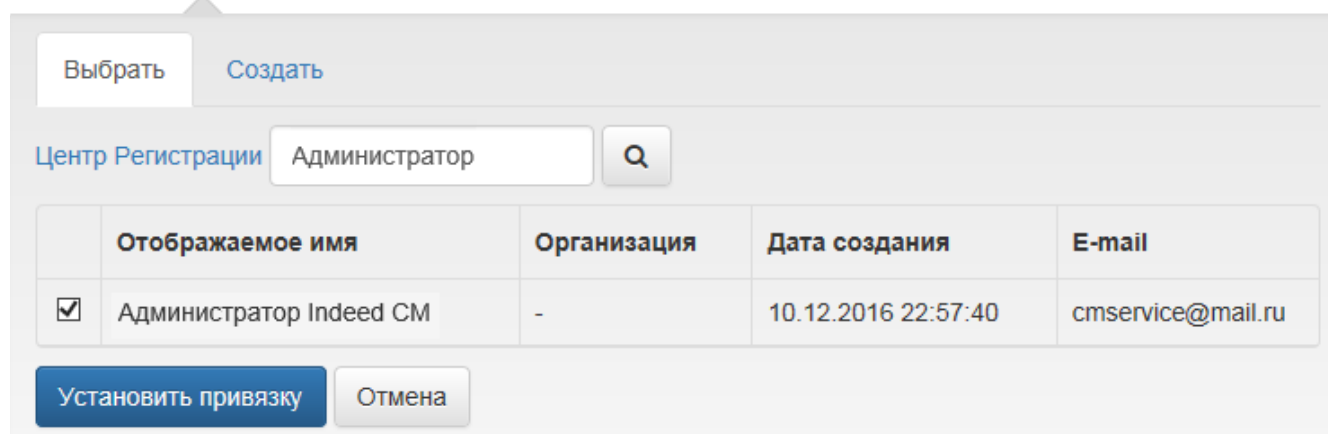


3. Введите имя пользователя центра регистрации КriptoПро УЦ 2.0 и укажите папку, в которой располагаются пользователи:



4. Нажмите кнопку поиска.

5. Отметьте нужного пользователя в результатах поиска и нажмите **Установить привязку**.



6. Установленную привязку можно отменить. Для этого нажмите **Пользователь КriptoПро 2.0** и затем **Отменить привязку**.

Пользователь КристоПро 2.0

Отображаемое имя	cmsservice
Папка	Центр Регистрации
Компонент	Значение
ФИО или псевдоним	Администратор Indeed CM
Адрес E-Mail	cmsservice@mail.ru
Отменить привязку Закрыть	

Для создания нового пользователя в каталоге КристоПро УЦ 2.0:

1. Перейдите в карточку пользователя.
2. Нажмите **Пользователь КристоПро 2.0** и перейдите на вкладку **Создать**. Вы можете отредактировать данные создаваемого пользователя. Перечень полей для редактирования, зависит от настроек используемого удостоверяющего центра КристоПро.

Пользователь КристоПро 2.0

Выбрать Создать

Центр Регистрации

Организация	Не задано ▼
ФИО или псевдоним	CMAdmin
Фамилия	
Имя и отчество	CMAdmin
Адрес E-Mail	
ОГРНИП	
Имя участника	CMAdmin@indeed-id.local
Создать Отмена	

 При создании пользователя КристоПро УЦ 2.0 некоторые поля свойств могут быть заполнены автоматически. Например, имя пользователя, адрес электронной почты, город, страна, организация. Эти данные Indeed CM получает из профиля пользователя Active Directory (см. раздел [Соответствия атрибутов](#) Мастера настройки Indeed CM) или из шаблона организации (см. раздел **Организации** политики использования устройств).

Разблокировка пользователя

Помимо блокировки устройства пользователя в Indeed Certificate Manager реализован и механизм блокировки учетной записи пользователя. Учетная запись пользователя блокируется в случае, если число неверных попыток ответов на секретные вопросы сравнялось с числом, заданным в параметре [Максимальное количество попыток аутентификации](#) политики использования устройств при попытке [Разблокировать устройство online](#) или выполнить вход в приложение [Дистанционное самообслуживание \(Remote Self Service\)](#).

 Заблокированный пользователь **не сможет использовать Remote Self Service и разблокировать/выключить устройство с использованием Indeed CM Credential Provider.**

Если заблокированы и устройство и пользователь, то оператор системы сможет разблокировать устройство, без разблокировки пользователя только в том случае, если в разделе Поведение политике использования устройств отключена опция [Проверять ответы на секретные вопросы](#).

В случае блокировки учетной записи пользователя, в журнал событий системы заносится соответствующая запись, а в карточке пользователя появляется соответствующий статус.



Белов Евгений Александрович Пользователь заблокирован

Логин	DEMO\Evgeniy.Belov
Путь	demo.local/Indeed CM RU/Белов Евгений Александрович
Политика	Базовая политика
E-mail	evgeniy.belov@demo.com
Телефон	+7 (905) 288-58-23

 [Загрузить фотографию](#)  [Пользователь КриптоПро 2.0](#)  [Пользователь КриптоПро DSS](#)  [Разблокировать пользователя](#)
 [Сбросить ответы на секретные вопросы](#)  [Сбросить пароль пользователя](#)  [Распечатать документ](#)

Назначенные устройства

 **Rutoken 2151, 0963474291**  Белов Евгений Александрович Выпущено

 [Выпустить устройство](#)  [Выпустить AirKey](#)  [Назначить устройство](#)  [Выпустить устройство КриптоПро DSS](#)

Для разблокировки пользователя нажмите **Разблокировать пользователя** и подтвердите действие нажатием кнопки **Разблокировать**.

Сброс ответов на секретные вопросы

Оператор Indeed Certificate Manager при необходимости может сбросить секретные вопросы пользователя и указанные ответы. В этом случае пользователь должен будет установить новые вопросы и задать ответы в приложении [Сервис самообслуживания](#) (Self Service).

Для сброса секретных вопросов пользователя:

1. В карточке пользователя нажмите **Сбросить ответы на секретные вопросы**.
2. Нажмите **Сбросить** для подтверждения действия.



Белов Евгений Александрович

Логин	DEMO\Evgeniy.Belov
Путь	demo.local/Indeed CM RU/Белов Евгений Александрович
Политика	Базовая политика
E-mail	evgeniy.belov@demo.com
Телефон	+7 (905) 288-58-23

Загрузить фотографию Пользователь КриптоПро 2.0 Пользователь КриптоПро DSS
 Сбросить ответы на секретные вопросы Сбросить пароль пользователя Распечатать документ

Вы уверены, что хотите сбросить ответы на секретные вопросы?

Сбросить

Отмена

Сброс пароля пользователя

- ✔ Отображение функции сброса пароля в карточке пользователя доступно при включении опции **Сброс пароля пользователя в Active Directory** в разделе **Общие функции** Мастера настройки Indeed CM.

Indeed Certificate Manager позволяет операторам и администраторам выполнить сброс доменного пароля пользователя. Сброс доменного пароля может использоваться в случае возникновения необходимости входа пользователя в операционную систему по паролю. Например: если пользователь забыл смарт-карту с сертификатом для аутентификации и не знает свой доменный пароль.

Для сброса пароля нажмите **Сбросить пароль пользователя**, задайте новое значение, опцию смены при первом входе (если необходимо) и время истечения срока действия пароля:

 Сбросить пароль пользователя

Новый пароль

Подтверждение пароля

☒ Пользователь должен поменять пароль при первом входе

Время истечения



Сбросить

Отмена

- ❗ Сервисная учетная запись для работы с каталогом пользователей (**servicecm**) должна обладать правами на **Сброс пароля** (Reset password) и на **Запись: pwdLastSet** (Write pwdLastSet) в Active Directory (см. раздел **Настройка каталога пользователей в Active Directory**).

Время истечения – значение, после которого пароль будет сброшен на случайное значение приложением Card Monitor.

Пароль будет состоять из:

- латинских строчных и прописных букв
- цифр
- 10 символов



Установленный пароль не будет записан в хранилище данных Indeed CM.

Выпуск устройств

Во время процедуры выпуска устройство персонализируется для пользователя: в соответствии с настройками назначенной политики использования устройств осуществляется инициализация устройства, генерируются ключевые пары, выпускаются необходимые сертификаты и происходит их запись в память устройства.

Создание запроса сертификата и запись на устройство происходят в следующем порядке:

1. Генерируется пара ключей на клиентской стороне с использованием криптопровайдера (CSP).
2. Формируется запрос на сертификат, в который вкладывается открытый ключ пользователя.
3. Запрос подписывается закрытым ключом пользователя.
4. Запрос подписывается ключом сервисной учетной записи оператора УЦ с необходимыми правами, которыми владеет сервер Indeed CM.
5. Запрос отправляется на удостоверяющий центр.
6. После одобрения на УЦ выпущенный сертификат записывается на носитель средствами криптопровайдера.

Для выпуска устройства пользователю выполните следующие действия:

1. Перейдите на вкладку **Пользователи** и выполните поиск пользователя.
2. Перейдите в карточку пользователя, щелкнув по его логину в результатах поиска.
3. Нажмите **Выпустить устройство**.

 Если политика использования устройств позволяет выбирать сертификаты для записи на устройство (опция **Необязательный сертификат** в параметрах шаблонов сертификатов), то такие сертификаты необходимо **Указать** и нажать **Далее**.

Выберите требуемые сертификаты

Microsoft

☐ Вход по смарт-карте

КриптоПро 2.0

☒ Квалифицированный пользователь

Далее

Отмена

 Если в политике использования устройств настроена [Интеграция со СМЭВ](#) и для записи на устройство выбран квалифицированный сертификат (Обязательный или необязательный), то требуется проверка данных пользователя в системе межведомственного электронного взаимодействия (СМЭВ).

4. Выполните **Проверку данных пользователя в СМЭВ**.

- **Введите данные пользователя для проверки в СМЭВ**
- Нажмите **Далее**, дождитесь окончания проверки, после чего продолжите выпуск устройства

5. Подключите устройство к компьютеру, задайте его имя и при необходимости укажите:

- **Инициализировать устройство**

 Опция **Инициализировать устройство** позволяет не только отключать инициализацию для конкретного устройства перед выпуском, но и включать ее если она выключена в разделе **Выпуск** политике использования устройств.

- **Имя устройства**

 Имя устройства может быть подставлено автоматически, если в разделе **Выпуск** в политике задана опция **Генерировать имя устройства автоматически**.

- **Комментарий к устройству**

 При включенной опции **Требовать указания комментария к устройству** в разделе **Выпуск** необходимо указать комментарий.

При включенной опции **Использовать комментарий устройства в качестве комментария пользователя к запросу на сертификат** в **Параметрах шаблона сертификата КристоПро УЦ 2.0** текст комментария будет добавлен в запрос.

- **Теги**

 Добавление тегов возможно, если они созданы администратором в разделе **Теги** на вкладке **Конфигурация**.

При включенной опции **Требовать указания тегов к устройству** в разделе **Выпуск** необходимо задать Теги.

- Если ведется учет СКЗИ, то укажите **Номер и дату документа** (приказа, распоряжения), в соответствии с которым пользователю будет изготовлено и назначено СКЗИ на пользователя. Информация об имеющихся у пользователя СКЗИ находится в разделе **Назначенные СКЗИ** карточки пользователя.
- Выберите **Организацию** пользователя, если Indeed CM использует данные шаблона организации для создания пользователя в каталоге Центра Регистрации КристоПро УЦ 2.0.
- В разделе **Дополнительно**, если устройство не добавлено в Indeed CM:

- **PIN-коды администратора и пользователя.** Значения PIN-кода пользователя и администратора могут быть пустыми. В этом случае они будут установлены в соответствии со значением в разделе [Типы устройств](#). Поддерживается ввод PIN-кодов для нескольких областей (например, для PKI и ГОСТ на устройствах JaCarta).
- **Ключ инициализации** для устройств eToken.

6. Для выпуска устройства нажмите **Выпустить**.

[+ Выпустить устройство](#) [+ Выпустить AirKey](#) [+ Назначить устройство](#)

☐ Инициализировать устройство

Имя устройства

Комментарий к устройству

Теги

Номер и дата документа
 

Устройство

[Дополнительно](#)

PIN-код пользователя

PIN-код администратора

7. Если в разделе **Выпуск** политике использования устройств включена опция [Инициализировать устройство](#), то в процессе выпуска отобразится соответствующее уведомление.

Устройство будет проинициализировано. Все данные на устройстве будут потеряны

☒ Инициализировать устройство

Имя устройства

Белов

Комментарий к устройству

Московский филиал

Теги

demo ×

Номер и дата документа

ВН-125

23.11.2021 14:49

Устройство

Актив Rutoken ECP 0: Rutoken

Дополнительно

PIN-код администратора

PIN-код администратора

Выпустить

Отмена

☒ Инициализировать устройство

Белов

Теги

Номер и дата документа

Устройство

Дополнительно ▼

ВЫПУСТИТЬ

8. После выпуска устройства в разделе **Назначенные устройства** карточки пользователя отобразятся сведения об устройстве:

- Тип и серийный номер
- Имя (если было указано)
- Комментарий (если был указан)
- Имя политики, с параметрами которой выпущено устройство
- Агенты (если устройство привязано к агентам)
- PIN-код администратора

✔ Доступно при включении опции **Просмотр SO PIN устройства** в разделе **Общие функции** Мастера настройки Indeed CM.

- Теги (если были указаны)
- Состояние (в ожидании, выпущено, выключено, отозвано)
- Записанные сертификаты: шаблон, имя центра сертификации, выдавшего сертификат, срок действия и текущее состояние

Для установки или изменения комментария нажмите , для отображения PIN-кода администратора нажмите .




Rutoken S, 0755398982


 Evgeniy Belov

Выпущено

Сбросить PIN-код
 Разблокировать
 Выключить
 Отозвать
 Заменить

Заменить на AirKey
 Обновить
 Заблокировать
 Сменить PIN-код администратора

Комментарий

Московский филиал 

Политика

Базовая политика

PIN-код администратора



Теги

rutoken

demo 

Сертификаты

Шаблон	УЦ	Действителен до	Состояние
Вход по смарт-карте	demo-DC-CA	14.04.2020 12:01	Действительный 




Rutoken ECP, 0756770190


 Evgeniy Belov

В ожидании

Если запрос на сертификат пользователя требует одобрения оператора удостоверяющего центра (см. раздел **Жизненный цикл устройств**), то текущее состояние этого запроса отобразится в карточке пользователя.

 Все возможные состояния сертификатов, закрытых ключей, запросов на сертификаты с их описанием приведены в разделе **Состояния сертификатов**.

 **Rutoken ECP, 0756770190**

 Evgeniy Belov

В ожидании

Отозвать

Заблокировать

Сменить PIN-код администратора



Комментарий

Московский филиал 

Политика

Базовая политика

PIN-код администратора



Теги

demo 

Сертификаты

Шаблон	УЦ	Действителен до	Состояние	
Вход по смарт-карте	demo-DC-CA	15.04.2020 14:46	Действительный	 
Пользователь со смарт-картой	demo-DC-CA		В ожидании	

9. После одобрения запроса на сертификат оператором удостоверяющего центра состояние запроса изменится на **Одобен**. После чего выпуск устройства может быть продолжен: станет доступна кнопка **Продолжить выпуск**.

 Даже если один из сертификатов был автоматически одобрен (находится в состоянии **Действительный**), он будет записан на устройство только после нажатия на **Продолжить выпуск**.
Выпуск устройства невозможен, пока оператором УЦ не будет одобрен каждый запрос на сертификат.

Rutoken ECP, 0756770190

Evgeniy Belov

В ожидании

Отозвать

Продолжить выпуск

Заблокировать

Сменить PIN-код администратора

Комментарий

Московский филиал

Политика

Базовая политика

PIN-код администратора

Теги

demo

Сертификаты

Шаблон	УЦ	Действителен до	Состояние
Вход по смарт-карте	demo-DC-CA	15.04.2020 14:46	Действительный
Пользователь со смарт-картой	demo-DC-CA		Одобен

10. По завершению процесса выпуска устройства будет отображен **случайный PIN-код пользователя** если политика выпуска устройства предполагает создание случайного PIN-кода и его отображение в момент выпуска. Установленный PIN-код пользователя может быть отправлен на электронную почту пользователя и/или его руководителя (**Событие: Установка PIN-кода** в разделе **Уведомления пользователя** политике использования устройств) или напечатан и отправлен пользователю в конверте.

Rutoken ECP, 0756770190

Evgeniy Belov

В ожидании

Отозвать

Продолжить выпуск

Заблокировать

Сменить PIN-код администратора

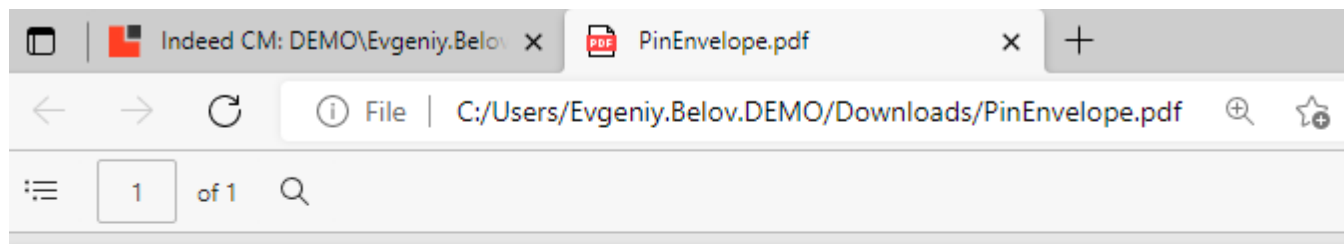
Устройство выпущено

PIN-код пользователя

Wu5fZ0

Заккрыть

Чтобы распечатать PIN-код пользователя нажмите . PIN-код будет сохранен в файле **PinEnvelope.pdf**.



Белов Евгений Александрович

Wu5fZ0

evgeniy.belov@demo.com

Rutoken ECP 0756770190

 Параметры печати содержатся в шаблоне **C:\inetpub\wwwroot\icm\Content\pinenvelope.xsl**.

По умолчанию на печать выводится информация о пользователе (имя и email) и устройстве (тип, серийный номер и PIN-код пользователя). Для изменения шаблона печати отредактируйте файл **pinenvelope.xsl**.

Проверка данных пользователя в СМЭВ



Проверка данных пользователя в системе межведомственного электронного взаимодействия (СМЭВ) доступна в карточке пользователя (опция Проверить пользователя в СМЭВ), а также при выпуске или обновлении устройства, если настроена [Интеграция со СМЭВ](#) и требуется выпустить или обновить квалифицированный сертификат согласно политике использования устройств.

1. Выберите **Тип пользователя** чьи данные необходимо проверить в СМЭВ:

- Физическое лицо
- Юридическое лицо
- Индивидуальный предприниматель

2. Введите **данные пользователя для проверки в СМЭВ** и нажмите **Далее**.

Введите данные пользователя для проверки в СМЭВ

Тип пользователя ☒ Физическое лицо ☐ Юридическое лицо
☐ Индивидуальный предприниматель

Фамилия Белов

Имя Евгений

Отчество Александрович

Пол Мужской

Дата рождения 01.10.1988

Место рождения г. Москва

Гражданство Россия

СНИЛС 027-733-198 62

ИНН 520205004556

Тип документа Паспорт гражданина РФ

Серия и номер документа 2202 919928

Дата выдачи 16.11.2002

Кем выдан Отделение УФМС России по гор. Москва

Код подразделения 770-011

Адрес регистрации

Область 78 Санкт-Петербург

Город Санкт-Петербург

Адрес Невский проспект, д. 84/2, кв. 34

Далее Отмена

3. Проверка данных пользователя может занять несколько часов.

- Нажмите **Проверить повторно** для редактирования данных пользователя и повторной проверки.
- Нажмите **Заккрыть** для продолжения проверки в фоновом режиме. Введенные данные при проверке сохраняются.

Проверка данных пользователя в СМЭВ

Проверка может занять несколько часов. Нажмите "Закрыть", если не хотите ждать. Проверка продолжится в фоновом режиме.
Введенные на предыдущем шаге данные сохраняются. Результат проверки будет отображен при следующей попытке выпуска или обновления сертификата.

Проверить повторно

Закрыть

4. Результат проверки будет отображен при следующей попытке выпуска или обновления устройства и доступен в **Журнале событий**.

- Если проверка данных пользователей прошла успешно:
 - Нажмите **Проверить повторно** для повторной проверки данных пользователя в СМЭВ. Например, если паспортные данные пользователя изменились с момента последней проверки.
 - Нажмите **Далее** для продолжения выпуска/обновления устройства. Введенные данные при проверке сохраняются.
 - Нажмите **Отмена** для отмены выпуска/обновления устройства.

Проверка данных пользователя прошла успешно 03.10.2022 10:52:56.

Проверить повторно

Далее

Отмена

- Если проверка данных пользователя в СМЭВ завершилась ошибкой:
 - Нажмите **Проверить повторно** для редактирования данных пользователя и повторной проверки.
 - Нажмите **Одобрить данные пользователя**, для принудительного подтверждения корректности введенных данных.

- ✓ Возможность одобрения данных пользователя может понадобиться в случаях, если в СМЭВ ещё не поступили недавно изменённые персональные данные пользователя (например, при смене фамилии или замене паспорта).

Опция доступна для администраторов и операторов системы, обладающих привилегией **Одобрение данных запроса СМЭВ** в ролевой модели.

- Нажмите **Отмена** для отмены выпуска/обновления устройства.

Персональные данные некорректны.

Проверить повторно

Одобрить данные пользователя

Отмена

Состояния сертификатов

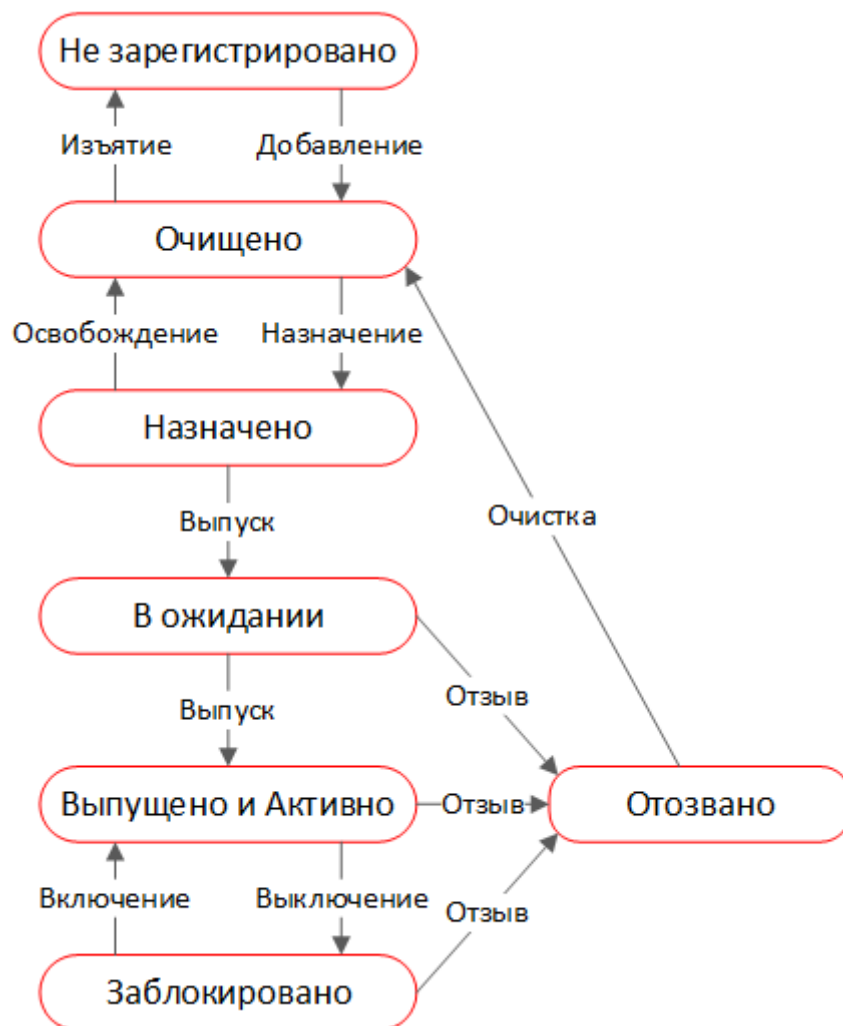
В Таблице 7 содержатся все возможные состояния сертификатов, закрытых ключей, запросов на сертификаты и их описание.

Таблица 7 – Состояния сертификатов.

Состояние сертификата	Описание
Действительный	Срок действия сертификата еще не истек. Сертификат пригоден для использования.
Отозван	Сертификат отозван. Отзыв может быть временным или окончательным. В случае временного отзыва (в результате выключения устройства), срок действия сертификата приостанавливается на период выключения устройства. После включения устройства сертификат снова становится действительным (если его срок действия не истек пока устройство было выключено). В случае окончательного отзыва (в результате отзыва устройства или его изъятия), сертификат более не может использоваться.
Истекает	Срок действия сертификата скоро закончится. Выполните обновление сертификата, если планируется его дальнейшее использование.
Ключ истекает	Срок действия закрытого ключа сертификата, выданного КриптоПро УЦ скоро закончится. Выполните обновление сертификата, если планируется его дальнейшее использование. Закрытый ключ в этом случае также будет обновлен.
Истек	Срок действия сертификата истек. Сертификат не пригоден для использования. Срок действия сертификата может быть продлен на период равный сроку его действия, заданный в шаблоне сертификата (см. раздел Обновление устройства).
Ошибка	Состояние сертификата не удалось определить. Возможно, центр сертификации недоступен. Сертификат не пригоден для использования.
Одобен	Запрос на сертификат одобрен администратором, но сертификат еще не выпущен пользователю.
Отклонен	Запрос на сертификат отклонён администратором.
В ожидании	Запрос на сертификат ожидает рассмотрения Оператором УЦ.

Жизненный цикл устройств

Жизненный цикл устройств (смарт-карт) в системе Indeed Certificate Manager.



Публикация выпущенных сертификатов

Выпущенные и записанные на устройство пользователя сертификаты в зависимости от настроек Indeed Certificate Manager могут быть опубликованы в:

- Локальное хранилище сертификатов пользователя на рабочей станции. Опция **Устанавливать сертификат в локальное хранилище** в Параметрах шаблона сертификата политики использования устройств.
- Каталог пользователей в Active Directory. Опция **Публиковать сертификат в каталоге пользователей**.
- Единую систему идентификации и аутентификации (ЕСИА). Опция **Публиковать сертификат в ЕСИА**.
- Файловое хранилище. Опция **Публиковать сертификат в файловое хранилище**.
- Базу приложений ЦФТ. Опция **Публиковать сертификат в ЦФТ**.

Печать персонального сертификата (запроса сертификата)

Печатные формы запроса на сертификат, сертификата, в том числе для отслеживаемых сертификатов и запроса на отзыв сертификата могут быть сохранены или отправлены пользователю на его E-mail в формате PDF.

Для печати нажмите , выберите требуемую форму: Сертификат, Запрос на сертификат или Запрос на отзыв сертификата и сохраните файл в формате PDF.

Для изменения стандартных шаблонов печати, общих для всех шаблонов сертификатов, добавленных в политику использования устройств, отредактируйте файлы **Консоли управления** и **Сервиса самообслуживания**.

Консоль управления:

- C:\inetpub\wwwroot\icm\Content\request_ru.xml – шаблон печати запроса
- C:\inetpub\wwwroot\icm\Content\cert_ru.xml – шаблон печати сертификата
- C:\inetpub\wwwroot\icm\Content\revocationRequest_ru.xml – шаблон печати запроса на отзыв сертификата

Сервис самообслуживания:

- C:\inetpub\wwwroot\icmservice\Content\request_ru.xml – шаблон печати запроса
- C:\inetpub\wwwroot\icmservice\Content\cert_ru.xml – шаблон печати сертификата
- C:\inetpub\wwwroot\icmservice\Content\revocationRequest_ru.xml – шаблон печати запроса на отзыв сертификата

Если для шаблонов сертификатов, добавленных в политику выпуска устройств требуется использовать разные шаблоны печати сертификата, запроса на сертификат или запроса на отзыв сертификата, то отредактируйте и загрузите их на вкладке **Конфигурация** Консоли управления в разделе [Шаблоны печати](#), и выберите в [Настройках шаблонов сертификатов](#).

Назначение устройства

Назначение устройства пользователю заключается в том, что устройство присваивается указанному пользователю, для того, чтобы он в последствии самостоятельно его выпустил при помощи приложения [Сервис самообслуживания](#) (Self Service).

! Одно устройство может одновременно принадлежать только одному пользователю. У одного пользователя может быть несколько устройств. Возможность пользователям самостоятельно назначать себе устройства в сервисе самообслуживания задается администратором в разделе [Поведение](#) политики использования устройств, действующей на пользователя.

Для назначения устройства пользователю выполните следующие действия:

1. Перейдите в карточку пользователя и нажмите **Назначить устройство**.
2. Если устройство доступно, подключите его к компьютеру.
3. Если PIN-код администратора не соответствует значению, заданному производителем (или значению, указанному в **Типе устройства**), то укажите PIN-код администратора для каждой области в разделе **Дополнительно** и нажмите **Назначить**.

Назначенные устройства

Нет назначенных устройств

[+ Выпустить устройство](#) [+ Назначить устройство](#)

☒ Устройство доступно

☐ Устройство недоступно

Устройство

ARDS JaCarta 0: IDProtect (X) ▾

[Дополнительно](#) ✓

PIN-код администратора

PIN-код администратора

PIN-код администратора (ГОСТ)

PIN-код администратора (ГОСТ)

Назначить

Отмена

4. Если устройство недоступно, но известны его серийный номер и тип, укажите их и нажмите **Назначить**.

Назначенные устройства

Нет назначенных устройств

[+ Выпустить устройство](#) [+ Назначить устройство](#)

☐ Устройство доступно

☒ Устройство недоступно

Серийный номер и тип устройства

0755398982

Rutoken S

Назначить

Отмена

5. Назначенное устройство имеет статус **Назначено** в карточке пользователя.

Отмена назначения устройства

Назначенное пользователю, но ещё не выпущенное устройство можно отозвать.

1. Для отмены назначения устройства перейдите на карточку пользователя, выберите назначенное устройство и нажмите **Отменить назначение**.
2. Если назначенное устройство поддерживает аппаратную криптографию и в системе ведется учет СКЗИ, то укажите **Номер и дату документа** (приказа, распоряжения), в соответствии с которым у пользователя изымается СКЗИ (Тип: Ключевой носитель). Информация об имеющихся в системе средствах криптографической защиты информации располагается в разделе [СКЗИ](#).
3. Подтвердите действие нажатием кнопки **Отменить назначение**.

▼  Rutoken ECP, 0894130607

Назначено

Выпустить

Отменить назначение

Сменить PIN-код администратора

↺

Номер и дата документа

ВН-121

23.11.2021 15:24



Отменить назначение

Отмена

Сброс PIN-кода устройства

Оператор Indeed Certificate Manager может сбросить PIN-код устройства пользователя. В этом случае PIN-код, заданный пользователем, изменяется на значение, указанное в разделе **Типы устройств**.

 Если в разделе **Выпуск** политики использования устройств включена опция **Инициализировать устройство**, то PIN-код пользователя будет сброшен на значение, указанное в **Параметрах инициализации** типа устройства.

Для сброса PIN-кода пользователя выполните следующие действия:

1. Перейдите на вкладку **Пользователи** и выполните поиск пользователя.
2. Перейдите в карточку пользователя, щелкнув по его логину в результатах поиска.
3. Выберите нужное устройство и раскройте информацию о нем.
4. Нажмите **Сбросить PIN-код**:
 - Подключите устройство и нажмите **Сбросить**
 - Если устройство недоступно, выберите опцию **Сбросить PIN-код пользователя на агенте** для создания задачи на Клиентском Агенте

Назначенные устройства

▼

Rutoken ECP, 0894130607

Evgeniy Belov

Выпущено

Сбросить PIN-код

Разблокировать

Выключить

Отозвать

Заменить

Заменить на AirKey

Обновить

Заблокировать

Сменить PIN-код администратора

☐ Сбросить PIN-код пользователя на агенте

Вставьте устройство и нажмите 'Сбросить'

Сбросить

Отмена

После сброса PIN-кода администратором, пользователь сможет задать новый PIN-код самостоятельно, при помощи приложения **Сервис самообслуживания** (Self Service).

Разблокировка устройства

В случае, если пользователь ввел неверный PIN-код устройства больше определенного количества раз, оно блокируется. Максимальное количество попыток ввода PIN-кода пользователем задается администратором в разделе **Выпуск > Инициализация устройства** политики использования устройств.

Существует два режима разблокировки устройства пользователя:

1. [Online-разблокировка](#)
2. Offline-разблокировка:
 - [Offline-разблокировка в окне входа Windows](#)



Разблокировка устройства (смарт-карты, USB-токена) на экране входа в Windows не поддерживается при удаленном подключении через Remote Desktop.

- [Offline-разблокировка в Windows сессии](#)

Online-разблокировка

Осуществляется пользователем в окне входа операционной системы Windows.

Пользователь отвечает на секретные вопросы, задает и подтверждает новый PIN-код, после чего устройство разблокируется.



Для online-разблокировки обязательными условиями является:

- Наличие соединения рабочей станции пользователя, к которой подключено заблокированное устройство, с сервером Indeed Certificate Manager.
- У пользователя заданы ответы на секретные вопросы в [Сервисе самообслуживания](#) (Self Service). Если секретные вопросы пользователя не установлены, online-разблокировка устройства будет недоступна. Разблокировать устройство можно будет в [offline-режиме](#).

Ниже приведен пример online-разблокировки устройства в окне входа операционной системы Windows 11. Механизм разблокировки устройства в операционных системах Windows других версий выглядит похожим образом.

1. Введите ответы на секретные вопросы и нажмите .



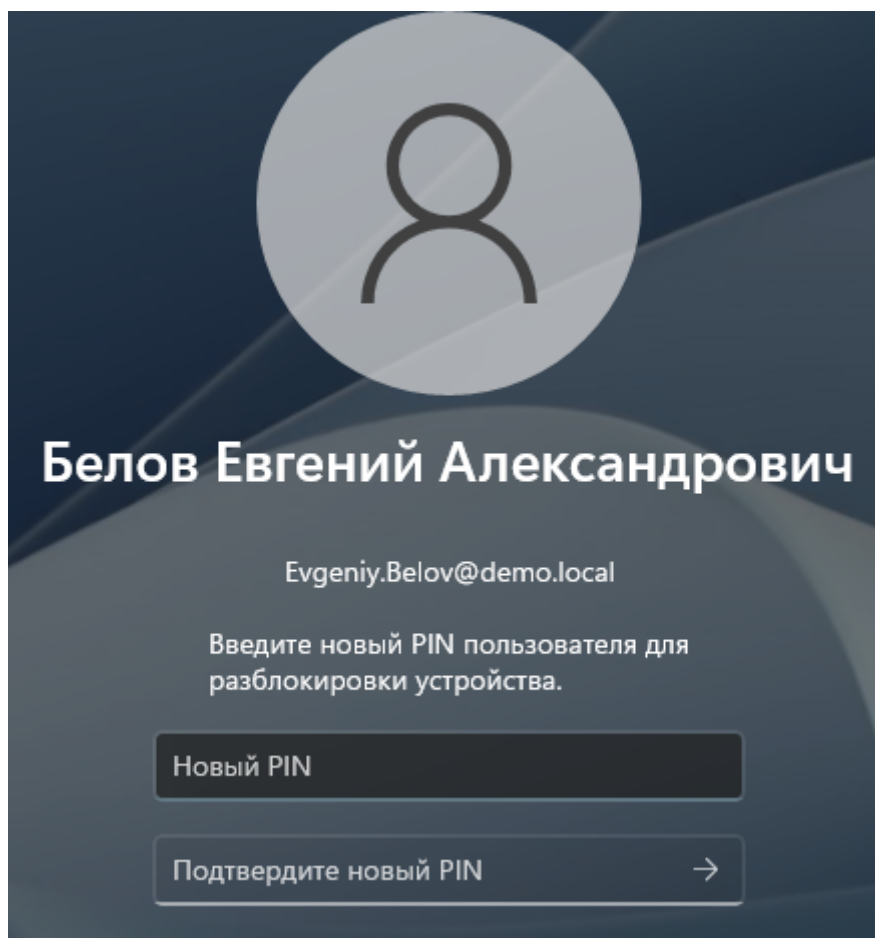
Белов Евгений Александрович

Evgeniy.Belov@demo.local

Устройство заблокировано. Введите ответы на секретные вопросы для его разблокировки.

Как звали вашего лучшего друга детства?

2. Введите **Новый PIN** и его **Подтверждение**.



Белов Евгений Александрович

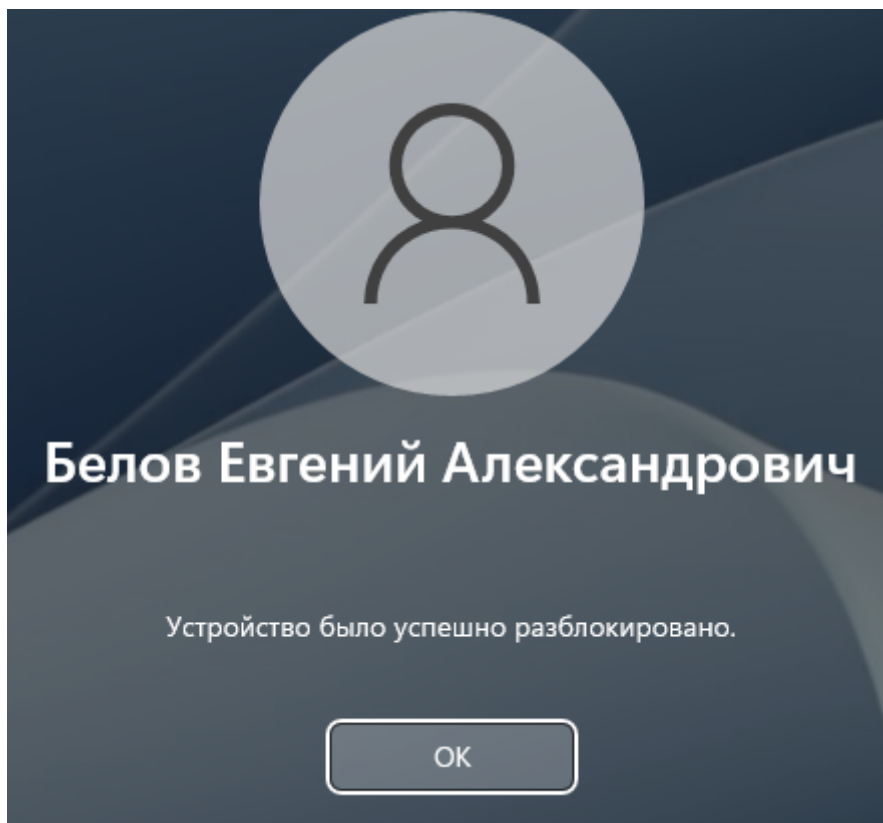
Evgeniy.Belov@demo.local

Введите новый PIN пользователя для разблокировки устройства.

Новый PIN

Подтвердите новый PIN →

3. В случае успешной разблокировки устройства появится соответствующее сообщение.



Белов Евгений Александрович

Устройство было успешно разблокировано.

OK

Offline-разблокировка в окне входа Windows

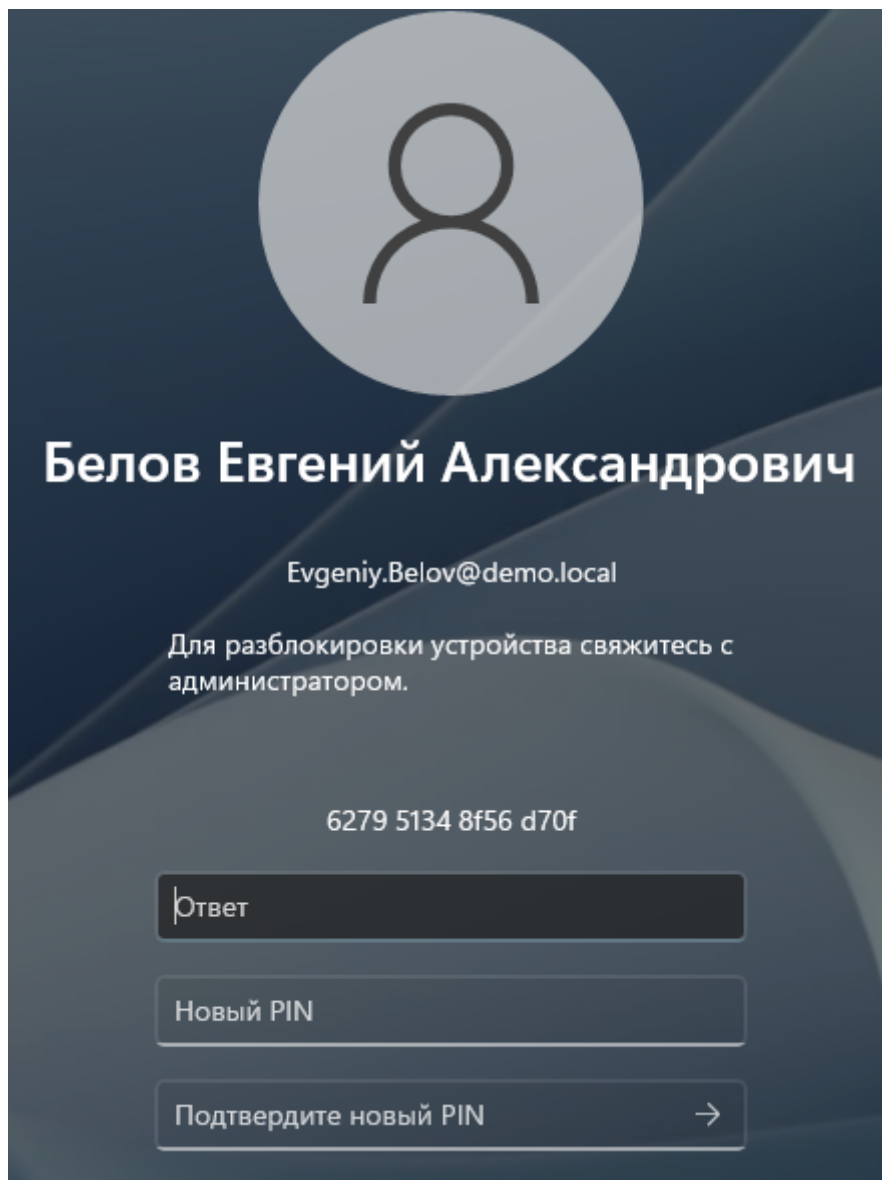
Offline-разблокировка осуществляется оператором системы по принципу аутентификации вида запрос-ответ (англ. challenge-response authentication mechanism).



Разблокировка устройства (смарт-карты, USB-токена) на экране входа в Windows не поддерживается при удаленном подключении через Remote Desktop.

При исчерпании заданного числа попыток ввода PIN-кода, пользователь получает сообщение о том, что его устройство заблокировано. Вместе с сообщением пользователь получает уникальный 16-ти символьный код-запрос. Пользователю необходимо связаться с оператором системы (например, по телефону), подтвердить свою личность, ответив на секретные вопросы и сообщить полученный код.

Ниже на рисунке приведен пример экрана offline-разблокировки устройства в окне входа операционной системы Windows 11. Механизм разблокировки устройства в операционных системах Windows других версий выглядит похожим образом.



Белов Евгений Александрович

Evgeniy.Belov@demo.local

Для разблокировки устройства свяжитесь с администратором.

6279 5134 8f56 d70f

Ответ

Новый PIN

Подтвердите новый PIN →

Оператор системы открывает карточку пользователя и в перечне действий над устройством выбирает пункт **Разблокировать**. Прежде, чем выполнить генерацию ответного кода для разблокировки устройства, администратор системы задает секретный вопрос (или несколько вопросов, в зависимости от настроек политики использования устройств) и вводит полученный от пользователя ответ в соответствующую форму.

 Опция **Разрешить офлайновую разблокировку** может быть отключена в разделе **Поведение** политики использования устройств. В этом случае кнопка **Разблокировать** в карточке устройства будет недоступна. Необходимость проверки ответов на секретные вопросы при offline-разблокировке определяется опцией **Проверять ответы на секретные вопросы** в разделе **Поведение** политики использования устройств.

Назначенные устройства

▼ Rutoken ECP, 0756770190

Выпущено

Сбросить PIN-код

Разблокировать

Выключить

Отозвать

Заменить

Обновить

↺

Пожалуйста, ответьте на секретные вопросы

Как называется наша компания?

OK

Отмена

Если ответы на все вопросы даны верно, то оператор вводит код, который ему сообщает пользователь и система генерирует ответный код, который оператор сообщает пользователю.

Назначенные устройства

▼ Rutoken ECP, 0756770190

Выпущено

Сбросить PIN-код

Разблокировать

Выключить

Отозвать

Заменить

Обновить

↺

Пожалуйста, введите запрос и нажмите 'Получить ответ'

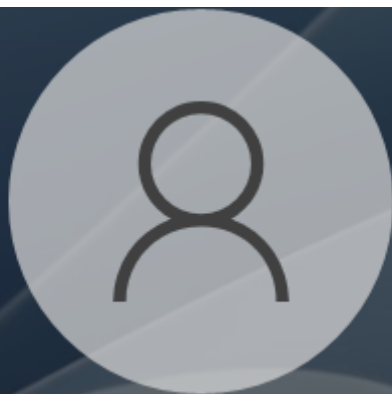
Запрос

Ответ

Получить ответ

Закрыть

Пользователь вводит код, полученный от оператора, и задает новый PIN-код устройства. В случае успешной разблокировки отображается соответствующее сообщение.



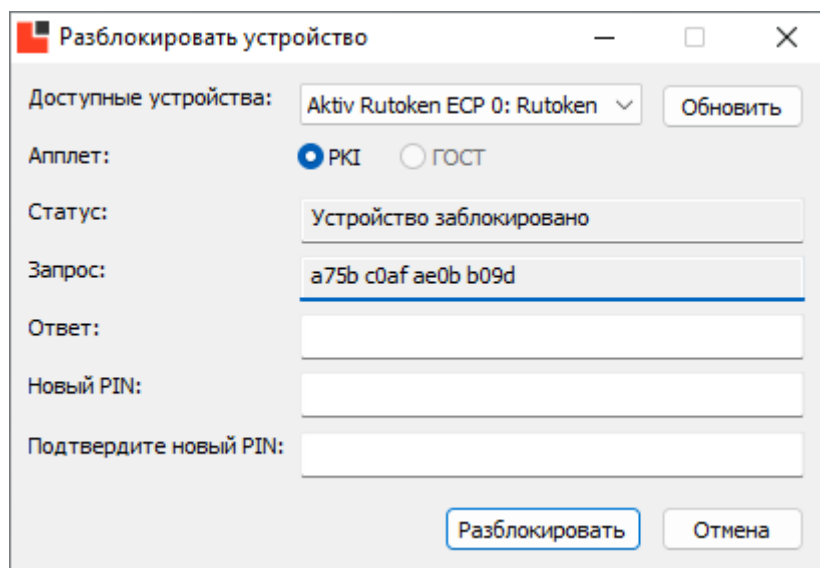
Белов Евгений Александрович

Устройство было успешно разблокировано.

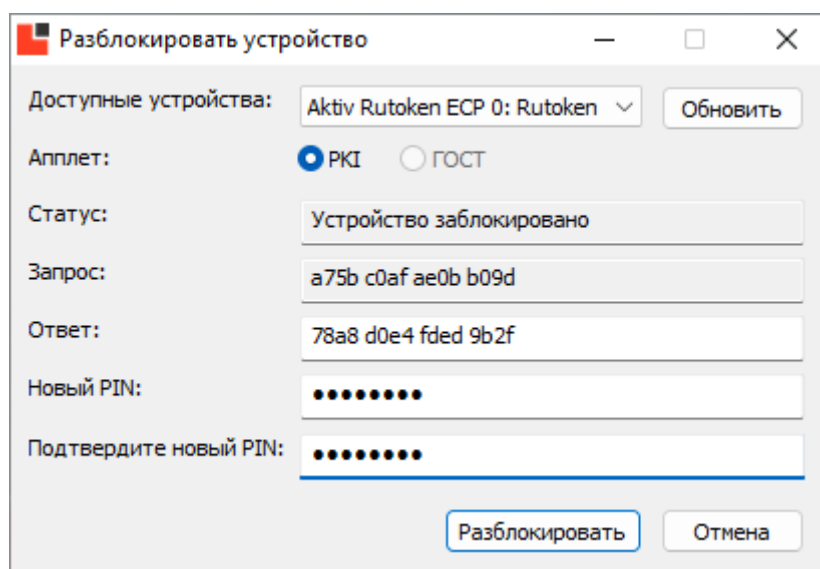
ОК

Offline-разблокировка в Windows сессии

Если устройство не используется для входа на рабочую станцию и было заблокировано, то в этом случае для его разблокировки применяется утилита **Indeed CM - Unblock** (*Пуск – Все программы – Indeed*. Расположение по умолчанию: **%ProrgamFiles (x86)/IndeedCM /IndeedCM.Unblock.exe**). Подключите устройство к компьютеру и запустите утилиту. Выберите устройство из списка и апплет (PKI или ГОСТ).



В поле **Запрос** появится код разблокировки устройства, который нужно сообщить оператору Indeed CM. Оператор может запросить у вас ответы на секретные вопросы для подтверждения личности и сообщит код ответа. Введите его в поле **Ответ** утилиты разблокировки, задайте новый PIN-код, подтвердите его и нажмите **Разблокировать**.



После этого ваше устройство разблокируется (значение поля **Статус** станет «**Устройство не заблокировано**»), а PIN-код изменится на указанный. Завершите работу с утилитой **Indeed CM - Unblock**.

Выключение и включение устройства

Устройство пользователя может быть выключено на определенный промежуток времени и затем снова включено. Например, на период отпуска сотрудника.

 Выключение и включение устройства оператором осуществляется без подключения устройства к рабочей станции.

Для выключения устройства пользователя выполните следующие действия:

1. Перейдите на вкладку **Пользователи** и выполните поиск пользователя.
2. Перейдите в карточку пользователя, щелкнув по его логину в результатах поиска.
3. Выберите нужное устройство и раскройте информацию о нем.
4. Нажмите **Выключить**.

 При выключении устройства Indeed Certificate Manager сможет отозвать все сертификаты, хранящиеся на нем. Для этого необходимо в политике использования устройств включить опцию **Отзывать сертификат при отзыве /выключении устройства**. Сертификаты будут отозваны с отметкой **Приостановка действия** (Certificate hold). Для возобновления действия сертификатов необходимо включить устройство.

При попытке использования выключенного устройства для аутентификации пользователь получит сообщение о том, что его сертификаты отозваны. Для включения устройства пользователя выполните следующие действия:

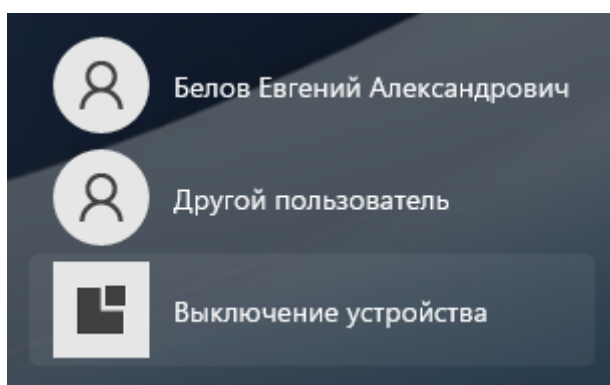
1. Перейдите на вкладку **Пользователи** и выполните поиск пользователя.
2. Перейдите в карточку пользователя, щелкнув по его логину в результатах поиска.
3. Выберите нужное устройство и раскройте информацию о нем.
4. Нажмите **Включить**.

Выключение устройства без выполнения входа в систему

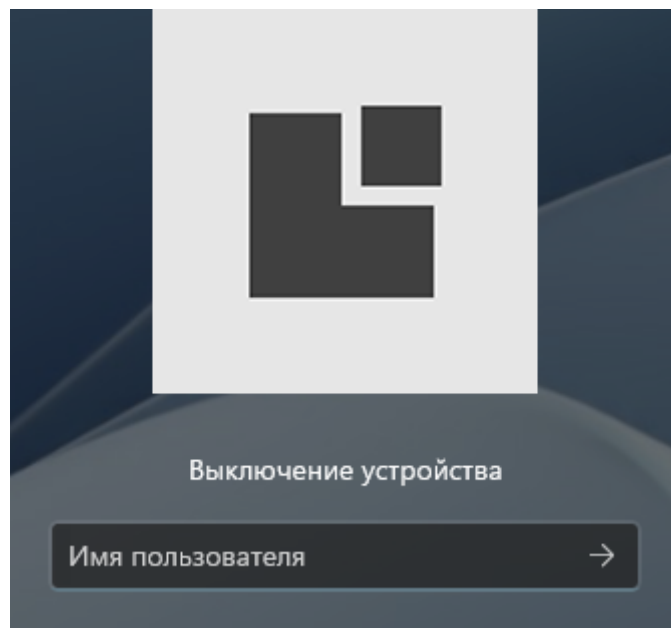
В экстренном случае пользователь может самостоятельно выключить устройство без выполнения входа в операционную систему.

- ❗ Выключение устройства доступно только в том случае, если у рабочей станции, с которой осуществляется операция, есть связь с сервером Indeed Certificate Manager и у пользователя заданы ответы на секретные вопросы. Возможность выключения устройства может быть отключена для определенных категорий пользователей (см. раздел [Настройка online-разблокировки устройств](#)).

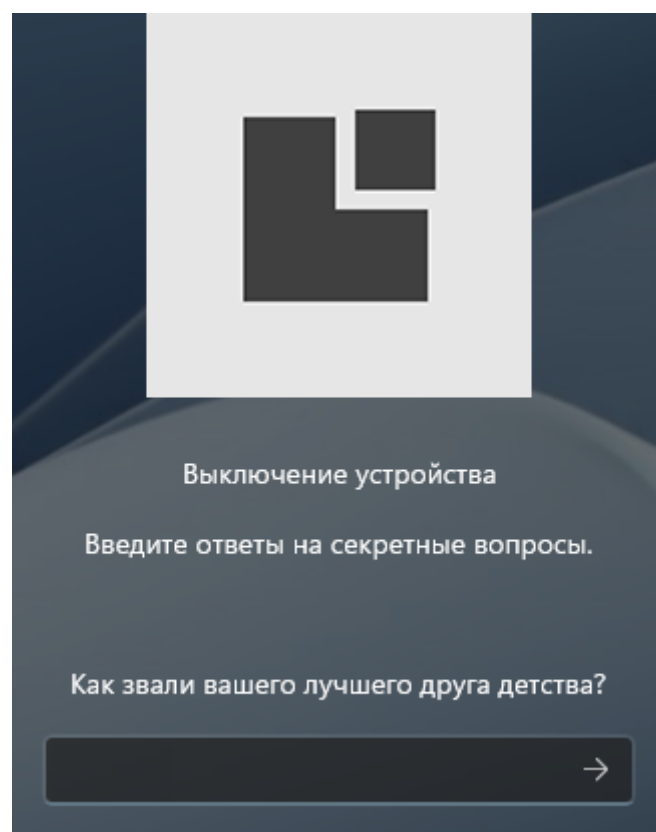
1. Для выключения устройства выберите **Выключение устройства** на экране входа Windows. Ниже на рисунке приведен пример для операционной системы Windows 11. Механизм выключения в операционных системах Windows других версий выглядит похожим образом.



2. Укажите имя пользователя (логин или UPN), устройство (USB-токен или смарт-карту) которого необходимо выключить.

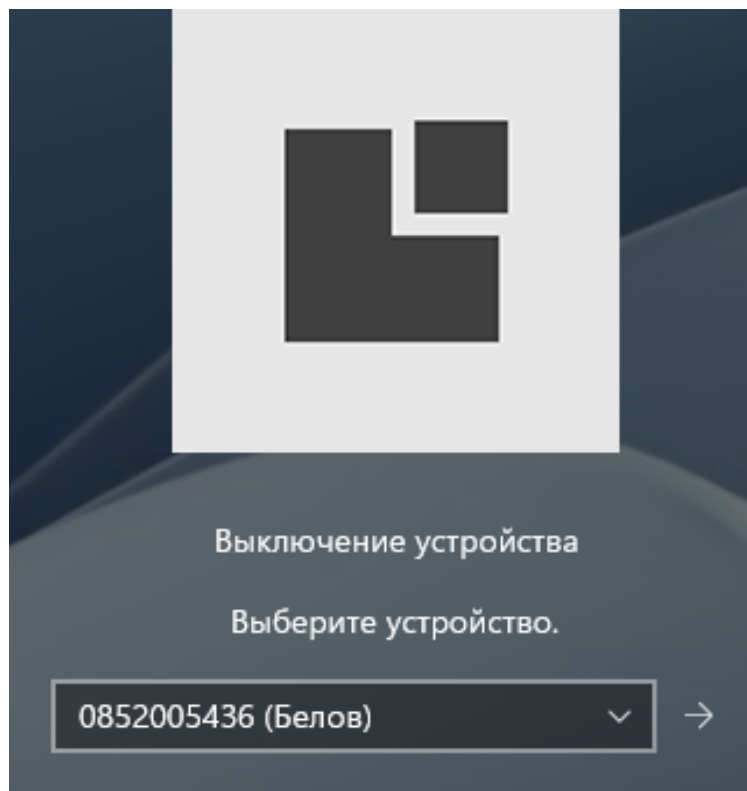


3. Введите ответы на секретные вопросы.

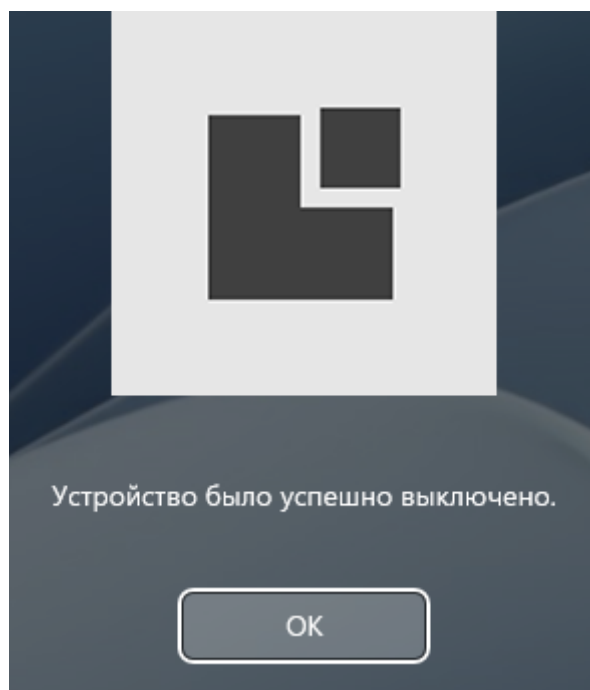


4. Выберите устройство из списка выпущенных устройств пользователя и нажмите





В случае успешного выключения устройства появится соответствующее сообщение.



Отзыв устройства

Устройство может быть отозвано оператором (или пользователем, если определены соответствующие настройки в политике использования устройств) в случае его повреждения, утери, необходимости обновления или изъятия.

 При включенной в политике использования устройств опции **Отзывать сертификат при отзыве/выключении устройства** все сертификаты пользователя, хранящиеся на устройстве, будут отозваны без возможности их восстановления.

Для отзыва устройства пользователя выполните следующие действия:

1. Перейдите на вкладку **Пользователи** и выполните поиск пользователя.
2. Перейдите в карточку пользователя, щелкнув по его логину в результатах поиска.
3. Выберите нужное устройство и раскройте информацию о нем.
4. Нажмите **Отозвать**.
5. Укажите **Причину отзыва**:
 - **Устройство неисправно** – устройство технически неисправно или уничтожено
 - **Устройство утеряно** – устройство утеряно
 - **Обновление устройства** – обновление устройства (например, замена старого устройства новым)
 - **Изъятие устройства** – удаление устройства из системы в связи с увольнением сотрудника (значение по умолчанию)
 - **Компрометация устройства** – подозрение на то, что ключ был скомпрометирован, при этом устройство не утеряно и исправно

 В случае, если устройство отзывается по причине того, что было утеряно или скомпрометировано, то все сертификаты, записанные на нем, будут отозваны (даже если не включена опция **Отзывать сертификат при отзыве/выключении устройства** в политике использования устройств).

Назначенные устройства

▼  **Rutoken S, 0755398982**  Evgeniy Belov Выпущено

Сбросить PIN-код

Разблокировать

Выключить

Отозвать

Заменить

Заменить на AirKey

Обновить

Заблокировать

Сменить PIN-код администратора

Причина отзыва

Изъятие устройства ▼

☐ Очистить устройство на агенте

Отозвать

Отмена

6. Нажмите кнопку **Отозвать**, если устройство доступно или создайте задачу на агенте, выбрав опцию **Очистить устройство на агенте**.

Причина отзыва устройства отображается в карточке пользователя. При попытке использования отозванного устройства для аутентификации пользователь получит сообщение о том, что его сертификаты отозваны.

Изъятие устройства

Отозванное устройство пользователя остается закрепленным за ним и может быть либо заменено (см. раздел **Замена устройства**) либо изъято. Для изъятия устройства пользователя выполните следующие действия:

1. Перейдите на вкладку **Пользователи** и выполните поиск пользователя.
2. Перейдите в карточку пользователя, щелкнув по его логину в результатах поиска.
3. Выберите нужное устройство и раскройте информацию о нем.
4. Нажмите **Изъять**.

▼  Rutoken ECP, 0894130607  Белов Отозвано

Заменить

Заменить на AirKey

Изъять

Сменить PIN-код администратора

↺

Содержимое устройства будет удалено и устройство будет отвязано от пользователя

☒ Устройство доступно

☐ Устройство недоступно (потеряно или повреждено)

Номер и дата документа

ВН-543

23.11.2021 16:06



☒ Очистить устройство

☐ Инициализировать устройство

Дополнительно ▼

Оставьте поле 'Новый PIN-код пользователя' пустым, если хотите использовать значение, установленное производителем устройства

Новый PIN-код пользователя

Вставьте устройство и нажмите 'Изъять'

Изъять

Отмена

5. Если устройство доступно, выберите соответствующий пункт, подключите его к рабочей станции и при необходимости выберите опции:

- **Очистить устройство** – После изъятия с устройства удалятся все сертификаты, записанные при помощи Indeed CM. Сертификаты, запросы, ключи, записанные без участия Indeed CM удалены не будут.
- **Инициализировать устройство** – После изъятия с устройства удалятся все имеющиеся на нем данные. Параметры инициализации будут использоваться такие же, как при включении опции **Инициализировать устройство при добавлении**.
- Если при выпуске устройства было создано СКЗИ, то необходимо указать **Номер и дату документа**, на основании которого происходит уничтожение /изъятие СКЗИ в процессе изъятия.
- Укажите **PIN-код пользователя**, который должен быть установлен на устройстве после его изъятия. Если PIN-код пользователя не будет задан, то после изъятия устройства будет установлен PIN-код, указанный в файле типа устройства.

 PIN-код необходимо устанавливать в том случае, если PIN-код пользователя, указанный в файле типа устройства (см. **Управление типами устройств**), не соответствует требованиям PIN-кода, установленным для данного типа устройства при инициализации в момент выпуска (см. [Параметры инициализации устройства](#)).

6. Подтвердите действие нажатием кнопки **Изъять**.

7. Если устройство недоступно, выберите соответствующий пункт и нажмите **Изъять**.

Замена устройства

Indeed Certificate Manager позволяет выполнять временную или постоянную замену устройств пользователей. В этом случае содержимое одного устройства будет полностью перенесено на другое устройство.

Временная замена

Новое устройство будет выдано на определенный срок. Например, сотрудник забыл свою смарт-карту дома. Для работы в офисе оператор выпускает ему новую, задавая срок действия устройства.

В этом случае действие сертификатов на забытой дома карте сотрудника будет приостановлено. Действительные сертификаты и ключи будут записаны на новую смарт-карту (устройство). В карточке пользователя отображаются два устройства:

- **Основное** устройство **Rutoken S** выключено и действие всех сертификатов, находящихся на нем приостановлено.
- **Устройство-дубликат Rutoken ECP** выпущено с ограниченным сроком действия (выделен **красным**).



Белов Евгений Александрович

Логин	DEMO\Evgeniy.Belov
Путь	demo.local/Indeed CM RU/Белов Евгений Александрович
Политика	Базовая политика
E-mail	evgeniy.belov@demo.com
Телефон	+7 (905) 288-58-23

[Загрузить фотографию](#) [Пользователь КriptoПро 2.0](#) [Сбросить ответы на секретные вопросы](#)
[Сбросить пароль пользователя](#)

Назначенные устройства

>	Rutoken ECP, 0756770190	Евгений Белов	01.04.2017 0:00	Выпущено
>	Rutoken S, 0755398982	Евгений Белов		Выключено

[+ Выпустить устройство](#) [+ Назначить устройство](#)

Постоянная замена

Заменяемое устройство будет отозвано, вместо него будет выпущено новое. На новое устройство будут записаны все данные заменяемого устройства (ключевые пары, сертификаты). Сертификаты, хранящиеся на заменяемом устройстве, будут отозваны без возможности восстановления.

 При замене устройства PIN-код устройства не переносится на новое устройство. Устройство-дубликат будет иметь PIN-код, в соответствии с настройками политики использования устройств:

- установленный производителем по умолчанию
- заданный администратором в параметрах инициализации устройства
- случайный

Изменить PIN-код устройства пользователь может в [Сервисе самообслуживания](#) (Self Service) если определены соответствующие настройки в политике использования устройств.

Для замены устройства пользователя выполните следующие действия:

1. Перейдите на вкладку **Пользователи** и выполните поиск пользователя.
2. Перейдите в карточку пользователя, щелкнув по его логину в результатах поиска.
3. Выберите нужное устройство и раскройте информацию о нем.
4. Нажмите **Заменить**.
5. Укажите тип замены: **Временная** или **Постоянная**.
 - Если требуется временная замена, укажите срок окончания действия временного устройства.
 - Если требуется постоянная замена, укажите причину.
6. Задайте имя устройства (может быть подставлено автоматически, если в политике использования устройств разрешено соответствующее действие).
7. Подключите новое устройство к компьютеру.
8. Укажите PIN-код администратора в разделе **Дополнительно**, если новое устройство не добавлено в Indeed CM и нажмите **Заменить** для замены устройства или **Отмена** для возврата к карточке пользователя.

 Если определены соответствующие настройки в политике использования устройств, то в процессе замены новое устройство будет инициализировано. Все данные, хранящиеся на устройстве будут удалены.

Назначенные устройства

▼

Rutoken ECP SC, 0862287369

Евгений Белов

Выпущено

Сбросить PIN-код

Разблокировать

Выключить

Отозвать

Заменить

Обновить

↺

Устройство будет проинициализировано. Все данные на устройстве будут потеряны

☒ Временная

☐ Постоянная

Время истечения

18.08.2017 00:00

📅

Имя устройства

Евгений Белов

☒ Устройство

☐ Принтер

ARDS JaCarta 0: IDProtect (▼)

Дополнительно

📄

PIN-код администратора

PIN-код администратора

PIN-код администратора (ГОСТ)

PIN-код администратора (ГОСТ)

Заменить

Отмена

Если Indeed Certificate Manager интегрирован с Indeed AirKey Enterprise, то аппаратное устройство может быть заменено на виртуальную карту AirKey. Для замены на AirKey нажмите **Заменить на AirKey** в панели доступных действий с устройством.

Обновление устройства

Обновление устройства необходимо в случаях если:

- Срок действия одного или нескольких сертификатов истек (или истекает)
- Пользователю была назначена новая политика (например, с большим приоритетом)
- На устройстве были добавлены сертификаты вне Indeed CM (если в политике использования устройств [Включено отслеживание сертификатов](#))
- В политике использования устройств:
 - изменилось количество шаблонов сертификатов
 - добавлены/удалены общие сертификаты
 - присутствует хотя бы один необязательный сертификат (для последующей его записи/удаления на устройство/с устройства)
 - включен или отключен коннектор к Indeed Access Manager
 - включен или отключен коннектор к Secret Net Studio

Если пользователю была назначена новая политика, то обновление содержимого устройства будет произведено следующим образом:

1. Сертификаты, которые есть в текущей политике, действующей на пользователя, но отсутствуют в новой, удалятся.
2. Сертификаты, которые есть в новой политике, но отсутствуют в текущей, будут выпущены и записаны на устройство.
3. Сертификаты, присутствующие в обеих политиках, останутся без изменений.

Администратор может обновить содержимое устройства без его перевыпуска или создать задачу на клиентском агенте, установленным на рабочей станции пользователя. Обновление содержимого устройства по умолчанию также доступно и пользователю в приложении [Сервис самообслуживания \(Self Service\)](#).

Для обновления устройства выполните следующие действия:

1. Перейдите на вкладку **Пользователи** и выполните поиск пользователя.
2. Перейдите в карточку пользователя, щелкнув по его логину в результатах поиска.
3. Выберите нужное устройство и раскройте информацию о нем.
4. Нажмите **Обновить**.
 - Если устройство недоступно и используется конфигурация с клиентскими Агентами, то выберите параметр **Обновить устройство на агенте**
 - Подключите устройство к компьютеру, введите **PIN-код пользователя** и нажмите **Обновить**

▼ Rutoken ECP, 0894130607 Evgeniy Belov

Выпущено

Сбросить PIN-код

Разблокировать

Выключить

Отозвать

Заменить

Заменить на AirKey

Обновить

Заблокировать

Сменить PIN-код администратора

☐ Обновить устройство на агенте

PIN-код пользователя

Вставьте устройство и нажмите 'Обновить'

Обновить

Отмена

 Если в политике использования устройств настроена [Интеграция со СМЭВ](#) и при обновлении устройства выбран квалифицированный сертификат (Обязательный или необязательный), то требуется проверка данных пользователя в системе межведомственного электронного взаимодействия (СМЭВ).

5. Выполните [Проверку данных пользователя в СМЭВ](#).

- Введите данные пользователя для проверки в СМЭВ
- Нажмите **Далее**, дождитесь окончания проверки, после чего продолжите обновление устройства

6. Если на устройство были добавлены сертификаты вне Indeed CM и в политике использования устройств [Включено отслеживание сертификатов](#), то при обновлении устройства данные сертификаты могут быть выбраны для отслеживания.

▼

Rutoken ECP, 0894130607

Evgeniy Belov

Выпущено

Сбросить PIN-код

Разблокировать

Выключить

Отозвать

Заменить

↺

Заменить на AirKey

Обновить

Заблокировать

Сменить PIN-код администратора

На устройстве обнаружены следующие сертификаты. Выберите сертификаты, которые будут отслеживаться

Субъект	Издатель	Действителен до
☒ Operator	Головной УЦ ООО "КРИПТО-ПРО"	22.04.2021 15:00

OK

Выпуск устройства с печатью

Если опция **Включить печать устройства** в политике использования устройств включена, то выпуск устройств в форм факторе смарт-карты в Indeed Certificate Manager может быть объединен с печатью изображения или текста на них. В этом случае смарт-карта помещается в лоток подачи карт принтера и в процессе выпуска на неё записываются сертификаты и наносится изображение в соответствии с заданным шаблоном печати.



Обязательным условием печати на устройствах является наличие на рабочей станции, с которой происходит печать следующих компонентов:

- Драйвера принтера EDISecure XID8300
- Настроенного соединения с принтером в утилите EDI Secure Connect
- Компонента поддержки принтера **IndeedCM.EdiSecure.Middleware**
- Подключенного через интерфейс USB принтера XID8300



Драйвера принтера EDISecure XID8300 и утилита EDI Secure Connect поставляется производителем вместе с принтером.

IndeedCM.EdiSecure.Middleware поставляется в составе дистрибутива Indeed CM.

Для выпуска смарт-карты с печатью выполните следующие действия:

1. Перейдите на вкладку **Пользователи** и выполните поиск пользователя.
2. Перейдите в карточку пользователя, щелкнув по его логину в результатах поиска.
3. Нажмите **Выпустить устройство**.
4. Укажите **Имя устройства**.



Имя устройства может быть подставлено автоматически. См. **Настройки выпуска устройства**.

5. Если политика использования устройств подразумевает выбор сертификатов, выберите нужные и нажмите **Далее**.
6. Укажите способ выпуска устройства **Принтер**. Имя подключенного принтера подставится автоматически.

Назначенные устройства

Нет назначенных устройств

[+ Выпустить устройство](#) [+ Назначить устройство](#)

Имя устройства

☐ Устройство ☒ Принтер

[Дополнительно](#) 

7. Поместите карту в лоток подачи принтера.

8. Нажмите **Выпустить**.

Кроме того, система позволяет наносить изображение на ранее выпущенные (без использования принтера) карты. Для печати на ранее выпущенной карте выполните следующие действия:

1. Поместите карту в лоток принтера.
2. Перейдите на вкладку **Пользователи** и выполните поиск пользователя.
3. Перейдите в карточку пользователя, щелкнув по его логину в результатах поиска.
4. Выберите нужную карту и раскройте информацию о ней.
5. Нажмите **Печатать**.

Массовый выпуск смарт-карт

При использовании Indeed Certificate Manager с принтером смарт-карт (опция [Включить поддержку принтера смарт-карт](#) в политике использования устройств) существует возможность массового выпуска карт пользователям. В этом случае оператор определяет группу пользователей, которым необходимо выпустить карты, помещает нужное количество карт в лоток принтера и запускает процесс массового выпуска.

Режим массового выпуска имеет следующие особенности и ограничения:

- Отсутствует возможность выбора необязательных сертификатов. Будут выпущены только обязательные. Необязательные сертификаты, в случае необходимости, следует выпустить для каждого пользователя отдельно через карточку пользователя или сервис самообслуживания.
- Отсутствует возможность указания имени карты. Имя будет пустым или сформированным по правилам, обозначенным в политике использования устройств.
- Отсутствует возможность создать автоматически документ учета СКЗИ. В случае необходимости, такой документ следует указать вручную в карточке пользователя.
- При возникновении любой ошибки массовый выпуск останавливается. Для дальнейшей работы следует устранить ошибку или исключить проблемного пользователя из списка и запустить массовый выпуск заново.
- При нажатии кнопки Отмена во время массового выпуска загруженная в принтер карта будет выпущена, выпуск следующей карты не будет начат.
- Массовый выпуск может осуществляться как с печатью данных на карте, так и без.



Обязательным условием печати на устройствах является наличие на рабочей станции, с которой происходит печать следующих компонентов:

- Драйвера принтера EDISecure XID8300
- Настроенного соединения с принтером в утилите EDI Secure Connect
- Компонента поддержки принтера **IndeedCM.EdiSecure.Middleware**
- Подключенного через интерфейс USB принтера XID8300



Драйвера принтера EDISecure XID8300 и утилита EDI Secure Connect поставляется производителем вместе с принтером.

IndeedCM.EdiSecure.Middleware поставляется в составе дистрибутива Indeed CM.

Для массового выпуска устройств выполните следующие действия:

1. Перейдите на страницу сервиса <https://<адрес сервера Indeed CM >/icm/bulkissue>
2. Выполните поиск пользователей (например, по месту расположения). Результат поиска отобразится в таблице слева.
3. Отметьте среди найденных пользователей всех, кому необходимо выпустить смарт-карты и нажмите  .
4. Нажмите **Выпустить**. Имя будет подставлено автоматически.
5. Нажмите **Выпустить**.

Массовый выпуск

Корневой контейнер

cmad.indeed

Общее имя(CN)

Общее имя(CN)

Контейнер

msk

Имя

Имя

Фамилия

Фамилия

☐ Отображать заблокированные учетные записи

☐	Общее имя(CN)	Имя и фамилия	Контейнер
☒	Алексей Дмитриев	Алексей Дмитриев	cmad.indeed/MSK Office (Обособленное подразделение)
☒	Евгений Белов	Евгений Белов	cmad.indeed/MSK Office (Обособленное подразделение)
☐	Кирилл Руссков	Кирилл Руссков	cmad.indeed/MSK Office (Обособленное подразделение)

>

<

☐	Общее имя(CN)	Имя и фамилия	Контейнер
☐	Алексей Дмитриев	Алексей Дмитриев	cmad.indeed/MSK Office (Обособленное подразделение)
☐	Евгений Белов	Евгений Белов	cmad.indeed/MSK Office (Обособленное подразделение)

➕ Выпустить

Принтер

XID 8300 (DS)

Выпустить

Отмена

Прогресс выпуска карты для каждого пользователя отображается в нижней части экрана. Выпуск карты можно приостановить нажав **Пауза** или отменить, нажав **Отмена**.

+ Выпустить

Пользователь: Евгений Белов

Загрузка карты

Пауза

Отмена

В случае возникновения ошибки при массовом выпуске, пользователь, на котором произошла ошибка, выделяется красным, а в нижней части экрана отображается текст ошибки.

Массовый выпуск

Корневой контейнер

Общее имя(CN)

Контейнер

Имя

Фамилия

☐ Отображать заблокированные учетные записи

☐	Общее имя(CN)	Имя и фамилия	Контейнер
☒	Алексей Дмитриев	Алексей Дмитриев	smad.indeed/MSK Office (Обособленное подразделение)
☒	Евгений Белов	Евгений Белов	smad.indeed/MSK Office (Обособленное подразделение)
☐	Кирилл Руссков	Кирилл Руссков	smad.indeed/MSK Office (Обособленное подразделение)

Выпустить

Пользователь: Евгений Белов

Смарт-карта не отвечает на сигнал сброса состояния.

Повторить

Пропустить

Отмена

После устранения ошибки выпуск можно повторить нажав на соответствующую кнопку. Для игнорирования ошибки и продолжения массового выпуска карт нажмите **Пропустить**. Для отмены массового выпуска для всех пользователей нажмите **Отмена**.

Назначенные СКЗИ

СКЗИ может быть закреплено за пользователем при **Назначении устройства** (Тип: Ключевой носитель), при **Выпуске устройства** пользователю (Тип: Ключевой документ, Ключевой носитель), или в любой другой момент времени в разделе **СКЗИ**. Назначенные на пользователя СКЗИ отображаются в его карточке:

Назначенные СКЗИ

Наименование	Серийный номер	Номер экземпляра	Состояние
▶ ☐ Ключевой носитель - Rutoken ECP	0894130607		Назначено 
▼ ☐ Ключевой документ	0894130607	688D78EC-0799-4A62-B775-1F7913E04E73	Назначено 

Отметка об изготовлении
Изготовитель: Adm
Номер и дата документа: ВН-127, 04.09.2020 13:52

[+ Добавить СКЗИ](#) [# Редактировать СКЗИ](#) [- Уничтожить/изъять СКЗИ](#)

Печать СКЗИ

Если в систему добавлены **Шаблоны печати** для соответствующего типа СКЗИ, то имеется возможность распечатать СКЗИ по заданным шаблонам:

1. Для печати средства криптографической защиты информации нажмите .
2. Выберите **Шаблон печати** и нажмите **Печать**.

Назначенные СКЗИ

Наименование	Серийный номер	Номер экземпляра	Состояние
▼ ☐ Лицензия - КриптоПро CSP 5.0	4040Q-73010-KYE6B-N510U-3F07H		Назначено 

Печать СКЗИ

Шаблон печати

Шаблон лицензии ▼

Печать

Отмена

[+ Добавить СКЗИ](#) [# Редактировать СКЗИ](#) [- Уничтожить/изъять СКЗИ](#)

Добавление СКЗИ

1. Нажмите **Добавить СКЗИ** для закрепления нового средства криптографической защиты информации за пользователем.
2. Задайте значения параметров СКЗИ:
 - **Тип** (Дистрибутив, Лицензия, Документация, Ключевой документ, Ключевой носитель, Пользовательский). Обязательно для заполнения.
 - **Описание**. Обязательно для заполнения.
 - **Серийный номер**. Обязательно для заполнения.
 - **Номер экземпляра**. При создании СКЗИ в момент выпуска устройства, устанавливается автоматически имя контейнера, содержащего ключевую пару. Необязательное поле для заполнения.
 - **Номер и дата документа**, на основании которого добавляется СКЗИ. Обязательно для заполнения.
3. Нажмите **Добавить**.

[➕ Добавить СКЗИ](#) [✎ Редактировать СКЗИ](#) [🗑 Уничтожить/изъять СКЗИ](#)

Добавить СКЗИ

Тип

Дистрибутив ▼

Описание

КриптоПро CSP 5.0

Серийный номер

4040Q-93010-06E9A-0WNNHK-H2376

Номер экземпляра

4040Q-93010

Номер и дата документа

ВН-321/48 04.09.2020 15:21 📅

Добавить **Отмена**

Редактирование СКЗИ

Имеющиеся у пользователя СКЗИ могут быть отредактированы уполномоченным сотрудником: оператором или администратором Indeed CM.

1. Для редактирования выберите средство криптографической защиты информации и нажмите **Редактировать СКЗИ**.

Назначенные СКЗИ

Наименование	Серийный номер	Номер экземпляра	Состояние
☒ Дистрибутив - КриптоПро CSP 5.0	4040Q-93010-06E9A-0WNHK-H2376	4040Q-93010	Назначено

Отметка об изготовлении
Изготовитель: Adm
Номер и дата документа: ВН-321/48, 04.09.2020 15:21

[+ Добавить СКЗИ](#) [✎ Редактировать СКЗИ](#) [🗑 Уничтожить/изъять СКЗИ](#)

Поля, доступные для редактирования:

- Отметка о передаче
- Отметка о возврате
- Отметка о выдаче
- Отметка о подключении
- Примечание
- Дополнительные поля (дополнительные атрибуты, заданные в разделе [Журнал учета СКЗИ](#) Мастера настройки Indeed CM)

 Перечень полей указан в соответствии с типовой формой журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (для органа криптографической защиты информации), утвержденной Приказом ФАПСИ от 13 июня 2001 г. 152.

2. Внесите необходимые изменения и нажмите **Сохранить**.

Уничтожение и изъятие СКЗИ

1. Для уничтожения или изъятия СКЗИ выберите средство криптографической защиты информации и нажмите **Уничтожить/изъять СКЗИ**.
 - Укажите имя сотрудника, выполняющего уничтожение/изъятие СКЗИ.
 - **Номер и дату документа**, на основании которого осуществляется уничтожение /изъятие.
 - Выберите опцию **Использовать повторно** в случае повторного использования СКЗИ (например: при выдаче дистрибутива другому сотруднику).
2. Нажмите **Уничтожить/Изъять**.

Уничтожить/изъять СКЗИ

Сотрудник, производивший уничтожение/изъятие

Olga Nikiforova

Номер и дата документа

ВН-541/53

04.09.2020 15:33



☒ Использовать повторно

Уничтожить/Изъять

Отмена

События пользователя

В карточке пользователя отображается информация о пяти последних событиях в системе Indeed Certificate Manager для данного пользователя. Список событий можно обновить нажав кнопку . Чтобы посмотреть расширенную информацию по необходимому событию, нажмите .

Последние события 

Время	Код	Событие	Сервис	Тип устройства	Серийный номер	Инициатор
  04.09.2020 8:46:13	5	Выпуск устройства	Консоль управления	Rutoken ECP	0894130607	DEMO\Adm
Устройство успешно выпущено. Пользователь: Evgeniy Belov Политика: Базовая политика Устройство: Rutoken ECP:0894130607 Сертификаты: Квалифицированный пользователь:7A115F002CAC688A4E3A811098B28EB5 Общие сертификаты: Отслеживаемые сертификаты: Инициатор: DEMO\Adm						
  04.09.2020 8:46:12	301	Добавление СКЗИ	Консоль управления			DEMO\Adm
  03.09.2020 18:00:01	4	Отмена назначения устройства	Консоль управления	Rutoken ECP	0894130607	DEMO\Adm
  03.09.2020 18:00:01	303	Уничтожение/изъятие СКЗИ	Консоль управления			DEMO\Adm
  03.09.2020 17:46:43	1004	Отмена назначения устройства	Консоль управления	Rutoken ECP	0894130607	DEMO\Adm

[Просмотреть все](#) 

Для просмотра полного списка событий и перехода в раздел [Журнал](#) нажмите **Просмотреть все**.

Устройства

Подключенные устройства

Поиск по подключенному устройству применяется в случае, если устройство физически доступно, но никаких других данных о нем нет (например, сотрудник нашел утерянный USB-токен и передал его администратору).

Перейдите на вкладку **Подключенное устройство**, подключите устройство к рабочей станции и нажмите .

Поиск устройства

Подключенное устройство

Расширенный

Aktiv Rutoken ECP 0: Rutoken ECP

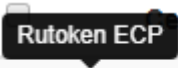


[+ Добавить устройство](#) [+ Выпустить устройство](#) [+ Выпустить AirKey](#) [✎ Изменить теги](#) [+ Создать задачи](#)

[+ Импортировать устройства](#)

☐	Серийный номер	Комментарий	Пользователь	Политика	Состояние	
☐	 0894130607	Бухгалтерия	Evgeniy Belov	Базовая политика	Выпущено	

Тип устройства можно просмотреть наведя указатель мыши на изображение устройства.

	Серийный номер	Комментарий	Пользователь
  0894130607	Бухгалтерия	Evgeniy Belov	

Другие доступные операции:

- [Добавление устройства](#)
- [Выпуск устройства](#)
- [Удаление устройства](#)
- [Инициализация пустых устройств](#)
- [Изменение тегов устройств](#)
- [Создание массовых задач на клиентском агенте](#)
- [Пакетное добавление устройств](#)

Расширенный поиск устройств

Расширенный поиск применяется в случае, если устройство физически недоступно, но известны некоторые его данные (серийный номер или его часть, тип устройства, комментарий, состояние, статус содержимого, имя пользователя, политика, назначенные теги). Поиск осуществляется по одному или нескольким (всем) параметрам.

Чтобы выполнить поиск, укажите известные данные устройства и нажмите .

✓ Для вывода списка всех устройств введите символ * в поле Серийный номер и выполните поиск.

Для поиска устройства по части серийного номера введите символ * и известную часть номера.

Поиск устройства

Подключенное устройство

Расширенный

Серийный номер

Тип

Серийный ном

Не задано

Комментарий

Комментарий

Состояние

Не задано

Статус содержимого

Не задано

Пользователь

evgeniy belov

Политика

Не задано

Теги



[+ Добавить устройство](#) [+ Выпустить устройство](#) [+ Выпустить AirKey](#) [✎ Изменить теги](#) [+ Создать задачи](#)
[+ Импортировать устройства](#)

☐	Серийный номер	Комментарий	Пользователь	Политика	Состояние	
☐	 0894130607	Бухгалтерия	Evgeniy Belov	Базовая политика	Выпущено	
☐	 0755398982		Evgeniy Belov	Базовая политика	Выпущено	

⚠ Для фильтрации карт по статусу содержимого требуется [настроенный по расписанию запуск службы Card Monitor](#).

Результаты поиска устройств могут быть сохранены в виде файла. Для создания файла с результатами поиска нажмите  и выберите формат (PDF или CSV). Сохраните полученный файл.

Для просмотра содержимого устройства нажмите . Для просмотра PIN-кода администратора нажмите .

[+ Добавить устройство](#)
[+ Выпустить устройство](#)
[+ Выпустить AirKey](#)
[✎ Изменить теги](#)
[+ Создать задачи](#)
[+ Импортировать устройства](#)

☐	Серийный номер	Комментарий	Пользователь	Политика	Состояние	
☐	 0894130607	Бухгалтерия	Evgeniy Belov	Базовая политика	Выпущено	

Сбросить PIN-код
Разблокировать
Выключить
Отозвать
Заменить
Заменить на AirKey
Обновить

Заблокировать
Сменить PIN-код администратора

Имя устройства

Evgeniy Belov

Комментарий

Бухгалтерия 

Политика

Базовая политика

PIN-код администратора



Теги

demo

rutoken 

Сертификаты

Шаблон	УЦ	Действителен до	Состояние	
Вход по смарт-карте	demo-DC-CA	06.02.2021 10:10	Действительный	 

Заккрыть

Для изменения комментария или тегов нажмите  в соответствующих полях.


 Администраторам Indeed CM доступен просмотр PIN-кодов всех добавленных в систему устройств. Администраторам отдельных политик доступен просмотр только PIN-кодов устройств, назначенных/выпущенных пользователям этих политик.

Добавление устройства

1. Для добавления устройства в Indeed Certificate Manager подключите устройство к компьютеру и нажмите **Добавить устройство**.
2. Если добавляемое устройство поддерживает аппаратную криптографию и в системе ведется учет СКЗИ, то укажите **Номер и дату документа** (приказа, распоряжения), в соответствии с которым будет изготовлено СКЗИ (Тип: Ключевой носитель). Информация об имеющихся в системе средствах криптографической защиты информации располагается в разделе [СКЗИ](#).
3. Устройство добавляется двумя способами:
 - **Без указания PIN-кода администратора** - установленный на устройстве PIN-код администратора должен совпадать с указанным в разделе **Типы устройств**.
 - **С указанием PIN-кода администратора** - установленный на устройстве PIN-код администратора указывается в одноименном поле после нажатия кнопки **Дополнительно**.
4. Нажмите **Добавить**.



При добавлении устройства PIN-код администратора заменяется на случайный или указанный в разделе [Типы устройств](#) конфигурации системы.



После добавления устройства с установкой случайного PIN-кода администратора вне Indeed CM будет невозможно разблокировать PIN-код пользователя и провести инициализацию отдельных видов устройств.

Поиск устройства

Подключенное устройство

Расширенный

Aktiv Rutoken ECP 0: Rutoken ECP

Q

[+ Добавить устройство](#) [+ Выпустить устройство](#) [+ Выпустить AirKey](#) [✎ Изменить теги](#) [+ Импортировать устройства](#)

Считыватель

Aktiv Rutoken ECP 0: Rutoken ECP

Номер и дата документа

ВН-121

25.11.2021 11:33



[Дополнительно](#)

PIN-код администратора

PIN-код администратора

Добавить

Отмена

5. После добавления устройства нажмите **Заккрыть**. Устройства можно добавлять автоматически подключая их последовательно к одному и тому же считывателю.

Устройство добавлено

Вставьте следующее устройство в считыватель '**Aktiv Rutoken ECP 0**' или нажмите 'Заккрыть' для завершения процесса

Заккрыть

Выпуск устройства

Выпуск устройств и виртуальных карт AirKey в разделе **Устройства** аналогичен выпуску из [Карточки пользователя](#).

Удаление устройства

Удаление устройства из Indeed Certificate Manager возможно как при наличии устройства, так и без него.

❗ Если PIN-код администратора устройства был изменен на случайный при добавлении устройства (опция [Устанавливать неслучайный PIN-код администратора](#) выключена в разделе **Конфигурация > Типы устройств**), то при удалении устройства без подключения к рабочей станции PIN-код администратора останется случайным и неизвестным!

Для удаления устройства выполните его поиск и нажмите  .

☐	Серийный номер	Комментарий	Пользователь	Политика	Состояние	
☐	 0894130607				Пустое	 

Удалить устройство

- ☒ Устройство доступно
☐ Устройство недоступно (потеряно или повреждено)

Номер и дата документа



- ☐ Инициализировать устройство

Вставьте устройство и нажмите 'Удалить'

1. Если **Устройство доступно**:

- Если удаляемое устройство поддерживает аппаратную криптографию и в системе ведется учет СКЗИ, то укажите **Номер и дату документа** (приказа, распоряжения), в соответствии с которым будет уничтожено СКЗИ (Тип: Ключевой носитель) по данному устройству.
- Подключите его к компьютеру и нажмите **Удалить**.



При включении опции **Инициализировать устройство** все содержимое (в том числе, сертификаты, записанные до ввода устройства в Indeed CM) будет удалено.

2. Если **Устройство недоступно**, выберите соответствующий пункт:

- Если удаляемое устройство поддерживает аппаратную криптографию и в системе ведется учет СКЗИ, то укажите **Номер и дату документа** (приказа, распоряжения), в соответствии с которым будет уничтожено СКЗИ (Тип: Ключевой носитель) по данному устройству.
- Нажмите **Удалить**.

Возможно изъятие устройства у пользователя, если оно было выпущено ранее и затем отозвано, без удаления из системы. Действие применимо как для доступного, так и для недоступного устройства.

Инициализация пустых устройств

Indeed CM позволяет выполнять инициализацию добавленных устройств, находящихся в состоянии **Пустое** (не закрепленных за пользователем), в том числе с использованием клиентского агента.

 Операция **Инициализировать** доступна, если задана соответствующая привилегия в разделе **Роли**.

1. Выберите устройство и нажмите  для просмотра его содержимого.

☐	Серийный номер	Комментарий	Пользователь	Политика	Состояние	
☐	 0755398982				Пустое	

Инициализировать

Сменить PIN-код администратора

Комментарий



PIN-код администратора



Теги



Заккрыть

2. Подключите устройство к рабочей станции и нажмите **Инициализировать**. Если устройство недоступно, то для создания задачи на клиентском агенте выберите опцию **Инициализировать устройство на агенте**.

- Нажмите **Инициализировать**, если PIN-код администратора на устройстве совпадает с сохраненным в хранилище системы.

После инициализации PIN-код администратора на устройстве и в базе не изменится, PIN-код пользователя будет сброшен на значение, указанное в **Типе устройства**.

Инициализировать

Сменить PIN-код администратора

☐ Инициализировать устройство на агенте

Устройство будет проинициализировано. Все данные на устройстве будут потеряны

[Дополнительно >](#)

Вставьте устройство и нажмите 'Инициализировать'

Инициализировать

Отмена

- Если PIN-код администратора на устройстве не совпадает с сохраненным в хранилище системы, то укажите его в разделе **Дополнительно**. Задайте **Новый PIN-код пользователя**, если требуется установить его в процессе выполнения инициализации, и нажмите **Инициализировать**.
После инициализации PIN-код администратора в хранилище системы будет заменен на указанное значение.

Инициализировать

Сменить PIN-код администратора

☐ Инициализировать устройство на агенте

Устройство будет проинициализировано. Все данные на устройстве будут потеряны

[Дополнительно ▾](#)

PIN-код администратора

Новый PIN-код пользователя

Вставьте устройство и нажмите 'Инициализировать'

Инициализировать

Отмена



Для устройств **Rutoken** и **eToken** возможно провести инициализацию с PIN-кодом администратора в состоянии: известный, неизвестный, заблокированный.

- если PIN-код администратора не указан, то после инициализации на устройство будет записан PIN-код, сохраненный в базе Indeed CM
- если PIN-код администратора указан, то после инициализации он будет записан на устройство и в базу Indeed CM

Изменение тегов

Изменение тегов доступно для нескольких устройств сразу.

✓ Теги создаются в разделе **Теги** на вкладке **Конфигурация** администратором.

Для добавления или удаления тегов перейдите в раздел **Устройства** на вкладку **Расширенный** поиск, выберите требуемые устройства и нажмите **Изменить теги**.

Поиск устройства

Подключенное устройство

Расширенный

Серийный номер

Тип

Серийный ном

Не задано

Комментарий

Комментарий

Состояние

Не задано

Статус содержимого

Не задано

Пользователь

evgeniy below

Политика

Не задано

Теги

Q

[+ Добавить устройство](#) [+ Выпустить устройство](#) [+ Выпустить AirKey](#) [✎ Изменить теги](#) [+ Создать задачи](#)
[+ Импортировать устройства](#)

☒	Серийный номер	Комментарий	Пользователь	Политика	Состояние	
☒	0894130607	Бухгалтерия	Evgeniy Belov	Базовая политика	Выпущено	
☒	0755398982	Подпись документов	Evgeniy Belov	Базовая политика	Выпущено	

Укажите **Теги для добавления** или **Теги для удаления** и нажмите **Изменить**:

[+ Добавить устройство](#) [+ Выпустить устройство](#) [+ Выпустить AirKey](#) [✎ Изменить теги](#) [+ Создать задачи](#)
[+ Импортировать устройства](#)

Теги для добавления

demo x rutoken x

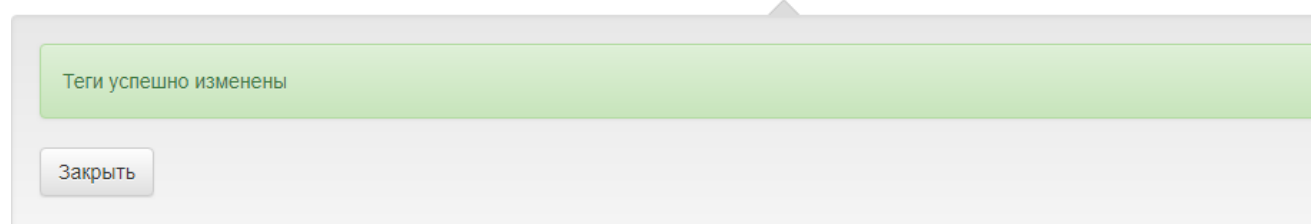
Теги для удаления

Изменить

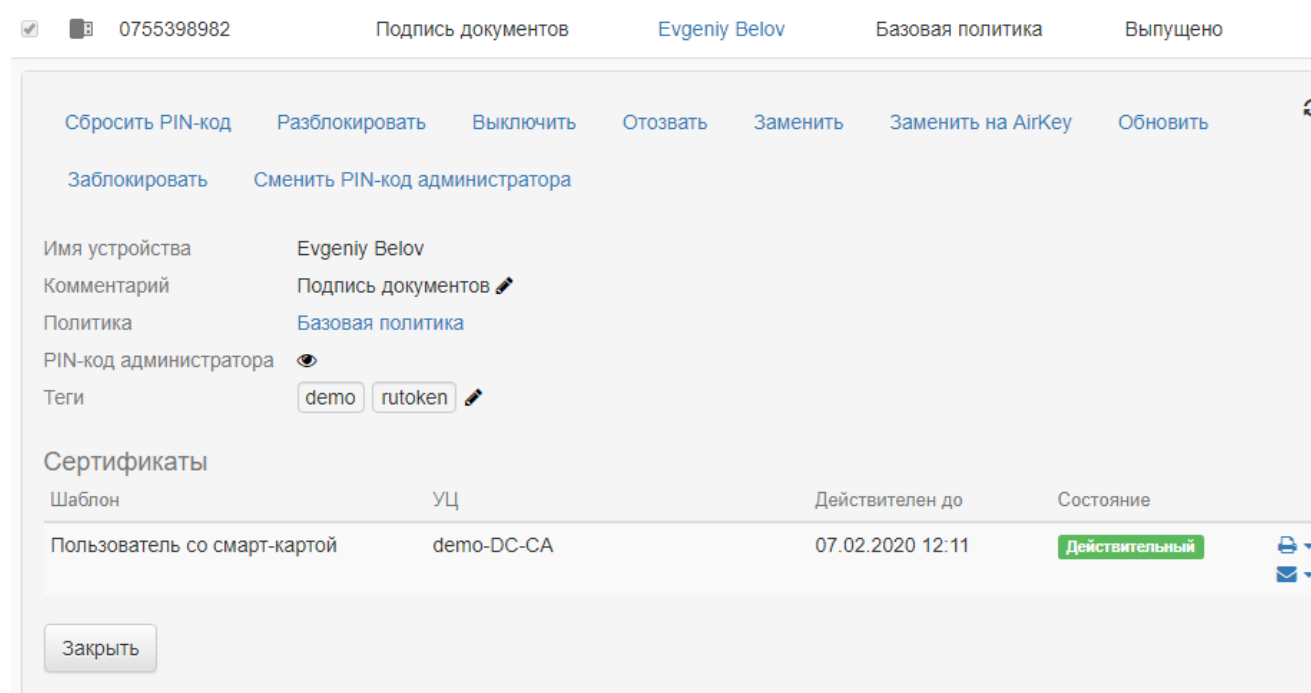
Отмена

☒	Серийный номер	Комментарий	Пользователь	Политика	Состояние	
☒	0894130607	Бухгалтерия	Evgeniy Belov	Базовая политика	Выпущено	
☒	0755398982	Подпись документов	Evgeniy Belov	Базовая политика	Выпущено	

При успешном изменении тегов появится соответствующее сообщение:



Проверить, что теги были изменены, можно посмотрев содержимое выбранного устройства. Выберите устройство и нажмите .



Для изменения уже назначенных тегов нажмите  в поле **Теги**.

Пакетное добавление устройств

Для пакетного добавления устройств на вкладке **Устройства**:

1. Нажмите **Импортировать устройства**.
2. Загрузите подготовленный **Файл устройств**.
3. Нажмите **Импортировать**.

Поиск устройства

Подключенное устройство

Расширенный

ACS CCID USB Reader 0: IDProtect (X)

+

Добавить устройство

+

Выпустить устройство

+

Выпустить AirKey

Изменить теги

+

Создать задачи

+

Импортировать устройства

Файл устройств

Cards.csv

Импортировать

Отмена

Поддерживается импорт устройств из файла в формате TXT (UTF-8) и CSV. Файл должен содержать строки с набором полей следующего формата:

**Serial Number;Card Type;Model;Form Factor;Admin PIN;Gost Admin PIN;Comment;Tags;
SKZI Document Number;Time Created**

- **Serial Number** - серийный номер устройства.
- **Card Type** - тип устройства. Необходимо указывать имя типа в том виде, в котором он указан в разделе **Типы устройств**.

Serial Number и **Card Type** являются обязательными параметрами.

- **Model** - модель устройства доступна только для устройств [JaCarta](#), [eToken PRO Java 72K](#) и [IDPrime MD](#), если в разделе **Типы устройств** для данных карт добавлено разделение по различным моделям.
- **Form Factor** - форм-фактор устройства. Поддерживаются:
 - SmartCard (по умолчанию)
 - UsbToken
 - MicroSD



Если форм-фактор не указан, то устройство будет добавлено как смарт-карта.

- **Admin PIN** - значение PIN-кода администратора, которое будет присвоено всем перечисленным в файле импорта устройствам.
- **Gost Admin PIN** - значение PIN-кода администратора ГОСТ областей для устройств JaCarta\JaCarta-2, которое будет присвоено всем перечисленным в файле импорта устройствам.
- **Comment** - комментарий к устройствам.
- **Tags** - теги к устройствам. Указываемые теги необходимо предварительно создать в разделе **Теги**.



Если требуется добавить несколько тегов для импортируемых устройств, то в файле импорта укажите их через запятую: Ter1,Ter2.

- **SKZI Document Number** - если импортируемые устройства поддерживают аппаратную криптографию и в системе ведется учет СКЗИ, то укажите **Номер документа** (приказа, распоряжения), в соответствии с которым произведена постановка на учет СКЗИ (Тип: Ключевой носитель). Информация об имеющихся в системе средствах криптографической защиты информации располагается в разделе [СКЗИ](#).
- **Time Created** - время создания документа. Указывается в формате ууууММддННммсс (UTC). Если значение не указано, то в качестве времени создания документа автоматически подставляется время импорта СКЗИ.

Если вместо поля **Serial Number** (Серийный номер) устройства прописано значение **default**, то значения оставшихся полей (Card Type; Model; Form Factor; Admin PIN; Gost Admin PIN; Comment; Tags; SKZI Document Number; Time Created) данной строки будут использоваться как значения по умолчанию для соответствующих полей последующих строк, т.е. для последующих строк необходимо указать только серийный номер и поле, которое отличается от указанного в строке default.

В представленном ниже примере в файл добавлены:

- USB-токены **Rutoken S** с серийными номерами: 0755398982, 0756309531, с указанным комментарием: Московский офис и тегами: VPN, IT.
- USB-токены **Rutoken ECP** с серийными номерами: 0894130607, 0894130536, с указанным комментарием: Бухгалтерия, тегом: VPN и номером документа СКЗИ: ВН-169 от 04.12.2022 в 16:42:00 по московскому времени (GMT+3).
- Смарт-карты **Rutoken ECP** с серийными номерами: 0862287268, 0862287403, с указанным номером документа СКЗИ: ВН-170 от 29.03.2022 в 14:15:00 по московскому времени (GMT+3).
- USB-токен **Rutoken 2151** с серийным номером: 0963474291, с указанным номером документа СКЗИ: ВН-171 от текущего числа и времени.
- USB-токены **ESMART Token 64K** с серийными номерами: 609BC06881C7, B0B340508942.
- Смарт-карты **ESMART Token 64K** с серийными номерами: E0D8806291CB, D050806291CB.
- Смарт-карта **eToken PRO Java 72K** модели **eToken PRO Java 72K OS755** с серийным номером: 01сес45d.
- USB-токены **JaCarta PKI/Flash** (без ГОСТ области) модели **JC210** с серийными номерами: 0B53002004417597, 0B53001122617597.
- Смарт-карта **JaCarta PKI** (без ГОСТ области) модели **JC300** с серийным номером: 0153001910367618.



Для импорта устройств **JaCarta PKI** (без ГОСТ области) необходимо выполнить разделение **JaCarta** по различным моделям и в файле импорта обязательно указать поле модель устройства (Model).

- USB-токены **JaCarta-2 SE/PKI/ГОСТ** модели **JC267-1236J.J01Q01** с серийными номерами: 6082057494937678, 4C54001522634C50 и с указанным номером документа СКЗИ: ВН-172 от текущего числа и времени.
- Смарт-карта **JaCarta PKI/ГОСТ** модели **JC305** с серийным номером: 0B53001917347618 и с указанным номером документа СКЗИ: ВН-173 от 12.04.2022 в 17:55:00 по московскому времени (GMT+3).

Пример Файла устройств:

```
default;Rutoken S;;UsbToken;87654321;;Московский офис;VPN,IT;;
0755398982
0756309531
default;Rutoken ECP;;UsbToken;87654321;;Бухгалтерия;VPN;ВН-169;20220412134200
0894130607
0894130536
default;Rutoken ECP SC;;;87654321;;;ВН-170;20220329111500
0862287268
0862287403
default;Rutoken 2151;;UsbToken;87654321;;;ВН-171;
0963474291
default;ESMART Token 64K;;UsbToken;12345678;;;;
609BC06881C7
B0B340508942
E0D8806291CB;;;SmartCard;;;;
D050806291CB;;;SmartCard;;;;
default;eToken PRO Java 72K;eToken PRO Java 72K OS755;SmartCard;1234567890;;;;
01cec45d
default;JaCarta;JC210;UsbToken;00000000;;;;
0B53002004417597
0B53001122617597
default;JaCarta;JC300;SmartCard;00000000;;;;
0153001910367618
default;JaCarta;JC267-1236J.J01Q01;UsbToken;00000000;1234567890;;;ВН-172;
6082057494937678
4C54001522634C50
0B53001917347618;;JC305;SmartCard;;;;ВН-173;20220412145500
```

Агенты

✔ Раздел доступен если выполнена настройка Indeed CM для работы с клиентскими агентами (опция **Разрешить использование клиентских агентов** в разделе **Клиентский агент** Мастера настройки Indeed CM) и предоставленной привилегии **Просмотр репозитория агентов** членам Роли.

⚠ Если в разделе **Клиентский агент** Мастера настройки Indeed CM отключена **Автоматическая регистрация агентов**, то после установки и настройки Агента на рабочей станции он появится в разделе со статусом **Ожидает регистрации**.

Поиск агента

Имя	Статус	Имя компьютера
Имя	Ожидает регистрации ▼	Имя компьютера
Операционная система	IP-адрес	Комментарий
Операционная система	IP-адрес	Комментарий

Имя агента	Имя компьютера	Операционная система	IP-адрес	Комментарий	Статус
Win7x86.demo.local	Win7x86.demo.local	Windows 7 Service Pack 1 (x86)	192.168.43.133		Ожидает регистрации
Indeedcmru.demo.local	Indeedcmru.demo.local	Windows Server 2016 (x64)	::1		Ожидает регистрации

Для поиска Агента укажите один или несколько параметров:

- **Имя агента** – по умолчанию в качестве имени задается версия операционной системы, на которой установлен Агент. Имя можно изменить в профиле Агента.
- **Имя компьютера** – DNS имя компьютера.
- **Операционная система** – версия операционной системы, на которой установлен Агент.
- **IP-адрес** – IP-адрес компьютера (IPv4 или IPv6), на котором установлен Агент.
- **Комментарий** – комментарий, заданный администратором Indeed CM в профиле Агента.
- **Статус** – текущее состояние Агента. Возможные значения:
 - Не задано – поиск производится без учёта статуса
 - Ожидает регистрации
 - Зарегистрирован
 - Отклонен

Поддерживаемые шаблоны поиска:

- Полное совпадение – **Win7x86.demo.local**
- Частичное совпадение – ***86.demo.local** или ***demo***
- Все результаты – *****

Перейдите в [Профиль Агента](#), нажав на его имя в результатах поиска и нажмите **Зарегистрировать** для подтверждения запроса на регистрацию или отклоните запрос нажав **Отклонить**.

Win7x86.demo.local



Имя компьютера	Win7x86.demo.local
Операционная система	Windows 7 Service Pack 1 (x86)
Комментарий	
IP-адрес	192.168.43.133
Статус регистрации	Ожидает регистрации
Дата регистрации	29.07.2019 13:02
Дата последней активности	29.07.2019 13:02
SID компьютера	S-1-5-21-626637504-300677628-431683531
Доменный SID компьютера	S-1-5-21-170561308-2550214590-1584262309-1110
MAC адрес	00-0C-29-9D-AF-6A

Агент в состоянии ожидания регистрации

☒ Зарегистрировать ☐ Отклонить

Вы уверены, что хотите зарегистрировать агента?

Зарегистрировать

Отмена

В области уведомления Windows появится значок .



- [Профиль Агента](#)
- [Назначение устройства в Агенте](#)
- [Контроль за использованием устройств](#)
- [Назначение задач](#)
 - [Сброс PIN-кода пользователя](#)
 - [Смена PIN-кода администратора](#)
 - [Очистка устройства на агенте](#)
 - [Обновление устройства на агенте](#)
 - [Блокировка устройства](#)
 - [Инициализация устройства на агенте](#)
 - [Массовые задачи](#)
- [Мониторинг подключенных устройств](#)
- [Журнал событий](#)

Профиль Агента

В профиле содержится информация об Агенте, сессиях пользователей, привязанных устройствах и последних событиях, связанных с Агентом.

Win7x86.demo.local

Имя компьютера	Win7x86.demo.local
Операционная система	Windows 7 Service Pack 1 (x86)
Комментарий	
IP-адрес	192.168.43.133
Статус регистрации	Зарегистрирован
Дата регистрации	29.07.2019 13:02
Дата последней активности	29.07.2019 13:02
SID компьютера	S-1-5-21-626637504-300677628-431683531
Доменный SID компьютера	S-1-5-21-170561308-2550214590-1584262309-1110
MAC адрес	00-0C-29-9D-AF-6A

[✎ Изменить имя](#) [✎ Изменить комментарий](#)

Сессии

Нет активных сессий

Привязанные устройства

Нет привязанных устройств

[+ Привязать устройство](#)

Последние события

	Время	Событие	Сервис
▶ 	29.07.2019 13:02:18	Регистрация агента	Сервис регистрации агентов

[Просмотреть все ➔](#)

Имя Агента (Win7x86.demo.local выделено крупным шрифтом) – обязательный параметр. По умолчанию в качестве значения используется DNS-имя компьютера, на котором установлен Агент. Для редактирования нажмите **Изменить имя**.

Комментарий – необязательный параметр. По умолчанию отсутствует. Для установки или редактирования комментария нажмите **Изменить комментарий**.

Сессии – сессии пользователей, выполнивших вход на рабочую станцию (не обязательно по смарт-карте) или сессии сервисных служб (отображаются, когда рабочая станция включена).

Существует два типа сессий пользователя:

- **Консольная** – пользователь выполнил вход на рабочую станцию напрямую
- **Терминальная** – пользователь подключился к рабочей станции удаленно (например, по RDP)

Привязанные устройства – список устройств, закрепленных администратором Indeed CM за Агентом.

Последние события – последние пять событий, связанных с работой Агента.

Пример профиля Агента с сессиями и устройством пользователя:

Win7x86.demo.local



Имя компьютера	Win7x86.demo.local
Операционная система	Windows 7 Service Pack 1 (x86)
Комментарий	
IP-адрес	192.168.43.133
Статус регистрации	Зарегистрирован
Дата регистрации	29.07.2019 13:02
Дата последней активности	29.07.2019 13:29
SID компьютера	S-1-5-21-626637504-300677628-431683531
Доменный SID компьютера	S-1-5-21-170561308-2550214590-1584262309-1110
MAC адрес	00-0C-29-9D-AF-6A

[✎ Изменить имя](#) [✎ Изменить комментарий](#)

Сессии

> NT AUTHORITY\SYSTEM 1
> DEMO\Evgeniy.Belov 1 Консольная

Привязанные устройства

Серийный номер	Тип	Комментарий	Пользователь	Состояние
0894130913	Rutoken ECP		Evgeniy Belov	Выпущено

[+ Привязать устройство](#)

Последние события

Время	Событие	Сервис	Тип устройства	Серийный номер	Пользователь
▶ 29.07.2019 13:32:22	Подключение устройства	Сервис агентов	Rutoken ECP	0894130913	NT AUTHORITY\SYSTEM

Назначение устройства в Агенте

Агент Indeed CM автоматически определяет подключенные к рабочей станции устройства (USB-токены, смарт-карты) и запрашивает у сервера Indeed Certificate Manager перечень задач, которые требуется выполнить с устройствами. Закреплять устройство пользователя за его рабочей станцией в этом случае не требуется.

Закрепление устройства за рабочей станцией (Агентом) позволит контролировать использование устройств в организации. Например, Агент сможет выполнять определенные действия при подключении незакрепленных за ним устройств (см. **Контроль за использованием устройств**).

Для закрепления устройства за Агентом перейдите в раздел **Привязанные устройства** в профиле Агента и нажмите **Привязать устройство**.

- Если устройство доступно, подключите его к рабочей станции или выберите из списка подключенных и нажмите **Привязать**:

Привязанные устройства

Нет привязанных устройств

[+ Привязать устройство](#)

- ☒ Устройство доступно
☐ Устройство недоступно

Устройство

Aktiv Rutoken ECP 0: CP_RutokenEC ▼

Привязать

Отмена

- Если устройство недоступно, то укажите его серийный номер, тип и нажмите **Привязать**:

Привязанные устройства

Нет привязанных устройств

 [Привязать устройство](#)

- ☐ Устройство доступно
- ☒ Устройство недоступно

Серийный номер и тип устройства



Привязать

Отмена

Устройство отобразится в разделе **Привязанные устройства** профиля Агента. Для отвязки устройства нажмите  и затем **Отвязать**.

Привязанные устройства

Серийный номер	Тип	Комментарий	Пользователь	Состояние
 0898392427	Rutoken ECP			Пустое

Отвязать устройство

Отвязать

Отмена

Контроль за использованием устройств

Для привязанных к Агенту устройств в разделе **Контроль** политики Indeed Certificate Manager задаются настройки использования. При подключении устройства к рабочей станции Агент, установленный на ней, реагирует на события:

- **При нарушении условий привязки устройства к агенту.** Например, пользователь подключил к своей рабочей станции чужую смарт-карту, и она не привязана к его Агенту.
- **При нарушении условий привязки устройства и пользователя.** Например, пользователь выполнил вход на рабочую станцию по смарт-карте, привязанной к его Агенту, а затем сменил учетную запись в операционной системе.

 Для пользователей составного каталога и каталога КриптоПро УЦ 2.0 контроль за привязкой пользователя к Агенту не осуществляется.

При обнаружении Агентом одного из событий возможны действия:

- Запись события в журнал Indeed CM
- Блокировка пользовательской сессии, запись события
- Блокировка устройства, запись события
- Блокировка пользовательской сессии и устройства, запись события

Если выбрано действие **Блокировка пользовательской сессии** или **Блокировка пользовательской сессии и устройства**, то необходимо указать **Таймаут до блокировки пользовательской сессии**, максимальное значение 5 секунд.

Контроль за использованием устройств

Действие, выполняемое при нарушении условий привязки устройства к агенту

Блокировка пользовательской сессии и устройства, запись события

▼

Сообщение при нарушении условий привязки устройства к агенту

Подключенное устройство {model}: {sn} запрещено использовать на данном ПК.

Таймаут до блокировки пользовательской сессии (сек.)

5

Для включения отслеживания Агентом привязки сессии пользователя к подключенному устройству включите опцию **Включить проверку привязки устройства к пользователю**. Если предполагается использование Агентов и устройств на рабочих станциях, не входящих в домен вашей организации, то включите опцию **Проверять условия привязки устройства к пользователю на компьютерах, не включенных в домен**.

☒ Включить проверку привязки устройства к пользователю

☒ Проверять условия привязки устройства к пользователю на компьютерах, не включенных в домен

Действие, выполняемое при нарушении условий привязки устройства к пользователю

Блокировка пользовательской сессии, запись события

Сообщение при нарушении условий привязки устройства к пользователю

Подключенное устройство {model}: {sn} не соответствует сессии пользователя.

Таймаут до блокировки пользовательской сессии (сек.)

5

Сохранить

Задайте сообщение, которое будет отображаться пользователю при нарушении привязки и действие, которое должен выполнить Агент в этом случае.

В сообщениях пользователю допустимо использовать следующие атрибуты:

- {sn} – вывод серийного номера устройства
- {atr} – вывод значения [ATR](#) устройства
- {model} – вывод модели устройства
- {label} – вывод метки устройства

Пример:

"Подключенное устройство {model}: {sn} не соответствует сессии пользователя."

Назначение задач

Управление устройствами и их содержимым осуществляется Агентами через задачи. Если задача не требует действия от пользователя, то её выполнит любой агент, а если требует (например, ввод ответов на секретные вопросы для разблокировки устройства), то задачу выполнит только тот агент, к которому привязано устройство.



Операции, требующие действий пользователя, выполняются только внутри сессии пользователя в операционной системе.

Если привязка устройства к Агенту не установлена и контроль за привязкой устройства к сессии пользователя не включен, то задачи, требующие действия от пользователя, будут выполнены любым Агентом в сессии любого пользователя.

Выполнение задач происходит следующим образом:

1. При подключении устройства к рабочей станции Агент запрашивает у сервера Indeed Certificate Manager назначенные на устройство задачи.
2. Если устройство было подключено ранее к рабочей станции, то Агент будет запрашивать список задач у сервера через заданный интервал времени. По умолчанию каждые 30 секунд.

Задачи, выполняемые Агентом Indeed CM:

- [Сброс PIN-кода пользователя](#)
- [Смена PIN-кода администратора](#)
- [Очистка устройства при его отзыве оператором](#)
- [Инициализация устройства при его отзыве оператором](#)
- [Обновление содержимого устройства](#)
- [Блокировка устройства](#)
- [Инициализация устройства на агенте](#)
- [Назначение массовых задач на устройства](#)
- [Рассылка сообщений пользователю](#)

Задачи для Агента назначаются в разделе [Устройства](#) или в [Карточке пользователя](#).

Задачи (операции) с устройством могут быть выполнены с участием Агента или без него, только с участием Агента или только без его участия.

- Задачи, выполняемые с участием агента имеют соответствующую **опцию** и **уведомление** при ее включении.

▼  Rutoken ECP, 0898392427  Евгений Белов Выпущено

Сбросить PIN-код

Разблокировать

Выключить

Отозвать

Заменить

Заменить на AirKey

Обновить

Заблокировать

Сменить PIN-код администратора

☒ Сбросить PIN-код пользователя на агенте

Будет создана задача по сбросу PIN-кода пользователя

Комментарий

Комментарий

Сбросить

Отмена

- Задачи, которые могут быть выполнены только Агентом Indeed CM имеют уведомление.

▼  Rutoken ECP, 0898392427  Евгений Белов Выпущено

Сбросить PIN-код

Разблокировать

Выключить

Отозвать

Заменить

Заменить на AirKey

Обновить

Заблокировать

Сменить PIN-код администратора

Будет создана задача по блокировке устройства

Комментарий

Комментарий

Заблокировать

Отмена

Назначенная задача добавляется в раздел **Назначенные задачи** в свойствах устройства и отображается в нем до тех пор, пока не будет выполнена или отменена.

▼  **Rutoken ECP, 0898392427**  Evgeniy Belov Выпущено

[Сбросить PIN-код](#) [Разблокировать](#) [Выключить](#) [Отозвать](#) [Заменить](#)

[Заменить на AirKey](#) [Обновить](#) [Заблокировать](#) [Сменить PIN-код администратора](#)

Комментарий Демо 

Политика [Базовая политика](#)

PIN-код администратора 

Теги

rutoken

demo 

Сертификаты

Шаблон	УЦ	Действителен до	Состояние
Вход по смарт-карте	demo-DC-CA	11.04.2020 16:27	Действительный 

Назначенные задачи

Тип	Комментарий	Дата создания	Статус
Сброс PIN-кода	PIN-код забыт	12.04.2019 16:56	Ожидает выполнения 

В свойствах задачи отображаются:

- Тип
- Комментарий
- Дата создания
- Статус

Статус задачи:

Ожидает выполнения

– Задача ожидает выполнения (включения рабочей станции с Агентом, подключения устройства к рабочей станции или завершения выполнения предыдущей задачи).

Выполняется

– Агент Indeed CM приступил к выполнению задачи.

Выполняется

– Задача выполняется слишком долго (более 10 минут).

Выполнена

– Задача успешно выполнена.

Ошибка

– При выполнении задачи возникла ошибка.

Если задача ожидает выполнения или выполняется слишком долго, то её можно **отменить**. Для этого нажмите  и подтвердите действие.

Сброс PIN-кода пользователя

Нажмите **Сбросить PIN-код** в свойствах устройства и включите опцию **Сбросить PIN-код пользователя на агента**. Укажите **Комментарий** (отобразится в [Журнале событий](#) Indeed Certificate Manager) и нажмите **Сбросить**.

❗ Сбросить можно забытый или заблокированный PIN-код пользователя. Для выполнения операции пользователю потребуется ввести ответы на секретные вопросы. Убедитесь, что вопросы и ответы на них установлены в **Self Service**.

Назначенные устройства

▼  **Rutoken ECP, 0898392427**  Евгений Белов Выпущено

Сбросить PIN-код

Разблокировать

Выключить

Отозвать

Заменить

Заменить на AirKey

Обновить

Заблокировать

Сменить PIN-код администратора

☒ Сбросить PIN-код пользователя на агенте

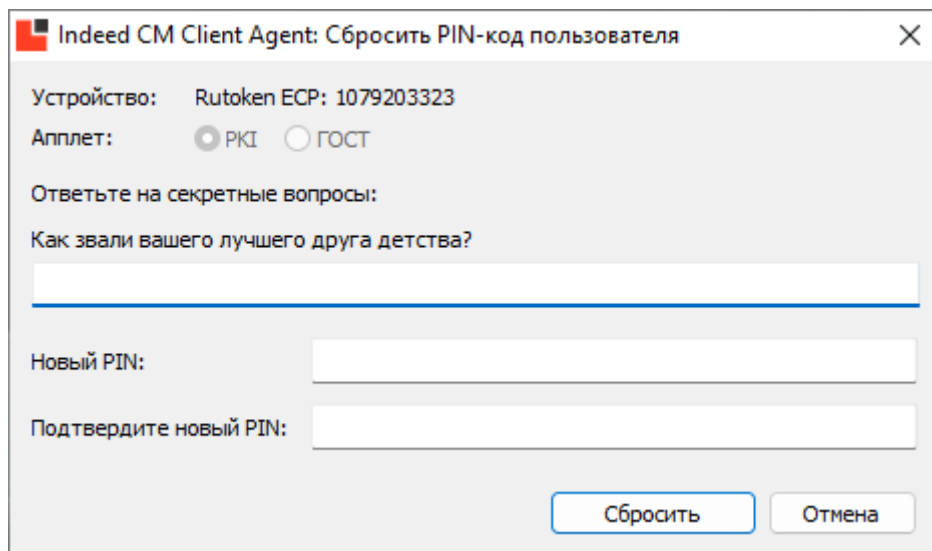
Будет создана задача по сбросу PIN-кода пользователя

Комментарий

Комментарий

Сбросить Отмена

При выполнении задачи Агент запустит на рабочей станции пользователя утилиту разблокировки. Сброс PIN-кода пользователя произойдет после того, как он ответит на секретные вопросы, задаст новый PIN-код и нажмет **Сбросить**.



Indeed CM Client Agent: Сбросить PIN-код пользователя

Устройство: Rutoken ECP: 1079203323

Апплет: ☒ PKI ☐ ГОСТ

Ответьте на секретные вопросы:

Как звали вашего лучшего друга детства?

Новый PIN:

Подтвердите новый PIN:

Сбросить Отмена

Если пользователь нажмет **Отмена**, то задача перейдет в состояние **Ожидает выполнения**, а в Журнал Indeed CM запишется событие об отмене задачи пользователем. Повторный запрос ответов на секретные вопросы для разблокировки устройства появится в сессии пользователя через 60 секунд.

❗ Для разблокировки устройств с несколькими логическими областями (например, JaCarta PKI/ГОСТ) создайте две задачи для поочередного сброса PIN-кодов каждой области.

Смена PIN-кода администратора

Нажмите **Сменить PIN-код администратора** в свойствах устройства, задайте и подтвердите **Новый PIN-код администратора**. Укажите **Комментарий** при необходимости и нажмите **Сменить**.

▼  **Rutoken ECP, 0894130607**  Evgeniy Belov Выпущено

Сбросить PIN-код

Разблокировать

Выключить

Отозвать

Заменить

Заменить на AirKey

Обновить

Заблокировать

Сменить PIN-код администратора

Будет создана задача по смене PIN-кода администратора

Новый PIN-код администратора

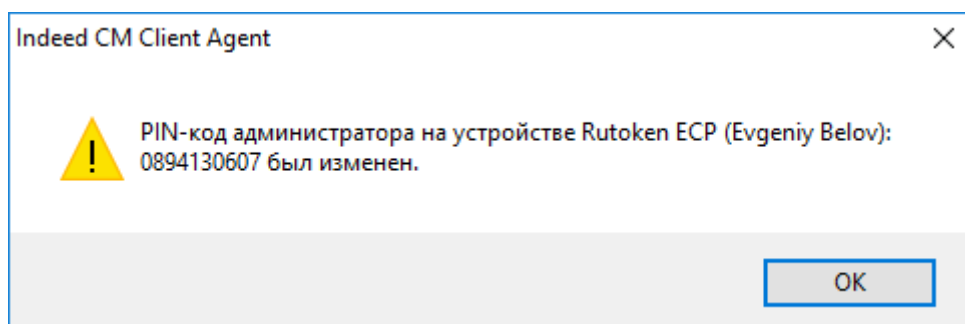
Подтверждение PIN-кода

Комментарий

Сменить

Отмена

PIN-код администратора изменится автоматически при подключении устройства к рабочей станции с установленным Агентом Indeed Certificate Manager. Сведения о выполнении задачи с указанным комментарием запишутся в **Журнал событий** Indeed CM. Если для операции **Смены PIN-кода администратора на устройстве** в разделе **Сообщения пользователю** политики использования устройств указан текст сообщения, то пользователь получит уведомление о выполнении задачи.



Очистка устройства на агенте

Нажмите **Отозвать** в карточке устройства, укажите **Причину отзыва** и включите опцию **Очистить устройство на агенте**.

▼ Rutoken ECP, 0894130607 Белов Выпущено

Сбросить PIN-код Разблокировать Выключить **Отозвать** Заменить ↺
Заменить на AirKey Обновить Заблокировать Сменить PIN-код администратора

Причина отзыва
Изъятие устройства ▼

☒ Очистить устройство на агенте

Номер и дата документа
ВН-545/21 23.11.2021 15:33 📅

☒ Очистить устройство
☐ Инициализировать устройство

Оставьте поле 'Новый PIN-код пользователя' пустым, если хотите использовать значение, установленное производителем устройства

Новый PIN-код пользователя
Новый PIN-код пользовател

Комментарий
Комментарий

[Дополнительно ▼](#)
☒ Отменить назначение устройства на пользователя

Отозвать Отмена

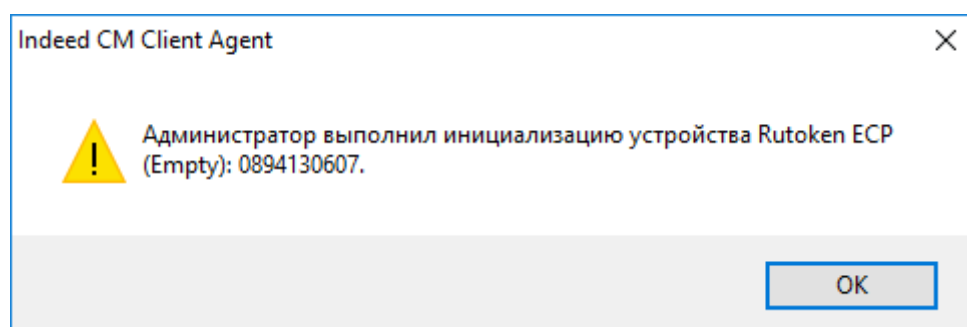
- Если при выпуске устройства было создано/назначено СКЗИ, то необходимо указать **Номер и дату документа**, на основании которого происходит уничтожение (Ключевой документ) /изъятие (Ключевой носитель) СКЗИ в процессе отзыва устройства.
- **Очистка устройства** предполагает удаление всех сертификатов, которые были записаны при помощи Indeed Certificate Manager, сертификаты и ключи, хранившиеся на устройстве до ввода в Indeed CM удалены не будут.
- **Инициализация устройства** приведет к удалению всего содержимого, политики паролей (если она была на устройстве) и изменит имя устройства.
 - Укажите **Новый PIN-код пользователя**, который должен быть установлен на устройстве после его изъятия. Если PIN-код пользователя не будет задан, то после изъятия устройства будет установлен PIN-код, указанный в файле **Типа устройства**.

 PIN-код необходимо устанавливать в том случае, если PIN-код пользователя, указанный в файле типа устройства (см. [Управление типами устройств](#)), не соответствует требованиям PIN-кода, установленным для данного типа устройства при инициализации в момент выпуска (см. [Параметры инициализации устройства](#)).

- Если необходимо отвязать устройство от пользователя, то нажмите **Дополнительно** и включите опцию **Отменить назначение устройства на пользователя**. Если опция выключена, то устройство после очистки или инициализации останется закрепленным за пользователем и может быть выпущено им повторно.

Для создания задачи нажмите **Отозвать**.

Если была выбрана опция **Инициализировать устройство** и для данной операции в разделе [Сообщения пользователю](#) политики использования устройств указан текст сообщения, то пользователь получит уведомление о выполнении задачи.



Обновление устройства на агенте

Нажмите **Обновить** в свойствах устройства и включите опцию **Обновить устройство на агенте**. Выберите сертификаты, если политика выпуска устройств это позволяет, и укажите **Комментарий** при необходимости. Для создания задачи нажмите **Обновить**.

Назначенные устройства

▼  **Rutoken ECP, 0898392427**  Евгений Белов Выпущено

Сбросить PIN-код

Разблокировать

Выключить

Отозвать

Заменить

Заменить на AirKey

Обновить

Заблокировать

Сменить PIN-код администратора

☒ Обновить устройство на агенте

Будет создана задача по обновлению устройства

Выберите требуемые сертификаты

Microsoft

☒ Вход по смарт-карте

Комментарий

Обновить

Отмена

Для обновления содержимого Агент запросит у пользователя PIN-код обновляемого устройства, когда оно будет подключено к рабочей станции пользователя. Введите PIN-код и нажмите **Обновить**.

 **Indeed CM Client Agent: Обновление устройства** ✕

Обновление устройства назначено администратором. Введите PIN-код устройства и не отключайте его от компьютера до завершения обновления.

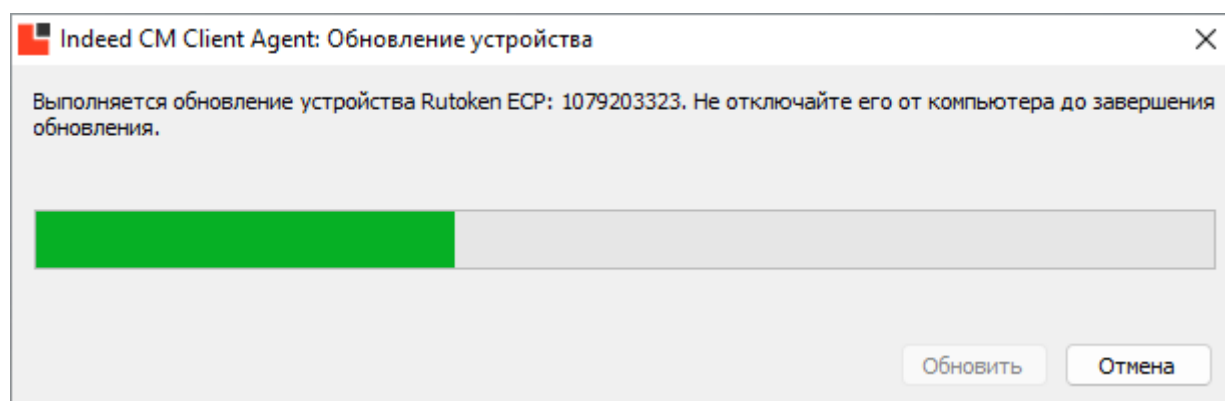
PIN-код пользователя

Обновить

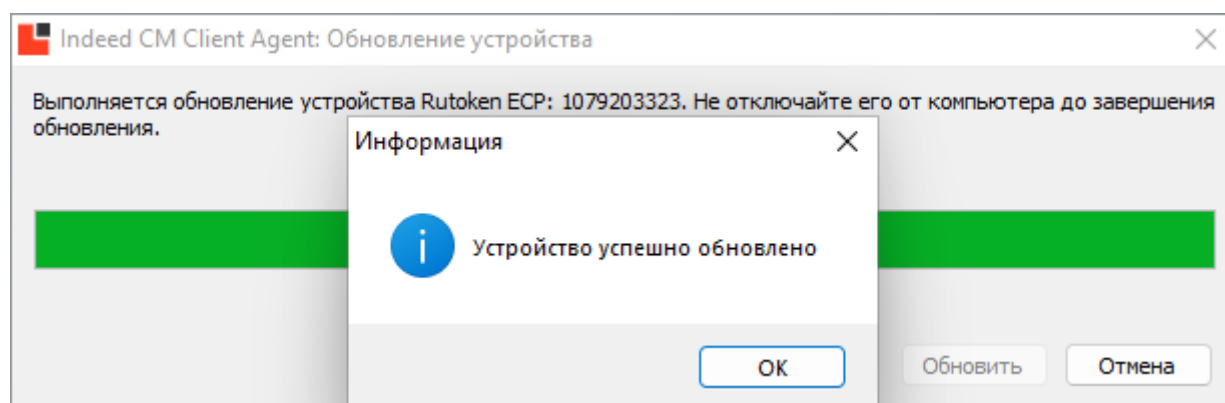
Отмена

Если PIN-код неверный, отобразится соответствующее сообщение и обновление выполнено не будет.

Если введен верный PIN-код пользователя, то начнется обновление устройства.



После успешного завершения обновления отобразится соответствующее сообщение.



Блокировка устройства

Нажмите **Заблокировать** в свойствах устройства и укажите **Комментарий** при необходимости. Для создания задачи нажмите **Заблокировать**.

▼  **Rutoken ECP, 0894130607**  Evgeniy Belov Выпущено

Сбросить PIN-код

Разблокировать

Выключить

Отозвать

Заменить

Заменить на AirKey

Обновить

Заблокировать

Сменить PIN-код администратора

Будет создана задача по блокировке устройства

Комментарий

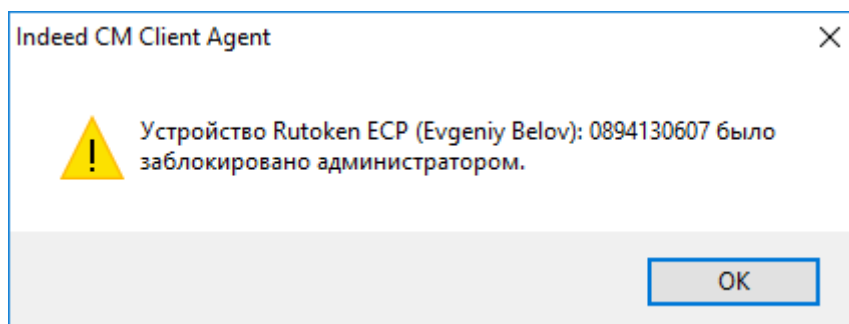
Комментарий

Заблокировать Отмена

После выполнения задачи PIN-код пользователя заблокируется.

 Если на устройстве несколько областей (например, PKI и ГОСТ), то PIN-код пользователя заблокируется для каждой области.

Если для операции **Блокировка PIN-кода пользователя** в разделе **Сообщения пользователю** политики использования устройств указан текст сообщения, то пользователь получит уведомление. Пример сообщения пользователю:



Инициализация устройства на агенте

Indeed CM позволяет выполнять инициализацию добавленных устройств на клиентском агенте, находящихся в состоянии **Пустое**.

В карточке устройства нажмите **Инициализировать** и выберите опцию **Инициализировать устройство на агенте**:

- Нажмите **Инициализировать**, если PIN-код администратора на устройстве совпадает с сохраненным в хранилище системы.
После выполнения задачи PIN-код администратора на устройстве и в базе не изменится, PIN-код пользователя будет сброшен на значение, указанное в [Типе устройства](#).

☐	Серийный номер	Комментарий	Пользователь	Политика	Состояние	
☐	 0755398982				Пустое	 

Инициализировать

Сменить PIN-код администратора



☒ Инициализировать устройство на агенте

Устройство будет проинициализировано. Все данные на устройстве будут потеряны

Будет создана задача по инициализации устройства

Комментарий

Дефолтное состояние

[Дополнительно](#) 

Вставьте устройство и нажмите 'Инициализировать'

Инициализировать

Отмена

- Если PIN-код администратора на устройстве не совпадает с сохраненным в хранилище системы, то укажите его в разделе **Дополнительно**. Задайте **Новый PIN-код пользователя**, если требуется его установить в процессе выполнения инициализации, и нажмите **Инициализировать**.
После инициализации PIN-код администратора в хранилище системы будет заменен на указанное значение.

Инициализировать

Сменить PIN-код администратора

↺

☒ Инициализировать устройство на агенте

Устройство будет проинициализировано. Все данные на устройстве будут потеряны

Будет создана задача по инициализации устройства

Комментарий

Дефолтное состояние

[Дополнительно ▾](#)

PIN-код администратора

.....

Новый PIN-код пользователя

.....

Вставьте устройство и нажмите 'Инициализировать'

Инициализировать

Отмена



Для устройств **Rutoken** и **eToken** возможно провести инициализацию с PIN-кодом администратора в состоянии: известный, неизвестный, заблокированный.

- если PIN-код администратора не указан, то после инициализации на устройство будет записан PIN-код, сохраненный в базе Indeed CM
- если PIN-код администратора указан, то после инициализации он будет записан на устройство и в базу Indeed CM

Массовые задачи

Массовые задачи – задачи, которые возможно назначить на несколько устройств сразу:

- Блокировка устройства
- Смена PIN-кода администратора
- Обновление устройства

Массовые задачи назначаются на выбранные устройства и будут выполняться по мере подключения устройств к Агентам Indeed Certificate Manager. Для создания массовой задачи перейдите на вкладку **Устройства**, выберите требуемые устройства и нажмите **Создать задачи**.

Поиск устройства

Подключенное устройство

Расширенный

Серийный номер

Тип

Серийный ном

Не задано

Комментарий

Комментарий

Состояние

Не задано

Статус содержимого

Не задано

Пользователь

evgeniy below

Политика

Не задано

Теги

Q

[+ Добавить устройство](#) [+ Выпустить устройство](#) [+ Выпустить AirKey](#) [✎ Изменить теги](#) [+ Создать задачи](#)
[+ Импортировать устройства](#)

☒	Серийный номер	Комментарий	Пользователь	Политика	Состояние	
☒	0894130607	Бухгалтерия	Evgeniy Below	Базовая политика	Назначено	✎
☒	0755398982		Evgeniy Below	Базовая политика	Выпущено	✎

Выберите задачу, укажите набор параметров уникальный для каждой задачи и нажмите **Создать**.

[+ Добавить устройство](#) [+ Выпустить устройство](#) [+ Выпустить AirKey](#) [✎ Изменить теги](#) [+ Создать задачи](#)
[+ Импортировать устройства](#)

☐ Блокировка устройства

☒ Смена PIN-кода администратора

☐ Обновление устройства

Количество выбранных устройств: 2

Новый PIN-код администратора

.....

Подтверждение PIN-кода

.....

Комментарий

Компрометация PIN-кода

Создать

Отмена

Задачи появятся в карточках устройств, а в разделе [Журнал](#) будут фиксироваться события о результатах выполнения задач на каждом агенте.

Мониторинг подключенных устройств

Клиентский агент проверяет все подключенные поддерживаемые устройства (смарт-карты, USB-токены) к рабочей станции пользователя и фиксирует в системный [Журнал](#) наступление следующих событий:

- Наличие устройств с заблокированным PIN-кодом Пользователя и Администратора (в том числе для ГОСТ-областей, если поддерживается устройством)
- Попытки ввода неверных PIN-кодов Пользователя и Администратора (в том числе для ГОСТ-областей, если поддерживается устройством)
- Подключение незарегистрированных устройств

При длительном отсутствии связи агента с сервером Indeed CM соответствующее событие фиксируется в системный журнал службой Card Monitor.

 Период отсутствия связи агента с сервером задается в разделе [Служба Card Monitor](#) Мастера настройки Indeed CM.

Последние события 

	Время	Событие	Сервис	Тип устройства	Серийный номер	Пользователь
▶ 	11.12.2019 18:10:30	Отсутствие связи с агентом	Монитор устройств			
▶ 	11.12.2019 18:08:04	Обнаружена блокировка PIN-кода администратора на устройстве	Сервис агентов	Rutoken ECP SC T0	0862287268	DEMO\Evgeniy.Belov
▶ 	11.12.2019 18:08:04	Ввод неверного PIN-кода администратора на устройстве	Сервис агентов	Rutoken ECP SC T0	0862287268	DEMO\Evgeniy.Belov
▶ 	11.12.2019 18:07:37	Обнаружена блокировка PIN-кода пользователя на устройстве	Сервис агентов	Rutoken ECP SC T0	0862287268	DEMO\Evgeniy.Belov
▶ 	11.12.2019 18:07:37	Ввод неверного PIN-кода пользователя на устройстве	Сервис агентов	Rutoken ECP SC T0	0862287268	DEMO\Evgeniy.Belov

[Просмотреть все](#) 

Для устройств, присутствующих в базе Indeed CM в состоянии "Выпущено", "В ожидании", "Отозвано", "Выключено" и "Назначено" имеется возможность рассылки почтовых уведомлений Администраторам системы при фиксировании следующих событий:

- Обнаружена блокировка PIN-кода администратора на устройстве
- Обнаружена блокировка PIN-кода пользователя на устройстве
- Ввод неверного PIN-кода администратора на устройстве
- Ввод неверного PIN-кода пользователя на устройстве

✓ **Создание уведомлений Администратора и Настройка шаблонов почтовых уведомлений** о данных событиях осуществляется в политике использования устройств.

Таблица 8 – События, передаваемые в Indeed CM устройствами аутентификации.

Производитель устройств	Список поддерживаемых событий
Компания «Актив»	Обнаружение блокировки PIN-кода пользователя / администратора на устройстве. Ввод неверного PIN-кода пользователя / администратора на устройстве.
Компания Индид	Обнаружение блокировки PIN-кода пользователя / администратора на устройстве.
Аладдин Р.Д.	Обнаружение блокировки PIN-кода пользователя / администратора на устройстве Ввод неверного PIN-кода пользователя / администратора на устройстве.
ACS	Обнаружение блокировки PIN-кода пользователя на устройстве. Ввод неверного PIN-кода пользователя на устройстве.
Avest	Обнаружение блокировки PIN-кода пользователя / администратора на устройстве.
Bit4id	Обнаружение блокировки PIN-кода пользователя / администратора на устройстве.
CRYPTAS	Обнаружение блокировки PIN-кода пользователя / администратора на устройстве. Ввод неверного PIN-кода пользователя / администратора на устройстве.
Cryptovision	Обнаружение блокировки PIN-кода пользователя / администратора на устройстве.
Feitian	Обнаружение блокировки PIN-кода пользователя / администратора на устройстве.
HID	Фиксирование событий не поддерживается.
ISBC	Обнаружение блокировки PIN-кода пользователя / администратора на устройстве.
Kaztoken	Обнаружение блокировки PIN-кода пользователя / администратора на устройстве. Ввод неверного PIN-кода пользователя / администратора на устройстве.

Microsoft VSC (TPM) Microsoft Windows Hello for Business (WHfB)	Фиксирование событий не поддерживается.
Registry	Фиксирование событий не поддерживается.
RSA	Обнаружение блокировки PIN-кода пользователя / администратора на устройстве.
Thales Group (Ex Gemalto and SafeNet)	Обнаружение блокировки PIN-кода пользователя / администратора на устройстве. Ввод неверного PIN-кода пользователя / администратора на устройстве.
Yubico	Фиксирование событий не поддерживается.

Журнал событий

Сведения о работе Агентов Indeed Certificate Manager заносятся в журналы сервера и клиента. События Агентов фиксируют сервисы: **Сервис регистрации агентов**, **Сервис агентов** и **Монитор устройств**.

Для просмотра событий Агентов во вкладке **Журнал** Консоли управления Indeed CM отфильтруйте содержимое журнала по одному из сервисов или по событиям.

Журнал

Тип события	Событие	Сервис
Не задано	Не задано	Сервис регистрации агентов
Пользователь	Тип устройства	Серийный номер
Общее имя(CN)	Не задано	Серийный номер
С	До	Инициатор
05.09.2018 00:00	19.09.2018 00:00	Инициатор

События Агента на рабочей станции пользователя записываются в локальный журнал событий **Indeed CM** и передаются на сервер. Если связи с сервером Indeed CM нет, то события хранятся на рабочей станции пользователя и будут отправлены на сервер, когда связь с ним восстановится.

Просмотр событий

Файл Действие Вид Справка

← → ↻ ?

Просмотр событий (Локальный журнал)

- Настраиваемые представления
- Журналы Windows
- Журналы приложений и служб
 - IndeedCM
 - Internet Explorer
 - Microsoft
 - ThinPrint Diagnostics
 - Windows PowerShell
 - Служба управления клиентскими устройствами
 - События оборудования
- Подписки

Уровень	Дата и время	Источник
Сведения	18.09.2018 12:31:55	IndeedCM
Предупреждение	18.09.2018 12:31:05	IndeedCM
Ошибка	17.09.2018 16:43:38	IndeedCM
Сведения	17.09.2018 16:34:49	IndeedCM
Сведения	17.09.2018 16:34:45	IndeedCM
Сведения	17.09.2018 16:34:44	IndeedCM
Сведения	17.09.2018 16:34:49	IndeedCM
Сведения	17.09.2018 16:34:45	IndeedCM
Сведения	17.09.2018 16:34:44	IndeedCM

СКЗИ



Раздел доступен если включена опция [Вести журнал учета СКЗИ](#) в разделе **Журнал учета СКЗИ** Мастера настройки Indeed CM и предоставлена привилегия на [Просмотр репозитория СКЗИ](#) членам Роли.

Для поиска СКЗИ установите параметры выборки:

- **Тип** (Не задано, Дистрибутив, Лицензия, Документация, Ключевой документ, Ключевой носитель, Пользовательский)
- **Описание**
- **Пользователь**
- **Серийный номер**
- **Номер экземпляра**
- **Состояние** (Не задано, Изготовлено, Назначено, Передано, Возвращено, Выдано, Установлено, Уничтожено/Изъято)
- **Период времени поиска**

Пример вывода результатов поиска СКЗИ за указанный период времени:

Поиск СКЗИ

Тип	Описание	Пользователь
Не задано	Описание	Общее имя(CN)
Серийный номер	Номер экземпляра	Состояние
Серийный номер	Номер экземпляра	Не задано
С		До
07.09.2020 16:30		08.09.2020 00:00

[Добавить СКЗИ](#) [Назначить СКЗИ](#) [Редактировать СКЗИ](#) [Уничтожить/изъять СКЗИ](#) [Импортировать СКЗИ](#)

Всего найдено: 3

	Время	Наименование	Пользователь	Серийный номер	Номер экземпляра	Состояние	
▼ ☐	07.09.2020 16:33:04	Дистрибутив - КристоПро CSP 5.0	Evgeniy Belov	4040Q-93010-06E9A-0WNNHK-H2376	4040Q-93010	Установлено	📄
Отметка об изготовлении Изготовитель: Adm Номер и дата документа: ВН-321/48, 04.09.2020 15:21 Отметка о передаче Получатель: Evgeniy Belov Номер и дата документа: ВН-329/24, 06.09.2020 16:41 Номер и дата подтверждения: ВН-331/13, 07.09.2020 10:20 Отметка о выдаче Номер и дата документа: П-63/514, 07.09.2020 12:37 Отметка о подключении Установщик: Maria Ivanova Номер и дата документа: П-63/524, 07.09.2020 16:14 Номер аппаратных средств: 0894130607 Место установки: Санкт-Петербург, ул. Малая Морская 12 APM: WKS61-2563-003 Номер кабинета: 311 Формуляр: ЖТЯИ.00050-03 30 01							
▶ ☐	07.09.2020 16:37:04	Ключевой носитель - Rutoken ECP	Evgeniy Belov	0894130607		Назначено	📄
▶ ☐	07.09.2020 16:39:03	Ключевой документ	Evgeniy Belov	0894130607	B1CB97C1-DBB2-4CC5-A6F5-C7086269A6C1	Назначено	📄

Результаты поиска СКЗИ могут быть сохранены в виде файла. Для создания файла с результатами поиска нажмите  и выберите формат (PDF или CSV). Сохраните полученный файл.

СКЗИ

Параметры поиска

С: 07.09.2020 16:30

До: 08.09.2020 0:00

Результат

N	Наименование	Пользователь	Серийный номер	Номер экземпляра	Состояние
1	Дистрибутив - КриптоПро CSP 5.0	Evgeniy Belov	4040Q-93010-06E9A-0WNNK-H2376	4040Q-93010	Установлено
Отметка об изготовлении Изготовитель: Adm Номер и дата документа: ВН-321/48, 04.09.2020 15:21 Отметка о передаче Получатель: Evgeniy Belov Номер и дата документа: ВН-329/24, 06.09.2020 16:41 Номер и дата подтверждения: ВН-331/13, 07.09.2020 10:20 Отметка о выдаче Номер и дата документа: П-63/514, 07.09.2020 12:37 Отметка о подключении Установщик: Maria Ivanova Номер и дата документа: П-63/524, 07.09.2020 16:14 Номер аппаратных средств: 0894130607 Место установки: Санкт-Петербург, ул. Малая Морская 12 APM: WKS61-2563-003 Номер кабинета: 311 Формуляр: ЖТЯИ.00050-03 30 01					
2	Ключевой носитель - Rutoken ECP	Evgeniy Belov	0894130607		Назначено
Отметка об изготовлении Изготовитель: Maria Ivanova Номер и дата документа: ВН-105, 07.09.2020 16:37					
3	Ключевой документ	Evgeniy Belov	0894130607	B1CB97C1-DBB2-4CC5-A6F5-C7086269A6C1	Назначено
Отметка об изготовлении Изготовитель: Maria Ivanova Номер и дата документа: ВН-234/57, 07.09.2020 16:39					

Операции с СКЗИ

Добавление, редактирование и уничтожение/изъятие СКЗИ аналогичны таковым в [Карточке пользователя](#).

Добавление СКЗИ

СКЗИ может быть создано вручную или автоматически при [Добавлении устройств](#), поддерживающих аппаратную криптографию (Тип: Ключевой носитель), при [Выпуске устройства](#) пользователю (Тип: Ключевой документ, Ключевой носитель, если устройство выпускается без предварительного добавления в систему).

1. Нажмите **Добавить СКЗИ** для ручного создания нового средства криптографической защиты информации.
2. Задайте значения параметров СКЗИ:
 - **Тип** (Дистрибутив, Лицензия, Документация, Ключевой документ, Ключевой носитель, Пользовательский). Обязательно для заполнения.
 - **Описание**. Обязательно для заполнения.
 - **Серийный номер**. Обязательно для заполнения.
 - **Номер экземпляра**. Необязательное поле для заполнения.
 - **Номер и дата документа**, на основании которого добавляется СКЗИ. Обязательно для заполнения.
3. Нажмите **Добавить**.

Добавить СКЗИ

Тип

Лицензия

Описание

КриптоПро CSP 5.0

Серийный номер

4040Q-73010-KYE6B-N510U-3F07H

Номер экземпляра

4040Q-73010

Номер и дата документа

ВН-319/21

08.09.2020 08:54

Добавить

Отмена

Назначение СКЗИ

Изготовленные СКЗИ могут быть закреплены за пользователями.

1. Выберите изготовленные средства криптографической защиты информации (одно или несколько), которые необходимо закрепить за пользователем и нажмите **Назначить СКЗИ**.
2. Выполните поиск пользователя, за которым необходимо закрепить выбранные СКЗИ, и выберите его, нажав **Выбрать**.

Пользователь

Выберите пользователя

demo.local

Olga



	Общее имя(CN)	Имя и фамилия	E-mail	Контейнер
☒	Olga Nikiforova	Olga Nikiforova	olga.nikiforova@demo.com	demo.local/Users

Выбрать

Отмена

3. Нажмите **Назначить**. При этом состояние выбранных СКЗИ будет изменено с **Изготовлено** на **Назначено**. Закрепленные за пользователем СКЗИ будут доступны в его карточке в разделе **Назначенные СКЗИ**.

Назначенные СКЗИ

	Наименование	Серийный номер	Номер экземпляра	Состояние	
▼	☐ Лицензия - КriptoПро CSP 5.0	4040Q-73010-KYE6B-N510U-3F07H	4040Q-73010	Назначено	

Отметка об изготовлении
Изготовитель: Maria Ivanova
Номер и дата документа: BH-319/21, 08.09.2020 8:54

[+ Добавить СКЗИ](#) [# Редактировать СКЗИ](#) [- Уничтожить/изъять СКЗИ](#)

Редактирование СКЗИ

СКЗИ могут быть отредактированы уполномоченным сотрудником: оператором или администратором Indeed CM.

1. Для редактирования выберите средства криптографической защиты информации (одно или несколько) и нажмите **Редактировать СКЗИ**.

[+ Добавить СКЗИ](#) [# Назначить СКЗИ](#) [# Редактировать СКЗИ](#) [- Уничтожить/изъять СКЗИ](#) [+ Импортировать СКЗИ](#)

Всего найдено: 2

	Время	Наименование	Пользователь	Серийный номер	Номер экземпляра	Состояние	
▶ ☒	08.09.2020 11:28:50	Лицензия - КriptoПро CSP 5.0	Olga Nikiforova	4040Q-73010-KYE6B-N510U-3F07H	4040Q-73010	Назначено	
▶ ☒	08.09.2020 12:06:23	Лицензия - КriptoПро CSP 4.0 R4		4040Q-63010-C4N6R-0NKZH-14NDX	4040Q-63010	Изготовлено	

Поля, доступные для редактирования:

- Отметка о передаче
- Отметка о возврате
- Отметка о выдаче
- Отметка о подключении
- Примечание
- Дополнительные поля (дополнительные атрибуты, заданные в разделе [Журнал учета СКЗИ](#) Мастера настройки Indeed CM)



Перечень полей указан в соответствии с типовой формой журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (для органа криптографической защиты информации), утвержденной Приказом ФАПСИ от 13 июня 2001 г. 152.

2. Внесите необходимые изменения и нажмите **Сохранить**.

Уничтожение и изъятие СКЗИ

1. Для уничтожения или изъятия СКЗИ выберите средства криптографической защиты информации и нажмите **Уничтожить/изъять СКЗИ**.

- Укажите имя сотрудника, выполняющего уничтожение/изъятие СКЗИ.
- **Номер и дату документа**, на основании которого осуществляется уничтожение /изъятие.
- Выберите опцию **Использовать повторно** в случае повторного использования СКЗИ (например: при передаче лицензии или дистрибутива другому сотруднику).

2. Нажмите **Уничтожить/Изъять**.

[+ Добавить СКЗИ](#) [+ Назначить СКЗИ](#) [+ Редактировать СКЗИ](#) [- Уничтожить/изъять СКЗИ](#) [+ Импортировать СКЗИ](#)

Уничтожить/изъять СКЗИ

Сотрудник, производивший уничтожение/изъятие

Victor Osipov

Номер и дата документа

ВН-573/14

09.09.2020 16:27



☒ Использовать повторно

Уничтожить/Изъять

Отмена

Всего найдено: 2

	Время	Наименование	Пользователь	Серийный номер	Номер экземпляра	Состояние	
▶ ☒	08.09.2020 11:28:50	Лицензия - КриптоПро CSP 5.0	Olga Nikiforova	4040Q-73010-KYE6B-N510U-3F07H	4040Q-73010	Установлено	
▶ ☒	08.09.2020 12:06:23	Лицензия - КриптоПро CSP 4.0 R4		4040Q-63010-C4N6R-0NKZH-14NDX	4040Q-63010	Установлено	

Пакетный импорт СКЗИ

Для пакетного импорта СКЗИ на вкладке **СКЗИ**:

1. Нажмите **Импортировать СКЗИ**.
2. Загрузите подготовленный **Файл СКЗИ**.
3. Нажмите **Импортировать**.

Поиск СКЗИ

Тип	Описание	Пользователь
Не задано	Описание	Общее имя(CN)
Серийный номер	Номер экземпляра	Состояние
Серийный номер	Номер экземпляра	Не задано
С		До
26.09.2020 00:00		30.09.2020 00:00
		Q

[+ Добавить СКЗИ](#) [+ Назначить СКЗИ](#) [+ Редактировать СКЗИ](#) [- Уничтожить/изъять СКЗИ](#) [+ Импортировать СКЗИ](#)

Файл СКЗИ

Поддерживается импорт средств криптографической защиты информации из файла в формате TXT (UTF-8) и CSV. Файл должен содержать строки с набором полей следующего формата:

Serial Number;Instance Number;SKZI Type;Description;Document Number;Time Created

- **Serial Number** - серийный номер СКЗИ.
- **Instance Number** - номер экземпляра. [Необязательное поле для заполнения.](#)
- **SKZI Type** - тип документа СКЗИ: Distributive, License, Documentation, KeyDocument, Card, Custom.
- **Description** - описание документа.
- **Document Number** - номер документа, на основании которого осуществляется [добавление СКЗИ.](#)
- **Time Created** - время создания документа. Указывается в формате ууууММддННммсс (UTC). Если значение не указано, то в качестве времени создания документа автоматически подставляется время импорта СКЗИ.

 Serial Number, SKZI Type, Description и Document Number являются обязательными параметрами.

Если вместо поля **Serial Number** (Серийный номер СКЗИ) прописано значение **default**, то значения полей (SKZI Type;Description;Document Number;Time Created) данной строки будут использоваться как значения по умолчанию для соответствующих полей последующих строк, т.е. для последующих строк необходимо указать только Серийный номер СКЗИ, Номер экземпляра (если необходимо) и поле, которое отличается от указанного в строке **default**.

В представленном ниже примере **Файла импорта СКЗИ** добавлены:

- **Дистрибутив КriptoПро CSP 4.0** и его копия с серийным номером: 4040P-73010-04F65-67N08-637V1 по номеру документа ВН-337
- **Дистрибутив КriptoПро CSP 5.0** и его копия с серийным номером: 4040Q-93010-04F65-UUZDG-E81NX по номеру документа ВН-338
- **Лицензия КriptoПро CSP 4.0** с серийным номером: 4040Q-43010-KYE6B-C1857-0NKZH по номеру документа ВН-339
- **Лицензия КriptoПро CSP 5.0** с серийным номером: 4040N-53010-KYE6B-CFTHW-TFAL7 по номеру документа ВН-339
- **Документация Формуляр: ЖТЯИ.00102 01 30 01 КriptoПро CSP 5.0 KC2** (исполнение 2-Base) регистрационный номер СФ/124-3727 от 13.08.2019

Пример Файла СКЗИ:

default;;Distributive;КриптоПро CSP 4.0;ВН-337;20200926181600
4040P-73010-04F65-67N08-637V1
4040P-73010-04F65-67N08-637V1;Копия-1
4040Q-93010-04F65-UUZDG-E81NX;;;КриптоПро CSP 5.0;ВН-338
4040Q-93010-04F65-UUZDG-E81NX;Копия-1;;КриптоПро CSP 5.0;ВН-338
default;;License;КриптоПро CSP 4.0;ВН-339;20200926182900
4040Q-43010-KYE6B-C1857-0NKZH
4040N-53010-KYE6B-CFTHW-TFAL7;;;КриптоПро CSP 5.0
ЖТЯИ.00102 01 30 01;Экз.1;Documentation;Формуляр КриптоПро CSP 5.0 KC2 (исполнение 2-Base);СФ/124-3727 от 13.08.2019;20190813000000

Журналы учета



Раздел доступен при включенной опции **Журнал учета устройств и сертификатов** в разделе **Общие функции** Мастера настройки Indeed CM и предоставленной привилегии **Просмотр журнала учета** членам Роли.

Под журналом учёта понимается набор полей, сконфигурированных в **Шаблонах журналов** на вкладке **Конфигурация**, содержащих данные об устройствах и сертификатах, их владельцах и системах, в которых эти устройства/сертификаты используются.

Записи в журнал учета заносятся автоматически при выпуске, замене, изъятии или обновлении устройств (для журнала сертификатов) в Консоли управления Indeed CM или в Сервисе самообслуживания.

В разделе **Журнал учета** администратор или оператор могут выбрать созданный журнал и запросить необходимую информацию при помощи фильтров, настроенных для конкретного журнала:

Журналы учета

Журнал учета	С	До
Сертификаты	13.09.2019 12:50	20.09.2019 00:00
Серийный номер сертификата	Серийный номер устройства	Имя пользователя устройства
Серийный номер сертификата	Серийный номер устройства	Имя пользователя устройства
Дата начала действия сертификата	Дата окончания действия сертификата	

[+ Добавить запись](#)

Время	Серийный номер сертификата	Серийный номер устройства	Имя пользователя устройства	Дата начала действия сертификата	Дата окончания действия сертификата	
▶ 13.09.2019 12:51:53	2889A200C7AA42AD422F84F2D69C4C97	0894130913	Evgeniy Belov	13.09.2019 12:41:47	13.12.2020 12:51:47	
▼ 19.09.2019 10:43:00	6A000000BB881DEC2A5A4EC55B0001000000BB	0755398982	Evgeniy Belov	19.09.2019 10:32:49	18.09.2020 10:32:49	✎ ✕
Серийный номер сертификата: 6A000000BB881DEC2A5A4EC55B0001000000BB Серийный номер устройства: 0755398982 Имя пользователя устройства: Evgeniy Belov Дата начала действия сертификата: 19.09.2019 10:32:49 Дата окончания действия сертификата: 18.09.2020 10:32:49 Тип устройства: Rutoken S Комментарий: ЭП E-mail: evgeniy.belov@demo.com Контейнер сертификата: 4B29A101-6F26-4671-8335-5714EFFB58AA Владелец: CN=Evgeniy Belov, CN=Users, DC=demo, DC=local Издатель: CN=demo-DC-CA, DC=demo, DC=local						
▶ 19.09.2019 10:44:48	6A000000BC1A26D175DA0A88240001000000BC	0894130913	Maria Ivanova	19.09.2019 10:34:45	18.09.2020 10:34:45	✎ ✕

Для добавления записи вручную нажмите **Добавить запись**, заполните **Обязательные поля** и нажмите **Добавить**.

Для редактирования уже созданной записи нажмите  , отредактируйте необходимые поля и нажмите **Сохранить**. Для удаления записи нажмите  .

Для выгрузки журналов учета в файл, нажмите  и выберите формат XLSX или CSV.

Журнал

Записи о всех операциях во всех приложениях Indeed Certificate Manager отражаются в журнале событий **Indeed CM/Operational** на сервере Indeed CM. В разделе **Журнал** администратор или оператор могут запрашивать необходимую информацию при помощи фильтров.

Журнал

Тип события	Событие	Сервис
Не задано	Не задано	Не задано
Пользователь	Тип устройства	Серийный номер
Общее имя(CN)	Не задано	Серийный номер
С	До	Инициатор
02.08.2020 00:00	06.08.2020 00:00	Инициатор

✓ Переопределить атрибут имени пользователя для поиска возможно в разделе **Журнал событий** Мастера настройки Indeed CM.

Возможные значения:

- **Общее имя (CN)** - Значение по умолчанию
- **sAMAccountName**
- **userPrincipalName**
- **Пользовательский**

Indeed CM ведет учет событий следующих типов:

- **Информация** – успешное выполнение любой операции
- **Ошибка** – завершение любой операции с ошибкой
- **Предупреждение** – события, требующие внимания администратора системы

	Время	Код	Событие	Сервис	Пользователь	Тип устройства	Серийный номер	Инициатор	
▼ ⓘ	06.08.2020 10:47:54	7	Выключение устройства	Консоль управления	Evgeniy Belov	Rutoken S	0755398982	DEMO\Adm	
Устройство успешно выключено. Пользователь: Evgeniy Belov Устройство: Rutoken S:0755398982 Инициатор: DEMO\Adm									
▼ ⚠	06.08.2020 10:47:32	2103	Блокировка пользователя	Сервис удаленного обслуживания	Evgeniy Belov				
Пользователь заблокирован. Пользователь: Evgeniy Belov Инициатор:									
▼ ✖	06.08.2020 10:47:32	1102	Аутентификация	Сервис удаленного обслуживания	Evgeniy Belov				
Произошла ошибка при аутентификации пользователя. Пользователь: Evgeniy Belov Инициатор: Сообщение об ошибке: Неверные ответы									

Полный список событий приведен в разделе **Список событий Indeed CM**.

Журнал

Тип события	Событие	Сервис
Не задано	Не задано	Не задано
Пользователь	Тип устройства	Серийный номер
Общее имя(CN)	Не задано	Серийный номер
С	До	Инициатор
06.08.2020 10:45	07.08.2020 00:00	Инициатор

	Время	Код	Событие	Сервис	Пользователь	Тип устройства	Серийный номер	Инициатор	
▶	06.08.2020 10:51:19	6	Включение устройства	Сервис удаленного обслуживания	Evgeniy Belov	Rutoken S	0755398982	DEMO\Evgeniy.Belov	
▶	06.08.2020 10:51:11	102	Аутентификация	Сервис удаленного обслуживания	Evgeniy Belov				
▶	06.08.2020 10:50:12	101	Изменение ответов на секретные вопросы	Сервис самообслуживания	Evgeniy Belov			DEMO\Evgeniy.Belov	
▶	06.08.2020 10:49:54	105	Сброс ответов на секретные вопросы	Консоль управления	Evgeniy Belov			DEMO\Adm	
▶	06.08.2020 10:49:48	104	Разблокировка пользователя	Консоль управления	Evgeniy Belov			DEMO\Adm	
▶	06.08.2020 10:47:54	7	Выключение устройства	Консоль управления	Evgeniy Belov	Rutoken S	0755398982	DEMO\Adm	
▶	06.08.2020 10:47:32	2103	Блокировка пользователя	Сервис удаленного обслуживания	Evgeniy Belov				
▶	06.08.2020 10:47:32	1102	Аутентификация	Сервис удаленного обслуживания	Evgeniy Belov				
▶	06.08.2020 10:46:32	14	Изменение PIN-кода	Сервис самообслуживания	Evgeniy Belov	Rutoken S	0755398982	DEMO\Evgeniy.Belov	
▶	06.08.2020 10:45:55	5	Выпуск устройства	Консоль управления	Evgeniy Belov	Rutoken S	0755398982	DEMO\Adm	
▶	06.08.2020 10:45:55	351	Добавление записи в журнал учета	Консоль управления				DEMO\Adm	
▶	06.08.2020 10:45:54	351	Добавление записи в журнал учета	Консоль управления				DEMO\Adm	

Для формирования отчета о событиях нажмите и выберите формат. Доступно сохранение в формате PDF и CSV.

Отчет по событиям в формате PDF.

События

Параметры поиска

С: 06.08.2020 10:45

До: 07.08.2020 0:00

Результат

N	Тип события	Время	Код	Событие	Сервис
1	Информация	06.08.2020 7:51:19	6	Включение устройства	Сервис удаленного обслуживания
Устройство успешно включено. Пользователь: Evgeniy Belov Устройство: Rutoken S:0755398982 Инициатор: DEMO\Evgeniy.Belov					
2	Информация	06.08.2020 7:51:11	102	Аутентификация	Сервис удаленного обслуживания
Пользователь успешно аутентифицирован. Пользователь: Evgeniy Belov Инициатор:					
3	Информация	06.08.2020 7:50:12	101	Изменение ответов на секретные вопросы	Сервис самообслуживания
Ответы на секретные вопросы успешно изменены. Пользователь: Evgeniy Belov Инициатор: DEMO\Evgeniy.Belov					
4	Информация	06.08.2020 7:49:54	105	Сброс ответов на секретные вопросы	Консоль управления
Ответы на секретные вопросы успешно сброшены. Пользователь: Evgeniy Belov Инициатор: DEMO\Adm					
5	Информация	06.08.2020 7:49:48	104	Разблокировка пользователя	Консоль управления
Пользователь успешно разблокирован. Пользователь: Evgeniy Belov Инициатор: DEMO\Adm					
6	Информация	06.08.2020 7:47:54	7	Выключение устройства	Консоль управления
Устройство успешно выключено. Пользователь: Evgeniy Belov Устройство: Rutoken S:0755398982 Инициатор: DEMO\Adm					
7	Предупреждение	06.08.2020 7:47:32	2103	Блокировка пользователя	Сервис удаленного обслуживания
Пользователь заблокирован. Пользователь: Evgeniy Belov Инициатор:					
8	Ошибка	06.08.2020 7:47:32	1102	Аутентификация	Сервис удаленного обслуживания
Произошла ошибка при аутентификации пользователя. Пользователь: Evgeniy Belov Инициатор: Сообщение об ошибке: Неверные ответы					
9	Информация	06.08.2020 7:46:32	14	Изменение PIN-кода	Сервис самообслуживания
PIN-код устройства успешно изменен. Пользователь: Evgeniy Belov Устройство: Rutoken S:0755398982 Инициатор: DEMO\Evgeniy.Belov					
10	Информация	06.08.2020 7:45:55	5	Выпуск устройства	Консоль управления
Устройство успешно выпущено. Пользователь: Evgeniy Belov Политика: Базовая политика Устройство: Rutoken S:0755398982 Сертификаты: Вход по смарт-карте: 6A00000364DD2362357D5874C6000100000364 Общие сертификаты: Отслеживаемые сертификаты: Инициатор: DEMO\Adm					
11	Информация	06.08.2020 7:45:55	351	Добавление записи в журнал учета	Консоль управления

Запись успешно добавлена. Журнал учета: Сертификаты Поля: Серийный номер сертификата: 6A00000364DD2362357D5874C6000100000364 Серийный номер устройства: 0755398982 Имя пользователя устройства: Evgeniy Belov Дата начала действия сертификата: 06.08.2020 10:35:41 Дата окончания действия сертификата: 06.08.2021 10:35:41 Тип устройства: Rutoken S Комментарий: E-mail: evgeniy.belov@demo.com Контейнер сертификата: 23406B58-9D1D-4908-B6A7-A2078219429F Владелец: E=evgeniy.belov@demo.com, CN=Evgeniy Belov, CN=Users, DC=demo, DC=local Издатель: CN=demo-DC-CA, DC=demo, DC=local Должность: Организация: Инициатор: DEMO\Adm					
12	Информация	06.08.2020 7:45:54	351	Добавление записи в журнал учета	Консоль управления
Запись успешно добавлена. Журнал учета: Устройства Поля: Серийный номер устройства: 0755398982 Тип устройства: Rutoken S Имя пользователя устройства: Evgeniy Belov E-mail пользователя: evgeniy.belov@demo.com Комментарий устройства: Модель устройства: Организация: Должность: Инициатор: DEMO\Adm					

Список событий

Код	Тип	Событие	Описание
1	Информация	Добавление устройства	Устройство успешно добавлено. Устройство: Инициатор:
1001	Ошибка	Добавление устройства	Произошла ошибка при добавлении устройства. Устройство: Инициатор: Сообщение об ошибке:
2	Информация	Удаление устройства	Устройство успешно удалено. Устройство: Инициатор:
1002	Ошибка	Удаление устройства	Произошла ошибка при удалении устройства. Устройство: Инициатор: Сообщение об ошибке:
3	Информация	Назначение устройства	Устройство успешно назначено. Пользователь: Политика: Устройство: Инициатор:
1003	Ошибка	Назначение устройства	Произошла ошибка при назначении устройства. Пользователь: Устройство: Инициатор: Сообщение об ошибке:
4	Информация	Отмена назначения устройства	Назначение устройства успешно отменено. Пользователь: Устройство: Инициатор:
1004	Ошибка	Отмена назначения устройства	Произошла ошибка при отмене назначения устройства. Пользователь: Устройство: Инициатор: Сообщение об ошибке:
5	Информация	Выпуск устройства	Устройство успешно выпущено. Пользователь: Политика: Устройство: Сертификаты: Общие сертификаты: Отслеживаемые сертификаты: Инициатор:
1005	Ошибка	Выпуск устройства	Произошла ошибка при выпуске устройства. Пользователь: Устройство: Инициатор: Сообщение об ошибке:
6	Информация	Включение устройства	Устройство успешно включено. Пользователь: Устройство: Инициатор:

1006	Ошибка	Включение устройства	Произошла ошибка при включении устройства. Пользователь: Устройство: Инициатор: Сообщение об ошибке:
7	Информация	Выключение устройства	Устройство успешно выключено. Пользователь: Устройство: Инициатор:
1007	Ошибка	Выключение устройства	Произошла ошибка при выключении устройства. Пользователь: Устройство: Инициатор: Сообщение об ошибке:
8	Информация	Отзыв устройства	Устройство успешно отозвано. Пользователь: Устройство: Причина: Сертификаты: Инициатор:
1008	Ошибка	Отзыв устройства	Произошла ошибка при отзыве устройства. Пользователь: Устройство: Причина: Инициатор: Сообщение об ошибке:
9	Информация	Обновление устройства	Устройство успешно обновлено. Пользователь: Устройство: Новые сертификаты: Обновленные сертификаты: Удаленные сертификаты: Новые общие сертификаты: Удаленные общие сертификаты: Отслеживаемые сертификаты: Новая политика: Инициатор:
1009	Ошибка	Обновление устройства	Произошла ошибка при обновлении устройства. Пользователь: Устройство: Инициатор: Сообщение об ошибке:
10	Информация	Замена устройства	Устройство успешно заменено. Пользователь: Устройство: Новое Устройство: Сертификаты: Общие сертификаты: Дата истечения: Инициатор:
1010	Ошибка	Замена устройства	Произошла ошибка при замене устройства. Пользователь: Устройство: Новое устройство: Инициатор: Сообщение об ошибке:

11	Информация	Очистка устройства	Устройство успешно очищено. Пользователь: Устройство: Состояние устройства: Инициатор:
1011	Ошибка	Очистка устройства	Произошла ошибка при очистке устройства. Пользователь: Устройство: Инициатор: Сообщение об ошибке:
12	Информация	Сброс PIN-кода	PIN-код устройства успешно сброшен. Пользователь: Устройство: Инициатор:
1012	Ошибка	Сброс PIN-кода	Произошла ошибка при сбросе PIN-кода устройства. Пользователь: Устройство: Инициатор: Сообщение об ошибке:
13	Информация	Разблокировка устройства	Код разблокировки успешно сгенерирован. Пользователь: Устройство: Инициатор:
1013	Ошибка	Разблокировка устройства	Произошла ошибка при генерации кода разблокировки. Пользователь: Устройство: Инициатор: Сообщение об ошибке:
14	Информация	Изменение PIN-кода	PIN-код устройства успешно изменен. Пользователь: Устройство: Инициатор:
1014	Ошибка	Изменение PIN-кода	Произошла ошибка при изменении PIN-кода устройства. Пользователь: Устройство: Инициатор: Сообщение об ошибке:
15	Информация	Выпуск устройства ожидает решения	Выпуск устройства ожидает решения. Пользователь: Политика: Устройство: Сертификаты: Общие сертификаты: Отслеживаемые сертификаты: Инициатор:
16	Информация	Обновление устройства ожидает решения	Выпуск устройства ожидает решения. Пользователь: Устройство: Новые сертификаты: Обновленные сертификаты: Удаленные сертификаты: Новые общие сертификаты: Удаленные общие сертификаты: Отслеживаемые сертификаты: Новая политика: Инициатор:

17	Информация	Замена устройства ожидает решения	Замена устройства ожидает решения. Пользователь: Устройство: Новое устройство: Сертификаты: Общие сертификаты: Дата истечения: Инициатор:
18	Информация	Отмена обновления устройства	Обновление устройства успешно отменено. Пользователь: Устройство: Инициатор:
1018	Ошибка	Отмена обновления устройства	Произошла ошибка при отмене обновления устройства. Пользователь: Устройство: Инициатор: Сообщение об ошибке:
19	Информация	Предварительное обновление устройства	Предварительное обновление устройства успешно выполнено. Пользователь: Устройство: Отозванные сертификаты: Инициатор:
1019	Ошибка	Предварительное обновление устройства	Произошла ошибка при предварительном обновлении устройства. Пользователь: Устройство: Инициатор: Сообщение об ошибке:
20	Информация	Импортирование устройства	Устройство успешно импортировано. Пользователь: Устройство: Состояние: Сертификаты: Инициатор:
1020	Ошибка	Импортирование устройства	Устройство успешно импортировано. Пользователь: Устройство: Состояние: Сертификаты: Инициатор:
21	Информация	Изменение комментария	Комментарий устройства успешно изменен. Устройство: Комментарий: Инициатор:
1021	Ошибка	Изменение комментария	Произошла ошибка при изменении комментария устройства. Устройство: Инициатор: Сообщение об ошибке:
22	Информация	Просмотр PIN-кода администратора	PIN-код администратора устройства просмотрен. Устройство: Инициатор:
23	Информация	Смена PIN-кода администратора	PIN-код администратора устройства успешно изменен Пользователь: Устройство: Инициатор:

1023	Ошибка	Смена PIN-кода администратора	Произошла ошибка при изменении PIN-кода устройства. Пользователь: Устройство: Инициатор: Сообщение об ошибке:
24	Информация	Изменение тега	Теги устройства успешно изменены. Устройство: Новые теги: Удаленные теги: Инициатор:
1024	Ошибка	Изменение тега	Произошла ошибка при изменении тегов устройства. Устройство: Новые теги: Удаленные теги: Инициатор: Сообщение об ошибке:
25	Информация	Инициализация устройства	Устройство успешно инициализировано. Устройство: Инициатор:
1025	Ошибка	Инициализация устройства	Произошла ошибка при инициализации устройства. Устройство: Инициатор: Сообщение об ошибке:
101	Информация	Изменение ответов на секретные вопросы	Ответы на секретные вопросы успешно изменены. Пользователь: Инициатор:
1101	Ошибка	Изменение ответов на секретные вопросы	Произошла ошибка при изменении ответов на секретные вопросы. Пользователь: Инициатор: Сообщение об ошибке:
102	Информация	Аутентификация	Пользователь успешно аутентифицирован. Пользователь: Инициатор:
1102	Ошибка	Аутентификация	Произошла ошибка при аутентификации пользователя. Пользователь: Инициатор: Сообщение об ошибке:
2103	Предупреждение	Блокировка пользователя	Пользователь заблокирован. Пользователь: Инициатор:
104	Информация	Разблокировка пользователя	Пользователь успешно разблокирован. Пользователь: Инициатор:
1104	Ошибка	Разблокировка пользователя	Произошла ошибка при разблокировке пользователя. Пользователь: Инициатор: Сообщение об ошибке:
105	Информация	Сброс ответов на секретные вопросы	Ответы на секретные вопросы успешно сброшены. Пользователь: Инициатор:

1105	Ошибка	Сброс ответов на секретные вопросы	Произошла ошибка при сбросе ответов на секретные вопросы. Пользователь: Инициатор: Сообщение об ошибке:
106	Информация	Сброс пароля	Пароль пользователя успешно сброшен. Пользователь: Время истечения: Инициатор:
1106	Информация	Сброс пароля	Произошла ошибка при сбросе пароля пользователя. Пользователь: Инициатор: Сообщение об ошибке:
111	Информация	Проверка в СМЭВ	Данные пользователя отправлены на проверку в СМЭВ. Пользователь: Инициатор:
112	Информация	Результат проверки в СМЭВ	Проверка данных пользователя в СМЭВ прошла успешно. Пользователь: Инициатор:
1112	Ошибка	Результат проверки в СМЭВ	Проверка данных пользователя в СМЭВ завершилась ошибкой. Пользователь: Инициатор: Сообщение об ошибке:
113	Информация	Публикация сертификата в ЕСИА	Данные сертификата опубликованы в СМЭВ для регистрации в ЕСИА. Пользователь: Сертификат: Инициатор:
1113	Ошибка	Публикация сертификата в ЕСИА	Произошла ошибка при публикации сертификата в СМЭВ для регистрации в ЕСИА. Пользователь: Сертификат: Инициатор: Сообщение об ошибке:
201	Информация	Создание политики	Политика успешно создана. Имя политики: Контейнер: Группа: Приоритет: Скопирована с: Инициатор:
1201	Ошибка	Создание политики	Произошла ошибка при создании политики. Имя политики: Контейнер: Группа: Приоритет: Инициатор: Сообщение об ошибке:
202	Информация	Удаление политики	Политика успешно удалена. Имя политики: Инициатор:

1202	Ошибка	Удаление политики	Произошла ошибка при удалении политики. Имя политики: Инициатор: Сообщение об ошибке:
203	Информация	Изменение политики	Политика успешно изменена. Имя политики: Инициатор:
1203	Ошибка	Изменение политики	Произошла ошибка при изменении политики. Имя политики: Инициатор: Сообщение об ошибке:
204	Информация	Добавление лицензии	Лицензия успешно добавлена. Тип: Действительна с: Действительна по: Количество: Инициатор:
1204	Ошибка	Добавление лицензии	Произошла ошибка при добавлении лицензии. Инициатор: Сообщение об ошибке:
205	Информация	Удаление лицензии	Лицензия успешно удалена. Тип: Действительна с: Действительна по: Количество: Инициатор:
1205	Ошибка	Удаление лицензии	Произошла ошибка при удалении лицензии. Инициатор: Сообщение об ошибке:
206	Информация	Добавление типа устройства	Тип устройства успешно добавлен. Имя: Инициатор:
1206	Ошибка	Добавление типа устройства	Произошла ошибка при добавлении типа устройства. Имя: Инициатор: Сообщение об ошибке:
207	Информация	Удаление типа устройства	Тип устройства успешно удален. Имя: Инициатор:
1207	Ошибка	Удаление типа устройства	Произошла ошибка при удалении типа устройства. Имя: Инициатор: Сообщение об ошибке:
208	Информация	Изменение типа устройства	Тип устройства успешно изменен. Имя: Инициатор:
1208	Ошибка	Изменение типа устройства	Произошла ошибка при изменении типа устройства. Имя: Инициатор: Сообщение об ошибке:
209	Информация	Добавление узла организационной структуры	Узел организационной структуры успешно добавлен. Путь: Инициатор:

1209	Ошибка	Добавление узла организационной структуры	Произошла ошибка при добавлении узла организационной структуры. Путь: Инициатор: Сообщение об ошибке:
210	Информация	Удаление узла организационной структуры	Узел организационной структуры успешно удален. Путь: Инициатор:
1210	Ошибка	Удаление узла организационной структуры	Произошла ошибка при удалении узла организационной структуры. Путь: Инициатор: Сообщение об ошибке:
211	Информация	Переименование узла организационной структуры	Узел организационной структуры успешно переименован. Старый путь: Новый путь: Инициатор:
1211	Ошибка	Переименование узла организационной структуры	Произошла ошибка при переименовании узла организационной структуры. Старый путь: Новый путь: Инициатор: Сообщение об ошибке:
212	Информация	Перемещение узла организационной структуры	Узел организационной структуры успешно перемещен. Старый путь: Новый путь: Инициатор:
1212	Ошибка	Перемещение узла организационной структуры	Произошла ошибка при перемещении узла организационной структуры. Старый путь: Новый путь: Инициатор: Сообщение об ошибке:
213	Информация	Добавление связанных объектов каталога	Связанные объекты каталога успешно добавлены. Путь: Пользователи: Группы: Контейнеры: Инициатор:
1213	Ошибка	Добавление связанных объектов каталога	Произошла ошибка при добавлении связанных объектов каталога. Путь: Пользователи: Группы: Контейнеры: Инициатор: Сообщение об ошибке:
214	Информация	Удаление связанных объектов каталога	Связанные объекты каталога успешно удалены. Путь: Пользователи: Группы: Контейнеры: Инициатор:

1214	Ошибка	Удаление связанных объектов каталога	Произошла ошибка при удалении связанных объектов каталога. Путь: Пользователи: Группы: Контейнеры: Инициатор: Сообщение об ошибке:
215	Информация	Создание роли	Роль успешно создана. Имя: Тип: Пользователи: Группы: Привилегии: Разрешить: Запретить: Инициатор:
1215	Ошибка	Создание роли	Произошла ошибка при создании роли. Имя: Тип: Пользователи: Группы: Привилегии: Разрешить: Запретить: Инициатор: Сообщение об ошибке:
216	Информация	Удаление роли	Роль успешно удалена. Имя: Инициатор: Сообщение об ошибке:
1216	Ошибка	Удаление роли	Произошла ошибка при удалении роли. Имя: Инициатор: Сообщение об ошибке:
217	Информация	Изменение роли	Роль успешно изменена. Имя: Новые пользователи: Удаленные пользователи: Новые группы: Удаленные группы: Новые привилегии: Разрешить: Запретить: Удаленные привилегии: Разрешить: Запретить: Инициатор:
1217	Ошибка	Изменение роли	Произошла ошибка при изменении роли. Имя: Новые пользователи: Удаленные пользователи: Новые группы: Удаленные группы: Новые привилегии: Разрешить: Запретить: Удаленные привилегии: Разрешить: Запретить: Инициатор: Сообщение об ошибке:

218	Информация	Создание назначения политики	Назначение политики успешно создано. Имя политики: Контейнер: Группа: Приоритет: Инициатор:
1218	Ошибка	Создание назначения политики	Произошла ошибка при создании назначения политики. Имя политики: Контейнер: Группа: Приоритет: Инициатор: Сообщение об ошибке:
219	Информация	Удаление назначения политики	Назначение политики успешно удалено. Имя политики: Контейнер: Группа: Инициатор:
1219	Ошибка	Удаление назначения политики	Произошла ошибка при удалении назначения политики. Имя политики: Контейнер: Группа: Инициатор: Сообщение об ошибке:
220	Информация	Изменение назначения политики	Назначение политики успешно изменено. Имя политики: Контейнер: Группа: Приоритет: Инициатор:
1220	Ошибка	Изменение назначения политики	Произошла ошибка при изменении назначения политики. Имя политики: Контейнер: Группа: Приоритет: Инициатор: Сообщение об ошибке:
221	Информация	Добавление роли в назначение политики	Роль успешно добавлена в назначение политики. Имя политики: Контейнер: Группа: Имя роли: Пользователи: Группы: Инициатор:
222	Информация	Удаление роли из назначения политики	Роль успешно удалена из назначения политики. Имя политики: Контейнер: Группа: Имя роли: Пользователи: Группы: Инициатор:

223	Информация	Изменение роли в назначении политики	Роль успешно изменена в назначении политики. Имя политики: Контейнер: Группа: Имя роли: Новые пользователи: Удаленные пользователи: Новые группы: Удаленные группы: Инициатор:
224	Информация	Создание тега	Тег успешно создан. Имя: Инициатор:
1224	Информация	Создание тега	Произошла ошибка при создании тега. Имя: Инициатор: Сообщение об ошибке:
225	Информация	Удаление тега	Тег успешно удален. Имя: Инициатор:
1225	Ошибка	Удаление тега	Произошла ошибка при удалении тега. Имя: Инициатор: Сообщение об ошибке:
226	Информация	Изменение тега	Тег успешно изменен. Имя: Новое имя: Инициатор:
1226	Ошибка	Изменение тега	Произошла ошибка при изменении тега. Имя: Новое имя: Инициатор: Сообщение об ошибке:
227	Информация	Добавление шаблона печати	Шаблон печати успешно добавлен. Имя: Тип: Инициатор:
1227	Ошибка	Добавление шаблона печати	Произошла ошибка при добавлении шаблона печати. Имя: Тип: Инициатор: Сообщение об ошибке:
228	Информация	Удаление шаблона печати	Шаблон печати успешно удален. Имя: Инициатор:
1228	Ошибка	Удаление шаблона печати	Произошла ошибка при удалении шаблона печати. Имя: Инициатор: Сообщение об ошибке:
229	Информация	Изменение шаблона печати	Шаблон печати успешно изменен. Имя: Инициатор:
1229	Ошибка	Изменение шаблона печати	Произошла ошибка при изменении шаблона печати. Имя: Инициатор: Сообщение об ошибке:

230	Информация	Создание справочника журнала учета	Справочник успешно создан. Имя: Инициатор:
1230	Ошибка	Создание справочника журнала учета	Произошла ошибка при создании справочника. Имя: Инициатор: Сообщение об ошибке:
231	Информация	Удаление справочника журнала учета	Справочник успешно удален. Имя: Инициатор:
1231	Ошибка	Удаление справочника журнала учета	Произошла ошибка при удалении справочника. Имя: Инициатор: Сообщение об ошибке:
232	Информация	Изменение справочника журнала учета	Справочник успешно изменен. Имя: Инициатор:
1232	Ошибка	Изменение справочника журнала учета	Произошла ошибка при изменении справочника. Имя: Инициатор: Сообщение об ошибке:
233	Информация	Создание шаблона журнала учета	Шаблон журнала успешно создан. Имя: Тип объектов: Инициатор:
1233	Ошибка	Создание шаблона журнала учета	Произошла ошибка при создании шаблона журнала. Имя: Тип объектов: Инициатор: Сообщение об ошибке:
234	Информация	Удаление шаблона журнала учета	Шаблон журнала успешно удален. Имя: Инициатор:
1234	Ошибка	Удаление шаблона журнала учета	Произошла ошибка при удалении шаблона журнала. Имя: Инициатор: Сообщение об ошибке:
235	Информация	Изменение шаблона журнала учета	Шаблон журнала успешно изменен. Имя: Инициатор:
1235	Ошибка	Изменение шаблона журнала учета	Произошла ошибка при изменении шаблона журнала. Имя: Инициатор: Сообщение об ошибке:
351	Информация	Изменение записи в журнале учёта	Запись успешно добавлена. Журнал учета: Поля: Инициатор:
1351	Ошибка	Изменение записи в журнале учёта	Произошла ошибка при добавлении записи. Журнал учета: Поля: Инициатор: Сообщение об ошибке:

352	Информация	Изменение записи в журнале учёта	Запись успешно изменена. Журнал учета: Поля: Новые поля: Инициатор:
1352	Ошибка	Изменение записи в журнале учёта	Произошла ошибка при изменении записи. Журнал учета: Поля: Новые поля: Инициатор: Сообщение об ошибке:
353	Информация	Изменение записи в журнале учёта	Запись успешно удалена. Журнал учета: Поля: Инициатор:
1353	Ошибка	Изменение записи в журнале учёта	Произошла ошибка при удалении записи. Журнал учета: Поля: Инициатор: Сообщение об ошибке:
1801	Ошибка	Отправка уведомления	Произошла ошибка при отправке уведомления. Сообщение об ошибке:
Код	Тип	Событие	Описание
600	Информация	Регистрация агента	Регистрация агента. Имя агента: Операционная система: IP адрес: Инициатор:
1600	Ошибка	Регистрация агента	Произошла ошибка при регистрации агента. Имя агента: Операционная система: IP адрес: Инициатор: Сообщение об ошибке:
2600	Предупреждение	Регистрация агента	Агент с именем 'Имя Агента' уже зарегистрирован. Имя агента: Операционная система: IP адрес: Инициатор:
601	Информация	Получение сертификата агента	Получение сертификата агента. Имя агента: Инициатор:
1601	Ошибка	Получение сертификата агента	Произошла ошибка при получении сертификата агента. Имя агента: Инициатор: Сообщение об ошибке:
602	Информация	Обновление сертификата агента	Имя агента: Инициатор:
1602	Ошибка	Обновление сертификата агента	Произошла ошибка при обновлении сертификата агента. Имя агента: Инициатор: Сообщение об ошибке:

603	Информация	Привязка устройства к агенту	Устройство успешно привязано к агенту. Имя агента: Инициатор:
1603	Ошибка	Привязка устройства к агенту	Произошла ошибка при привязывании устройства к агенту. Имя агента: Инициатор: Сообщение об ошибке:
604	Информация	Удаление привязки устройства к агенту	Устройство успешно отвязано от агента. Имя агента: Инициатор:
1604	Ошибка	Удаление привязки устройства к агенту	Произошла ошибка при удалении привязки устройства к агенту. Имя агента: Инициатор: Сообщение об ошибке:
605	Информация	Удаление агента	Агент успешно удален Имя агента: Инициатор:
1605	Ошибка	Удаление агента	Произошла ошибка при удалении агента. Имя агента: Инициатор: Сообщение об ошибке:
606	Информация	Регистрация агента	Агент успешно зарегистрирован. Имя агента: Инициатор:
1606	Ошибка	Регистрация агента	Произошла ошибка при регистрации агента. Имя агента: Инициатор: Сообщение об ошибке:
607	Информация	Отклонение агента	Агент успешно отклонен. Имя агента: Инициатор:
1607	Ошибка	Отклонение агента	Произошла ошибка при отклонении агента. Имя агента: Инициатор: Сообщение об ошибке:
608	Информация	Добавление задачи	Задача успешно добавлена. Устройство: Тип задачи: Комментарий: Инициатор:
1608	Ошибка	Добавление задачи	Произошла ошибка при добавлении задачи. Устройство: Тип задачи: Комментарий: Инициатор: Сообщение об ошибке:
609	Информация	Удаление задачи	Задача успешно удалена. Устройство: Тип задачи: Комментарий: Инициатор:

1609	Ошибка	Удаление задачи	Произошла ошибка при удалении задачи. Устройство: Тип задачи: Комментарий: Инициатор: Сообщение об ошибке:
610	Информация	Обновление имени агента	Имя агента успешно обновлено. Текущее имя агента: Новое имя агента: Инициатор:
1610	Ошибка	Обновление имени агента	Произошла ошибка при обновлении имени агента. Текущее имя агента: Новое имя агента: Инициатор: Сообщение об ошибке:
611	Информация	Обновление комментария агента	Комментарий агента успешно обновлен. Имя агента: Текущий комментарий агента: Новый комментарий агента: Инициатор:
1611	Ошибка	Обновление комментария агента	Произошла ошибка при обновлении комментария агента. Имя агента: Текущий комментарий агента: Новый комментарий агента: Инициатор: Сообщение об ошибке:
612	Информация	Выполнение задачи	Задача была успешно выполнена. Информация о сессии: Идентификатор сессии: Пользователь: Sid: Тип сессии: Имя агента: Устройство: Тип задачи: Комментарий: Создана пользователем: Инициатор:
1612	Ошибка	Выполнение задачи	Не удалось выполнить задачу. Информация о сессии: Идентификатор сессии: Пользователь: Sid: Тип сессии: Имя агента: Устройство: Тип задачи: Комментарий: Создана пользователем: Описание ошибки при выполнении задачи Инициатор: Сообщение об ошибке:

613	Информация	Отмена задачи пользователем	Задача была отменена пользователем. Информация о сессии: Идентификатор сессии: Пользователь: Sid: Тип сессии: Имя агента: Устройство: Тип задачи: Комментарий: Создана пользователем: Инициатор:
1613	Ошибка	Отмена задачи пользователем	Пользователю не удалось отменить задачу. Информация о сессии: Идентификатор сессии: Пользователь: Sid: Тип сессии: Имя агента: Устройство: Тип задачи: Комментарий: Создана пользователем: Инициатор: Сообщение об ошибке:
614	Информация	Обновление задачи	Задача успешно обновлена. Устройство: Тип задачи: Старый комментарий: Новый комментарий: Инициатор:
1614	Ошибка	Обновление задачи	Произошла ошибка при обновлении задачи. Устройство: Тип задачи: Старый комментарий: Новый комментарий: Инициатор: Сообщение об ошибке:
2615	Предупреждение	Подключение незарегистрированного устройства	Подключение незарегистрированного устройства. Информация о сессии: Идентификатор сессии: Пользователь: Sid: Тип сессии: Информация об устройстве: Серийный номер: Метка: Тип: Модель: Atr: Идентификатор агента: Имя агента: Инициатор:
2616	Предупреждение	Отсутствие связи с агентом	Длительное отсутствие связи с агентом. Идентификатор агента: Имя агента: Инициатор:

700	Информация	Инициализация сессий	Инициализация сессий. Количество сессий: Информация о сессиях: Идентификатор агента: Имя агента: Инициатор:
701	Информация	Пользователь вошел в систему	Пользователь вошел в систему. Идентификатор сессии: Пользователь: Sid: Тип сессии: Идентификатор агента: Имя агента: Инициатор:
702	Информация	Пользователь вышел из системы	Пользователь вышел из системы. Идентификатор сессии: Пользователь: Sid: Тип сессии: Идентификатор агента: Имя агента: Инициатор:
703	Информация	Компьютер заблокирован	Компьютер заблокирован. Идентификатор сессии: Пользователь: Sid: Тип сессии: Идентификатор агента: Имя агента: Инициатор:
704	Информация	Компьютер разблокирован	Компьютер разблокирован. Идентификатор сессии: Пользователь: Sid: Тип сессии: Идентификатор агента: Имя агента: Инициатор:
705	Информация	Пользователь подключился к сеансу	Пользователь подключился к сеансу. Идентификатор сессии: Пользователь: Sid: Тип сессии: Идентификатор агента: Имя агента: Инициатор:
706	Информация	Пользователь отключился от сеанса	Пользователь отключился от сеанса. Идентификатор сессии: Пользователь: Sid: Тип сессии: Идентификатор агента: Имя агента: Инициатор:

707	Информация	Пользователь подключился к терминальному сеансу	Пользователь подключился к терминальному сеансу. Идентификатор сессии: Пользователь: Sid: Тип сессии: Идентификатор агента: Имя агента: Инициатор:
708	Информация	Пользователь отключился от терминального сеанса	Пользователь отключился от терминального сеанса. Идентификатор сессии: Пользователь: Sid: Тип сессии: Идентификатор агента: Имя агента: Инициатор:
709	Информация	Подключение устройства	Подключение устройства. Идентификатор сессии: Пользователь: Sid: Тип сессии: Информация об устройстве: Серийный номер: Метка: Тип: Модель: Atr: Идентификатор агента: Имя агента: Инициатор:
710	Информация	Отключение устройства	Отключение устройства. Идентификатор сессии: Пользователь: Sid: Тип сессии: Информация об устройстве: Серийный номер: Метка: Тип: Модель: Atr: Идентификатор агента: Имя агента: Инициатор:
2711	Предупреждение	Нарушение привязки устройства к пользователю	Нарушение привязки устройства к пользователю. Информация о сессии: Идентификатор сессии: Пользователь: Sid: Тип сессии: Настройки привязки: Серийный номер: Atr: Ожидаемый Sid пользователя: Действие: Идентификатор агента: Имя агента: Инициатор:

2712	Предупреждение	Нарушение привязки устройства к агенту	Нарушение привязки устройства к агенту. Информация о сессии: Идентификатор сессии: Пользователь: Sid: Тип сессии: Настройки привязки: Серийный номер: Atr: Ожидаемый идентификатор агента: Действие: Идентификатор агента: Имя агента: Инициатор:
2714	Предупреждение	Блокировка пользовательской сессии	Устройство не удовлетворяет условиям привязки. Блокировка пользовательской сессии. Информация о сессии: Идентификатор сессии: Пользователь: Sid: Тип сессии: Серийный номер: Atr: Идентификатор агента: Имя агента: Инициатор:
2715	Предупреждение	Блокировка устройства	Устройство не удовлетворяет условиям привязки. Блокировка устройства. Информация о сессии: Идентификатор сессии: Пользователь: Sid: Тип сессии: Серийный номер: Atr: Идентификатор агента: Имя агента: Инициатор:
2716	Предупреждение	Блокировка пользовательской сессии и устройства	Устройство не удовлетворяет условиям привязки. Блокировка пользовательской сессии и устройства. Информация о сессии: Идентификатор сессии: Пользователь: Sid: Тип сессии: Серийный номер: Atr: Идентификатор агента: Имя агента: Инициатор:

1720	Ошибка	Обнаружена блокировка PIN-кода администратора на устройстве	Обнаружена блокировка PIN-кода администратора на устройстве. Информация об устройстве: Серийный номер: Метка: Тип: Модель: Atr: Апплет: Информация о сессии: Идентификатор сессии: Пользователь: Sid: Тип сессии: Идентификатор агента: Имя агента: Инициатор:
2721	Предупреждение	Обнаружена блокировка PIN-кода пользователя на устройстве	Обнаружена блокировка PIN-кода пользователя на устройстве. Информация об устройстве: Серийный номер: Метка: Тип: Модель: Atr: Апплет: Информация о сессии: Идентификатор сессии: Пользователь: Sid: Тип сессии: Идентификатор агента: Имя агента: Инициатор:
1722	Ошибка	Ввод неверного PIN-кода администратора на устройстве	Ввод неверного PIN-кода администратора на устройстве. Информация об устройстве: Серийный номер: Метка: Тип: Модель: Atr: Апплет: Информация о сессии: Идентификатор сессии: Пользователь: Sid: Тип сессии: Идентификатор агента: Имя агента: Инициатор:

2723	Предупреждение	Ввод неверного PIN-кода пользователя на устройстве	Ввод неверного PIN-кода пользователя на устройстве. Информация об устройстве: Серийный номер: Метка: Тип: Модель: Attr: Апплет: Информация о сессии: Идентификатор сессии: Пользователь: Sid: Тип сессии: Идентификатор агента: Имя агента: Инициатор:
Код	Тип	Событие	Описание
230	Информация	Создание справочника журнала учета	Справочник успешно создан. Имя: Инициатор:
1230	Ошибка	Создание справочника журнала учета	Произошла ошибка при создании справочника. Имя: Инициатор: Сообщение об ошибке:
231	Информация	Удаление справочника журнала учета	Справочник успешно удален. Имя: Инициатор:
1231	Ошибка	Удаление справочника журнала учета	Произошла ошибка при удалении справочника. Имя: Инициатор: Сообщение об ошибке:
232	Информация	Изменение справочника журнала учета	Справочник успешно изменен. Имя: Инициатор:
1232	Ошибка	Изменение справочника журнала учета	Произошла ошибка при изменении справочника. Имя: Инициатор: Сообщение об ошибке:
233	Информация	Создание шаблона журнала учета	Шаблон журнала успешно создан. Имя: Тип объектов: Инициатор:
1233	Ошибка	Создание шаблона журнала учета	Произошла ошибка при создании шаблона журнала. Имя: Тип объектов: Инициатор: Сообщение об ошибке:
234	Информация	Удаление шаблона журнала учета	Шаблон журнала успешно удален. Имя: Инициатор:
1234	Ошибка	Удаление шаблона журнала учета	Произошла ошибка при удалении шаблона журнала. Имя: Инициатор: Сообщение об ошибке:

235	Информация	Изменение шаблона журнала учета	Шаблон журнала успешно изменен. Имя: Инициатор:
1235	Ошибка	Изменение шаблона журнала учета	Произошла ошибка при изменении шаблона журнала. Имя: Инициатор: Сообщение об ошибке:
351	Информация	Изменение записи в журнале учёта	Запись успешно добавлена. Журнал учета: Поля: Инициатор:
1351	Ошибка	Изменение записи в журнале учёта	Произошла ошибка при добавлении записи. Журнал учета: Поля: Инициатор: Сообщение об ошибке:
352	Информация	Изменение записи в журнале учёта	Запись успешно изменена. Журнал учета: Поля: Новые поля: Инициатор:
1352	Ошибка	Изменение записи в журнале учёта	Произошла ошибка при изменении записи. Журнал учета: Поля: Новые поля: Инициатор: Сообщение об ошибке:
353	Информация	Изменение записи в журнале учёта	Запись успешно удалена. Журнал учета: Поля: Инициатор:
1353	Ошибка	Изменение записи в журнале учёта	Произошла ошибка при удалении записи. Журнал учета: Поля: Инициатор: Сообщение об ошибке:
Код	Тип	Событие	Описание
301	Информация	Добавление СКЗИ	СКЗИ успешно добавлено. Пользователь: Наименование: Серийный номер: Номер экземпляра: Инициатор:
1301	Ошибка	Добавление СКЗИ	Произошла ошибка при добавлении СКЗИ. Пользователь: Наименование: Серийный номер: Номер экземпляра: Инициатор: Сообщение об ошибке:
302	Информация	Обновление СКЗИ	СКЗИ успешно обновлено. Пользователь: Наименование: Серийный номер: Номер экземпляра: Инициатор:

1302	Ошибка	Обновление СКЗИ	Произошла ошибка при обновлении СКЗИ. Пользователь: Наименование: Серийный номер: Номер экземпляра: Инициатор: Сообщение об ошибке:
303	Информация	Уничтожение/изъятие СКЗИ	СКЗИ успешно уничтожено/изъято. Пользователь: Наименование: Серийный номер: Номер экземпляра: Инициатор:
1303	Ошибка	Уничтожение/изъятие СКЗИ	Произошла ошибка при уничтожении/изъятии СКЗИ. Пользователь: Наименование: Серийный номер: Номер экземпляра: Инициатор: Сообщение об ошибке:
304	Информация	Назначение СКЗИ	СКЗИ успешно назначено. Пользователь: Наименование: Серийный номер: Номер экземпляра: Инициатор:
1304	Ошибка	Назначение СКЗИ	Произошла ошибка при назначении СКЗИ. Пользователь: Наименование: Серийный номер: Номер экземпляра: Инициатор: Сообщение об ошибке:

Код	Тип	Событие	Описание
501	Информация	Выпуск устройства КристоПро DSS	Устройство КристоПро DSS успешно выпущено. Пользователь: Политика: Сертификаты: Инициатор:
1501	Ошибка	Выпуск устройства КристоПро DSS	Произошла ошибка при выпуске устройства КристоПро DSS. Пользователь: Политика: Инициатор: Сообщение об ошибке:
502	Информация	Включение устройства КристоПро DSS	Устройство КристоПро DSS успешно включено. Пользователь: Инициатор:
1502	Ошибка	Включение устройства КристоПро DSS	Произошла ошибка при включении устройства КристоПро DSS. Пользователь: Политика: Инициатор: Сообщение об ошибке:
503	Информация	Выключение устройства КристоПро DSS	Устройство КристоПро DSS успешно выключено. Пользователь: Инициатор:

1503	Ошибка	Выключение устройства КристоПро DSS	Произошла ошибка при выключении устройства КристоПро DSS. Пользователь: Инициатор: Сообщение об ошибке:
504	Информация	Отзыв устройства КристоПро DSS	Устройство КристоПро DSS успешно отозвано. Пользователь: Причина: Сертификаты: Инициатор:
1504	Ошибка	Отзыв устройства КристоПро DSS	Произошла ошибка при отзыве устройства КристоПро DSS. Пользователь: Причина: Инициатор: Сообщение об ошибке:
505	Информация	Обновление устройства КристоПро DSS	Устройство КристоПро DSS успешно обновлено. Пользователь: Новые сертификаты: Обновленные сертификаты: Удаленные сертификаты: Новая политика: Инициатор:
1505	Ошибка	Обновление устройства КристоПро DSS	Произошла ошибка при обновлении устройства КристоПро DSS. Пользователь: Инициатор: Сообщение об ошибке:
506	Информация	Удаление устройства КристоПро DSS	Устройство КристоПро DSS успешно удалено. Пользователь: Инициатор:
1506	Ошибка	Удаление устройства КристоПро DSS	Произошла ошибка при удалении устройства КристоПро DSS. Пользователь: Инициатор: Сообщение об ошибке:
507	Информация	Выпуск устройства КристоПро DSS ожидает решения	Выпуск устройства КристоПро DSS ожидает решения. Пользователь: Политика: Сертификаты: Инициатор:
508	Информация	Обновление устройства КристоПро DSS ожидает решения	Обновление устройства КристоПро DSS ожидает решения. Пользователь: Новые сертификаты: Обновленные сертификаты: Удаленные сертификаты: Новая политика: Инициатор:
509	Информация	Отмена обновления устройства КристоПро DSS	Обновление устройства КристоПро DSS успешно отменено. Пользователь: Инициатор:
1509	Ошибка	Отмена обновления устройства КристоПро DSS	Произошла ошибка при отмене обновления устройства КристоПро DSS. Пользователь: Инициатор: Сообщение об ошибке:

Код	Тип	Событие	Описание
401	Информация	Добавление AirKey к компьютеру	AirKey был добавлен к компьютеру. Устройство: Компьютер:
1401	Ошибка	Добавление AirKey к компьютеру	Произошла ошибка при добавлении AirKey к компьютеру. Устройство: Компьютер: Сообщение об ошибке:
402	Информация	Удаление AirKey от компьютера	AirKey был удален от компьютера. Устройство: Компьютер:
1402	Ошибка	Удаление AirKey от компьютера	Произошла ошибка при удалении AirKey от компьютера. Устройство: Компьютер: Сообщение об ошибке:
403	Информация	Создание кода подключения AirKey к компьютеру	Код подключения AirKey к компьютеру успешно создан. Устройство: Компьютер:
1403	Ошибка	Создание кода подключения AirKey к компьютеру	Произошла ошибка при создании кода подключения AirKey к компьютеру. Устройство: Компьютер: Сообщение об ошибке:

Руководство пользователя

Рядовые пользователи имеют доступ к web-приложениям **Сервис самообслуживания** (Self Service) и **Сервис удаленного самообслуживания** (Remote Self Service), где могут управлять своими устройствами самостоятельно.

- [Сервис самообслуживания \(Self Service\)](#)
- [Сервис удаленного самообслуживания \(Remote Self Service\)](#)

Сервис самообслуживания (Self Service)

Web-приложение Сервис самообслуживания (Self Service) предназначено для пользователей Indeed Certificate Manager и позволяет им самостоятельно осуществить определенные операции с устройствами. Аутентификация в приложение осуществляется в соответствии с выбранной на этапе развертывания системы конфигурацией.

Доступ к приложению осуществляется по адресу **<https://<FQDN сервера Indeed CM>/icmservice>**

После входа пользователя в сервис самообслуживания ему доступна информация о себе, сгруппированная в виде таблицы с полями: имя, логин, электронная почта, телефон и фото.

 Информация о пользователе (имя, имя для входа в домен, электронная почта, телефон и фото) добавляется в систему Indeed CM автоматически из профиля пользователя в Active Directory. Изменения, внесенные в профиль пользователя в Active Directory, моментально отображаются и в Self Service.



Белов Евгений Александрович

Логин DEMO\Evgeniy.Belov
E-mail evgeniy.belov@demo.com
Телефон +7 (905) 288-58-23

[Изменить ответы на секретные вопросы](#) [Пользователь КристоПро 2.0](#)

Ваши устройства

Выберите устройство для выполнения необходимой операции

▼ **Rutoken S, 0755398982** Evgeniy Belov

Выпущено

Действия

Содержимое

Обновить содержимое устройства

Обновить содержимое устройства, если срок его действия истекает, истек или была обновлена политика

Временно выключить устройство

Временно выключить устройство, если оно не нужно в течение продолжительного периода времени

Сообщить о том, что устройство неисправно, утеряно или скомпрометировано

Отозвать устройство для предотвращения использования ваших учетных данных

Изменить PIN-код устройства

Изменить PIN-код устройства, если вы предполагаете, что кто-либо другой узнал его

> **AirKey, f9a104e93d054e59** Evgeniy Belov

Выпущено

i Набор действий с устройством, доступных пользователю в приложении Self Service определяется администратором Indeed CM в разделе **Конфигурация > Политики > Поведение** Консоли управления.

Возможные операции, доступные для пользователя в Сервисе самообслуживания:

- Выпуск устройств в сервисе самообслуживания
 - Выпуск устройств Registry
 - Выпуск TPM Virtual Smart Card (VSC)
 - Выпуск Windows Hello for Business (WHfB)
- Операции с устройствами AirKey
 - Выпуск устройств AirKey
 - Подключение устройства AirKey к рабочей станции
- Изменение ответов на секретные вопросы
- Обновление устройств
- Выключение и включение устройств
- Выключение устройств без выполнения входа в систему
- Отзыв и очистка устройств
- Сброс и изменение PIN-кода устройств
- Просмотр содержимого устройства
- Загрузка файлов и ресурсов
- Клиентский агент Indeed CM
 - Сброс и разблокировка PIN-кода
 - Обновление содержимого устройства
- Выгрузка сертификата DSS на рабочую станцию пользователя

Выпуск устройств в сервисе самообслуживания

Пользователь может получить уже готовое к работе устройство у оператора службы поддержки или администратора Indeed Certificate Manager, либо выпустить его самостоятельно, получив “чистое” устройство у оператора службы поддержки. В случае если пользователь получил полностью готовое к работе устройство, то при входе в Сервис самообслуживание (Self Service) отобразится информация о нём, также пользователю может быть предложено выполнить следующие действия:

- **Установить секретные вопросы и ответы на них** (доступно при первом входе в Сервис самообслуживания перед выпуском устройства).



Белов Евгений Александрович

Логин	DEMO\Evgeniy.Belov
E-mail	evgeniy.belov@demo.com
Телефон	+7 (905) 288-58-23

Для работы с системой задайте ответы на секретные вопросы

Секретные вопросы необходимы для подтверждения операций с вашими устройствами

Секретный вопрос

Выберите вопрос



Ответ

ОК



Количество секретных вопросов и необходимость установки на их ответов в сервисе самообслуживания задается администратором Indeed CM в разделах **Поведение** и **Аутентификация** политики использования устройств, действующей на пользователя.

- **Выпустить устройство самостоятельно** (если выпущенных устройств нет, и выпуск разрешен настройками политики использования устройств администратором).

В процессе выпуска устройства возможен выбор сертификатов для записи на устройство. Список таких сертификатов будет отображен в диалоге выпуска.



Белов Евгений Александрович

Логин	DEMO\Evgeniy.Belov
E-mail	evgeniy.belov@demo.com
Телефон	+7 (905) 288-58-23

Перед началом работы вам необходимо выпустить устройство

Выберите требуемые сертификаты

Microsoft

☐ Вход по смарт-карте

КриптоПро 2.0

☐ Сертификат физического лица

Далее

 Возможность выбора сертификатов для записи на устройство настраивается администратором Indeed CM.

Если в политике использования устройств настроена [Интеграция со СМЭВ](#), то выборе шаблона квалифицированного сертификата выполняется проверка данных пользователя в системе межведомственного электронного взаимодействия (СМЭВ).

В форму проверки в СМЭВ подставляются данные пользователя из ресурсной системы (каталога пользователей). Пользователь может проверить данные на соответствие и изменить их, если настройками политики использования устройств администратором разрешено редактирование данных в форме проверки в СМЭВ. Если редактирование данных в форме проверки СМЭВ запрещено пользователю, то он может внести недостающие данные и продолжить выпуск устройства.



Белов Евгений Александрович

Логин DEMO\Evgeniy.Belov
E-mail evgeniy.belov@demo.com
Телефон +7 (905) 288-58-23

Перед началом работы вам необходимо выпустить устройство

Введите данные пользователя для проверки в СМЭВ

Тип пользователя

☒ Физическое лицо ☐ Юридическое лицо ☐ Индивидуальный предприниматель

Фамилия

Белов

Имя

Евгений

Отчество

Александрович

Пол

Мужской

Дата рождения

01.10.1988



Место рождения

г. Москва

Гражданство

Россия

СНИЛС

027-733-198 62

ИНН

520205004556

Тип документа

Паспорт гражданина РФ

Серия и номер документа

2202 919928
Дата выдачи 16.11.2002
Кем выдан Отделение УФМС России по гор. Москва
Код подразделения 770-011
Адрес регистрации Область 78 Санкт-Петербург
Город Санкт-Петербург
Адрес пр-кт. Невский, д.84/2, кв. 34
Далее Отмена

При выпуске устройство может быть инициализировано, если соответствующая опция включена в политике использования устройств.

❗ Если в политике использования устройств администратором включена опция **Инициализации устройства**, то в процессе выпуска все данные, хранящиеся на нем, будут удалены.

Выпуск устройства при первом входе в приложение Self Service. Пользователю разрешен самостоятельный выпуск устройств, включена обязательная инициализация устройства перед выпуском и ведется учет СКЗИ:



Белов Евгений Александрович

Логин	DEMO\Evgeniy.Belov
E-mail	evgeniy.belov@demo.com
Телефон	+7 (905) 288-58-23

Перед началом работы вам необходимо выпустить устройство

Задайте имя устройства

Устройство будет проинициализировано. Все данные на устройстве будут потеряны

Имя устройства

Евгений Белов

Номер документа

Номер документа

Устройство

ARDS JaCarta 0: IDProtect (X)



[Дополнительно](#) ▼

PIN-код администратора

PIN-код администратора

PIN-код администратора (ГОСТ)

PIN-код администратора (ГОСТ)

Выпустить

В случае ведения учета СКЗИ в Indeed CM при выпуске устройства необходимо указать **Номер и дату документа**, на основании которого осуществляется выпуск средства криптографической защиты.

Введите **PIN-код администратора** (если устройство не добавлено в Indeed CM) и **PIN-код пользователя** (доступно при отключенной инициализации устройства) в разделе Дополнительно. Значения PIN-кода пользователя и администратора могут быть пустыми. В этом случае они будут установлены в соответствии со значением в разделе **Конфигурация > Типы устройств**. Поддерживается ввод PIN-кодов для нескольких областей (например, для PKI и ГОСТ на устройствах JaCarta). Для выпуска устройства нажмите **Выпустить**.

Если администратором в политике использования устройств разрешена **Генерация случайного PIN-кода пользователя и его отображение в сервисе самообслуживания**, то по завершению процесса выпуска устройства вы увидите свой PIN-код. Также PIN-код может быть отправлен на вашу электронную почту или электронную почту вашего руководителя, если в политике использования устройств настроены соответствующие почтовые уведомления.



Белов Евгений Александрович

Логин	DEMO\Evgeniy.Belov
E-mail	evgeniy.belov@demo.com
Телефон	+7 (905) 288-58-23

Перед началом работы вам необходимо выпустить устройство

Устройство выпущено

PIN-код пользователя

1Qe0Bn

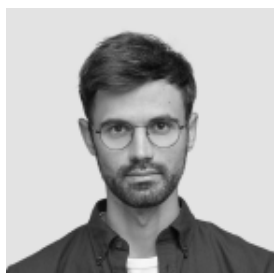
Закрыть

По завершению процесса выпуска устройства нажмите **Закрыть**. После выпуска устройства появится раздел Ваши устройства, где будут отображены сведения о выпущенном устройстве:

- Тип
- Серийный номер
- Имя
- Статус

Если вы не задавали секретные вопросы при выпуске, перейдите к созданию секретных вопросов (см. [Изменение ответов на секретные вопросы](#)).

Если запрос на сертификат требует одобрения оператора удостоверяющего центра, то выпуск устройства будет разделен на два этапа: отправку запроса и запись сертификата на устройство после одобрения запроса. После отправки запроса появится сообщение: **Выпуск устройства ожидает решения**. Нажмите кнопку **Заккрыть**.



Белов Евгений Александрович

Логин	DEMO\Evgeniy.Belov
E-mail	evgeniy.belov@demo.com
Телефон	+7 (905) 288-58-23

Перед началом работы вам необходимо выпустить устройство

Выпуск устройства ожидает решения

Заккрыть

После одобрения запроса оператором удостоверяющего центра в карточке пользователя появится информация о выпускаемом устройстве. Статус устройства при этом будет **В ожидании**. После одобрения запроса оператором удостоверяющего центра выпуск устройства можно будет продолжить нажав **Продолжить выпуск устройства**.



Белов Евгений Александрович

Логин DEMO\Evgeniy.Belov
E-mail evgeniy.belov@demo.com
Телефон +7 (905) 288-58-23

[? Изменить ответы на секретные вопросы](#) [Пользователь КriptoПро 2.0](#)

Ваши устройства

▼ Rutoken S, 0755398982

Евгений Белов

В ожидании

Действия

Содержимое

↻

Продолжить выпуск устройства

Продолжить выпуск устройства

Сообщить о том, что устройство неисправно или утеряно

Отозвать устройство для предотвращения использования ваших учетных данных

Выпуск устройств Registry

Требования

- Для рабочей станции пользователя Администратором системы [разрешен выпуск устройств Registry компьютера и/или пользователя](#).
- В конфигурацию системы добавлен тип устройства [Registry.xml](#).
- На рабочей станции установлен компонент **IndeedCM.Registry.Middleware**.

Если требования соблюдены, то при выпуске устройства в Self Service пользователю будут доступны считыватели **Registry - Machine** и **Registry - User**.



Особенности:

- Поддерживается выпуск только RSA сертификатов.
- Не поддерживается работа с PIN-кодами.
- Не поддерживается инициализация устройства.



Белов Евгений Александрович

Логин DEMO\Evgeniy.Belov
E-mail evgeniy.belov@demo.com
Телефон +7 (905) 288-58-23

[Изменить ответы на секретные вопросы](#) [Пользователь КриптоПро 2.0](#)

Ваши устройства

[+ Выпустить устройство](#)

Выпустить устройство

Задайте имя устройства

Имя устройства

Evgeniy Belov

Устройство

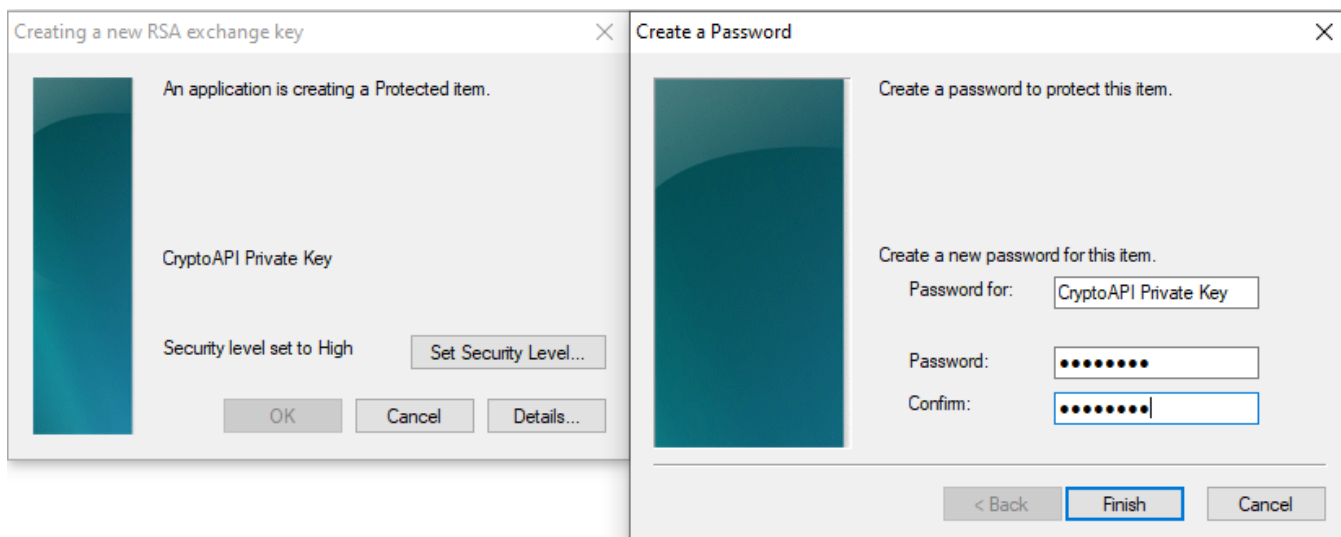
Registry - User: Registry ▼

Выпустить

Отмена

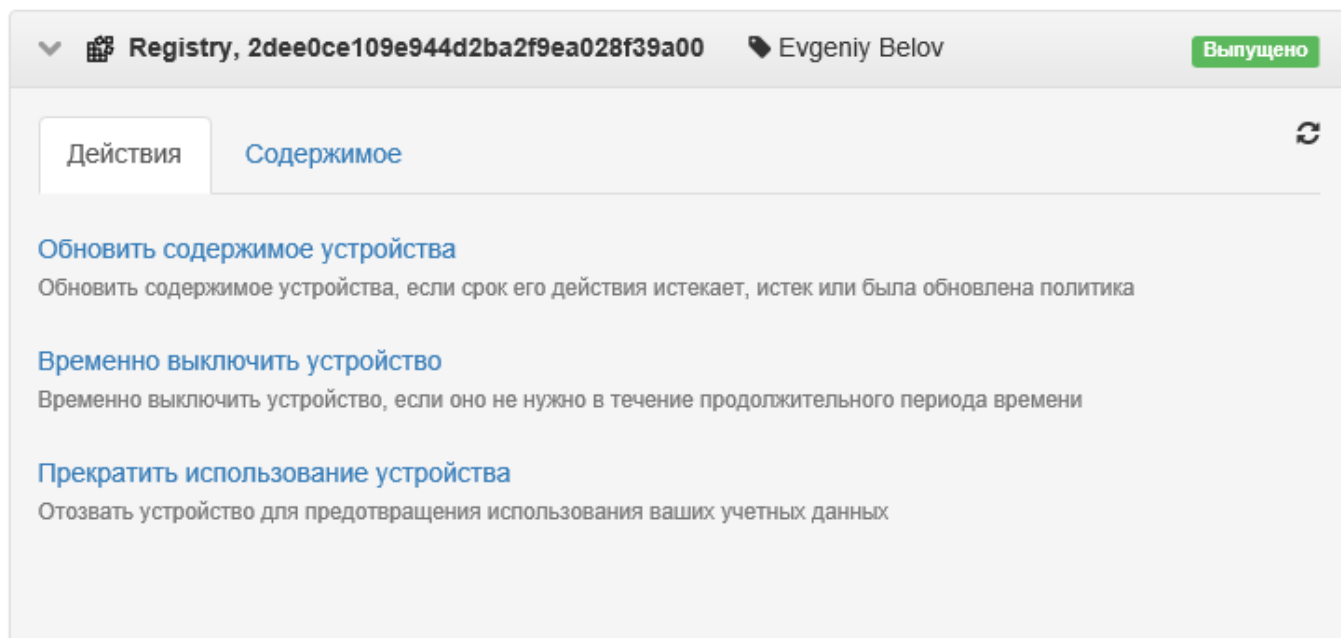
После нажатия кнопки **Выпустить** Indeed Certificate Manager создаст запрос на сертификат на УЦ и если в шаблоне сертификата была выбрана опция **При регистрации выводить запрос и требовать от пользователя ответ, если используется закрытый ключ** (Prompt the user during enrollment and require user input when the private key is used) на вкладке **Обработка запроса** (Request Handling), то в ходе выпуска требуется создать пароль на контейнер закрытого ключа:

- Нажмите **Выбор уровня безопасности..** (Set security Level..) в окне создания приватного RSA-ключа и задайте пароль, удовлетворяющий требованиям безопасности вашей организации.
- Нажмите **Finish** и **OK**.



❗ **Сброс пароля на контейнер при его утере невозможен. Требуется перевыпуск сертификата.**

Сертификаты с закрытыми ключами запишутся в хранилище сертификатов пользователя или компьютера.



Выпуск TPM Virtual Smart Card (VSC)

Требования

- Включена опция [Работа с TPM Virtual Smart Card](#) в разделе **Общие функции** Мастера настройки Indeed CM.
- В конфигурацию системы добавлен тип устройства [Tpm.xml](#).

 Для возможности разблокировки устройств TPM PIN-код администратора при добавлении должен меняться на случайный или на любой неслучайный TripleDES.

- Рабочая станция пользователя оснащена Доверенным платформенным модулем 2.0 (Trusted Platform Module).
- На рабочей станции установлен компонент **IndeedCM.TPM.Middleware**.

При выпуске устройства в Self Service пользователю будет предложено **Создать виртуальное устройство TPM** или выбрать подключенное аппаратное устройство.

Особенности:

- Поддерживается выпуск только RSA сертификатов.
- Не поддерживается инициализация устройства.



Белов Евгений Александрович

Логин DEMO\Evgeniy.Belov
E-mail evgeniy.belov@demo.com
Телефон +7 (905) 288-58-23

[? Изменить ответы на секретные вопросы](#) [Пользователь КриптоПро 2.0](#)

Ваши устройства

[+ Выпустить устройство](#)

Выпустить устройство

Задайте имя устройства

Имя устройства

Устройство

Создать виртуальное устройство TPM

Выпустить

Отмена

После нажатия кнопки **Выпустить** Indeed CM создаст виртуальную карту и закрепит ее за пользователем. Виртуальная карта TPM может использоваться как и аппаратные устройства на рабочей станции пользователя. Например, для аутентификации в домене.

Действия

Содержимое

**Обновить содержимое устройства**

Обновить содержимое устройства, если срок его действия истекает, истек или была обновлена политика

Временно выключить устройство

Временно выключить устройство, если оно не нужно в течение продолжительного периода времени

Прекратить использование устройства

Отозвать устройство для предотвращения использования ваших учетных данных

Сбросить PIN-код устройства

Сбросить PIN-код устройства, если оно заблокировано или вы предполагаете, что кто-либо другой узнал его

Выпуск Windows Hello for Business (WHfB)

Требования

- В инфраструктуре выполнено развертывание [Windows Hello for Business](#).
- Включена опция [Работа с Windows Hello for Business](#) в разделе **Общие функции** Мастера настройки Indeed CM.
- В конфигурацию системы добавлен тип устройства [Whfb.xml](#).
- Рабочая станция пользователя оснащена Доверенным платформенным модулем 2.0 (Trusted Platform Module).
- На рабочей станции установлен компонент **IndeedCM.WHfB.Middleware**.

При выпуске устройства в Self Service пользователю будет предложено **Настроить WHfB** и ли выбрать подключенное аппаратное устройство.



Особенности:

- Поддерживается выпуск сертификатов RSA 2048.
- Для пользователя на компьютере можно создать только одно устройство WHfB.
- Максимальное количество устройств WHfB на одном компьютере с Windows 10 составляет 10.
- Не поддерживается инициализация устройства.



Белов Евгений Александрович

Логин DEMO\Evgeniy.Belov
E-mail evgeniy.belov@demo.com
Телефон +7 (905) 288-58-23

[Изменить ответы на секретные вопросы](#) [Пользователь КриптоПро 2.0](#)

Ваши устройства

[+ Выпустить устройство](#)

Выпустить устройство

Задайте имя устройства

Имя устройства

Устройство

После нажатия кнопки **Выпустить** Indeed CM вызовет настройку PIN-кода для Windows Hello:

В вашей организации требуется использовать Windows Hello

Пароль легко украсть. Функция Windows Hello предоставляет сочетание двух факторов – вашего устройства и биометрии или ПИН-кода – вместо пароля для входа на устройство, в приложения и службы.

Как может PIN-код быть более безопасным, чем длинный пароль?



Задать PIN-код

Нажмите **Задать PIN-код** (Set up PIN), введите учетные данные для основной и пользовательской (с помощью Indeed CM MFA адаптера) проверки подлинности и нажмите **Submit**.

×

AD FS

For security reasons, we require additional information to verify your account

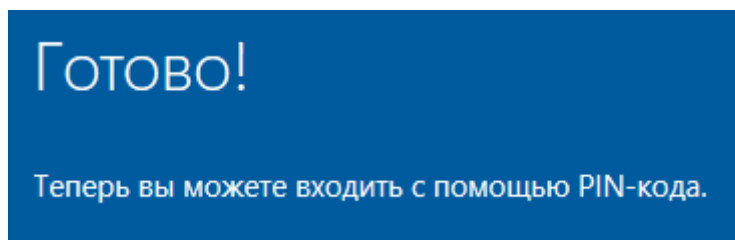
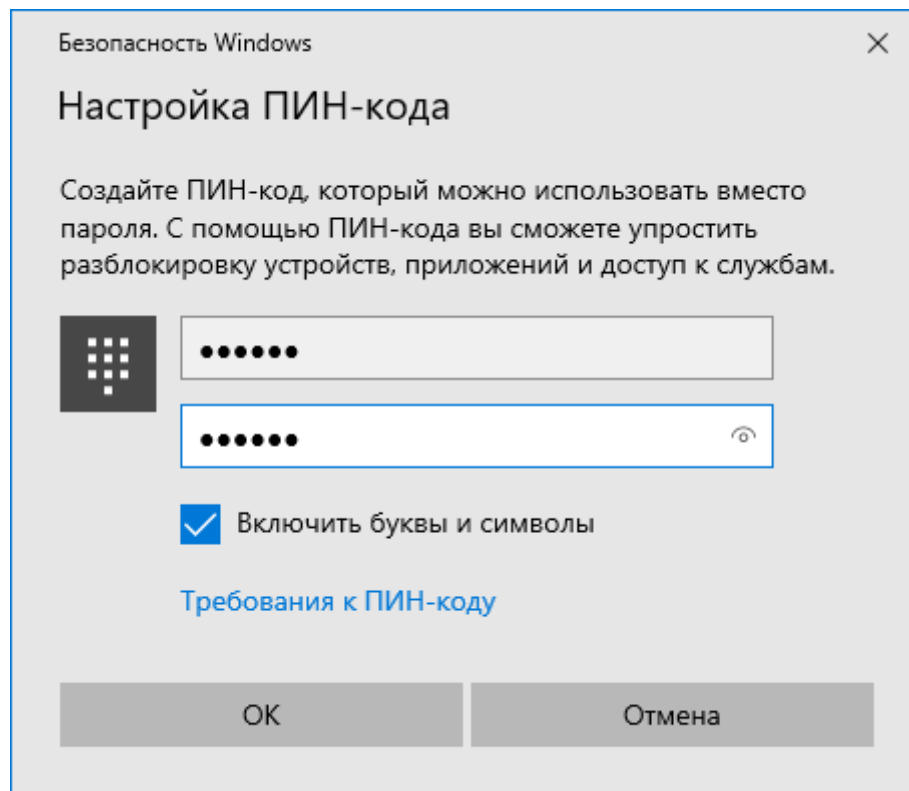
This content is provided by the Indeed CM MFA adapter.

Token

Submit

© 2018 Microsoft

Создайте PIN-код и нажмите **OK**.



После успешного создания PIN-кода Indeed CM продолжит выпуск карты:

- Запросит сертификаты по шаблонам добавленным в политику использования устройств.
- Запишет их на устройство.
- Закрепит устройство за пользователем.

WHfB может использоваться как и аппаратные устройства на рабочей станции пользователя. Например, для аутентификации в домене.

Действия

Содержимое

Обновить содержимое устройства

Обновить содержимое устройства, если срок его действия истекает, истек или была обновлена политика

Временно выключить устройство

Временно выключить устройство, если оно не нужно в течение продолжительного периода времени

Прекратить использование устройства

Отозвать устройство для предотвращения использования ваших учетных данных

Операции с устройствами AirKey

В разделе описаны основные доступные операции с устройствами Indeed AirKey Enterprise в Сервисе самообслуживания (Self Service) Indeed Certificate Manager:

- Выпуск устройства AirKey
- Обновление устройсва
- Выключение/Включение устройства
- Отзыв устройства
- Сброс\Изменение PIN-кода
- Подключение устройства AirKey к рабочей станции

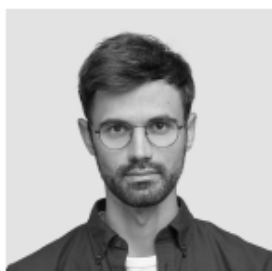
Обновление, Выключение, Включение, Отзыв и Сброс\Изменение PIN-кода выполняются по аналогии с аппаратными устройствами в [Сервисе самообслуживания](#) (Self Service).

[Выпуск устройства AirKey](#) и [Подключение устройства AirKey к рабочей станции](#) описаны подробно в соответствующих пунктах.

Выпуск устройств AirKey

Выпуск устройства AirKey включается администратором Indeed Certificate Manager в настройках политики использования устройств (опция [Разрешить пользователю выпуск AirKey устройств](#) в разделе Поведение). Как и в случае с аппаратными устройствами, для выпуска виртуального устройства на рабочей станции пользователя должен быть установлен компонент **IndeedCM.AirKey.Middleware** и драйвер **IndeedID.AirKey.Runtime**.

При выпуске устройства пользователю будет предложено **Создать новое устройство AirKey** или выбрать подключенное аппаратное устройство:



Белов Евгений Александрович

Логин	DEMO\Evgeniy.Belov
E-mail	evgeniy.belov@demo.com
Телефон	+7 (905) 288-58-23

[? Изменить ответы на секретные вопросы](#) [Пользователь КриптоПро 2.0](#)

Ваши устройства

[+ Выпустить устройство](#)

Выпустить устройство

Задайте имя устройства

Имя устройства

Evgeniy Belov

Устройство

Создать новое устройство AirKey ▼

Выпустить

Отмена

После выпуска устройства оно автоматически свяжется с рабочей станцией пользователя. Список разрешенных для подключения выпущенного устройства компьютеров отображается в свойствах устройства AirKey.

Ваши устройства

▼

AirKey, 80c889c722f34550

Evgeniy Belov

Выпущено

Действия

Содержимое

↺

Обновить содержимое устройства

Обновить содержимое устройства, если срок его действия истекает, истек или была обновлена политика

Временно выключить устройство

Временно выключить устройство, если оно не нужно в течение продолжительного периода времени

Прекратить использование устройства

Отозвать устройство для предотвращения использования ваших учетных данных

Сбросить PIN-код устройства

Сбросить PIN-код устройства, если оно заблокировано или вы предполагаете, что кто-либо другой узнал его

Разрешенные компьютеры

WIN10X64TPM.demo.local

Подключение устройства AirKey к рабочей станции

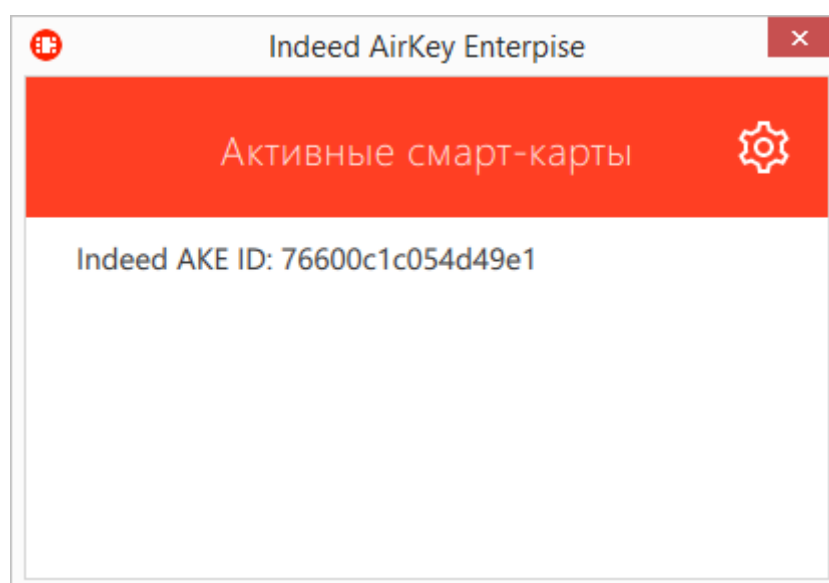
После установки AirKey Runtime в области уведомлений панели задач Windows появится индикатор подключенных устройств AirKey. Если к рабочей станции не подключено ни одного устройства, или связь с Indeed AirKey Enterprise Server не установлена, то индикатор будет **серого** цвета, если подключено хотя бы одно устройство – **красного**.



Подключение устройства возможно двумя способами:

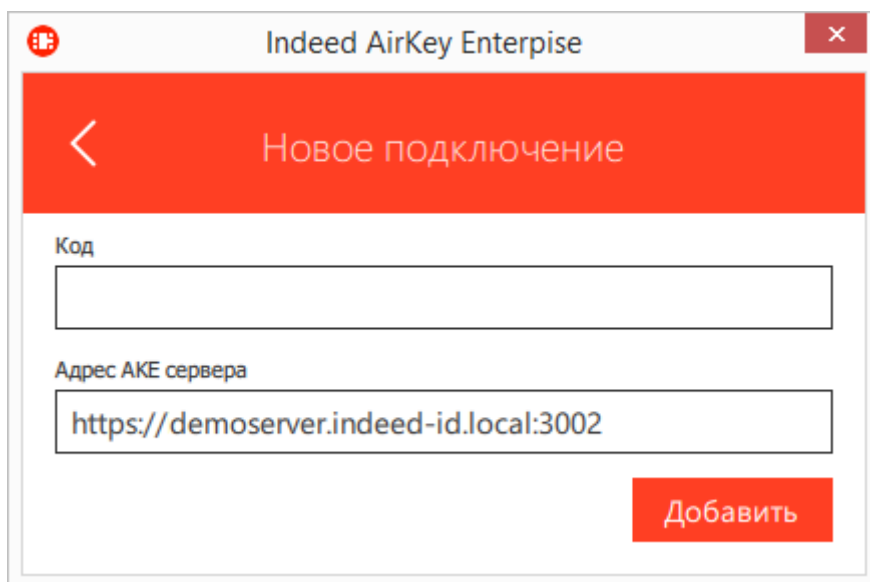
- **Подключение через Indeed CM.** Выпущенное пользователем устройство автоматически подключается к разрешенным компьютерам, если они располагаются в корпоративной сети предприятия.
- **Подключение через панель управления Indeed AirKey Enterprise.** Применяется в случае, если устройство не может быть подключено автоматически (например, при нахождении компьютера за пределами корпоративной сети предприятия). Пользователь вручную добавляет ранее выпущенное оператором устройство к компьютеру в приложении Indeed AirKey Enterprise.

Просмотреть подключенные автоматически устройства можно в панели управления Indeed AirKey Enterprise, щелкнув на значок в области уведомлений Windows. В разделе **Активные смарт-карты** отображаются автоматически подключенные к рабочей станции устройства. Для каждого устройства указан ID (серийный номер), отображаемый в сервисах Indeed CM.



Для добавления и подключения устройства AirKey к компьютеру откройте **панель**

управления Indeed AirKey Enterprise, нажмите  и затем кнопку . Введите **Код**, полученный от оператора, выпустившего устройство и нажмите **Добавить**. Код действителен в течение часа и может быть использован только один раз. Адрес сервера Indeed AirKey Enterprise подставляется автоматически.



Indeed AirKey Enterprise

< Новое подключение

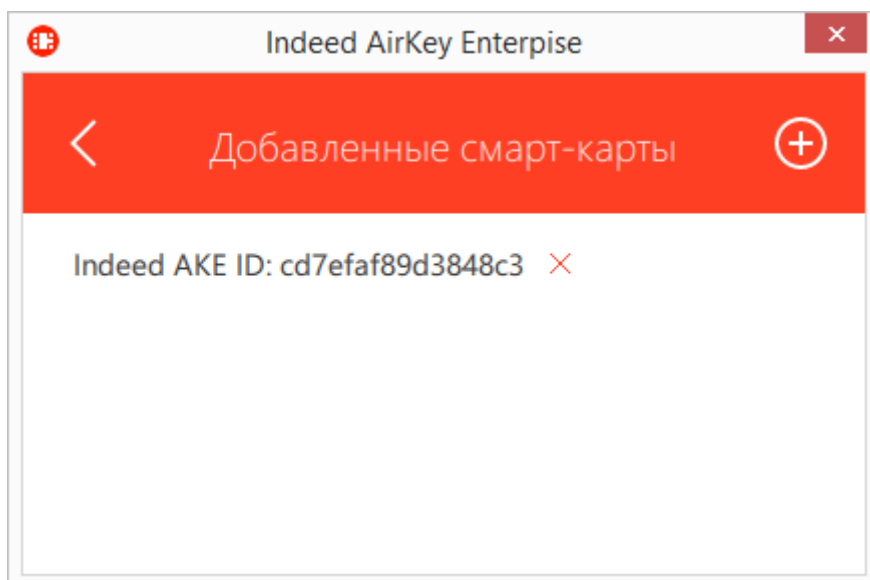
Код

Адрес АКЕ сервера

https://demoserver.indeed-id.local:3002

Добавить

После добавления устройство AirKey отобразится в панели управления. Для удаления устройства нажмите  и подтвердите действие.



Indeed AirKey Enterprise

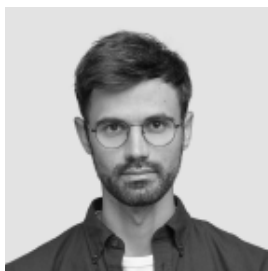
< Добавленные смарт-карты +

Indeed AKE ID: cd7efaf89d3848c3 X

Изменение ответов на секретные вопросы

Чтобы изменить ответы на заданные секретные вопросы, нажмите **Изменить ответы на секретные вопросы**. Выберите вопрос из списка доступных и задайте на него ответ. Нажмите **ОК** для сохранения изменений или **Отмена**.

i Возможность изменения ответов на секретные вопросы настраивается администратором Indeed CM в разделе **Поведение** политики использования устройств.



Белов Евгений Александрович

Логин	DEMO\Evgeniy.Belov
E-mail	evgeniy.belov@demo.com
Телефон	+7 (905) 288-58-23

i Изменить ответы на секретные вопросы Пользователь КристоПро 2.0

Секретные вопросы

Секретные вопросы необходимы для подтверждения операций с вашими устройствами

Секретный вопрос

Ваш любимый цвет? ▼

Ответ

ОК

Отмена

Обновление устройств

Обновление устройства необходимо в случаях если:

- Срок действия одного или нескольких сертификатов истек (или истекает)
- Администратором Indeed Certificate Manager была назначена новая политика для вашего пользователя
- На устройстве были добавлены сертификаты вне Indeed CM (если в политике использования устройств [Включено отслеживание сертификатов](#))
- В политике использования устройств:
 - изменилось количество шаблонов сертификатов
 - добавлены/удалены общие сертификаты
 - присутствует хотя бы один необязательный сертификат (для последующей его записи/удаления на устройство/с устройства)
 - включена или отключена интеграция с Indeed Access Manager
 - включена или отключена интеграция с Secret Net Studio

 Возможность обновления устройства настраивается администратором Indeed CM в разделе **Поведение** политики использования устройств.

Для обновления устройства выполните следующие действия:

1. Нажмите **Обновить содержимое устройства**.
2. Подключите устройство к компьютеру, введите PIN-код и нажмите **Обновить**.

Ваши устройства



 Rutoken ECP, 0894130607

 Evgeniy Belov

Выпущено

Обновить устройство

PIN-код пользователя

Вставьте устройство и нажмите 'Обновить'

Обновить

Отмена

3. Если на устройство были добавлены сертификаты вне Indeed CM и в политике использования устройств **Включено отслеживание сертификатов**, то при обновлении устройства данные сертификаты могут быть выбраны для отслеживания.

▼  Rutoken ECP, 0894130607  Evgeniy Belov Выпущено

Обновить устройство

На устройстве обнаружены следующие сертификаты. Выберите сертификаты, которые будут отслеживаться

Субъект	Издатель	Действителен до
☒ Operator	Тестовый головной УЦ	22.04.2021 15:00

OK

4. После того, как устройство будет обновлено, нажмите **Заккрыть**.

 Если запрос на сертификат требует одобрения оператора удостоверяющего центра, то обновление устройства будет состоять из двух этапов: отправки запроса на сертификат и записи сертификата на устройство (если запрос будет одобрен). Процесс обновления с подтверждением запроса оператором аналогичен процессу выпуска устройства с подтверждением оператором удостоверяющего центра.

Выключение и включение устройств

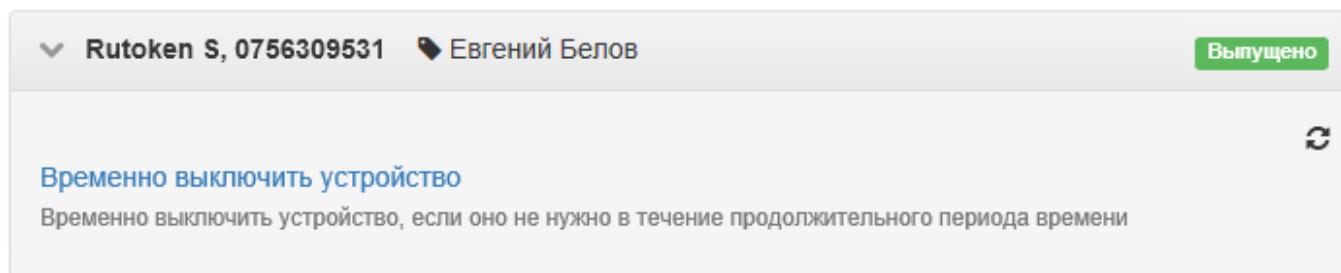
Устройство пользователя может быть выключено на определенный промежуток времени и затем снова включено. Например, на период отпуска. В зависимости от настроек политики использования устройств вам могут быть доступны следующие действия:

- Выключение и включение устройства
- Только выключение устройства
- Только включение устройства

 Выключение и включение осуществляется без подключения карты к рабочей станции.

Для выключения устройства выполните следующие действия:

1. Нажмите **Временно выключить устройство**.



2. Подтвердите своё действие нажатием кнопки **Выключить**.
3. После того, как устройство будет выключено, нажмите **Заккрыть**.
4. Статус устройства изменится с **Выпущено** на **Выключено**.

 При выключении устройства все или только некоторые из записанных на него сертификатов могут быть отозваны. Настройку отзыва сертификатов при выключении устройства задает администратор Indeed CM.

Для включения устройства выполните следующие действия:

1. Нажмите **Включить устройство**.

 **Rutoken S, 0756309531**  **Евгений Белов**

Выключено

Включить устройство
Включить устройство для того, что бы было возможно использовать его снова

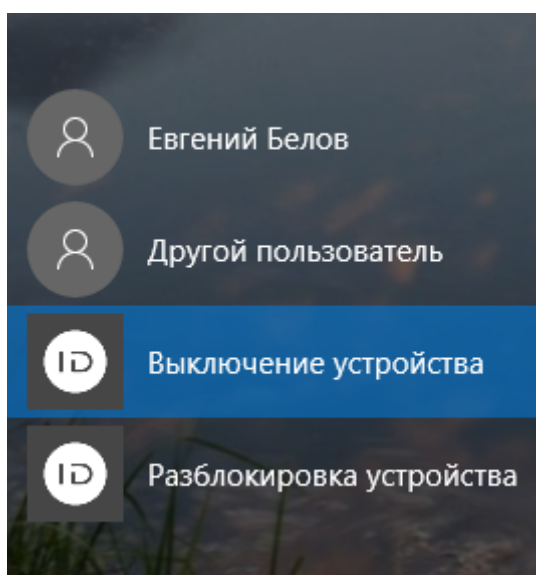
2. Подтвердите своё действие нажатием кнопки **Включить**.
3. После того, как устройство будет включено, нажмите **Заккрыть**.
4. Статус устройства изменится с **Выключено** на **Выпущено**.

Выключение устройств без выполнения входа в систему

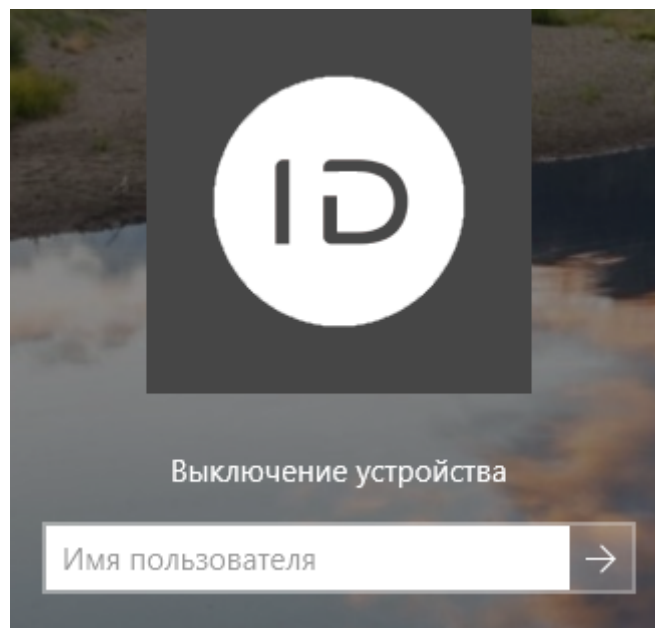
В экстренном случае (например, забыли карту дома или потеряли в общественном месте, а обнаружили это только придя на работу) пользователь может самостоятельно выключить устройство без выполнения входа в операционную систему.

❗ Выключение устройства доступно только в том случае, если у рабочей станции, с которой осуществляется операция, есть связь с сервером Indeed Certificate Manager и у пользователя настроены секретные вопросы. Функция выключения устройства без выполнения входа в операционную систему может быть отключена администратором. В этом случае соответствующий пункт не отображается на экране выбора пользователей.

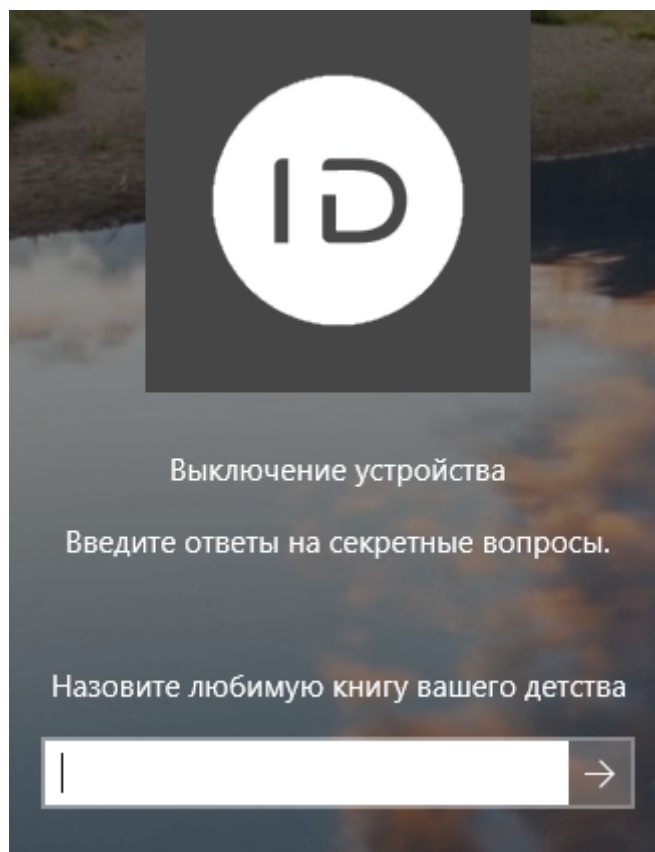
1. Для выключения устройства выберите **Выключение устройства** на экране выбора пользователей. Ниже на рисунке приведен пример для операционной системы Windows 10. Механизм выключения в операционных системах Windows 7 и Windows 8 выглядит похожим образом.



2. Укажите ваше имя пользователя (логин), устройство (смарт-карту) которое необходимо выключить.

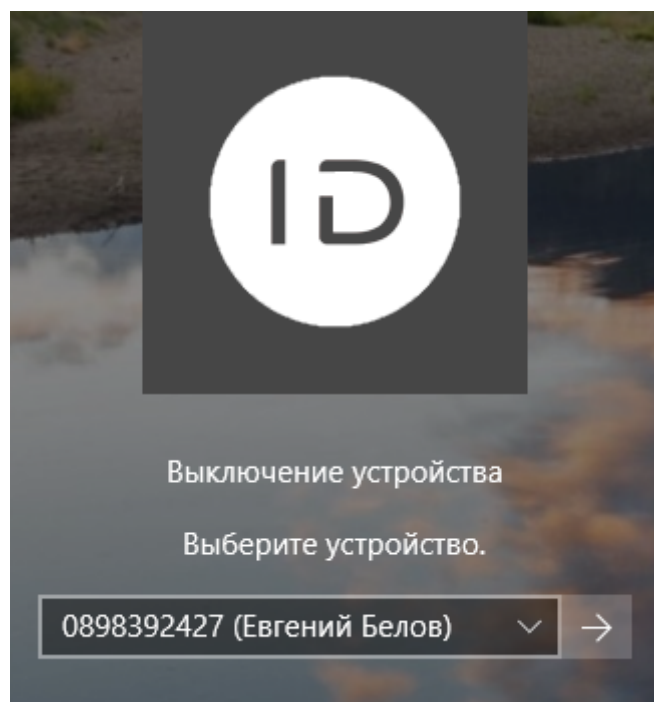


3. Введите ответы на секретные вопросы.

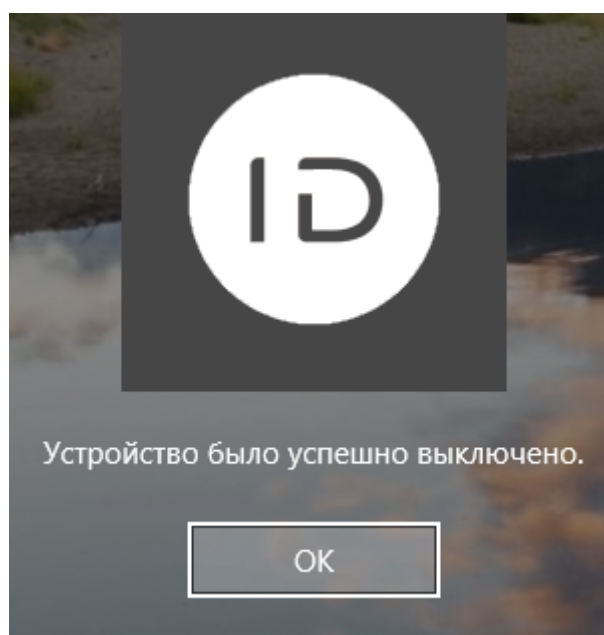


4. Выберите устройство из списка выпущенных устройств пользователя и нажмите





В случае успешного выключения устройства появится соответствующее сообщение.



Отзыв и очистка устройств

Устройство пользователя может быть отозвано в случае его повреждения, утери или компрометации.

 При отзыве устройства все или только некоторые из записанных на него сертификатов могут быть отозваны без возможности восстановления. Настройку **Отзывать сертификат при отзыве или выключении устройства** задает администратор Indeed Certificate Manager.

Для отзыва устройства выполните следующие действия:

1. Нажмите **Сообщить о том, что устройство неисправно, утеряно или скомпрометировано**.
2. Укажите причину отзыва:
 - Устройство неисправно
 - Устройство утеряно
 - Компрометация устройства
3. Нажмите кнопку **Отозвать**.
4. После того, как устройство будет отозвано, нажмите **Заккрыть**.
5. Статус устройства изменится с **Выпущено** на **Отозвано**.

Отозванное оператором Indeed CM устройство можно очистить. Для очистки устройства подключите его к своей рабочей станции и нажмите **Очистить устройство**.

 Для очистки и удалении устройств TPM, Registry, WHfB нажмите **Удалить устройство**.

Ваши устройства

▼ Rutoken S, 0755398982

Евгений Белов

Отозвано

Очистить устройство 

Номер документа

[Дополнительно](#) ▼

Оставьте поле 'Новый PIN-код пользователя' пустым, если хотите использовать значение, установленное производителем устройства

Новый PIN-код пользователя

Пожалуйста, вставьте устройство и нажмите 'Очистить'

Очистить

Отмена

 При очистке устройства все данные, записанные на него при помощи Indeed CM, будут удалены.

Если на очищаемом устройстве содержатся средства криптографической защиты информации (СКЗИ), подлежащие учету в соответствии с законодательством РФ, то в процессе очистки имеющиеся СКЗИ будут уничтожены. В этом случае необходимо указать **Номер документа**, в соответствии с которым выполняется уничтожение СКЗИ.

При очистке устройства PIN-код пользователя может быть изменен. Indeed CM может изменить его назначение, установленное по умолчанию, или на значение, соответствующее используемой в вашей компании политике безопасности (требования к длине и сложности пароля). Укажите **Новый PIN-код пользователя**, который должен быть установлен на устройстве после его очистки или оставьте это поле пустым для установки PIN-кода по умолчанию и нажмите **Очистить**. После очистки устройство останется закрепленным за вами в Indeed CM и может быть повторно выпущено (см. **Выпуск устройства**).

Сброс и изменение PIN-кода устройств

Если пользователь забыл PIN-код своего устройства и заблокировал его, он может сбросить PIN-код и задать новый. При этом устройство разблокируется.

 Возможность сброса PIN-кода настраивается администратором Indeed Certificate Manager в политике использования устройств раздел **Поведение**.

Если есть основания полагать, что PIN-код пользователя устройства стал известен кому-то другому, то он может изменить его.

Сброс PIN-кода

Для сброса PIN-кода устройства выполните следующие действия:

1. Нажмите **Сбросить PIN-код устройства**.
2. Подключите устройство к компьютеру.
3. Задайте новый PIN-код и подтвердите его.
4. Нажмите **Сбросить**.
5. После того, как PIN-код будет сброшен, нажмите **Заккрыть**.

Ваши устройства

 Rutoken S, 0755398982  Евгений Белов

Выпущено

Сбросить PIN-код 

Новый PIN-код

Подтверждение PIN-кода

Пожалуйста, вставьте устройство и нажмите 'Сбросить'

Сбросить

Отмена

Изменение PIN-кода

Для изменения PIN-кода устройства выполните следующие действия:

1. Нажмите **Изменить PIN-код устройства**.
2. Подключите устройство к компьютеру.
3. Введите текущий PIN-код, задайте новый PIN-код и подтвердите его.
4. Нажмите **Изменить**.
5. После того, как PIN-код будет изменен, нажмите **Заккрыть**.

Ваши устройства

▼ Rutoken S, 0755398982

 Евгений Белов

Выпущено

Изменить PIN-код

Для изменения PIN-кода необходимо ввести старый PIN-код. В случае, если он был утрачен, обратитесь к администратору системы

Текущий PIN-код

Новый PIN-код

Подтверждение PIN-кода

Пожалуйста, вставьте устройство и нажмите 'Изменить'

Изменить

Отмена

Просмотр содержимого устройства

Если настройками системы разрешено отображение содержимого устройства в Self Service, то в свойствах выпущенного устройства будет доступна вкладка **Содержимое**, содержащая сведения о сертификатах, находящихся на устройстве.

✔ Опция **Просмотр содержимого устройства** в разделе **Общие функции** Мастера настройки Indeed CM.

При необходимости пользователь может распечатать сведения о сертификате и(или) его запросе. Печать осуществляется по нажатию кнопки .

Ваши устройства

▼  Rutoken ECP, 0894130607  Evgeniy Belov Выпущено

Действия

Содержимое

↻

Сертификаты

Шаблон	УЦ	Действителен до	Состояние
Вход по смарт-карте	demo-DC-CA	21.01.2021 12:11	Действительный 

Отслеживаемые сертификаты

Субъект	Издатель	Действителен до	Состояние
Operator	Тестовый головной УЦ	22.04.2021 15:00	Действительный 

Сертификат

Запрос на сертификат

Загрузка файлов и ресурсов

Если при настройке системы администратором добавлены файлы и/или ссылки для использования в сервисе самообслуживания (Self Service), то пользователь может воспользоваться ими перейдя по ссылке: <https://<FQDN сервера Indeed CM>/icmservice/>



Downloads или нажав в личном кабинете кнопку .



Опция **Загрузка файлов и ресурсов** в разделе **Общие функции** Мастера настройки Indeed CM.

На странице **Загрузки** будут доступны ресурсы, добавленные администратором:



Загрузки

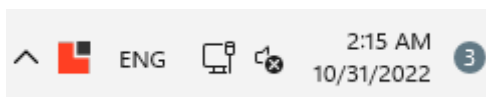
- [Инструкция по работе в сервисе самообслуживания](#)
- [Пользовательский компонент для работы с устройствами JaCarta](#)
- [Пользовательский компонент для работы с устройствами Рутокен](#)
- [Панель управления Рутокен](#)
- [Цепочка сертификатов УЦ](#)

Если добавлен файл, то при нажатии на ссылку начнется его скачивание, если веб-страница - то она откроется в новой вкладке.

Клиентский агент Indeed CM

На рабочей станции пользователя может быть установлен Клиентский Агент Indeed CM, который позволит администраторам назначать задачи для устройств пользователя (USB-токенов, смарт-карт) и выполнять их в полностью автоматическом или полуавтоматическом режиме.

Агент запускается автоматически. В области уведомлений отображается логотип  когда а Агент активен.

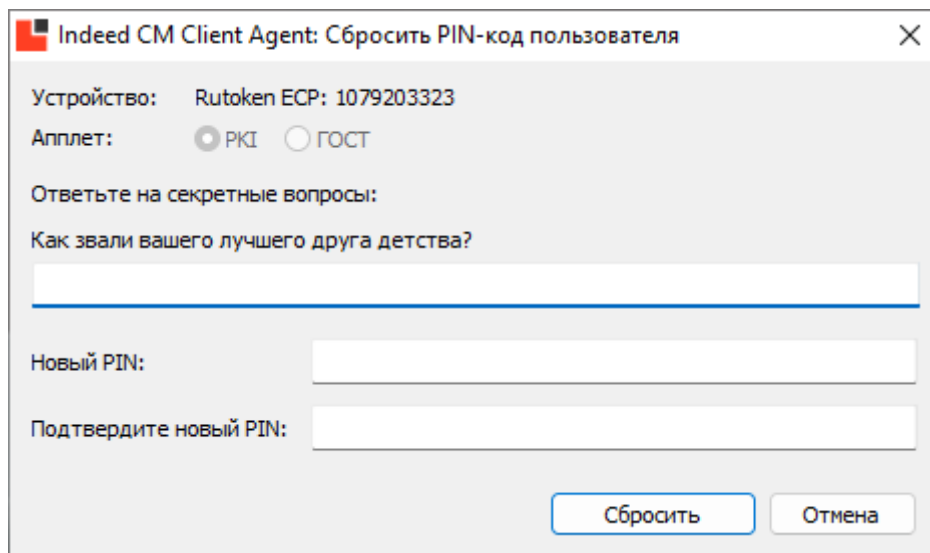


Задачи, требующие действия пользователя:

- [Сброс и разблокировка PIN-кода](#)
- [Обновление содержимого устройства](#)

Сброс и разблокировка PIN-кода

Если вы забыли PIN-код устройства или заблокировали его, сообщите об этом ответственному администратору в вашей организации. Он создаст задачу по сбросу PIN-кода для вашего устройства. Подключите его к компьютеру и дождитесь появления формы сброса PIN-кода.

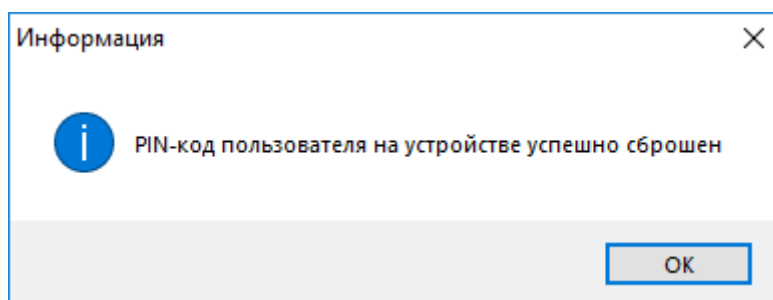


The screenshot shows a dialog box titled "Indeed CM Client Agent: Сбросить PIN-код пользователя". It contains the following fields and controls:

- Устройство: Rutoken ECP: 1079203323
- Апплет: ☒ PKI ☐ ГОСТ
- Ответьте на секретные вопросы:
Как звали вашего лучшего друга детства?
[Text input field]
- Новый PIN: [Text input field]
- Подтвердите новый PIN: [Text input field]
- Buttons: Сбросить, Отмена

❗ Для сброса PIN-кода у вас должны быть заданы ответы на секретные вопросы. Если вы не помните ответы, измените их в **Сервисе самообслуживания** (Self Service).

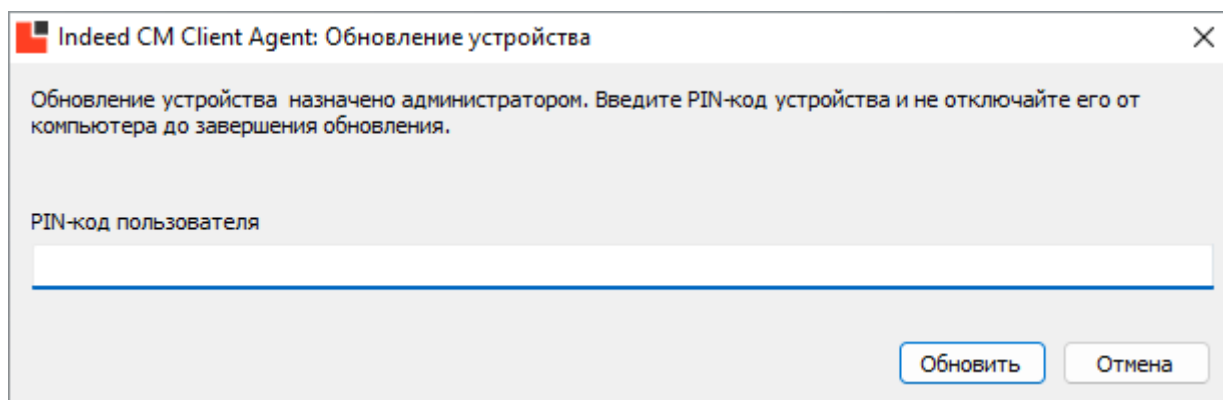
Введите ответ на один или несколько секретных вопросов, задайте новый PIN-код, его подтверждение и нажмите **Сбросить**. В случае успешного сброса появится сообщение.



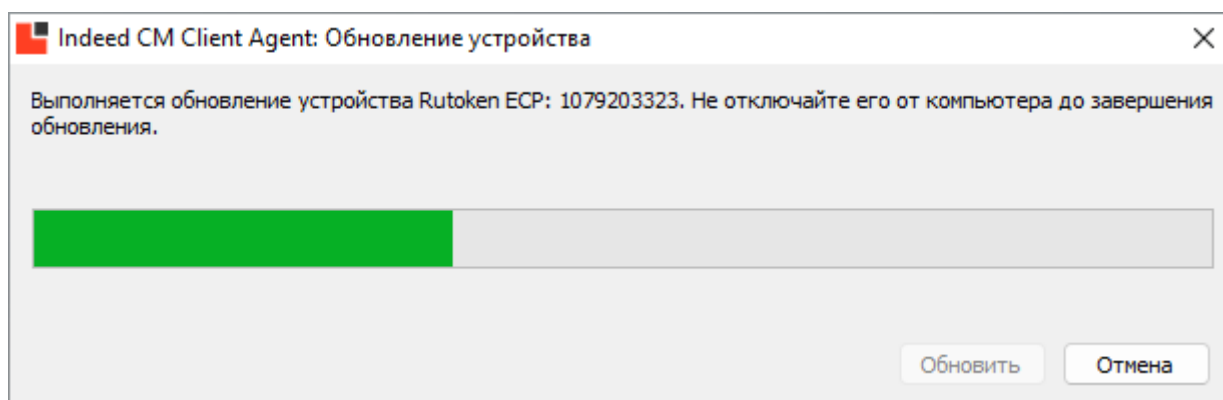
Обновление содержимого устройства

Обновление устройства может потребоваться, если срок действия одного или нескольких сертификатов на вашем устройстве подходит к концу, или вам потребовался другой сертификат.

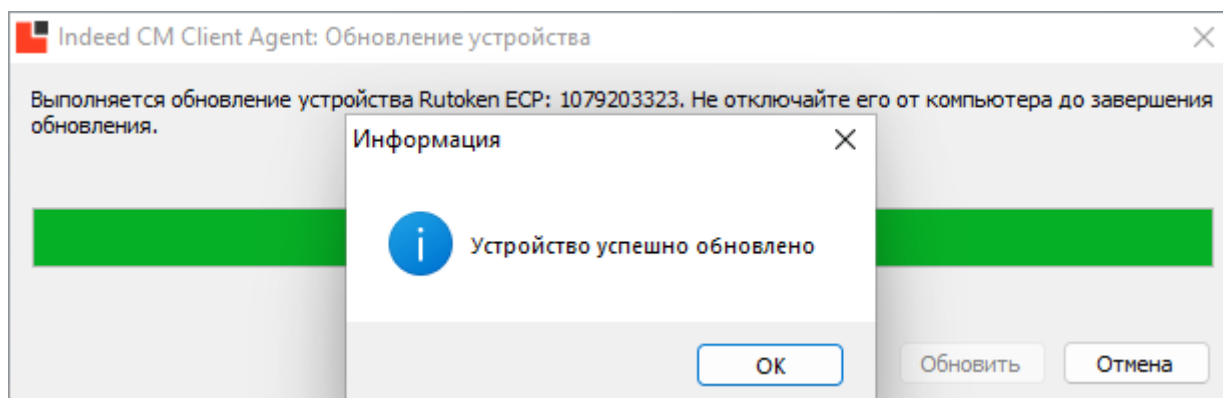
Администратор Indeed Certificate Manager создаст задачу по обновлению содержимого вашего устройства и при подключении его к компьютеру появится форма обновления.



Введите PIN-код и нажмите **Обновить**. После этого начнется процесс обновления содержимого устройства. Обновление может длиться несколько минут. Ход обновления сопровождается графической полосой.



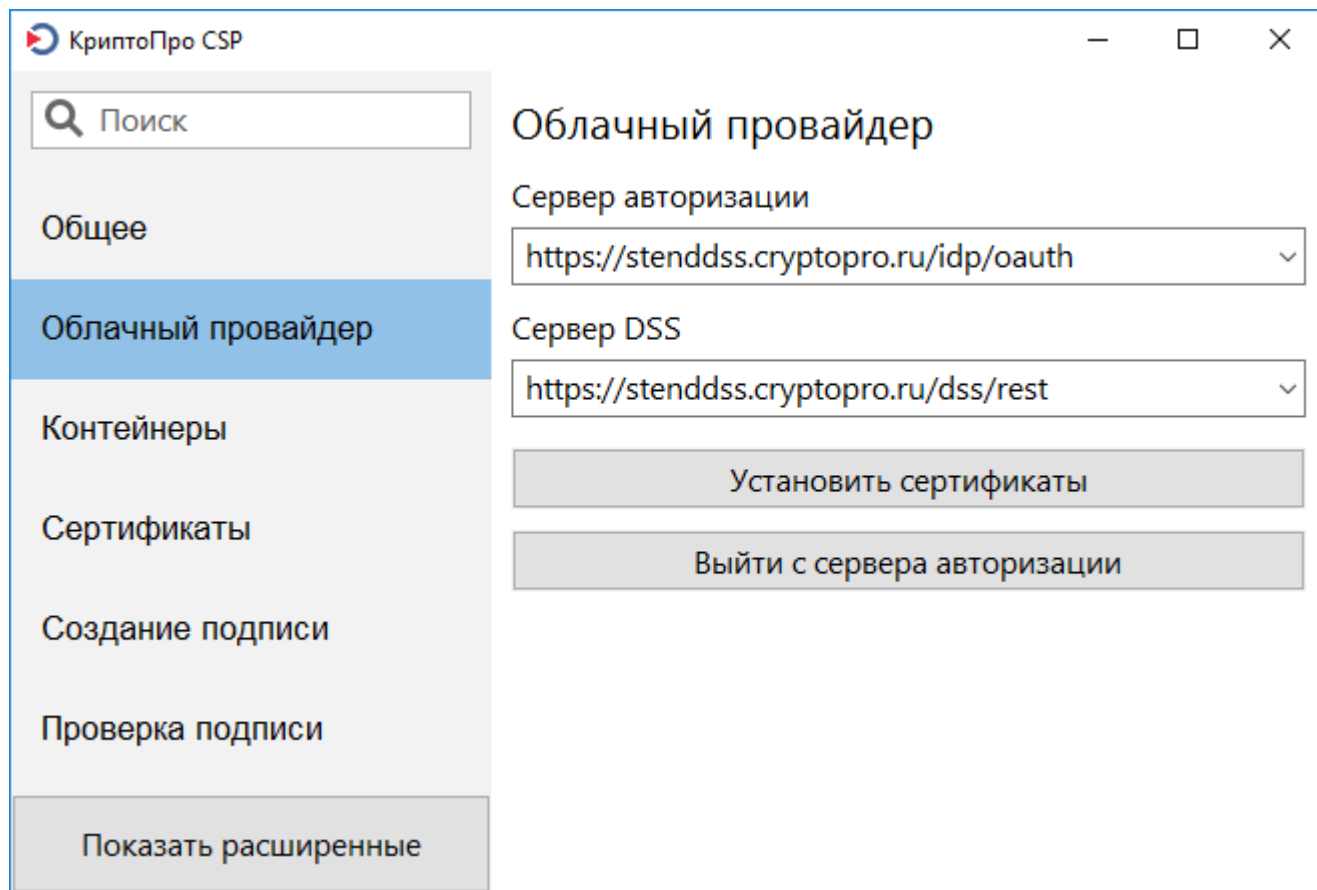
После успешного завершения обновления отобразится соответствующее сообщение.



В случае ошибки обновления её текст появится в информационном сообщении.

Выгрузка сертификата DSS на рабочую станцию пользователя

Для выгрузки сертификата из облачного хранилища запустите компонент **Инструменты КriptoПро** и перейдите в раздел **Облачный провайдер**, укажите URL-адрес для сервера авторизации и сервера DSS.



КriptoПро CSP

Поиск

Облачный провайдер

Сервер авторизации
https://stenddss.cryptopro.ru/idp/oauth

Сервер DSS
https://stenddss.cryptopro.ru/dss/rest

Установить сертификаты

Выйти с сервера авторизации

Нажмите на кнопку **Установить сертификат**, введите логин и пароль от личного кабинета пользователя DSS, и нажмите **Войти**. После успешной установки отобразится сообщение **Установка сертификатов завершилась успехом**.

CryptoPro Web Authentication

КРИПТОПРО

Вход в
SignServer

← Evgeniy Belov

.....

Войти

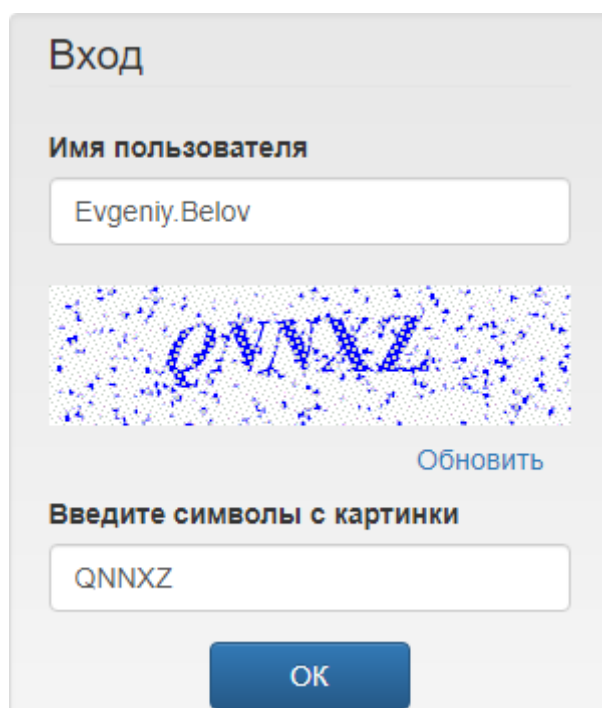
☐ Запомнить пароль

Сервис удаленного самообслуживание (Remote Self Service)

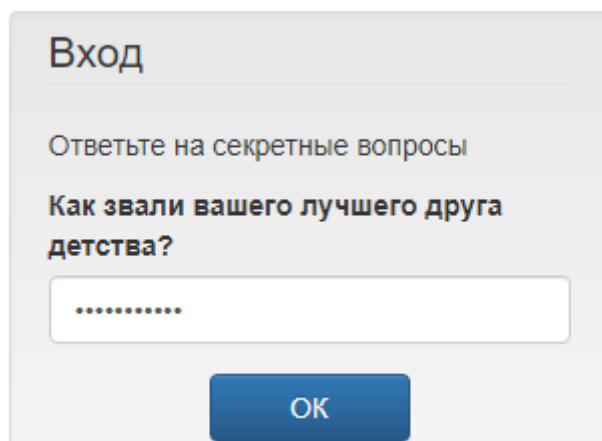
Приложение предназначено для выполнения операций с устройством без подключения его к компьютеру, за исключением случая [разблокировки устройства при помощи утилиты Indeed CM - Unblock](#). Сервис может быть доступен из сети Интернет (из командировки, из дома и т.п.). Аутентификация в приложение осуществляется по секретным вопросам.

Доступ к приложению осуществляется по адресу: <https://<FQDN сервера Indeed CM>/icmremote>

Для входа в Сервис удаленного самообслуживания введите Имя пользователя (логин) и символы с изображения.



Для доступа к карточке пользователя требуется аутентификация по секретным вопросам.



В случае указания верных ответов на секретные вопросы пользователь получает доступ к управлению своими устройствами.



Белов Евгений Александрович

Логин	DEMO\Evgeniy.Belov
E-mail	evgeniy.belov@demo.com
Телефон	+7 (905) 288-58-23

Ваши устройства

▼  **Rutoken ECP, 0894130913**  Evgeniy Belov Выпущено

Временно выключить устройство

Временно выключить устройство, если оно не нужно в течение продолжительного периода времени

Сообщить о том, что устройство неисправно, утеряно или скомпрометировано

Отозвать устройство для предотвращения использования ваших учетных данных

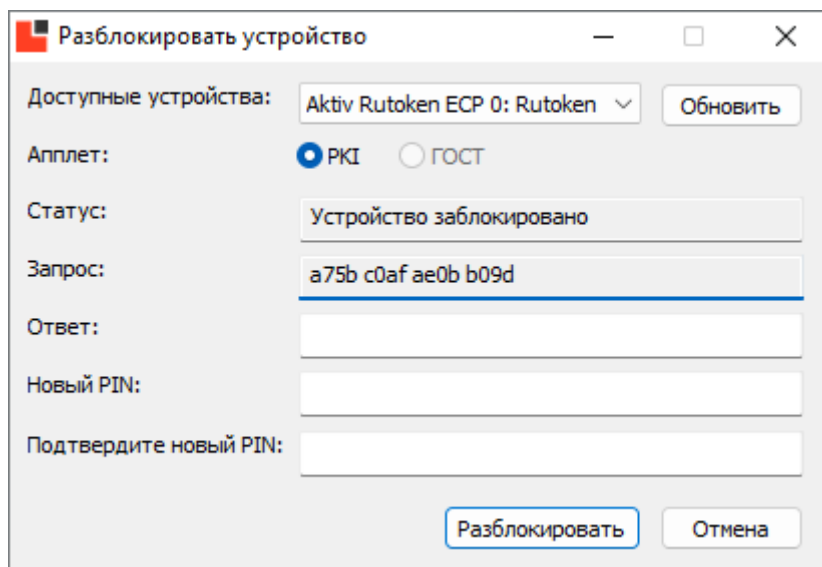
Разблокировать устройство

Получить код для разблокировки устройства

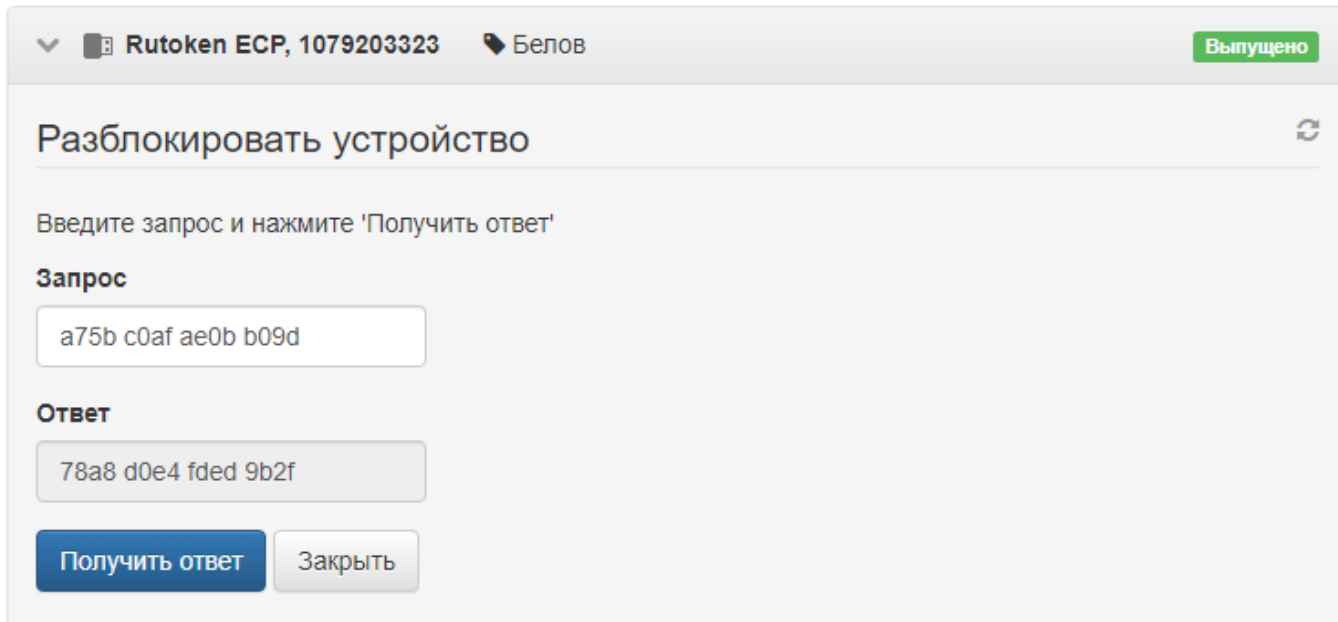
Операции [выключения](#), [включения](#) и [отзыва устройств](#) производятся так же, как и в Сервисе самообслуживания.

Для разблокировки устройства используйте утилиту Indeed CM - Unblock.

1. Запустите утилиту Indeed CM - Unblock (*Пуск – Все программы – Indeed*.
Расположение по умолчанию: %ProrgamFiles%/IndeedCM/IndeedCM.Unblock.exe).
2. Выберите устройство из списка в интерфейсе утилиты и скопируйте код разблокировки из поля **Запрос**.



3. Выберите нужное устройство и нажмите **Разблокировать устройство**, введите код разблокировки устройства из утилиты в поле **Запрос** и нажмите кнопку **Получить ответ**.



4. Введите полученный код ответа в поле **Ответ** утилиты разблокировки, ведите новый PIN-код, его подтверждение и нажмите кнопку **Разблокировать**.

Разблокировать устройство

Доступные устройства:

Aktiv Rutoken ECP 0: Rutoken

Обновить

Апплет:

☒ PKI ☐ ГОСТ

Статус:

Устройство заблокировано

Запрос:

a75b c0af ae0b b09d

Ответ:

78a8 d0e4 fded 9b2f

Новый PIN:

••••••••

Подтвердите новый PIN:

••••••••

Разблокировать

Отмена

Дополнительные инструкции

Indeed CM API

Indeed CM Client Browser Extension

Indeed CM Card Template Designer

- Создание шаблона печати
- Приложение 1

Миграция с Aladdin JaCarta Management System

- Создание политики использования устройств
- Настройка файла конфигурации утилиты миграции
- Работа с утилитой IndeedCM.Migrate.JMS.exe

Миграция с SafeNet Authentication Manager

- Настройка Indeed CM для работы с данными из SAM
 - Создание политик использования устройств
- Настройка утилиты миграции IndeedCM.Migrate.SAM
 - Заполнение файла конфигурации IndeedCM.Migrate.SAM.exe.config
 - Заполнение файла конфигурации unity.config
 - Работа с утилитой IndeedCM.Migrate.SAM

Работа с ключевыми носителями

- Устройства JaCarta
 - Работа с устройствами JaCarta при обновлении Indeed CM на версию 4.2.0 и выше
 - Особенности работы с ГОСТ-областью устройств JaCarta
 - Добавление различных моделей JaCarta
- Добавление различных моделей eToken
- Изменение иконок устройства

Indeed CM API

Назначение

Набор API-функций позволяет управлять устройствами (токенами, смарт-картами) средствами клиентских приложений.

Использование

Доступ к API-функциям реализован через веб-приложение **icmapi**, входящее в состав сервера Indeed Certificate Manager. Для взаимодействия с Indeed CM через API в разделе **Роли** в конфигурации Indeed CM потребуются создать сервисную роль, включить в нее учетную запись, от имени которой будет производиться обращение по API, и определить для роли привилегии:

- Поиск пользователей
- Просмотр репозитория устройств
- Отзыв устройства
- Выключение устройства
- Включение устройства
- Обновление устройства

1. Cards - получить список устройств, добавленных в систему.

Тип запроса:

- GET

Параметры:

- без указания параметров
- offset - сдвиг на указанное количество устройств
- count - количество выводимых устройств
- filter.serialNumber - серийный номер устройства
- filter.cardTypeName - тип устройств
- filter.userName - имя пользователя устройства в формате **Логин** (sAMAccountName) или **UPN** (userPrincipalName)
- filter.comment - комментарий к устройствам
- filter.tags - теги устройств
- filter.state - состояние устройств:
 - Clean - пустое
 - Assigned - назначено
 - Pending - в ожидании
 - Issued - выпущено
 - Disabled - выключено
 - Revoked - отозвано
- filter.contentExpirationStatus - статус истечения содержимого устройства:
 - None - нет истекающих или истекших сертификатов
 - ManagedCertificatesExpiring - управляемые сертификаты истекают
 - ManagedCertificatesExpired - управляемые сертификаты истекли
 - CommonCertificatesExpiring - общие сертификаты истекают
 - CommonCertificatesExpired - общие сертификаты истекли
 - TracedCertificatesExpiring - отслеживаемые сертификаты истекают
 - TracedCertificatesExpired - отслеживаемые сертификаты истекли

Возвращаемые значения (список объектов CardInfo):

- id - идентификатор устройства
- serialNumber - серийный номер устройства
- cardTypeName - тип устройства
- cardModelName - модель устройства (доступна только для устройств [JaCarta](#), [eToken PRO Java 72K](#) и [IDPrime MD](#), если в разделе **Типы устройств** для данных карт добавлено разделение по различным моделям)
- atr - Answer To Reset устройства
- label - метка устройства
- comment - комментарий к устройству
- tags - теги устройства
- state - состояние устройства
- formFactor - форм-фактор устройства
- pacNumber - HID-метка устройства
- expirationDate - срок действия устройства в формате ISO 8601
- timeIssued - время выпуска устройства в формате ISO 8601
- timeDisabled - время выключения устройства в формате ISO 8601
- timeUpdated - время обновления устройства в формате ISO 8601
- timeRevoked - время отзыва устройства в формате ISO 8601

Пример вызова:

`http://localhost/icmapi/Cards` - вывод всех устройств

`http://localhost/icmapi/Cards?offset=0&count=50` - вывод 50 устройств без сдвига

2. Cards/{id}/Revoke - отозвать устройство пользователя.

Тип запроса:

- POST

Параметры:

- id - идентификатор устройства
- reason - причина отзыва устройства:
 - 0 - None
 - 1 - CardBroken
 - 2 - CardLost
 - 3 - CardUpgrade
 - 4 - CardExpired
 - 5 - CardWithdraw
 - 6 - UserRemoved
 - 7 - CardCompromised

Возвращаемые значения:

- нет

Пример вызова:

http://localhost/icmapi/cards/1/revoke

Тело запроса:

- Причина отзыва устройства - например { reason: 5 }

3. Cards/{id}/Disable - временно отключить устройство пользователя.

Тип запроса:

- POST

Параметры:

- id - идентификатор устройства

Возвращаемые значения:

- нет

Пример вызова:

`http://localhost/icmapi/cards/1/disable`

4. Cards/{id}/Enable - включить устройство пользователя.

Тип запроса:

- POST

Параметры:

- id - идентификатор устройства

Возвращаемые значения:

- нет

Пример вызова:

`http://localhost/icmapi/cards/1/enable`

5. Cards/{id}/Preupdate - отозвать неактуальный сертификат пользователя.

 Метод **Preupdate** необходим при изменении политики использования устройств. Если выпущенный сертификат не поддерживается в новой политике и включена опция **Отзывать сертификат при отзыве/выключении устройства** в шаблоне сертификата в старой политике, то он будет отозван.

Метод **Preupdate** нельзя выполнить для выключенного, назначенного, отозванного и ожидающего выпуск или обновление устройства.

Тип запроса:

- POST

Параметры:

- id - идентификатор устройства

Возвращаемые значения:

- ☐ нет

Пример вызова:

`http://localhost/icmapi/cards/1/preupdate`

Indeed CM Client Browser Extension

Назначение

Компонент Client Browser Extension обеспечивает поддержку множественных сессий пользователей на терминальном сервере. При подключении к терминальному серверу для каждого пользователя создается отдельная сессия с сброшенным устройством (смарт-картой, USB-токеном). Без поддержки множественных сессий пользователи будут видеть устройство первого подключившегося пользователя. Компонент входит в состав дистрибутива Indeed Certificate Manager и располагается в каталоге **\IndeedCM\IndeedCM.Client-vX.X.X**

Установка и настройка

1. Выполните вход на терминальный сервер с правами локального администратора.
2. Установите **IndeedCM.Client.Browser.Extension-vX.X.X.msi**.
3. Создайте файл реестра Windows (.reg) со следующим содержимым и сохраните его:

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\IndeedCM\Client\Server]
"MultipleServerMode"=dword:00000001
```

4. Примените значение файла реестра и выполните перезагрузку службы **IndeedCM.Client.Server.Monitor**.
5. [Настройте браузеры](#).

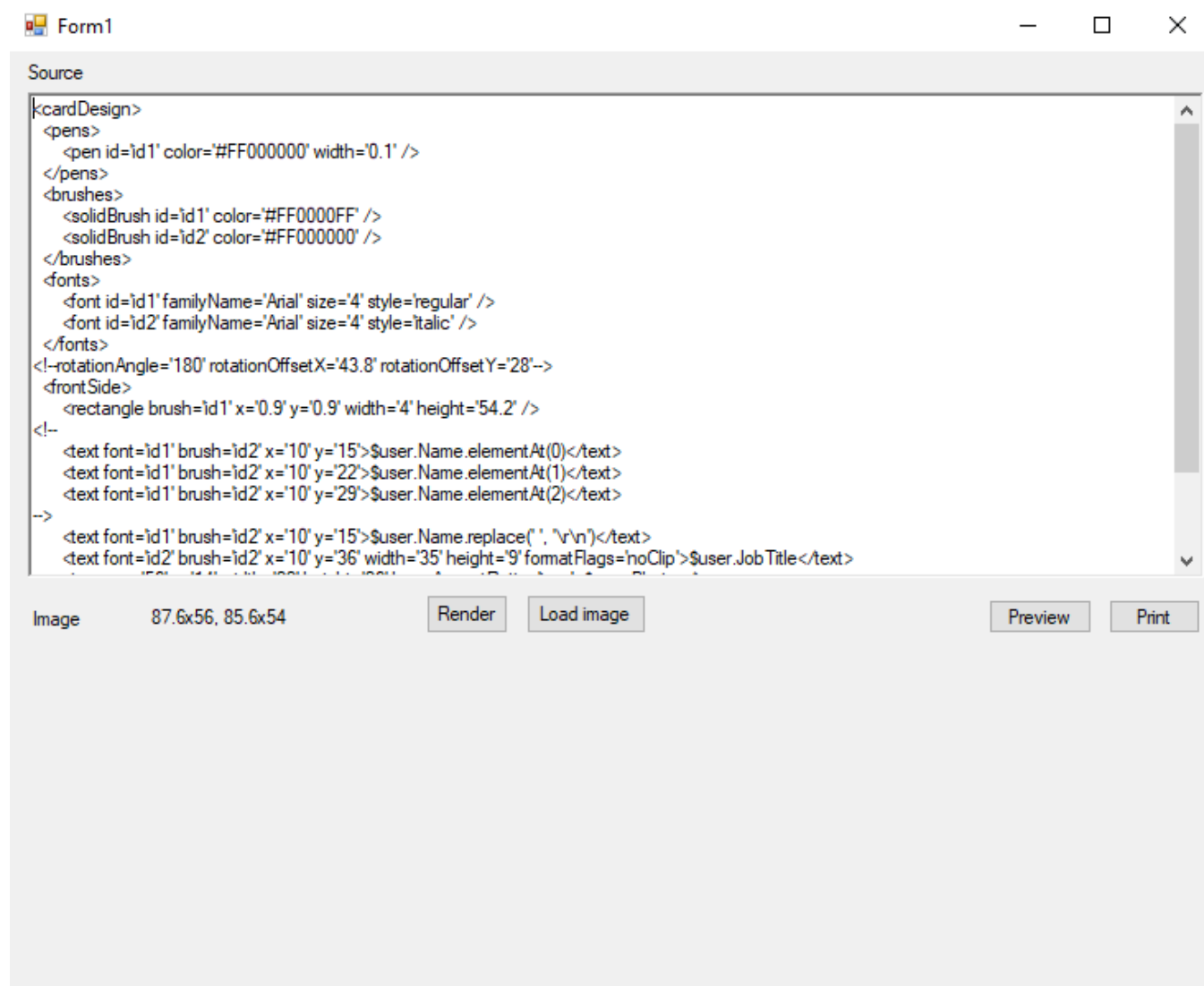
Indeed CM Card Template Designer

Утилита предназначена для создания шаблонов печати на смарт-картах, используемых с принтером **EDIsure XID 8100\8300**. Интеграция Indeed Certificate Manager с принтером позволяет выполнять следующие сценарии:

- выпускать смарт-карты пользователям используя считыватели принтера (контактный и бесконтактный) без печати
- выпускать смарт-карты пользователям используя считыватели принтера (контактный и бесконтактный) с печатью на карте изображения или текста
- печатать на смарт-картах изображение или текст без выпуска карты пользователям

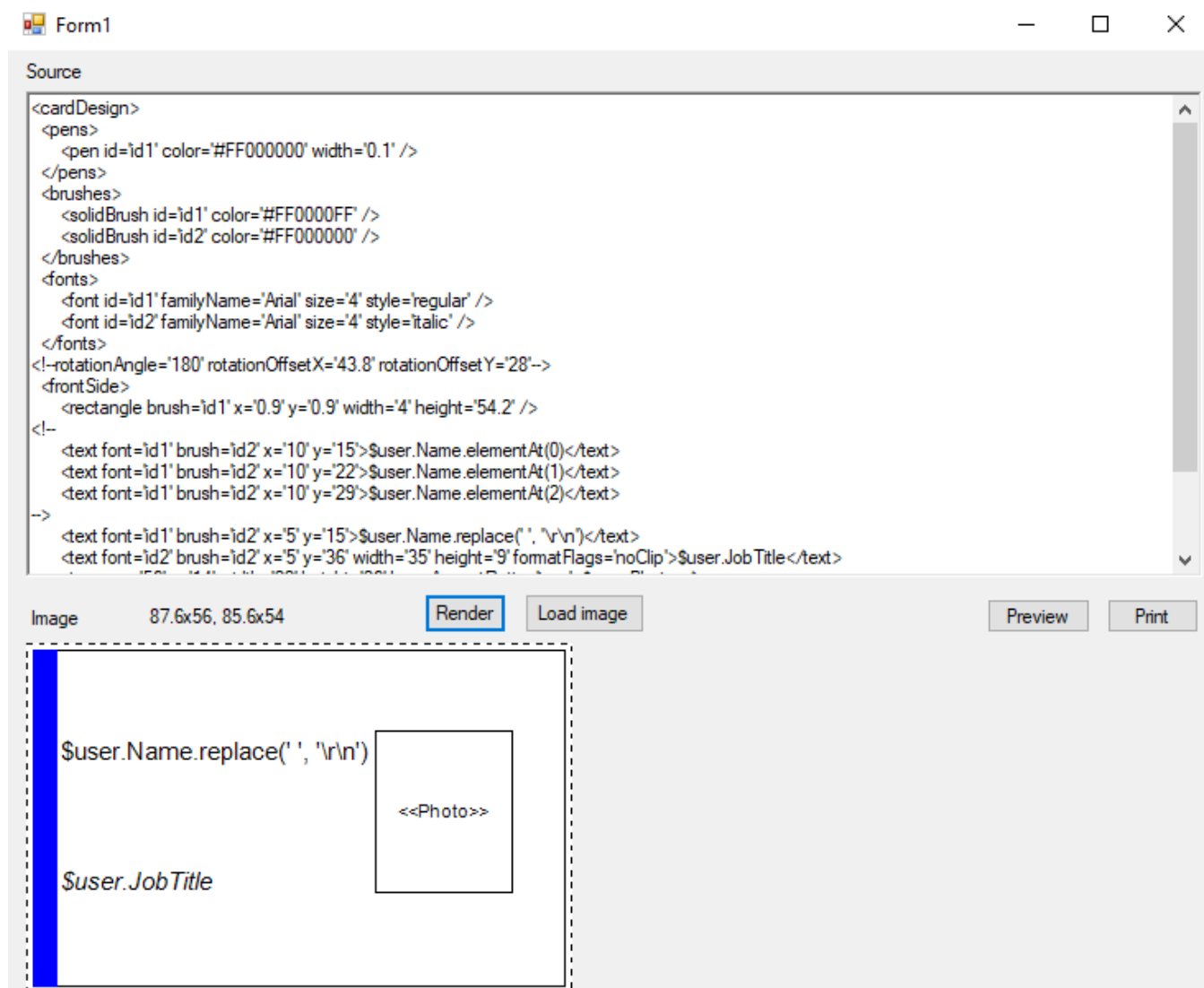
Работа с Card Template Designer

Card Template Designer предоставляется по запросу [службой технической поддержки компании Индид](#). Запустите приложение **cardTemplateDesigner.exe** из дистрибутива. После запуска в окне приложения будет загружен базовый шаблон печати:



Создание шаблона печати

Отредактируйте шаблон в поле **Source**. Для визуализации шаблона нажмите **Render**:



Для создания шаблонов в Card Template Designer используется **Windows GDI + API** в синтаксисе XML. Все содержимое шаблона должно находиться в секции `<cardDesign>... </cardDesign>`.

i Закомментированный текст внутри секций `<!-- ... -->` не учитывается при создании шаблона. Ниже приведены элементы, используемые при создании шаблонов печати.

Отображаемое имя шаблона

Имя шаблона отображается в интерфейсе Indeed CM. Задается в значении параметра **displayName** в секции `<cardDesign>`.

Пример:

```
<cardDesign displayName="Тестовый шаблон" >  
...  
</cardDesign>
```

Перо

Задается в секции **<pens>** с параметрами:

- pen id
- color
- width

Пример:

```
<pens>  
<pen id='id1' color='#FF000000' width='0.1' />  
</pens>
```

Описанная строка определяет цвет линии и толщину. В дальнейшем **pen id** задается как параметр в других секциях. Например, как контур прямоугольника:

```
<rectangle pen='id1' x='0.9' y='0.9' width='4' height='54.2' />
```



Для задания цвета используйте шестнадцатичное значение и степень прозрачности. Например, **#FFA52A2A**, где **FF** – полная непрозрачность коричневого цвета **A52A2A** . Таблицы цветов и прозрачности приведены в [Приложении 1](#).

Кисть

Задается в секции **<brushes>** с параметрами:

- brush id
- color

Пример:

```
<brushes>
<brush id='id1' color='#FF0000FF' />
</brushes>
```

В дальнейшем **brush id** задается как параметр в других секциях. Например, как цвет прямоугольника:

```
<rectangle brush='id1' x='0.9' y='0.9' width='4' height='54.2' />
```

Шрифт

Задается в секции **** с параметрами:

- font id
- familyName
- size
- style: regular, bold, italic, underline, strikeout

Пример:

```
<fonts>
<font id='id1' familyName='Arial' size='3' style='regular' />
<font id='id2' familyName='Arial' size='4' style='italic' />
</fonts>
```

Описанная структура определяет id, название, размер и начертание шрифтов. В дальнейшем **font id** задается как параметр в других секциях. Например, в секции **<text>**:

```
<text font='id1' brush='id2' x='10' y='15'>$user.Name.elementAt(0)</text>
<text font='id2' brush='id2' x='10' y='36'>$user.JobTitle</text>
```

Текст

Задается в составе секции **<text>** с параметрами:

- font
- brush
- x
- y
- width (опциональный)
- height (опциональный)
- horizontalAlignment: left, right, center (опциональный)
- verticalAlignment: top, bottom, center (опциональный)
- formatFlags (см. [подробное описание значений](#))
 - directionRightToLeft
 - directionVertical
 - displayFormatControl
 - fitBlackBox
 - lineLimit
 - measureTrailingSpaces
 - noClip
 - noFontFallback
 - noWrap

Пример:

```
<text font='id2' brush='id2' x='10' y='36' width='35' height='9'
formatFlags='noClip'>$user.JobTitle</text>
```

Описанная строка определяет шрифт, цвет, положение, размер и формат вывода должности пользователя, подставляемой из Active Directory.

Атрибуты пользователя Active Directory выводимые на печать

Данные пользователя (ФИО, должность, подразделение и т.д.) подставляются в шаблон из атрибутов Active Directory. Ниже приведен синтаксис для подстановки значений наиболее часто используемых атрибутов:

- \$user.Name
- \$user.LogonName
- \$user.PrincipalName
- \$user.FirstName
- \$user.LastName
- \$user.Email
- \$user.TelephoneNumber
- \$user.Country
- \$user.State
- \$user.Locality
- \$user.Organization
- \$user.OrgUnit
- \$user.Street
- \$user.JobTitle

Для печати данных из произвольного атрибута используйте синтаксис: `$user.attribute('имя атрибута Active Directory')`

Пример:

```
$user.attribute('Notes')
```

Перенос строк

Для переноса текста по строкам (например, разбивки ФИО пользователя, подставленного из Active Directory на несколько строк) можно использовать параметры **replace** (замена символа) или **elementAt** (извлечение элемента из строки).

Пример 1:

Фамилия, имя и отчество пользователя подставляются из атрибута Active Directory и пишутся в одну строку в шаблоне через пробелы:

```
<text font='id1' brush='id2' x='10' y='15'>$user.Name</text>
```

Пример 2:

Фамилия, имя и отчество пользователя подставляются из атрибута Active Directory, пробелы заменяются на перевод строки (`\r` – переход к началу строки, `\n` – переход на новую строку). В результате в шаблоне ФИО разбивается на три строки:

```
<text font='id1' brush='id2' x='10' y='15'>$user.Name.replace(",\r\n")</text>
```

Аналогичным образом может быть перенесено на несколько строк значение должности или подразделения пользователя. Вместо пробела `" "` может быть любой другой символ.

Для переноса извлеченного из Active Directory значения ФИО по строкам, без замены текста применяется **elementAt**. ФИО пользователя можно вывести в шаблоне построчно следующим образом:

```
<text font='id1' brush='id2' x='10' y='15'>$user.Name.elementAt(0)</text>  
<text font='id1' brush='id2' x='10' y='22'>$user.Name.elementAt(1)</text>  
<text font='id1' brush='id2' x='10' y='29'>$user.Name.elementAt(2)</text>
```

где:

- 0 – первое слово (например, Имя)
- 1 – второе слово (например, Фамилия)
- 2 – третье слово (например, Отчество)

Изображение

Задается в секции **<image>** с параметрами:

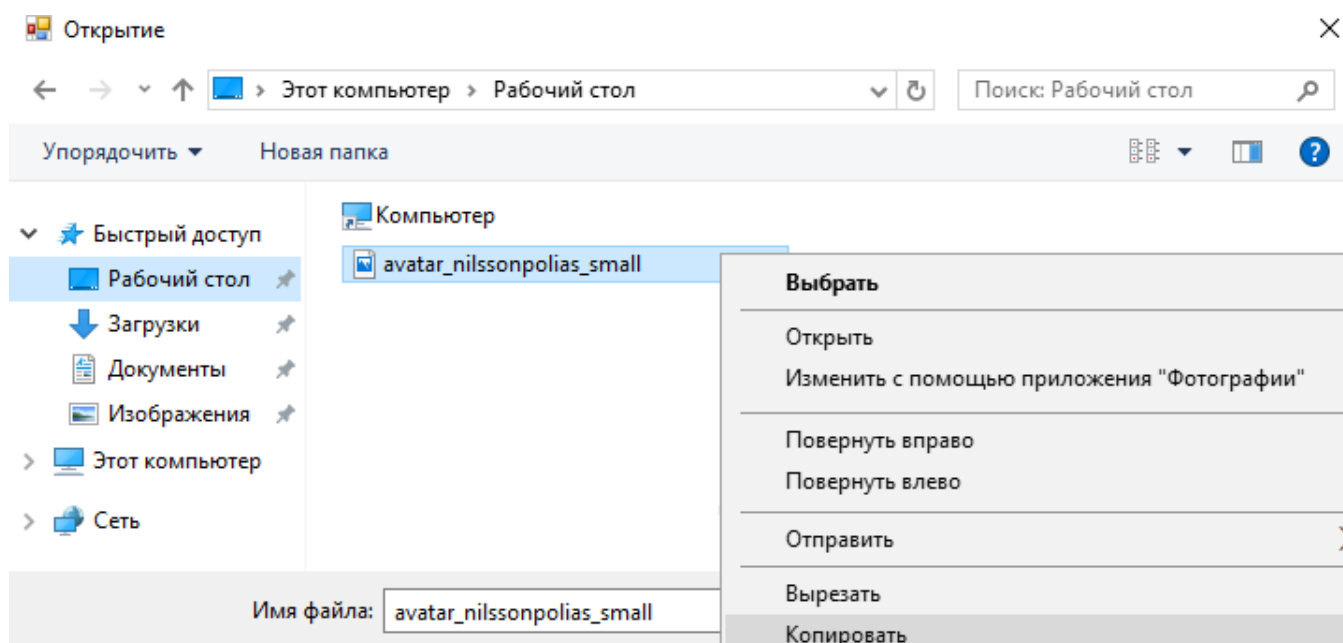
- x
- y
- width (опциональный)
- height (опциональный)
- keepAspectRatio (true или false)
- data (опциональный)

Пример:

```
<image x='56' y='14' width='22' height='26'  
keepAspectRatio='true'>$user.Photo</image>
```

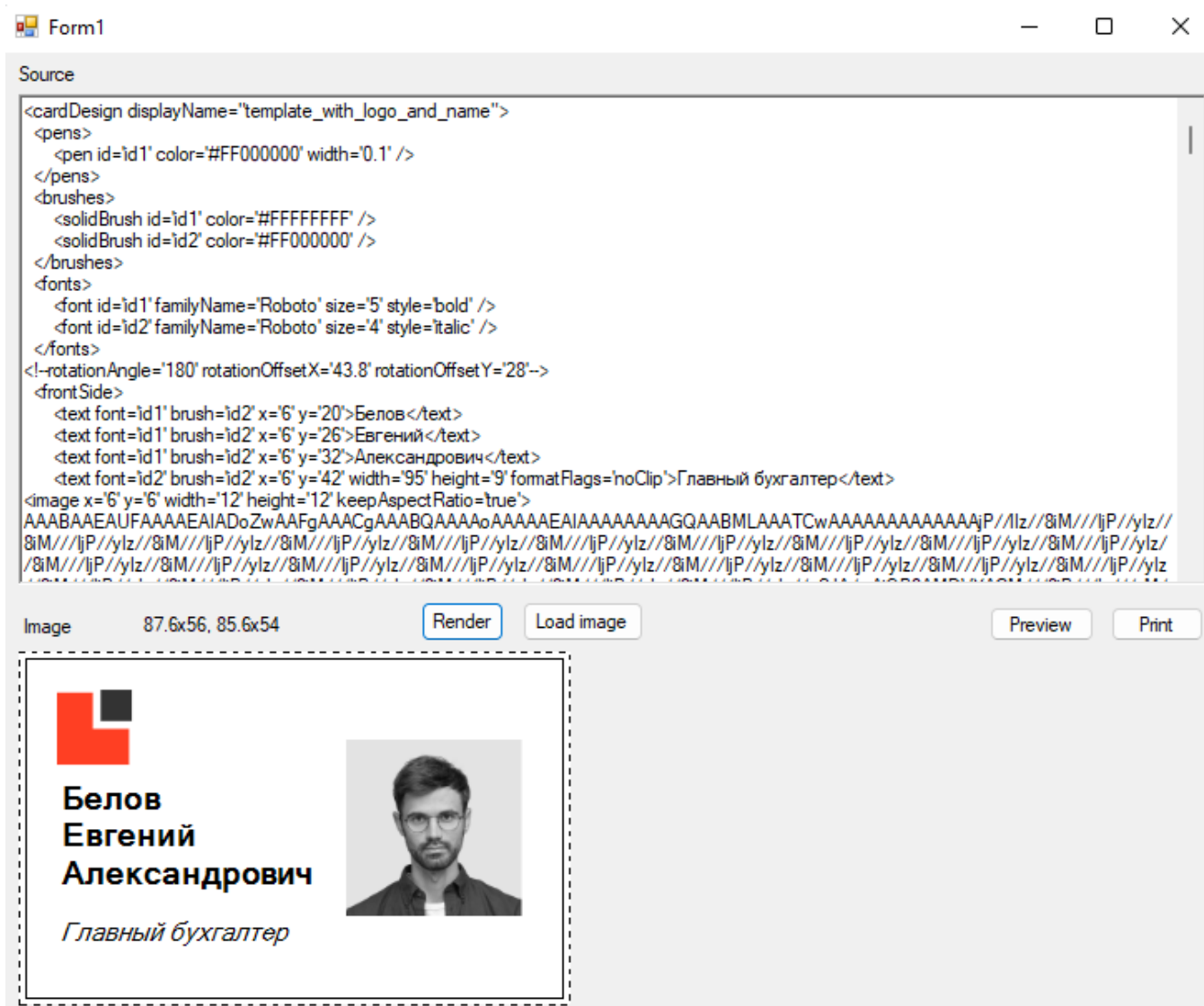
Описанная строка определяет положение, размер и следование пропорциям изображения, подставляемого из атрибута Active Directory (переменная **\$user.Photo**). Помимо переменной можно подставить и изображение в кодировке base64 (например, для добавления в шаблон логотипа компании) и затем визуализировать его выполнив следующие действия:

1. Нажмите **Load image** и перейдите в окно выбора изображения в формате JPEG. Размер изображения подбирается исходя из желаемого дизайна шаблона и размеров смарт-карты.
2. Кликните правой кнопкой мыши на изображении и нажмите **Копировать**.
3. Выберите изображение и нажмите **Открыть**.
4. В секции **<image>** удалите **\$user.Photo** и нажмите **Вставить**.
5. Нажмите **Render** для визуализации.



Ниже на рисунке приведен пример шаблона со статическим логотипом компании и подстановкой данных пользователя из Active Directory:

- Фамилии, имени и отчества с разбивкой по строкам, написанных жирным шрифтом
- Фотографии
- Должности, написанной курсивом



Прямоугольник

Задается в секции **<rectangle>** с параметрами:

- pen (опциональный)
- brush (опциональный)
- x
- y
- width (опциональный)
- height (опциональный)

Сторона карты

Сторона карты задается в секциях **<frontSide>** (передняя) и **<backSide>** (задняя). Внутри секции располагаются элементы, определяющие то, что должно быть напечатано на стороне (rectangle, text, image и т.д.).

Вращение

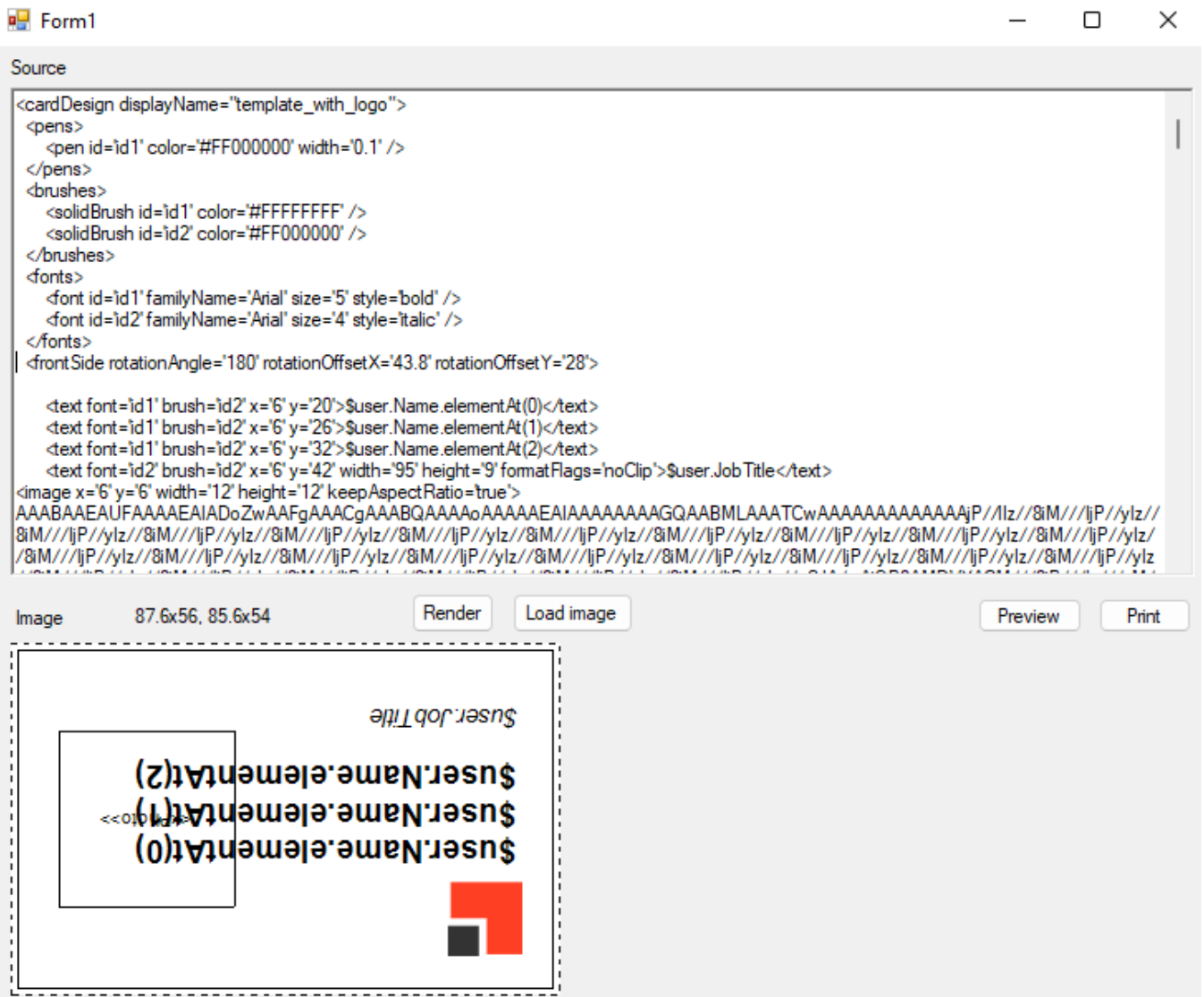
Содержимое стороны карты может быть развернуто при необходимости. Для разворота в секции стороны карты используйте параметры:

- rotationAngle
- rotationOffsetX
- rotationOffsetY

Пример:

```
<frontSide rotationAngle='180' rotationOffsetX='43.8' rotationOffsetY='28'>  
...  
</frontSide>
```

Ниже на рисунке приведен пример перевернутого на 180 градусов шаблона со статическим логотипом компании и подстановкой данных пользователя из Active Directory.



Приложение 1

HEX-коды цветов для использования при создании шаблона печати:

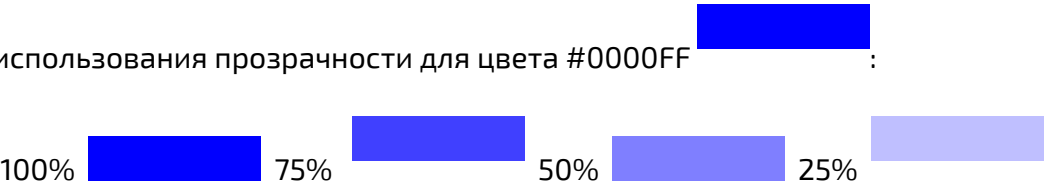
#F0F8FF		#2F4F4F		#20B2AA		#FFDAB9	
#FAEBD7		#00CED1		#87CEFA		#CD853F	
#00FFFF		#9400D3		#778899		#FFC0CB	
#7FFFD4		#FF1493		#B0C4DE		#DDA0DD	
#F0FFFF		#00BFFF		#FFFFFFE0		#B0E0E6	
#F5F5DC		#696969		#00FF00		#800080	
#FFE4C4		#1E90FF		#32CD32		#FF0000	
#000000		#B22222		#FAF0E6		#BC8F8F	
#FFEBCD		#FFFAF0		#FF00FF		#4169E1	
#0000FF		#228B22		#800000		#8B4513	
#8A2BE2		#FF00FF		#66CDAA		#FA8072	
#A52A2A		#DCDCDC		#0000CD		#F4A460	
#DEB887		#F8F8FF		#BA55D3		#2E8B57	
#5F9EA0		#FFD700		#9370DB		#FFF5EE	
#7FFF00		#DAA520		#3CB371		#A0522D	
#D2691E		#808080		#7B68EE		#C0C0C0	
#FF7F50		#008000		#00FA9A		#87CEEB	
#6495ED		#ADFF2F		#48D1CC		#6A5ACD	
#FFF8DC		#F0FFF0		#C71585		#708090	
#DC143C		#FF69B4		#191970		#FFFAFA	
#00FFFF		#CD5C5C		#F5FFFA		#00FF7F	
#00008B		#4B0082		#FFE4E1		#4682B4	
#008B8B		#FFFFFF0		#FFE4B5		#D2B48C	
#B8860B		#F0E68C		#FFDEAD		#008080	
#A9A9A9		#E6E6FA		#000080		#D8BFD8	
#006400		#FFF0F5		#FDF5E6		#FF6347	
#BDB76B		#7CFC00		#808000		#40E0D0	
#8B008B		#FFFACD		#6B8E23		#EE82EE	
#556B2F		#ADD8E6		#FFA500		#F5DEB3	
#FF8C00		#F08080		#FF4500		#FFFFFF	
#9932CC		#E0FFFF		#DA70D6		#F5F5F5	
#8B0000		#FAFAD2		#EEE8AA		#FFFF00	
#E9967A		#90EE90		#98FB98		#9ACD32	
#8FBC8F		#D3D3D3		#AFEEEE		#FFEFDD	
#483D8B		#FFB6C1		#DB7093		#FFA07A	

В Таблице 1 приведены HEX-коды процентного соотношения прозрачности. Где 100% – абсолютно непрозрачный цвет, 0% – абсолютно прозрачный.

Таблица 1 – HEX-коды для настройки прозрачности цветов.

100%	FF
95%	F2
90%	E6
85%	D9
80%	CC
75%	BF
70%	B3
65%	A6
60%	99
55%	8C
50%	80
45%	73
40%	66
35%	59
30%	4D
25%	40
20%	33
15%	26
10%	1A
5%	0D
0%	00

Пример использования прозрачности для цвета #0000FF  :



Миграция с Aladdin JaCarta Management System

Руководство описывает процедуру миграции данных (устройств и сертификатов Microsoft CA) из Aladdin JaCarta Management System (JMS) в Indeed Certificate Manager.

Миграция данных не изменяет базу JMS, состояние и содержимое устройств после переноса не изменится. Для перенесенных устройств и сертификатов в Indeed CM доступен полный набор действий (выпуск, отзыв, обновление содержимого и т.д.).

Утилита миграции переносит в Indeed CM данные устройств:

- Модель
- Форм фактор
- Состояние
- Метка
- PIN-код администратора
- Ключевая информация для JMS-коннектора MS PKI (9C66741E-E5B1-40E3-B047-9A2D598CA913)
 - Выпущенные на УЦ
 - Отслеживаемые (выпущены на стороннем УЦ)
- Связь с пользователем



Для JaCarta PKI/ГОСТ информация о ГОСТ-апплете не импортируется (в Indeed CM будут возможны операции только с PKI-областью устройства).



Не поддерживается перенос в Indeed CM сведений о:

- метках АМДЗ Аккорд
- сертификатах УЦ Валидата
- сертификатах УЦ КриптоПро

Если такие данные имеются на устройстве, то они не будут отображаться в Indeed CM после переноса, но остаются на устройстве.

Предварительные условия

Миграция данных возможна при соблюдении условий:

- С сервера JMS, на котором выполняется запуск утилиты миграции, есть сетевой доступ к серверу с базой данных Indeed CM.
- Каталог пользователей Indeed CM совпадает с каталогом пользователей JMS. Путь к каталогу пользователей задается в разделе **Каталог пользователей** > [Active Directory](#) Мастера настройки Indeed CM.
- В разделе **Конфигурация** > [Типы устройств](#) Indeed CM добавлены все типы устройств jaCarta, которые используются в JMS.
- В Indeed CM доступно достаточное количество свободных лицензий: в разделе **Конфигурация** > [Лицензии](#) есть действующая лицензия на достаточное количество пользователей.
- Для всех пользователей, устройства которых будут переноситься из JMS, должны быть [назначены политики использования устройств в Indeed CM](#).
- В политиках Indeed CM настроены те же УЦ и те же шаблоны сертификатов, что и в JMS.

Процедура миграции

Миграция данных осуществляется в несколько этапов:

- [Настройка файла конфигурации утилиты миграции](#)
- [Запуск утилиты миграции](#)

Создание политики использования устройств

Indeed Certificate Manager использует механизм политик выпуска устройств пользователям. Каждая политика содержит в себе параметры работы с устройством: перечень УЦ и шаблонов сертификатов, требования к установке PIN-кодов, перечень действий с устройством доступных пользователю и т.д. Каждая политика имеет свою область действия. Для каталога пользователей Indeed CM в Active Directory это:

- **Домен** (Domain)
- **Контейнер** (Container)
- **Подразделение** (Organizational Unit)

Всем пользователям, расположенным в объекте действия политики будут выпускаться устройства с определенными в политике параметрами. Действие политики может распространяться как на весь объект (домен, контейнер или подразделение), так и на отдельные группы пользователей, входящие в него. Если пользователь попадает под область действия нескольких политик выпуска устройств (например, состоит в двух группах, расположенных в одном OU), то действовать на пользователя будет политика с большим приоритетом.

Перед миграцией данных из JMS необходимо заранее создать одну или несколько политик использования устройств в Indeed CM (см. **Добавление и редактирование политик использования устройств**).

 Такая политика должна обязательно содержать те же самые УЦ и шаблоны, которые использовались для выпуска сертификатов в JMS.

В результате миграции данных из JMS все пользователи, обладающие токенами и сертификатами, попадут под действие ранее созданных политик Indeed CM.

Настройка файла конфигурации утилиты миграции

Для работы утилиты заполните файл конфигурации **IndeedCM.Migrate.JMS.exe.config**, находящийся в каталоге с утилитой.

Заполните секции:

- **<migrateJMSSettings>**:

operatorTokenPin - PIN-код администратора устройства, на котором записан сертификат оператора JMS. Необходим для монтирования криптохранилища JMS.

notIssuedTokenAdminPin - если ключевой носитель в JMS находится в состоянии "зарегистрирован" и ни разу не выпускался, то в этом параметре задается PIN-код администратора, который будет установлен на устройстве после переноса его в Indeed CM.

issuedTokenAdminPin - если ключевой носитель в JMS находится любом другом состоянии и выпускался без инициализации, то в параметре задается PIN-код администратора, который будет установлен на устройстве после переноса его в Indeed CM.

- **<sqlPersistenceSettings>**: параметры подключения к базе данных Indeed CM. Всю секцию можно перенести из файла конфигурации **Web.config** веб-приложения **icm**.
- **<adUserCatalogSettings>**: параметры подключения к каталогу пользователей в Active Directory. Всю секцию можно перенести из файла конфигурации **Web.config** веб-приложения **icm**.



Секции **sqlPersistenceSettings** и **adUserCatalogSettings** должны быть в расшифрованном виде. Для расшифровки секций используйте файл **decryptConfigsSQL_AKEAgent.bat** из дистрибутива сервера Indeed CM каталог **..\Misc\EncryptConfigs**. Запустите файл на сервере Indeed CM в командной строке, запущенной от имени администратора и дождитесь завершения расшифровки.

Для шифрования используйте файл **encryptConfigsSQL_AKEAgent.bat**.

Работа с утилитой IndeedCM.Migrate.JMS.exe

Запустите утилиту **IndeedCM.Migrate.JMS.exe** на сервере JMS в командной строке, запущенной от имени администратора.

Для работы с резервной копией базы данных JMS необходимо прописать в реестре сервера JMS путь к копии “боевой” базы.

По умолчанию строка подключения к базе хранится в значении параметра **ConnectionString** в разделе:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\Enterprise Application Platform Server\JaCarta Management System\default\DatabaseManager]
```

Миграция с SafeNet Authentication Manager

Руководство описывает процедуру миграции данных (устройств и сертификатов) из системы SafeNet Authentication Manager (SAM) в Indeed Certificate Manager.

Предварительные условия

Миграция данных возможна при соблюдении условий:

Со стороны SAM:

- Версия SafeNet Authentication Manager 8.0, 8.2 Rev E и 9.0 SP2/SP3
- Хранилище данных SAM в Active Directory
- Редакция удостоверяющего центра Microsoft, сертификаты которого будут перенесены
- Известны все типы устройств (USB-токенов, смарт-карт) и значения их ATR (Answer To Reset), которые используются в SAM и будут использоваться в Indeed CM.

Со стороны Indeed Certificate Manager:

- Версия Indeed CM Server 4.1.3 и выше
- Хранилище данных в Active Directory или Microsoft SQL

Процедура миграции

Миграция данных осуществляется в несколько этапов:

- [Настройка Indeed CM для работы с данными из SAM](#)
 - [Создание политик использования устройств](#)
- [Настройка утилиты миграции IndeedCM.Migrate.SAM](#)
 - [Заполнение файла конфигурации IndeedCM.Migrate.SAM.exe.config](#)
 - [Заполнение файла конфигурации unity.config](#)
 - [Работа с утилитой IndeedCM.Migrate.SAM](#)

Настройка Indeed CM для работы с данными из SAM

Прежде, чем приступать к выгрузке данных из SAM необходимо подготовить Indeed Certificate Manager к приему этих данных. Выполните следующие действия:

1. Убедитесь в том, что каталог пользователей Indeed CM совпадает с каталогом пользователей SAM. Путь к каталогу пользователей задается в разделе **Каталог пользователей** > **Active Directory** Мастера настройки Indeed CM.
2. Убедитесь в том, что в разделе **Конфигурация** > **Лицензии** есть действующая лицензия на достаточное количество пользователей.
3. Убедитесь в том, что в разделе **Конфигурация** > **Типы устройств** добавлены все типы устройств eToken, которые используются в SAM.
4. Для всех пользователей, устройства которых будут переноситься из SAM, должны быть **созданы и назначены политики использования устройств в Indeed CM**.

Создание политик использования устройств

Indeed Certificate Manager использует механизм политик выпуска устройств пользователям. Каждая политика содержит в себе параметры работы с устройством: перечень УЦ и шаблонов сертификатов, требования к установке PIN-кодов, перечень действий с устройством доступных пользователю и т.д. Каждая политика имеет свою область действия. Для каталога пользователей Indeed CM в Active Directory это:

- **Домен** (Domain)
- **Контейнер** (Container)
- **Подразделение** (Organizational Unit)

Всем пользователям, расположенным в объекте действия политики будут выпускаться устройства с определенными в политике параметрами. Действие политики может распространяться как на весь объект (домен, контейнер или подразделение), так и на отдельные группы пользователей, входящие в него. Если пользователь попадает под область действия нескольких политик выпуска устройств (например, состоит в двух группах, расположенных в одном OU), то действовать на пользователя будет политика с большим приоритетом.

Перед миграцией данных из SAM необходимо заранее создать одну или несколько политик использования устройств в Indeed CM (см. **Добавление и редактирование политик использования устройств**).

 Такая политика должна обязательно содержать те же самые УЦ и шаблоны, которые использовались для выпуска сертификатов в SAM.

В результате миграции данных из SAM все пользователи, обладающие токенами и сертификатами, попадут под действие ранее созданных политик Indeed CM.

Настройка утилиты миграции IndeedCM.Migrate.SAM

Перенос данных из SAM осуществляется при помощи утилиты [IndeedCM.Migrate.SAM.exe](#), расположенной в дистрибутиве сервера Indeed Certificate Manager (каталог Misc\SAMMigration). Для работы утилиты необходимо заполнить файлы конфигурации:

- [Заполнение файла конфигурации IndeedCM.Migrate.SAM.exe.config](#)
- [Заполнение файла конфигурации unity.config](#)
- [Работа с утилитой IndeedCM.Migrate.SAM](#)

Заполнение файла конфигурации IndeedCM.Migrate.SAM.exe.config

Откройте файл ...SAMMigration\IndeedCM.Migrate.SAM.exe.config от имени администратора в текстовом редакторе (например, в Блокнот) и заполните следующие секции:

- **samSettings** – параметры подключения к хранилищу данных SAM

– **MsCAConnectorId** – идентификатор коннектора к Microsoft CA. Значение параметра можно найти в xml-файле коннектора в каталоге SAM. Значение по умолчанию: {1A30B883-CD69-4cbb-8D61-E72E9697D8B1}.



Путь по умолчанию C:\Program

Files\SafeNet\Authentication\SAM\x64\Bin\MsCAConnectorDescriptor.xml

– **connectionString** - путь к файлу xml (в названии файла имя домена, в котором развернут SAM) с информацией для подключения к SAM серверу.



По умолчанию располагается по пути C:

\ProgramData\SafeNet\Authentication\SAM\

- **migrateSAMSettings** – параметры переноса данных

– **ignoreCMCertificateTemplateNotFoundError** – параметр импорта устройств.

Может иметь два значения:

true – из SAM импортируется устройство и только те сертификаты, находящиеся на нём, для которых в политике Indeed CM создан шаблон.

false – из SAM не импортируется устройство, если в политике Indeed CM нет хотя бы одного шаблона для сертификата, выпущенного в SAM.

При этом процесс импорта карт не останавливается ни в одном из случаев.

Атрибут не обязательный, значение по умолчанию: "false"

– **notIssuedTokenAdminPin** - если ключевой носитель в SAM находится в состоянии "зарегистрирован" и ни разу не выпускался, то в этом параметре задается PIN-код администратора, который будет установлен на устройстве после переноса его в Indeed CM.

– **issuedTokenAdminPin** – если ключевой носитель в SAM находится любом другом состоянии и выпускался без инициализации, то в параметре задается PIN-код администратора, который будет установлен на устройстве после переноса его в Indeed CM.

– **tokenTypes** – секция, в которой должны быть перечислены все устройства, которые необходимо перенести из SAM в Indeed CM. Необходимо указать модель устройства (токена, смарт-карты), product name, цвет устройства и значение ATR (Answer To Reset).

 Значение ATR для каждого устройства можно получить у производителя или при помощи стороннего ПО, обратившись в [службу технической поддержки Indeed-Id](#).

Если при работе утилиты **IndeedCM.Migrate.SAM.exe** с хранилищем SAM встречается устройство с моделью и product name, которые не указаны в секции **tokenTypes**, то такие устройства не будут перенесены в хранилище Indeed CM, а утилита выведет соответствующую ошибку.

- **adPersistenceSettings** – параметры подключения к хранилищу данных Indeed CM, расположенному в Active Directory. Содержимое секции должно полностью совпадать с содержимым одноименной секции файла конфигурации **Консоли управления Indeed CM** (icm\Web.config).
- **sqlPersistenceSettings** – параметры подключения к хранилищу данных Indeed CM в среде Microsoft SQL. По умолчанию секция закомментирована символами: `<!-- ... -->`. Содержимое секции должно полностью совпадать с содержимым одноименной секции файла конфигурации **Консоли управления Indeed CM** (icm\Web.config).
- **adUserCatalogSettings** – параметры подключения к каталогу пользователей Indeed CM, расположенному в Active Directory. Содержимое секции должно полностью совпадать с содержимым одноименной секции файла конфигурации **Консоли управления Indeed CM** (icm\Web.config).

Сохраните внесенные изменения.

Пример заполненных секций файла **IndeedCM.Migrate.SAM.exe.config** приведен ниже. В примере SAM развернут в домене **demo.local**, хранилище SAM, Indeed CM и каталог пользователей в Active Directory.

Пример заполненных секций:

```
<samSettings MsCAConnectorId="{1A30B883-CD69-4cbb-8D61-E72E9697D8B1}"
connectionString="C:\ProgramData\SafeNet\Authentication\SAM\demo.local.xml" />
<migrateSAMSettings ignoreCMCertificateTemplateNotFound="true"
notIssuedTokenAdminPin="adminpass"
issuedTokenAdminPin="adminpass2">
<tokenTypes>
<tokenType model="Token 12.0.0.0 12.0.12"
productName="SafeNet eToken 5110"
color="8"
atr="3bd5180081313a7d8073c8211030" />
<tokenType model="Token JC"
productName="eToken PRO Java 72K 05755"
color="4"
atr="3bd518008131fe7d8073c82110f4" />
</migrateSAMSettings>
<adPersistenceSettings path="LDAP://CN=Indeed CM,CN=Indeed Identity,
DC=demo,DC=local" userName="DEMO\cmadmin" password="Password1"
cryptoAlgName="AES"
cryptoKey="11d2f5051684451860ad177ebc39b55cacaf2a0a843b05ddf273b955c93ae015" />
<adUserCatalogSettings>
<rootContainers>
<container path="LDAP://OU=SAM_USERS,DC=demo,DC=local" userName="DEMO\cmadmin"
password="Password1" />
</rootContainers>
</adUserCatalogSettings>
```

Заполнение файла конфигурации unity.config

Откройте файл `...SAMMigration\unity.config` от имени администратора в текстовом редакторе (например, в Блокнот) и заполните секцию **container**:

- Все строки до `<register type="ISAMDbContext"... />` должны совпадать с теми, что указаны в файле конфигурации **Консоли управления Indeed CM** (`icm\unity.config`).

 Добавлять секции, которых по умолчанию нет в `unity.config` утилиты миграции (но есть в `icm\unity.config`) не нужно.

- `register type="IMigrateReporter" mapTo="IndeedCM.Migrate.SAM.Reporter.CSVMigrateReporter, IndeedCM.Migrate.SAM"/>` – определяет режим вывода отчета по работе утилиты миграции.

Если секция не закомментирована символами `<!-- ... -->`, то отчет будет записываться в csv-файл, созданный в папке расположения утилиты с именем **IndeedCM.Migrate.SAM.Report_dd-MM-yyyy_HH-mm-ss.csv**. По умолчанию отчет не будет создаваться.

- `<register type="IMigrateReporter" mapTo="IndeedCM.Migrate.SAM.Reporter.NullMigrateReporter, IndeedCM.Migrate.SAM"/>` – отключает создание отчета о работе утилиты миграции данных. По умолчанию секция закомментирована символами `<!-- ... -->`.

 Использование двух активных секций с параметрами `IndeedCM.Migrate.SAM.Reporter.CSVMigrateReporter, IndeedCM.Migrate.SAM` и `IndeedCM.Migrate.SAM.Reporter.NullMigrateReporter, IndeedCM.Migrate.SAM` не допускается. Одна из них обязательно должна быть закомментирована или удалена.

Сохраните внесенные изменения.

В примере Indeed CM развернут с использованием хранилища данных и каталога пользователей в Active Directory, разрешено создание отчета о работе утилиты миграции в csv-файле.

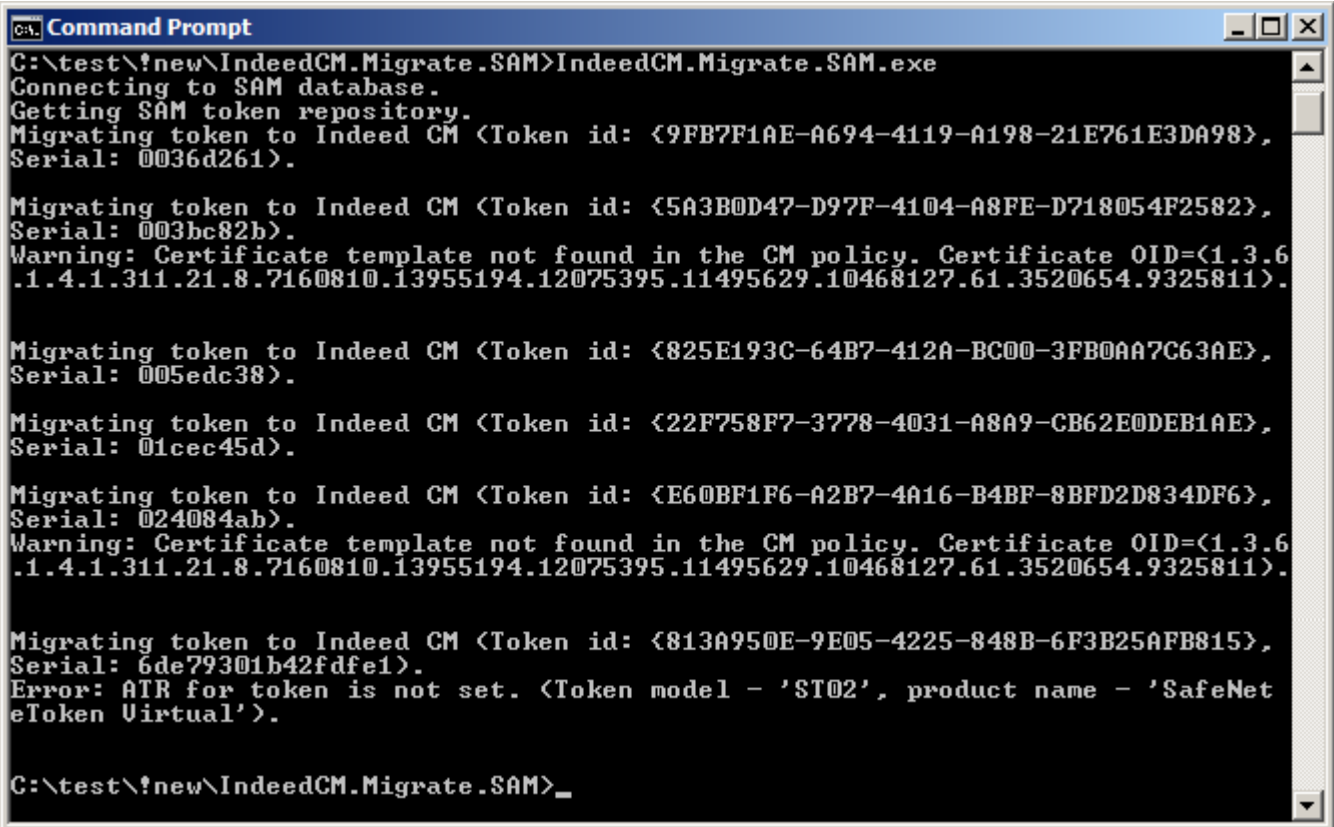
Пример заполненной секции файла unity.config:

```
<container>
  <register type="ICardRepository" mapTo="IndeedCM.Persistence.AD.CardRepository, IndeedCM.
Persistence.AD" />
  <register type="IUserDataRepository" mapTo="IndeedCM.Persistence.AD.UserDataRepository,
IndeedCM.Persistence.AD" />
  <register type="IPolicyRepository" mapTo="IndeedCM.Persistence.AD.PolicyRepository,
IndeedCM.Persistence.AD" />
  <register type="ICardTypeRepository" mapTo="IndeedCM.Persistence.AD.CardTypeRepository,
IndeedCM.Persistence.AD" />
  <register type="ILicenseRepository" mapTo="IndeedCM.Persistence.AD.LicenseRepository,
IndeedCM.Persistence.AD" />
  <register type="ISkziRepository" mapTo="IndeedCM.Persistence.AD.SkziRepository, IndeedCM.
Persistence.AD" />
  <register type="IUserCatalog" mapTo="IndeedCM.UserCatalog.AD.UserCatalog, IndeedCM.
UserCatalog.AD" />
  <register type="ISAMDbContext" mapTo="IndeedCM.Migrate.SAM_8_0.Core.SAMDbContext,
IndeedCM.Migrate.SAM_8_0" />
  <register type="ISAMHelpers" mapTo="IndeedCM.Migrate.SAM_8_0.Utls.SAMHelpers,
IndeedCM.Migrate.SAM_8_0" />
  <register type="IMigrateReporter" mapTo="IndeedCM.Migrate.SAM.Reporter.
CSVMigrateReporter, IndeedCM.Migrate.SAM" />
</container>
```

Работа с утилитой IndeedCM.Migrate.SAM

Для старта процесса миграции данных выполните следующие действия:

1. Выполните вход на сервер SAM под сервисной учетной записью SAM (Service Account).
2. Запустите утилиту в тестовом режиме **IndeedCM.Migrate.SAM.exe /test** в командной строке Windows, запущенной от имени администратора. Тестовый запуск утилиты требуется для генерации отчета о том, какие устройства и сертификаты будут перенесены в ходе миграции, а так же для вывода информации по возникшим ошибкам. В этом режиме работы утилиты данные с репозитория не переносятся, а так же не заносятся события в журнал.
3. Если в тестовом режиме не было выявлено никаких критических ошибок, то продолжите миграцию. Для этого запустите утилиту **IndeedCM.Migrate.SAM.exe** в командной строке Windows, запущенной от имени администратора.
4. В ходе работы утилита будет отображать выполняемые действия с устройствами и выводить сведения об ошибках.



```
Command Prompt
C:\test\!new\IndeedCM.Migrate.SAM>IndeedCM.Migrate.SAM.exe
Connecting to SAM database.
Getting SAM token repository.
Migrating token to Indeed CM <Token id: {9FB7F1AE-A694-4119-A198-21E761E3DA98},
Serial: 0036d261>.

Migrating token to Indeed CM <Token id: {5A3B0D47-D97F-4104-A8FE-D718054F2582},
Serial: 003bc82b>.
Warning: Certificate template not found in the CM policy. Certificate OID={1.3.6
.1.4.1.311.21.8.7160810.13955194.12075395.11495629.10468127.61.3520654.9325811}>.

Migrating token to Indeed CM <Token id: {825E193C-64B7-412A-BC00-3FB0AA7C63AE},
Serial: 005edc38>.

Migrating token to Indeed CM <Token id: {22F758F7-3778-4031-A8A9-CB62E0DEB1AE},
Serial: 01cec45d>.

Migrating token to Indeed CM <Token id: {E60BF1F6-A2B7-4A16-B4BF-8BFD2D834DF6},
Serial: 024084ab>.
Warning: Certificate template not found in the CM policy. Certificate OID={1.3.6
.1.4.1.311.21.8.7160810.13955194.12075395.11495629.10468127.61.3520654.9325811}>.

Migrating token to Indeed CM <Token id: {813A950E-9E05-4225-848B-6F3B25AFB815},
Serial: 6de79301b42fdfe1>.
Error: ATR for token is not set. <Token model - 'ST02', product name - 'SafeNet
eToken Virtual'>.

C:\test\!new\IndeedCM.Migrate.SAM>_
```

Если в файле конфигурации **IndeedCM.Migrate.SAM.exe.config** включена опция ведения отчета, то файл отчета с именем **IndeedCM.Migrate.SAM.Report_dd-MM-yyyy_HH-mm-ss.csv** будет создан автоматически в каталоге с утилитой миграции.

Пример содержимого файла отчета, открытого при помощи Microsoft Excel:

	A	B	C	D	E
1	SAMTokenId	TokenSerialNumber	Status	StatusDescription	ExStackTrace
2	{9FB7F1AE-A694-4119-A198-21E761E3DA98}	0036d261	Success	Token has been successfully imported	
3	{5A3B0D47-D97F-4104-A8FE-D718054F2582}	003bc82b	Success	Token has been successfully imported	
4	{48389550-E500-4EB5-9144-1AD2ED9A8CE4}	005edc38	Success	Token has been successfully imported	
5	{22F758F7-3778-4031-A8A9-CB62E0DEB1AE}	01cec45d	Success	Token has been successfully imported	
6	{E60BF1F6-A2B7-4A16-B4BF-8BFD2D834DF6}	024084ab	Success	Token has been successfully imported	
7	{CED8DAED-3863-4457-8FD8-FFBB847AB8BE}	2533c7052520	Success	Token has been successfully imported	
8	{89BFCC4A-B3F6-46A9-B786-63D28356C0DF}	2656440a0e2e	Success	Token has been successfully imported	
9	{813A950E-9E05-4225-848B-6F3B25AFB815}	6de79301b42fdfe1	Failed	Failed to import token	System.Exception: ATR for token is not set. (Token model - 'ST02', product name - 'SafeNet eToken Virtual').

События успешности или ошибки переноса данных могут быть записаны в журнал на сервере Indeed Certificate Manager.

▼	13.04.2017 4:58:33	Импортирование устройства	Утилита миграции SAM	eToken PRO Java 72K (JC1.0b)	003bc82b	IID\Administrati
Произошла ошибка при импортировании устройства. Устройство: eToken PRO Java 72K (JC1.0b):003bc82b Сообщение об ошибке: Card with serial number '003bc82b' and ATR '3bd5180081313a7d8073c8211030' already exists in the Indeed CM repository. Инициатор: IID\Administrator						
▼	13.04.2017 4:58:12	Импортирование устройства	Утилита миграции SAM	samuser3	eToken PRO 32K (C)	50391501
Устройство успешно импортировано. Пользователь: samuser3 Устройство: eToken PRO 32K (C):50391501 Состояние: Assigned Сертификаты: Инициатор: IID\Administrator						

Для записи событий миграции в журнал сервера Indeed CM необходимо использовать компонент **IndeedCM.EventLog.Proxy**, который позволяет записывать события в журнал сервера с удаленных рабочих станций (других серверов Indeed CM или сервера SAM, на котором работает утилита миграции).

Для настройки записи событий утилиты миграции данных в журнал событий сервера Indeed CM выполните следующие действия:

1. Откройте файл **...SAMMigration\IndeedCM.Migrate.SAM.exe.config** от имени администратора в текстовом редакторе (например, в Блокнот) и добавьте элемент **proxyServer** в секцию **eventLogAuditSettings** со следующими атрибутами:
 - **url** – путь к сервису eventlogproxy, развернутому на сервере Indeed CM
 - **userName** – имя пользователя, под которым осуществлять подключение к сервису (должно совпадать с именем в секции authorization файле web.config приложения eventlogproxy)
 - **password** – пароль учетной записи, используемой для подключения к сервису

Пример заполненной секции:

```
<proxyServer url="https://server2012r2.demo.local/eventlogproxy"
userName="DEMO\Administrator" password="P@ssw0rd" />
```

2. Сохраните изменения.

3. Установите компонент **IndeedCM.EventLog.Proxy** (располагается в каталоге дистрибутива сервера) на сервере Indeed CM.

4. Откройте файл **C:\inetpub\wwwroot\eventlogproxy\Web.config** от имени администратора в текстовом редакторе (например, в Блокнот) и укажите в секции **authorization** учетные данные для доступа к сервису **eventlogproxy**.

Пример заполненной секции:

```
<authorization>
  <deny users="?" />
  <allow users="DEMO\Administrator"/>
  <deny users="*" />
</authorization>
```

5. Сохраните изменения.

Работа с ключевыми носителями

Данное руководство, предназначенное для администраторов предприятий, поможет ознакомиться с процедурой подготовки и использованием устройств семейства JaCarta и eToken для работы в Indeed Certificate Manager версии 4.2.0 и выше.

Indeed CM взаимодействует с устройствами (USB-токенами и смарт-картами) посредством **IndeedCM.Middleware**. Также для работы необходимо ПО, обеспечивающее работу в поддерживаемых ОС – **Единый клиент JaCarta** для устройств JaCarta или **SafeNet Authentication Client** для устройств eToken. Оба компонента устанавливаются на рабочих местах операторов Indeed CM и на рабочих станциях пользователей.

Устройства JaCarta

- [Работа с устройствами JaCarta при обновлении Indeed CM на версию 4.2.0 и выше](#)
- [Особенности работы с ГОСТ-областью устройств JaCarta](#)
- [Добавление различных моделей JaCarta](#)

Добавление различных моделей eToken

Изменение иконок устройства

Устройства JaCarta

- [Работа с устройствами JaCarta при обновлении Indeed CM на версию 4.2.0 и выше](#)
- [Особенности работы с ГОСТ-областью устройств JaCarta](#)
- [Добавление различных моделей JaCarta](#)

Работа с устройствами JaCarta при обновлении Indeed CM на версию 4.2.0 и выше

В версиях Indeed Certificate Manager до 4.2.0 работа с устройствами JaCarta осуществлялась с 3DES ключом администратора. Начиная с версии 4.2.0 вместо 3DES ключа используется PIN-код администратора устройства. Прежде, чем приступить к обновлению Indeed CM до версии 4.2.0 необходимо выполнить следующие действия с устройствами JaCarta, введенными в Indeed CM:

1. Отозвать и изъять у пользователей все выпущенные устройства JaCarta.
2. Удалить с обязательным подключением к рабочей станции все устройства JaCarta на вкладке **Устройства**.

 В случае удаления без подключения, PIN-код администратора на устройстве будет иметь случайное и неизвестное никому значение, которое было установлено системой Indeed CM при добавлении устройства. Выполнить инициализацию такого устройства будет невозможно.

3. Перевести все выведенные из Indeed CM устройства с 3DES ключа на PIN-код администратора.

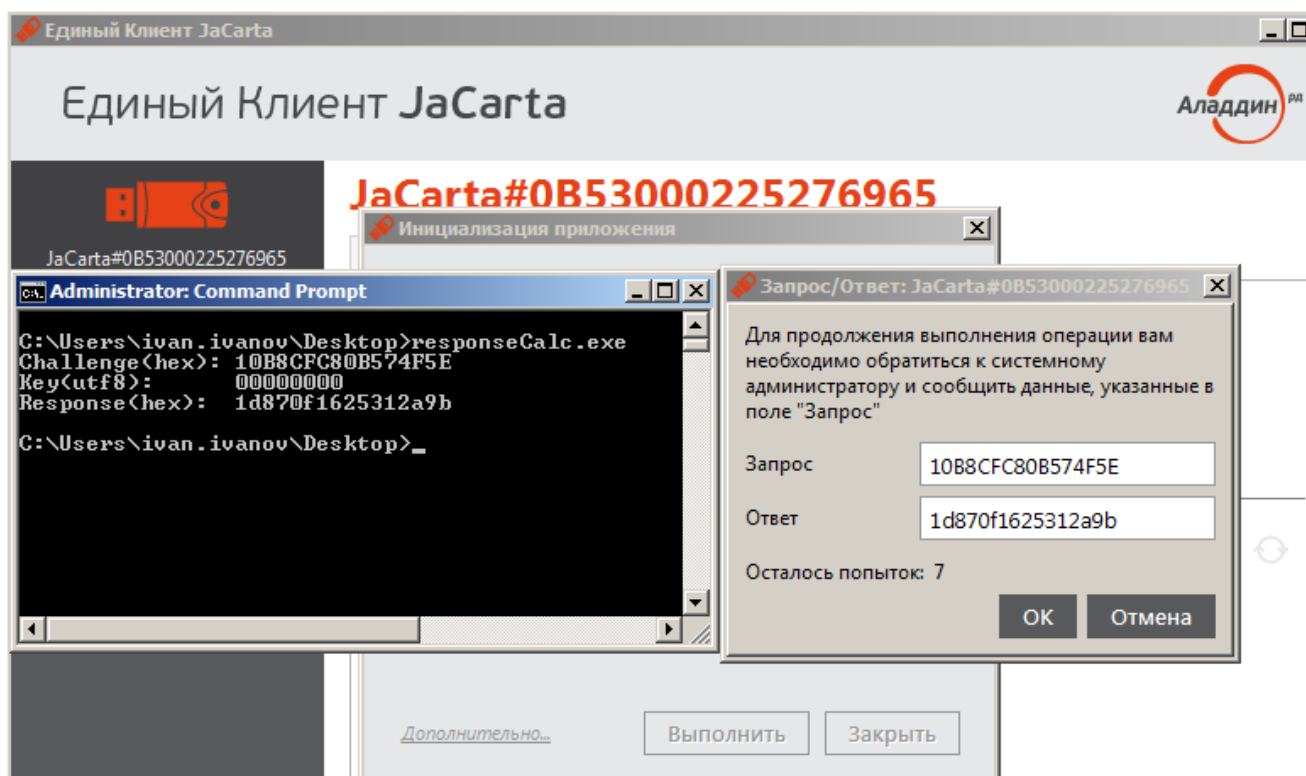
Для перевода с 3DES на PIN администратора выполните следующие действия:

1. Подключите USB токен или смарт-карту JaCarta к рабочей станции с установленным ПО Единый клиент JaCarta.
2. Переключитесь в **режим администратора**.
3. Перейдите на вкладку **PKI** и нажмите Инициализировать. . .
4. Установите в качестве PIN-кода пользователя значение **11111111**.
5. Нажмите **Дополнительно. . .**
6. Установите в качестве PIN-кода администратора значение **00000000** и нажмите **ОК**.
7. Нажмите **Выполнить** в окне **Инициализация приложения** и подтвердите действие.
8. Скопируйте код из поля **Запрос** в буфер обмена.
9. Запустите утилиту **responseCalc.exe** в командной строке Windows, запущенной от имени Администратора (Run as Administrator), вставьте значение из буфера в строку **Challenge(hex)** и нажмите **Enter**.

 Утилита **responseCalc.exe** предоставляется по запросу [службой технической поддержки Indeed-Id](#).

10. Введите значение **00000000** в поле **Key(utf8)** и нажмите **Enter**.

11. Скопируйте значение поля **Response(hex)** в поле **Ответ** окна **Запрос/Ответ Единого клиента JaCarta**:



12. Нажмите **OK**.

13. Дождитесь завершения инициализации устройства.

14. Повторите пункты 1-13 для каждого устройства, которое использовалось в прежних версиях Indeed CM (до 4.2.0).

15. Обновите сервер Indeed CM на версию не ниже 4.2.0.

16. В разделе **Конфигурация > Типы устройств** удалите файл типа устройства JaCarta.

17. Добавьте файл типа устройства **JaCarta-pin.xml** из дистрибутива сервера Indeed CM.

18. Добавьте инициализированные на работу с PIN-кодом администратора устройства JaCarta в Indeed CM версии 4.2.0.

Полученные от производителя новые устройства JaCarta по умолчанию настроены на работу через PIN-код администратора. Никаких подготовительных операций с такими устройствами для работы с Indeed CM версии 4.2.0 и выше выполнять не нужно.

Особенности работы с ГОСТ-областью устройств JaCarta

При использовании устройств JaCarta с PKI/ГОСТ-областями (за исключением устройств JaCarta-2) следует учитывать перечисленные особенности:

1. PIN-код администратора области ГОСТ по умолчанию меняется на случайный после добавления устройства в Indeed Certificate Manager.

 Начиная с версии Indeed CM 4.4.0 для вновь добавляемых устройств JaCarta есть возможность смены PIN-кода администратора при добавлении устройства на неслучайное значение. Случайный PIN-код администратора, установленный при добавлении устройств в прошлых версиях Indeed CM доступен для просмотра администраторам Indeed CM в **Карточке пользователя**.

При удалении устройства из Indeed CM с подключением устройства к рабочей станции случайный PIN-код администратора ГОСТ области меняется на значение, указанное в разделе **Конфигурация > Типы устройств**.

2. PIN-код пользователя для области ГОСТ может быть установлен и изменен только при инициализации устройства в результате выпуска (ограничение устройства).

3. При изъятии у пользователя устройства с подключением к рабочей станции необходимо ввести PIN-код пользователя для области ГОСТ. Если PIN-код пользователя для области ГОСТ неизвестен, то такое устройство изымается у пользователя без подключения к рабочей станции. Повторный выпуск такого устройства должен осуществляться только с инициализацией, в результате которой будет задан новый (известный пользователю и/или оператору) PIN-код пользователя для области ГОСТ.

4. При разблокировке области ГОСТ PIN-код пользователя не изменяется, а происходит сброс счетчика попыток ввода до блокировки в значение равное 10 (ограничение устройства).

Для PIN-кода пользователя области ГОСТ **не поддерживаются в политиках Indeed CM из-за ограничения устройства**:

- Парольная политика в разделе **Выпуск > Инициализация устройства**.
- Опция **Пользователь должен поменять PIN-код при первом входе** в разделе **Выпуск**.

Для PIN-кода пользователя области ГОСТ поддерживаются в политиках Indeed CM:

- Опция **Установить случайный PIN-код пользователя** в разделе **Выпуск**. При этом случайный PIN-код будет одинаковым для областей PKI и ГОСТ.
- Опция **Блокировать устройство** в разделе **Выпуск**.
- Установка PIN-кода в параметрах инициализации устройства.

При использовании устройств **JaCarta-2 с PKI/ГОСТ1, ГОСТ2-областями** следует учитывать перечисленные особенности:

1. Управление PIN-кодами пользователей областей ГОСТ1 и ГОСТ2 в Indeed CM происходит синхронно, т.е. смена PIN-кода ГОСТ1 повлечет за собой смену и PIN-кода ГОСТ2 и наоборот. Аналогично и для прочих операций (сброс, разблокировка).
2. PIN-коды пользователя для обоих ГОСТ-областей могут быть установлены или изменены только при инициализации устройства (при выпуске смарт-карты с включенной опцией **Инициализировать устройство**), при этом очистка содержимого устройства для ГОСТ2-области не происходит. Новое значение PIN-кода необходимо указать в параметрах инициализации для устройств JaCarta-2.
3. Для добавления устройства в Indeed CM PIN-код администратора ГОСТ1 должен совпадать с PUK-кодом области ГОСТ2. Таким образом, изменить PIN-код администратора ГОСТ1 при выпуске устройства не получится, т.е. все устройства JaCarta-2 после взятия под контроль Indeed CM будут иметь PIN-код администратора, заданный производителем (**1234567890**).



Для того чтобы изменить PIN-код администратора ГОСТ1 необходимо:

- Изменить PUK-код через АРМ-администратора JaCarta (предоставляется разработчиком устройств JaCarta).
- Изменить PIN-код администратора ГОСТ1 через АРМ (или Единый клиент).

Для работы в Indeed CM с новым PIN-кодом администратора ГОСТ1 необходимо:

- Прописать новые значения в типе устройства JaCarta.
- **Выпустить устройство** с включенными опциями **Добавлять устройства автоматически** и **Инициализировать устройство** через Indeed CM.

4. Для PKI-области инициализация проходит с очисткой содержимого и изменением PIN-кодов администратора и пользователя согласно заданным политикам инициализации в Indeed CM.

Добавление различных моделей JaCarta

Устройства JaCarta по умолчанию не разделяются по моделям при добавлении в Indeed Certificate Manager. Для разделения устройств по моделям и установки параметров инициализации для каждой модели при добавлении в Indeed CM выполните следующее:

1. Откройте файл **JaCarta-pin.xml** из дистрибутива сервера Indeed CM (\Misc\CardTypes).
2. Раскомментируйте секцию **<models>** удалив тег **<!-- ... -->**.

```
<models>
  <model name="JaCarta PKI/ГОСТ/Flash" rawModel="JC216" hasGostApplet="true"/>
  <model name="JaCarta PKI/ГОСТ" rawModel="JC205|JC305|JC005|JC005-123J.J01 v3.0"
hasGostApplet="true"/>
  <model name="JaCarta-2 PKI/ГОСТ" rawModel="JC207-12.F27 v4.0" hasGostApplet="true"/>
  <model name="JaCarta-2 SE" rawModel="JC267-1236J.J01Q01|JC267-1236.Q01" hasGostApplet="
true"/>
  <model name="JaCarta PKI" rawModel="JC000|JC200|JC300" hasGostApplet="false"/>
  <model name="JaCarta PKI/Flash" rawModel="JC210" hasGostApplet="false"/>
  <model name="JaCarta PKI/BIO" rawModel="JC303" hasGostApplet="false"/>
</models>
```

 Обратитесь в [службу технической поддержки компании Индид](#), если моделей устройств JaCarta, используемых в вашей организации нет в списке.

3. Сохраните изменения в файле.
4. Добавьте файл **JaCarta-pin.xml** в раздел **Конфигурация > Типы устройств** консоли управления Indeed CM (включите опцию **Заменить существующий**, если устройства JaCarta использовались в Indeed CM ранее).
5. При редактировании типа устройства JaCarta нажмите **Добавить настройки модели устройства**, выберите модель и нажмите **Добавить**.

Настройки моделей устройств

 **Добавить настройки модели устройства**

Модель устройства

JaCarta PKI/ГОСТ/Flash ▼

Добавить

Отмена

6. Установите параметры для выбранной модели и нажмите **Сохранить**.

Настройки моделей устройств

JaCarta PKI/ГОСТ/Flash

PIN-код администратора

PIN-код пользователя

PIN-код администратора (ГОСТ)

PIN-код пользователя (ГОСТ)

- ☒ Инициализировать устройство при добавлении
- ☒ Устанавливать неслучайный PIN-код администратора
- ☒ Устанавливать неслучайный PIN-код администратора (ГОСТ)

[+ Добавить настройки модели устройства](#)

Сохранить

Отмена



Для применения фильтрации устройств по моделям все ранее добавленные в Indeed CM устройства JaCarta должны быть выведены из системы и добавлены повторно.

Если модель добавляемого устройства не найдена, либо если настройки моделей отсутствуют, то к устройству будут применены настройки по умолчанию.

Добавление различных моделей eToken

Некоторые устройства eToken не разделяются по моделям при добавлении в Indeed Certificate Manager. Устройства **eToken PRO Java 72K OS755**, **SafeNet eToken 5110** и **IDCore 30B** имеют одинаковый **ATR (Answer-to-Reset)**, он указан в конфигурационном файле **eTokenProJava72K.xml**. Это значит, что при добавлении в Indeed CM оба устройства будут определены как **eToken PRO Java 72K**. Для разделения устройств по моделям и установки параметров инициализации для каждой модели при добавлении в Indeed CM выполните следующее:

1. Откройте файл в **eTokenProJava72K.xml** из дистрибутива Indeed CM (\Misc\CardTypes) в текстовом редакторе, например в Блокнот.
2. Раскомментируйте секцию **<models>** удалив тег **<!-- ... -->**.

```
<models>
  <model name="eToken PRO Java 72K OS755" rawModel="eToken PRO Java 72K OS755"
hasGostApplet="false" />
  <model name="SafeNet eToken 5105" rawModel="SafeNet eToken 510x" hasGostApplet="false"
/>
  <model name="SafeNet eToken 5110" rawModel="SafeNet eToken 5110" hasGostApplet="false"
/>
  <model name="IDCore30B eToken 1.7.7" rawModel="IDCore30B eToken 1.7.7" hasGostApplet="
false" />
</models>
```

3. Сохраните изменения.
4. Добавьте файл **eTokenProJava72K.xml** в раздел **Конфигурация > Типы устройств** консоли управления Indeed CM (включите опцию **Заменить существующий**, если устройства eToken использовались в Indeed CM ранее).
5. При редактировании типа устройства eToken нажмите **Добавить настройки модели устройства**, выберите модель и нажмите **Добавить**.

Настройки моделей устройств

+ Добавить настройки модели устройства

Модель устройства

eToken PRO Java 72K OS755 ▼

Добавить

Отмена

6. Установите параметры для выбранной модели и нажмите **Сохранить**.

Настройки моделей устройств

eToken PRO Java 72K OS755

PIN-код администратора

PIN-код пользователя

☒ Инициализировать устройство при добавлении

☒ Устанавливать неслучайный PIN-код администратора

[+ Добавить настройки модели устройства](#)

Сохранить

Отмена



Для применения фильтрации устройств по моделям все ранее добавленные в Indeed CM устройства **eToken PRO Java 72K** должны быть выведены из системы и добавлены повторно.

Если модель добавляемого устройства не найдена, либо если настройки моделей отсутствуют, то к устройству будут применены настройки по умолчанию.

Изменение иконок устройства

В Indeed Certificate Manager существует набор изображений, который отображает фактор устройства: USB-токен; Смарт-карта.

	Серийный номер	Тип	Состояние	
	003bc82b	eToken PRO Java 72K (JC1.0b)	Пустое	 
	0641367757	Rutoken S	Пустое	 

Для изменения иконок необходимо:

1. Подготовить изображение в формате **.png** с максимальным размером **20x20 px**.
2. Для формирования имени файла воспользуйтесь следующим шаблоном **<Название типа устройства>_<Название модели>**, где:

- **Название типа устройства** - имя, указанное в конфигурационном файле устройства.xml. Название типа находится в секции **<name>...</name>**
- **Название модели** - если в конфигурационном файле **.xml** есть данные о нескольких устройствах, то необходимо указать точное название модели. Название модели находится в секции

```
<models>
  <model name="..." />
</models>
```

 В названии файла запрещены символы: /, \, :, *, ?, ", <, >, |. Если они встречаются в названии типа устройства или модели, то их необходимо удалить. Все пробелы необходимо заменить символом подчеркивания "_".

Пример:

- Rutoken_S.png - изменение иконки для устройств **Rutoken S**
- eToken_PRO_Java_72K_eToken_PRO_Java_72K_OS755.png - изменение иконки для устройств типа **eToken PRO Java 72K**, модели **eToken PRO Java 72K OS755**.

3. Скопируйте изображение в:

- C:\inetpub\wwwroot\icm\Content\images
- C:\inetpub\wwwroot\icmremote\Content\images
- C:\inetpub\wwwroot\icmservice\Content\images

4. Откройте веб-приложение **icm** и перейдите в раздел **Устройства**.

Серийный номер	Тип
 003bc82b	eToken PRO Java 72K (JC1.0b) (eToken PRO Java 72K OS755)
 0641367757	Rutoken S

Сбор программных логов

Наличие программных логов позволяет специалистам службы поддержки определить возможные причины проблемных ситуаций и принять меры по их устранению.

- [Сбор логов серверных компонентов](#)
- [Сбор логов клиентских компонентов](#)
 - [Ошибки сбора логов и способы их устранения](#)
- [Сбор логов инсталлятора](#)

Сбор логов серверных компонентов

1. Перейдите в каталог сервиса, логи которого необходимо получить:

Сервисы Indeed CM:

- Консоль управления (Management Console) - icm - %SystemDrive%\inetpub\wwwroot\icm
- Сервис самообслуживания (Self-Service) - icmservice - %SystemDrive%\inetpub\wwwroot\icmservice
- Сервис удаленного обслуживания (Remote Self-Service) - icmremote - %SystemDrive%\inetpub\wwwroot\icmremote
- Сервис online-разблокировки и выключения смарт-карт - credprovapi - %SystemDrive%\inetpub\wwwroot\icmprovapi
- Сервис API - icmapapi - %SystemDrive%\inetpub\wwwroot\icmapapi
- Служба Монитора устройств (Card Monitor) - %ProgramFiles%\Indeed CM\CardMonitor

Сервисы Агента:

- Сервис регистрации агентов - agentregistrationapi - %SystemDrive%\inetpub\wwwroot\IndeedCM Agent Site\agentregistrationapi
- Сервис агентов - agentserviceapi - %SystemDrive%\inetpub\wwwroot\IndeedCM Agent Site\agentserviceapi

Сервисы Indeed AirKey Enterprise - %SystemDrive%\inetpub\wwwroot\Indeed.AirKey.EntServer

2. Откройте файл **Web.nlog** (NLog.config для Card Monitor и AirKey Enterprise) в текстовом редакторе, например, в Блокнот, запущенном от имени администратора, и измените параметр *minlevel*="Off" на **"Trace"** для сбора логов:

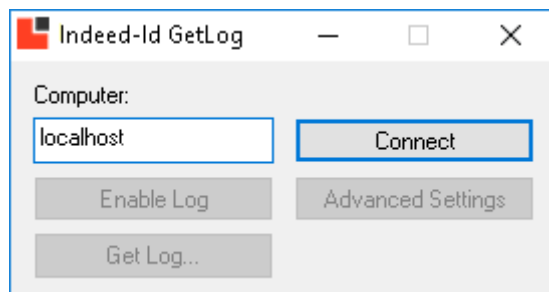
```
<logger name="*" minlevel="Trace" writeTo="file" />
```

3. Сохраните изменения в файле.
4. Перейдите в каталог **Logs**, расположенный в каталоге сервиса и удалите существующие логи.
5. Воспроизведите проблему.
6. Вернитесь в каталог **Logs**, расположенный в каталоге сервиса и убедитесь в том, что в нем появились подкаталоги с файлами отладочной информации.
7. Пришлите каталог **Logs** со всем его содержимым на адрес службы технической поддержки support@indeed-id.com с описанием воспроизведения проблемы.
8. Для отключения логирования измените значение параметра *minlevel* с "**Trace**" на "**Off**" и сохраните изменения в файле.

Сбор логов клиентских компонентов

Сбор программных логов осуществляется с помощью утилиты **Indeed-Id GetLog**, поставляемой в составе дистрибутива Indeed Certificate Manager.

Запустите приложение **IndeedID.GetLog.exe** из каталога GetLog дистрибутива Indeed CM.

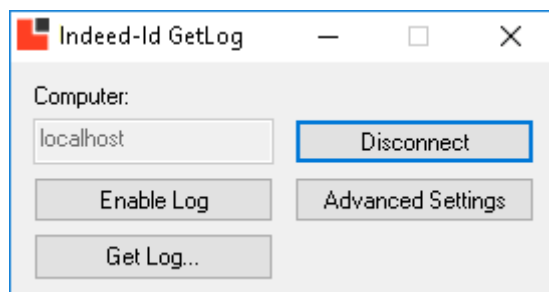


! Для работы утилиты Indeed-Id GetLog необходимы права локального администратора. На операционных системах начиная с Windows Vista и выше запуск утилиты осуществляется от имени администратора (Run As Administrator).

Подключение к компьютеру

Для подключения к компьютеру выполните следующие действия:

1. В поле **Computer** введите имя или ip-адрес удаленного компьютера. Для подключения к локальному компьютеру введите *localhost* или ip-адрес *127.0.0.1*.
2. Нажмите **Connect** для соединения с указанным компьютером. После установки соединения станет доступна кнопка включения/отключения логов (**Enable Log /Disable Log**), кнопка получения логов (**Get Log...**), кнопка перехода к дополнительным настройкам (**Advanced Settings**) и кнопка отключения (**Disconnect**).

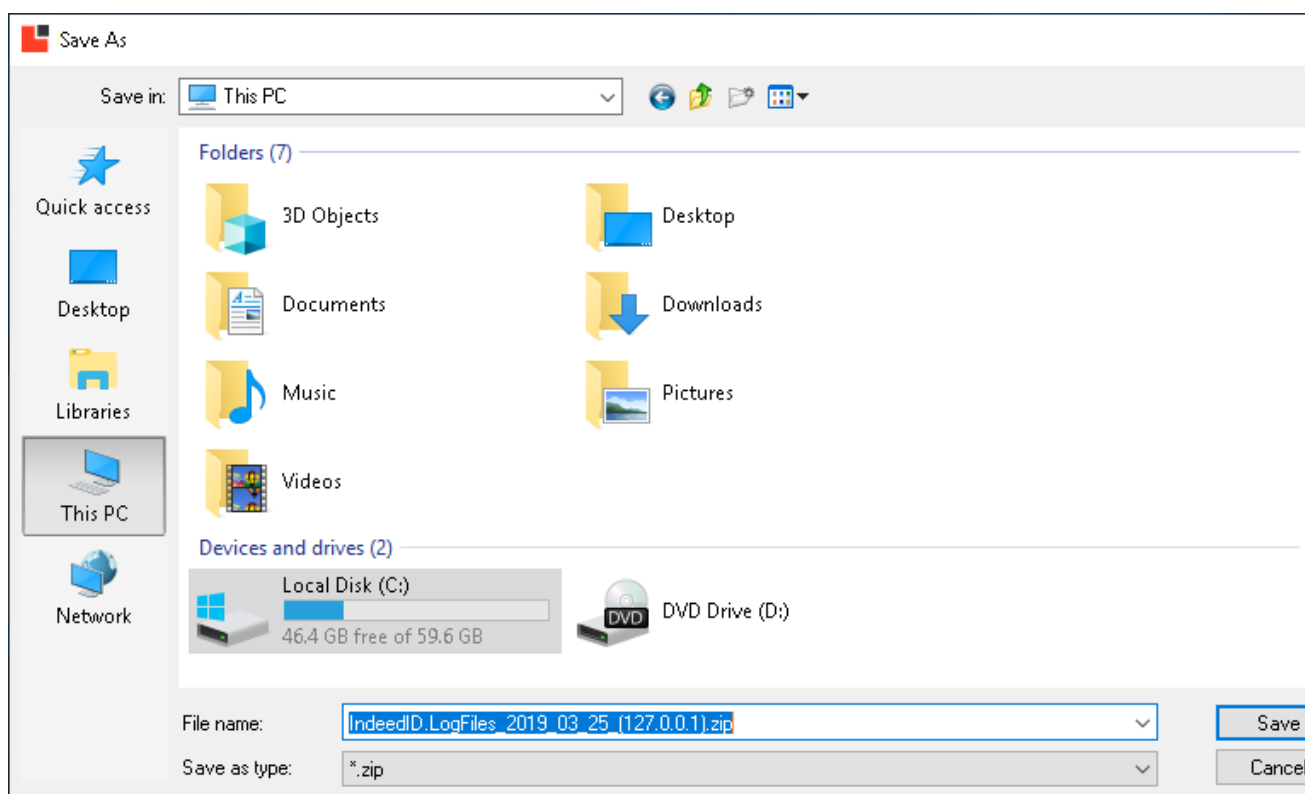


❗ Для установки подключения к удаленному компьютеру под управлением Windows Vista и выше убедитесь в том, что на удаленном компьютере запущена и не заблокирована служба **Инструментарий управления Windows (WMI)** (Windows Management Instrumentation (WMI)), см. подробнее в разделе [Ошибки сбора логов и способы их устранения](#).

Включение, отключение и сбор логов

Для включения и отключения логов выполните следующие действия:

1. Выполните подключение к компьютеру.
2. Для включения логов нажмите **Enable Log**.
3. Если сбор логов требуется для выявления причин проблемной ситуации, выполните необходимые действия для воспроизведения проблемы.
4. Для отключения логов нажмите **Disable Log**.
5. Для получения логов нажмите **Get Log...**
6. Укажите каталог для сохранения zip-архива и нажмите **Сохранить**.



i Запись лог-файлов по умолчанию осуществляется в каталог **\WINDOWS\System32\LogFiles\Indeed-Id.**

Для доступа к лог-файлам удаленного компьютера по умолчанию используется сетевой каталог **ADMIN\$\System32\LogFiles\Indeed-Id.**

Каталог для записи логов задается опцией **Use alternative location** в разделе **Advanced Settings.**

7. Для отключения от компьютера нажмите **Disconnect** и закройте приложение.

Дополнительные настройки

Для перехода к дополнительным настройкам нажмите **Advanced Settings** в главном окне Indeed-Id GetLog. В окне Advanced Settings доступны следующие настройки:

The screenshot shows the 'Advanced Settings' dialog box with the following configuration:

Setting	Value
Max. log size (bytes):	1000000000
Max. log file age (s):	86400
Cleaner interval (s):	3600
Activity checking period (ms):	60000
Enable log cycling	☒
Max. size of a log file (bytes):	100000000
Max. number of saved log files:	5
Use alternative location	☐
Alternative location	ADMIN\$\System32\LogFiles

Buttons: OK, Cancel

- **Max. log size (bytes)** – максимальный размер в байтах всех файлов в каталоге. Значение по умолчанию – 1Гб. При достижении указанного значения содержимое каталога будет автоматически удалено, за исключением файлов логов, время изменения которых не превышает значение поля Max. log file age.
- **Max. log file age (s)** – "возраст" файла лога в секундах. Если размер логов в каталоге превысил значение Max. log size, то из каталога будут удалены все файлы, дата изменения которых старше значения указанного в Max.log file age.
Например: максимальный размер всех логов в каталоге ...LogFiles\Indeed-Id равен 1Гб (Max.log size (bytes) = 1000000000), а возраст файла лога - 24 часа (Max.log file age (s) = 86400). Когда размер папки с логами превысит 1Гб, то из нее удалятся все файлы, кроме тех, что были записаны за последние сутки.
- **Cleaner interval (s)** – интервал проверки размера каталога с логами в секундах. Значение по умолчанию – 1 час (3600 секунд).
- **Activity checking period (ms)** – интервал проверки активности логирования в миллисекундах. Прежде, чем начать запись логов, компонент Indeed ID (например, IndeedCM Agent) проверит, включено ли на рабочей станции логирование. По умолчанию интервал проверки составляет 1 минуту (60 000 миллисекунд).
- **Enable log cycling** – режим циклической записи логов. Если опция включена, то логи каждого процесса будут записываться согласно заданным настройкам по количеству файлов и размеру.

Max. size of a log file (bytes) – максимальный размер лог-файла в байтах. Значение по умолчанию – 10Мб (1000000 байт). При достижении заданного размера содержимое файла перезапишется новыми данными.

Max. number of saved log files – максимальное количество сохраняемых лог-файлов. Значение по умолчанию – 5, без учета текущего записываемого файла. Если установленное количество файлов превышено, самый ранний удалится, а запись логов продолжится во вновь созданный файл.

- **Use alternative location** – альтернативный каталог записи логов. Если опция выключена, логи записываются в каталоги по умолчанию:

Локальный путь: \WINDOWS\System32\LogFiles\Indeed-Id

Сетевой путь: ADMIN\$\System32\LogFiles\Indeed-Id

Ошибки сбора логов и способы их устранения

0x800706BA The RPC server is unavailable

При попытке подключения к удаленному компьютеру.

Возможные причины:

Ошибка может возникать если на удаленном компьютере под управлением Windows Vista и выше остановлена или заблокирована служба **Инструментарий управления Windows (WMI)** (Windows Management Instrumentation (WMI)).

Действия по устранению:

Для запуска службы выполните следующие действия:

1. В **Панели управления** (Control Panel) выберите **Брандмауэр Windows** (Windows Firewall) > **Разрешение взаимодействия с приложением или компонентом в брандмауэре Windows** (Allow a program or feature through Windows Firewall).
2. Нажмите **Изменить параметры** (Change Settings) и включите опцию **Инструментарий управления Windows (WMI)** (Windows Management Instrumentation (WMI)).

0x000004B3 No network provider accepted the given network path

При попытке подключения к удаленному компьютеру.

Возможные причины:

Удаленный компьютер недоступен по сети.

Действия по устранению:

Проверьте параметры сетевого подключения.

0x80070005 Access is denied или The network path is not accessible. Access is denied

При попытке подключения к компьютеру.

Возможные причины:

1. У пользователя, под учетной записью которого запущен Indeed-Id GetLog, отсутствуют права на чтение и/или изменение ветки реестра Windows, содержащей параметры записи логов.
2. У пользователя отсутствуют права на запись в каталог сохранения логов.

Действия по устранению:

Решение 1:

Предоставьте учетной записи пользователя необходимые права на ветку реестра:

1. В **Редакторе реестра** Windows (Registry Editor) раскройте ветку реестра
HKEY_LOCAL_MACHINE\SOFTWARE\Indeed - Id
2. Выберите узел **Logging**, вызовите правой кнопкой мыши контекстное меню и выберите пункт **Разрешения** (Permissions).
3. В диалоге **Разрешения на логирование** (Permissions for Logging) нажмите **Добавить** (Add) и выберите нужную учетную запись.
4. Предоставьте выбранной учетной записи права **Полный контроль** (Full Control) и **Чтение** (Read).
5. Для сохранения изменений нажмите **Применить** (Apply). Чтобы изменения в правах вступили в силу, пользователю необходимо выйти из системы и выполнить повторный вход.

Решение 2:

Предоставьте учетной записи пользователя необходимые права в указанном каталоге.

0x80070035 The network path was not found

При попытке сохранения логов.

Возможные причины:

Недоступен сетевой каталог, используемый для доступа к лог-файлам (по умолчанию используется каталог ADMIN\$\System32\LogFiles).

Действия по устранению:

Проверьте параметры доступа к сетевому каталогу.

0x80070003 The system cannot find the file specified

При попытке сохранения логов.

Возможные причины:

Неверно указан путь к сетевому каталогу для сохранения файлов.

Действия по устранению:

Укажите правильный сетевой путь.

Сбор логов инсталлятора

Все инсталляторы Indeed Certificate Manager представляют собой msi-пакеты.

Отладочные логи для msi-пакетов можно получить стандартными средствами **Windows Installer**, запустив установку через командную строку с определенными параметрами.

Формат команды для запуска msi-пакета с записью логов:

msiexec /i <путь к файлу инсталлятора> /lv <путь к файлу с логами>

После завершения работы инсталлятора файл с логами с подробным описанием проблемы необходимо передать в [службу технической поддержки Компании Индид](#).

Примеры:

- **msiexec /i *IndeedCM.Client.Tools-v. .x64.ru-ru.msi* /lv *log.txt***

Данная команда запускает установочный пакет Indeed CM Client Tools из текущей папки. Логи инсталлятора пишутся в файл log.txt, который расположен в этой же папке.

- **msiexec /i *D:\IndeedCM.Client\IndeedCM.Client.Tools-v. .x64.ru-ru.msi* /lv *C:\install_log.txt***

Данная команда запускает установочный пакет Indeed CM Client Tools из папки D:\IndeedCM.Client. Логи инсталлятора пишутся в файл install_log.txt, который расположен в корне диска C.

В случае когда необходимо собрать логи инсталлятора при установке компонента через механизм групповых политик и нет возможности задать параметры командной строки можно воспользоваться механизмом включения логов Windows Installer с помощью ключа в реестре.

Для включения логов необходимо в реестре в ветке

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer создать ключ

Reg_SZ: Logging с значением **voicewarmupx**. Выключение логов происходит после задания пустого значения ключа **Logging**.

В случае необходимости включить и выключить отладочные логи инсталляторов Indeed-Id можно с помощью reg-файлов, которые входят в состав дистрибутива и находятся в папке `\GetLog\Regfiles` (файлы **MSI logs On.reg** и **MSI logs Off.reg**).

- Запуск файла **MSI logs On.reg** включает запись отладочных логов инсталляторов на рабочей станции.
- Запуск файла **MSI logs Off.reg** выключает запись отладочных логов на рабочей станции.

Файл с логамы сохраняется в папку «Temp». Имя нового файла журнала выбирается произвольно, но начинается с букв «**Msi**» и заканчивается расширением **.log**. Чтобы определить местоположение папки «Temp», введите в командную строку следующее:

```
cd %temp%
```

Контакты

Служба поддержки

Если у вас возникли вопросы, связанные с документацией, или вы столкнулись с проблемами в планировании инфраструктуры Indeed Certificate Manager, трудностями при установке, настройке, или ошибками при эксплуатации, то вы можете обратиться в службу технической поддержки:

- Email - support@indeed-id.com
- Телефон - 8-800-333-09-06 (звонок бесплатный)
- Портал поддержки - <https://support.indeed-id.ru>

Отдел по работе с клиентами

Если у вас возникли вопросы, по условиям приобретения или сотрудничества, то вы можете обратиться к руководителю по работе с ключевыми заказчиками:

- Контактное лицо - **Бегунова Екатерина**
- Email - sales@indeed-company.ru
- Телефон - +7 (495) 640-06-09
- Адрес - 123317, Москва, IQ Квартал, Пресненская набережная 10, ст. 2, офис 165

Стоимость предоставления права на использование продукта определяется индивидуально исходя из потребностей заказчика.