Indeed Certificate Manager

Техническая документация

Версия: 7.0

Дата: 08.05.2026

Содержание

О продукте

Программный комплекс Indeed Certificate Manager (Indeed CM) – централизованная система управления инфраструктурой открытых ключей.

Indeed CM обеспечивает полный контроль над ключевыми носителями на всех этапах их жизненного цикла, позволяет вести учет средств криптографической защиты информации (СКЗИ), решать проблемы пользователей, связанные с эксплуатацией ключевых носителей, без обращения к администраторам.

Ключевые функции

- управление сертификатами в течение всего жизненного цикла;
- управление устройствами (USB-токенами и смарт-картами);
- контроль использования устройств на рабочих станциях пользователей через клиентский агент;
- управление средствами криптографической защиты информации (СКЗИ) в течение всего жизненного цикла;
- управление документами через сервис внутреннего электронного документооборота;
- журналирование всех операций, генерация отчетов для регуляторов и отправка уведомлений о событиях системы администраторам и пользователям;
- управление устройствами через API;
- разграничение прав доступа (администраторы, операторы, пользователи) и гибкая настройка привилегий;
- веб-портал для самостоятельной работы пользователей с сертификатами и устройствами, для взаимодействия с администратором.

Совместимость

Платформы	• ОС Windows • ОС Linux (в том числе Astra Linux и РЕД ОС, сертифицированные ФСТЭК)
Каталоги пользователей	• Microsoft Active Directory • Центр Регистрации КриптоПро УЦ

Удостоверяющие центры	• Microsoft CA • КриптоПро УЦ 2.0 и КриптоПро PKI-Кластер • КриптоПро DSS • Валидата УЦ
Хранилище данных	• Microsoft SQL Server • PostgreSQL • Postgres Pro

Интеграции

- **Система межведомственного электронного взаимодействия (СМЭВ)**

  В процессе выпуска или обновления устройства можно одновременно проверить данные пользователя в СМЭВ, а также получить квалифицированный сертификат, зарегистрировать его в ЕСИА и записать на устройство.

- **Indeed Access Manager**

  Одна операция выпуска устройства в Indeed CM позволяет записать сертификат и автоматически зарегистрировать вход по смарт-карте/USB-ключу и PIN-коду в Indeed AM.

- **Secret Net Studio**

  При выпуске устройства в Indeed CM оно автоматически регистрируется в базе данных SNS. Пользователь получает персональный идентификатор SNS, который записывается на устройство.

Компоненты

Indeed Certificate Manager состоит из серверных и клиентских компонентов. Для хранения данных и настроек можно использовать базы данных Microsoft SQL, PostgreSQL, Postgres Pro Standard, Postgres Pro Enterprise.

Серверные компоненты

Ядром системы является Indeed CM Server. Серверная инфраструктура включает в себя следующие компоненты:

- **Консоль управления** (Management Console) – консоль управления для администраторов и операторов;
- **Сервис самообслуживания** (Self-Service) – личный кабинет пользователя;
- **Сервис удаленного обслуживания** (Remote Self-Service) – сервис удаленного обслуживания пользователей за пределами домена;
- **API** – сервис API для управления жизненным циклом устройств и средств криптографической защиты информации (СКЗИ) и для интеграции со сторонними системами;
- **CredProvAPI** – сервис онлайн-разблокировки и выключения устройств;
- **Card Monitor** – служба для мониторинга состояния устройств, которая устанавливается вместе с Indeed CM Server;
- **Клиентский агент** (Indeed CM Agent) – сервис регистрации клиентских агентов и сервис для удаленного управления устройствами пользователей;
- **Мастер настройки Indeed CM** (Indeed CM Configuration Wizard) – мастер настройки Indeed CM;
- **OpenID Connect Server** – сервер для аутентификации пользователей в веб-приложениях Indeed CM по протоколу OpenID Connect;
- **MSCA Proxy** – дополнительный компонент для настройки интеграции с Центрами сертификации Microsoft Enterprise CA, находящимися за пределами домена, в котором развернут Indeed CM;
- **Event Log Proxy** – дополнительный компонент для записи событий с нескольких серверов Indeed CM в единый журнал событий Windows;
- **Indeed Log Server** – дополнительный компонент для записи событий с нескольких серверов Indeed CM в единый журнал событий Windows, базы данных Microsoft SQL или

PostgreSQL и SysLog.

> **ПОДСКАЗКА**
>
> Веб-приложения OpenID Connect Server, MSCA Proxy, Event Log Proxy и Indeed Log Server являются обязательными для инсталляций Indeed CM под управлением ОС Linux и дополнительными для инсталляций под управлением ОС Windows.

Вспомогательные утилиты

- *Storage.sql* – скрипт наполнения базы данных Microsoft SQL;
- *Storage-Postgre.sql* – скрипт наполнения базы данных PostgreSQL;
- *Cm.CertEnroll.MsCA.exe* – утилита для выпуска сертификата Агент регистрации для сервисной учетной записи с Microsoft Enterprise CA;
- *Cm.Agent.Cert.Generator*– утилита для создания сертификатов клиентского агента;
- *Cm.Persistence.KeyGen.exe* – утилита для создания ключа шифрования базы данных Indeed CM.

Клиентские компоненты

- **Indeed CM Middleware** – компонент, который предоставляет единый интерфейс для управления устройствами, подключенными к рабочей станции;
- **Indeed CM Client Tools**
  - **Credential Provider** – компонент для разблокировки устройств, используемых для аутентификации в ОС Windows;
  - **Indeed CM Unblock** – компонент для разблокировки устройств в сессии операционной системы;
- **Indeed CM Agent** – клиентский агент для удаленного управления устройствами пользователей;
- **Indeed CM Client Browser Extension** – компонент для поддержки множественных сессий пользователей на терминальном сервере.

Лицензирование

Лицензии Indeed Certificate Manager делятся на следующие типы:

- основная лицензия Indeed Certificate Manager;
- лицензии для дополнительных модулей.

Как добавить лицензию в Indeed CM

Основная лицензия Indeed Certificate Manager

Основная лицензия обязательна, без нее не работают остальные лицензии.

Лицензия позволяет выпускать все физические устройства, которые поддерживаются в Indeed CM:

- аппаратные смарт-карты и USB-токены;
- устройства TPM Virtual Smart Card и Windows Hello for Business;
- устройства Registry с записью сертификатов в локальное хранилище компьютера или пользователя.

Учитывается количество пользователей Indeed CM.

Лицензия считается занятой, если назначить или выпустить пользователю хотя бы одну смарт-карту или USB-токен. Если выпустить два и более устройства, то будет занята всего одна лицензия. Количество сертификатов на устройстве не учитывается.

Лицензия освобождается, если изъять у пользователя все назначенные устройства.

Лицензии можно докупить. При необходимости можно перераспределить лицензии между пользователями — отозвать лицензию у одних пользователей и назначить другим.

Лицензии для дополнительных модулей

Отдельно лицензируются следующие модули:

- Indeed AirCard Enterprise;
- КриптоПро DSS;
- Клиентский агент (Indeed CM Agent).

Лицензия Indeed AirCard Enterprise позволяет использовать виртуальные смарт-карты. Учитывается количество пользователей с устройством AirCard.

Лицензия для интеграции с сервисом электронной подписи КриптоПро DSS дает право на управление ключами и сертификатами КриптоПро DSS в инфраструктуре Indeed CM. Учитывается количество пользователей с сертификатами КриптоПро DSS.

Лицензия Indeed CM Agent позволяет удаленно управлять устройствами пользователей с помощью агентов. Учитывается количество рабочих станций, на которые устанавливаются агенты для взаимодействия с сервером Indeed CM.

Срок действия лицензии

По сроку действия лицензии бывают:

- бессрочные — не ограниченные по времени;
- по подписке — выдаются на 1 год.

На период пилотного внедрения и тестирования продукта можно запросить временную лицензию.

Если срок действия лицензий истек или все лицензии исчерпаны, вам будут недоступны следующие операции:

- выпуск новых устройств новым пользователям;
- добавление ключей и сертификатов КриптоПро DSS в инфраструктуру Indeed CM;
- регистрация новых клиентских агентов.

Чтобы обновить лицензию, обратитесь к вашему менеджеру в компании Индид.

> **ПРИМЕЧАНИЕ**
>
> При покупке бессрочной лицензии или лицензии по подписке у вас есть возможность обращаться в техническую поддержку компании Индид и обновлять Indeed Certificate Manager. Информацию по условиям обслуживания (SLA) можно просмотреть на сайте компании Индид.

Системные требования

Серверные компоненты

Системные требования для серверных компонентов

Клиентские компоненты

Системные требования для клиентских компонентов

Сетевое взаимодействие

Схема сетевого взаимодействия между компонентами Indeed CM

Устройства

Список поддерживаемых устройств аутентификации и электронной подписи

Серверные компоненты

Перед установкой серверных компонентов убедитесь, что IT-инфраструктура компании соответствует системным требованиям.

Аппаратные требования

- не менее 8 ГБ оперативной памяти;
- не менее 50 ГБ свободного дискового пространства.

Программные требования

Операционная система

- Windows Server 2008 SP2 x64 (с обновлением KB980368);
- Windows Server 2008 R2 SP1;
- Windows Server 2012/2012 R2;
- Windows Server 2016;
- Windows Server 2019;
- Windows Server 2022;
- Debian 9–12;
- Astra Linux Special Edition 1.6–1.8;
- Ubuntu 18.04 LTS–25.04 LTS;
- Red Hat Enterprise Linux 8–9;
- CentOS Stream 8–9;
- РЕД ОС 7.2–7.3.4.

> **ПРИМЕЧАНИЕ**
>
> Убедитесь, что в ОС Windows параметр **Язык программ, не поддерживающих Юникод** имеет значение **Русский (Россия)**.

Веб-сервер

- Internet Information Services (IIS) 7.0 и выше для ОС Windows;

- Nginx 1.22.1 и выше в качестве обратного прокси-сервера (Reverse Proxy) для ОС Linux;
- Apache 2.4.25 и выше в качестве обратного прокси-сервера (Reverse Proxy) для ОС Linux;

Дополнительные компоненты Microsoft

- Microsoft .NET Core 3.1;
- Microsoft .NET Framework 4.5 и выше.

Компоненты КриптоПро

- КриптоПро CSP 4.0 R4 и выше для выпуска сертификатов в Microsoft Enterprise CA по алгоритмам ГОСТ Р34.10-2001/2012, КриптоПро УЦ 2.0, Валидата УЦ;
- КриптоПро CSP 5.0 и выше для интеграции с КриптоПро DSS 2.0;
- КриптоПро CSP 5.0 R2 для ОС Linux.

> **ПРИМЕЧАНИЕ**
>
> Чтобы установить защищенное TLS-соединение между сервером Indeed CM и Центрами Регистрации КриптоПро и Валидата УЦ, вам необходима серверная лицензия КриптоПро CSP. КриптоПро и Валидата УЦ защищены в соответствии с государственными стандартами РФ.

Требования к окружению

Каталог пользователей

- Active Directory;
- Центр Регистрации КриптоПро УЦ 2.0.

Центр сертификации

- Центр сертификации Microsoft (Microsoft Enterprise CA), настроенного на выпуск сертификатов с использованием КриптоПро CSP:
  - на базе Windows Server 2003 и 2008 (редакция Enterprise и выше);
  - на базе Windows Server 2012/2012 R2;
  - на базе Windows Server 2016;
  - на базе Windows Server 2019;

    - на базе Windows Server 2022.
- КриптоПро УЦ 2.0;
- Валидата УЦ версий 3.1, 4.0.

Хранилище данных

- Microsoft SQL Server 2012 SP2 и выше;
- PostgreSQL 12 и выше;
- Postgres Pro Standard, Postgres Pro Enterprise 12 и выше.

Поставщики службы криптографии (CSP)

RSA:

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

> **ПРИМЕЧАНИЕ**
>
> Поддерживается в том числе и в связке с КриптоПро УЦ 2.0.

ГОСТ Р34.10-2001/2012:

- КриптоПро CSP 4.0 R4 и выше;
- Аппаратная криптография Рутокен ЭЦП PKI, Рутокен ЭЦП 2.0, Рутокен 2151, Рутокен ЭЦП 3.0, JaCarta ГОСТ, JaCarta-2 ГОСТ, ESMART Token ГОСТ, MS_KEY K-"Ангара".

> **ПРИМЕЧАНИЕ**
>
> Поддерживается в том числе и в связке с Microsoft Enterprise CA.

Клиентские компоненты

Перед установкой клиентских компонентов убедитесь, что IT-инфраструктура компании соответствует системным требованиям.

Аппаратные требования

Не менее 300 МБ свободного дискового пространства.

Программные требования

Операционная система

- Windows Vista SP2 x86/x64;
- Windows 7 SP1 x86/x64;
- Windows 8/8.1 x86/x64;
- Windows 10 x86/x64;
- Windows 11 x86/x64;
- Windows Server 2008 SP2 x86/x64 (с обновлением KB980368);
- Windows Server 2008 R2 SP1;
- Windows Server 2012/2012 R2;
- Windows Server 2016;
- Windows Server 2019;
- Windows Server 2022;
- Debian 10–11;
- Astra Linux Special Edition 1.6–1.8;
- Astra Linux Common Edition 2.12;
- Ubuntu 18.04 LTS и выше;
- Red Hat Enterprise Linux 8–9;
- CentOS Stream 8–9;
- РЕД ОС 7.3–8;
- Альт Рабочая станция 9–10.

Требования к окружению

- установленные драйверы (PKI-менеджеры) используемых смарт-карт и USB-токенов;
- Microsoft Edge Chromium 88.0.705.81 и выше;
- Google Chrome или Chromium 88.0.4324 и выше;
- Яндекс.Браузер 21.3.0 и выше;
- Mozilla Firefox 60.0.2 и выше;
- КриптоПро CSP 4.0 R4 и выше для выпуска сертификатов в Microsoft Enterprise CA по алгоритмам ГОСТ Р34.10-2001/2012, КриптоПро УЦ 2.0, Валидата УЦ;
- КриптоПро CSP 5.0 и выше для интеграции с КриптоПро DSS 2.0.

Сетевое взаимодействие

Сервер Indeed CM

Веб-приложения, HTTP, HTTPS

- 80 (TCP);
- 443 (TCP);
- 3001/3002 (TCP) для Indeed AirCard Enterprise;
- 3003 (TCP) для Indeed CM Agent.

Почтовые уведомления, SMTP сервер

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

Active Directory

- 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

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

PostgreSQL

5432 (TCP/UDP) - PostgreSQL default port.

Microsoft Enterprise CA

- 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.

> **ПРИМЕЧАНИЕ**
>
> 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 и КриптоПро DSS 2.0

443 (TCP).

Валидата УЦ

13434 (TCP) – порт по умолчанию для RPC сервера Центра Регистрации Валидата УЦ в онлайн-режиме работы.

Indeed Access Manager

- 80 (TCP);
- 443 (TCP).

Secret Net Studio

- 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

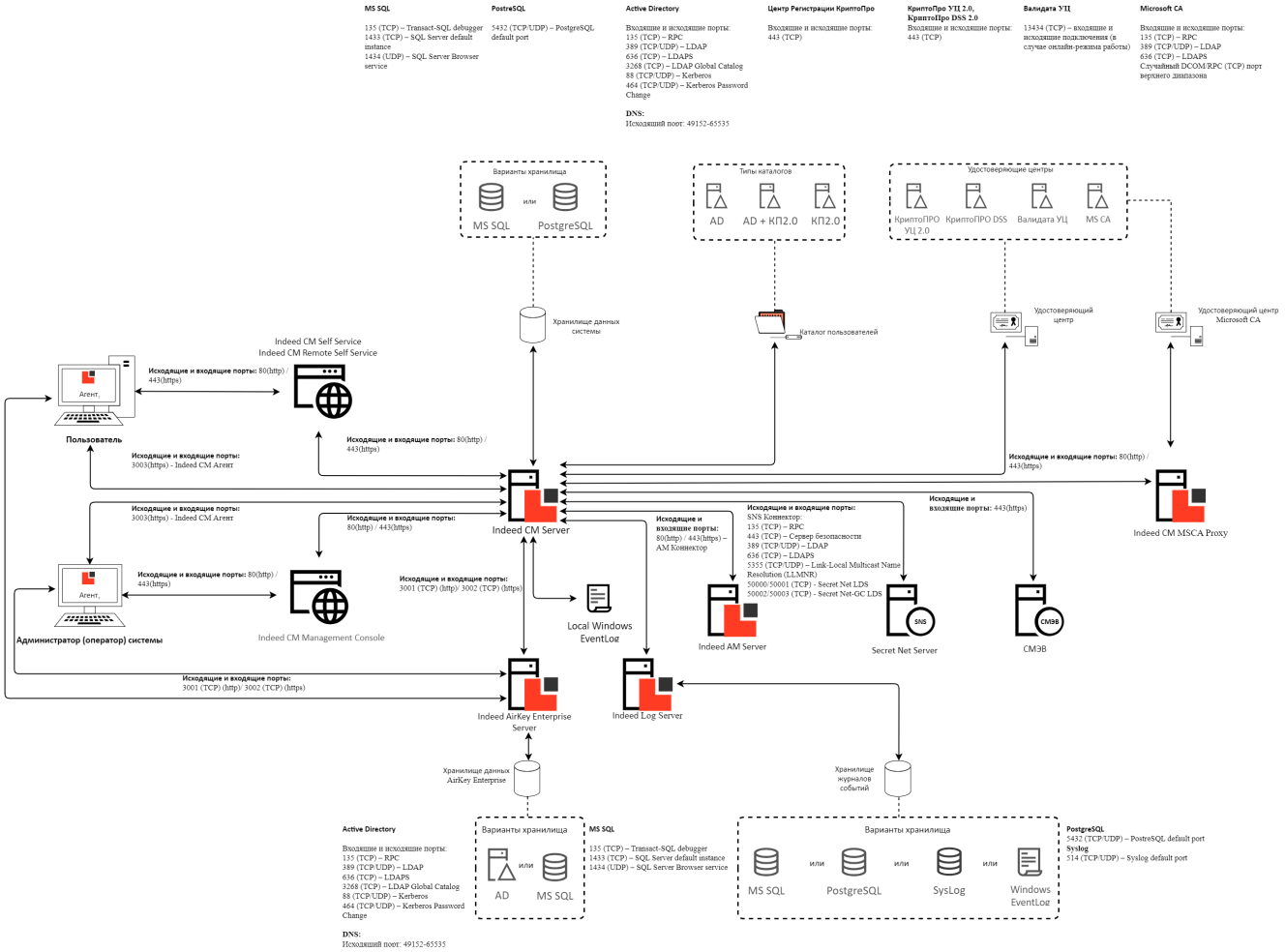
DNS

53 (TCP/UDP), исходящие подключения.

Веб-приложения, HTTP, HTTPS

- 80 (TCP);
- 443 (TCP);
- 3001/3002 (TCP) для Indeed AirCard Enterprise;
- 3003 (TCP) для Indeed CM Agent.

Схема сетевого взаимодействия



Устройства

ОС Windows

Производитель	Модель
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
Компания «Актив»	Рутокен S Рутокен Lite и смарт-карта Рутокен Lite Рутокен ЭЦП PKI и смарт-карта Рутокен ЭЦП PKI Рутокен ЭЦП 2.0 и смарт-карта Рутокен ЭЦП 2.0 Рутокен 2151 и смарт-карта Рутокен 2151 Рутокен ЭЦП 3.0 NFC и смарт-карта Рутокен ЭЦП 3.0 NFC
Компания Индид	Сетевая смарт-карта AirCard
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

Производитель	Модель
HID	Crescendo C1150 Series Crescendo C1300 Series Crescendo C2300 Series
ISBC	ESMART Token USB 64K и ESMART Token CARD 64K ESMART Token USB 192K и ESMART Token CARD 192K ESMART Token USB ГОСТ и ESMART Token CARD ГОСТ MS_KEY K-"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 (SafeNet и 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

ОС Linux

Производитель	Модель
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
Компания «Актив»	Рутокен Lite и смарт-карта Рутокен Lite Рутокен ЭЦП PKI и смарт-карта Рутокен ЭЦП PKI Рутокен ЭЦП 2.0 и смарт-карта Рутокен ЭЦП 2.0 Рутокен 2151 и смарт-карта Рутокен 2151 Рутокен ЭЦП 3.0 NFC и смарт-карта Рутокен ЭЦП 3.0 NFC
ISBC	ESMART Token USB 64K и ESMART Token CARD 64K ESMART Token USB 192K и ESMART Token CARD 192K ESMART Token USB ГОСТ и ESMART Token CARD ГОСТ
Thales (SafeNet и Gemalto) Поддерживается только выпуск RSA сертификатов.	SafeNet eToken PRO 32k SafeNet eToken PRO 64k eToken PRO Java 72K OS755 SafeNet eToken 5105 SafeNet eToken 5110 IDCore30B eToken 1.7.7

Порядок установки

Порядок установки и настройки Indeed Certificate Manager зависит от окружения, в котором система будет развернута. Данные системы могут храниться в базе данных Microsoft SQL или PostgreSQL. Каталог пользователей системы можно расположить 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.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Поддержка хранилища данных системы в Active Directory прекращена в версии 7.0.0.

Предварительные настройки инфраструктуры

Подготовьте инфраструктуру для работы Indeed CM.

1. Настройте каталог пользователей в Active Directory или в Центре Регистрации КриптоПро УЦ 2.0. Если каталог пользователей расположен только в Центре Регистрации КриптоПро УЦ 2.0, настройте аутентификацию в веб-сервисах Indeed CM по сертификатам.
2. Создайте хранилище данных в Microsoft SQL или PostgreSQL.
3. Настройте интеграцию с удостоверяющим центром:

- Microsoft Enterprise CA
- КриптоПро УЦ 2.0
- КриптоПро DSS
- Валидата УЦ

Установка и настройка Indeed CM

Windows

1. Установите Internet Information Services (IIS) на сервер под управлением ОС Windows.
2. Установите платформу .NET Core.
3. Установите и настройте серверные компоненты Indeed CM.
4. Установите и настройте клиентские компоненты Indeed CM.
5. Настройте [браузеры](/certificate-manager/7.0/install/browser-settings?os=ОС Windows) на рабочих станциях администраторов, операторов и пользователей Indeed CM.
6. Установите и настройте Клиентский агент Indeed CM Agent (дополнительный компонент системы).

Linux

1. Установите веб-сервер NGINX или Apache HTTP Server на рабочую станцию под управлением ОС Linux и настройте его в качестве обратного прокси-сервера.
2. Установите платформу .NET Core.
3. Установите и настройте серверные компоненты Indeed CM:
    1. Indeed CM Server.
    2. Журналирование.
    3. Параметры системы.
    4. Сервер авторизации пользователей OpenID Connect.
4. Установите и настройте клиентские компоненты Indeed CM.
5. Настройте [браузеры](/certificate-manager/7.0/install/browser-settings?os=ОС Linux) на рабочих станциях администраторов, операторов и пользователей Indeed CM.
6. Установите и настройте Клиентский агент Indeed CM Agent (дополнительный компонент системы).

Установка и настройка

Каталог пользователей

Active Directory или Центр Регистрации КриптоПро

Хранилище данных

Создание хранилища данных в Microsoft SQL, PostgreSQL и Postgres Pro

Центры сертификации

Настройка удостоверяющих центров для интеграции с Indeed CM

Веб-сервер

Настройка веб-сервера для работы серверных компонентов Indeed CM

Платформа .NET Core

Установка .NET для работы серверных компонентов Indeed CM

Серверные компоненты

Установка и настройка серверных компонентов Indeed CM

Клиентские компоненты

Установка клиентских компонентов Indeed CM

Браузеры

Настройка браузеров для доступа к веб-приложениям Indeed CM

Каталог пользователей

Настройте каталог пользователей в Active Directory или в Центре Регистрации КриптоПро УЦ 2.0.

Active Directory

Чтобы данные о пользователях появились в Indeed CM:

1. Подготовьте в Active Directory объект (домен, контейнер, подразделение) с конечными пользователями.
2. Создайте сервисную учетную запись для чтения и записи атрибутов пользователей. Вы можете распределить права между несколькими сервисными учетными записями или создать одну сервисную учетную запись с максимальным набором прав доступа к объектам Active Directory.

Выполните следующие действия:

1. Откройте свойство **Безопасность** (Security) объекта, где хранятся пользователи Indeed CM.
2. Нажмите **Дополнительно** (Advanced). Нажмите **Добавить** (Add) → **Выбрать субъект** (Select a principal).
3. В текстовом поле **Введите имена выбираемых объектов** (Enter the object name to select) введите имя сервисной учетной записи (**servicecm**) и нажмите **ОК**.
4. В выпадающем списке **Применяется к** (Applies to) выберите **Дочерние объекты: Пользователь** (Descendant User objects).
5. В списке **Разрешений** (Permissions) выберите:
   - **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) для возможности **сбросить пароль пользователя** с помощью Indeed CM.
6. В списке **Свойств** (Properties) отметьте пункты:
   - **Запись: pwdLastSet** (Write pwdLastSet) для возможности сбросить пароль пользователя.

- **Запись: thumbnailPhoto** (Write thumbnailPhoto) или **Запись: jpegPhoto** (Write jpegPhoto) для **загрузки фотографии пользователя** в Active Directory с помощью Indeed CM.
- **Запись: userAccountControl** (Write userAccountControl) для работы опции **Требовать логон по смарт-карте**.
- **Запись: userCertificate** (Write userCertificate) для **публикации сертификата КриптоПро 2.0** в профиле пользователя Active Directory.

7. Нажмите **ОК** и затем **Применить** (Apply).

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Установите одинаковый набор прав сервисной учетной записи для каждого объекта, где хранятся пользователи Indeed CM.

Если политики безопасности домена запрещают чтение всех свойств пользователя, выдайте сервисной учетной записи права на чтение атрибутов пользователей и атрибутов объекта, где хранятся пользователи Indeed CM. Для этого:

1. В оснастке **Редактирование ADSI** (ADSI edit) откройте свойство **Безопасность** (Security) объекта, где хранятся пользователи Indeed CM.
2. Для области применения **Этот объект и все дочерние объекты** (This object and all descendant objects):
    1. В списке **Разрешений** (Permissions) отметьте **Список содержимого** (List contents).
    2. 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):
    1. В списке **Разрешений** (Permissions) отметьте **Список содержимого** (List contents).
    2. В списке **Свойств** (Properties) выберите чтение/запись следующих наборов свойств и атрибутов:

- **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).

> ⓘ **ПРИМЕЧАНИЕ**
>
> Приведены отображаемые имена **LDAP** (LDAP Display Name).
>
> Предоставление прав доступа к набору свойств значительно улучшает производительность и упрощает управление безопасностью (подробнее на сайте компании Microsoft).

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).

Атрибут (LDAP Display Name)	Common Name	Комментарий
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).

Атрибут (LDAP Display Name)	Common Name	Комментарий
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).

Атрибут (LDAP Display Name)	Common Name	Комментарий
userPrincipalName	User Principal Name	Входит в набор свойств «Открытые сведения» (Public Information).

КриптоПро УЦ 2.0

Чтобы данные о пользователях появились в Indeed CM:

1. Создайте сервисную группу пользователей в Центре Регистрации КриптоПро 2.0.
2. Создайте сервисную учетную запись, от имени которой Indeed CM будет обращаться к УЦ для запроса сертификатов пользователей. Вы можете использовать любую учетную запись, уже созданную в Центре Регистрации, поместив ее в предварительно созданную и наделенную необходимыми полномочиями сервисную группу Indeed CM.

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:

Набор разрешений для сервисной группы пользователей

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. Разрешение необходимо выдать и для корневой папки «Центр Регистрации» с наследованием для чтения списка пользователей.
Запись свойств	Папка	Запись свойств объекта. Необходимо выдать и для корневой папки «Центр Регистрации» с наследованием для публикации списка отозванных сертификатов
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

Наименование разрешения	Тип объекта	Комментарий
Одобрение сертификата	Пользователь, шаблон	Одобрение запроса сертификата для пользователя. Необходимо выдать и для корневой папки «Центр Регистрации» с наследованием.
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.

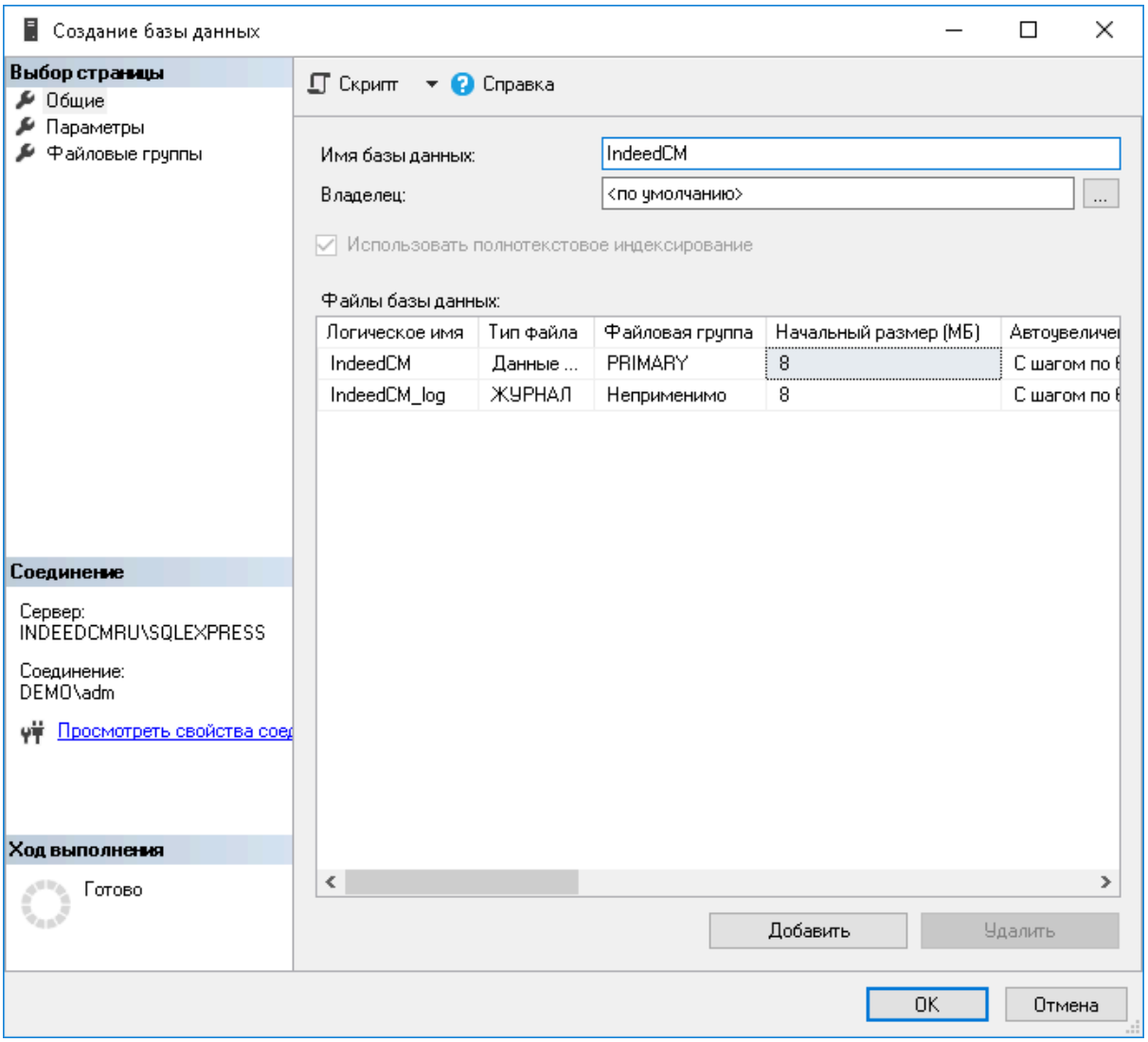
Хранилище данных

Indeed Certificate Manager работает с базами данных Microsoft SQL, PostgreSQL и Postgres Pro. База данных создается вручную, а для ее наполнения используются скрипты, входящие в состав дистрибутива Indeed CM (*\IndeedCM.WindowsServer\Misc*).

Microsoft SQL

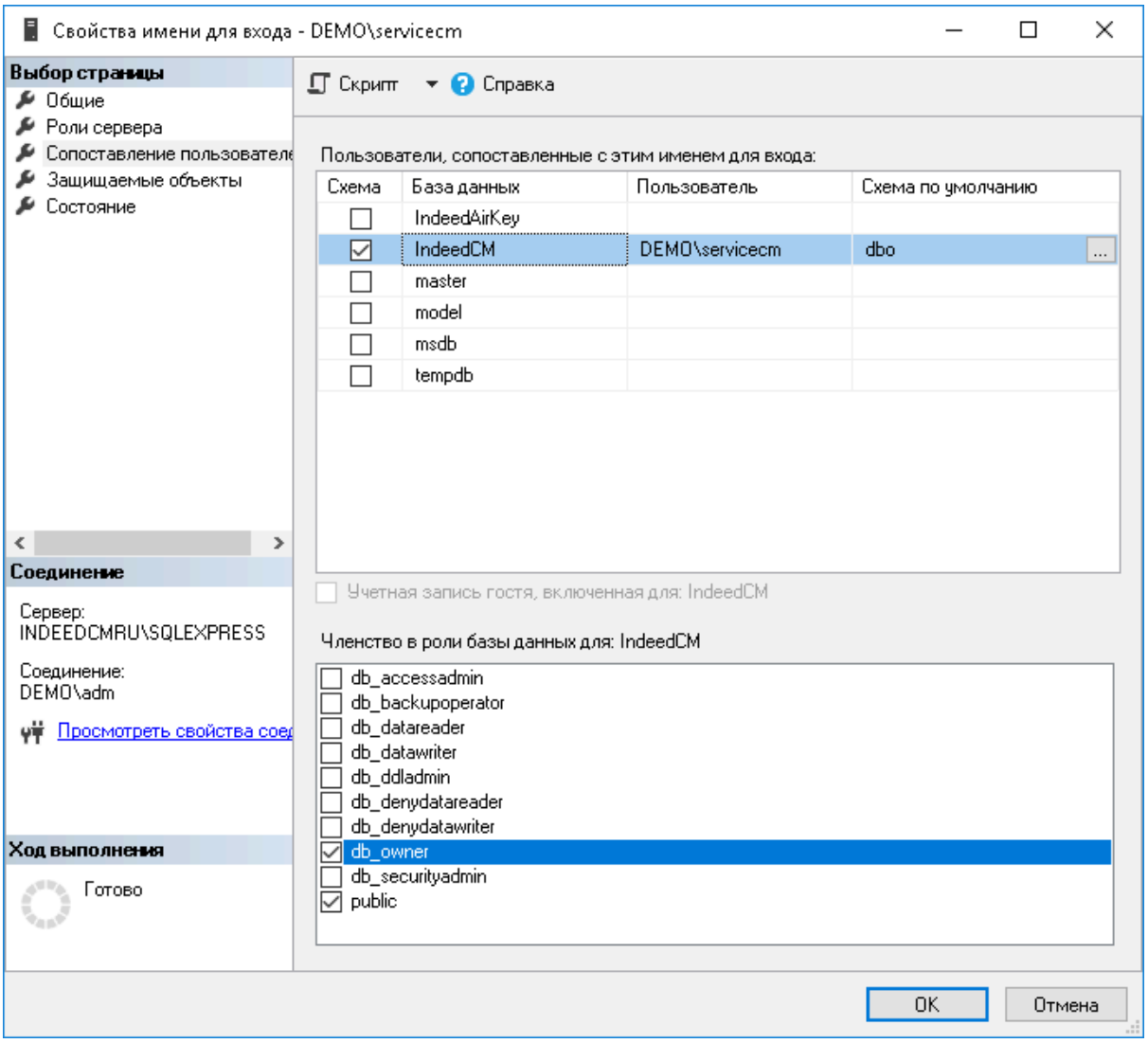
1. Создайте базу данных в среде SQL Management Studio с произвольным именем:

    1. В окне **Обозреватель объектов** (Object Explorer) нажмите правой кнопкой мыши по вкладке **Базы данных** (Databases).
    2. Выберите **Создать базу данных...** (New Database...).
    3. Укажите **Имя базы данных:** (Database name:) и нажмите **OK**.



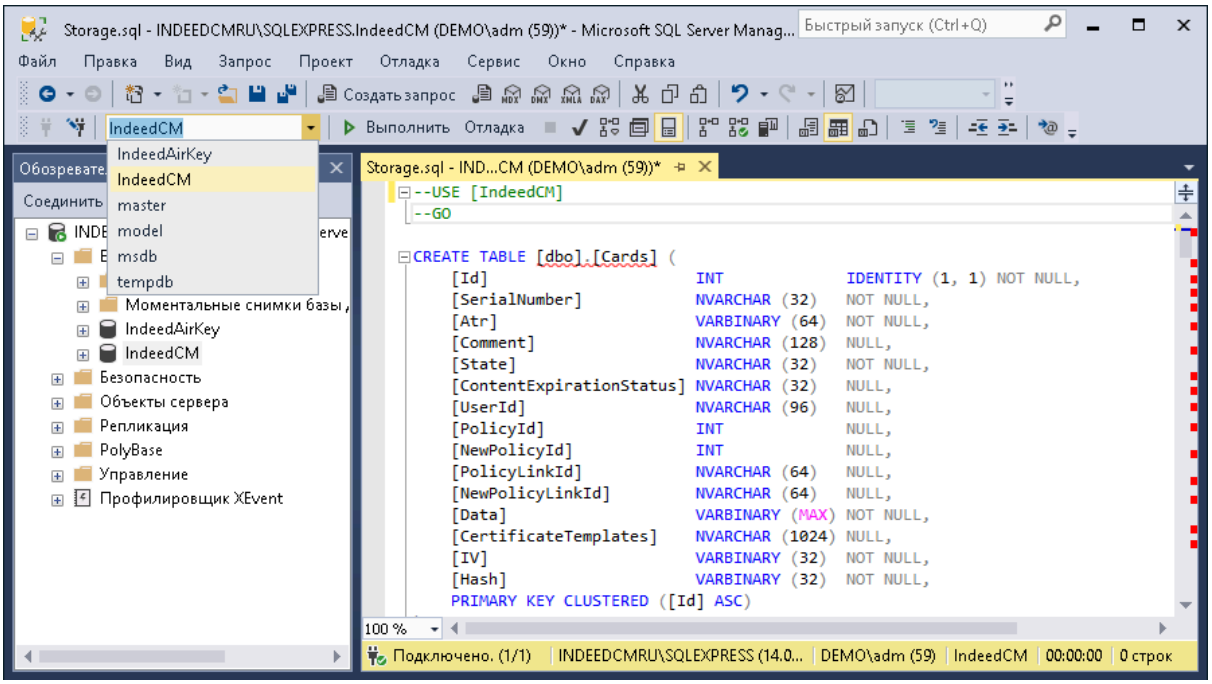
2. Используйте локальную учетную запись SQL или учетную запись Active Directory (например, **servicecm**) и наделите ее необходимыми правами для работы с созданной базой данных. Эта учетная запись будет использоваться для выполнения операций чтения и записи в базу данных. Подключение к базе с использованием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

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



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

1. Выберите меню **Файл** (File) → **Открыть** (Open) → **Файл**...(File...), укажите путь к файлу *Storage.sql* (*\IndeedCM.WindowsServer\Misc*) и нажмите **Открыть** (Open).
2. 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.
3. Нажмите **Выполнить** (Execute).

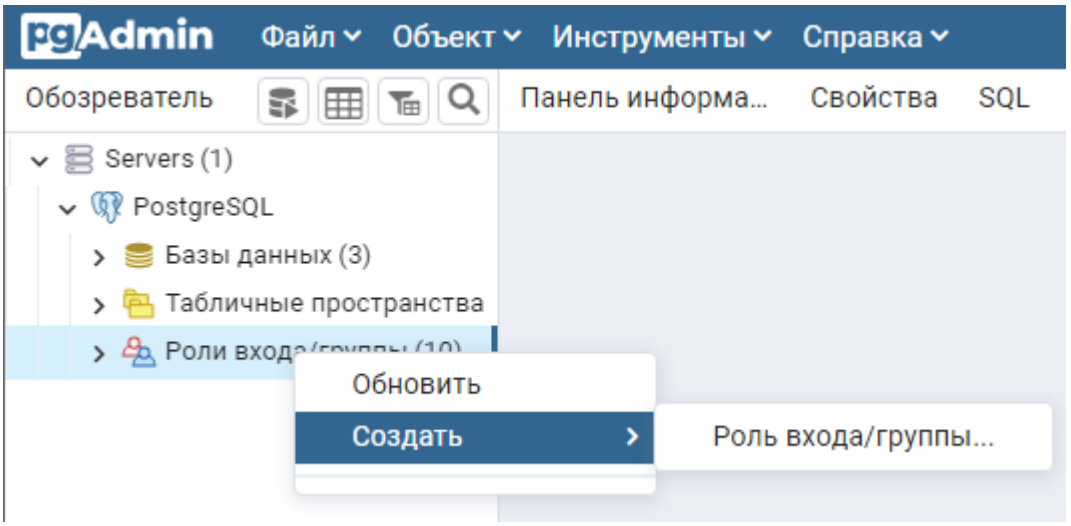


PostgreSQL и Postgres Pro

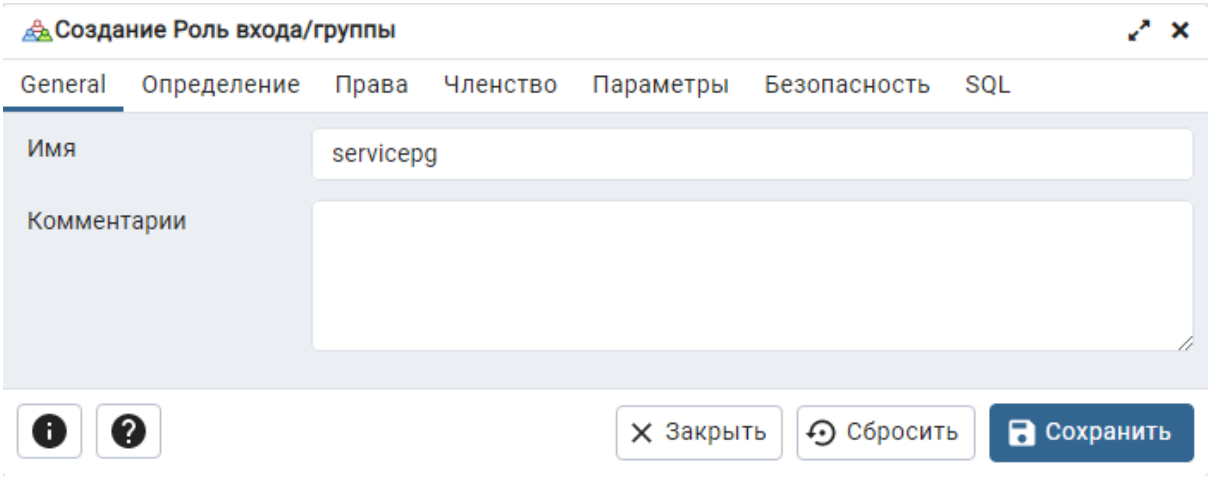
Создайте сервисную учетную запись и базу данных. Настройте удаленное подключение к базе данных.

Сервисная учетная запись

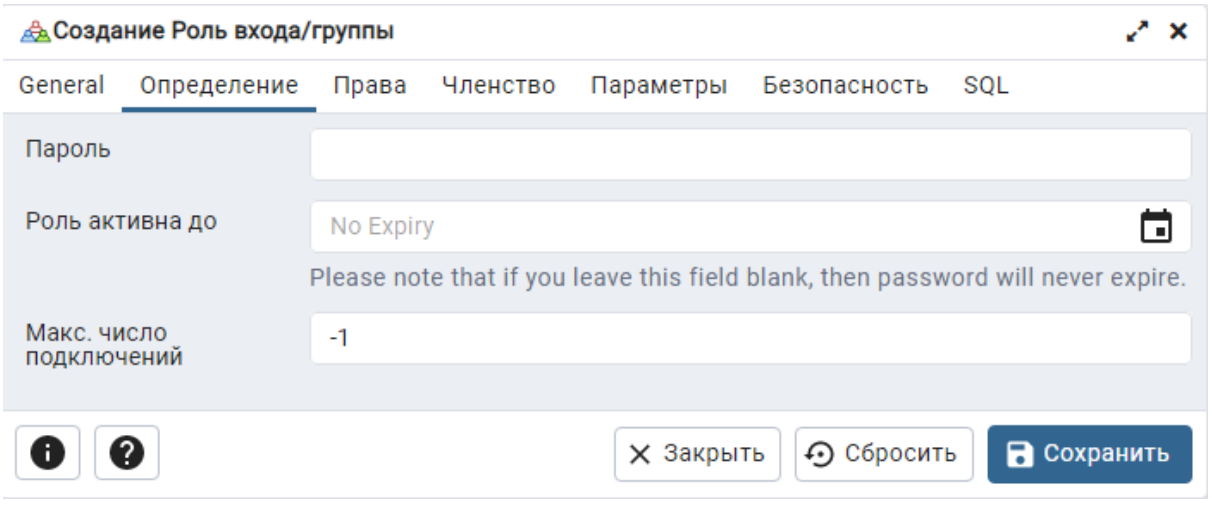
1. Откройте **pgAdmin**, укажите мастер пароль и подключитесь к серверу.
2. В разделе **Обозреватель** (Browser) правой кнопкой мыши нажмите по пункту меню **Роли входа/группы** (Login/Group Roles).
3. Выберите **Создать** → **Роль входа/группы** (Create → Login/Group Role…).



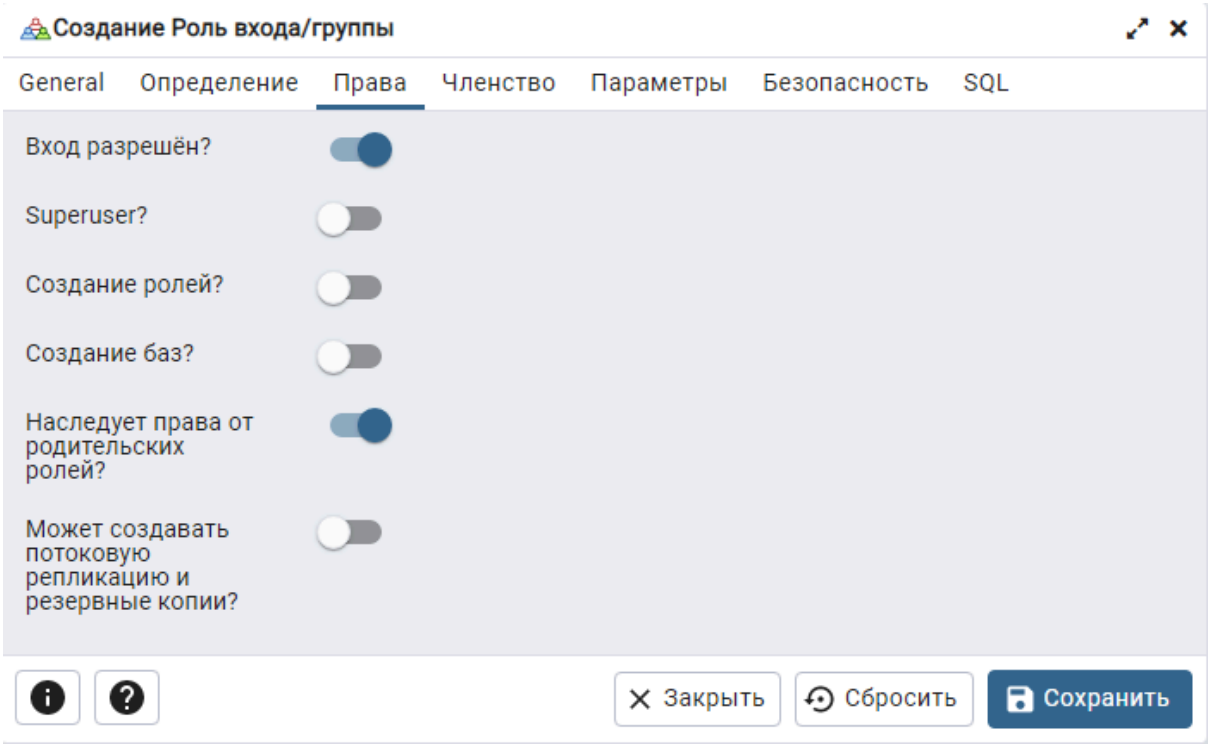
4. На вкладке **Общие** (General), в поле **Имя** (Name), укажите произвольное имя пользователя, например **servicepg**.



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 учетной записи требуется отключить срок действия пароля.



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

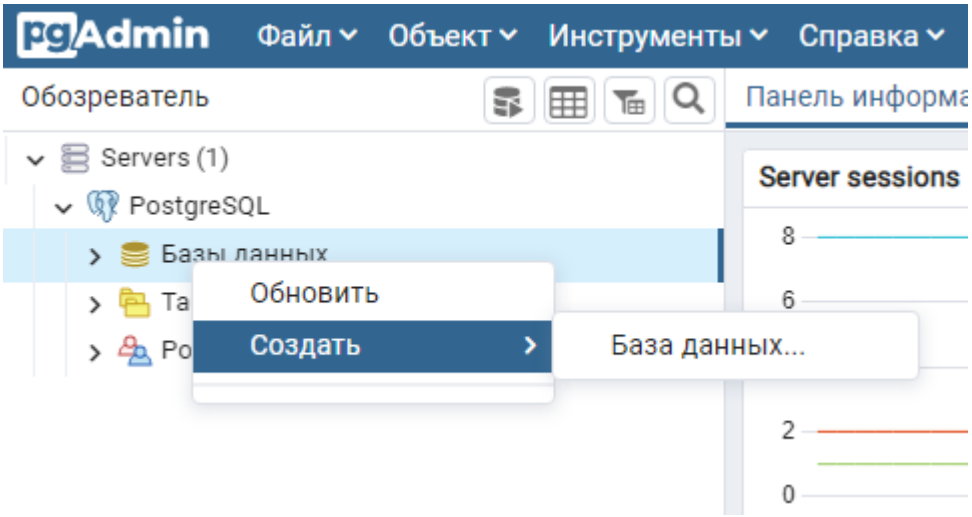


7. Оставьте остальные значения по умолчанию и нажмите **Сохранить** (Save).

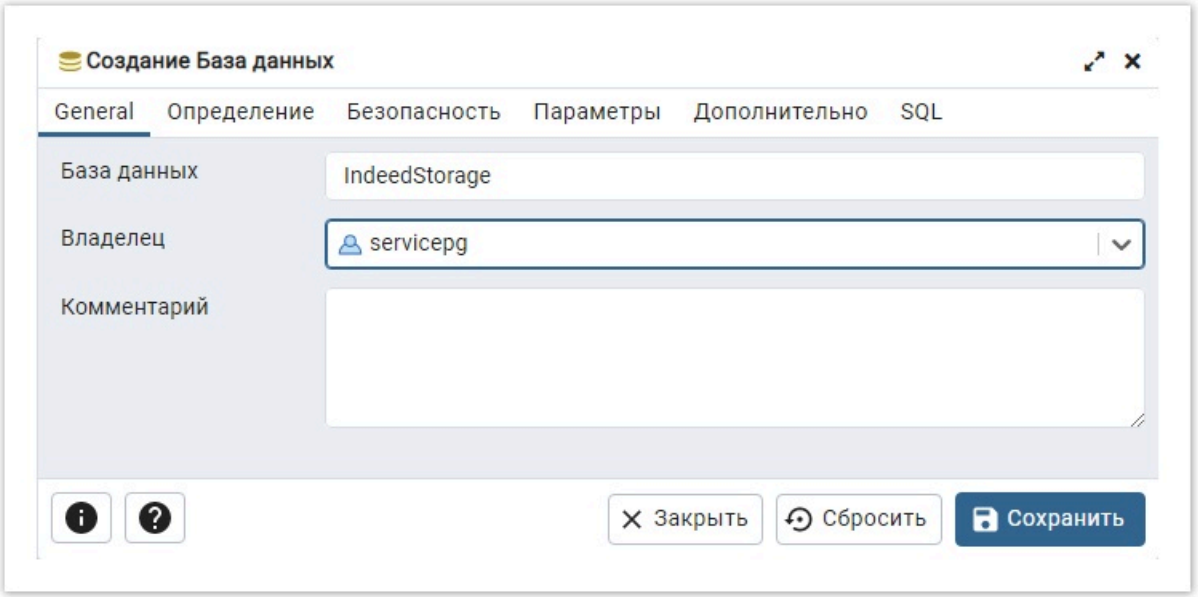
База данных

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

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

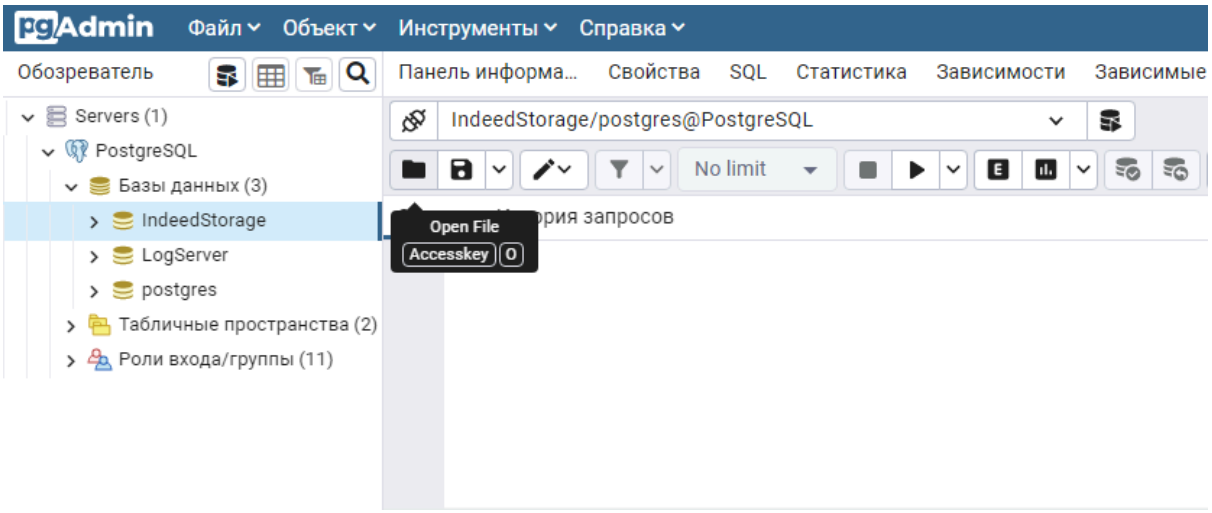


3. На вкладке **Общие** (General) укажите название базы данных в поле **База данных** (Database), например, **IndeedStorage**, выберите пользователя, созданного на первом этапе (**servicepg**) из списка **Владелец** (Owner) и нажмите **Сохранить** (Save).

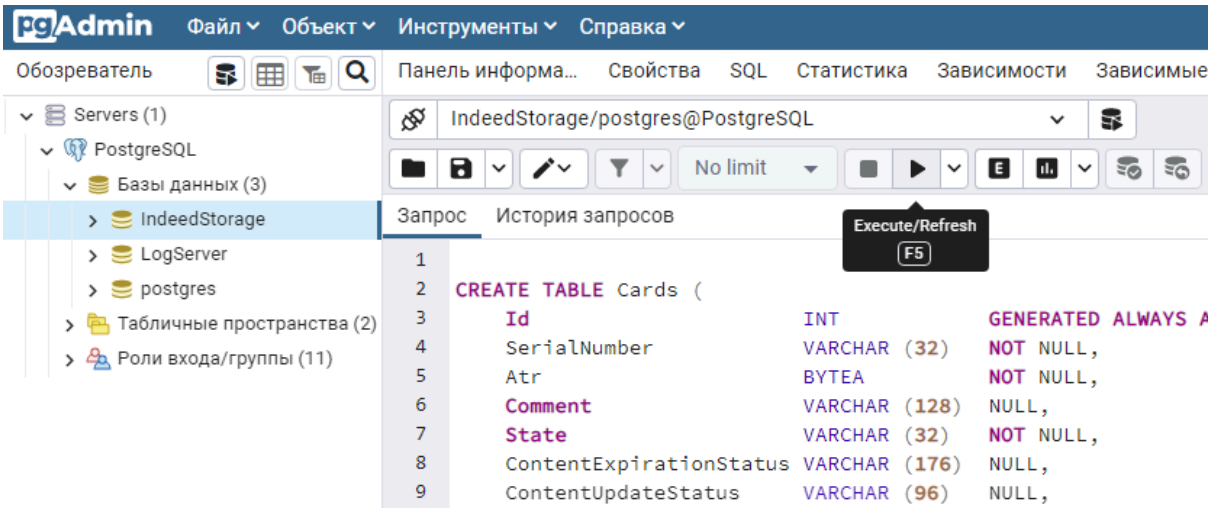


2. Выберите в **Обозревателе** (Browser) созданную базу данных (**IndeedStorage**) и выполните скрипт *Storage-Postgre.sql*:

   1. Выберите меню **Инструменты** (Tools) → **Запросник** (Query Tool).
   2. В меню запросника нажмите на значок  для открытия файла скрипта и укажите путь к файлу *Storage-Postgre.sql* (*\IndeedCM.WindowsServer\Misc*). Нажмите **Выбрать** (Select).

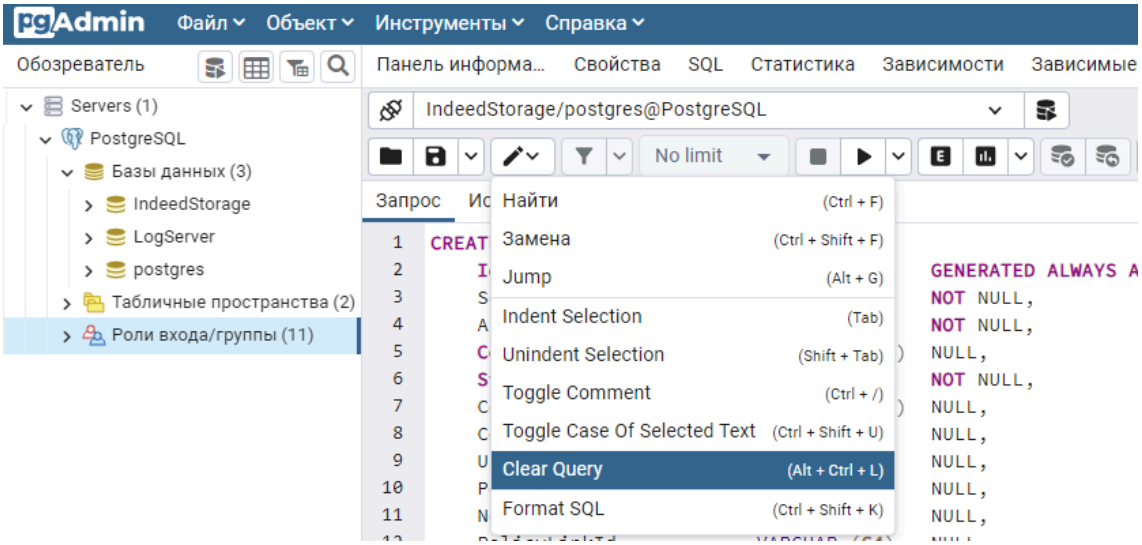


   3. В меню запросника нажмите на кнопку **Выполнить** (Execute/Refresh)  .



3. Предоставьте сервисной учетной записи привилегии на таблицы базы данных:

    1. Нажмите в меню запросника на кнопку  затем выберите **Clear Query**, чтобы очистить поле запроса к базе данных.



    2. Введите текст запроса, указав в запросе имя учетной записи:

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

> **ПРИМЕР ЗАПРОСА**
>
> ```
> GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA public TO servicepg;
> ```

3. В меню запросника нажмите на кнопку **Выполнить** (Execute/Refresh)  .

Удаленное подключение к базе данных

Откройте конфигурационный файл *pg_hba.conf*:

> **РАСПОЛОЖЕНИЕ ФАЙЛА PG_HBA.CONF**
>
> PostgreSQL:
>
> Для ОС Windows *C:\Program Files\PostgreSQL\<номер версии>\data*
> Для ОС Linux */etc/postgresql/<номер версии>/main*
>
> Postgres Pro:
>
> Для ОС Linux */var/lib/pgpro/<номер версии>/data*

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 удаленного сервера Indeed Certificate Manager.
- `METHOD` - метод аутентификации пользователя.

> **ПРИМЕР СТРОКИ**
>
> ```
> host IndeedStorage servicepg 192.200.1.0/24 md5
> ```

Центры сертификации

Microsoft CA

Настройка работы Microsoft CA

КриптоПро УЦ 2.0

Настройка работы КриптоПро УЦ 2.0

КриптоПро DSS 2.0

Настройка работы КриптоПро DSS 2.0

Валидата УЦ

Настройка работы Валидата УЦ

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

Перейдите к инструкции по подключению к центру сертификации Microsoft через компонент Indeed CM MSCA Proxy, если:

- центр сертификации Microsoft располагается за пределами домена, в котором развернут сервер Indeed CM под управлением ОС Windows;
- сервер Indeed CM установлен на ОС Linux.

Создание сервисной учетной записи для работы с Microsoft CA

Создайте сервисную учетную запись, от имени которой Indeed CM будет запрашивать сертификаты пользователей в центре сертификации (ЦС):

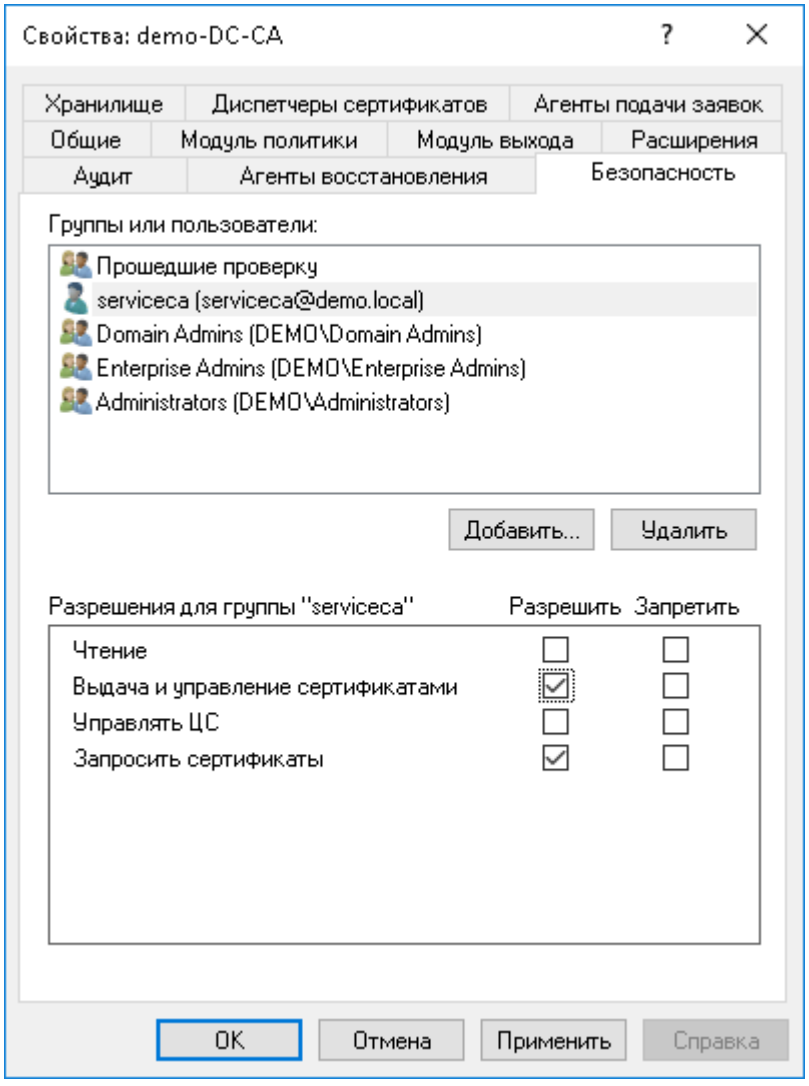
1. Создайте учетную запись пользователя в Active Directory.
2. Откройте оснастку **Центр сертификации** (Certification Authority), выберите центр сертификации и перейдите в его **Свойства** (Properties).
3. На вкладке **Безопасность** (Security) нажмите **Добавить** (Add) и укажите имя созданной учетной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

ПОДСКАЗКА

Включите разрешение **Управлять ЦС** (Manage CA), чтобы иметь возможность **Публиковать список отозванных сертификатов** при настройке шаблонов сертификатов для центра сертификации.

ПРЕДУПРЕЖДЕНИЕ

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



Настройка шаблонов сертификатов

Настройте шаблон сертификата **Агент регистрации** (Enrollment Agent) и шаблоны сертификатов пользователей.

Агент Регистрации

Для работы Microsoft CA с Indeed CM необходим шаблон сертификата **Агент регистрации** (Enrollment Agent).

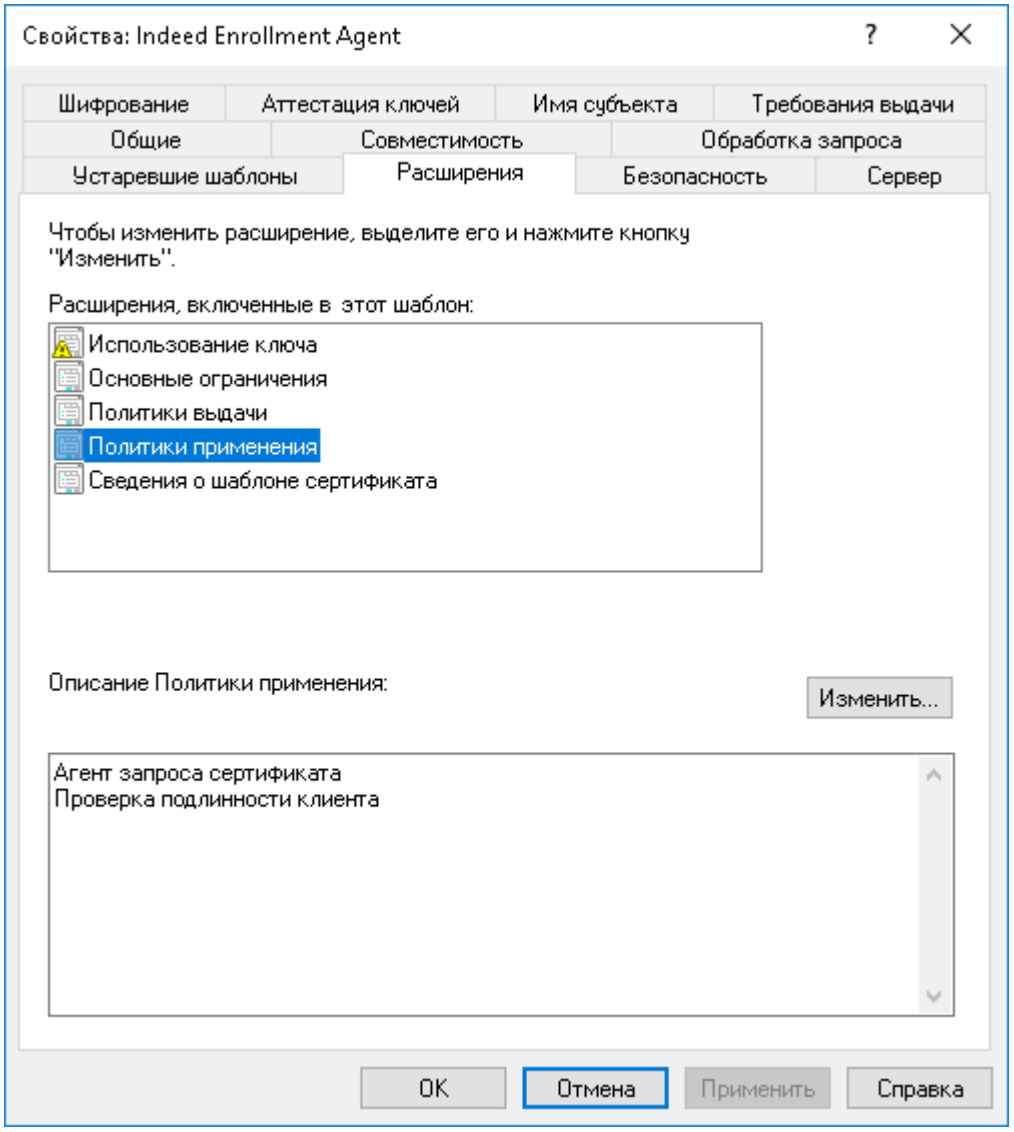
Сертификат **Агент регистрации** (Enrollment Agent) – это обязательный сертификат, который позволяет запрашивать сертификаты от имени конечных пользователей по шаблонам сертификатов, которые будут использоваться в Indeed CM.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Сертификат **Агент регистрации** (Enrollment Agent) добавляется в Indeed CM только один раз и выдается только на имя сервисной учетной записи.
>
> Убедитесь, что сертификат **Агент регистрации** не добавлен в политики использования устройств, иначе пользователи будут иметь возможность самостоятельно подписывать сертификаты в УЦ, что создает угрозу безопасности.

Создайте и настройте шаблон сертификата **Агент регистрации**:

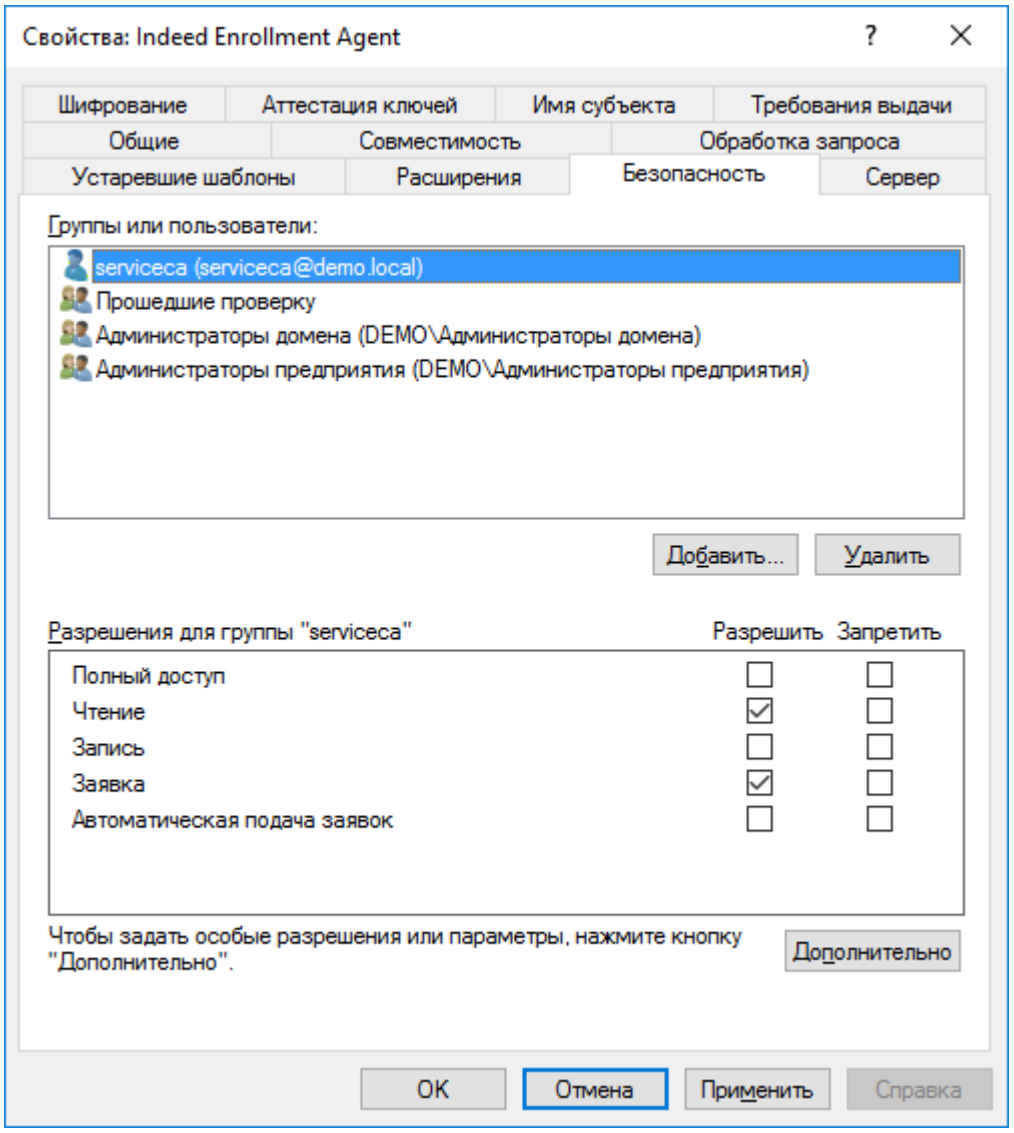
1. Откройте консоль управления **Центр сертификации** (Certification Authority).
2. Перейдите в раздел **Шаблоны сертификатов** (Certificate Templates), нажмите правой кнопкой мыши и выберите **Управление** (Manage).
3. Нажмите правой кнопкой мыши по шаблону **Агент регистрации** (Enrollment Agent) и выберите **Скопировать шаблон** (Duplicate Template).
4. Перейдите на вкладку **Общие** (General) и в поле **Отображаемое имя шаблона** (Template display name) введите **Indeed Enrollment Agent**. Измените **Период действия** (Validity period) в соответствии с потребностями вашей организации.
5. На вкладке **Шифрование** (Cryptography) в поле **Минимальный размер ключа** (Minimum key size) укажите необходимую длину ключа. Рекомендуемая длина ключа - 2048 бит.
6. На вкладке **Расширения** (Extensions) выберите расширение **Политики применения** (Application Policies) и нажмите **Изменить...** (Edit...)..
    1. Нажмите **Добавить...** (Add...) в появившемся окне.
    2. Выберите политику применения **Проверка подлинности клиента** (Client Authentication) из предложенного списка.

3. Нажмите **ОК**.



7. На вкладке **Безопасность** (Security) нажмите **Добавить...** (Add...).

    1. В поле **Введите имена выбираемых объектов** (Enter the object names to select) введите имя сервисной учетной записи (**serviceca**) и нажмите **ОК**.
    2. В разделе **Разрешения для группы** (Permissions for) установите флажок **Разрешить** (Allow) для привилегий **Чтение** (Read) и **Заявка** (Enroll).



8. Нажмите **ОК**, чтобы сохранить настройки шаблона.

Сертификаты пользователей

Подготовьте шаблоны сертификатов для различных назначений (политик применения), которые будут использоваться для выпуска сертификатов конечным пользователям Indeed CM.

Например, создайте и настройте шаблон сертификата пользователя **Вход со смарт-картой** (Smartcard Logon), который будет использоваться для выпуска сертификатов, предназначенных для входа в операционную систему по смарт-карте:

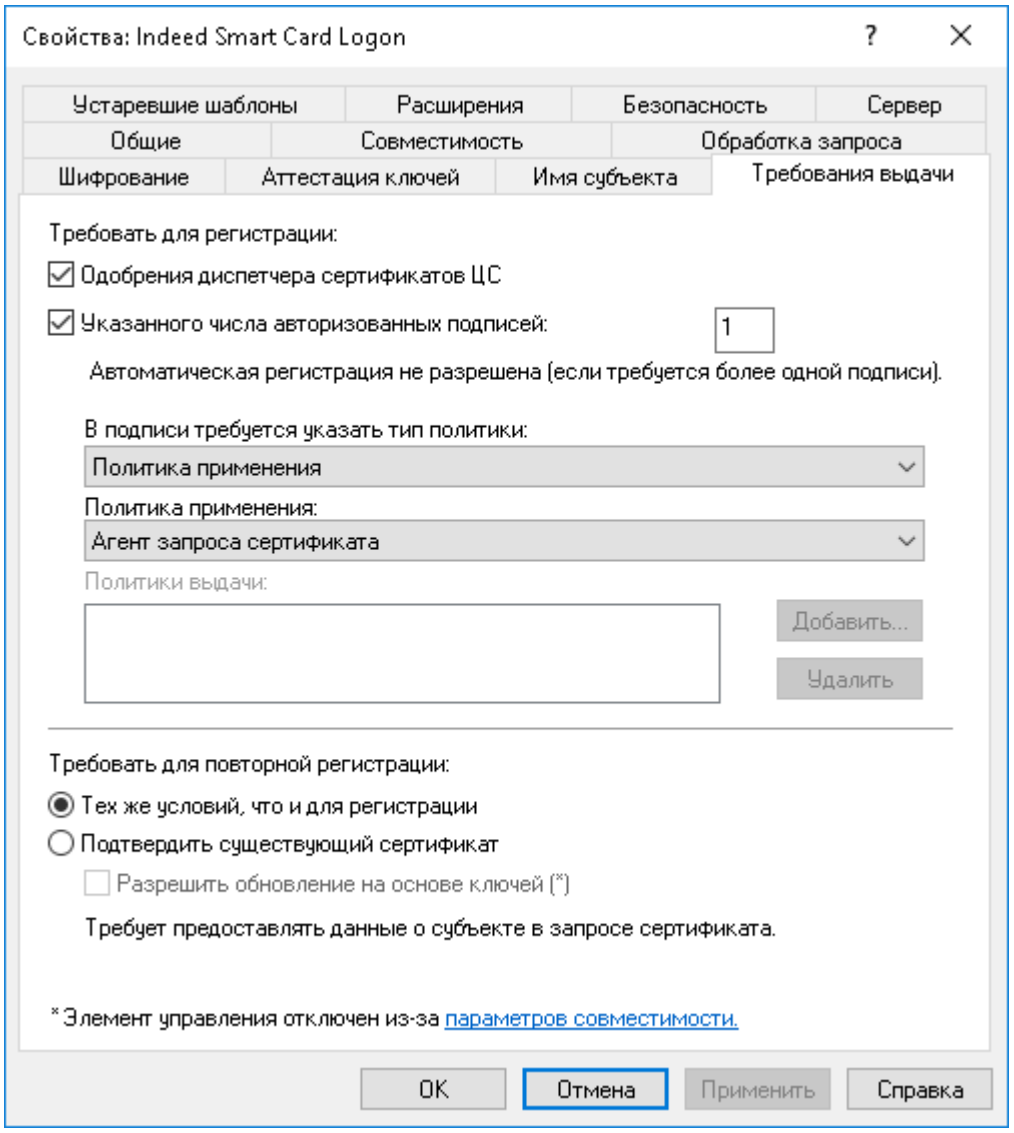
1. Откройте консоль управления **Центр сертификации** (Certification Authority).
2. Перейдите в раздел **Шаблоны сертификатов** (Certificate Templates), нажмите правой кнопкой мыши и выберите **Управление** (Manage).

3. Нажмите 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.

> **ПОДСКАЗКА**
>
> Опция доступна для Microsoft CA 2008/2008R2 и выше. В предыдущих версиях минимальный размер ключа настраивается на вкладке **Обработка запроса** (Request Handling).
> Обратите внимание на размер ключей шифрования, указанный в свойствах шаблонов сертификатов. Чтобы снизить риск несанкционированного доступа к конфиденциальной информации, компания Microsoft выпустила 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 блокируют ключи RSA меньше 1024 бит.

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

    1. Установите опцию **Одобрения диспетчера сертификатов ЦС** (CA certificate manager approval).
    2. Установите флажок **Указанного числа авторизованных подписей** (This number of authorized signatures) и укажите число подписей, равное **1** (значение по умолчанию).
    3. Выберите **Политики применения** (Application Policy) из списка **В подписи требуется указать тип политики** (Policy type required in signature).
    4. Выберите **Агент запроса сертификата** (Certificate Request Agent) из списка **Политика применения** (Application Policy).
    5. 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).



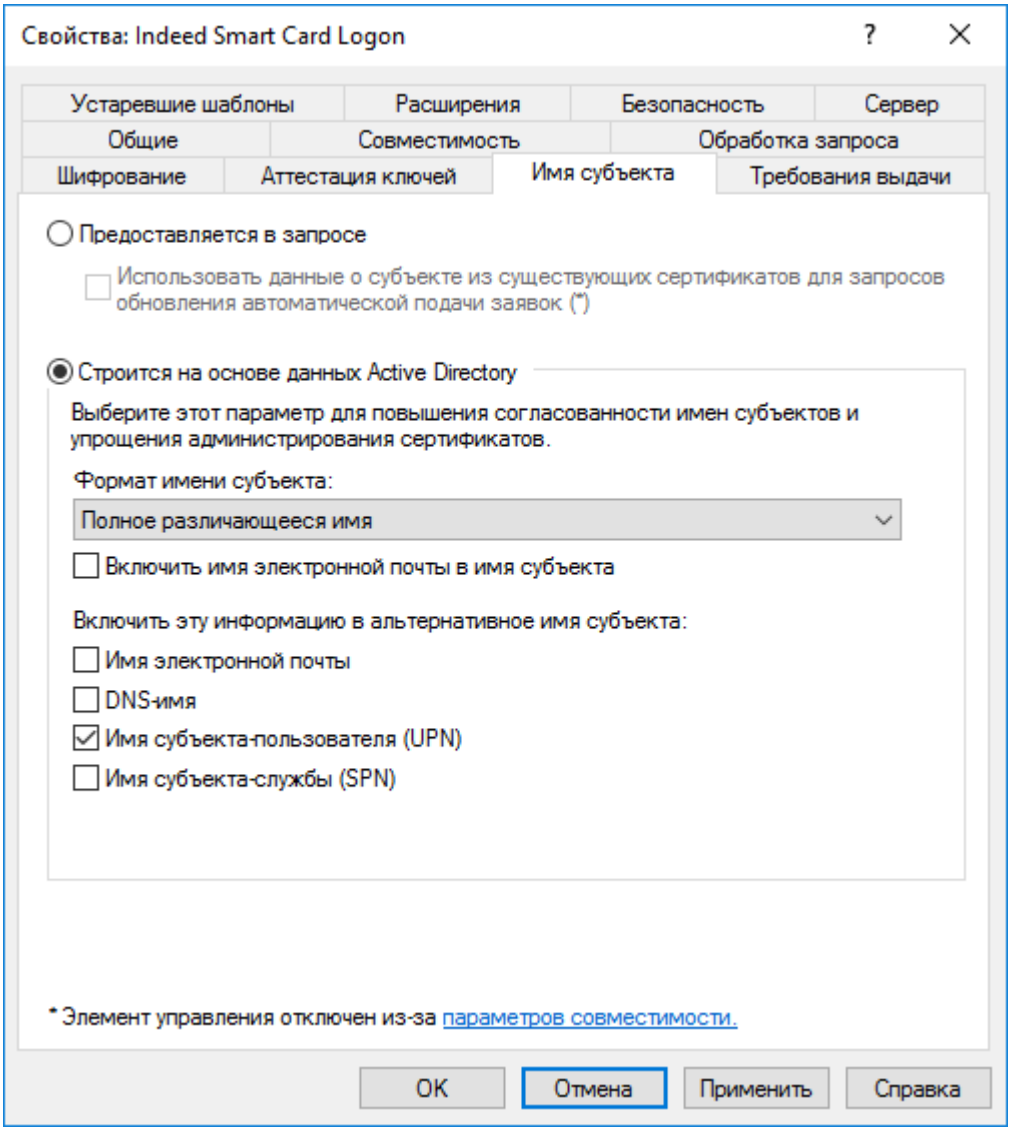
7. Перейдите на вкладку **Имя субъекта** (Subject Name). В зависимости от назначения сертификата выберите следующие настройки:

Строится на основе данных Active Directory

Выберите **Строится на основе данных Active Directory** (Build from this Active Directory information), если по данному шаблону будут формироваться сертификаты с назначением *Вход со смарт-картой* (SmartCard Logon, OID 1.3.6.1.4.1.311.20.2) и *Проверка подлинности клиента* (Client Authentication, OID 1.3.6.1.5.5.7.3.2).

1. Выберите **Полное различающееся имя** (Fully distinguished name) из списка **Формат имени субъекта** (Subject name format).
2. Установите флажок **Имя субъекта-пользователя (UPN)** (User principal name (UPN)).

3. 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 по данному шаблону будут выпускаться сертификаты для пользователей, у которых не указан адрес электронной почты в Active Directory.



Предоставляется в запросе

Выберите **Предоставляется в запросе** (Supply in the request), если по данному шаблону будут формироваться следующие сертификаты:

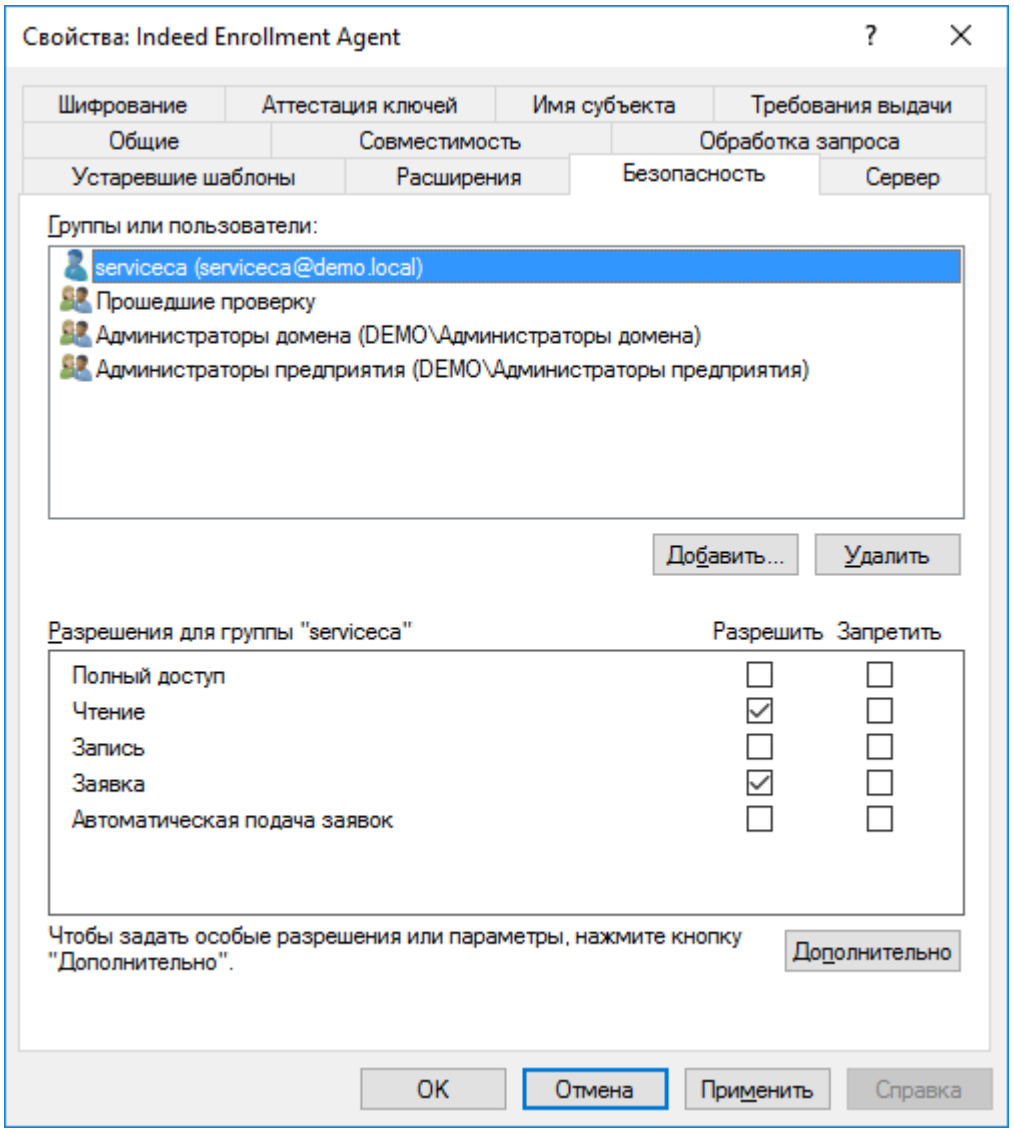
- сертификаты для защиты электронной почты (электронная подпись, шифрование) с назначением *Защита электронной почты* (Secure Email, OID 1.3.6.1.5.5.7.3.4),
- сертификаты с назначением *Подпись документов* (Document Signing, OID 1.3.6.1.4.1.311.10.3.12),
- ГОСТ-сертификаты для защиты электронной почты и подписи документов.

> **ПРИМЕЧАНИЕ**
>
> Имя субъекта сертификата будет сформировано из запроса на сертификат. Атрибуты для формирования имени субъекта (Subject) и альтернативного имени субъекта (Subject Alternative Name) можно указать в Консоли управления: **Конфигурация → Политики → Настройки PKI → Microsoft →** Шаблоны.

8. На вкладке **Безопасность** (Security) нажмите **Добавить...** (Add...).

    1. В поле **Введите имена выбираемых объектов** (Enter the object names to select) введите имя сервисной учетной записи (**serviceca**) и нажмите **ОК**.
    2. В разделе **Разрешения для группы** (Permissions for) установите флажок **Разрешить** (Allow) для привилегий **Чтение** (Read) и **Заявка** (Enroll).

> **ПРЕДУПРЕЖДЕНИЕ**
>
> Выдайте аналогичные разрешения сервисной учетной записи для всех шаблонов сертификатов, которые будут использоваться в Indeed CM.



9. Нажмите **ОК**, чтобы сохранить настройки шаблона.

Добавление шаблонов сертификатов

1. Откройте консоль управления **Центр сертификации** (Certification Authority) и дважды нажмите на имя ЦС.
2. Нажмите 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. Выберите шаблон обязательного сертификата **Indeed Enrollment Agent**, а также все остальные шаблоны сертификатов (например, **Indeed Smart Card Logon**), которые будут выпускаться конечным пользователям системы.
5. Нажмите **ОК**.

Выпуск сертификата Агент регистрации

Сервисный пользователь с сертификатом **Агент регистрации** (Enrollment Agent) необходим в Indeed CM, чтобы от его имени Indeed CM запрашивал и подписывал запросы на сертификаты для всех остальных пользователей.

Сертификат можно создать:

- с помощью утилиты **Cm.CertEnroll.MsCA**;
- в диспетчере сертификатов пользователя.

Cm.CertEnroll.MsCA

Утилита **Cm.CertEnroll.MsCA** находится в каталоге *IndeedCM.WindowsServer\Misc* дистрибутива Indeed CM.

Для выпуска сертификата с назначением Enrollment Agent запустите от имени учетной записи с правами локального администратора на сервере Indeed CM утилиту *Cm.CertEnroll.MsCA.exe* с параметрами `/e userName password` и `/t templateName`, где:

- `userName` – имя сервисной учетной записи для работы с центрами сертификации (**serviceca**);
- `password` – пароль сервисной учетной записи;
- `templateName` – имя шаблона сертификата Агента регистрации. Поддерживаются шаблоны с любыми именами, имеющие **Улучшенный ключ** (Extended Key Usage) **Агент запроса сертификата** (Certificate Request Agent).

Пример

```
Cm.CertEnroll.MsCA.exe /e serviceca p@ssw0rd
/t=”IndeedEnrollmentAgent”
```

Результат работы утилиты

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

Если запрос на сертификат должен быть одобрен оператором удостоверяющего центра (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: lr-IndeedEnrollmentAgent-175d9490-7481-4a29-b567-
503d39747354
Please accept request and then install certificate.
```

После одобрения запроса в УЦ необходимо выполнить команду для установки сертификата в хранилище. Для этого запустите утилиту *Cm.CertEnroll.MsCA.exe* с параметром `/i userName password requestId containerName`, где:

- `userName` – имя сервисной учетной записи для работы с центрами сертификации;
- `password` – пароль сервисной учетной записи;
- `requestId` – порядковый номер запроса на сертификат;
- `containerName` – имя ключевого контейнера.

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

Если вам необходимо выпустить сертификат **Агент регистрации** (Enrollment Agent) с определенного центра сертификации (например, если в домене несколько центров сертификации), запустите утилиту с параметром `/c`, в котором укажите имя ЦС в формате `CAMachineName\CAName`, где:

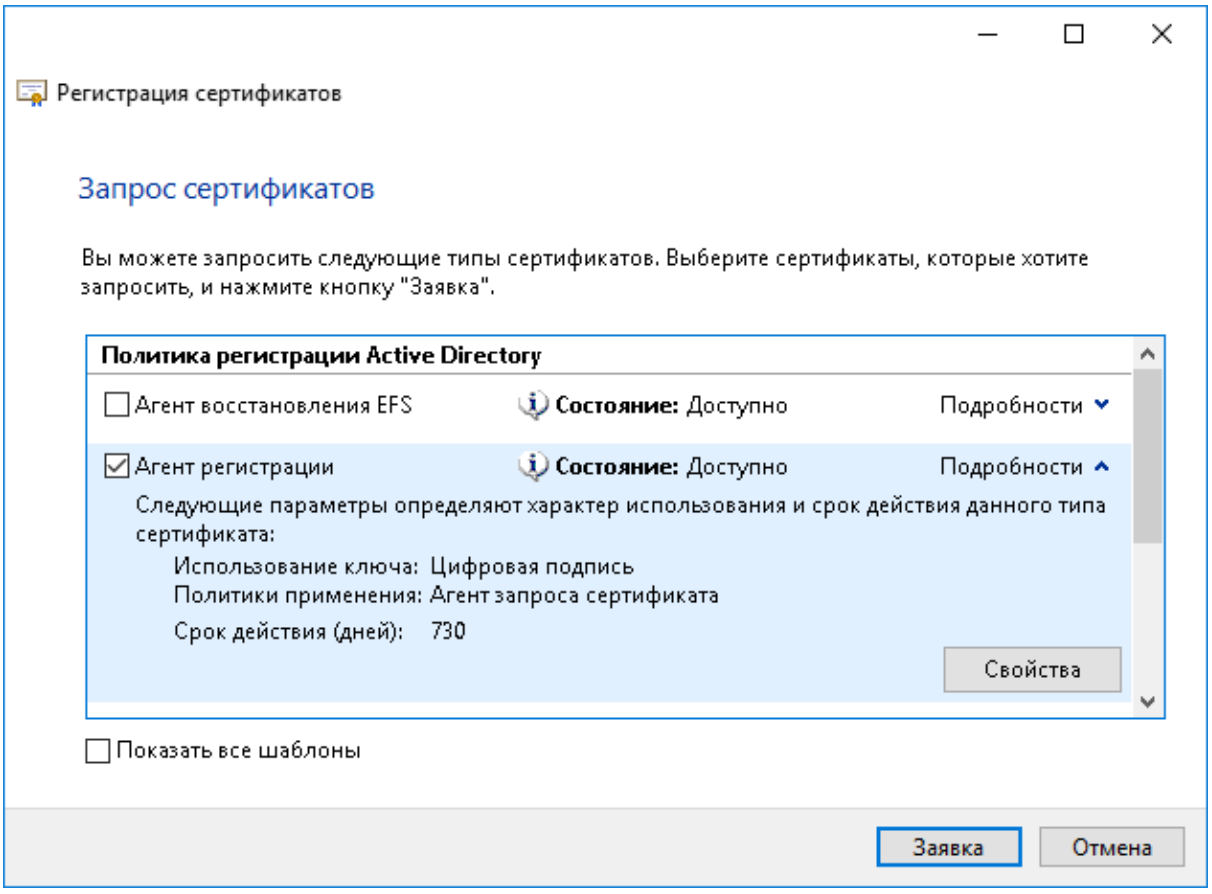
- `CAMachineName` – DNS-имя сервера с ролью центра сертификации;
- `CAName` – имя центра сертификации.

Пример запуска с указанием Центра сертификации

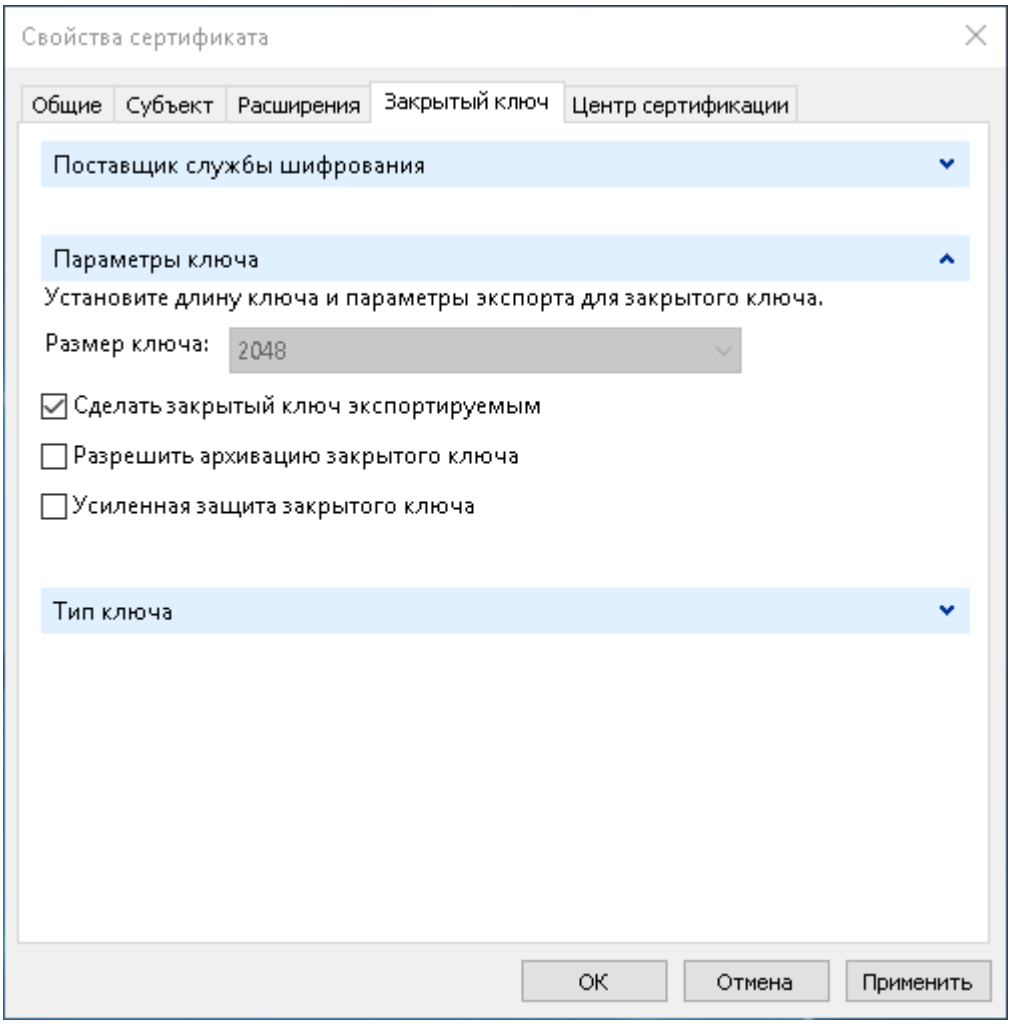
```
Cm.CertEnroll.MsCA.exe /e serviceca p@ssw0rd
/t=”IndeedEnrollmentAgent” /c=”msca.demo.local\Indeed-Demo-CA”
```

Диспетчер сертификатов

1. Выполните вход в систему 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 перейдите в **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).

    1. Перейдите в оснастку **Сертификаты** (Certificates) компьютера и нажмите правой кнопкой мыши на сертификате.
    2. Выберите **Все задачи** (All tasks) → **Управление закрытыми ключами...** (Manage Private Keys...).
    3. Нажмите **Добавить** (Add), укажите сервисную учетную запись (**serviceca**).
    4. Выставите право **Полный доступ** (Full control).
    5. Нажмите **Применить** (Apply).

Подключение к Microsoft CA через Indeed CM MS CA Proxy

Indeed Certificate Manager может взаимодействовать с центрами сертификации Microsoft, которые находятся за пределами домена сервера Indeed CM. Например, конфигурация с несколькими независимыми доменами с самостоятельными центрами сертификации в каждом, а Indeed CM развернут только в одном из этих доменов.

При выпуске сертификата Indeed CM обращается к Indeed CM MS CA Proxy, а тот, используя сертификат Агента Регистрации, передает запрос на целевой центр сертификации.

Приложение MS CA Proxy можно установить только на систему под управлением ОС Windows. Системные требования для установки совпадают с требованиями для установки серверных компонентов.

Выберите инструкцию по установке и настройке приложения Indeed CM MS CA Proxy в зависимости от операционной системы, где установлен сервер Indeed CM:

Windows

1. Создайте во внешнем для системы домене сервисную учетную запись для работы с центром сертификации Microsoft.
2. Настройте для сервисной учетной записи шаблон **Агент регистрации** и выпустите для этой учетной записи сертификат по этому шаблону. Сертификат **Агент регистрации** должен располагаться в **Хранилище сертификатов рабочей станции** (Local computer), на которой установлен компонент Indeed CM MS CA Proxy.
3. Установите компонент *IndeedCM.MSCA.Proxy-<номер версии>.x64.ru-ru.msi* из каталога *IndeedCM.WindowsServer* дистрибутива системы на рабочую станцию в домене с внешним УЦ.
4. Запустите редактор Блокнот от имени администратора и откройте файл конфигурации MS CA Proxy — *C:\inetpub\wwwroot\cm\mscaproxy\Web.config*.
5. В секции `caProxySettings` укажите :

- Имя центра сертификации в параметре `ca` в формате `CAMachineName\CAName`, где:
  - `CAMachineName` – DNS-имя сервера с ролью центра сертификации.
  - `CAName` – имя центра сертификации.
- Данные учетной записи (логин и пароль), обладающей сертификатом **Агент регистрации** в параметрах `userName` и `password`.

- **Отпечаток** (Thumbprint) сертификата **Агент регистрации** в параметре `enrollmentAgentCertificateThumbprint`.

```
<caProxySettings ca="servercm.external.com\EXTERNAL-CA"
userName="EXTERNAL\serviceca" password="p@ssw0rd"
enrollmentAgentCertificateThumbprint="dbd1859d27395860843643ebe17e2
```

6. Задайте параметры аутентификации. Для подключения Windows-сервера Indeed CM к приложению MS CA Proxy используется аутентификация Windows. В параметре `allow users` укажите сервисную учетную запись из домена, где установлен Indeed CM MSCA Proxy.

```
<authentication mode="Windows" />
<authorization>
   <deny users="?" />
   <allow users="EXTERNAL\serviceca" />
   <deny users="*" />
</authorization>
```

7. Сохраните изменения в файле и закройте файл конфигурации.
8. Перезапустите пул приложения Indeed CM MS CA Proxy, чтобы сохранить изменения:

    1. Откройте Диспетчер служб IIS (Internet Information Services Manager) и в левом меню выберите **Пул приложений IIS** (Application pools).
    2. Выберите приложение Indeed CM MS CA Proxy и в правом меню нажмите **Перезапуск** (Recycle).

Linux

1. Создайте во внешнем для системы домене сервисную учетную запись для работы с центром сертификации Microsoft.
2. Настройте для сервисной учетной записи шаблон **Агент регистрации** и выпустите для этой учетной записи сертификат по этому шаблону. Сертификат **Агент регистрации** должен располагаться в **Хранилище сертификатов рабочей станции** (Local computer), на которой установлен компонент Indeed CM MS CA Proxy.

3. Установите компонент *IndeedCM.MSCA.Proxy-<номер версии>.x64.ru-ru.msi* из каталога *IndeedCM.LinuxServer* дистрибутива системы на рабочую станцию в домене с внешним УЦ.
4. Запустите редактор Блокнот от имени администратора и откройте файл конфигурации MS CA Proxy — *C:\inetpub\wwwroot\cm\mscaproxy\Web.config*.
5. В секции `caProxySettings` укажите :

- Имя центра сертификации в параметре `ca` в формате `CAMachineName\CAName`, где:
  - `CAMachineName` – DNS-имя сервера с ролью центра сертификации.
  - `CAName` – имя центра сертификации.
- Данные учетной записи (логин и пароль), обладающей сертификатом **Агент регистрации** в параметрах `userName` и `password`.
- **Отпечаток** (Thumbprint) сертификата **Агент регистрации** в параметре `enrollmentAgentCertificateThumbprint`.

```
<caProxySettings ca="servercm.external.com\EXTERNAL-CA"
userName="EXTERNAL\serviceca" password="p@ssw0rd"
enrollmentAgentCertificateThumbprint="dbd1859d27395860843643ebe17e2
```

6. Задайте параметры аутентификации. Для подключения Linux-сервера Indeed CM к MS CA Proxy используется аутентификация по сертификатам.

- В секции `appSettings` укажите значение **True** в параметре `authorizeByCertificate`. В параметре `allowedCertificateThumbprints` укажите отпечаток клиентского сертификата, разрешенного к предъявлению сервером Indeed CM.

```
<appSettings>
   <add key="authorizeByCertificate" value="true" />
   <add key="allowedCertificateThumbprints"
value="aba8b93d73343f2182e3c1c40482b2ae2d75b6ec" />
</appSettings>
```

- Укажите значение **None** в параметре `authentication` и закомментируйте секцию `authorization`.

```
<authentication mode="None" />
<!--
   <authorization>
       <deny users="?"/>
       <allow users="*" />
       <deny users="*" />
   </authorization>
-->
```

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Убедитесь, что выполнены следующие требования для аутентификации по сертификатам в ОС Linux:
>
> - поле **Улучшенный ключ** (Enhanced Key Usage) сертификата содержит значение **Проверка подлинности клиента** (Client Authentication).
> - сертификат установлен в хранилище сертификатов сервера Indeed CM.

7. Сохраните изменения в файле и закройте файл конфигурации.
8. Настройте MS CA Proxy для приема сертификатов клиента - сервера Indeed CM. Для этого откройте Диспетчер служб IIS (Internet Information Services Manager) и выполните следующие действия:

    1. Выберите приложение MS CA Proxy и перейдите в **Параметры SSL** (SSL Settings).
    2. В списке **Сертификаты клиента** (Client certificates) выберите значение **Принимать** (Accept).
    3. Перезапустите пул приложения Indeed CM MS CA Proxy, чтобы сохранить изменения. В левом меню выберите **Пул приложений IIS** (Application pools). Выберите приложение Indeed CM MS CA Proxy и в правом меню нажмите **Перезапуск** (Recycle).

КриптоПро УЦ 2.0

Для настройки работы Indeed Certificate Manager с КриптоПро УЦ 2.0 выполните следующие действия:

1. Создайте сервисную группу 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.

Если каталог пользователей расположен только в Центре Регистрации КриптоПро УЦ 2.0, настройте аутентификацию в веб-сервисах Indeed CM по сертификатам.

Создание сервисной учетной записи для работы с КриптоПро УЦ

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 CM.

1. Запустите от имени администратора браузер Internet Explorer, Google Chrome, Chromium или Яндекс.Браузер 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:
    1. Укажите в заявке имя сервисной учетной записи и e-mail.
    2. Запомните или запишите выданный ЦР идентификатор и временный пароль.
    3. Укажите дополнительную информацию или пропустите этот шаг.
    4. Завершите регистрацию.
3. **Одобрите запрос** на регистрацию нового пользователя 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 Indeed CM создайте шаблон сертификата, на основе которого впоследствии будет выпущен сертификат агента подачи заявок:

1. Откройте узел **Шаблоны сертификатов** в утилите **Диспетчер УЦ**.
2. Создайте шаблон сертификата **Indeed CM Service User** на основе шаблона **Пользователь:**

    1. Укажите **Срок действия** сертификата.
    2. В разделе **Параметры создания ключа** выберите **Ключ принадлежит: Компьютеру** и включите опцию **Разрешить экспорт ключа**.
    3. В разделе **Настройка расширений сертификата** выберите **Улучшенный ключ (2.5.29.37)** и нажмите **Изменить...**.
    4. Нажмите **Изменить...** в окне **Настройки расширения**.
    5. Поставьте отметку напротив пункта **Агент запроса сертификата** и два раза нажмите **ОК**.

3. **Примените** изменения в шаблоне.
4. Нажмите правой кнопкой мыши по корневому узлу **Роли УЦ** и нажмите **Обновить**.

Выпуск сертификата агента подачи заявок

Чтобы выпустить сертификат агента подачи заявок:

1. С рабочей станции, на которой установлен сервер Indeed CM, выполните вход в личный кабинет пользователя КриптоПро 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 КриптоПро.

5. Загрузите и сохраните изготовленный сертификат.

Для инсталляций с несколькими серверами Indeed CM

Если в инфраструктуре развернуто несколько серверов Indeed CM, то сертификат сервисного пользователя необходимо выпустить с экспортируемым закрытым ключом. Перенесите этот сертификат и его контейнер закрытого ключа на каждый сервер Indeed CM.

6. Установите сертификат в контейнер локального хранилища рабочей станции.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Не устанавливайте пароль на контейнер закрытого ключа сертификата агента подачи заявок при установке сертификата.

7. Выдайте системе **права на чтение закрытого ключа сертификата сервисной учетной записи**, который был установлен на предыдущем шаге.

    1. Перейдите в оснастку **Сертификаты** (Certificates) компьютера, на котором установлен сервер Indeed CM.
    2. Нажмите правой кнопкой мыши на сертификате, выберите **Все задачи** (All tasks) → **Управление закрытыми ключами...** (Manage Private Keys...).
    3. Нажмите **Добавить** (Add), укажите сервер в меню **Размещение** (Location), укажите локальную группу **IIS_IUSRS** в поле **Введите имена выбранных объектов** (Enter the object names to select), нажмите **Проверить имена** (Check Names) и **ОК**.
    4. Выставите права **Полный доступ** (Full Control) и **Чтение** (Read).
    5. Нажмите **Применить** (Apply).

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

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

Настройка аутентификации в веб-сервисах Indeed CM по сертификатам

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

1. Зарегистрируйте нового пользователя КриптоПро УЦ. В качестве имени пользователя укажите полное имя рабочей станции, на которой установлен сервер Indeed CM.
2. С сервера Indeed CM войдите в личный кабинет пользователя Крипто Про УЦ по идентификатору и временному паролю учетной записи сервера.
3. Создайте запрос на сертификат. Укажите 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 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.

    1. Запустите оснастку **Сертификаты** (Certificates) для локального компьютера на сервере Indeed CM.
    2. Перейдите в раздел **Личные** (Personal) → **Сертификаты** (Certificates).
    3. Нажмите правой кнопкой мыши на сертификат, установленный при помощи КриптоПро CSP, выберите **Все задачи** (All tasks) → **Управление закрытыми ключами...**(Manage Private Keys...).
    4. Нажмите **Добавить** (Add), укажите сервер в меню **Размещение** (Location), укажите локальную группу **IIS_IUSRS** в поле **Введите имена выбранных объектов** (Enter the object names to select), нажмите **Проверить имена** (Check Names) и **ОК**.
    5. Выставите права **Полный доступ** (Full Control).
    6. Нажмите **Применить** (Apply).

КриптоПро DSS 2.0

ПАК "КриптоПро DSS" версии 2.0 предназначен для защищенного хранения закрытых ключей пользователей и для удаленного выполнения операций по созданию электронной подписи.

Интеграция с Indeed Certificate Manager позволяет выпускать средства облачной аутентификации и вести их централизованный учет. 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

> **ПРИМЕЧАНИЕ**
>
> 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 в комплект поставки ПАК "КриптоПро DSS".

Настройка интеграции

Для работы с КриптоПро DSS используется учетная 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 КриптоПро УЦ 2.0 и корневой сертификат DSS в **Доверенные корневые центры сертификации** (Trusted Root Certification Authorities) на сервере Indeed CM.
3. Выдайте системе **права на чтение закрытого ключа сертификата Оператора DSS**.

    1. Перейдите в оснастку **Сертификаты** (Certificates) компьютера, на котором установлен сервер Indeed CM.
    2. Нажмите правой кнопкой мыши на сертификат, выберите **Все задачи** (All tasks) → **Управление закрытыми ключами...**(Manage Private Keys...).
    3. Нажмите **Добавить** (Add), укажите сервер в меню **Размещение** (Location), укажите локальную группу **IIS_IUSRS** в поле **Введите имена выбранных объектов** (Enter the object names to select), нажмите **Проверить имена** (Check Names) и **ОК**.
    4. Выдайте право **Полный доступ** (FullControl).
    5. Нажмите **Применить** (Apply).

4. Выдайте права на папку с пользователями в КриптоПро УЦ 2.0 для учетной записи **Оператор DSS**:

    1. Создайте группу безопасности, например **DSS Operators**, и добавьте в нее учетную запись **Оператор DSS**.
    2. Откройте свойства папки, где будут располагаться пользователи DSS, перейдите на вкладку Безопасность и добавьте созданную группу **DSS Operators**.
    3. Выдайте группе следующие права:

Права 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

Наименование разрешения	Тип объекта	Комментарий
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

Для настройки работы Indeed Certificate Manager с Валидата УЦ выполните следующие действия:

1. Настройте режим работы с Валидата УЦ: офлайн или онлайн.

В офлайн-режиме в УЦ обрабатываются запросы пользователей в формате PKCS#10, после чего сертификаты выдаются пользователям. В онлайн-режиме работы с Валидата УЦ сервер Indeed CM заменяет собой АРМ Оператора ЦР Валидата.

2. Настройте шаблоны сертификатов пользователей.

Офлайн-режим работы

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

- корневой и промежуточные сертификаты Валидата УЦ
- актуальный файл Списка Отозванных Сертификатов (COC)
- подкаталог для входящих незащищенных запросов пользователей (в формате PKCS#10)
- подкаталог сертификатов для выдачи конечным пользователям

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

Онлайн-режим работы

Для работы Indeed Certificate Manager с Валидата УЦ в онлайн-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.

> **ПРИМЕЧАНИЕ**
>
> 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 значения **Оператор Центра Регистрации** (OID: 1.3.6.1.4.1.10244.6.1) и **Проверка подлинности TLS клиента** (OID: 1.3.6.1.5.5.7.3.2).

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

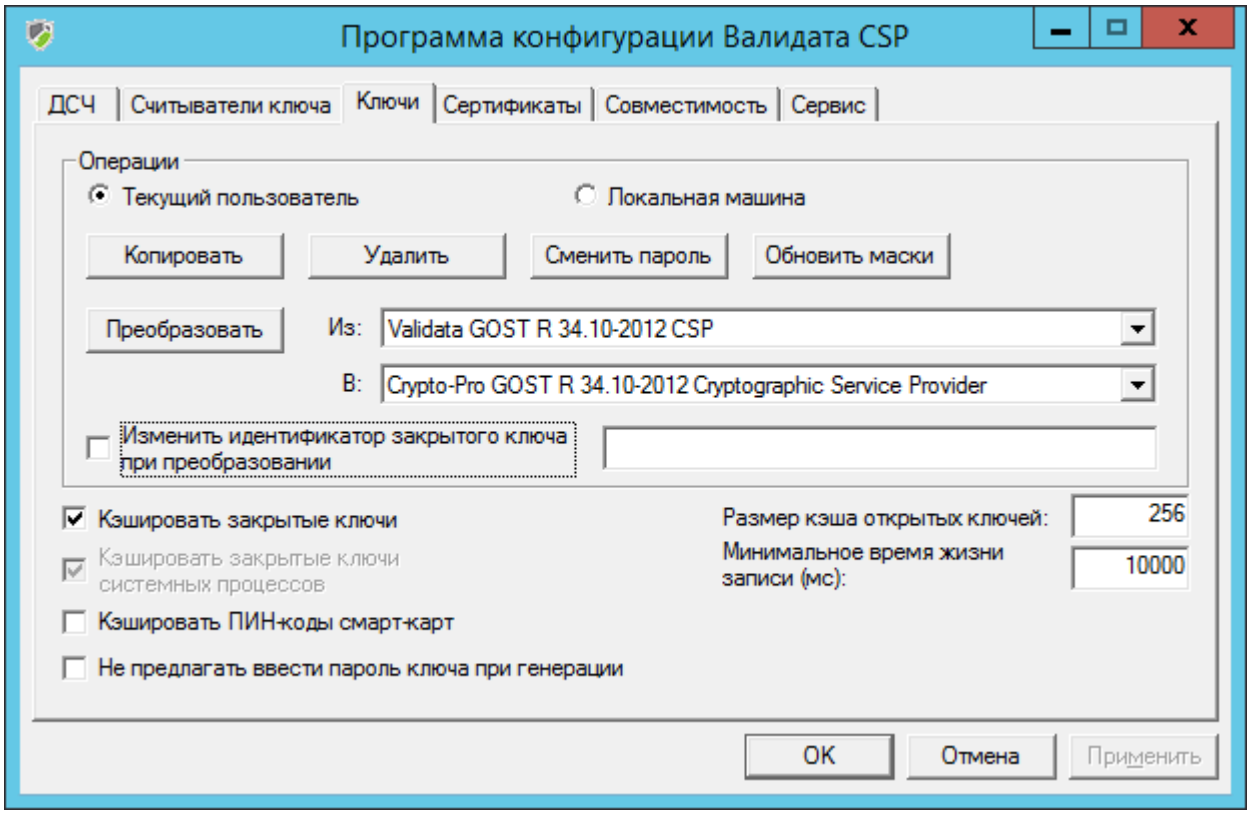
Ниже описан процесс выпуска сертификата Оператора ЦР в Центре Регистрации Валидата УЦ с использованием Валидата CSP:

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 **права на чтение закрытого ключа сертификата Оператора**, который был установлен на предыдущем шаге:

    1. Перейдите в оснастку **Сертификаты** (Certificates) компьютера, на котором установлен сервер Indeed CM.
    2. Нажмите правой кнопкой мыши на сертификате, выберите **Все задачи** (All tasks) → **Управление закрытыми ключами...** (Manage Private Keys...).
    3. Нажмите **Добавить** (Add), укажите сервер в меню **Размещение** (Location), укажите локальную группу **IIS_IUSRS** в поле **Введите имена выбранных объектов** (Enter the object names to select), нажмите **Проверить имена** (Check Names) и **ОК**.
    4. Выставите права **Полный доступ** (Full Control) и **Чтение** (Read).
    5. Нажмите **Применить** (Apply).

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).

Шаблоны сертификатов пользователей

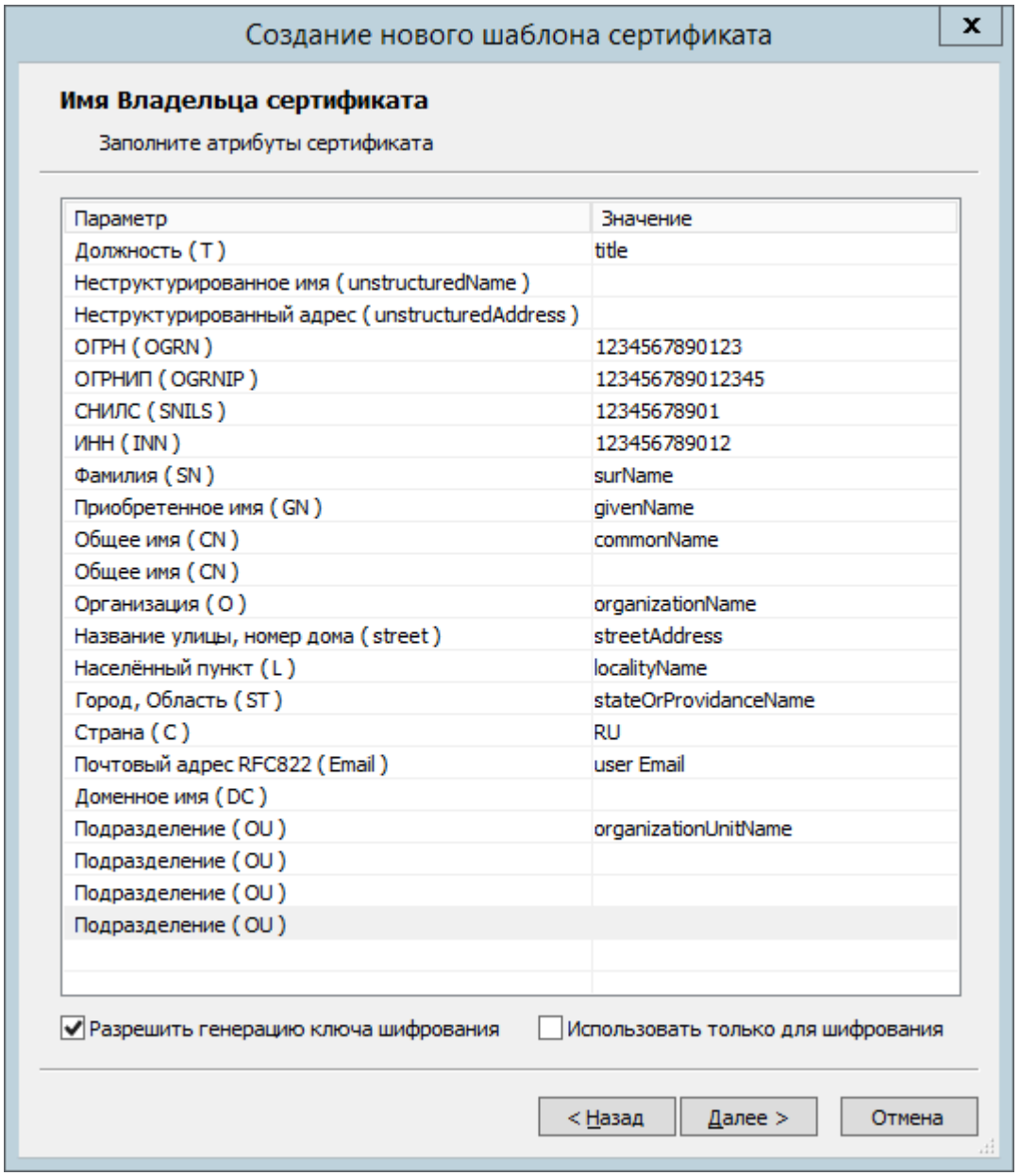
Для работы с Indeed Certificate Manager необходимо предварительно подготовить шаблоны сертификатов в Центре Регистрации Валидата УЦ в формате XML, которые будут использоваться для выпуска сертификатов конечным пользователям.

Процесс настройки шаблона сертификата пользователя в Центре Регистрации Валидата УЦ:

1. 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**. При необходимости установите опцию **Разрешить генерацию ключа шифрования**, чтобы создать ключ шифрования для сертификата. Если опция не выбрана, то пользователю, для которого создается сертификат, будет запрещено иметь ключ шифрования.

Поддерживаемые атрибуты для построения X.500-имени пользователя

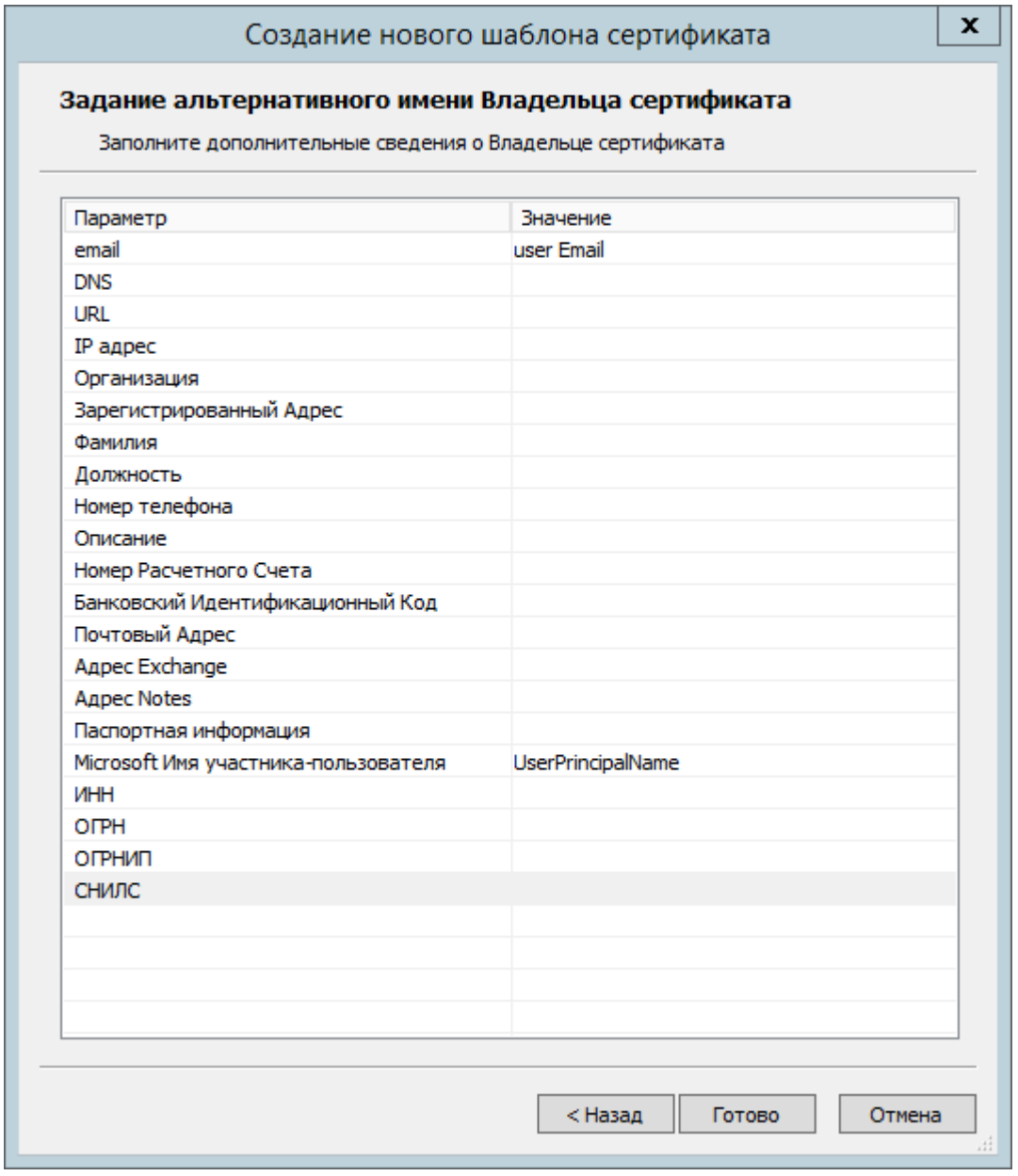
- Должность (T)
- Неструктурированное имя (unstructuredName)
- Неструктурированный адрес (unstructuredAddress)
- ОГРН (OGRN)
- ОГРНИП (ORGNIP)
- СНИЛС (SNILS)
- ИНН (INN)
- ИНН юридического лица (INNLE)
- Фамилия (SN)
- Приобретенное имя (GN)
- Общее имя (CN)
- Организация (O)
- Название улицы, номер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



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
- имя участника-пользователя (User Principal Name)



Чтобы использовать созданный шаблон в Indeed CM, очистите значения заполненных атрибутов в текстовом редакторе и перекодируйте шаблон 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>
```

Веб-сервер

IIS

Настройка веб-сервера Internet Information Services

NGINX

Настройка веб-сервера NGINX

Apache HTTP Server

Настройка веб-сервера Apache

IIS

Для работы серверных компонентов Indeed CM под управлением ОС Windows установите веб-сервер Internet Information Services (IIS) версии 7.0 или 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)

ПОДСКАЗКА

Для быстрой установки Internet Information Services (IIS) с требуемыми модулями используйте скрипт PowerShell, расположенный в каталоге *\IIS.Setup.Scripts* дистрибутива системы.
Для развертывания сервера Indeed CM необходимо выполнить установку Microsoft .NET Framework 4.5 и Microsoft .NET Core 3.1 после установки и настройки компоненов Internet Information Services (IIS).

NGINX

Для работы серверных компонентов Indeed CM на ОС Linux настройте веб-сервер Nginx в качестве обратного прокси-сервера:

1. Установите веб-сервер.
2. Выпустите SSL/TLS-сертификат.
3. Настройте конфигурационный файл.

RHEL-based

Установка веб-сервера

Для установки Nginx должен быть подключен и настроен репозиторий пакетов nginx. Если это не было сделано автоматически, добавьте репозиторий вручную.

1. Установите пакеты, необходимые для подключения yum-репозитория:

   ```
   sudo yum install yum-utils
   ```

2. Для подключения yum-репозитория создайте файл с именем */etc/yum.repos.d/nginx.repo* со следующим содержимым:

```
[nginx-stable]
name=nginx stable repo
baseurl=http://nginx.org/packages/centos/$releasever/$basearch/
gpgcheck=1
enabled=1
gpgkey=https://nginx.org/keys/nginx_signing.key
module_hotfixes=true

[nginx-mainline]
name=nginx mainline repo
baseurl=http://nginx.org/packages/mainline/centos/$releasever/$base
gpgcheck=1
enabled=0
gpgkey=https://nginx.org/keys/nginx_signing.key
module_hotfixes=true
```

3. Выполните следующую команду:

```
sudo yum install nginx
```

В случае запроса подтверждения GPG-ключа проверьте, что отпечаток ключа совпадает с *573B FD6B 3D8F BC64 1079 A6AB ABF5 BD82 7BD9 BF62*.

Документация по установке на прочие ОС доступна на портале NGINX.

Выпуск SSL/TLS сертификата

Для настройки защищенного соединения выпустите SSL/TLS сертификат на имя рабочей станции с установленным nginx. Используйте самоподписанный сертификат или выпустите сертификат на УЦ.

Самоподписанный сертификат

1. Создайте самоподписанный корневой сертификат утилитой openssl:

```
openssl genrsa -out ca.key 2048
openssl req -x509 -new -nodes -key ca.key -out ca.crt -days
3650 -subj "/CN=selfCA"
```

2. Создайте файл конфигурации *SSL.conf*, который содержит настройки для генерации запроса на сертификат веб-сервера (вместо SERVER_FQDN подставьте DNS-имя рабочей станции с nginx):

```
nano SSL.conf
```

Пример файла SSL.conf для генерации самоподписанного сертификата

```
[ req ]
default_bits = 2048
encrypt_key = no
default_md = sha256
utf8 = yes
string_mask = utf8only
prompt = no
distinguished_name = req_distinguished_name
req_extensions = req_ext
[ req_distinguished_name ]
commonName = SERVER_FQDN
[ req_ext ]
subjectAltName = @alt_names
keyUsage = nonRepudiation, digitalSignature,
keyEncipherment
basicConstraints = CA:FALSE
extendedKeyUsage = serverAuth
[alt_names]
DNS.1 = SERVER_FQDN
```

3. Создайте утилитой openssl запрос на сертификат и выпустите сертификат для веб-сервера с помощью самоподписанного сертификата:

```
openssl genrsa -out SSL.key 2048
openssl req -new -sha256 -out SSL.csr -key SSL.key -config
SSL.conf
openssl x509 -req -days 365 -in SSL.csr -CA ca.crt -CAkey
ca.key -CAcreateserial -extfile SSL.conf -extensions req_ext -
out SSL.crt
```

4. Скопируйте файлы сертификата и ключа в папку, которая указана в файле конфигурации nginx:

```
sudo cp ./SSL.crt /etc/ssl/certs/
sudo cp ./SSL.key /etc/ssl/private/
```

5. Добавьте сертификат корневого УЦ в доверенные на рабочей станции с установленным nginx.

```
sudo cp ./ca.crt /etc/pki/ca-trust/source/anchors/
sudo update-ca-trust extract
```

6. Сделайте сертификат доверенным в домене, например, с помощью групповых политик.

Выпуск сертификата на УЦ

1. Выпустите сертификат на УЦ, например на Microsoft CA, экспортируйте данный сертификат в формате PFX (с закрытым ключом, с цепочкой корневых/промежуточных УЦ) на рабочую станцию с установленным nginx.

> ⓘ **ТРЕБОВАНИЯ К СЕРТИФИКАТУ**
>
> - **Субъект** (Subject) сертификата содержит FQDN сервера Indeed CM.
> - **Дополнительное имя субъекта** (Subject Alternative Name) сертификата содержит атрибут **DNS-имя** (DNS Name) (FQDN сервера Indeed CM). Например: *server.demo.local* или соответствующую запись с подстановочными знаками, например: *.demo.local* (Wildcard certificate).
> - **Улучшенный ключ** (Enhanced Key Usage) сертификата должен содержать значение "Проверка подлинности сервера" (Server Authentication).

2. Добавьте сертификат корневого УЦ в доверенные на рабочей станции с установленным nginx.

```
sudo cp ./root-ca.crt /etc/pki/ca-trust/source/anchors/
sudo update-ca-trust extract
```

3. Разделите PFX сертификат на файл цепочки сертификатов и ключ, оставьте файл ключа без пароля и подставьте имя импортированного файла вместо *PFXFILE*:

```
openssl pkcs12 -in PFXFILE.pfx -chain -nokeys | sed -ne '/-
BEGIN CERTIFICATE/,/END CERTIFICATE/p' > SSL.crt
openssl pkcs12 -in PFXFILE.pfx -nocerts -out SSLencrypted.key
openssl rsa -in SSLencrypted.key -out SSL.key
```

Файл цепочки сертификатов должен быть следующего вида:

```
-----BEGIN CERTIFICATE-----
#Ваш сертификат#
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
#Промежуточный сертификат#
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
#Корневой сертификат#
-----END CERTIFICATE-----
```

4. Скопируйте файлы цепочки сертификатов и ключа в папку, которая указана в файле конфигурации nginx:

```
sudo cp ./SSL.crt /etc/ssl/certs/
sudo cp ./SSL.key /etc/ssl/private/
```

Настройка конфигурационного файла

Для работы Indeed CM настройте nginx, чтобы веб-сервер обслуживал запросы и отправлял их на проксируемый адрес – сервис Indeed CM.

Работа nginx и его модулей определяется в конфигурационном файле *nginx.conf*. В зависимости от операционной системы он расположен в каталоге */usr/local/nginx/conf*, */etc/nginx* или */usr/local/etc/nginx*.

Таблица рекомендуемых к использованию директив

Контекст	Директива	Значение по умолчанию	Рекомендуемое значение	
http	proxy_buffer_size	4k|8k	16k	Уве пер зап
	proxy_buffers	8 4k | 8 8k	4 16k	Уве пер зап
	types_hash_max_size	1024	4096	Уве хра кол
	client_max_body_size	1m	10m	Уве заг
server	listen	80	443 ssl	Изм HT HT
			3003 ssl	Пор кон аге
	server_name	—	*	* Тр име Исп зап

Контекст	Директива	Значение по умолчанию	Рекомендуемое значение	
	ssl_certificate	—	/etc/ssl/private/SSL.crt	Для фай серт корн
	ssl_certificate_key	—	/etc/ssl/private/SSL.key	Для закр
	ssl_verify_client	off	optional_no_ca	Доб серт аген
location	proxy_pass	—	*	*Одн нап Inde loca серв* *Точ http http* Где кото SER имя
	include	—	/etc/nginx/conf.d/proxy.conf	Нек каж кон созд дир вме

Контекст	Директива	Значение по умолчанию	Рекомендуемое значение	
	proxy_http_version	1.0	1.1	Вер под
	proxy_cache_bypass	—	$http_upgrade	Опр буд
	proxy_set_header	—	Upgrade $http_upgrade	Опр пос
			Connection keep-alive	Для
			Host $host	Для сер
			X-Real-IP $remote_addr	По про пол зад
			X-Forwarded-For $proxy_add_x_forwarded_for	Под фор про при $pr
			X-Forwarded-Proto $scheme	Веб про для
	fastcgi_buffers	8 4k|8k	16 16k	Опр чте под

Контекст	Директива	Значение по умолчанию	Рекомендуемое значение	
	fastcgi_buffer_size	4k|8k	32k	Опр част
	proxy_set_header	—	x-ssl-client-cert $ssl_client_escaped_cert	Дир при кли сер

Вследствие использования в конфигурации многократного описания контекстов *location*, определенный набор директив будет повторяться.

Для удобства конфигурации вынесите данный набор директив в отдельный файл, а в описании контекста включите директивы из данного файла (директива *include*).

1. Создайте файл с многократно используемыми директивами. Можно разместить такой файл с расширением CONF в каталоге */etc/nginx/conf.d/*.

   Рекомендуемое содержимое файла proxy.conf для работы с Indeed CM

   ```
   proxy_http_version 1.1;
   proxy_set_header   Upgrade $http_upgrade;
   proxy_set_header   Connection keep-alive;
   proxy_set_header   Host $host;
   proxy_cache_bypass $http_upgrade;
   proxy_set_header   X-Real-IP $remote_addr;
   proxy_set_header   X-Forwarded-For $proxy_add_x_forwarded_for;
   proxy_set_header   X-Forwarded-Proto $scheme;
   fastcgi_buffers 16 16k;
   fastcgi_buffer_size 32k;
   ```

2. Сконфигурируйте основной файл конфигурации nginx. Имена контекстов *location* должны совпадать с путем к проксируемому сервису.

Пример файла nginx.conf для работы с Indeed CM

```
user www-data;
worker_processes auto;
error_log /var/log/nginx/error.log notice;
events {    worker_connections 1024;    }

http {
 proxy_buffer_size   64k;
 proxy_buffers   4 64k;
 types_hash_max_size     4096;
 add_header X-Frame-Options sameorigin always;
     add_header X-Content-Type-Options nosniff;

 log_format  main  '[$time_local] $remote_addr VIA $scheme --
- $status --- $request \n $ssl_client_fingerprint';
 access_log  /var/log/nginx/access.log  main;
 sendfile                on;
 tcp_nopush              on;
 include                 /etc/nginx/mime.types;
 default_type            application/octet-stream;

 server {
     listen              443 ssl;
     server_name         $hostname;

     ssl_certificate     "/etc/ssl/certs/SSL.crt";
     ssl_certificate_key "/etc/ssl/private/SSL.key";

     location /cm/mc
     {   include /etc/nginx/conf.d/proxy.conf;   proxy_pass
http://localhost:5001/cm/mc;    }
     location /cm/ss
     {   include /etc/nginx/conf.d/proxy.conf;   proxy_pass
http://localhost:5002/cm/ss;    }
     location /cm/rss
     {   include /etc/nginx/conf.d/proxy.conf;   proxy_pass
http://localhost:5003/cm/rss;   }
```

```
      location /cm/api
      {   include /etc/nginx/conf.d/proxy.conf;   proxy_pass
http://localhost:5004/cm/api;   }
      location /cm/credprovapi
      {   include /etc/nginx/conf.d/proxy.conf;   proxy_pass
http://localhost:5005/cm/credprovapi;   }
      location /cm/oidc
      {   include /etc/nginx/conf.d/proxy.conf;   proxy_pass
http://localhost:5008/cm/oidc;  }
      location /cm/wizard
      {   proxy_pass http://localhost:5009;  }
      location /api
     {    include /etc/nginx/conf.d/proxy.conf;   proxy_pass
http://localhost:5010/api;  }
 }

 server {
      listen              3003 ssl;
      server_name         $hostname;

      ssl_certificate     "/etc/ssl/certs/SSL.crt";
      ssl_certificate_key "/etc/ssl/private/SSL.key";
      ssl_verify_client   optional_no_ca;

      location /agentregistrationapi
      { include /etc/nginx/conf.d/proxy.conf;   proxy_pass
http://localhost:5006/agentregistrationapi;  }
      location /agentserviceapi
      { include /etc/nginx/conf.d/proxy.conf;   proxy_pass
http://localhost:5007/agentserviceapi;
                                              proxy_set_header
x-ssl-client-cert $ssl_client_escaped_cert;  }
 }
}
```

3. Примените изменения в конфигурационном файле. Для этого перезагрузите конфигурацию или перезапустите nginx. Для перезагрузки конфигурации выполните команду:

```
sudo nginx -s reload
```

Debian-based

Установка веб-сервера

1. Установите пакеты, необходимые для подключения apt-репозитория:

   Ubuntu:

   ```
   sudo apt install curl gnupg2 ca-certificates lsb-release ubuntu-keyring
   ```

   Debian:

   ```
   sudo apt install curl gnupg2 ca-certificates lsb-release debian-archive-keyring
   ```

2. Импортируйте официальный ключ, используемый apt для проверки подлинности пакетов:

   ```
   curl https://nginx.org/keys/nginx_signing.key | gpg --dearmor | sudo tee /usr/share/keyrings/nginx-archive-keyring.gpg >/dev/null
   ```

3. Для подключения apt-репозитория выполните следующую команду:

   ```
   echo "deb [signed-by=/usr/share/keyrings/nginx-archive-keyring.gpg] http://nginx.org/packages/ubuntu `lsb_release -cs` nginx" | sudo tee /etc/apt/sources.list.d/nginx.list
   ```

4. Выполните следующую команду:

```
sudo apt update
sudo apt install nginx
```

Документация по установке на прочие ОС доступна на портале NGINX.

Выпуск SSL/TLS сертификата

Для настройки защищенного соединения выпустите SSL/TLS сертификат на имя рабочей станции с установленным nginx. Используйте самоподписанный сертификат или выпустите сертификат на УЦ.

Самоподписанный сертификат

1. Создайте самоподписанный корневой сертификат утилитой openssl:

   ```
   openssl genrsa -out ca.key 2048
   openssl req -x509 -new -nodes -key ca.key -out ca.crt -days
   3650 -subj "/CN=selfCA"
   ```

2. Создайте файл конфигурации *SSL.conf*, который содержит настройки для генерации запроса на сертификат веб-сервера (вместо SERVER_FQDN подставьте DNS-имя рабочей станции с установленным nginx):

   ```
   nano SSL.conf
   ```

Пример файла SSL.conf для генерации самоподписанного сертификата

```
[ req ]
default_bits = 2048
encrypt_key = no
default_md = sha256
utf8 = yes
string_mask = utf8only
prompt = no
distinguished_name = req_distinguished_name
req_extensions = req_ext
[ req_distinguished_name ]
commonName = SERVER_FQDN
[ req_ext ]
subjectAltName = @alt_names
keyUsage = nonRepudiation, digitalSignature,
keyEncipherment
basicConstraints = CA:FALSE
extendedKeyUsage = serverAuth
[alt_names]
DNS.1 = SERVER_FQDN
```

3. Создайте утилитой openssl запрос на сертификат и выпустите сертификат для веб-сервера с помощью самоподписанного сертификата:

```
openssl genrsa -out SSL.key 2048
openssl req -new -sha256 -out SSL.csr -key SSL.key -config
SSL.conf
openssl x509 -req -days 365 -in SSL.csr -CA ca.crt -CAkey
ca.key -CAcreateserial -extfile SSL.conf -extensions req_ext -
out SSL.crt
```

4. Скопируйте файлы сертификата и ключа в папку, которая указана в файле конфигурации nginx:

```
sudo cp ./SSL.crt /etc/ssl/certs/
sudo cp ./SSL.key /etc/ssl/private/
```

5. Добавьте сертификат корневого УЦ в доверенные на рабочей станции с установленным nginx.

```
sudo cp ./ca.crt /usr/local/share/ca-certificates/
sudo update-ca-certificates -f
```

6. Сделайте сертификат доверенным в домене, например, с помощью групповых политик.

Выпуск сертификата на УЦ

1. Выпустите сертификат на УЦ, например на Microsoft CA, и экспортируйте сертификат в формате PFX (с закрытым ключом, с цепочкой корневых/промежуточных УЦ) на рабочую станцию с установленным nginx.

> ⓘ **ТРЕБОВАНИЯ К СЕРТИФИКАТУ**
>
> - **Субъект** (Subject) сертификата содержит FQDN сервера Indeed CM.
> - **Дополнительное имя субъекта** (Subject Alternative Name) сертификата содержит атрибут **DNS-имя** (DNS Name) (FQDN сервера Indeed CM). Например: *server.demo.local* или соответствующую запись с подстановочными знаками, например: *.demo.local* (Wildcard certificate).
> - **Улучшенный ключ** (Enhanced Key Usage) сертификата должен содержать значение "Проверка подлинности сервера" (Server Authentication).

2. Добавьте сертификат корневого УЦ в доверенные на рабочей станции с установленным nginx.

```
sudo cp ./root-ca.crt /usr/local/share/ca-certificates/
sudo update-ca-certificates -f
```

3. Разделите PFX сертификат на файл цепочки сертификатов и ключ, оставьте файл ключа без пароля и подставьте имя импортированного файла вместо *PFXFILE*:

```
openssl pkcs12 -in PFXFILE.pfx -chain -nokeys | sed -ne '/-BEGIN CERTIFICATE/,/END CERTIFICATE/p' > SSL.crt
openssl pkcs12 -in PFXFILE.pfx -nocerts -out SSLencrypted.key
openssl rsa -in SSLencrypted.key -out SSL.key
```

Файл цепочки сертификатов должен быть следующего вида:

```
-----BEGIN CERTIFICATE-----
#Ваш сертификат#
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
#Промежуточный сертификат#
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
#Корневой сертификат#
-----END CERTIFICATE-----
```

4. Скопируйте файлы цепочки сертификатов и ключа в папку, которая указана в файле конфигурации nginx:

```
sudo cp ./SSL.crt /etc/ssl/certs/
sudo cp ./SSL.key /etc/ssl/private/
```

Настройка конфигурационного файла

Для работы Indeed CM требуется настроить nginx, чтобы он обслуживал запросы и отправлял их на проксируемый адрес – сервис Indeed CM.

Работа nginx и его модулей определяется в конфигурационном файле *nginx.conf*. В зависимости от операционной системы он расположен в каталоге */usr/local/nginx/conf*, */etc/nginx* или */usr/local/etc/nginx*.

Таблица рекомендуемых к использованию директив

Контекст	Директива	Значение по умолчанию	Рекомендуемое значение	
http	proxy_buffer_size	4k|8k	16k	Уве пер зап
	proxy_buffers	8 4k | 8 8k	4 16k	Уве пер зап
	types_hash_max_size	1024	4096	Уве хра кол
	client_max_body_size	1m	10m	Уве заг
server	listen	80	443 ssl	Изм HT HT
			3003 ssl	Пор кон аге
	server_name	—	*	* Тр име Исп зап

Контекст	Директива	Значение по умолчанию	Рекомендуемое значение	
	ssl_certificate	—	/etc/ssl/private/SSL.crt	Для фай серт корн
	ssl_certificate_key	—	/etc/ssl/private/SSL.key	Для закр
	ssl_verify_client	off	optional_no_ca	Доб серт аген
location	proxy_pass	—	*	*Одн нап Inde loca серв* *Точ http http* Где кото SER имя
	include	—	/etc/nginx/conf.d/proxy.conf	Нек каж кон созд дир вме

Контекст	Директива	Значение по умолчанию	Рекомендуемое значение	
	proxy_http_version	1.0	1.1	Вер под
	proxy_cache_bypass	—	$http_upgrade	Опр буд
	proxy_set_header	—	Upgrade $http_upgrade	Опр пос
			Connection keep-alive	Для
			Host $host	Для сер
			X-Real-IP $remote_addr	По про пол зад
			X-Forwarded-For $proxy_add_x_forwarded_for	Под фор про при $pr
			X-Forwarded-Proto $scheme	Веб про для
	fastcgi_buffers	8 4k|8k	16 16k	Опр чте под

Контекст	Директива	Значение по умолчанию	Рекомендуемое значение	
	fastcgi_buffer_size	4k|8k	32k	Опр част
	proxy_set_header	—	x-ssl-client-cert $ssl_client_escaped_cert	Дир при кли сер

Из-за использования в конфигурации многократного описания контекстов *location*, определенный набор директив будет повторяться.

Для удобства конфигурации вынесите данный набор директив в отдельный файл, а в описании контекста включите директивы из данного файла (директива *include*).

1. Создайте файл с многократно используемыми директивами. Можно разместить такой файл с расширением CONF в каталоге */etc/nginx/conf.d/*.

   Рекомендуемое содержимое файла proxy.conf для работы с Indeed CM

   ```
   proxy_http_version 1.1;
   proxy_set_header   Upgrade $http_upgrade;
   proxy_set_header   Connection keep-alive;
   proxy_set_header   Host $host;
   proxy_cache_bypass $http_upgrade;
   proxy_set_header   X-Real-IP $remote_addr;
   proxy_set_header   X-Forwarded-For $proxy_add_x_forwarded_for;
   proxy_set_header   X-Forwarded-Proto $scheme;
   fastcgi_buffers 16 16k;
   fastcgi_buffer_size 32k;
   ```

2. Сконфигурируйте основной файл конфигурации nginx. Имена контекстов *location* должны совпадать с путем к проксируемому сервису.

Пример файла nginx.conf для работы с Indeed CM

```
user www-data;
worker_processes auto;
error_log /var/log/nginx/error.log notice;
events {    worker_connections 1024;    }

http {
 proxy_buffer_size   64k;
 proxy_buffers   4 64k;
 types_hash_max_size     4096;
 add_header X-Frame-Options sameorigin always;
      add_header X-Content-Type-Options nosniff;

 log_format  main  '[$time_local] $remote_addr VIA $scheme --
- $status --- $request \n $ssl_client_fingerprint';
 access_log  /var/log/nginx/access.log  main;
 sendfile                on;
 tcp_nopush              on;
 include                 /etc/nginx/mime.types;
 default_type            application/octet-stream;

 server {
      listen              443 ssl;
      server_name         $hostname;

      ssl_certificate     "/etc/ssl/certs/SSL.crt";
      ssl_certificate_key "/etc/ssl/private/SSL.key";

     location /cm/mc
     {   include /etc/nginx/conf.d/proxy.conf;   proxy_pass
http://localhost:5001/cm/mc;    }
     location /cm/ss
     {   include /etc/nginx/conf.d/proxy.conf;   proxy_pass
http://localhost:5002/cm/ss;    }
     location /cm/rss
     {   include /etc/nginx/conf.d/proxy.conf;   proxy_pass
http://localhost:5003/cm/rss;   }
```

```
     location /cm/api
     {   include /etc/nginx/conf.d/proxy.conf;   proxy_pass
http://localhost:5004/cm/api;   }
     location /cm/credprovapi
     {   include /etc/nginx/conf.d/proxy.conf;   proxy_pass
http://localhost:5005/cm/credprovapi;   }
     location /cm/oidc
     {   include /etc/nginx/conf.d/proxy.conf;   proxy_pass
http://localhost:5008/cm/oidc;  }
     location /cm/wizard
     {   proxy_pass http://localhost:5009;  }
     location /api
   {    include /etc/nginx/conf.d/proxy.conf;   proxy_pass
http://localhost:5010/api;   }
 }

 server {
      listen              3003 ssl;
      server_name         $hostname;

      ssl_certificate     "/etc/ssl/certs/SSL.crt";
      ssl_certificate_key "/etc/ssl/private/SSL.key";
      ssl_verify_client   optional_no_ca;

      location /agentregistrationapi
      { include /etc/nginx/conf.d/proxy.conf;   proxy_pass
http://localhost:5006/agentregistrationapi;  }
      location /agentserviceapi
      { include /etc/nginx/conf.d/proxy.conf;   proxy_pass
http://localhost:5007/agentserviceapi;
                                          proxy_set_header
x-ssl-client-cert $ssl_client_escaped_cert;  }
 }
}
```

3. Примените изменения в конфигурационном файле. Для этого перезагрузите конфигурацию или перезапустите nginx. Для перезагрузки конфигурации выполните команду:

```
sudo nginx -s reload
```

Apache HTTP Server

Для работы серверных компонентов Indeed CM на ОС Linux настройте веб-сервер Apache в качестве обратного прокси-сервера:

1. Установите веб-сервер.
2. Выпустите SSL/TLS-сертификат.
3. Настройте модули и конфигурацию.
4. Настройте сайт Apache.

RHEL-based

Установка веб-сервера

Установите веб-сервер Apache с помощью следующих команд:

```
sudo yum install httpd
sudo systemctl enable httpd
sudo systemctl start httpd
```

Или установите веб-сервер Apache из исходного кода. Подробнее на портале Apache.

Выпуск SSL/TLS сертификата

Для настройки защищенного соединения выпустите SSL/TLS сертификат на имя рабочей станции с установленным веб-сервером Apache. Используйте самоподписанный сертификат или выпустите сертификат на УЦ:

Самоподписанный сертификат

1. Создайте самоподписанный корневой сертификат утилитой openssl:

```
openssl genrsa -out ca.key 2048
openssl req -x509 -new -nodes -key ca.key -out ca.crt -days
3650 -subj "/CN=selfCA"
```

2. Создайте файл конфигурации SSL.conf, который содержит настройки для генерации запроса на сертификат веб-сервера (вместо SERVER_FQDN подставьте DNS-имя рабочей станции с установленным Apache):

```
nano SSL.conf
```

Пример файла SSL.conf для генерации самоподписанного сертификата

```
[ req ]
default_bits = 2048
encrypt_key = no
default_md = sha256
utf8 = yes
string_mask = utf8only
prompt = no
distinguished_name = req_distinguished_name
req_extensions = req_ext
[ req_distinguished_name ]
commonName = SERVER_FQDN
[ req_ext ]
subjectAltName = @alt_names
keyUsage = nonRepudiation, digitalSignature,
keyEncipherment
basicConstraints = CA:FALSE
extendedKeyUsage = serverAuth
[alt_names]
DNS.1 = SERVER_FQDN
```

3. Создайте утилитой openssl запрос на сертификат и выпустите сертификат для веб-сервера с помощью самоподписанного сертификата:

```
openssl genrsa -out SSL.key 2048
openssl req -new -sha256 -out SSL.csr -key SSL.key -config
SSL.conf
openssl x509 -req -days 365 -in SSL.csr -CA ca.crt -CAkey
ca.key -CAcreateserial -extfile SSL.conf -extensions req_ext -
out SSL.crt
```

4. Скопируйте файлы сертификата и ключа в папку, которая указана в файле конфигурации Apache:

```
sudo cp ./SSL.crt /etc/httpd/ssl/certs
sudo cp ./SSL.key /etc/httpd/ssl/private
```

5. Добавьте сертификат корневого УЦ в доверенные на рабочей станции с установленным Apache.

```
sudo cp ./ca.crt /etc/pki/ca-trust/source/anchors/
sudo update-ca-trust extract
```

6. Сделайте сертификат доверенным в домене, например, с помощью групповых политик.

Выпуск сертификата на УЦ

1. Выпустите сертификат на УЦ, например на Microsoft CA, экспортируйте данный сертификат в формате PFX (с закрытым ключом, с цепочкой корневых/ промежуточных УЦ) на рабочую станцию с установленным веб-сервером Apache.

> **ПРИМЕЧАНИЕ**
>
> **Субъект** (Subject) сертификата должен содержать FQDN сервера Apache. **Дополнительное имя субъекта** (Subject Alternative Name) сертификата должно содержать атрибут **DNS-имя** (DNS Name) (FQDN сервера Apache). Например: *server.demo.local* или соответствующую запись с подстановочными знаками, например: **.demo.local* (Wildcard certificate).
> **Улучшенный ключ** (Enhanced Key Usage) сертификата должен содержать значение **Проверка подлинности сервера** (Server Authentication).

2. Разделите PFX сертификат на файл цепочки сертификатов и ключ, оставьте файл закрытого ключа без пароля и подставьте имя импортированного файла вместо PFXFILE:

```
openssl pkcs12 -in PFXFILE.pfx -chain -nokeys | sed -ne '/-BEGIN CERTIFICATE/,/END CERTIFICATE/p' > SSL.crt
openssl pkcs12 -in PFXFILE.pfx -cacerts -nokeys | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > root-ca.crt
openssl pkcs12 -in PFXFILE.pfx -nocerts -out SSLencrypted.key
openssl rsa -in SSLencrypted.key -out SSL.key
rm SSLencrypted.key
```

Файл цепочки сертификатов *SSL.crt* должен быть следующего вида:

```
-----BEGIN CERTIFICATE-----
#Ваш сертификат#
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
#Промежуточный сертификат#
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
#Корневой сертификат#
-----END CERTIFICATE-----
```

3. На рабочей станции с установленным веб-сервером Apache добавьте сертификат корневого УЦ в список доверенных.

```
sudo cp root-ca.crt /etc/pki/ca-trust/source/anchors/
sudo update-ca-trust extract
```

4. Скопируйте файлы цепочки сертификатов и ключа в папку, которая будет указана в найстройках сайта Apache:

```
sudo mkdir /etc/ssl
sudo cp SSL.crt /etc/httpd/ssl/certs
sudo cp SSL.key /etc/httpd/ssl/private
```

Настройка модулей и конфигурации

1. Установите модуль **mod_ssl**:

```
sudo yum install -y mod_ssl
```

2. Добавьте в конфигурационный файл *httpd.conf* (расположение по умолчанию */etc/httpd/conf/httpd.conf*) следующие директивы:

```
Listen 3003
LimitRequestLine 16384
LimitRequestFieldSize 16384
ServerName SERVER_FQDN
Header append X-FRAME-OPTIONS "SAMEORIGIN"
Header set X-Content-Type-Options "nosniff"
```

В данном месте и далее замените *SERVER_FQDN* на имя используемого сервера.

Настройка сайта

Для работы Indeed CM создайте сайт в Apache, чтобы он обслуживал запросы и отправлял их на проксируемый адрес – сервис Indeed CM.

1. Создайте файл сайта */etc/httpd/conf.d/SERVER_FQDN.conf*:

```
sudo touch /etc/httpd/conf.d/SERVER_FQDN.conf
```

2. Заполните файл рекомендуемым содержимым.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> В параметрах `SSLCertificateFile` и `SSLCertificateKeyFile` указаны пути к созданным/импортированным в предыдущих шагах файлам сертификата и закрытого ключа. Проверьте указанные пути и имена файлов.

Рекомендуемое содержимое файла SERVER_FQDN.conf

```
<VirtualHost *:80>
   RewriteEngine On
   RewriteCond %{HTTPS} !=on
   RewriteRule ^(.*)$ https://%{HTTP_HOST}%{REQUEST_URI}/$1
[R=301,L]
</VirtualHost>

<VirtualHost *:443>
   Protocols h2 http/1.1
   SSLCertificateFile /etc/httpd/ssl/certs/SSL.crt
   SSLCertificateKeyFile /etc/httpd/ssl/private/SSL.key
   SSLCipherSuite @SECLEVEL=1:ECDHE-ECDSA-AES128-GCM-
SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-
SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-
POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-
SHA256:DHE-RSA-AES256-GCM-SHA384

   ErrorLog ${APACHE_LOG_DIR}/error.log
   CustomLog ${APACHE_LOG_DIR}/access.log combined

   SSLEngine on
   SSLProtocol -all +TLSv1.2
   SSLHonorCipherOrder off
   SSLCompression off
   SSLSessionTickets on
   SSLUseStapling off
   SSLProxyEngine on
   SetEnv nokeepalive ssl-unclean-shutdown
   RequestHeader set X-Forwarded-Proto https
   Header always set Strict-Transport-Security "max-age=63072000"

   ProxyPreserveHost On

       ProxyPass /cm/mc http://localhost:5001/cm/mc
       ProxyPassReverse /cm/mc http://localhost:5001/cm/mc
```

```
        ProxyPass /cm/ss http://localhost:5002/cm/ss
        ProxyPassReverse /cm/ss http://localhost:5002/cm/ss

        ProxyPass /cm/rss http://localhost:5003/cm/rss
        ProxyPassReverse /cm/rss http://localhost:5003/cm/rss

        ProxyPass /cm/api http://localhost:5004/cm/api
        ProxyPassReverse /cm/api http://localhost:5004/cm/api

        ProxyPass /cm/credprovapi
http://localhost:5005/cm/credprovapi
        ProxyPassReverse /cm/credprovapi
http://localhost:5005/cm/credprovapi

        ProxyPass /cm/oidc http://localhost:5008/cm/oidc
        ProxyPassReverse /cm/oidc http://localhost:5008/cm/oidc

        ProxyPass /cm/wizard http://localhost:5009/cm/wizard
        ProxyPassReverse /cm/wizard
http://localhost:5009/cm/wizard

</VirtualHost>

<VirtualHost *:3003>
   protocols h2 http/1.1

   SSLCertificateFile /etc/httpd/ssl/certs/SSL.crt
   SSLCertificateKeyFile /etc/httpd/ssl/private/SSL.key
   SSLCipherSuite @SECLEVEL=1:ECDHE-ECDSA-AES128-GCM-
SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-
SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-
POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-
SHA256:DHE-RSA-AES256-GCM-SHA384

   ErrorLog ${APACHE_LOG_DIR}/error.log
   CustomLog ${APACHE_LOG_DIR}/access.log combined
```

```
    SSLEngine on
    SSLProtocol -all +TLSv1.2
    SSLHonorCipherOrder off
    SSLCompression off
    SSLSessionTickets on
    SSLUseStapling off
    SSLProxyEngine on
    RequestHeader set X-Forwarded-Proto https
    Header always set Strict-Transport-Security "max-age=63072000"

        ProxyPass /agentregistrationapi
http://localhost:5006/agentregistrationapi
        ProxyPassReverse /agentregistrationapi
http://localhost:5006/agentregistrationapi

    <Location "/agentserviceapi">
        SSLVerifyClient optional_no_ca
        SSLOptions +ExportCertData
        RequestHeader unset x-ssl-client-cert
        RequestHeader set x-ssl-client-cert "expr=%{escape:%
{SSL_CLIENT_CERT}}"
        #RequestHeader set x-ssl-client-cert "expr=%{escape:%
{SSL_CLIENT_S_DN}}"

        ProxyPass http://localhost:5007/agentserviceapi
        ProxyPassReverse http://localhost:5007/agentserviceapi
    </Location>
</VirtualHost>
```

3. Перечитайте файл конфигурации:

```
sudo httpd -t
sudo systemctl restart httpd
```

Debian-based

Установка веб-сервера

Установите веб-сервер Apache с помощью следующих команд:

```
sudo apt install apache2
sudo systemctl enable apache2
sudo service apache2 start
```

Или установите веб-сервер Apache из исходного кода. Подробнее на портале Apache.

Выпуск SSL/TLS сертификата

Для настройки защищенного соединения выпустите SSL/TLS сертификат на имя рабочей станции с установленным веб-сервером Apache. Используйте самоподписанный сертификат или выпустите сертификат на УЦ.

Самоподписанный сертификат

1. Создайте самоподписанный корневой сертификат утилитой openssl:

   ```
   openssl genrsa -out ca.key 2048
   openssl req -x509 -new -nodes -key ca.key -out ca.crt -days
   3650 -subj "/CN=selfCA"
   ```

2. Создайте файл конфигурации SSL.conf, который содержит настройки для генерации запроса на сертификат веб-сервера (вместо SERVER_FQDN подставьте DNS-имя рабочей станции с установленным Apache):

   ```
   nano SSL.conf
   ```

Пример файла SSL.conf для генерации самоподписанного сертификата

```
[ req ]
default_bits = 2048
encrypt_key = no
default_md = sha256
utf8 = yes
string_mask = utf8only
prompt = no
distinguished_name = req_distinguished_name
req_extensions = req_ext
[ req_distinguished_name ]
commonName = SERVER_FQDN
[ req_ext ]
subjectAltName = @alt_names
keyUsage = nonRepudiation, digitalSignature,
keyEncipherment
basicConstraints = CA:FALSE
extendedKeyUsage = serverAuth
[alt_names]
DNS.1 = SERVER_FQDN
```

3. Создайте утилитой openssl запрос на сертификат и выпустите сертификат для веб-сервера с помощью самоподписанного сертификата:

```
openssl genrsa -out SSL.key 2048
openssl req -new -sha256 -out SSL.csr -key SSL.key -config
SSL.conf
openssl x509 -req -days 365 -in SSL.csr -CA ca.crt -CAkey
ca.key -CAcreateserial -extfile SSL.conf -extensions req_ext -
out SSL.crt
```

4. Скопируйте файлы сертификата и ключа в папку, которая указана в файле конфигурации Apache:

```
sudo cp ./SSL.crt /etc/ssl/certs/
sudo cp ./SSL.key /etc/ssl/private/
```

5. Добавьте сертификат корневого УЦ в доверенные на рабочей станции с установленным Apache.

```
sudo cp ./ca.crt /etc/pki/ca-trust/source/anchors/
sudo update-ca-trust extract
```

6. Сделайте сертификат доверенным в домене, например, с помощью групповых политик.

Выпуск сертификата на УЦ

1. Выпустите сертификат на УЦ, например на Microsoft CA, экспортируйте данный сертификат в формате PFX (с закрытым ключом, с цепочкой корневых/промежуточных УЦ) на рабочую станцию с установленным веб-сервером Apache.

> **ПРИМЕЧАНИЕ**
>
> **Субъект** (Subject) сертификата должен содержать FQDN сервера Apache.
> **Дополнительное имя субъекта** (Subject Alternative Name) сертификата должно содержать атрибут **DNS-имя** (DNS Name) (FQDN сервера Apache). Например: *server.demo.local* или соответствующую запись с подстановочными знаками, например: **.demo.local* (Wildcard certificate).
> **Улучшенный ключ** (Enhanced Key Usage) сертификата должен содержать значение **Проверка подлинности сервера** (Server Authentication).

2. Разделите PFX сертификат на файл цепочки сертификатов и ключ, сделайте файл закрытого ключа без пароля (вместо PFXFILE подставьте имя импортированного файла):

```
openssl pkcs12 -in PFXFILE.pfx -chain -nokeys | sed -ne '/-BEGIN CERTIFICATE/,/END CERTIFICATE/p' > SSL.crt
openssl pkcs12 -in PFXFILE.pfx -cacerts -nokeys | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > root-ca.crt
openssl pkcs12 -in PFXFILE.pfx -nocerts -out SSLencrypted.key
openssl rsa -in SSLencrypted.key -out SSL.key
rm SSLencrypted.key
```

Файл цепочки сертификатов *SSL.crt* должен быть следующего вида:

```
-----BEGIN CERTIFICATE-----
#Ваш сертификат#
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
#Промежуточный сертификат#
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
#Корневой сертификат#
-----END CERTIFICATE-----
```

3. На рабочей станции с установленным веб-сервером Apache добавьте сертификат корневого УЦ в список доверенных.

```
sudo cp root-ca.crt /usr/local/share/ca-certificates/
sudo update-ca-certificates -f
```

4. Скопируйте файлы цепочки сертификатов и ключа в папку, которая будет указана в настройках сайта Apache:

```
sudo cp ./SSL.crt /etc/ssl/certs/
sudo cp ./SSL.key /etc/ssl/private/
```

Настройка модулей и конфигурации

Apache реализован в виде ядра и модулей, которые подключаются по необходимости использования дополнительной функциональности.

1. Для работы системы включите модули:

```
sudo a2enmod proxy
sudo a2enmod proxy_http
sudo a2enmod ssl
sudo a2enmod headers
sudo a2enmod rewrite
sudo systemctl restart apache2
```

2. Добавьте в конфигурационный файл *apache2.conf* (расположение по умолчанию */etc/apache2/apache2.conf*) следующие директивы:

```
Listen 3003
LimitRequestLine 16384
LimitRequestFieldSize 16384
ServerName SERVER_FQDN
Header append X-FRAME-OPTIONS "SAMEORIGIN"
Header set X-Content-Type-Options "nosniff"
```

   В данном месте и далее замените *SERVER_FQDN* на имя используемого сервера.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> При установке Apache в ОС Astra Linux в файле *apache2.conf* может потребоваться отключение параметра AstraMode, подробнее на портале Astra Linux.

Настройка сайта

Для работы Indeed CM создайте сайт в Apache, чтобы он обслуживал запросы и отправлял их на проксируемый адрес – сервис Indeed CM.

1. Создайте файл сайта */etc/apache2/sites-available/SERVER_FQDN.conf*

```
sudo touch /etc/apache2/sites-available/SERVER_FQDN.conf
```

2. Заполните файл рекомендуемым содержимым.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> В параметрах `SSLCertificateFile` и `SSLCertificateKeyFile` указаны пути к созданным/импортированным в предыдущих шагах файлам сертификата и закрытого ключа. Проверьте указанные пути и имена файлов.

Рекомендуемое содержимое файла SERVER_FQDN.conf

```
<VirtualHost *:80>
    RewriteEngine On
    RewriteCond %{HTTPS} !=on
    RewriteRule ^(.*)$ https://%{HTTP_HOST}%{REQUEST_URI}/$1
[R=301,L]
</VirtualHost>

<VirtualHost *:443>
    Protocols h2 http/1.1
    SSLCertificateFile /etc/ssl/certs/SSL.crt
    SSLCertificateKeyFile /etc/ssl/private/SSL.key
    SSLCipherSuite @SECLEVEL=1:ECDHE-ECDSA-AES128-GCM-
SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-
SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-
POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-
SHA256:DHE-RSA-AES256-GCM-SHA384

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    SSLEngine on
    SSLProtocol -all +TLSv1.2
    SSLHonorCipherOrder off
    SSLCompression off
    SSLSessionTickets on
    SSLUseStapling off
    SSLProxyEngine on
    SetEnv nokeepalive ssl-unclean-shutdown
    RequestHeader set X-Forwarded-Proto https
    Header always set Strict-Transport-Security "max-
age=63072000"

    ProxyPreserveHost On

        ProxyPass /cm/mc http://localhost:5001/cm/mc
        ProxyPassReverse /cm/mc http://localhost:5001/cm/mc
```

```
        ProxyPass /cm/ss http://localhost:5002/cm/ss
        ProxyPassReverse /cm/ss http://localhost:5002/cm/ss

        ProxyPass /cm/rss http://localhost:5003/cm/rss
        ProxyPassReverse /cm/rss http://localhost:5003/cm/rss

        ProxyPass /cm/api http://localhost:5004/cm/api
        ProxyPassReverse /cm/api http://localhost:5004/cm/api

        ProxyPass /cm/credprovapi
http://localhost:5005/cm/credprovapi
        ProxyPassReverse /cm/credprovapi
http://localhost:5005/cm/credprovapi

        ProxyPass /cm/oidc http://localhost:5008/cm/oidc
        ProxyPassReverse /cm/oidc http://localhost:5008/cm/oidc

        ProxyPass /cm/wizard http://localhost:5009/cm/wizard
        ProxyPassReverse /cm/wizard
http://localhost:5009/cm/wizard

</VirtualHost>

<VirtualHost *:3003>
    protocols h2 http/1.1

    SSLCertificateFile /etc/ssl/certs/SSL.crt
    SSLCertificateKeyFile /etc/ssl/private/SSL.key
    SSLCipherSuite @SECLEVEL=1:ECDHE-ECDSA-AES128-GCM-
SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-
SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-
POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-
SHA256:DHE-RSA-AES256-GCM-SHA384

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
```

```
    SSLEngine on
    SSLProtocol -all +TLSv1.2
    SSLHonorCipherOrder off
    SSLCompression off
    SSLSessionTickets on
    SSLUseStapling off
    SSLProxyEngine on
    RequestHeader set X-Forwarded-Proto https
    Header always set Strict-Transport-Security "max-
age=63072000"

        ProxyPass /agentregistrationapi
http://localhost:5006/agentregistrationapi
        ProxyPassReverse /agentregistrationapi
http://localhost:5006/agentregistrationapi

    <Location "/agentserviceapi">
        SSLVerifyClient optional_no_ca
        SSLOptions +ExportCertData
        RequestHeader unset x-ssl-client-cert
        RequestHeader set x-ssl-client-cert "expr=%{escape:%
{SSL_CLIENT_CERT}}"
        #RequestHeader set x-ssl-client-cert "expr=%{escape:%
{SSL_CLIENT_S_DN}}"

        ProxyPass http://localhost:5007/agentserviceapi
        ProxyPassReverse http://localhost:5007/agentserviceapi
    </Location>
</VirtualHost>
```

3. Перечитайте файл конфигурации и включите файл сайта:

```
sudo a2ensite SERVER_FQDN
sudo apachectl configtest
sudo systemctl restart apache2
```

Платформа .NET Core

Для работы серверных компонентов установите платформу .NET Core версии 3.1.

Платформа .NET Core является кроссплатформенной средой разработки с открытым исходным кодом от компании Microsoft. Поддерживается на ОС Windows и Linux.

Информация о последней версии продуктов .NET Core, исполняемые файлы для установки и исходный код доступны на сайте Microsoft.

Windows

До установки .NET Core убедитесь, что вы установили и настроили компоненты IIS.

Чтобы установить .NET Core:

1. Скачайте исполняемый файл с сайта Microsoft из раздела **ASP.NET Core Runtime → Installers → Hosting bundle**.
   Для работы на ОС Windows рекомендуется использовать Hosting bundle ASP.NET Core Runtime, в котором содержится .NET Runtime и поддержка IIS.
2. Запустите файл.

Linux

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Для установки .NET Core на ОС Linux требуется учетная запись с правами суперпользователя.

Чтобы установить .NET Core:

1. Скачайте с сайта Microsoft архив ASP.NET Core Runtime для нужной архитектуры Linux из раздела **Binaries**. Для работы на ОС Linux достаточно минимальной версии продукта .NET Core Runtime.

2. Откройте терминал, распакуйте скачанный архив в каталог */usr/share/dotnet* и создайте ссылку на исполняемый файл в каталоге для объявления исполняемых объектов ОС.

Пример

```
DOTNET_FILE=aspnetcore-runtime-3.1.32-linux-x64.tar.gz
sudo mkdir -p /usr/share/dotnet
sudo tar zxf $DOTNET_FILE -C /usr/share/dotnet
sudo ln -s /usr/share/dotnet/dotnet /usr/bin/dotnet
```

3. Проверьте установку .NET Core:

```
dotnet --info
```

Серверные компоненты

Для установки и настройки серверных компонентов Indeed Certificate Manager выполните следующие действия:

1. Установите сервер Indeed CM.
2. Настройте параметры системы.
3. Для инсталляций Indeed CM на ОС Linux настройте сервер авторизации пользователей OpenID Connect.
4. Для инсталляций Indeed CM на ОС Linux или конфигураций с несколькими серверами настройте единый журнал событий.

Если используется конфигурация с Indeed CM Agent, то выполните его установку и настройку.

Indeed CM Server

Установка сервера Indeed CM

Настройка параметров системы

Мастер настройки Indeed CM

OpenID Connect

Настройка сервера OpenID Connect

Indeed CM ЭДО

Функция внутреннего электронного документооборота

Единый журнал событий

Настройка записи событий в общий журнал

Indeed CM Agent

Настройка клиентского агента

Indeed CM Server

Indeed CM состоит из следующих сервисов:

- **Консоль управления** (Management Console) – веб-приложение **mc**;
- **Сервис самообслуживания** (Self-Service) – веб-приложение **ss**;
- **Сервис удаленного самообслуживания** за пределами домена (Remote Self-Service) – веб-приложение **rss**;
- **Сервис разблокировки и выключения устройств** – веб-приложение **credprovapi**;
- **Сервис API** – веб-приложение **api**;
- **Сервер OpenID Connect** – веб-приложение **oidc**;
- **Сервис отслеживания состояния устройств** – Служба Card Monitor, не имеет веб-приложения;
- **Сервис регистрации агентов** – веб-приложение **agentregistrationapi**;
- **Сервис агентов для удаленного выполнения задач** – веб-приложение **agentserviceapi**.

> **ПРИМЕЧАНИЕ**
>
> Каждый сервис имеет собственные файлы конфигурации и настройки доступа.

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

Windows

1. Запустите файл **IndeedCM.Server-<*номер версии*>.x64.ru-ru.msi** из каталога *IndeedCM.WindowsServer* дистрибутива системы и установите сервер, следуя указаниям мастера.

2. Выберите способ контроля доступа для всех приложений системы: аутентификация Windows или по персональным сертификатам пользователей.

   Аутентификация Windows

   При выборе аутентификации Windows будут заданы следующие параметры контроля доступа:

- **Проверка подлинности** (Authentication):
  - **Проверка подлинности Windows** (Windows Authentication) для следующих веб-приложений: Консоль управления (mc), Сервис самообслуживания (ss), Сервис API (api). Остальные способы отключены.
  - **Анонимная проверка подлинности** (Anonymous Authentication) для следующих веб-приложений: Сервис удаленного самообслуживания (rss), Сервис разблокировки смарт-карт (credprovapi), Сервисы клиентских агентов (agentregistrationapi, agentserviceapi).
  - **Анонимная проверка подлинности** (Anonymous Authentication) и **Проверка подлинности с помощью форм** (Forms Authentication) для приложения Сервис удаленного самообслуживания (rss).
- **Параметры SSL** (SSL Settings):
  - **Требовать SSL** (Require SSL) для всех веб-приложений.
  - **Сертификаты клиента** (Client certificates):
    - **Игнорировать** (Ignore) для следующих веб-приложений: Консоль управления (mc), Сервис самообслуживания (ss), Сервис удаленного самообслуживания (rss), Сервис разблокировки смарт-карт (credprovapi), Сервис API (api), Сервис регистрации клиентских агентов (agentregistrationapi).
    - **Требовать** (Require) для веб-приложения Сервис агентов (agentserviceapi).

Аутентификация по персональным сертификатам пользователей

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

- **Проверка подлинности** (Authentication):
  - **Анонимная проверка подлинности** (Anonymous Authentication) для всех веб-приложений. Остальные способы отключены.
  - **Анонимная проверка подлинности** (Anonymous Authentication) и **Проверка подлинности с помощью форм** (Forms Authentication) для приложения Сервис удаленного самообслуживания (rss).
- **Параметры SSL** (SSL Settings):
  - **Требовать SSL** (Require SSL) для всех веб-приложений.

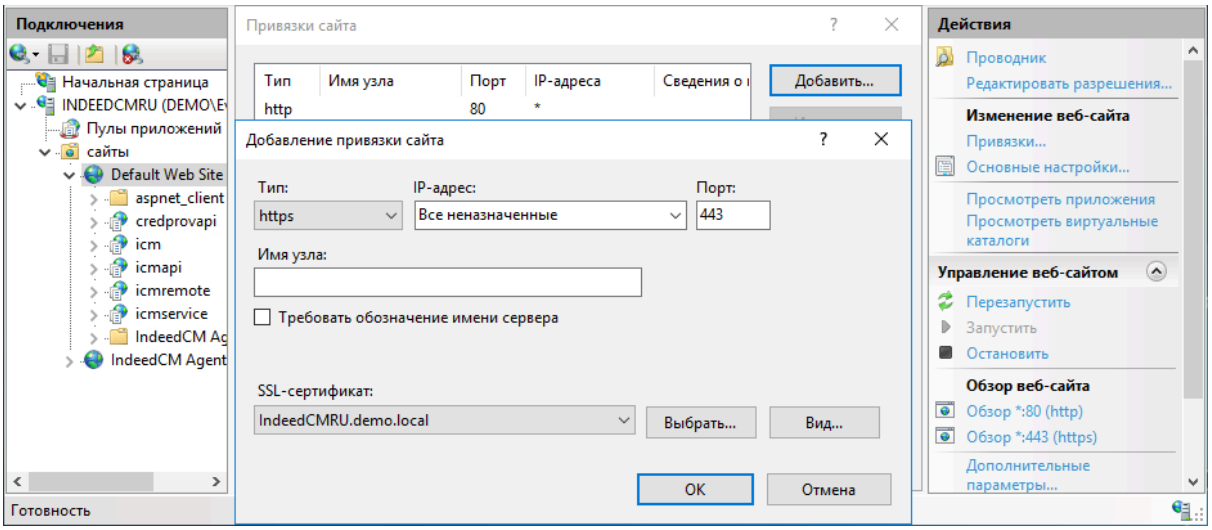
- **Сертификаты клиента** (Client certificates):
  - **Игнорировать** (Ignore) для следующих веб-приложений: Сервис удаленного самообслуживания (rss), Сервис разблокировки смарт-карт (credprovapi), Сервис регистрации клиентских агентов (agentregistrationapi).
  - **Требовать** (Require) для для следующих веб-приложений: Консоль управления (mc), Сервис самообслуживания (ss), Сервис API (api), Сервис агентов (agentserviceapi).

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Если каталог пользователей находится в Active Directory, то сертификаты, используемые для аутентификации, должны содержать значение **User Principal Name** (UPN). В веб-приложения невозможно войти, если в сертификате нет значения UPN.

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

3. Выпустите SSL/TLS-сертификат и привяжите его в **Диспетчере служб IIS** (Internet Information Services (IIS) Manager) для сайта **Default Web Site**:

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



> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> **Субъект** (Subject) сертификата должен содержать атрибут **Общее имя** (Common name) (FQDN сервера Indeed CM).
>
> **Дополнительное имя субъекта** (Subject Alternative Name) сертификата должно содержать атрибут **DNS-имя** (DNS Name) (FQDN сервера Indeed CM). Например: *server.demo.local* или соответствующую запись с подстановочными знаками, например: *. *demo.local* (Wildcard certificate).
>
> **Улучшенный ключ** (Enhanced Key Usage) сертификата должен содержать значение **Проверка подлинности сервера** (Server Authentication).

Linux

RHEL-based

1. Установите RPM пакет через пакетный менеджер из дистрибутива Indeed Certificate Manager. Для использования пакетного менеджера требуются права суперпользователя.

   ```
   sudo rpm -i cm.-<номер версии>.x86_64.rpm
   ```

2. Установите TrueType шрифты Windows для корректной работы Сервиса удаленного самообслуживания. В RHEL и производных дистрибутивах пакет называется *msttcore-fonts-installer*:

   ```
   sudo yum install -y msttcore-fonts-installer
   fc-cache -f -v
   ```

Debian-based

1. Установите DEB пакет через пакетный менеджер из дистрибутива Indeed Certificate Manager. Для использования пакетного менеджера требуются права суперпользователя.

   ```
   sudo dpkg -i cm.-<номер версии>_amd64.deb
   ```

2. Установите TrueType шрифты Windows для корректной работы Сервиса удаленного самообслуживания. В Debian и производных дистрибутивах пакет называется *ttf-mscorefonts-installer*:

   ```
   wget
   http://ftp.ru.debian.org/debian/pool/contrib/m/msttcorefonts/ttf
   mscorefonts-installer_3.8.1_all.deb
   sudo dpkg -i ttf-mscorefonts-installer_3.8.1_all.deb
   fc-cache -f -v
   ```

3. Настройте управление приложениями.

   Во время установки сервера для управления приложениями создаются файлы служб systemd. Данная подсистема инициализации и управления службами позволяет запускать приложения автоматически при старте сервера Indeed CM и держать их запущенными без участия пользователя.

   По умолчанию systemd запускает приложения Indeed CM от имени учетной записи www-data.

ПРИМЕЧАНИЕ

В RHEL и производных дистрибутивах учетная запись www-data по умолчанию отсутствует. Учетную запись www-data можно добавить через утилиту useradd или заменить используемую учетную запись пользователя (директива `User=<имя пользователя>`) в файлах служб *cm-<имя сервиса>.service*, располагающихся в директории */etc/systemd/system*.

Пример команды для создания пользователя www-data

```
useradd -d /var/www -m www-data -s /sbin/nologin
```

Пример файла службы Консоли управления, запускаемой от имени нестандартной учетной записи cm_adm

```
[Unit]
Description=Indeed CM Management Console Application

[Service]
WorkingDirectory=/opt/indeed/cm/mc/
ExecStart=/opt/indeed/cm/mc/Cm.Web.ManagementConsole
Restart=always
RestartSec=10
KillSignal=SIGINT
SyslogIdentifier=cm-mc
User=cm_adm
Environment=ASPNETCORE_URLS="http://localhost:5001"
Environment=ASPNETCORE_ENVIRONMENT=Production
Environment=DOTNET_PRINT_TELEMETRY_MESSAGE=false

[Install]
WantedBy=multi-user.target
```

Чтобы включить автозапуск и немедленный старт приложений, выполните файл сценария *start-cm-services.sh* из директории с дистрибутивом Indeed Certificate Manager:

```
chmod +x start-cm-services.sh
sudo ./start-cm-services.sh
```

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Для запуска любого файла сценария требуются разрешения на выполнение у данного файла. В ходе работы сценария требуются права суперпользователя.

4. Для корректной работы приложений настройте параметры системы через Мастер настройки (рекомендуется) или вручную.
5. Для безопасной работы с других машин настройте веб-сервер. В инструкциях описывается привязка SSL/TLS-сертификатов и настройка подключения по протоколу HTTPS.

Служба Card Monitor

Card Monitor – это служба для контроля использования устройств (USB-токенов и смарт-карт). Устанавливается вместе с сервером Indeed CM.

Служба Card Monitor выполняет следующие операции:

- отзыв и изъятие устройств пользователей, чьи учетные записи были удалены из каталога пользователей Indeed CM;
- отзыв временных устройств с истекшим сроком действия;
- выключение устройств пользователей, если их учетные записи были отключены в Active Directory;
- удаление пользователей из каталога пользователей Indeed CM, если их учетные записи были отключены в Active Directory;
- установка и сброс статуса сертификатов на устройстве;
- обновление содержимого устройства;
- регистрация события *Длительное отсутствие связи с агентом* в системный журнал;
- удаление агентов, которые были неактивны в течение настраиваемого периода времени;

- рассылка почтовых уведомлений администраторам и пользователям Indeed CM.

Настройка привилегий

Для работы Card Monitor необходимо создать сервисную роль в разделе **Конфигурация → Роли** Консоли управления, включить в нее учетную запись, от имени которой будет работать Card Monitor, и определить для роли следующие привилегии:

- выключение устройства;
- обновление устройства;
- отмена обновления устройства;
- отзыв и очистка устройства;
- отмена назначения устройства;
- удаление устройства;
- удаление агента;
- удаление задачи;
- удаление записи из журнала учета.

Если настроена интеграция с КриптоПро DSS и AirCard Enterprise, то задайте привилегии для работы с данными устройствами:

- выключение устройства КриптоПро DSS;
- обновление устройства КриптоПро DSS;
- отмена обновления устройства КриптоПро DSS;
- отзыв устройства КриптоПро DSS;
- удаление устройства КриптоПро DSS;
- удаление AirCard.

Настройка параметров системы

На этапе развертывания Indeed CM необходимо указать нужные значения в файлах конфигурации для каждого сервиса. Файлы конфигурации настраиваются в Мастере настройки Indeed CM.

Установка и аутентификация

Мастер настройки является независимым компонентом и устанавливается отдельно. Выберите инструкцию в зависимости от ОС, где установлен сервер Indeed CM.

Windows

1. Запустите файл *IndeedCM.Wizard-<номер версии>.x64.ru-ru.msi* из каталога *IndeedCM.WindowsServer* дистрибутива Indeed CM и выполните установку. Мастер настройки устанавливается в каталог *C:\inetpub\wwwroot\cm\wizard*.
2. Получите код аутентификации. Запустите пул приложения IIS IndeedCM Wizard, код сохранится в файл *wizard_authentication_code.txt* в каталоге *C:\inetpub\wwwroot\cm\wizard\logs*.
3. Откройте файл *wizard_authentication_code.txt* и скопируйте код аутентификации.
4. Откройте браузер и перейдите по адресу *https://<FQDN сервера Indeed CM>/cm/wizard*.
5. Введите код в поле **Код аутентификации** и нажмите **Войти**.

> **ПРИМЕЧАНИЕ**
>
> Если вы не смогли получить код аутентификации через запуск пула приложения IndeedCM Wizard, перезапустите службу IIS.

Linux

RHEL-based

1. Установите Мастер настройки из RPM-пакета *cm.wizard-<номер версии>.x86_64.rpm*:

```
sudo rpm -i cm.wizard-<номер версии>.x86_64.rpm
```

Debian-based

1. Установите Мастер настройки из DEB пакета *cm.wizard-<номер версии>_amd64.deb*.

```
sudo dpkg -i cm.wizard-<номер версии>_amd64.deb
```

2. Запустите bash-скрипт `start-cm-wizard.sh`, расположенный в каталоге с дистрибутивом сервера Indeed CM.

```
sudo bash ./start-cm-wizard.sh
```

3. Получите код аутентификации. Код аутентификации доступен при выводе запуска скрипта `start-cm-wizard.sh`.
4. Откройте браузер и перейдите по адресу *https://<FQDN сервера Indeed CM>/cm/wizard*.
5. Введите код в поле **Код аутентификации** и нажмите **Войти**.

Как еще получить код аутентификации

Способ 1. Запустите службу cm-wizard.service. Код сохранится в файл *wizard_authentication_code.txt* в каталоге */opt/indeed/cm/wizard/logs*.
Способ 2. Выполните команду `systemctl status`:

```
sudo systemctl status cm-wizard.service | grep AuthenticationCode
```

Способ 3. Получите код из журнала приложения systemd юнита cm-wizard.service по команде:

```
sudo journalctl -u cm-wizard.service | grep AuthenticationCode
```

Код аутентификации выводится на экран терминала.

Функции системы

В разделе **Общие функции** выберите настройки Консоли управления и Сервиса самообслуживания.

Журнал событий

Настройте работу журнала событий.

1. Укажите атрибут, по значению которого выполняется поиск пользователей в журнале событий. Значение по умолчанию: CN (Common name).
2. Выберите опцию:

- **Использовать локальный журнал Windows**, чтобы записывать события с одного или нескольких серверов в единый журнал Windows.
- **Использовать Log Server**, чтобы записывать события с нескольких серверов Indeed CM в единый журнал Windows, SysLog, базу данных Microsoft SQL или PostgreSQL.

Использовать локальный журнал Windows

События будут записываться в локальный журнал Windows.

Если в инфраструктуре развернуто несколько серверов Indeed CM, вы можете использовать компонент Indeed CM Event Log Proxy, чтобы все серверы записывали события в единый журнал Windows:

1. Установите и настройте приложение Indeed CM Event Log Proxy. Инструкция по установке Indeed CM Event Log Proxy
2. Включите опцию **Включить Event Log Proxy**.
3. Укажите URL подключения к Event Log Proxy. Например, `https://server.demo.local/cm/eventlogproxy`.
4. Если сервер Indeed CM установлен на ОС Windows, введите данные учетной записи с правами на доступ к единому журналу событий (из секции `authorization` файла *Web.config* приложения Event Log Proxy).
   Если сервер Indeed CM установлен на ОС Linux, в поле **Отпечаток сертификата** укажите отпечаток клиентского сертификата, который предъявляет сервер Indeed CM для подключения к Event Log Proxy (из параметра `allowedCertificateThumbprints` файла *appsettings.json* приложения Event Log Proxy).

Использовать Log Server

Если в инфраструктуре развернуто несколько серверов Indeed CM, вы можете использовать приложение Indeed Log Server, чтобы все серверы записывали события в единый журнал Windows, SysLog, базу данных Microsoft SQL или PostgreSQL.

1. Установите и настройте приложение Indeed Log Server. Инструкция по установке Indeed Log Server
2. Укажите URL подключения к Indeed Log Server. Например, `https://server.demo.local/ls/api` для ОС Windows, `https://server.demo.local/api` для ОС Linux.

Журнал учета СКЗИ

Если в вашей организации ведется учет СКЗИ, включите опцию **Вести журнал учета СКЗИ**.

При необходимости укажите дополнительные атрибуты для полей, которые будут отображаться в журнале учета СКЗИ.

Удостоверяющие центры

Настройте параметры работы с удостоверяющими центрами.

Microsoft CA

Включите опцию **Включить интеграцию с Microsoft Enterprise CA**.

Вы можете дополнительно **Разрешить выпуск сертификатов для пользователей внешнего сопоставленного каталога Active Directory** и указать атрибут Active Directory, по которому можно получить дополнительный e-mail пользователя.

КриптоПро УЦ 2.0

Включите опцию **Включить интеграцию с КриптоПро УЦ 2.0**. Дополнительно можно настроить опции:

- **Отображать привязку пользователя к КриптоПро УЦ в сервисе самообслуживания**;
- **Разрешить выпуск сертификатов на имя общей учетной записи**;
- **Публиковать сертификаты пользователей КриптоПро УЦ 2.0 в базе приложений ЦФТ**.

При необходимости укажите информацию о расположении пользователей в Центре Регистрации:

1. Нажмите **Добавить**.
2. Введите имя УЦ, которое отображается в Консоли управления ЦР в разделе **Центры сертификации**.
3. Введите идентификатор папки с пользователями. Идентификатор отображается в Консоли управления ЦР в колонке **Идентификатор папки**.

КриптоПро DSS

Включите опцию **Включить интеграцию с КриптоПро DSS**.

Чтобы в Сервисе самообслуживания отображалась информация о связи пользователя с каталогом КриптоПро DSS, включите опцию **Отображать привязку пользователя к КриптоПро DSS в сервисе самообслуживания**.

Валидата УЦ

Включите опцию **Включить интеграцию с Валидата УЦ**.

AirCard Enterprise

Укажите настройки интеграции с Indeed AirCard Enterprise:

1. Включите опцию **Включить интеграцию с Indeed AirCard Enterprise**.
2. Введите URL подключения к серверу AirCard Enterprise, например, `https://aircard.demo.local:3002`. Убедитесь, что указанный порт открыт для входящих подключений на сервере AirCard.
3. Укажите отпечаток клиентского сертификата, чтобы установить защищенное соединение сервера Indeed CM и сервера AirCard Enterprise.
4. Укажите время существования незарегистрированных смарт-карт AirCard (в секундах). По истечении указанного времени служба Card Monitor автоматически удалит незарегистрированные смарт-карты AirCard. Значение по умолчанию – 120 секунд.

Подробнее в документации Indeed AirCard Enterprise

Клиентский агент

Настройте параметры работы клиентских агентов Indeed CM.

1. Установите и настройте компонент Indeed CM Agent. Как установить Indeed CM Agent
2. Включите опцию **Разрешить использование клиентских агентов**.
3. Выберите способ идентификации агента в домене и вне домена для регистрации в Indeed CM:
   - **Не задано**. Значение по умолчанию.
   - **Использовать машинный GUID**. Использовать значение `MachineGuid` рабочей станции.
   - **Генерировать новый GUID**. Выберите данную опцию, если у нескольких рабочих станций одно значение `MachineGuid`.
   - **Использовать доменный SID компьютера**.
   - **Использовать SID компьютера**. Выберите данную опцию, если агент установлен на внедоменную рабочую станцию. Идентификатору агента присваивается строковое значение `MachineGuid` из ветки реестра *[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography]* рабочей станции.

Смена стратегии генерации идентификатора агента

Если вам нужно сменить стратегию генерации идентификатора агента после первоначальной настройки Indeed CM, выполните следующее:

1. Остановите сервисы агентов agentregistrationapi и agentserviceapi на сервере Indeed CM.
2. Удалите все клиентские агенты в разделе **Агенты** Консоли управления или выполните запрос в базу данных Indeed CM, чтобы удалить зарегистрированные агенты и их сессии.
3. Примените изменения в Мастере настройки и распространите измененный файл конфигурации сервиса agentregistrationapi на сервере Indeed CM.
4. Запустите сервисы агентов agentregistrationapi и agentserviceapi.

4. Чтобы регистрировать агенты без подтверждения администратора, включите опцию **Автоматическая регистрация Агентов**. После установки и настройки агента на рабочей станции он появится в разделе **Агенты** Консоли управления Indeed CM со статусом *Зарегистрирован*.

5. Загрузите сертификат агента – файл корневого сертификата сервисов агента с закрытым ключом в формате JSON *agent_root_ca.json*.

6. Выберите **Уровень журналирования событий агентом**.

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

8. Имя заголовка HTTP-запроса сертификата указано по умолчанию. Если Indeed CM используется с балансировщиком нагрузки, включите опцию **Передавать только поле 'Субъект' сертификата агента в заголовках HTTP-запросов**, чтобы снизить трафик.

Каталог пользователей

Настройте подключение к каталогу пользователей Indeed CM. Можно использовать несколько каталогов пользователей. Как создать каталог пользователей

Active Directory

Чтобы настроить подключение к каталогу пользователей в Microsoft Active Directory:

1. Нажмите **Добавить**.
2. Укажите данные учетной записи, у которой есть права на доступ к каталогу пользователей: имя в формате DOMAIN\UserName или UserName@DNSDomainName и пароль.
3. Укажите DNS-имя домена или контроллера домена.
4. Укажите путь к контейнеру с пользователями в формате Distinguished Name. Для работы со всеми пользователями выберите корень домена.
5. Если вы используете протокол LDAPS для доступа к каталогам, включите опцию **Использовать LDAPS**.
6. Если необходимо, выберите имя атрибута Active Directory, который содержит фотографию пользователя, чтобы отображать ее в интерфейсе Indeed CM или напечатать на смарт-карте.
7. Нажмите **Сохранить**.

ЦР КриптоПро УЦ 2.0

Чтобы настроить подключение к каталогу пользователей в Центре Регистрации КриптоПро УЦ 2.0:

1. Нажмите **Добавить**.
2. В выпадающем списке выберите атрибут имени пользователя, по которому определяется его уникальность при аутентификации в веб-приложениях Indeed CM:
   - E-mail;
   - Common name;
   - User Principal Name;
   - Пользовательский. Укажите OID атрибута имени пользователя.
3. Укажите отпечаток сертификата сервисной учетной записи, который будет использоваться для подключения к ЦР КриптоПро УЦ 2.0 для просмотра списка пользователей.

4. Укажите URL подключения к Центру Регистрации. Например, `https://cryptopro.demo.local/RA/RegAuthLegacyService.svc`.
5. Нажмите **Сохранить**.

Соответствия атрибутов

Вы можете настроить соответствие между атрибутами удостоверяющего центра и атрибутами пользователей в каталоге.

Если соответствие атрибутов настроено, при выпуске устройства для пользователя в Indeed CM, этого пользователя можно автоматически зарегистрировать в удостоверяющем центре.

Обновляемые атрибуты

Вы можете настроить список атрибутов пользователя Active Directory, при изменении которых необходимо обновить сертификат на устройстве.

Изменения можно отслеживать только для атрибутов из полей **Субъект** (Subject) и **Дополнительное имя субъекта** (Subject Alternative Name) сертификата.

> **ПРИМЕЧАНИЕ**
>
> В параметрах шаблонов сертификатов Microsoft CA и КриптоПро УЦ 2.0 по умолчанию отслеживаются атрибуты Общее имя, E-mail и UPN-имя пользователя.

Чтобы отслеживать атрибут:

1. Нажмите **Добавить**.
2. Укажите имя атрибута в каталоге пользователей.
3. Укажите отображаемое имя атрибута.
4. Укажите имя X.500 или OID атрибута в сертификате. По указанному значению выполняется поиск атрибута в сертификате.
5. Нажмите **Сохранить**.

Контроль доступа

Выберите способ контроля доступа к сервисам Indeed CM:

- **Аутентификация Windows**
  Этот способ позволяет аутентифицироваться через учетные данные пользователя в ОС Windows и используется для инсталляций Indeed CM на доменной рабочей станции под управлением ОС Windows.

- **Аутентификация OpenID Connect**
  Этот способ позволяет аутентифицироваться через сервер OpenID Connect и используется для инсталляций Indeed CM на доменной или внедоменной рабочей станции под управлением ОС Windows.
  Перейдите в раздел **OpenID Connect** и укажите параметры подключения к серверу OpenID Connect.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Убедитесь, что вы выбрали тот же способ аутентификации при установке сервера Indeed CM на ОС Windows.

Администратор ролей

Администратор ролей – учетная запись с правами на управление ролями в Indeed CM.

Укажите имя администратора ролей в формате DOMAIN\UserName или UserName@DNSDomainName. При первом запуске Indeed CM войдите в Консоль управления от имени указанной учетной записи.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Убедитесь, что учетная запись администратора ролей входит в каталог пользователей.

Хранилище данных

Настройте подключение к хранилищу данных. Как создать хранилище данных

1. Выберите тип хранилища данных: Microsoft SQL или PostgreSQL.
2. Настройте подключение к хранилищу. Введите имя сервера, имя экземпляра (для Microsoft SQL), номер порта и имя базы данных.
3. Выберите способ аутентификации для подключения к серверу базы данных:

- Microsoft SQL: аутентификация Windows или SQL Server. Для подключения к SQL Server введите имя пользователя и пароль.
- PostgreSQL: введите имя пользователя и пароль.

4. При необходимости настройте дополнительные параметры:
   - минимальный размер пула;
   - максимальный размер пула;
   - время ожидания подключения;
   - время жизни соединения;
   - число повторов подключения;
   - интервал повтора подключения.

Ключ шифрования хранилища данных

Данные Indeed CM хранятся и передаются в зашифрованном виде. В выпадающем списке выберите алгоритм шифрования и нажмите **Сгенерировать**. Сохраните резервную копию ключа шифрования.

Служба Card Monitor

Определите настройки Card Monitor – службы для контроля использования устройств.

Подробнее о работе службы Card Monitor

Card Monitor устанавливается автоматически вместе с сервером Indeed CM и выполняет следующие операции:

- отзыв и изъятие устройств пользователей, учетные записи которых удалены из каталога пользователей;
- отзыв временных устройств с истекшим сроком действия;
- выключение устройств пользователей, учетные записи которых были отключены;
- удаление учетных записей из каталога пользователей, учетные записи которых были отключены;
- установка или сброс статуса содержимого устройства;
- регистрация события *Длительное отсутствие связи с агентом* в журнале событий;
- удаление агентов, которые были неактивны в течение настраиваемого периода времени;
- рассылка почтовых уведомлений администраторам и пользователям о следующих событиях:
  - 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.

1. Для регулярного запуска службы Card Monitor укажите учетную запись, которая состоит в группе Администраторов (Administrators) на сервере Indeed CM и имеет разрешение на **Вход в качестве пакетного задания** (Log on as a batch job) в политике Active Directory.
2. Настройте время запуска службы Card Monitor.
3. В разделе **Операции с пользователями, чьи учетные записи Active Directory отключены (Account is disabled)** можно настроить следующее:
   - **Выключать устройства пользователей**. Card Monitor выключит устройства пользователей, учетные записи которых были отключены в каталоге пользователей. Если в параметрах шаблонов сертификатов используемого УЦ дополнительно включить опцию **Отзывать сертификат при отзыве или выключении устройства**,

то срок действия сертификатов, записанных на устройства, будет приостановлен в УЦ, и сертификаты будут отозваны.

- **Включить фильтр удаленных пользователей**. Отключенные учетные записи, попадающие под условие фильтра, считаются удаленными из каталога пользователей. Устройства у удаленных пользователей отзываются.
  Укажите атрибут пользователя и значение атрибута. Например, атрибут DistinguishedName со значением `OU=Fired users,DC=demo,DC=local`.

4. При необходимости настройте параметры работы с неактивными агентами:
   - **Занести событие в журнал, если агент неактивен больше (мин.)**. При отсутствии связи агента с сервером Card Monitor регистрирует это событие в системном журнале по истечении указанного времени.
   - **Удалить агент, если он неактивен больше (дней)**. При отсутствии связи агента с сервером Card Monitor удаляет агент из базы данных по истечении указанного времени.

Для работы службы Card Monitor необходима отдельная сервисная роль. Подробнее о роли для работы Card Monitor

Подтверждение

1. Проверьте настройки всех разделов Мастера.
2. Нажмите **Применить**.

Все настроенные параметры записываются в файлы конфигурации приложений и сохраняются в каталог *C:\inetpub\wwwroot\cm\wizard\configs* для ОС Windows и */opt/indeed/cm/wizard/configs/* для ОС Linux. Файлы конфигурации нужно применить на сервере Indeed CM.

Результаты

Включите опцию **Сохранить файлы конфигурации**, чтобы выгрузить файлы в архив.

Если вы устанавливаете Indeed CM впервые, рекомендуем сохранить копию настроенных параметров. Включите опцию **Сохранить резервную копию параметров конфигурации** и задайте пароль от файла.

Резервная копия настроек содержит все параметры, определенные при установке для всех сервисов, а также алгоритм и ключ шифрования базы данных. Храните файл резервной копии в

защищенном месте.

Восстановление настроек

Вы можете восстановить настройки конфигурации Indeed CM из резервной копии, если вам необходимо:

- обновить сервер Indeed CM;
- перенести сервер на новую рабочую станцию;
- установить дополнительные серверы.

Чтобы восстановить конфигурацию из файла:

1. Перейдите в раздел Мастера **Восстановление настроек**.
2. Нажмите **Восстановить параметры конфигурации из резервной копии**.
3. Загрузите файл.
4. Если резервная копия была зашифрована, введите пароль.

Применение файлов конфигурации на сервере Indeed CM

Примените файлы конфигурации, созданные Мастером настройки, на сервере Indeed CM.

Windows

1. Откройте консоль Powershell от имени администратора.
2. Перейдите в директорию *C:\inetpub\wwwroot\cm\wizard\configs*.
3. Запустите Powershell-скрипт *deploy_configuration.ps1*:

```
.\deploy_configuration.ps1
```

4. В процессе выполнения Powershell-скрипта укажите пароль учетной записи, используемой для запуска службы Card Monitor.

ПОДСКАЗКА

Рекомендуется указать локальную учетную запись, от имени которой запускаются остальные веб-приложения Indeed CM.

Файлы конфигурации всех сервисов Indeed CM расположены в корневом каталоге веб-приложений IIS по пути *%SystemDrive%\inetpub\wwwroot\cm*. Файлы конфигурации службы Card Monitor расположены в каталоге *%ProgramFiles%\Indeed CM\CardMonitor*.

Linux

Примените файлы конфигурации, созданные Мастером настройки, на сервере Indeed CM.

1. Откройте эмулятор терминала.
2. Перейдите в директорию */opt/indeed/cm/wizard/configs*.
3. Убедитесь, что файл скрипта имеет права на исполнение, и запустите bash-скрипт *deploy_configuration.sh*:

```
sh ./deploy_configuration.sh
```

4. В процессе выполнения bash-скрипта укажите учетную запись, от имени которой будет запускаться служба Card Monitor.

ПОДСКАЗКА

Рекомендуется указать локальную учетную запись, от имени которой запускаются остальные веб-приложения Indeed CM.

Если в инфраструктуре развернуто несколько серверов Indeed CM, примените файлы конфигурации на каждом сервере. Файлы конфигурации всех сервисов Indeed CM располагаются в каталоге */opt/indeed/cm*.

Шифрование/расшифровка файлов конфигурации

В целях безопасности рекомендуется зашифровать файлы конфигурации приложений Indeed CM с помощью утилиты Cm.Config.DataProtector. Утилита поддерживает алгоритм шифрования AES с эффективной длиной ключа 256 бит. Ключ шифрования сохраняется на сервере Indeed CM.

Ключ шифрования находится по пути:

- ОС Windows: *C:\ProgramData\Indeed\cm\keys*
- ОС Linux: */etc/indeed/cm/keys*.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Создайте резервную копию ключа шифрования. Это позволит восстановить доступ к зашифрованным данным в случае утери или повреждения основного ключа. Копию ключа можно сохранить вместе с копией конфигурации Indeed CM.

Windows

Шифрование

1. Перейдите в каталог с дистрибутивом сервера Indeed CM по пути *Misc\dataprotector*.
2. Запустите PowerShell от имени администратора.
3. Выполните одну из команд:

- шифрование всех файлов конфигурации, расположенных в стандартных директориях (*C:\inetpub\wwwroot\<название компонента>\appsettings.json*):

```
.\Cm.Config.DataProtector protect
```

- шифрование файлов конфигурации отдельных компонентов:

```
.\Cm.Config.DataProtector protect --app <название компонента>
```

Пример команды

```
.\Cm.Config.DataProtector protect --app ManagementConsole
```

Названия компонентов Indeed CM

- Консоль управления – ManagementConsole
- Сервис самообслуживания – SelfService
- Служба Card Monitor – CardMonitor
- CredentialProvider
- Сервис удаленного самообслуживания – RemoteService
- Сервис API – Api
- Сервис очистки AirCard – AirCardCleaner
- Сервис регистрации агентов – AgentRegistrationApi
- Сервис агентов – AgentServiceApi
- Сервер OpenID Connect – Oidc

- шифрование файла конфигурации, расположенного вне стандартной директории:

```
.\Cm.Config.DataProtector protect --app <название компонента> --file "путь к файлу appsettings.json"
```

Пример команды

```
.\Cm.Config.DataProtector protect --app CardMonitor --file "C:\Program Files\Indeed CM\CardMonitor\appsettings.json"
```

Расшифровка

1. Перейдите в каталог с дистрибутивом сервера Indeed CM по пути *Misc\dataprotector*.
2. Запустите PowerShell от имени администратора.
3. Выполните одну из команд:

- расшифровка всех файлов конфигурации, расположенных в стандартных директориях (*C:\inetpub\wwwroot\<название компонента>\appsettings.json*):

```
.\Cm.Config.DataProtector unprotect
```

- расшифровка файлов конфигурации отдельных компонентов:

```
.\Cm.Config.DataProtector unprotect --app <название компонента>
```

Пример команды

```
.\Cm.Config.DataProtector unprotect --app ManagementConsole
```

Названия компонентов Indeed CM

- Консоль управления – ManagementConsole
- Сервис самообслуживания – SelfService
- Служба Card Monitor – CardMonitor
- CredentialProvider
- Сервис удаленного самообслуживания – RemoteService
- Сервис API – Api
- Сервис очистки AirCard – AirCardCleaner
- Сервис регистрации агентов – AgentRegistrationApi
- Сервис агентов – AgentServiceApi
- Сервер OpenID Connect – Oidc

- расшифровка файла конфигурации, расположенного вне стандартной директории:

```
.\Cm.Config.DataProtector unprotect --app <название компонента> --file "путь к файлу appsettings.json"
```

Пример команды

```
.\Cm.Config.DataProtector unprotect --app CardMonitor --file "C:\Program Files\Indeed CM\CardMonitor\appsettings.json"
```

Linux

Шифрование

1. Перейдите в директорию с дистрибутивом сервера Indeed CM по пути *Misc\dataprotector*.
2. Откройте Linux Bash.
3. Выполните одну из команд:

- шифрование всех файлов конфигурации, расположенных в стандартных директориях (*/opt/indeed/cm/<название компонента>/appsettings.json*):

```
dotnet Cm.Config.DataProtector.dll protect
```

- шифрование файлов конфигурации отдельных компонентов:

```
dotnet Cm.Config.DataProtector.dll protect --app <название
компонента>
```

Пример команды

```
dotnet Cm.Config.DataProtector.dll protect --app
ManagementConsole
```

Названия компонентов Indeed CM

- Консоль управления – ManagementConsole
- Сервис самообслуживания – SelfService
- Служба Card Monitor – CardMonitor
- CredentialProvider
- Сервис удаленного самообслуживания – RemoteService
- Сервис API – Api
- Сервис очистки AirCard – AirCardCleaner
- Сервис регистрации агентов – AgentRegistrationApi
- Сервис агентов – AgentServiceApi
- Сервер OpenID Connect – Oidc

- шифрование файла конфигурации, расположенного вне стандартной директории:

```
dotnet Cm.Config.DataProtector.dll protect --app <название компонента> --file "путь к файлу appsettings.json"
```

Пример команды

```
dotnet Cm.Config.DataProtector.dll protect --app ManagementConsole --file "/opt/indeed/cm/mc/appsettings.json"
```

Расшифровка

1. Перейдите в директорию с дистрибутивом сервера Indeed CM по пути *Misc\dataprotector*.
2. Откройте Linux Bash.
3. Выполните одну из команд:

- шифрование всех файлов конфигурации, расположенных в стандартных директориях (*???*):

```
dotnet Cm.Config.DataProtector.dll protect
```

- шифрование файлов конфигурации отдельных компонентов:

```
dotnet Cm.Config.DataProtector.dll protect --app <название
компонента>
```

Пример команды

```
dotnet Cm.Config.DataProtector.dll protect --app
ManagementConsole
```

Названия компонентов Indeed CM

- Консоль управления – ManagementConsole
- Сервис самообслуживания – SelfService
- Служба Card Monitor – CardMonitor
- CredentialProvider
- Сервис удаленного самообслуживания – RemoteService
- Сервис API – Api
- Сервис очистки AirCard – AirCardCleaner
- Сервис регистрации агентов – AgentRegistrationApi
- Сервис агентов – AgentServiceApi
- Сервер OpenID Connect – Oidc

- шифрование файла конфигурации, расположенного вне стандартной директории:

```
dotnet Cm.Config.DataProtector.dll protect --app <название
компонента> --file "путь к файлу appsettings.json"
```

Пример команды

```
dotnet Cm.Config.DataProtector.dll protect --app
ManagementConsole --file "/opt/indeed/cm/mc/appsettings.json"
```

Отключение Мастера

В целях безопасности рекомендуется отключить веб-приложение Мастер настройки Indeed CM после завершения процесса конфигурации.

Windows

1. Откройте оснастку **Диспетчер служб IIS** (Internet Information Services Manager).
2. В дереве компонентов **IIS** сервера выберите пункт **Пулы приложений** (Application Pools).
3. В списке **Пулы приложений** выберите **IndeedCM Wizard**.
4. В меню **Действия** в правой части окна Диспетчера служб IIS выберите **Остановить**.

Linux

1. Откройте эмулятор терминала.
2. Выполните команду:

```
sudo systemctl stop cm-wizard.service
```

OpenID Connect

Сервер OpenID Connect предназначен для аутентификации пользователей в веб-приложениях Indeed CM по протоколу OpenID Connect.

Является обязательным для инсталляций системы под управлением ОС Linux и дополнительным для инсталляций под управлением ОС Windows.

> **ПРИМЕЧАНИЕ**
>
> OpenID Connect (OIDC) - это протокол аутентификации и авторизации, разработанный на основе OAuth 2.0, который добавляет слой идентификации к протоколу OAuth. Он позволяет приложениям проверять идентичность пользователя и получать информацию о нем от провайдера идентификации (Identity Provider, IdP).

Windows

Установите сервер OIDC из дополнительного пакета *IndeedCM.Oidc.Server-<номер версии>.x64.ru-ru.msi*. После установки выполните следующие действия:

1. Загрузите сертификат подписи JWT-токенов.
2. Настройте конфигурационный файл *appsettings.json*.

Сертификат подписи JWT-токенов

1. Поместите сертификат подписи JWT-токенов в хранилище *Локальный компьютер - Личное*. В качестве сертификата подписи можно использовать SSL/TLS-сертификат, например, используемый для работы веб-сервера Indeed CM.
2. Предоставьте IIS полный доступ к закрытому ключу сертификата подписи:

    1. Перейдите в оснастку **Сертификаты** (Certificates) компьютера, на котором установлен сервер OIDC.
    2. Кликните правой кнопкой мыши на сертификате, выберите **Все задачи** (All tasks) → **Управление закрытыми ключами...** (Manage Private Keys...).
    3. Нажмите **Добавить** (Add), укажите сервер в меню **Размещение** (Location), укажите локальную группу **IIS_IUSRS** в поле **Введите имена выбранных**

объектов (Enter the object names to select), нажмите **Проверить имена** (Check Names) и **ОК**.

4. Выставите права **Полный доступ** (Full Control) и **Чтение** (Read).
5. Нажмите **Применить** (Apply).

Настройка файла appsettings.json

Настройте конфигурационный файл сервера OIDC через Мастер настройки Indeed CM в разделе **Контроль доступа - OpenID Connect**. После завершения работы Мастера создается файл *appsettings.json* (*C:\inetpub\wwwroot\cm\oidc\appsettings.json*).

В секции `authentication` файла *appsettings.json* указан метод аутентификации пользователей, который будет использовать сервер OIDC. Выберите один из методов: Windows или WindowsCustom. Мастер настройки выставляет значение Windows.

> **МЕТОДЫ WINDOWS И WINDOWS CUSTOM**
>
> Метод Windows используется, если сервер Indeed CM развернут на доменной рабочей станции под управлением ОС Windows.
>
> Метод WindowsCustom используется, если сервер Indeed CM развернут вне домена или пользователи домена Active Directory находятся за пределами домена сервера Indeed CM, и с сервером нет трастовых отношений.

По умолчанию сервер OIDC использует локальную базу данных SQLite. База данных SQLite используется для инсталляций с одним сервером Indeed CM. В этом случае данные сервера OIDC будут храниться в каталоге */opt/indeed/cm/oidc/data*.

Для инсталляций с несколькими серверами Indeed CM используйте базу данных Microsoft SQL или PostgreSQL. Для этого измените секции `defaultConnection` и `provider`:

SQLite

Внесение изменений не требуется. Секции имеют следующие значения:

- `defaultConnection`: "Filename=./data/oidc-server.sqlite3"
- `provider`: "sqlite"

Microsoft SQL

Создайте базу данных в СУБД и настройте в файле подключение к этой базе данных. В примере для подключения к базе данных используется SQL аутентификация:

- `defaultConnection`: "Data Source=172.17.0.10;Initial Catalog=oidcdb;Persist Security Info=True;User ID=servicesql;Password=p@ssw0rd"
- `provider`: "mssql"

PostgreSQL

Создайте базу данных в СУБД и настройте в файле подключение к этой базе данных. Если вы используете файл PGPASS, не включайте директиву `Password` в строку подключения:

- `defaultConnection`: "Host=172.17.0.11;Port=5432;Database=oidcdb;Username=servicepg;Password=p@ssw0rd"
- `provider`: "pgsql"

Перезагрузите сервер OIDC, чтобы применить изменения в конфигурационном файле.

Пример заполненного файла конфигурации для ОС Windows

```
{
"pathBase": "/cm/oidc",
"culture": "ru",
"certHeaderName": "x-ssl-client-cert",
"connectionStrings": {
  "defaultConnection": "Filename=./data/oidc-server.sqlite3"
},
"database": {
  "provider": "sqlite"
},
"oidc": {
  "clients": [
    {
      "clientId": "ManagementConsole",
      "clientSecret":
"9d5d705e1cf5c12b2a5432c5a40c711e6505e939ca2d7cf0df48fc505c022329",
      "displayName": "Management console",
      "type": "confidential",
      "consentType": "implicit",
      "permissions": [ "ept:authorization", "ept:token",
"ept:logout", "gt:authorization_code", "rst:code", "scp:profile",
"scp:roles" ],
      "requirements": [ "ft:pkce" ],
      "redirectUris": [ "https://server.demo.local/cm/mc/signin-
oidc" ],
      "postLogoutRedirectUris": [
"https://server.demo.local/cm/mc/signout-callback-oidc" ]
    },
    {
      "clientId": "SelfService",
      "clientSecret":
"319e8b577563b7c6f27653d72b49659d16f06e0a150fd3a224002c778432319d",
      "displayName": "Self-service",
      "type": "confidential",
      "consentType": "implicit",
      "permissions": [ "ept:authorization", "ept:token",
```

```
"ept:logout", "gt:authorization_code", "rst:code", "scp:profile",
"scp:roles" ],
      "requirements": [ "ft:pkce" ],
      "redirectUris": [ "https://server.demo.local/cm/ss/signin-
oidc" ],
      "postLogoutRedirectUris": [
"https://server.demo.local/cm/ss/signout-callback-oidc" ]
    },
    {
      "clientId": "WebApi",
      "clientSecret":
"9a9c56e5e8090c7fbcdffcc13537fc60d7a2f8547cc92131893e88cf08a7d5f9",
      "displayName": "Web api",
      "type": "confidential",
      "consentType": "implicit",
      "permissions": [ "ept:introspection" ],
      "requirements": [],
      "redirectUris": [],
      "postLogoutRedirectUris": []
    },
    {
      "clientId": "WebApiClient",
      "clientSecret": null,
      "displayName": "Web api client",
      "type": "public",
      "consentType": "implicit",
      "permissions": [ "ept:token", "gt:password", "scp:profile",
"scp:roles", "scp:webapi" ],
      "requirements": [],
      "redirectUris": [],
      "postLogoutRedirectUris": []
    }
  ],
  "signingCertificateThumbprint":
"fed6d86ce6caa079f80d1b6c089cddf109d19c2d",
  "useEphemeralSigningKey": false,
  "disableTransportSecurityRequirement": false,
```

```
    "accessTokenLifetime": 43200,
    "identityTokenLifetime": 43200,
    "authentication": "Windows",
    "allowRememberLogin": false
  },
  "ldap": {
    "directories": [
      {
        "server": "DC_SERVER",
         "port": 389,
         "secureSocketLayer": false,
         "verifyServerCertificate": false,
         "authType": "Basic",
         "userName": "ACCOUNT_NAME",
         "password": "ACCOUNT_PASSWORD",
         "domainDnsName": "DOMAIN_DNS_NAME",
         "domainNetbiosName": "DOMAIN_NETBIOS_NAME"
      }
    ]
  },
  "Logging": {
    "LogLevel": {
      "Default": "Information",
      "Microsoft": "Warning",
      "Microsoft.Hosting.Lifetime": "Information"
    }
  },
  "AllowedHosts": "*"
  }
```

Linux

Сервер OIDC является частью дистрибутива Indeed CM и устанавливается вместе с сервером системы. После установки сервера OIDC выполните следующие действия:

1. Загрузите сертификат подписи JWT-токенов.
2. Настройте конфигурационный файл *appsettings.json*.

Сертификат подписи JWT-токенов

> **ПОДСКАЗКА**
>
> В качестве сертификата подписи можно использовать SSL/TLS-сертификат, например, используемый для работы веб-сервера Indeed CM.

В ОС Linux сертификат использует пользователь, от имени которого запускается сервер OIDC (по умолчанию *www-data*).

Поместите сертификат вместе с закрытым ключом в файл формата PFX в поддиректорию домашнего каталога данного пользователя *~/.dotnet/corefx/cryptography/x509stores/my/* и освободите файл сертификата от пароля.

Для создания такого файла используйте сертификат и закрытый ключ, созданные на этапе настройки веб-сервера NGINX или Apache, или создайте их заново с помощью следующих команд (подставьте имя импортированного файла PFX вместо PFXFILE.pfx):

```
mkdir -p ~/.dotnet/corefx/cryptography/x509stores/my/
openssl pkcs12 -in PFXFILE.pfx -chain -nokeys | sed -ne '/-BEGIN
CERTIFICATE/,/END CERTIFICATE/p' > SSL.crt
openssl pkcs12 -in PFXFILE.pfx -nocerts -out SSLencrypted.key
openssl rsa -in SSLencrypted.key -out SSL.key
rm -f SSLencrypted.key
openssl pkcs12 -export -out
~/.dotnet/corefx/cryptography/x509stores/my/SSL.pfx -inkey SSL.key -
in SSL.crt
```

Настройка файла appsettings.json

Настройте конфигурационный файл сервера OIDC через Мастер настройки Indeed CM в разделе **Контроль доступа**. После завершения работы Мастера создается файл *appsettings.json* (*/opt/indeed/cm/oidc/appsettings.json*).

По умолчанию сервер OIDC использует локальную базу данных SQLite. База данных SQLite используется для инсталляций с одним сервером Indeed CM. В этом случае данные сервера

OIDC будут храниться в каталоге */opt/indeed/cm/oidc/data*.

Для инсталляций с несколькими серверами Indeed CM используйте базу данных Microsoft SQL или PostgreSQL. Для этого измените секции `defaultConnection` и `provider`:

SQLite

Внесение изменений не требуется. Секции имеют следующие значения:

- `defaultConnection`: "Filename=./data/oidc-server.sqlite3"
- `provider`: "sqlite"

Microsoft SQL

Создайте базу данных в СУБД и настройте в файле подключение к этой базе данных. В примере для подключения к базе данных используется SQL аутентификация:

- `defaultConnection`: "Data Source=172.17.0.10;Initial Catalog=oidcdb;Persist Security Info=True;User ID=servicesql;Password=p@ssw0rd"
- `provider`: "mssql"

PostgreSQL

Создайте базу данных в СУБД и настройте в файле подключение к этой базе данных. Если вы используете файл PGPASS, не включайте директиву `Password` в строку подключения:

- `defaultConnection`: "Host=172.17.0.11;Port=5432;Database=oidcdb;Username=servicepg;Password=p@ssw0rd"
- `provider`: "pgsql"

Перезагрузите сервер OIDC, чтобы применить изменения в конфигурационном файле.

Пример заполненного файла конфигурации для ОС Linux

```
{
  "pathBase": "/cm/oidc",
  "culture": "ru",
  "certHeaderName": "x-ssl-client-cert",
  "connectionStrings": {
    "defaultConnection":
"Host=172.17.0.11;Port=5432;Database=oidcdb;Username=servicepsql;Pa
  },
  "database": {
    "provider": "pgsql"
  },
  "oidc": {
    "clients": [
      {
        "clientId": "ManagementConsole",
        "clientSecret":
"6e08e2f151262ddd8db961a18a8d7f3bb2ecaf1ccdf6037b9292a358b56f2ff6",
        "displayName": "Management console",
        "type": "confidential",
        "consentType": "implicit",
        "permissions": [ "ept:authorization", "ept:token", "ept:log
"gt:authorization_code", "rst:code", "scp:profile", "scp:roles" ],
        "requirements": [ "ft:pkce" ],
        "redirectUris": [ "https://astra-174-srv/cm/mc/signin-oidc"
        "postLogoutRedirectUris": [ "https://astra-174-srv/cm/mc/si
oidc" ]
      },
      {
        "clientId": "SelfService",
        "clientSecret":
"48f410e3268d418a89b3d21073fa4962c816adb19899365c3472eb24b1a876af",
        "displayName": "Self-service",
        "type": "confidential",
        "consentType": "implicit",
        "permissions": [ "ept:authorization", "ept:token", "ept:log
"gt:authorization_code", "rst:code", "scp:profile", "scp:roles" ],
```

```
        "requirements": [ "ft:pkce" ],
        "redirectUris": [ "https://astra-174-srv/cm/ss/signin-oidc"
        "postLogoutRedirectUris": [ "https://astra-174-srv/cm/ss/si
oidc" ]
      },
      {
        "clientId": "WebApi",
        "clientSecret":
"e79b81d198478ccb852e8dd7f8ea62750e9626722942ba7dbb57a17119a7d5f0",
        "displayName": "Web api",
        "type": "confidential",
        "consentType": "implicit",
        "permissions": [ "ept:introspection" ],
        "requirements": [],
        "redirectUris": [],
        "postLogoutRedirectUris": []
      },
      {
        "clientId": "WebApiClient",
        "clientSecret": null,
        "displayName": "Web api client",
        "type": "public",
        "consentType": "implicit",
        "permissions": [ "ept:token", "gt:password", "scp:profile",
"scp:webapi" ],
        "requirements": [],
        "redirectUris": [],
        "postLogoutRedirectUris": []
      }
    ],
    "signingCertificateThumbprint": "A85869C270CB2BDB113A28ADF24522
    "useEphemeralSigningKey": false,
    "disableTransportSecurityRequirement": false,
    "accessTokenLifetime": 43200,
    "identityTokenLifetime": 43200,
    "authentication": "WindowsCustom",
    "allowRememberLogin": false
```

```
  },
  "ldap": {
    "directories": [
      {
        "server": "demo.local",
        "port": 389,
        "secureSocketLayer": false,
        "verifyServerCertificate": false,
        "authType": "Basic",
        "userName": "DEMO\\servicecm",
        "password": "Q1w2e3r4",
        "domainDnsName": "demo.local",
        "domainNetbiosName": "DEMO"
      }
    ]
  },
  "Logging": {
    "LogLevel": {
      "Default": "Information",
      "Microsoft": "Warning",
      "Microsoft.Hosting.Lifetime": "Information"
    }
  },
  "AllowedHosts": "*"
}
```

Параметры файла appsettings.json

В файле заполнены секции и параметры, необходимые для работы Indeed CM:

- В параметре `signingCertificateThumbprint` указывается отпечаток сертификата подписи JWT-токенов.
- В секции `clients` Мастер настройки заполняет параметры `clientSecret` (секреты - это пароли, разрешенные для предъявления приложениям системы), `redirectUris` и `postLogoutRedirectUris` для корректной маршрутизации между OIDC и соответствующими веб-приложениями Indeed CM.
- В секции `authentication` указан метод аутентификации пользователей, который будет использовать сервер OIDC – **WindowsCustom**.
- Секция `ldap` заполняется, если в качестве метода аутентификации пользователей выбран **WindowsCustom**. В случае прохождения Мастером настройки секции заполняются автоматически, в случае ручной настройки укажите:
  - `server` - имя хоста или IP-адрес LDAP-сервера.
  - `port` - обычно LDAP-сервер принимает входящие соединения на порт 389 по протоколам TCP или UDP. Для LDAP-сеансов, инкапсулированных в SSL, обычно используется порт 636.
  - `secureSocketLayer` - опция для включения или отключения SSL (Secure Sockets Layer) для защищенного соединения.
  - `verifyServerCertificate` - опция для включения или отключения проверки сертификата сервера при использовании SSL.
  - `authType` - тип аутентификации, который будет использоваться при подключении к LDAP-серверу.
  - `userName` - имя сервисной учетной записи для работы с каталогов пользователем в формате `Имя домена(NetBIOS)\имя учетной записи`.
  - `password` - пароль от сервисной учетной записи.
  - `domainDnsName` - DNS-имя домена.
  - `domainNetbiosName` - NetBIOS-имя домена.

КАК УЗНАТЬ DNS-ИМЯ И NETBIOS-ИМЯ ДОМЕНА

Выполните в командной строке:

`set USERDNSDOMAIN`, чтобы узнать DNS-имя домена.
`set USERDOMAIN`, чтобы узнать NetBIOS-имя домена.

Indeed CM ЭДО

Внутренний электронный документооборот (Indeed CM ЭДО) позволяет администраторам, операторам и пользователям обмениваться документами внутри Indeed CM.

Поддерживаются документы следующих типов:

- **персональные данные** – копии документов, удостоверяющих личность: паспорт гражданина РФ, СНИЛС, ИНН;
- **запрос на сертификат** – подписанная копия заявления на создание сертификата ключа проверки электронной подписи;
- **сведения о сертификате** – подписанная копия сведения о сертификате ключа проверки электронной подписи;
- **запрос на отзыв сертификата** – подписанная копия заявления на прекращение действия сертификата ключа проверки электронной подписи;
- **пользовательские** – другие виды документов, например, подписанный регламент удостоверяющего центра.

> **ПРИМЕЧАНИЕ**
>
> Indeed CM ЭДО является дополнительным компонентом системы, его можно настроить во время первоначальной конфигурации или после развертывания Indeed CM.

Администраторы и операторы могут управлять документами в Консоли управления – раздел **Документы** в карточке пользователя.

Пользователи могут управлять документами в Сервисе самообслуживания в разделе **Ваши документы**.

Порядок настройки

1. Включите опцию **Внутренний документооборот** в разделе **Общие функции** Мастера настройки Indeed CM.
2. Откройте Консоль управления Indeed CM и перейдите в раздел **Конфигурация → Роли**.
3. Предоставьте администраторам и операторам привилегии из меню **Документы** – добавление, изменение, удаление, одобрение.

Единый журнал событий

Единый журнал событий используется для инсталляций Indeed Certificate Manager под управлением ОС Linux или в конфигурациях с несколькими серверами системы под управлением ОС Windows. Единый журнал событий позволяет записывать события со всех серверов в общий журнал.

Единый журнал можно настроить с помощью приложений Indeed CM Event Log Proxy или Indeed Log Server.

> **ПРИМЕЧАНИЕ**
>
> Приложения Indeed CM Event Log Proxy и Indeed Log Server можно установить только на систему под управлением ОС Windows. Например, на один из серверов Indeed CM или на отдельную рабочую станцию (в домене или вне домена).
>
> Системные требования совпадают с требованиями для установки серверных компонентов.

Indeed CM Event Log Proxy

Компонент Indeed CM Event Log Proxy позволяет записывать события с одного или нескольких серверов Indeed Certificate Manager в единый журнал Windows Event Log.

Установите и настройте приложение Indeed CM Event Log Proxy. Выберите инструкцию в зависимости от операционной системы, где установлен сервер Indeed CM:

Windows

1. Выполните вход на рабочую станцию с правами локального администратора.
2. Установите компонент **IndeedCM.EventLog.Proxy-<*номер версии*>.x64.ru-ru.msi** из каталога *IndeedCM.WindowsServer* дистрибутива сервера системы.
3. От имени администратора откройте в редакторе Блокнот файл конфигурации Event Log Proxy *C:\inetpub\wwwroot\cm\eventlogproxy\Web.config*.
4. Задайте параметры аутентификации. Для подключения Windows-сервера Indeed CM к Event Log Proxy используется аутентификация Windows.

В параметре `allow users` укажите учетную запись из домена, где установлен Event Log Proxy. Например, сервисную учетную запись для работы с Active Directory.

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

5. Сохраните изменения и закройте файл конфигурации.
6. Перезапустите пул приложения Indeed CM Event Log Proxy, чтобы сохранить изменения:

    1. Откройте Диспетчер служб IIS (Internet Information Services Manager) и в левом меню выберите **Пул приложений IIS** (Application pools).
    2. Выберите приложение IndeedCM Event Log Proxy и в правом меню нажмите **Перезапуск** (Recycle).

Linux

1. Выполните вход на рабочую станцию с правами локального администратора.
2. Установите компонент **IndeedCM.EventLog.Proxy-<*номер версии*>.x64.ru-ru.msi** из каталога *IndeedCM.LinuxServer* дистрибутива сервера системы.
3. От имени администратора откройте файл конфигурации Event Log Proxy *C:\inetpub\wwwroot\cm\eventlogproxy\Web.config*.
4. Задайте параметры аутентификации. Для подключения Linux-сервера Indeed CM к Event Log Proxy используется аутентификация по сертификатам.

    - В секции `appSettings` укажите значение **True** в параметре `authorizeByCertificate`. В параметре `allowedCertificateThumbprints` укажите отпечаток клиентского сертификата, разрешенного к предъявлению сервером Indeed CM.

```
<appSettings>
    <add key="authorizeByCertificate" value="true" />
    <add key="allowedCertificateThumbprints"
value="aba8b93d73343f2182e3c1c40482b2ae2d75b6ec" />
</appSettings>
```

- Укажите значение **None** в параметре `authentication` и закомментируйте секцию `authorization`.

```
<authentication mode="None" />
<!--
    <authorization>
        <deny users="?"/>
        <allow users="*" />
        <deny users="*" />
    </authorization>
-->
```

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Убедитесь, что выполнены следующие требования для аутентификации по сертификатам в ОС Linux:
>
> - Поле **Улучшенный ключ** (Enhanced Key Usage) сертификата содержит значение **Проверка подлинности клиента** (Client Authentication).
> - Сертификат установлен в хранилище сертификатов сервера Indeed CM.

5. Сохраните изменения и закройте файл конфигурации.
6. Настройте Indeed CM Event Log Proxy для приема сертификатов клиента - сервера Indeed CM. Для этого откройте Диспетчер служб IIS (Internet Information Services Manager) и выполните следующие действия:

    1. Выберите приложение Indeed CM Event Log Proxy и перейдите в **Параметры SSL** (SSL Settings).
    2. В списке **Сертификаты клиента** (Client certificates) выберите значение **Принимать** (Accept).

3. Перезапустите пул приложений IIS, чтобы сохранить изменения. В левом меню выберите **Пул приложений IIS** (Application pools). Выберите приложение IndeedCM Event Log Proxy и в правом меню нажмите **Перезапуск** (Recycle).

Indeed Log Server

Компонент Indeed Log Server позволяет записывать события с одного или нескольких серверов Indeed CM в единый журнал Windows Event Log, Microsoft SQL Server, PostgreSQL Server, SysLog Server.

Установка Indeed Log Server

1. Выполните вход на рабочую станцию с правами локального администратора.
2. Запустите *Indeed.LogServer-<номер версии>.x64.ru-ru.msi* из каталога *Indeed.Log.Server* дистрибутива системы и следуйте указаниям Мастера.
3. Из каталога *Indeed.Log.Server* скопируйте:
   - файл *cmSchema.config* в каталог *C:\inetpub\wwwroot\ls*,
   - файлы *cmEventLogTarget.config*, *cmMsSqlTarget.config*, *cmPgSqlTarget.config* и *cmSysLogTarget.config* в каталог *C:\inetpub\wwwroot\ls\targetConfigs*.

Настройка чтения и записи событий

Настройте чтение и запись событий в следующие хранилища:

- Windows Event Log
- MS SQL
- PostgreSQL
- Syslog

> ⓘ **ПРИМЕЧАНИЕ**
>
> Indeed Log Server поддерживает чтение событий только из одного хранилища (`ReadTargetId`), запись событий возможна одновременно в несколько хранилищ (`WriteTargets`).

Windows Event Log

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

   - 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.

MS SQL

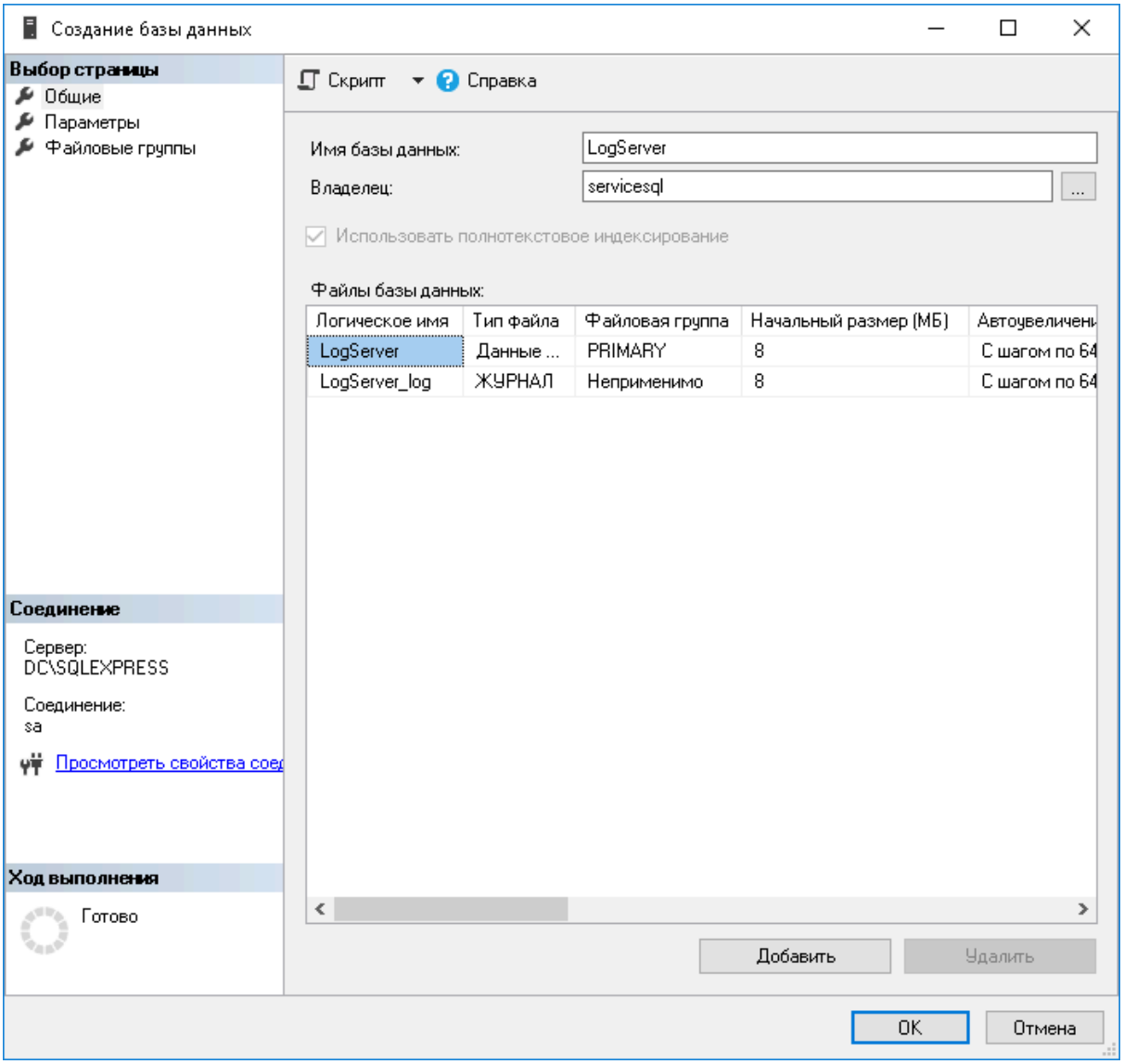
База для хранения данных Indeed Log Server создается вручную, а ее наполнение происходит автоматически.

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

   1. В окне **Обозреватель объектов** (Object Explorer) нажмите правой кнопкой мыши по вкладке **Базы данных** (Databases).
   2. Выберите **Создать базу данных...** (New Database...) и укажите **Имя базы данных:** (Database name:) например, **LogServer**.

3. В поле **Владелец:** (Owner:) определите владельца создаваемой базы.

4. Нажмите **ОК**, чтобы сохранить созданную базу данных.



> **ПРИМЕЧАНИЕ**
>
> Создайте или выберите любую внутреннюю учетную запись MS SQL или Active Directory, Например, сервисную учетную запись для работы Indeed CM.
>
> Указанная учетная запись после создания базы будет обладать правами **db_owner, public** и будет использоваться системой для выполнения операций записи/чтения в базу данных.

2. Перейдите в каталог *C:\inetpub\wwwroot\ls\targetConfigs* и отредактируйте файл *cmMsSqlTarget.config*:
`<Settings>…</Settings>`:

- `Data Source` - имя сервера Microsoft SQL Server или именованного экземпляра Microsoft SQL Server в формате `имя сервера\имя экземпляра`;
- `Database` - имя базы данных (ILS);
- `User Id` - сервисная учетная запись для работы с базами данных Indeed CM;
- `Password` - пароль сервисной учетной записи.

```
<Settings>
    <ConnectionString>Data
Source=MSSQL\SQLEXPRESS;Database=LogServer;User
Id=servicesql;Password=P@ssw0rd</ConnectionString>
</Settings>
```

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

- в секции `Application` добавьте:

```
<Application Id="cm" SchemaId="cmSchema">
    <ReadTargetId>cmMsSqlTarget</ReadTargetId>

    <WriteTargets>
        <TargetId>cmMsSqlTarget</TargetId>
    </WriteTargets>

    <AccessControl>
        <!--<CertificateAccessControl
CertificateThumbprint="001122...AA11" Rights="Read" />-->
    </AccessControl>
</Application>
```

- в секции `Targets` добавьте новый элемент:

```
<Targets>
    <Target Id="cmMsSqlTarget" Type="mssql"/>
</Targets>
```

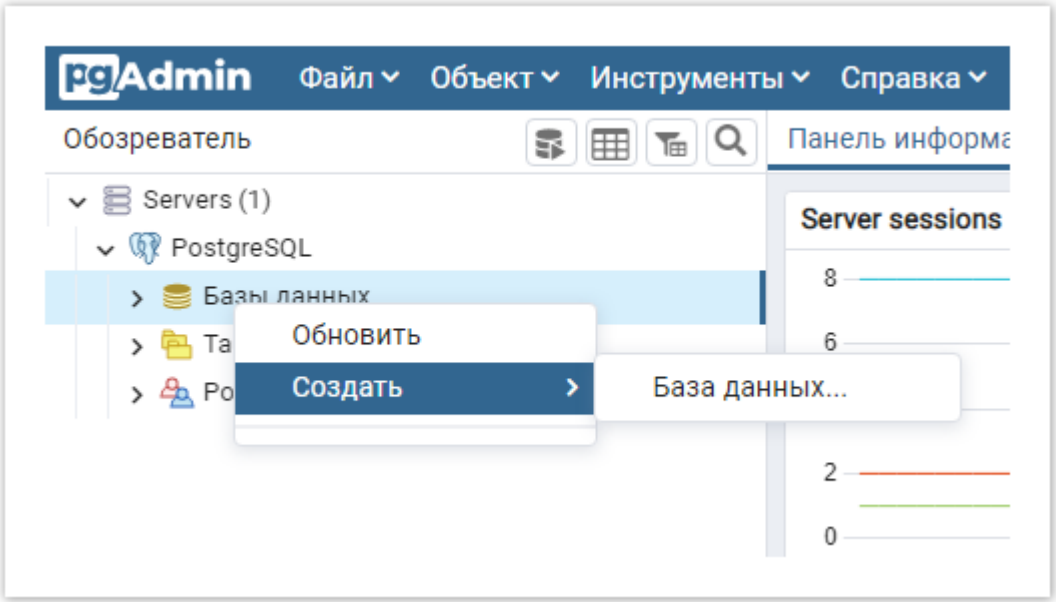
4. Сохраните изменения и закройте файл конфигурации.

PostgreSQL

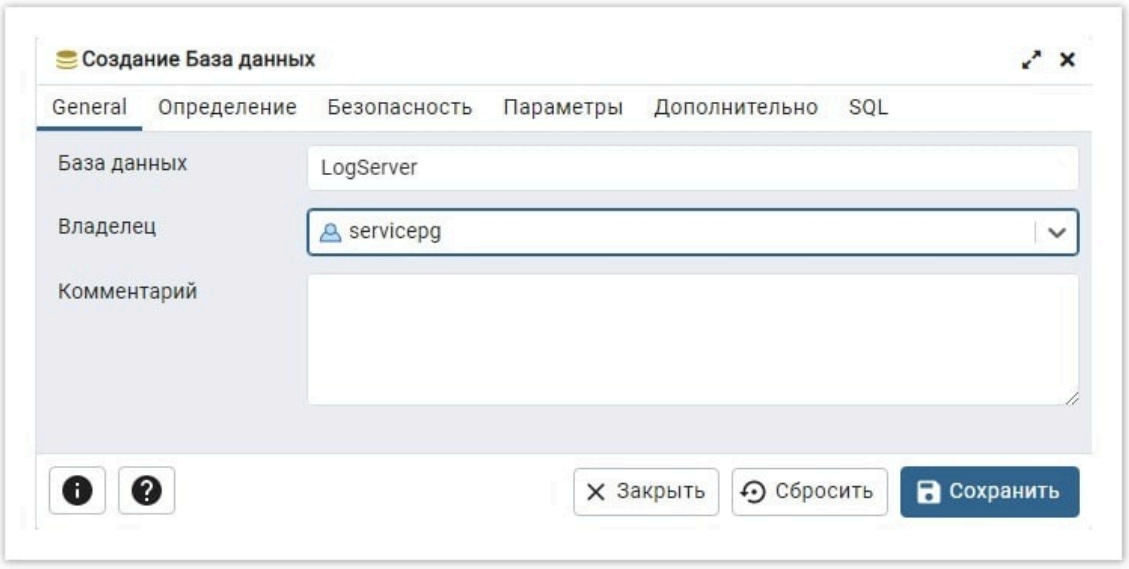
База для хранения данных Indeed Log Server создается вручную, а ее наполнение происходит автоматически.

1. Создайте базу данных в PostgreSQL, например, в среде **pgAdmin**:

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



    3. На вкладке **Общие** (General) укажите произвольное название базы данных в поле **База данных** (Database), например, **LogServer**, выберите из списка **Владелец** (Owner) сервисную четную запись, которая будет использоваться для подключения к базе данных (например, **servicepg**).
    4. Нажмите **Сохранить** (Save).



2. Предоставьте сервисной учетной записи привилегии на таблицы базы данных:

    1. Выделите созданную базу данных в списке и перейдите в меню **Запросника** (Query Tool) (нажмите на  или комбинацией клавиш ALT+SHIFT+Q).
    2. Введите текст запроса, указав в запросе имя учетной записи:

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

    3. В меню Запросника нажмите **Выполнить** (Execute/Refresh).

3. По умолчанию в PostgreSQL разрешены только локальные подключения к базам данных, поэтому для работы между различными серверами требуется настройка удаленного подключения к БД:

    1. В каталоге PostgreSQL откройте конфигурационный файл *pg_hba.conf*. Файл находится в каталоге *C:\Program Files\PostgreSQL\<номер версии>\data* в ОС Windows и в */etc/postgresql/<номер версии>/main* в *nix.
    2. В конце файла добавьте строку следующего типа:

```
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 (ALL для доступа ко всем базам данных);
- `USER` - имя пользователя, для которого будет доступно подключение (ALL для доступа всех пользователей);
- `ADDRESS` - IP-адрес удаленного сервера Indeed Certificate Manager (0.0.0.0/0 для доступа с любых адресов);
- `METHOD` - метод аутентификации пользователя (например, md5, scram-sha-256).

Примеры

```
host LogServer servicepg 192.200.1.0/24 md5
host ALL servicepg 10.0.0.0/8 md5
host ALL ALL 0.0.0.0/0 scram-sha-256
```

4. В каталоге *C:\inetpub\wwwroot\ls\targetConfigs* отредактируйте файл *cmPgSqlTarget.config*:
`<ConnectionString>…</ConnectionString>`:

- `Host` - имя сервера PostgreSQL Server;
- `Port` - порт для подключения к PostgreSQL (5432 — значение по умолчанию);
- `Database` - имя созданной в п.1 базы данных;
- `Username` - сервисная учетная запись для подключения к указанной базе данных;
- `Password` - пароль сервисной учетной записи.

```
<Settings>
    <ConnectionString>Host=SRV-
POSTGRESQL;Port=5432;Database=LogServer;Username=servicepg;Password
</Settings>
```

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

- в секции `Application` добавьте новый `TargetId` для `ReadTarget`, `WriteTarget`:

```
<Application Id="cm" SchemaId="cmSchema">
    <ReadTargetId>cmPgSqlTarget</ReadTargetId>

    <WriteTargets>
        <TargetId>cmPgSqlTarget</TargetId>
    </WriteTargets>

    <AccessControl>
        <!-- <CertificateAccessControl
CertificateThumbprint="001122...AA11" Rights="Read" /> -->
    </AccessControl>
</Application>
```

- в секции `Targets` добавьте новый элемент:

```
<Targets>
    <Target Id="cmPgSqlTarget" Type="pgsql"/>
</Targets>
```

Syslog

> **ПРИМЕЧАНИЕ**
>
> Возможности Syslog ограничены только записью событий (`WriteTargets`). В примере дополняется конфигурация из примера с PostgreSQL.

1. В каталоге *C:\inetpub\wwwroot\ls\targetConfigs* отредактируйте файл *cmSysLogTarget.config*:
   `<ConnectionString>…</ConnectionString>`:

   - `HostName` - имя или IP-адрес Syslog сервера;
   - `Port` - порт Syslog сервера (514 — порт по умолчанию);
   - `Protocol` - тип подключения к Syslog серверу: UDP, TCP, TCPoverTLS;
   - `Format` - опциональный параметр, определяет формат логов: Plain, CEF, LEEF;

- `SyslogVersion` - опциональный параметр, спецификация протокола: RFC3164, RFC5424.

```
<Settings HostName="SRV-SYSLOG" Port="514" Protocol="UDP"/>
```

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

- в секции `Application` добавьте новый `TargetId` для `WriteTarget`:

```
<Applications>
    <Application Id="cm" SchemaId="cmSchema">
        <ReadTargetId>cmPgSqlTarget</ReadTargetId>

        <WriteTargets>
            <TargetId>cmPgSqlTarget</TargetId>
            <TargetId>cmSysLogTarget</TargetId>
        </WriteTargets>

        <AccessControl>
            <!-- <CertificateAccessControl
CertificateThumbprint="001122...AA11" Rights="Read" /> -->
        </AccessControl>
    </Application>
</Applications>
```

- в секции `Targets` добавьте новый элемент:

```
<Targets>
    <Target Id="cmPgSqlTarget" Type="pgsql"/>
    <Target Id="cmSysLogTarget" Type="syslog"/>
</Targets>
```

Чтобы сохранить изменения, перезапустите пул приложений IIS:

1. Откройте Диспетчер служб IIS (Internet Information Services Manager) и в левом меню выберите **Пул приложений IIS** (Application pools).
2. Выберите приложение Indeed Log Server и в правом меню нажмите **Перезапуск** (Recycle).

Настройка Indeed CM для работы с единым журналом событий

Windows

1. Запустите Мастер настройки Indeed CM:
    1. Откройте браузер и перейдите по адресу `https://<FQDN сервера Indeed CM>/cm/wizard`.
    2. Введите код в поле **Код аутентификации** и нажмите **Войти**.
2. Перейдите в раздел **Журнал событий**.
3. Нажмите **Включить Event Log Proxy**, если для единого журнала событий используется приложение **Event Log Proxy**:
    - в поле **URL подключения к Event Log Proxy** укажите URL сервиса Event Log Proxy `https://<FQDN сервера>/cm/eventlogroxy`,
    - в поле **Имя сервисной учетной записи** укажите имя пользователя для подключения к сервису **eventlogproxy** (из секции `authorization` файла *Web.config* приложения Event Log Proxy).
4. Выберите **Использовать Log Server**, если единый журнал событий настроен через приложение **Indeed Log Server**, и укажите **URL подключения к Log Server** – URL сервиса Indeed Log Server `https://<FQDN сервера>/ls/api`.
5. Перейдите в раздел **Подтверждение** и нажмите **Применить**.
6. Примените настройки на сервере Indeed CM:
    1. Откройте консоль Powershell от имени администратора.
    2. Перейдите в директорию *C:\inetpub\wwwroot\cm\wizard\configs*.
    3. Запустите Powershell-скрипт `deploy_configuration.ps1`:

```
.\deploy_configuration.ps1
```

Если в инфраструктуре развернуто несколько серверов Indeed CM, примените файлы конфигурации на каждом сервере.

ПРИМЕЧАНИЕ

В целях безопасности рекомендуется отключить веб-приложение Мастер настройки Indeed CM после завершения конфигурации системы.

1. Откройте Диспетчер служб IIS (Internet Information Services Manager).
2. В левом меню выберите **Пулы приложений** (Application Pools).
3. В списке **Пулы приложений** (Application Pools) выберите **IndeedCM Wizard**.
4. В меню **Действия** (Application Pools Tasks) в правой части окна Диспетчера служб IIS выберите **Остановить**.

7. Перейдите в Консоль управления Indeed CM в браузере и выполните поиск в разделе **Журнал**.

Ожидаемый результат: отсутствие каких-либо ошибок.

ПОДСКАЗКА

Поиск в журнале может не дать результатов, если журнал на удаленном сервере не содержит никаких событий. Выполните в веб-приложениях системы любое действие, результат которого записывается в журнал. Например, выключите устройство, добавьте или измените комментарий и повторите поиск событий.

Linux

1. Запустите Мастер настройки Indeed CM:
    1. Откройте браузер и перейдите по адресу `https://<FQDN сервера Indeed CM>/cm/wizard`.
    2. Введите код в поле **Код аутентификации** и нажмите **Войти**.
2. Перейдите в раздел **Журнал событий**.
3. Нажмите **Включить Event Log Proxy**, если для единого журнала событий используется приложение **Event Log Proxy**:
    - в поле **URL подключения к Event Log Proxy** укажите URL сервиса Event Log Proxy `https://<FQDN сервера>/cm/eventlogroxy`,

- в поле **Отпечаток сертификата** укажите отпечаток клиентского сертификата, который предъявляет сервер Indeed CM для подключения к Event Log Proxy (из секции `appSettings` файла *Web.config* приложения Event Log Proxy).

4. Выберите **Использовать Log Server**, если единый журнал событий настроен через приложение **Indeed Log Server** и укажите **URL подключения к Log Server** – URL сервиса Indeed Log Server `https://<FQDN сервера>/ls/api`.
5. Перейдите в раздел **Подтверждение** и нажмите **Применить**.
6. Примените настройки на сервере Indeed CM:

    1. Откройте эмулятор терминала.
    2. Перейдите в директорию */opt/indeed/cm/wizard/configs*.
    3. Убедитесь, что файл скрипта имеет права на исполнение, и запустите bash-скрипт `deploy_configuration.sh`:

    ```
    sh ./deploy_configuration.sh
    ```

    Если в инфраструктуре развернуто несколько серверов Indeed CM, примените файлы конфигурации на каждом сервере.

> **ПРИМЕЧАНИЕ**
>
> В целях безопасности рекомендуется отключить веб-приложение Мастер настройки Indeed CM после завершения конфигурации системы.
>
> 1. Откройте эмулятор терминала.
> 2. Выполните команду:
>
> ```
> sudo systemctl stop cm-wizard.service
> ```

7. Перейдите в Консоль управления Indeed CM по адресу `https://<FQDN сервера Indeed CM>/cm/mc` и выполните поиск в разделе **Журнал**.

Ожидаемый результат: отсутствие каких-либо ошибок.

ПОДСКАЗКА

Поиск в журнале может не дать результатов, если журнал на удаленном сервере не содержит никаких событий. Выполните в веб-приложениях системы любое действие, результат которого записывается в журнал. Например, выключите устройство, добавьте или измените комментарий и повторите поиск событий.

Indeed CM Agent

Indeed CM Agent (клиентский агент Indeed CM) является дополнительным компонентом системы, который устанавливается после развертывания Indeed Certificate Manager.

Indeed CM Agent позволяет удаленно управлять и контролировать использование устройств пользователей (USB-токенов, смарт-карт).

С помощью агента на рабочих станциях пользователей в автоматическом режиме выполняются следующие операции:

- блокировка и сброс PIN-кода пользователя,
- обновление содержимого устройства,
- очистка и инициализация устройства при отзыве,
- смена PIN-кода администратора устройства,
- контроль использования устройств и блокировка пользовательской сессии и устройства,
- мониторинг устройств с информацией об устройствах с заблокированным PIN-кодом пользователя и администратора, о попытках ввода неверного PIN-кода и о подключении незарегистрированных устройств.

Indeed CM Agent устанавливается вместе с Indeed CM Middleware на рабочие станции, к которым подключаются устройства, выпущенные с помощью Indeed CM.

Установка и настройка Indeed CM Agent

Выберите инструкцию в зависимости от ОС, установленной на сервере Indeed CM:

Windows

Чтобы установить и настроить Indeed CM Agent, выполните следующие действия:

1. Создайте сертификаты сервисов агента.
2. Настройте защищенное соединение с сайтом сервисов агента.
3. Настройте Indeed CM для работы с клиентскими агентами.
4. Установите и настройте агенты на рабочих станциях.

Создание сертификатов сервисов агента

Для работы агента требуются следующие сертификаты:

- **CM Agent CA** – корневой сертификат сервисов агента. Используется для выдачи сертификатов рабочим станциям пользователей, на которых будут устанавливаться Агенты.
- **CM Agent SSL** – сертификат проверки подлинности, подписан корневым сертификатом. Необходим для установки двустороннего 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, а сервер Indeed CM проверяет его подлинность. После проверки сервер добавляет клиентский компьютер в список доверенных и может передавать на него задачи.

Сертификаты сервисов агента создаются с помощью утилиты **Cm.Agent.Cert.Generator**.

Параметры утилиты Cm.Agent.Cert.Generator

Генерация корневого и SSL-сертификата:

`/root` – генерация корневого сертификата сервисов агента.

`/rootKeySize` – размер закрытого ключа корневого сертификата сервисов агента (необязательный параметр, по умолчанию генерируется закрытый ключ размером 4096 бит, возможный диапазон от 512 до 8192 бит).

`/sn <DNS-имя сервера>` – генерация SSL-сертификата на указанное DNS-имя сервера.

`/csn` – генерация SSL-сертификата на имя сервера, на котором запущена утилита.

`/sslKeySize` – размер закрытого ключа SSL-сертификата (необязательный параметр, по умолчанию генерируется закрытый ключ размером 2048 бит, возможный диапазон от 512 до 4096 бит).

`/pwd` – пароль SSL-сертификата (необязательный параметр).

`/installToStore` – публикует сертификаты, выпущенные утилитой, в хранилища сертификатов сервера (необязательный параметр):

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

Генерация только SSL-сертификата с помощью корневого сертификата CM Agent CA:

`/rootKey` – путь до файла корневого сертификата сервисов агента.

`/ssl` – генерация SSL-сертификата сервисов агента.

`/sn <DNS-имя сервера>` – генерация SSL-сертификата на указанное DNS-имя сервера.

`/csn` – генерация SSL-сертификата на имя сервера, на котором запущена утилита.

`/pwd` – пароль SSL-сертификата (необязательный параметр).

`/sslKeySize` – размер закрытого ключа SSL-сертификата (необязательный параметр, по умолчанию генерируется закрытый ключ размером 2048 бит, возможный диапазон от 512 до 4096 бит).

Чтобы создать сертификаты сервисов агента:

1. Перейдите в каталог *IndeedCM.WindowsServer\Misc\AgentCertGenerator* на сервере Indeed CM.
2. От имени администратора запустите в командной строке утилиту **Cm.Agent.Cert.Generator** с параметрами и дождитесь завершения ее работы:

```
Cm.Agent.Cert.Generator.exe /root /csn /installToStore
```

В каталоге с утилитой появятся файлы:

- *agent_root_ca.json* - корневой сертификат сервисов агента с закрытым ключом в формате JSON;
- *agent_root_ca.cer* - корневой сертификат сервисов агента;
- *agent_root_ca.key* - закрытый ключ корневого сертификата сервисов агента;
- *agent_ssl_cert.cer* - SSL-сертификат сайта сервисов агента;
- *agent_ssl_cert.key* - закрытый ключ SSL-сертификата сайта сервисов агента;
- *agent_ssl_cert.pfx* - SSL-сертификат сервисов агента с закрытым ключом в формате PFX.

> ⓘ **ПРИМЕЧАНИЕ**
>
> Поместите сертификат **CM Agent CA (agent_root_ca.cer)** в **Доверенные корневые центры сертификации** (Trusted Root Certification Authorities) на сервере Indeed CM.

Для инсталляций с несколькими серверами Indeed CM

Если в вашей инфраструктуре развернуто несколько серверов Indeed CM с агентами, то для каждого сервера необходимо выпустить SSL-сертификат сервисов агента, используя общий корневой сертификат CM Agent CA. Корневой сертификат сервисов агента на всех серверах должен быть один и тот же.

Для создания SSL-сертификата дополнительного сервера или обновления истекшего сертификата перенесите на сервер каталог с утилитой **Cm.Agent.Cert.Generator** и корневой сертификат сервисов агента с закрытым ключом в формате JSON **(agent_root_ca.json)** и выполните команду:

```
Cm.Agent.Cert.Generator.exe /rootKey <путь к файлу
agent_root_ca.json> /ssl /sn <DNS-имя сервера IndeedCM>
/installToStore
```

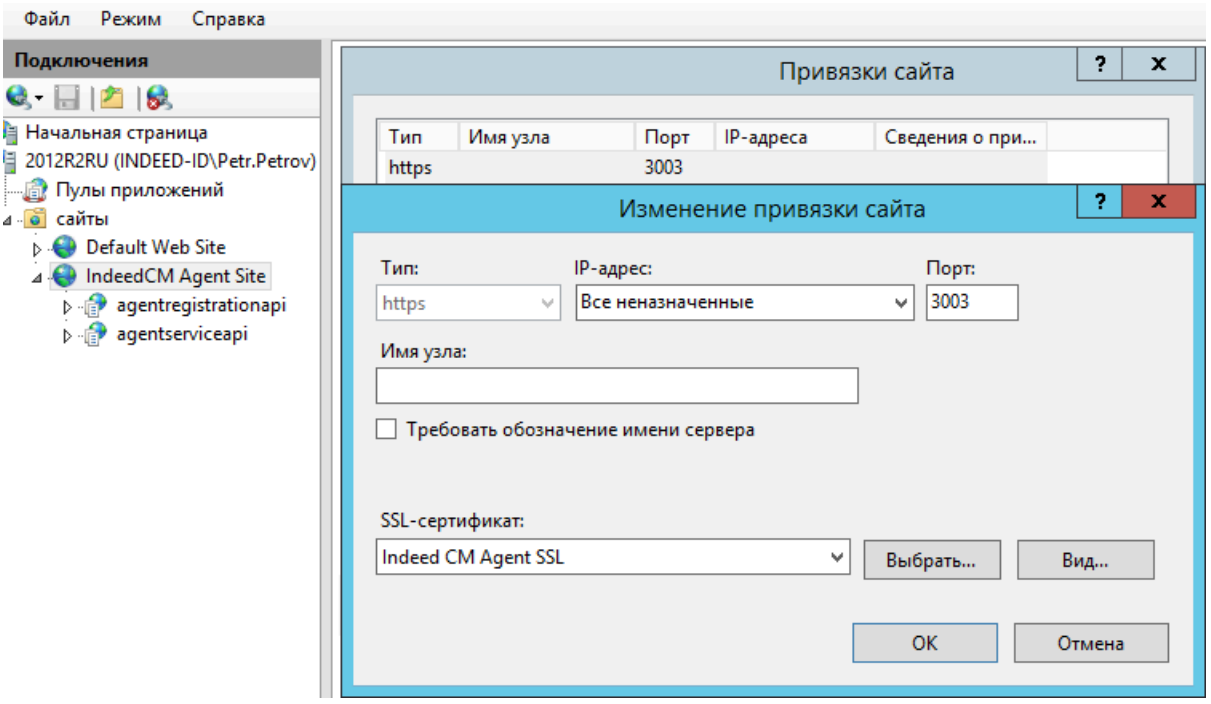
Пример

```
Cm.Agent.Cert.Generator.exe /rootKey
"C:\AgentCertGenerator\agent_root_ca.json" /ssl /sn server.demo.local
/installToStore
```

Настройка защищенного соединения с сайтом сервисов агента

1. Перейдите в **Диспетчер служб IIS** (Internet Information Services (IIS) Manager).
2. Выберите сайт **IndeedCM Agent Site** и перейдите в раздел **Привязки...** (Bindings...).
3. Выберите привязку по порту **3003**.
4. Нажмите **Изменить...** (Edit...).
5. Укажите в качестве **SSL-сертификата** сертификат **CM Agent SSL** или другой SSL/TLS-сертификат, выпущенный с любого доверенного УЦ в инфраструктуре на имя сервера системы и нажмите **OK**.

Пример настройки привязки для сайта IndeedCM Agent Site



Linux

Чтобы установить и настроить Indeed CM Agent, выполните следующие действия:

1. Создайте сертификаты сервисов агента.
2. Настройте защищенное соединение с сайтом сервисов агента.
3. Настройте Indeed CM для работы с клиентскими агентами.
4. Установите и настройте агенты на рабочих станциях.

Создание сертификатов сервисов агента

Для работы агента требуются следующие сертификаты:

- **CM Agent CA** – корневой сертификат сервисов агента. Используется для выдачи сертификатов рабочим станциям пользователей, на которых будут устанавливаться Агенты.
- **CM Agent SSL** – сертификат проверки подлинности, подписан корневым сертификатом. Необходим для установки двустороннего 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, а сервер Indeed CM проверяет его подлинность. После проверки сервер добавляет клиентский компьютер в список доверенных и может передавать на него задачи.

Сертификаты сервисов агента создаются с помощью утилиты **Cm.Agent.Cert.Generator**.

Параметры утилиты Cm.Agent.Cert.Generator

Генерация корневого и SSL-сертификата:

`/root` – генерация корневого сертификата сервисов агента.

`/rootKeySize` – размер закрытого ключа корневого сертификата сервисов агента (необязательный параметр, по умолчанию генерируется закрытый ключ размером 4096 бит, возможный диапазон от 512 до 8192 бит).

`/sn <DNS-имя сервера>` – генерация SSL-сертификата на указанное DNS-имя сервера.

`/csn` – генерация SSL-сертификата на имя сервера, на котором запущена утилита.

`/sslKeySize` – размер закрытого ключа SSL-сертификата (необязательный параметр, по умолчанию генерируется закрытый ключ размером 2048 бит, возможный диапазон от 512 до 4096 бит).

`/pwd` – пароль SSL-сертификата (необязательный параметр).

Генерация только SSL-сертификата с помощью корневого сертификата CM Agent CA:

`/rootKey` – путь до файла корневого сертификата сервисов агента.

`/ssl` – генерация SSL-сертификата сервисов агента.

`/sn <DNS-имя сервера>` – генерация SSL-сертификата на указанное DNS-имя сервера.

`/csn` – генерация SSL-сертификата на имя сервера, на котором запущена утилита.

`/pwd` – пароль SSL-сертификата (необязательный параметр).

`/sslKeySize` – размер закрытого ключа SSL-сертификата (необязательный параметр, по умолчанию генерируется закрытый ключ размером 2048 бит, возможный диапазон от 512 до 4096 бит).

`/installToStore` – публикует SSL-сертификат, выпущенный утилитой, в хранилище **Личных** сертификатов рабочей станции, на которой установлен сервер системы (необязательный параметр).

Чтобы создать сертификаты сервисов агента:

1. Откройте терминал на сервере Indeed CM, перейдите в директорию *IndeedCM.LinuxServer\Misc\AgentCertGenerator* и добавьте право на выполнение файла **Cm.Agent.Cert.Generator:**

```
sudo chmod +x Cm.Agent.Cert.Generator
```

2. Запустите утилиту с параметрами `/root /csn` и дождитесь завершения ее работы:

```
./Cm.Agent.Cert.Generator /root /csn
```

В каталоге с утилитой появятся файлы:

- *agent_root_ca.json* - корневой сертификат сервисов агента с закрытым ключом в формате JSON.
- *agent_root_ca.cer* - корневой сертификат сервисов агента.
- *agent_root_ca.key* - закрытый ключ корневого сертификата сервисов агента.
- *agent_ssl_cert.cer* - SSL-сертификат сайта сервисов агента.
- *agent_ssl_cert.key* - закрытый ключ SSL-сертификата сайта сервисов агента.
- *agent_ssl_cert.pfx* - SSL-сертификат сервисов агента с закрытым ключом в формате PFX.

> **ПРИМЕЧАНИЕ**
>
> Поместите сертификат **CM Agent CA (agent_root_ca.cer)** в **Доверенные корневые центры сертификации** (Trusted Root Certification Authorities) на сервере Indeed CM.

Для инсталляций с несколькими серверами Indeed CM

Если в вашей инфраструктуре развернуто несколько серверов Indeed CM с агентами, то для каждого сервера необходимо выпустить SSL-сертификат сервисов агента, используя общий корневой сертификат CM Agent CA. Корневой сертификат сервисов агента на всех серверах должен быть один и тот же.

Для создания SSL-сертификата дополнительного сервера или обновления истекшего сертификата перенесите на сервер каталог с утилитой **Cm.Agent.Cert.Generator** и корневой сертификат сервисов агента с закрытым ключом в формате JSON **(agent_root_ca.json)** и выполните команду:

```
./Cm.Agent.Cert.Generator /ssl /sn <DNS-имя сервера IndeedCM>
/rootKey <путь к файлу agent_root_ca.json>
```

Пример

```
./Cm.Agent.Cert.Generator /ssl /sn server.demo.local1 /rootKey
./agent_root_ca.json
```

Настройка защищенного соединения с сайтом сервисов агента

Выберите инструкцию в зависимости от ОС, установленной на сервер Indeed CM:

RHEL-based

1. Скопируйте SSL-сертификат сайта агентских сервисов, созданный утилитой **Cm.Agent.Cert.Generator**, и его приватный ключ в хранилище */etc/ssl/* на сервере Indeed CM, а корневой сертификат Агента – в хранилище доверенных корневых сертификатов.

   ```
   sudo cp ./agent_ssl_cert.cer /etc/ssl/
   sudo cp ./agent_ssl_cert.key /etc/ssl/
   sudo cp ./agent_root_ca.cer /etc/pki/ca-trust/source/anchors/
   ```

2. Запустите команду обновления хранилища доверенных корневых сертификатов.

   ```
   sudo update-ca-trust extract
   ```

3. Укажите пути до сертификата и закрытого ключа в конфигурационном файле используемого веб-сервера в разделе, который описывает сайт сервисов агента.

Debian-based

1. Скопируйте SSL-сертификат сайта агентских сервисов, созданный утилитой **Cm.Agent.Cert.Generator**, и его приватный ключ в соответствующие хранилища на сервере Indeed CM, а корневой сертификат Агента – в хранилище доверенных корневых сертификатов. Конвертируйте формат корневого сертификата Агента в CRT.

```
sudo cp ./agent_ssl_cert.cer /etc/ssl/certs/
sudo cp ./agent_ssl_cert.key /etc/ssl/private/
sudo cp ./agent_root_ca.crt /usr/local/share/ca-certificates/
```

2. Запустите команду обновления хранилища доверенных корневых сертификатов.

```
sudo update-ca-trust
```

3. Укажите пути до сертификата и закрытого ключа в конфигурационном файле используемого веб-сервера в разделе, который описывает сайт сервисов агента.

Пример конфигурационного файла веб-сервера NGINX

```
server {
        listen              3003 ssl;
        server_name         server.demo.local;

        ssl_certificate
"/etc/ssl/certs/server.demo.local_ssl_cert.cer";
        ssl_certificate_key
"/etc/ssl/private/server.demo.local_ssl_cert.key";
        ssl_verify_client   optional_no_ca;

        location /agentregistrationapi
             {   include /etc/nginx/conf.d/proxy.conf;
                proxy_pass
http://localhost:5006/agentregistrationapi;  }
        location /agentserviceapi
         {   include /etc/nginx/conf.d/proxy.conf;
                proxy_pass http://localhost:5007/agentserviceapi;
                proxy_set_header x-ssl-client-cert
$ssl_client_escaped_cert;  }
    }
```

Пример конфигурационного файла веб-сервера Apache

```
<VirtualHost *:3003>
    protocols h2 http/1.1

    SSLCertificateFile
/etc/apache2/ssl/server.demo.local_ssl_cert.crt
    SSLCertificateKeyFile
/etc/apache2/ssl/server.demo.local_ssl_cert.key
    SSLCipherSuite @SECLEVEL=1:ECDHE-ECDSA-AES128-GCM-
SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-
SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-
POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-
SHA256:DHE-RSA-AES256-GCM-SHA384

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    SSLEngine on
    SSLProtocol -all +TLSv1.2
    SSLHonorCipherOrder off
    SSLCompression off
    SSLSessionTickets on
    SSLUseStapling off
    SSLProxyEngine on
    RequestHeader set X-Forwarded-Proto https
    Header always set Strict-Transport-Security "max-
age=63072000"

        ProxyPass /agentregistrationapi
http://localhost:5006/agentregistrationapi
        ProxyPassReverse /agentregistrationapi
http://localhost:5006/agentregistrationapi

    <Location "/agentserviceapi">
        SSLVerifyClient optional_no_ca
        SSLOptions +ExportCertData
        RequestHeader unset x-ssl-client-cert
```

```
        RequestHeader set x-ssl-client-cert "expr=%{escape:%
{SSL_CLIENT_CERT}}"
        #RequestHeader set x-ssl-client-cert "expr=%{escape:%
{SSL_CLIENT_S_DN}}"

        ProxyPass http://localhost:5007/agentserviceapi
        ProxyPassReverse http://localhost:5007/agentserviceapi
    </Location>
</VirtualHost>
```

ПРИМЕЧАНИЕ

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

В качестве SSL/TLS-сертификата допускается использование RSA-сертификата, выпущенного с любого доверенного УЦ на имя сервера Indeed CM.

- **Субъект** (Subject) сертификата должен содержать атрибут **Общее имя** (Common name) (FQDN сервера системы).
- **Дополнительное имя субъекта** (Subject Alternative Name) сертификата должно содержать атрибут **DNS-имя** (DNS Name) (FQDN сервера системы).
  Например: *server.demo.local* или соответствующую запись с подстановочными знаками, например: *. *demo.local* (Wildcard certificate).
- **Улучшенный ключ** (Enhanced Key Usage) сертификата должен содержать значение **Проверка подлинности сервера** (Server Authentication).

Настройка Indeed CM для работы с клиентскими агентами

Настройте Indeed Certificate Manager на работу с агентами:

1. Запустите Мастер настройки Indeed CM:

1. Откройте браузер и перейдите по адресу `https://<FQDN сервера Indeed CM>/cm/wizard`.
2. Введите код в поле **Код аутентификации** и нажмите **Войти**.

2. Перейдите в раздел **Клиентский агент**.
3. Включите опцию **Разрешить использование клиентских агентов**.
4. Укажите стратегию генерации **Идентификатора агента для доменных/вне доменных компьтеров** для регистрации в Indeed CM:
   - **Не задано**. Значение по умолчанию.
   - **Использовать машинный GUID**. `MachineGuid` рабочей станции.
   - **Генерировать новый GUID**. Выберите данную опцию, если у нескольких рабочих станций будет одно значение `MachineGuid`.
   - **Использовать доменный SID компьютера**.
   - **Использовать SID компьютера**. Выберите данную опцию, если агент установлен на рабочую станцию, которая находится вне домена. Идентификатору агента присвоится строковое значение `MachineGuid` из ветки реестра *[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography]* рабочей станции.

> ⚠ **СМЕНА СТРАТЕГИИ ГЕНЕРАЦИИ ИДЕНТИФИКАТОРА АГЕНТА**
>
> Если вам нужно сменить **Стратегию генерации идентификатора агента** после первоначальной настройки Indeed CM, выполните следующие действия:
>
> 1. Остановите сервисы агентов agentregistrationapi и agentserviceapi на сервере Indeed CM.
> 2. Удалите все клиентские агенты в разделе **Агенты** Консоли управления или выполните запрос в базу данных системы для удаления зарегистрированных агентов и их сессий.
> 3. Примените изменения в Мастере настройки и распространите измененный файл конфигурации сервиса agentregistrationapi на сервере системы.
> 4. Запустите сервисы агентов agentregistrationapi и agentserviceapi.

5. Для регистрации агентов без подтверждения администратора включите опцию **Автоматическая регистрация Агентов**. Если включить опцию **Автоматическая регистрация Агентов**, то после установки и настройки Агента на рабочей станции он появится в разделе **Агенты** Консоли управления Indeed CM со статусом **Зарегистрирован**.

6. Загрузите сертификат агента – файл корневого сертификата сервисов агента с закрытым ключом в формате JSON *agent_root_ca.json*.
7. Выберите **Уровень журналирования событий агентом**:
    - все (значение по умолчанию),
    - только ошибки,
    - только предупреждения и ошибки.
8. Укажите **Периодичность получения данных с сервера** и **Интервал повторного выполнения отмененной пользователем задачи**.
9. **Имя заголовка HTTP-запроса сертификата** указано по умолчанию. Если Indeed CM используется с балансировщиком нагрузки. Включите опцию **Передавать только поле 'Субъект' сертификата агента в заголовках HTTP-запросов** при использовании Indeed CM с балансировщиком нагрузки, чтобы снизить трафик.
10. Перейдите в пункт **Подтверждение** и нажмите **Применить** для сохранения настроек.
11. Примените настройки на сервере Indeed CM.

Клиентские компоненты

Установите на рабочие станции пользователей следующие клиентские компоненты:

Indeed CM Client Tools

Компонент для разблокировки устройств

Indeed CM Middleware

Компонент для работы с USB-токенами и смарт-картами

Indeed CM Agent

Компонент для удаленного контроля устройств

Indeed CM Client Tools

Indeed CM Client Tools – клиентский компонент Indeed CM, необходимый для разблокировки устройств, которые используются для аутентификации в ОС Windows в режимах онлайн и офлайн, и для разблокировки устройств, которые не используются для входа в ОС.

Установите Indeed CM Client Tools на рабочие станции пользователей. Запустите файл **IndeedCM.Client.Tools-<*номер версии*>.ru-ru.msi** из каталога *IndeedCM.Client* дистрибутива системы и выполните установку, следуя указаниям мастера.

Разблокировка устройств реализована в двух режимах: онлайн и офлайн.

Онлайн
В онлайн-режиме рабочая станция пользователя, к которой подключено заблокированное устройство, имеет соединение с сервером Indeed CM. Соединение с сервером необходимо для аутентификации пользователя с помощью ответов на секретные вопросы. Для связи рабочих станций пользователей с сервером Indeed CM при онлайн-разблокировке рекомендуется использовать защищенное соединение https.

Офлайн
В офлайн-режиме оператор Indeed CM разблокирует устройство по принципу аутентификации вида запрос-ответ (challenge-response authentication mechanism). При исчерпании заданного числа попыток ввода PIN-кода пользователь получает сообщение о блокировке устройства и уникальный 16-символьный код-запрос. Пользователю необходимо связаться с оператором системы (например, по телефону) и подтвердить свою личность.

Настройка онлайн-разблокировки устройств

Настройте разблокировку устройств через групповые политики или реестр Windows (для рабочих станций вне домена Windows).

Групповые политики

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

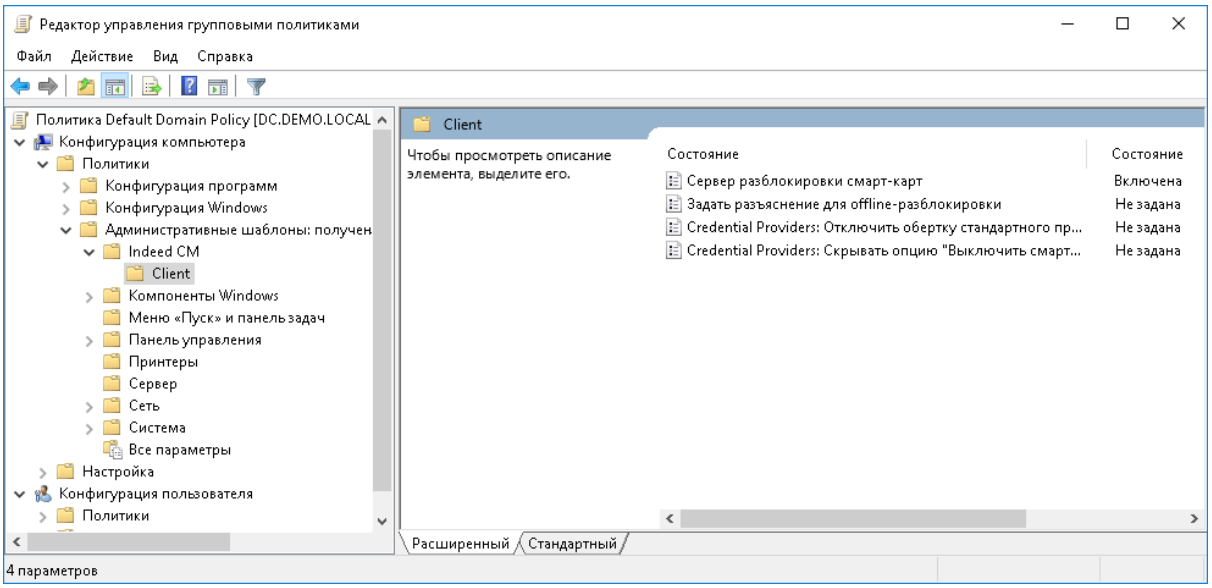
Добавьте административные шаблоны компании Индид:

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

> **ПРИМЕЧАНИЕ**
>
> При использовании локального хранилища ADMX-файлов поместите шаблоны компании Индид 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 ее значения:

- в параметре **URL сервиса** (Service URL) укажите ссылку на компонент **credprovapi**, размещенный на сервере Indeed CM: https://<*FQDN сервера Indeed CM*>/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 обновите политики.

При необходимости настройте дополнительные политики, определяющие работу сервиса разблокировки.

Дополнительные политики сервиса разблокировки

Политика	Параметры
Задать разъяснения для офлайн-разблокировки (Set explanations for offline unlocking)	Политика применяется к рабочим станциям пользователей. Если политика выключена или не определена, то при офлайн-разблокировке устройства текст разъяснения в Credential Provider не отображается. Если политика включена,то при офлайн-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.

Политика	Параметры
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.

Реестр Windows

Если сервер Indeed CM и рабочие станции пользователей находятся вне домена Windows, пропишите путь к приложению **credprovapi** 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
```

- `CredProvAPIURL`: задайте адрес приложения credprovapi на сервере Indeed CM.
- `AdminDetails`: задайте текст разъяснения для пользователя.
- `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.

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

Пример файла REG

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\IndeedCM\Client]
"CredProvAPIURL"="https://server.demo.local/cm/credprovapi"
"AdminDetails"="Свяжитесь с администратором по внутреннему номеру
1607"
"DisableServerCertificateChecking"=dword:00000000
"DisableSuspendCP"=dword:00000001
"DisableWrapperCP"=dword:00000001
```

В примере указано имя машины *server.demo.local*, включена проверка подлинности сертификата сервера, отключено отображение кнопки **Выключить смарт-карту** и включена опция разблокировки смарт-карты в отдельном Credential Provider на экране входа в ОС.

Indeed CM Middleware

Indeed CM Middleware – клиентский компонент Indeed CM, необходимый для работы с устройствами (USB-токенами, смарт-картами).

> **ПРИМЕЧАНИЕ**
>
> Для работы Indeed CM Middleware на рабочих станциях пользователей должны быть установлены драйвера и сервисные утилиты устройств и считывателей, которые будут использоваться с Indeed CM. Данное ПО не входит в комплект поставки Indeed CM.

Windows

Установите компоненты Middleware на рабочие станции операторов и пользователей под управлением ОС Windows.

Для разных типов устройств предусмотрены разные файлы Middleware.

Запустите файл **IndeedCM.<*имя типа устройства*>.Middleware.<*номер версии*>.ru-ru.msi** из каталога *IndeedCM.Client* дистрибутива системы и выполните установку, следуя указаниям мастера.

Таблица соответствия производителей, моделей устройств и файлов Middleware

Производитель	Модели устройств	Middleware
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	IndeedCM.JaCarta.Middleware-<*номер версии*>.ru-ru.msi
Компания «Актив»	Рутокен Lite и смарт-карта Рутокен Lite Рутокен S Рутокен ЭЦП PKI и смарт-карта Рутокен ЭЦП PKI Рутокен ЭЦП 2.0 и смарт-карта Рутокен ЭЦП 2.0 Рутокен 2151 и смарт-карта Рутокен 2151 Рутокен ЭЦП 3.0 NFC и смарт-карта Рутокен ЭЦП 3.0 NFC	IndeedCM.Rutoken.Middleware-<*номер версии*>.ru-ru.msi

Производитель	Модели устройств	Middleware
Компания Индид	Сетевая смарт-карта AirCard	IndeedCM.AirCard.Middleware-<*номер версии*>.ru-ru.msi
ACS	ACOS5-64	IndeedCM.ACOS.Middleware-<*номер версии*>.ru-ru.msi
Avest	Avest Key 256A	IndeedCM.Avest.Middleware-<*номер версии*>.ru-ru.msi
Bit4id	ID-One Cosmo	IndeedCM.Bit4Id.Middleware-<*номер версии*>.ru-ru.msi
CRYPTAS	TicTok V2/V3	IndeedCM.TicTok.Middleware-<*номер версии*>.ru-ru.msi
Cryptovision	ePasslet Suite v3.0, JCOP V3.0	IndeedCM.Cryptovision.Middleware-<*номер версии*>.ru-ru.msi
Feitian	ePass2003 (A1+, A2) BioPass2003	IndeedCM.ePass.Middleware-<*номер версии*>.ru-ru.msi
HID	Crescendo C1150 Series Crescendo C1300 Series Crescendo C2300 Series	IndeedCM.HID.Middleware-<*номер версии*>.ru-ru.msi

Производитель	Модели устройств	Middleware
ISBC	ESMART Token USB 64K и ESMART Token CARD 64K ESMART Token USB 192K и ESMART Token CARD 192K ESMART Token USB ГОСТ и ESMART Token CARD ГОСТ MS_KEY K-"Ангара"	IndeedCM.ESMART.Middleware-<*номер версии*>.ru-ru.msi
Kaztoken	Kaztoken, Kaztoken SC	IndeedCM.Kaztoken.Middleware-<*номер версии*>.ru-ru.msi
Microsoft	Реестр Локального компьютера Реестр Пользователя	IndeedCM.Registry.Middleware-<*номер версии*>.ru-ru.msi Для возможности выпуска устройств Registry с записью сертификатов в локальное хранилище компьютера и/или пользователя через Сервис самообслуживания включите поддержку устройств Registry через групповую политику.

Производитель	Модели устройств	Middleware
	TPM Virtual Smart Card (Microsoft VSC) - виртуальная смарт-карта на базе Trusted Platform Module v.2.0	IndeedCM.TPM.Middleware-<*номер версии*>.ru-ru.msi
	Windows Hello for Business (WHfB)	IndeedCM.WHfB.Middleware-<*номер версии*>.ru-ru.msi
RSA	RSA SecurID 800	IndeedCM.RSA.Middleware-<*номер версии*>.ru-ru.msi
Thales (SafeNet и 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-<*номер версии*>.ru-ru.msi
	IDPrime MD 830 IDPrime MD 840 IDPrime MD 3810 IDPrime MD 3811	IndeedCM.Gemalto.Middleware-<*номер версии*>.ru-ru.msi

Производитель	Модели устройств	Middleware
Yubico	YubiKey 5 Series	IndeedCM.YubiKey.Middleware-<*номер версии*>.ru-ru.msi

Linux

Установите компоненты Middleware на рабочие станции операторов и пользователей под управлением ОС Linux.

В Indeed CM для ОС Linux поддерживаются устройства Рутокен, JaCarta, ESMART и SafeNet eToken. Для всех типов устройств предусмотрен единый Middleware.

RHEL-based

Установите Middleware из пакета **cm.middleware-<*номер версии*>.x86_64.rpm**:

```
sudo rpm -i cm.middleware-<номер версии>.x86_64.rpm
```

Debian-based

Установите Middleware из пакета **cm.middleware-<*номер версии*>_amd64.deb**:

```
sudo dpkg -i cm.middleware_<номер версии>_amd64.deb
```

Таблица моделей устройств, поддерживаемых Indeed CM на ОС Linux

Производитель	Модели устройств
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
Компания «Актив»	Рутокен Lite и смарт-карта Рутокен Lite Рутокен ЭЦП PKI и смарт-карта Рутокен ЭЦП PKI Рутокен ЭЦП 2.0 и смарт-карта Рутокен ЭЦП 2.0 Рутокен 2151 и смарт-карта Рутокен 2151 Рутокен ЭЦП 3.0 NFC и смарт-карта Рутокен ЭЦП 3.0 NFC
ISBC	ESMART Token USB 64K и ESMART Token CARD 64K ESMART Token USB 192K и ESMART Token CARD 192K ESMART Token USB ГОСТ и ESMART Token CARD ГОСТ
Thales (SafeNet и 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

Поддержка устройств Registry

Настройте поддержку устройств Registry через групповые политики или реестр Windows (для рабочих станций вне домена Windows).

Групповые политики

Чтобы разрешить пользователям Indeed CM выпускать устройства Registry с записью сертификатов в локальное хранилище компьютера и/или пользователя через **Сервис самообслуживания**, настройте соответствующую групповую политику. Политика должна распространяться на рабочие станции пользователей Indeed CM.

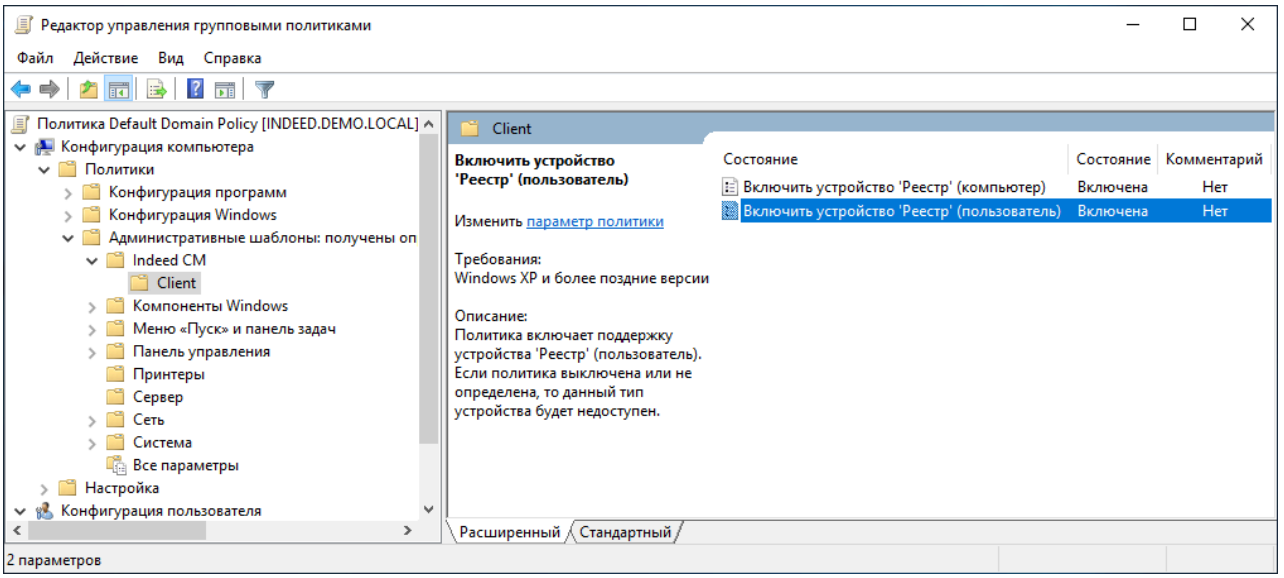
Добавьте административные шаблоны компании Индид:

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

> **ПРИМЕЧАНИЕ**
>
> При использовании локального хранилища ADMX-файлов поместите шаблоны 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 обновите политики.

Реестр Windows

Если сервер Indeed CM и рабочие станции пользователей находятся вне домена Windows, задайте возможность выпуска устройств Registry 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
```

- `MachineRegistryCardEnabled`: установите значение **1** (dword:00000001), если требуется выпуск сертификатов в локальное хранилище рабочей станции.
- `UserRegistryCardEnabled`: установите значение **1** (dword:00000001), если требуется выпуск сертификатов в хранилище пользователя рабочей станции.

Пример файла REG

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\IndeedCM\Client]
"MachineRegistryCardEnabled"=dword:00000001
"UserRegistryCardEnabled"=dword:00000001
```

В примере включена возможность выпускать устройства Registry в хранилище компьютера и пользователя.

Indeed CM Agent

Indeed CM Agent (клиентский агент Indeed CM) позволяет удаленно управлять и контролировать использование устройств пользователей (USB-токенов, смарт-карт).

Установите Indeed CM Agent вместе с Indeed CM Middleware на рабочие станции пользователей Indeed CM. Запустите файл **IndeedCM.Agent-<*номер версии*>.ru-ru.msi** из каталога *IndeedCM.Client* дистрибутива системы и установите Indeed CM Agent, следуя указаниям мастера. После установки агент запустится автоматически.

Задайте настройки для связи с сервером Indeed CM через групповые политики или реестр Windows.

Групповые политики

Для добавления административных шаблонов компании Индид выполните следующие действия:

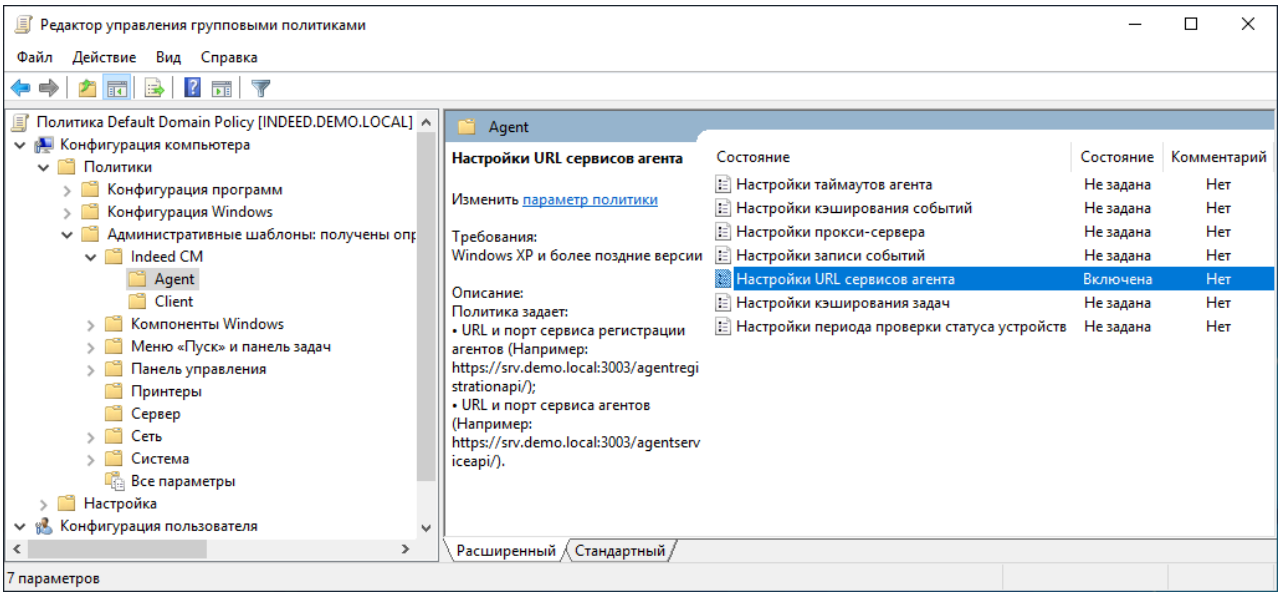
1. Скопируйте содержимое каталога *IndeedCM.Client\Misc* в центральное хранилище ADMX-файлов контроллера домена *C:\Windows\SYSVOL\domain\Policies\PolicyDefinitions*.

> **ПРИМЕЧАНИЕ**
>
> При использовании локального хранилища ADMX-файлов поместите шаблоны компании Индид 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 ее значения:

- в параметре **URL сервиса регистрации агентов** (Agents registration service URL) укажите веб-адрес и порт подключения к приложению **agentregistrationapi**, размещенного на сервере Indeed CM.
- в параметре **URL сервиса агентов** (Agents service URL) укажите веб-адрес и порт сервиса **agentserviceapi**.

> ⓘ **ПРИМЕРЫ URL**
>
> **URL сервиса регистрации агентов**:
> `https://server.demo.local:3003/agentregistrationapi/`
> **URL сервиса агентов**: `https://server.demo.local:3003/agentserviceapi/`



7. Свяжите этот объект политики с группой, членами которой являются рабочие станции пользователей Indeed CM.
8. Нажмите **Применить** (Apply) и обновите политики. Чтобы обновить политики, перезагрузите рабочую станцию с установленным клиентским агентом. Для принудительного обновления групповых политик без перезагрузки выполните команду `gpupdate/force`.

Вы можете настроить дополнительные политики, определяющие работу Агентов.

Дополнительные политики Агента

Политика	Параметры
Настройки таймаутов агентов (Agent's timeouts settings)	- 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)	- 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.

Политика	Параметры
Настройки кэширования задач (Tasks caching settings)	- 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

Реестр Windows

Создайте файл реестра REG со следующим содержанием:

```
Windows Registry Editor Version 5.00

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

ПОДСКАЗКА

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 веб-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 ИСПОЛЬЗОВАНИЯ ПРОКСИ-СЕРВЕРА

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

Пример файла REG

```
Windows Registry Editor Version 5.00

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

В примере файла REG указано имя сервера Indeed CM *server.demo.local*, протокол *https*, порт *3003*, прокси-сервер *https://192.168.10.10:443*.

⚠ **ПРЕДУПРЕЖДЕНИЕ**

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**.

Браузеры

Для доступа к веб-приложениям Indeed CM выполните настройку браузеров на рабочих станциях администраторов, операторов и пользователей.

Windows

Microsoft Edge, Google Chrome, Chromium, Яндекс.Браузер

1. Откройте **Панель управления** Windows (Control Panel), выберите **Свойства браузера** (Internet Options).
2. Перейдите на вкладку **Безопасность** (Security), выберите зону **Местная интрасеть** (Local Intranet), нажмите **Сайты** (Sites) → **Дополнительно** (Advanced).
3. Добавьте узлы:

- https://<*FQDN сервера Indeed CM*> (например, `https://server.demo.local`);
- адрес для работы через WebSocket `wss://localhost`.

> **ПОДСКАЗКА**
>
> Необходимые адреса можно добавить в зону **Местная интрасеть** (Local Intranet) через групповую политику **Список назначений зоны для веб-сайтов** (Site to Zone Assignment List).
>
> Политика располагается по пути: **Конфигурация пользователя** (User Configuration) → **Политики** (Policies) → **Административные шаблоны** (Administrative Templates) → **Компоненты Windows** (Windows Components) → Internet Explorer → **Панель управления браузером** (Internet Control Panel) → **Безопасность** (Security Page).

Mozilla Firefox

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

Linux

Установите в браузер расширение Indeed CM Middleware.

Google Chrome, Chromium, Яндекс.Браузер

Расширение можно установить следующими способами:

- через интернет-магазин Chrome;
- через файл CRX из дистрибутива Indeed CM LinuxClient.

Установка расширения через файл CRX

1. Запустите браузер и перейдите по ссылке:

- `chrome://extensions` для Google Chrome и Chromium,
- `browser://extensions` для Яндекс.Браузера.

2. Включите режим разработчика.
3. Нажмите **Загрузить распакованное расширение** в левом верхнем углу экрана.
4. Выберите каталог *IndeedCM.LinuxClient-v<номер версии>\cm.middleware.chrome.extension*.

Mozilla Firefox

1. Запустите браузер и перейдите по ссылке `about:addons`.
2. Нажмите  и выберите **Установить дополнение из файла…**.
3. Выберите файл *cm.middleware-1.0.xpi* из каталога *IndeedCM.LinuxClient-v<номер версии>* и нажмите **Открыть**.
4. Нажмите **Добавить** во всплывающем окне.

Руководство администратора

Операторы и администраторы могут управлять Indeed Certificate Manager в веб-приложении **Консоль управления** (Management Console).

Аутентификация в Консоли управления осуществляется в соответствии с конфигурацией, выбранной на этапе развертывания системы.

Консоль управления доступна по адресу *https://<FQDN сервера Indeed CM>/cm/mc*.

До начала работы с Indeed Certificate Manager выполните следующие действия:

1. Настройте привилегии пользователей
2. Добавьте файл лицензии в систему.
3. Добавьте необходимые типы устройств.
4. Настройте политики использования устройств.
5. Назначьте политики на пользователей Indeed CM.

Конфигурация

Политики

Создание и редактирование политик использования устройств

Назначения политик

Централизованное управление объектами или пользователями

Лицензии

Управление лицензиями

Типы устройств

Настройки типов и моделей устройств, управление PIN-кодами администратора и пользователя

Организационная структура

Объединение объектов каталога пользователей под действие одной политики использования устройств

Роли

Полномочия администраторов и операторов

Теги

Настройка тегов для гибкого учета устройств в организации

Шаблоны печати

Настройка шаблонов документов

СКЗИ

Управление средствами криптографической защиты информации

Журналы учета

Настройка справочников и шаблонов журналов

Политики

Политика определяет разрешенные и запрещенные действия пользователей при использовании устройств.

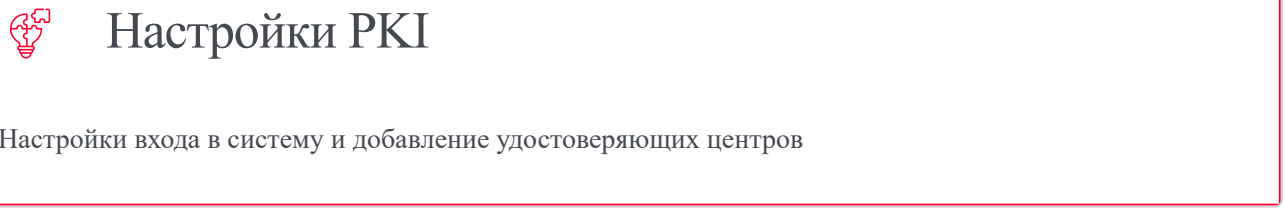
Создайте политики использования устройств:

1. Откройте Консоль управления Indeed Certificate Manager и перейдите на вкладку **Конфигурация → Политики**.
2. Нажмите **Создать политику**.
3. Укажите отображаемое имя политики в параметре **Имя** или скопируйте параметры ранее созданной политики в параметре **Копировать из**.
4. Нажмите **Создать**.

Чтобы удалить политику, выберите ее в списке и нажмите ✖ → **Удалить**.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Политику можно удалить только в том случае, если в Indeed CM нет ни одного устройства, выпущенного с применением этой политики.

После создания политики откроются ее параметры. В разделе **Общие** отображается имя политики, которое можно изменить в случае необходимости.



Secret Net Studio

Настройка интеграции с Secret Net Studio

СМЭВ

Настройка интеграции с Системой межведомственного электронного взаимодействия

Поведение

Настройка доступных действий для администраторов, операторов и пользователей Indeed CM

Выпуск

Настройка параметров выпуска и инициализации устройства

Аутентификация

Настройки аутентификации пользователей

Агенты

Параметры работы Indeed CM Agent

Принтер смарт-карт

Настройка интеграции с принтером смарт-карт

Уведомления

Настройки почтовых уведомлений о событиях Indeed CM

Настройки PKI

Настройте параметры входа в операционную систему:

- **Импортировать сертификаты УЦ**

Если опция включена, то при выпуске устройства на него будет записан корневой сертификат или цепочка сертификатов удостоверяющего центра (УЦ). Такие сертификаты не удаляются с устройства при его изъятии из Indeed CM.

> **ПРИМЕЧАНИЕ**
>
> Убедитесь, что устройство поддерживает запись корневого сертификата или цепочки сертификатов.

- **Требовать логон по смарт-карте**

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

> **ПРЕДУПРЕЖДЕНИЕ**
>
> - Сервисная учетная запись для работы с каталогом пользователей должна обладать правами на **Запись:userAccountControl** (Write userAccountControl) в Active Directory (см. раздел **Настройка каталога пользователей в Active Directory**).
> - Если включить опцию **Для интерактивного входа в сеть нужна смарт-карта** (Smart card is required for interactive logon) в профиле пользователя Active Directory, доменный пароль пользователя будет изменен на случайный, и срок действия этого пароля будет неограничен. Подробнее на сайте компании Microsoft.
> - Перед настройкой опции **Требовать логон по смарт-карте** убедитесь, что шаблон для сертификата **Вход со смарт-картой** (Smartcard Logon) добавлен в политику использования устройств.

Удостоверяющие центры

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

Indeed CM поддерживает работу с множеством УЦ. Вы можете добавить несколько УЦ для одной политики или создать несколько политик и для каждой указать свой УЦ.

Microsoft CA

ПОДСКАЗКА

Раздел доступен для настройки при активированной опции **Включить интеграцию с Microsoft CA Enterprise** в разделе **Microsoft CA** Мастера настройки Indeed CM.

Выберите инструкцию в зависимой от операционной системы, где установлен сервер Indeed CM:

Windows

Чтобы добавить УЦ, выполните следующие действия:

1. Нажмите **Добавить УЦ**.
2. В поле **Адрес** задайте адрес УЦ, если он не определился автоматически.
3. Укажите данные сервисной учетной записи, обладающей сертификатом **Агент регистрации** (Enrollment Agent).
4. Нажмите **Добавить**.

ПРЕДУПРЕЖДЕНИЕ

Наличие пользователя с сертификатом **Агент регистрации** (Enrollment Agent) является обязательным условием для работы Indeed CM с УЦ. От имени этого пользователя будут отправляться запросы в указанный УЦ на выдачу сертификатов пользователям Indeed CM. Учетные данные этого пользователя можно изменить после добавления УЦ в Indeed CM.

Для изменения учетных данных пользователя с сертификатом **Агент регистрации** (Enrollment Agent) выберите нужный удостоверяющий центр и нажмите  справа от имени пользователя.

Для удаления УЦ нажмите  .

Чтобы добавить УЦ, расположенный за пределами домена пользователей Indeed CM, выполните следующие действия:

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

> **ПРИМЕЧАНИЕ**
>
> Если Indeed CM развернут в лесу доменов, использовать Indeed CM MSCA Proxy необязательно. В этом случае в поле **Адрес** укажите имя УЦ.

3. Укажите данные учетной записи пользователя (логин в формате `ДОМЕН\ИМЯ` и пароль), обладающего сертификатом **Агент регистрации** (Enrollment Agent) на УЦ, расположенном вне домена с каталогом пользователей Indeed CM.
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*. Сертификаты пользователям этого домена выпускаются в УЦ, развернутом в этом домене. 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 в УЦ, расположенных в независимых доменах.

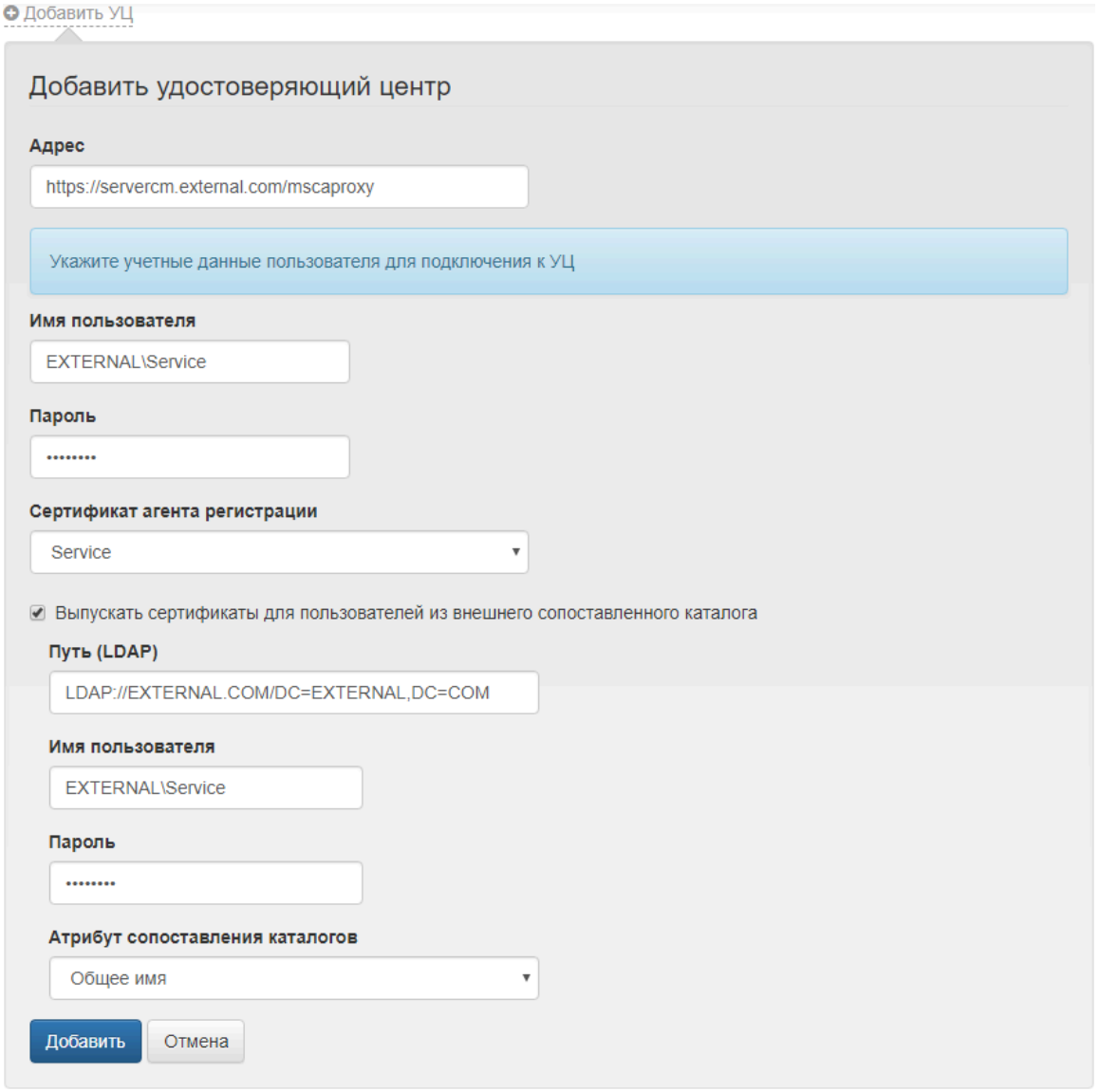
> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Выпуск сертификатов для пользователей внешнего каталога будет успешен только при совпадении атрибута соответствия с основным каталогом пользователей.
>
> **Например**: адрес электронной почты, указанный в свойствах учетной записи пользователя в домене *demo.local* должен совпадать с адресом электронной почты, указанным в свойствах учетной записи пользователя в домене *external.com*.

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

> 💡 **ПОДСКАЗКА**
>
> Для настройки разрешения на чтение только необходимого набора свойств перейдите в раздел **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



Linux

Чтобы добавить УЦ, выполните следующие действия:

1. Нажмите **Добавить УЦ**.
2. В поле **Адрес** укажите URL-адрес приложения Indeed CM MSCA Proxy.
3. В поле **Клиентский сертификат** выберите сертификат клиентской аутентификации для подключения к Indeed CM MSCA Proxy.

4. Нажмите **Добавить**.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Наличие сертификата клиентской аутентификации является обязательным условием для работы Indeed CM с Microsoft CA для инсталляций на ОС Linux.

Если УЦ находится за пределами домена пользователей Indeed CM:

1. Включите опцию **Выпускать сертификаты для пользователей из внешнего сопоставленного каталога**.
2. В поле **Путь (LDAP)** укажите путь к каталогу пользователей Indeed CM внешнего домена.

> ⓘ **ПРИМЕР**
>
> Indeed CM развернут в домене *demo.local*. Сертификаты пользователям этого домена выпускаются в УЦ, развернутом в этом домене. 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 в УЦ, расположенных в независимых доменах.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> 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*.

3. В поле **Имя пользователя** укажите учетную запись (в формате `ДОМЕН\ИМЯ`), обладающую правами на чтение всех свойств пользователей во внешнем домене.

ПОДСКАЗКА

Для настройки разрешения на чтение только необходимого набора свойств перейдите в раздел **Настройка каталога пользователей в Active Directory**.

4. 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.

КриптоПро УЦ 2.0

ПОДСКАЗКА

Раздел содержит параметры работы с удостоверяющими центрами КриптоПро УЦ 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.

Чтобы добавить удостоверяющий центр, выполните следующие действия:

1. Нажмите **Добавить УЦ**:

2. Введите **URL-адрес веб-службы Центра Регистрации**. В зависимости от используемого варианта исполнения КриптоПро УЦ 2.0 укажите:

   - URL-адрес в полном или сокращенном виде для вариантов исполнений 5, 6, 9, 10 для ОС Windows:

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

   - URL-адрес для вариантов исполнений для вариантов исполнений 15 и 16 для ОС Windows и ОС Astra Linux SE:

```
https://<host_name>
```

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

4. Выберите тип API в зависимости от используемого варианта исполнения КриптоПро УЦ 2.0:

   - REST для вариантов исполнений 15 и 16 для ОС Windows и ОС Astra Linux SE;
   - SOAP для вариантов исполнений 5, 6, 9, 10 для ОС Windows.

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

6. Установите связь между пользователями КриптоПро УЦ и пользователями каталога, если это требуется (опция **Устанавливать привязку между пользователем УЦ и пользователем каталога**).

7. Нажмите **Добавить**.

Установить связь между пользователями каталога и пользователями УЦ необходимо, если каталог пользователей 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 собственного УЦ выдавать сертификаты одного или нескольких других УЦ.

Если включить опцию **Устанавливать привязку между пользователем УЦ и пользователем каталога**, Indeed CM позволяет определить следующие параметры работы с УЦ:

- **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 КриптоПро УЦ 2.0 при выпуске или обновлении устройства. Например, поменять адрес электронной почты, если он изменился в профиле пользователя в Active Directory. Включите опцию **Обновлять учетные данные пользователя УЦ**, если необходимо обновить данные.

> **ПРИМЕЧАНИЕ**
>
> 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.

Валидата УЦ

> **ПОДСКАЗКА**
>
> 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 режиме онлайн и/или офлайн.

Офлайн-режим

1. Нажмите **Добавить УЦ**, чтобы добавить удостоверяющий центр.
2. Укажите **Каталог для обмена файлами с ЦР/ЦС** – каталог для обмена файлами Indeed CM с Центром Регистрации.

ПРИМЕЧАНИЕ

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

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

    1. Укажите **Подкаталог для запросов** – подкаталог для входящих незащищенных запросов пользователей в формате PKCS#10. Обработка запросов в формате PKCS#10 выполняется в ручном режиме на АРМ Администратора ЦР.
    2. Укажите **Подкаталог для сертификатов** – подкаталог сертификатов для выдачи конечным пользователям.

4. Нажмите **Добавить**.

Онлайн-режим

В онлайн-режиме Indeed CM заменяет 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.
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.

ПРИМЕЧАНИЕ

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.

ПРИМЕЧАНИЕ

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

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

    1. Укажите **Подкаталог для запросов** – подкаталог запросов в формате CMS/PKCS#7 для Центра Сертификации, обработанных Оператором ЦР.
    2. Укажите **Подкаталог для сертификатов** – подкаталог сертификатов в формате CMS/PKCS#7, обработанных Центром Сертификации.

6. Нажмите **Добавить**.

КриптоПро DSS 2.0

ПОДСКАЗКА

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.
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). Например, `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 учетные данные пользователя DSS**. Если опция включена, то при обновлении или выпуске устройства обновятся данные пользователя DSS.
4. Заполните поля и нажмите **Добавить**.

Общие сертификаты

Общие сертификаты используются в сценарии, когда сертификат, уже выпущенный вне Indeed CM, и закрытый ключ необходимо записать на устройства множества пользователей с помощью Indeed CM.

Особенности работы 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** задается в пункте **Уведомления администратора**. Рассылка происходит при достижении 10% до окончания срока действия сертификата. Для истекших сертификатов уведомления перестают отправляться.

> **ПРИМЕЧАНИЕ**
>
> 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.

Шаблоны сертификатов

В разделе **Шаблоны** задаются шаблоны для сертификатов пользователей.

> **ПРЕДУПРЕЖДЕНИЕ**
>
> Перед началом работы с шаблонами сертификатов в Indeed CM убедитесь, что необходимые шаблоны настроены и добавлены в центр сертификации Microsoft CA. См. разделы **Настройка шаблонов сертификатов** и **Добавление шаблонов сертификатов**.

Чтобы создать шаблон сертификата, нажмите **Создать шаблон сертификата**, задайте необходимые **Параметры шаблона сертификата** и нажмите **Создать**.

> **ПРИМЕЧАНИЕ**
>
> 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 .

Параметры шаблонов сертификатов

Настройте шаблоны сертификатов для используемых удостоверяющих центров.

Microsoft CA

Параметр	Описание
Имя	Имя шаблона сертификата
УЦ	Имя удостоверяющего центра.
Шаблон сертификата УЦ	Загружается из выбранного удостоверяющего центра.

Параметр	Описание
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 системе (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.

Параметр	Описание
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).

Параметр	Описание
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.
Создавать резервную копию ключа	Если опция включена, то при генерации ключевой пары на смарт-карте будет применена опция ее 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 выключена, 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.

Параметр	Описание
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. 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 Сервис самообслуживания записанные на него сертификаты добавятся в локальное хранилище пользователя на рабочей станции.

Параметр	Описание
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 список отозванных сертификатов	Если опция включена, то при выключении, включении и отзыве устройств список отозванных сертификатов (CRL) опубликуется вне очереди. Таким образом пользователь не сможет подписывать документы отозванным сертификатом. Опция доступна, если сервисная учетная запись для работы с Microsoft CA имеет разрешение **Управлять ЦС**.
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.

Параметр	Описание
Требовать подписанный документ сертификата перед продолжением выпуска/обновления устройства	Если опция включена, то сертификат будет записан на устройство только после того, как пользователь предоставит на проверку администратору подписанную форму сертификата. После одобрения запроса в УЦ форма сертификата будет доступна пользователю в Сервисе самообслуживания. Пользователь может скачать и подписать форму сертификата и предоставить ее на проверку.
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, 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 задан, то используется стандартный шаблон печати запроса на сертификат. Если в систему добавлены **Шаблоны печати запроса сертификата**, то выберите шаблон из выпадающего меню.

Параметр	Описание
Шаблон печати сертификата	Если параметр не задан, 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 задан, 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.
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.

КриптоПро УЦ 2.0

Параметр	Описание
Имя	Имя шаблона сертификата.
УЦ	Имя удостоверяющего центра.
Шаблон сертификата УЦ	Загружается из выбранного удостоверяющего центра.

Параметр	Описание
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 системе (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.
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.

Параметр	Описание
Создавать резервную копию ключа	Если опция включена, то при генерации ключевой пары на смарт-карте будет применена опция ее 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 выключена, то копии сертификатов и закрытых ключей не будут записаны на временное устройство при замене.
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.

Параметр	Описание
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. 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 сервис самообслуживания 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.

Параметр	Описание
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 список отозванных сертификатов (CRL) опубликуется вне очереди. Таким образом пользователь не сможет подписывать документы отозванным сертификатом.

Параметр	Описание
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.
Требовать подписанный документ сертификата перед продолжением выпуска/обновления устройства	Если опция включена, то сертификат будет записан на устройство только после того, как пользователь предоставит на проверку администратору подписанную форму сертификата. После одобрения запроса в УЦ форма сертификата будет доступна пользователю в Сервисе самообслуживания. Пользователь может скачать и подписать форму сертификата и предоставить ее на проверку.

Параметр	Описание
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 задан, 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 задан, то используется стандартный шаблон печати сертификата. Если в систему добавлены **Шаблоны печати сертификата**, то выберите шаблон из выпадающего меню.

Параметр	Описание
Шаблон печати запроса на отзыв сертификата	Если параметр не задан, 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.
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.

Валидата УЦ

Параметр	Описание
Имя	Имя шаблона сертификата.
УЦ	Имя удостоверяющего центра.
Шаблон сертификата УЦ	Загружается из выбранного удостоверяющего центра.

Параметр	Описание
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 системе (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.
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.
Создавать резервную копию ключа	Если опция включена, то при генерации ключевой пары на смарт-карте будет применена опция ее 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.

Параметр	Описание
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 выключена, то копии сертификатов и закрытых ключей не будут записаны на временное устройство при замене.
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. 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 Сервис самообслуживания записанные на него сертификаты добавятся в локальное хранилище пользователя на рабочей станции.

Параметр	Описание
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.

Параметр	Описание
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, 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 задан, 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 задан, то используется стандартный шаблон печати сертификата. Если в систему добавлены **Шаблоны печати сертификата**, то выберите шаблон из выпадающего меню.

Параметр	Описание
Шаблон печати запроса на отзыв сертификата	Если параметр не задан, 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.
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.

КриптоПро DSS 2.0

Параметр	Описание
Имя	Имя шаблона сертификата.
Сервер	Имя сервера DSS.
УЦ	Имя удостоверяющего центра.
Шаблон сертификата УЦ	Загружается из выбранного удостоверяющего центра.

Параметр	Описание
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.
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.
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.
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.

Параметр	Описание
Требовать подписанный документ сертификата перед продолжением выпуска/обновления устройства	Если опция включена, то сертификат будет записан на устройство только после того, как пользователь предоставит на проверку администратору подписанную форму сертификата. После одобрения запроса в УЦ форма сертификата будет доступна пользователю в Сервисе самообслуживания. Пользователь может скачать и подписать форму сертификата и предоставить ее на проверку.
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.

Indeed AM

> **ПОДСКАЗКА**
>
> Настройка доступна при включении опции **Интеграция с Indeed Access Manager** в разделе **Общие функции** Мастера настройки Indeed CM.

Indeed Certificate Manager можно интегрировать с другими продуктами компании Индид – Indeed Access Manager и Indeed AM Enterprise Single Sign-On. Интеграция позволит объединить в единый процесс операции выпуска устройства, запроса сертификата, записи сертификата и регистрации аутентификатора «Смарт-карта или USB-ключ + PIN» пользователя Indeed AM.

Выпущенное подобным образом устройство можно использовать 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 Indeed CM и Indeed AM состоит из двух этапов:

1. Установка и настройка компонентов.
2. Конфигурирование параметров интеграции.

Установка и настройка компонентов

1. Установите следующие компоненты:

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

> **ПОДСКАЗКА**
>
> **Indeed Administration Tools** поставляется в дистрибутиве Indeed Access Manager.
> **Indeed Extended Security Provider** и **Indeed AM SmartCard Provider** предоставляет по запросу служба технической поддержки компании Индид

2. Настройте Extended Security Provider:

1. Создайте группу безопасности Indeed-ID Enrollment Admins согласно Руководству по установке и эксплуатации Indeed Extended Security Provider.
2. Добавьте сервисную учетную запись в группы безопасности Indeed-ID User Admins и Indeed-ID Enrollment Admins.

Параметры интеграции с Indeed AM

Чтобы задать параметры интеграции с Indeed AM, перейдите в конфигурацию выбранной политики использования устройств и откройте раздел **Indeed AM**.

Параметр	Описание
Включить интеграцию с Indeed AM	Если опция включена, то при выпуске устройства в Indeed CM будет выпускаться и аутентификатор «Смарт-карта или USB-ключ + PIN» в 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 установлен 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.

Параметр	Описание
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.

Если удалить последний зарегистрированный аутентификатор пользователя, то разрешения на использование Indeed AM Windows Logon, Indeed AM Enterprise Single Sign-On и генерацию случайного пароля будут выключены.

ПРИМЕР

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

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

Indeed Certificate Manager можно интегрировать с продуктом компании "Код безопасности" – Secret Net Studio (SNS) версии 8.4 и выше. Интеграцию можно установить для инсталляций сервера Indeed CM на ОС Windows.

Возможности интеграции:

- при выпуске устройства в Indeed CM устройство будет добавлено в базу данных SNS (пользователю будет присвоен персональный идентификатор SNS), и на устройство будет записан персональный индентификатор SNS;
- при замене устройства в Indeed CM новое устройство будет добавлено в базу данных SNS и присвоено пользователю, если в базе данных SNS содержалась информация о заменяемом устройстве; если не было то запись идентификатора возможна через перевыпуск или обновление устройства
- при отзыве устройства у пользователя в Indeed CM отменится присвоение идентификатора пользователю, и устройство будет удалено из базы данных SNS.

Особенности интеграции:

- для интеграции SNS с устройствами, уже выпущенными в Indeed CM, устройства необходимо обновить;
- персональный идентификатор можно записать только на устройства, которые поддерживаются в SNS.

ПОДДЕРЖИВАЕМЫЕ ВЕРСИИ SECRET NET STUDIO

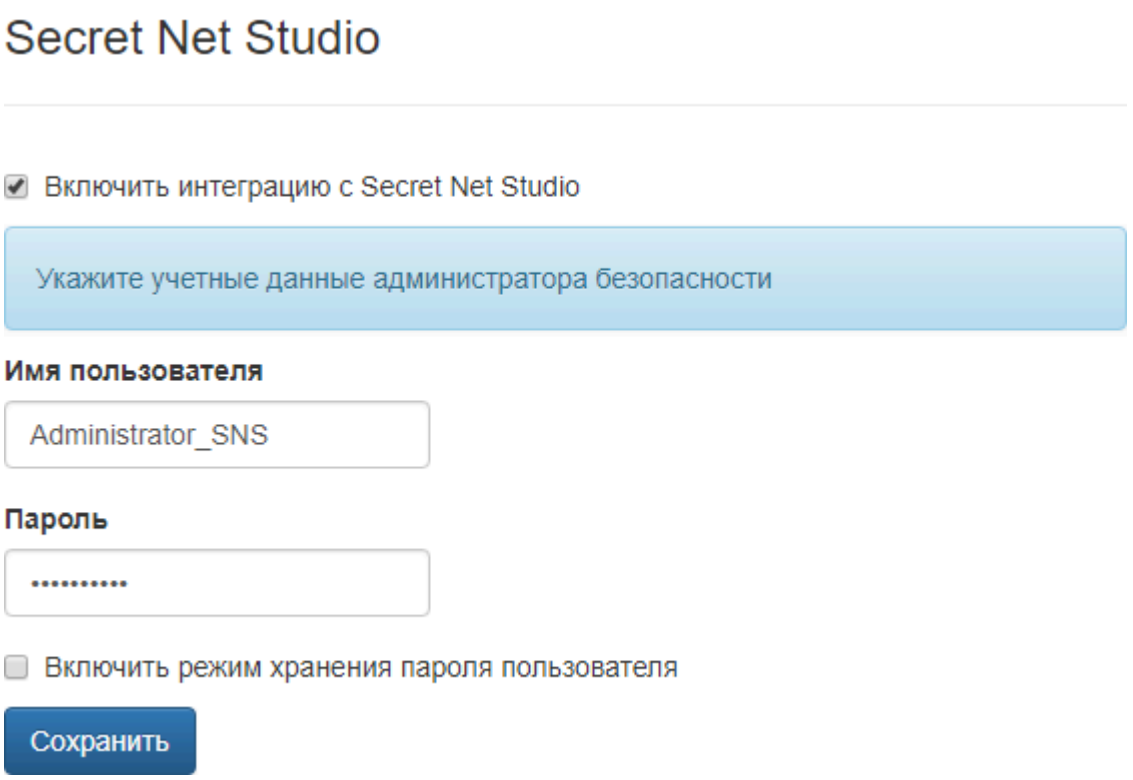
Indeed CM поддерживает Secret Net Studio версии 8.4 и выше:

- версия **8.4.2863** устанавливается с патчем **8_4_2863_106_Inc85078_Build80**;
- версия **8.5.5329** устанавливается с патчем **8_5_5329_64_Inc85077_Build43**;
- для версий 8.6 и выше не требуется установка дополнительных патчей.

Патчи предоставляет по запросу служба технической поддержки компании "Код безопасности".

Для интеграции Indeed CM с Secret Net Studio выполните следующие действия:

1. Для подключения к базе данных SNS установите на сервер Indeed CM "SNS клиент" с базовой функциональностью.
2. Установите "SNS клиент" на клиентские рабочие станции, с которых будут выпускаться устройства.
3. Откройте раздел **Конфигурация** в Консоли управления Indeed CM, перейдите в настройки политики использования устройств и выберите вкладку **Secret Net Studio**.
4. Нажмите **Включить интеграцию с Secret Net Studio**.
5. Укажите учетную запись, входящую в группу администраторов безопасности SNS.
6. Задайте опцию **Включить режим хранения пароля пользователя** при необходимости. При выпуске устройства в Indeed CM на него будет записан идентификатор SNS с режимом хранения доменного пароля пользователя.
7. Нажмите **Сохранить**.


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

СМЭВ

ПОДСКАЗКА

Настройка СМЭВ отображается в Консоли управления Indeed CM, если в разделе **Общие функции** Мастера настройки Indeed CM включить опцию **Интеграция со СМЭВ**.

Проверка данных пользователя в СМЭВ доступна при выпуске или обновлении устройства, если согласно политике использования устройств пользователю нужно выпустить или обновить сертификат КриптоПро УЦ 2.0 или Валидата УЦ.

Indeed Certificate Manager можно интегрировать 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. Нажмите **Включить интеграцию со СМЭВ**.
2. Укажите **URL-адрес шлюза КриптоПро СМЭВ**.
3. Выберите **Сертификат оператора шлюза СМЭВ**.
4. Нажмите **Сохранить**.

ПРИМЕЧАНИЕ

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

СМЭВ

Включить интеграцию со СМЭВ

URL-адрес шлюза КриптоПро СМЭВ

https://cryptopro/smevgateway/api/v2.1

Сертификат оператора шлюза СМЭВ

OperatorSmev

Сохранить

Поведение

В разделе **Поведение** политики использования устройств задаются настройки, которые определяют доступные операции для администраторов/операторов в Консоли управления и для пользователей в Сервисе самообслуживания.

Опция	Описание	Значение по умолчанию
Разрешить сброс PIN-кода устройства	Разрешить администратору сбросить PIN-кода пользователей устройств.	Включена
Разрешить пользователю сброс PIN-кода устройства	Разрешить пользователю сбросить PIN-кода своего устройства.	Отключена
Разрешить пользователю очистку устройства	Разрешить пользователю очистить содержимое своего устройства при его отзыве оператором с причинами **Изъятие устройства** и **Обновление устройства**. После очистки устройство останется назначенным пользователю.	Отключена
Разрешить пользователю обновление устройства	Разрешить пользователю обновлять сертификаты, хранящиеся на его устройстве, если их срок действия истек или истекает.	Включена
Разрешить пользователю выпуск устройства КриптоПро DSS	Если опция включена, то пользователи могут самостоятельно выполнять запрос и выпуск устройств DSS. Если опция выключена, то выпустить устройство КриптоПро DSS может только администратор или оператор.	Отключена

Опция	Описание	Значение по умолчанию
Разрешить пользователю выпуск AirCard карты	Если опция включена, то пользователи смогут самостоятельно выпускать карты AirCard в Сервисе самообслуживания. Выпуск карт AirCard возможен только при настроенной интеграции с Indeed AirCard Enterprise (см. установка и настройка Indeed AirCard Enterprise).	Отключена
Разрешить пользователю выключение устройства	Разрешить пользователю выключение своего устройства (если оно была включено ранее).	Включена
Разрешить пользователю выбор необязательных сертификатов при обновлении устройства	Если опция включена, то при обновлении устройства в Сервисе самообслуживания пользователь может записать на него сертификаты, отмеченные как необязательные, по шаблонам, выбранным из списка. Если опция выключена, то выбор шаблонов необязательных сертификатов не будет доступен пользователю при обновлении устройства. Вы можете задать сообщение, которое отображается в виде предупреждения в окне выбора необязательных сертификатов, когда пользователь выпускает или обновляет устройство. Для этого введите текст в поле **Сообщение пользователю при выборе необязательных сертификатов**.	Отключена

Опция	Описание	Значение по умолчанию
Разрешить пользователю выбор необязательных сертификатов при выпуске устройства	Если опция включена, то при выпуске устройства в Сервисе самообслуживания пользователь может записать на него сертификаты, отмеченные как необязательные, по шаблонам, выбранным из списка. Если опция выключена, то выбор шаблонов необязательных сертификатов не будет доступен пользователю при выпуске устройства.	Отключена
Разрешить пользователю включение устройства	Разрешить пользователю включить свое устройство, если оно было выключено ранее.	Включена
Разрешить пользователю удаление устройства КриптоПро DSS	Если опция включена, то пользователи могут самостоятельно отзывать и удалять устройство DSS. Если опция выключена, то отзывать и удалять устройства DSS могут только администраторы или операторы Indeed CM.	Отключена
Разрешить пользователю редактирование данных в форме проверки в СМЭВ	Если опция включена, то пользователи могут редактировать данные, полученные из Active Directory, в форме проверки в СМЭВ. Если опция выключена, то редактировать пользовательские данные в форме проверки в СМЭВ могут только администраторы или операторы Indeed CM.	Включена

Опция	Описание	Значение по умолчанию
Разрешить пользователю просмотр СКЗИ	Если опция включена, список СКЗИ будет доступен пользователям в Сервисе самообслуживания.	Отключена
Разрешить пользователю удаление документа	Если опция включена, то пользователи могут удалять свои документы в Сервисе самообслуживания.	Отключена
Разрешить пользователю отзыв устройства	Разрешить пользователю отзывать свои устройства.	Включена
Разрешить пользователю назначение устройства	Разрешить пользователю выпустить устройство, которое не назначили на этого пользователя.	Отключена
Разрешить пользователю изменение ответов на секретные вопросы	Если опция включена, то пользователи могут изменять ответы на секретные вопросы после их установки в Сервисе самообслуживания. Если опция выключена, то пользователям не смогут менять ответы на секретные вопросы. Администраторы и операторы могут сбросить ответы на секретные вопросы, чтобы пользователи могли их установить.	Отключена
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

Опция	Описание	Значение по умолчанию
Разрешить офлайновую разблокировку	Опция позволяет разблокировать устройство пользователя с привлечением администратора системы, если отсутствует соединение между рабочей станцией пользователя и сервером Indeed CM. Чтобы разблокировать устройство, пользователь должен знать ответы 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
Пользователь должен задать ответы на секретные вопросы при первом входе в сервис самообслуживания	Если опция включена, то при первичном входе в Сервис самообслуживания пользователь должен 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 не будет отображаться. Пользователь сможет установить секретные вопросы позднее в любой момент.	Включена

Опция	Описание	Значение по умолчанию
Добавлять устройство автоматически	Опция позволяет добавлять устройство в систему (если оно не было добавлено ранее) в момент выпуска или назначении устройства пользователю. Если опция выключена, то выпуск или назначение устройства, подключенного к компьютеру, но не добавленного в систему, запрещен.	Отключена

Опция	Описание	Значение по умолчанию
Включить отслеживание сертификатов	Если опция включена, то при выпуске устройства Indeed CM найдет на устройстве сертификаты и закрытые ключи. Поддерживается отслеживание сертификатов, выпущенных удостоверяющими центрами Microsoft CA, КриптоПро УЦ 2.0, ViPNet УЦ 4, Валидата УЦ. Indeed CM может отправить уведомление об истечении срока действия сертификатов. Для этого создайте для администратора и пользователя уведомление о событии **Отслеживаемые сертификаты истекают** в разделе **Уведомления**. Отслеживаемые сертификаты можно распечатать в Консоли управления и в Сервисе самообслуживания по стандартному шаблону печати сертификата. Чтобы данные по отслеживаемым сертификатам попадали в журналы учета, включите опцию **Добавлять отслеживаемые сертификаты** в журналы учета. Опция **Добавлять отслеживаемые сертификаты в журналы учета** доступна, если включить **Журнал учета устройств и сертификатов** в разделе **Общие функции** Мастера настройки Indeed CM.	Отключена

Выпуск

Задайте параметры выпуска и инициализации устройства.

Выпуск 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 можно отключить или включить инициализацию для конкретного устройства.

Опция	Описание
Установить случайный PIN-код пользователя	Если опция включена, то в процессе выпуска устройства будет установлен случайный PIN-код пользователя. При необходимости установите **Параметры генерации PIN-кода пользователя**: - использовать только цифры; - запрещенные символы - исключение символов при генерации случайного PIN-кода; - длина (от 4 до 31 символа); - отображать установленный PIN-код администратору в Консоли управления; - отображать установленный PIN-код пользователю в Сервисе самообслуживания; 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 можно отправить пользователю или его руководителю в почтовом уведомлении.

Опция	Описание
	Если в разделах **Выпуск** и **Инициализация устройства** указаны разные значения длины PIN-кода пользователя, то в процессе выпуска устройства будет использовано большее значение.
Пользователь должен поменять PIN-код при первом входе	Если опция включена, то пользователь должен сменить 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 его разблокировать любым доступным способом (в режиме онлайн или офлайн) и установить новый PIN-код.

Опция	Описание
Генерировать имя устройства автоматически	Если опция включена, то в качестве имени устройства можно использовать 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** пользователь может изменить подставленное имя перед выпуском устройства.
Требовать указания комментария к устройству	Если опция включена, то при выпуске устройства в Консоли управления администратор или оператор системы должен задать **Комментарий к устройству**.
Требовать указания тегов к устройству	Если опция включена, то при выпуске устройства в Консоли управления администратор или оператор системы должен задать **Теги** для устройства.
Отображать установленный пароль пользователя КриптоПро DSS администратору	Если опция включена, то при создании пользователя КриптоПро DSS и выпуске ему сертификата пароль будет отображен администратору в личной карточке пользователя.
Отображать установленный пароль пользователя КриптоПро DSS пользователю	Если опция включена, то при создании пользователя КриптоПро DSS и выпуске ему сертификата пароль будет отображен пользователю в Сервисе самообслуживания.

⚠ **ПРЕДУПРЕЖДЕНИЕ**

Нельзя одновременно установить следующие опции:

- **Блокировать устройство** и **Устанавливать случайный PIN-код пользователя**;
- **Блокировать устройство** и **Пользователь должен поменять PIN-код при первом входе**.

Политики сложности PIN-кода

Политики сложности PIN-кода, заданные в Indeed CM, распространяются на устройство при выпуске с инициализацией и сохраняются на устройстве до следующей инициализации.

Для настройки параметров инициализации:

1. Нажмите **Добавить параметры инициализации**.
2. Выберите тип устройства и нажмите **Ок**.
3. Установите параметры инициализации. Вы можете задать следующие настройки:
   - PIN-код пользователя;
   - минимальная длина PIN-кода;
   - максимальное количество попыток ввода PIN-кода;
   - максимальное количество попыток ввода PIN-кода администратора;
   - возможность сменить PIN-код пользователя.

ⓘ **ПРИМЕЧАНИЕ**

Набор параметров инициализации зависит от типа устройства. Если в политике не настроены параметры инициализации для любого выпускаемого устройства, то при включении инициализации установятся параметры по умолчанию из раздела **Типы устройств**.

4. Нажмите **Добавить**.

Для редактирования параметров нажмите ✎. Для удаления нажмите ✖.

Разрешенные устройства

По умолчанию можно выпускать устройства всех типов, добавленных в Indeed CM. Чтобы задать политику выпуска устройств определенного типа, нажмите **Добавить тип устройства**, выберите имя типа устройства и нажмите **Добавить**.

Количество типов устройств, разрешенных для выпуска, неограниченно. Для удаления типа устройства из списка разрешенных нажмите ✖ .

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Если устройства были выпущены в рамках политики и отсутствуют в списке разрешенных, операции с устройствами остаются доступными.

Аутентификация

Пользователи аутентифицируются по секретным вопросам в следующих случаях:

- при самостоятельной разблокировке устройства;
- при выключении устройства без выполнения входа в ОС;
- при доступе в Сервис удаленного самообслуживания;
- 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.
- **Максимальное количество попыток аутентификации** по секретным вопросам до блокировки пользователя. Значение по умолчанию – 3.

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

> **ПРИМЕЧАНИЕ**
>
> Если список секретных вопросов не задан, то у пользователя не будет возможности указать ответы на секретные вопросы в Сервисе самообслуживания.

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

Созданные вопросы можно изменить или удалить. Для изменения вопроса нажмите напротив нужного вопроса. Для удаления вопроса нажмите .

> **ПРЕДУПРЕЖДЕНИЕ**
>
> Секретный вопрос можно удалить только в том случае, если его не использует ни один из пользователей системы.

Агенты

Клиентский агент Indeed CM позволяет контролировать использование устройств на рабочих станциях пользователей.

В разделе **Агенты** можно задать настройки использования устройств и сообщения пользователю после успешного выполнения задач.

Настройки контроля использования устройства

Опция	Описание
Сообщение при нарушении условий привязки устройства к агенту	Уведомление для пользователя при подключении устройства к неразрешенной администратором рабочей станции. Если значение не задано, то уведомление не отобразится.
Действие, выполняемое при нарушении условий привязки устройства к агенту	Действие, которое выполнит Агент Indeed CM, если пользователь подключит устройство 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 при подключении устройства к рабочей станции Агент Indeed CM проверит, принадлежит ли устройство пользователю, который выполняет подключение.
Сообщение при нарушении условий привязки устройства к пользователю	Уведомление для пользователя при подключении устройства к рабочей станции с сессией другого пользователя. Если значение не задано, то уведомление не отобразится.

Опция	Описание
Действие, выполняемое при нарушении условий привязки устройства к пользователю	Действие, которое выполнит Агент Indeed CM, если пользователь подключит устройство 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, после которого сессия пользователя будет заблокирована, если блокировка выбрана как действие, которое должен выполнять Агент Indeed CM при нарушении правил использования устройства. Возможный интервал – от 0 до 5 секунд.

Сообщения пользователю после успешного выполнения задач

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

- блокировка устройства;
- смена PIN-кода администратора на устройстве;
- очистка устройства.

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 устройства

Устройство {model}: {sn} было заблокировано администратором.

Смена PIN-кода администратора на устройстве

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

Очистка устройства

Администратор выполнил очистку 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 через считыватели принтера (контактный и бесконтактный) без печати;
- выпускать смарт-карты пользователям через считыватели принтера (контактный и бесконтактный) с печатью на карте изображения или текста;
- печатать на смарт-картах изображение или текст без выпуска карты пользователям.

Если включить опцию **Включить поддержку принтера смарт-карт**, то при выпуске устройства можно выбрать считыватель, к которому подключена карта – считыватель рабочей станции или считыватель принтера.

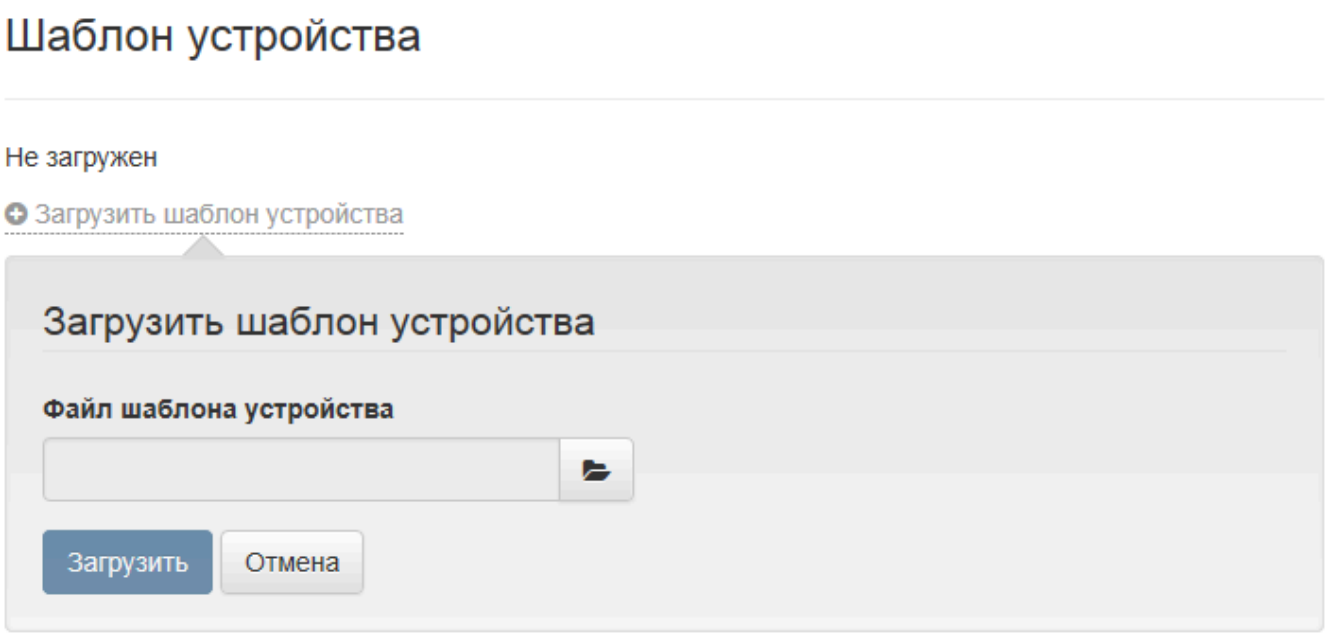
Если включить поддержку принтера смарт-карт, вам доступны следующие опции:

- **Читать RFID-метку устройства**. Если опция включена, то Indeed CM прочитает метку устройства и сохранит ее 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 на нем напечатается изображение/текст по загруженному шаблону печати.

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

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



ПОДСКАЗКА

Чтобы получить файл шаблона печати, обратитесь в службу технической поддержки компании Индид на support@indeed-id.com.

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

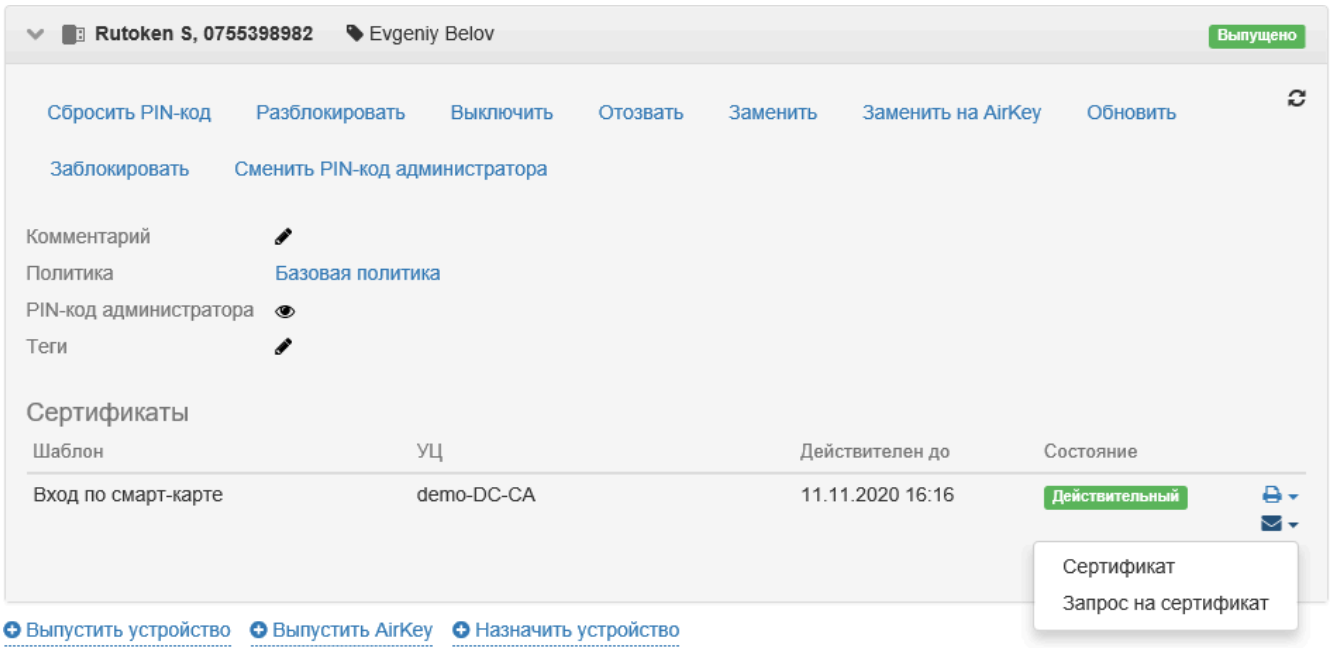
Настройка почтового сервера

Задайте настройки почтового сервера и отправьте тестовое сообщение для проверки его работы:

1. Укажите настройки почтового сервера, нажмите **Сохранить** и **Отправить тестовое сообщение**.
2. Укажите адрес электронной почты получателя и нажмите **Отправить**.

Если тестовое сообщение не удалось отправить, нажмите **Закрыть**, измените настройки почтового сервера и нажмите **Отправить**.

Если задать опцию **Включить уведомления пользователя**, то в Консоли управления при просмотре содержимого устройства пользователя администратор или оператор Indeed CM может отправить пользователю по электронной почте печатную форму сертификата, запроса на сертификат и запроса на отзыв сертификата в формате PDF.



Группы получателей

Настройте группы получателей уведомлений администраторов. Например, уведомления администратора могут получать специалисты по информационной безопасности вашей компании.

Чтобы установить группу получателей, нажмите **Создать группу**, укажите имя группы, введите адреса получателей и нажмите **Создать**.

Созданные группы получателей можно изменить или удалить. Для изменения группы выберите ее в списке и нажмите ✎. Для удаления группы нажмите ✖.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Группу получателей можно удалить только в том случае, если она не используется для рассылки уведомлений.

Уведомления администратора

Настройте почтовые уведомления для администраторов Indeed CM:

1. Нажмите **Создать уведомление**.
2. Выберите **Событие**, о котором необходимо оповестить администратора.

Список событий

- 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 КриптоПро DSS
- Выключение устройства
- Выключение устройства КриптоПро DSS
- Выпуск сертификата (Событие доступно для каждого добавленного шаблона сертификата в политику)
- Выпуск сертификата КриптоПро DSS (Событие доступно для каждого добавленного шаблона сертификата DSS в политику)
- Выпуск устройства
- Выпуск устройства КриптоПро DSS
- Выпуск устройства КриптоПро DSS ожидает решения
- Выпуск устройства ожидает решения
- Добавление AirCard 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 КриптоПро DSS
- Обновление устройства КриптоПро DSS ожидает решения
- Обновление устройства ожидает решения
- Общие сертификаты истекают
- Одобрение выпуска устройства
- Одобрение выпуска устройства КриптоПро DSS
- Одобрение замены устройства
- Одобрение обновления устройства
- Одобрение обновления устройства КриптоПро DSS
- Отзыв устройства
- Отзыв устройства КриптоПро DSS
- Отклонение выпуска устройства
- Отклонение выпуска устройства КриптоПро DSS
- Отклонение замены устройства
- Отклонение обновления устройства
- Отклонение обновления устройства КриптоПро DSS
- Отмена назначения устройства
- Отмена обновления устройства
- Отмена обновления устройства КриптоПро DSS
- Отслеживаемые сертификаты истекают
- Очистка устройства
- Политика была обновлена
- Политика пользователя была изменена
- Политика пользователя устройства КриптоПро DSS была изменена
- Политика устройства КриптоПро DSS была обновлена
- Разблокировка пользователя
- Разблокировка устройства
- Сброс PIN-кода
- Сброс ответов на секретные вопросы
- Сброс пароля пользователя
- Содержимое устройства истекает

- Содержимое устройства КриптоПро DSS истекает
- Создание кода подключения AirCard к компьютеру
- Удаление AirCard от компьютера
- Удаление устройства КриптоПро DSS
- Уничтожение/изъятие СКЗИ

3. Укажите **Тип события**: информация, ошибка или предупреждение.
4. Выберите **Группу получателей**. В качестве адресатов можно выбрать:
   - 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.
6. Нажмите **Создать**.

Созданные уведомления можно изменить или удалить. Для изменения уведомления выберите его в списке и нажмите ✎. Для удаления уведомления нажмите ✖.

Уведомления пользователя

> **ПРИМЕЧАНИЕ**
>
> Уведомления по электронной почте работают, если в свойствах учетной записи пользователя в Active Directory указан адрес электронной почты.

Настройте почтовые уведомления для пользователей Indeed CM:

1. Нажмите **Создать уведомление**.
2. Выберите **Событие**, о котором необходимо оповестить пользователя.

Список событий

- Атрибуты пользователя были изменены
- Аутентификация
- Блокировка пользователя
- Включение устройства
- Включение устройства КриптоПро DSS
- Выключение устройства
- Выключение устройства КриптоПро DSS
- Выпуск сертификата (Событие доступно для каждого добавленного шаблона сертификата в политику)
- Выпуск сертификата КриптоПро DSS (Событие доступно для каждого добавленного шаблона сертификата DSS в политику)
- Выпуск устройства
- Выпуск устройства КриптоПро DSS
- Выпуск устройства КриптоПро DSS ожидает решения
- Выпуск устройства ожидает решения
- Добавление AirCard 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 КриптоПро DSS
- Обновление устройства КриптоПро DSS ожидает решения
- Обновление устройства ожидает решения
- Одобрение выпуска устройства
- Одобрение выпуска устройства КриптоПро DSS
- Одобрение замены устройства

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

3. Укажите **Тип события**: информация, ошибка или предупреждение.

4. Укажите **Период отправки (дней)** - количество дней, через которое уведомление будет отправлено повторно.
5. При необходимости включите опцию **Отправлять копию менеджеру** (руководителю) в выбранном событии пользователя.
6. Нажмите **Создать**.

> **ПРИМЕЧАНИЕ**
>
> Опция **Отправлять копию менеджеру** доступна 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).

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

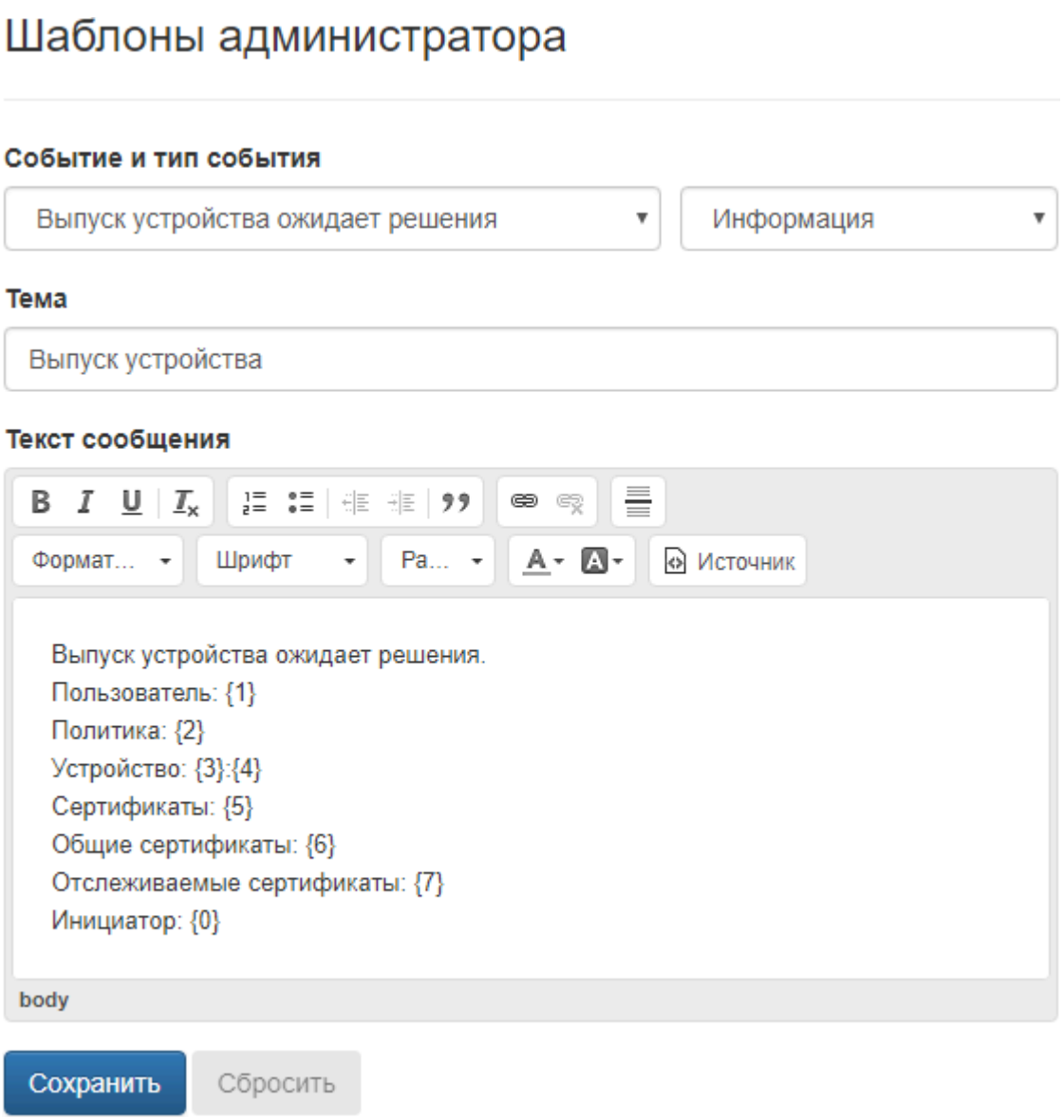
Шаблоны администратора

Настройте шаблоны почтовых уведомлений о событиях Indeed CM, которые будут рассылаться администраторам. В базовом варианте почтовое уведомление содержит следующую информацию:

- **Тема**. Формируется по названию события, например, «Выпуск устройства».
- **Текст сообщения**. Формируется по названию сообщения и его типу, может содержать информацию об инициаторе, пользователе, сертификатах и устройствах.

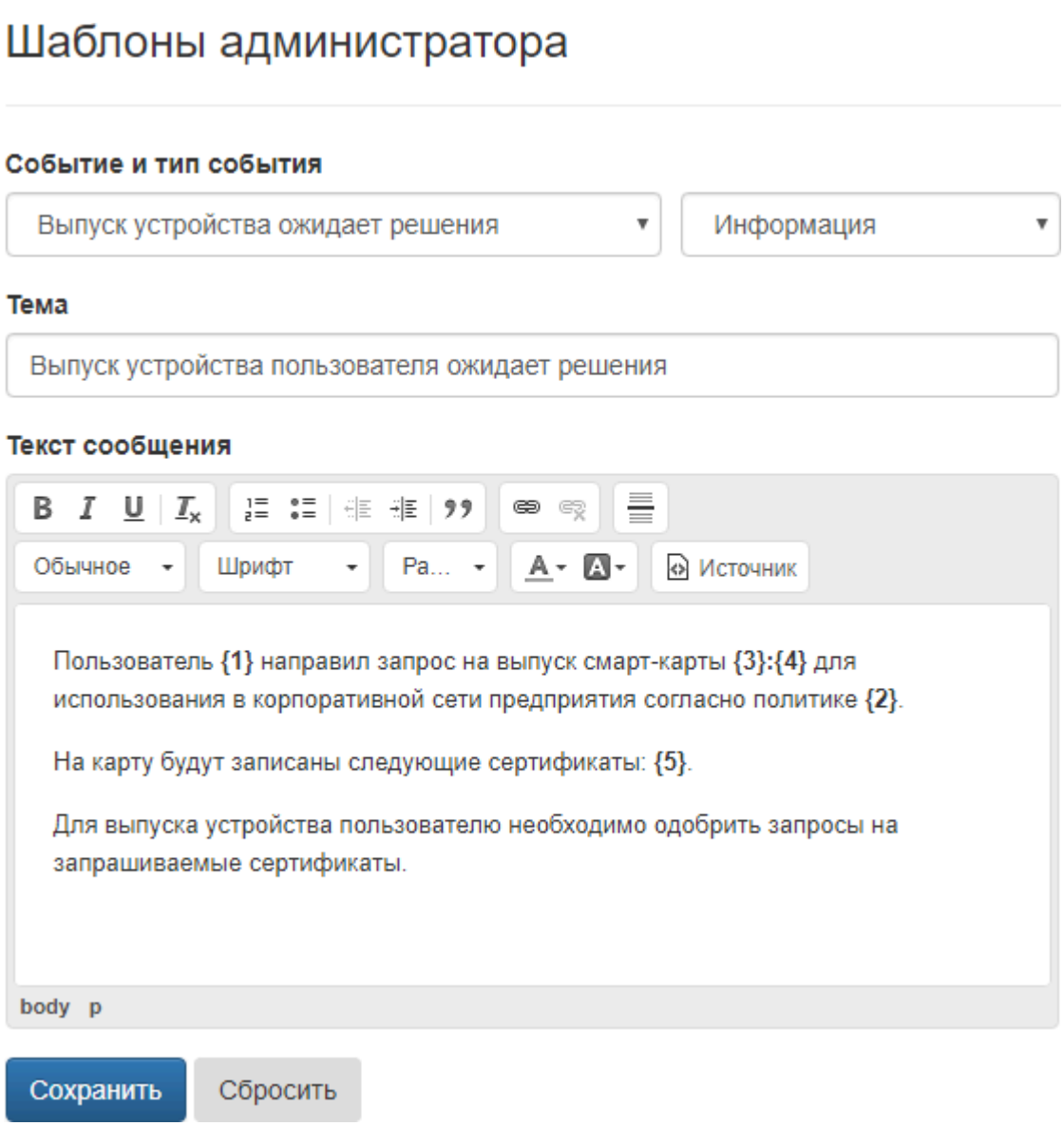
Для каждого уведомления в одной политике использования устройств настраивается только один шаблон.

На основе базового шаблона, Indeed CM сформирует и отправит электронное письмо следующего содержания:



Базовый шаблон можно изменить. Indeed CM позволяет использовать HTML-теги для форматирования текста сообщения.

Пример персонализированного шаблона уведомления

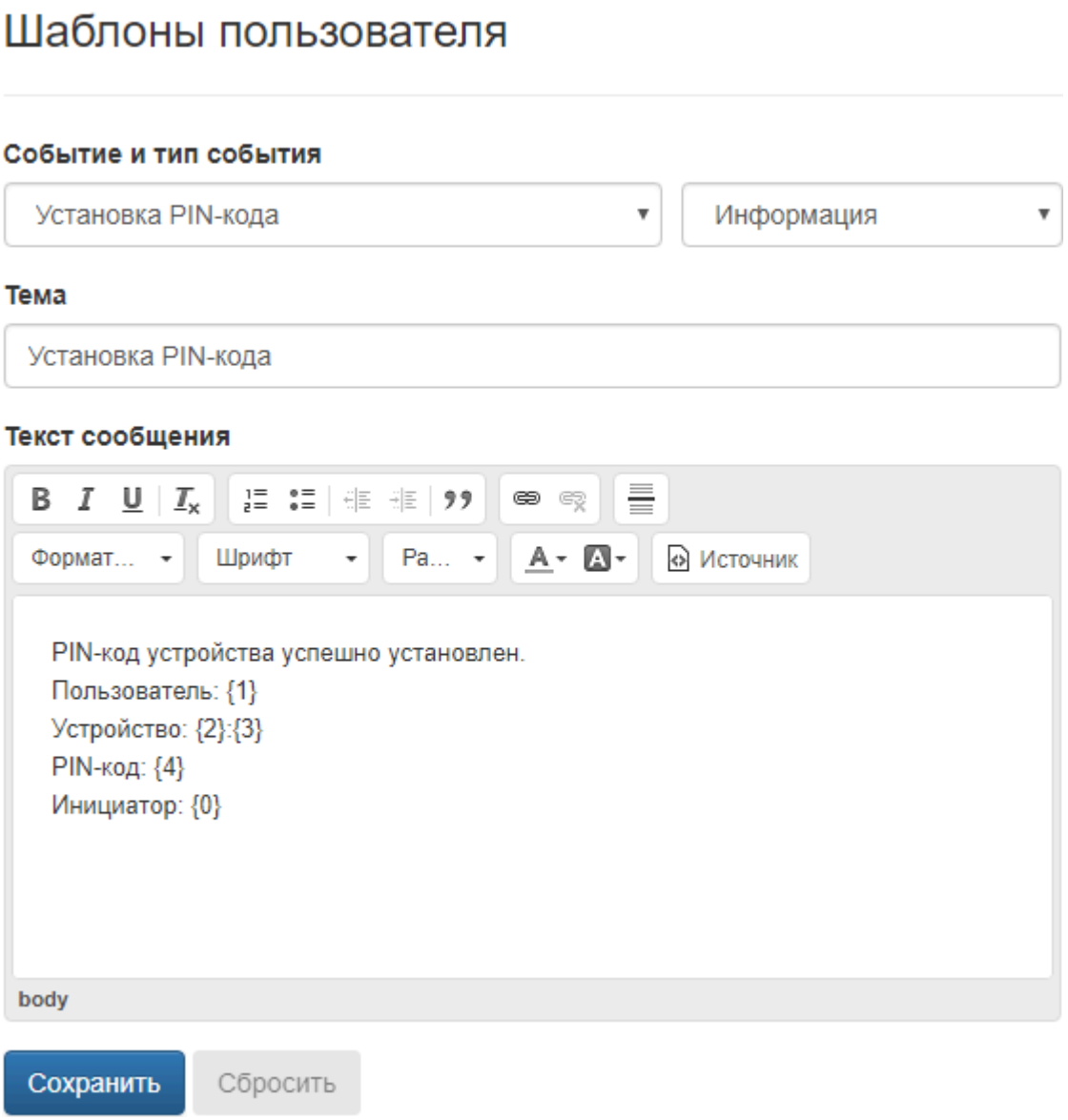


Шаблоны пользователя

Настройте шаблоны почтовых уведомлений о событиях Indeed CM, 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 по названию события, например, «Установка PIN-кода».
- **Текст сообщения**. Формируется по названию сообщения и его типа, может содержать информацию об инициаторе, пользователе и устройствах.



Базовый шаблон можно изменить в зависимости политики безопасности вашей компании.

ПОДСКАЗКА

Текст письма можно дополнить сообщением о конфиденциальности информации в письме или указаниями к действиям, которые должны предпринять получатели письма.

Назначения политик

Настройте назначения, чтобы централизованно применять политики к объектам или пользователям.

Политики распространяются на следующие объекты:

- **Active Directory**: Домен (Domain), Контейнер (Container), Подразделение (Organizational Unit);
- **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.

> **ПРИМЕЧАНИЕ**
>
> Действие политики может распространяться как на весь объект (домен, контейнер или подразделение), так и на отдельные группы пользователей в составе объекта.
>
> 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**, выберите политику из списка и задайте следующие параметры:

- **Контейнер** – область действия политики. Контейнером может быть подразделение Active Directory, папка Центра Регистрации КриптоПро УЦ 2.0 или узел организационной структуры Indeed CM.
- **Группы** – дополнительный фильтр для распространения политики. Например, на один контейнер с пользователями организации можно назначить 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 на пользователя будет действовать политика с большим приоритетом.
- **Роли** – если в разделе **Роли** есть хотя бы одна локальная роль, то ее можно добавить в создаваемое назначение политики и задать пользователей роли.

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

Лицензии

Подробнее о лицензировании Indeed Certificate Manager можно узнать в разделе Лицензирование.

Для получения лицензий вам необходим идентификатор системы:

1. Откройте Консоль управления и перейдите в раздел **Конфигурация → Лицензии**.
2. Скопируйте значение из поля **Идентификатор системы** и отправьте вашему менеджеру в компании Индид или в службу технической поддержки компании Индид.

Вам отправят файл лицензии.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Идентификатор системы — это уникальный код, который зависит от расположения каталогов пользователей Indeed CM. Если вы переместили каталог, существующие лицензии станут недействительными. Для обновления лицензий обратитесь в службу технической поддержки компании Индид.

Чтобы загрузить новую лицензию, нажмите **Добавить лицензию**, укажите файл лицензии и нажмите **Добавить**.

Чтобы удалить лицензию из системы, выберите ее в списке и нажмите ✖ **→ Удалить**.

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, внесите изменения в Indeed CM.

Добавление

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

> **ПОДСКАЗКА**
>
> Файлы для устройств различных типов находятся в каталоге *\Misc\CardTypes* дистрибутива Indeed CM Server.

Список файлов для типов устройств

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	AirCard	AirCard.xml

Производитель	Модель устройства	Файл типа устройства
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.xm
Cryptovision	ePasslet Suite v3.0, JCOP V3.0	cv-ePassletSuite3.0-JCOP3.0.xml
Feitian	ePass2003 (A1+, A2)	ePass2003.xml
	BioPass2003	

Производитель	Модель устройства	Файл типа устройства
HID	Crescendo C1150 Series	CrescendoC1150.xml
	Crescendo C1300 Series	CrescendoC1300.xml
	Crescendo C2300 Series	CrescendoC2300.xml
ISBC	ESMART Token USB 64K и ESMART Token CARD 64K	EsmartToken64K.xml
	ESMART Token USB 192K и ESMART Token CARD 192K	EsmartToken192K.xml
	ESMART Token ГОСТ	EsmartTokenGOST.xml
	ESMART Token CARD 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

Производитель	Модель устройства	Файл типа устройства
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 устройства в Indeed CM отобразится его имя.

Редактирование

Файл типа устройства по умолчанию содержит предустановленные значения PIN-кода администратора и пользователя (в том числе и для ГОСТ-области). Эти значения можно изменить 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 .

ПОДСКАЗКА

Наличие ГОСТ-области зависит от производителя и модели устройства.

При редактировании устройства доступны следующие опции:

Инициализировать устройство при добавлении

Если опция включена, то:

- 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.

ПРИМЕЧАНИЕ

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 PIN-код, известный только Indeed CM.
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 PIN-код для ГОСТ-области, известный только Indeed CM.
Если опция включена, то при добавлении устройства будет установлен указанный PIN-код для ГОСТ-области.

Удаление

Для удаления типа устройства, выберите его в списке, нажмите ✖ и **Удалить**.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Удалить тип устройства можно только в том случае, если в Indeed CM нет ни одного устройства этого типа.

Организационная структура

ПОДСКАЗКА

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.

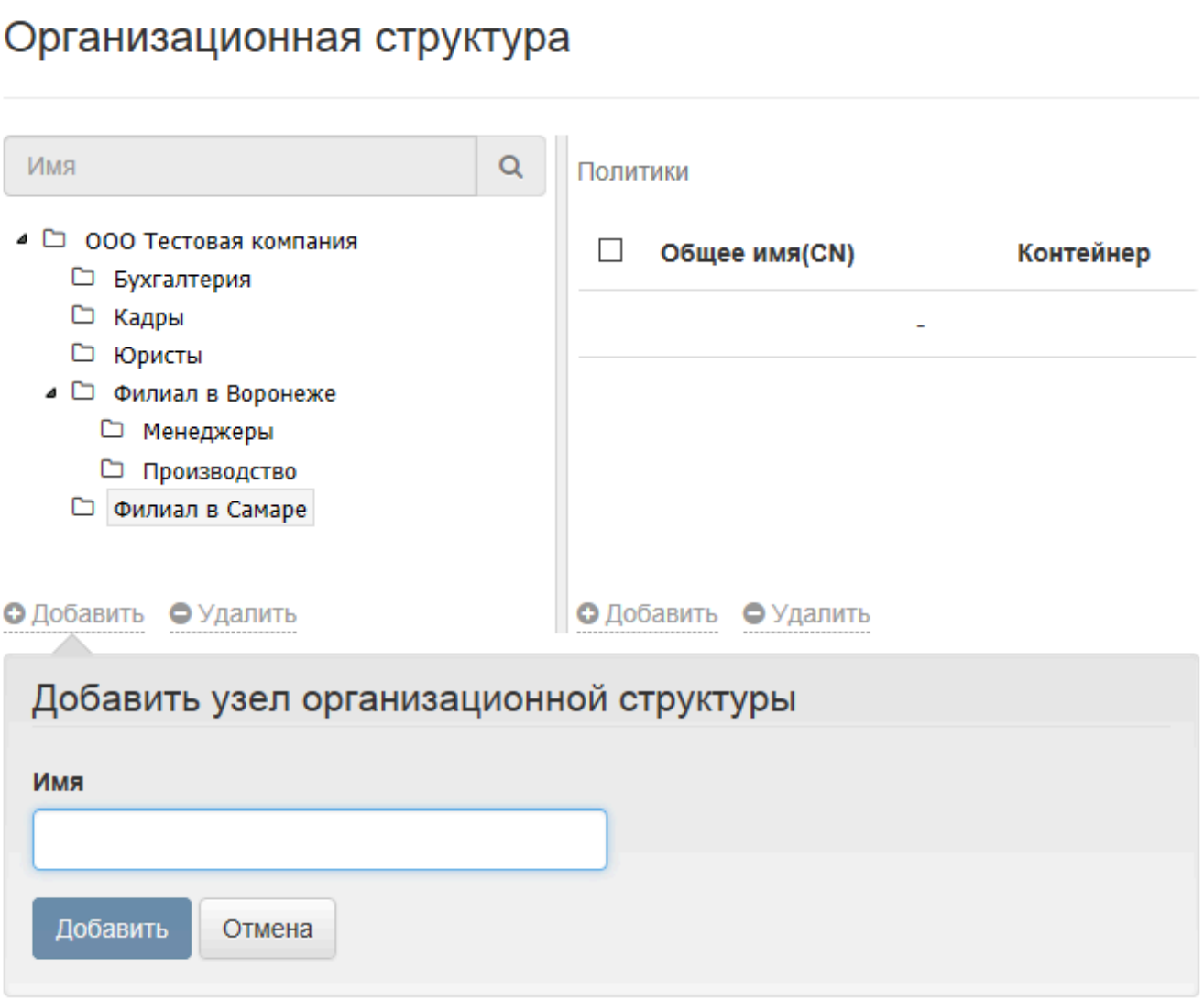
Устройства в Indeed Certificate Manager выпускаются пользователям по заданным правилам. Правила использования устройств задаются в политиках использования устройств, которые распространяются на указанную область. Область распространения политики – объект каталога пользователей. Например, подразделение 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.

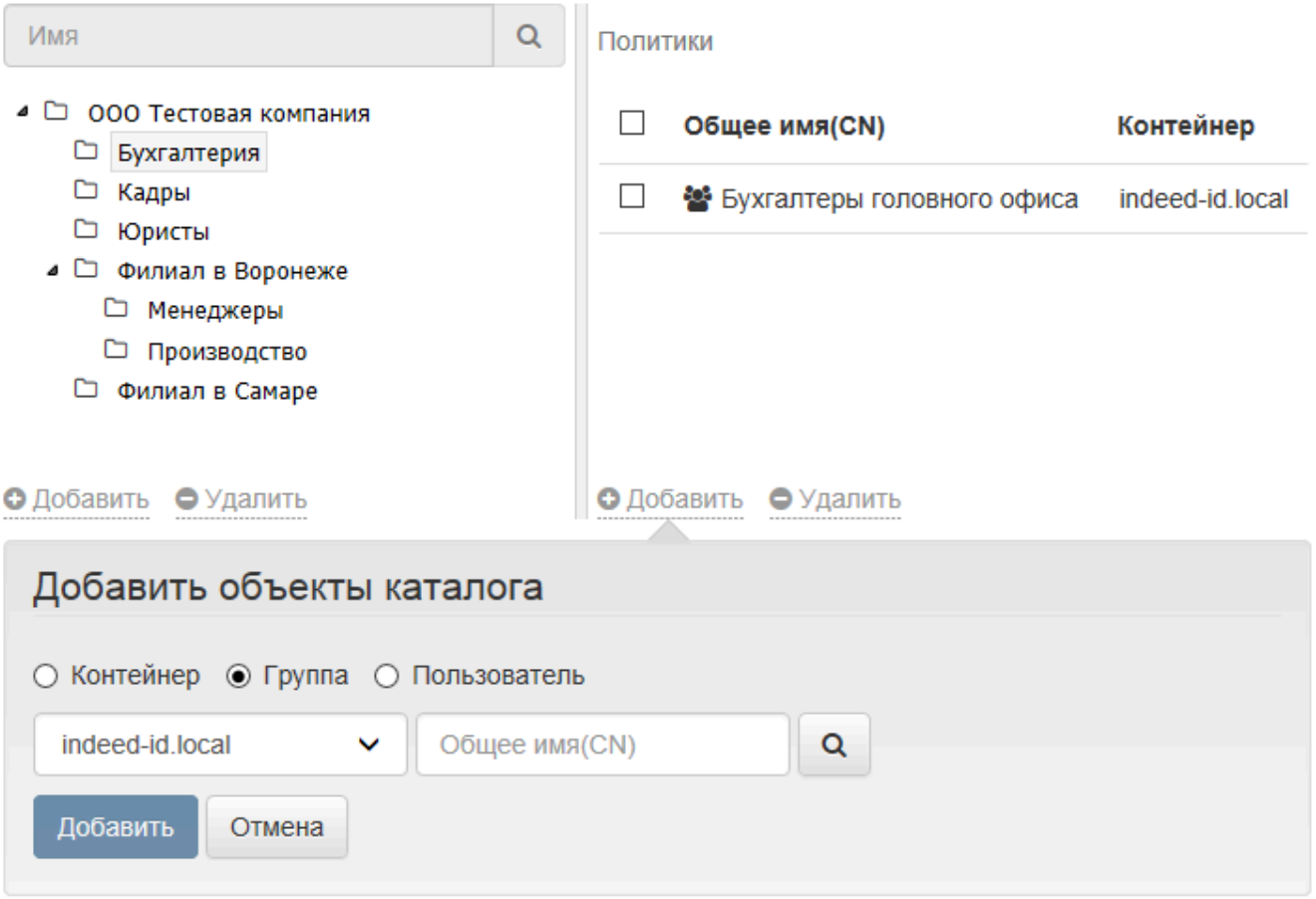
Для удаления созданного узла выберите его и нажмите **Удалить**.

Для переименования узла нажмите по нему два раза левой кнопкой мыши или нажмите F2.

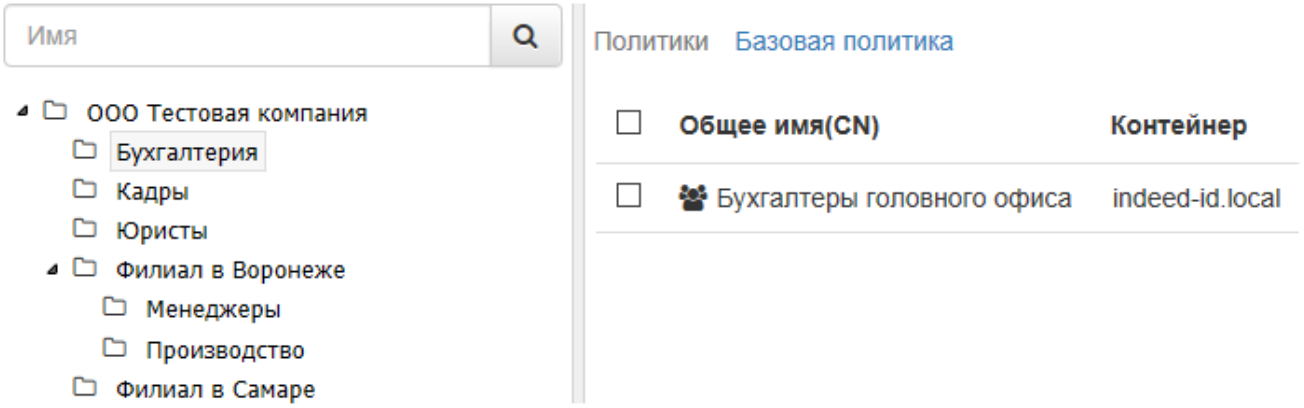


Для добавления объектов в узел нажмите **Добавить** в правой части окна редактирования организационной структуры. При создании структуры используются объекты каталога пользователей: контейнеры, подразделения и группы Active Directory, папки Центра Регистрации КриптоПро УЦ.

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**.



Назначенная на узел политика отображается в правой части окна:



Роли

В разделе **Роли** настраиваются полномочия администраторов и операторов, доступные в Консоли управления Indeed Certificate Manager.

> **ПОДСКАЗКА**
>
> Для первоначальной настройки привилегий используйте учетную запись, указанную при настройке параметров системы в разделе **Администратор ролей** Мастера настройки Indeed CM.

Есть два вида роли:

- **глобальная** – распространяется на все политики использования устройств;
- **локальная** – распространяется только на указанные политики.

В Indeed CM по умолчанию установлены роли **Администраторов** и **Операторов**.

Чтобы добавить локальную роль в политики, откройте раздел **Конфигурация** Консоли управления Indeed CM и перейдите в раздел **Назначения политик** .

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. Пользователи включаются в состав роли персонально или через членство в группах Active Directory. Для изменения роли нажмите ✎.

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

Чтобы добавить пользователей в глобальную роль и настроить привилегии, выполните следующие действия:

1. Нажмите **Добавить** в окне создания или редактирования роли.
2. Выберите **Группу безопасности** Active Directory.
3. Укажите **Общее имя** (CN) или **Логин** (sAMAccountName) пользователя.
4. Нажмите **Добавить**.
5. Задайте **Привилегии** для членов роли.
6. Нажмите **Сохранить**.

ПРИМЕЧАНИЕ

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

Роль для работы службы Card Monitor

Для работы службы Card Monitor создайте отдельную сервисную роль, включите в нее учетную запись, от имени которой будет работать Card Monitor, и определите для роли следующие привилегии:

- выключение устройства;
- обновление устройства;
- отмена обновления устройства;
- отзыв и очистка устройства;
- отмена назначения устройства;
- удаление устройства;
- удаление агента;
- удаление задачи;
- удаление записи из журнала учета.

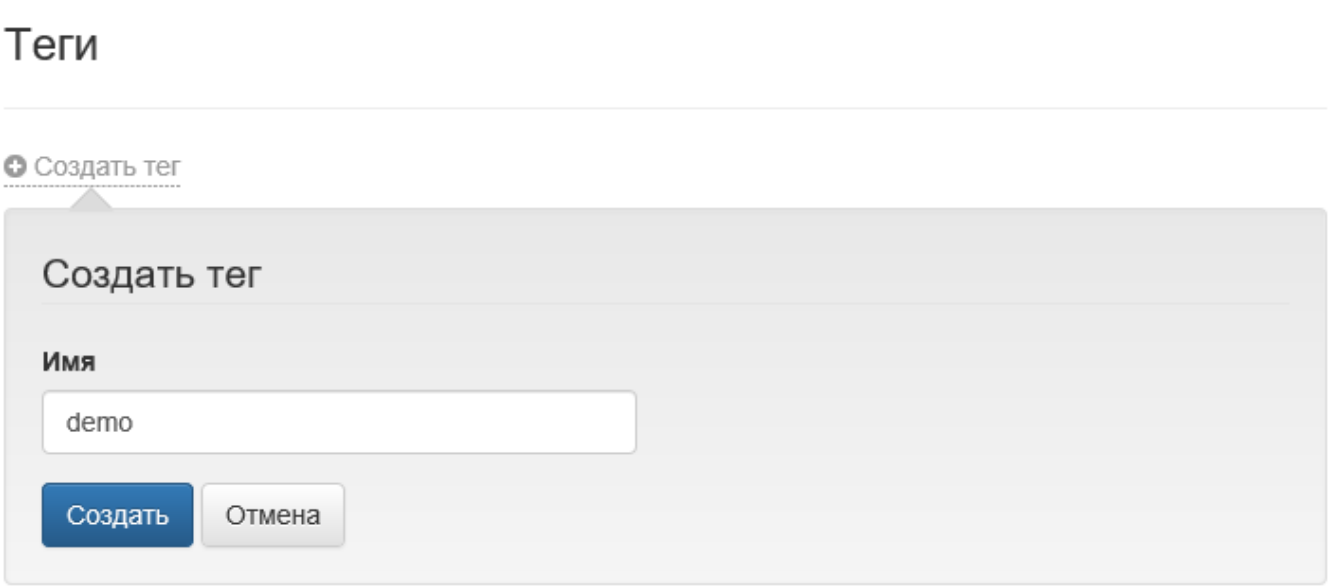
Если настроена интеграция с КриптоПро DSS и AirCard Enterprise, то задайте привилегии для работы с данными устройствами:

- выключение устройства КриптоПро DSS;
- обновление устройства КриптоПро DSS;
- отмена обновления устройства КриптоПро DSS;
- отзыв устройства КриптоПро DSS;
- удаление устройства КриптоПро DSS;
- удаление AirCard.

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**.



Созданные теги можно назначить на устройство:

- при пакетном добавлении устройств;
- при выпуске устройства;
- при просмотре содержимого устройства;
- при измененииии тегов на вкладке **Устройства**;
- в карточке пользователя.

Теги помогают при поиске устройств в Консоли управления на вкладке **Устройства → Расширенный поиск**.

Шаблоны печати

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

Добавление

Для создания шаблона нажмите **Добавить шаблон 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**.

> **ПРИМЕЧАНИЕ**
>
> Для типов объектов СКЗИ поддерживаются шаблоны в формате RTF.
>
> 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**.

Для редактирования добавленного шаблона нажмите , для удаления нажмите .

Настройка шаблона печати СКЗИ

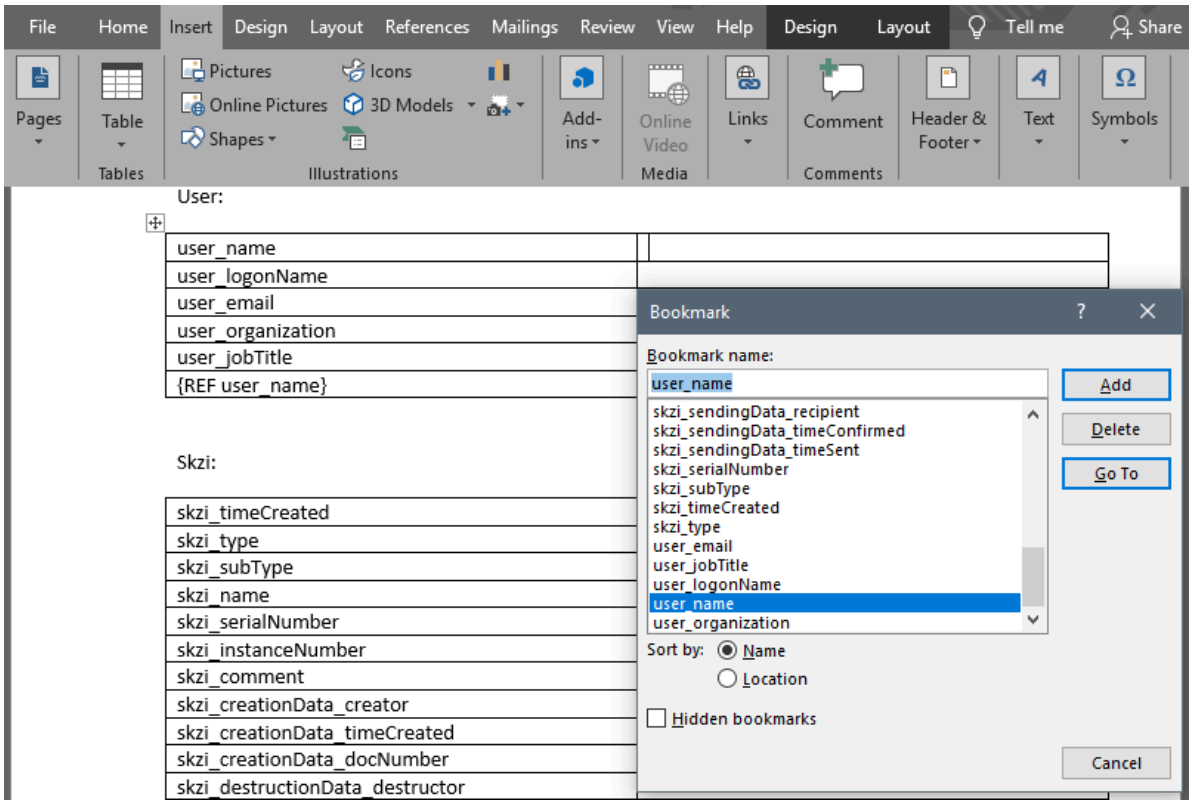
Вы можете настроить шаблон печати СКЗИ с помощью функции **Закладок** (Bookmark) в Microsoft Word. Поддерживаются шаблоны в формате RTF.

Для настройки шаблона печати воспользуйтесь демонстрационным шаблоном. В левом столбце указаны имена атрибутов, в правом подставлены **Закладки** (Bookmarks) для данных атрибутов.

Шаблон печати СКЗИ

Пример настройки шаблона печати СКЗИ

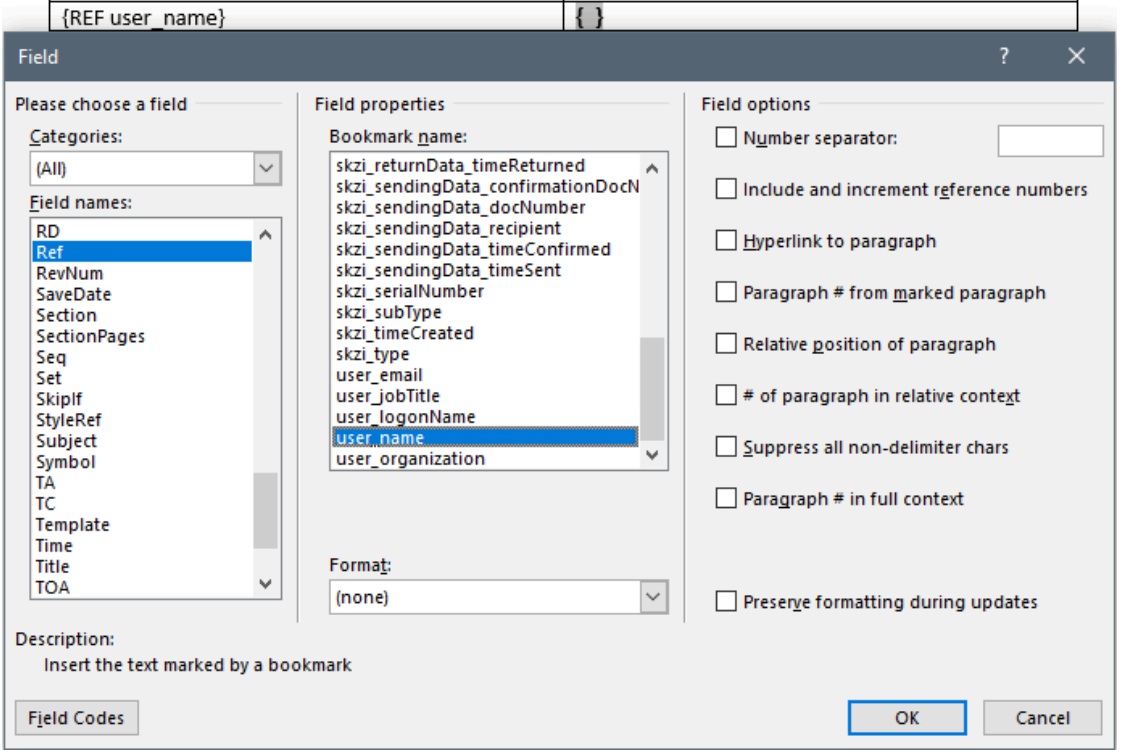
1. Откройте в Microsoft Word шаблон печати, в который необходимо добавить поля для автоматического заполнения из журнала СКЗИ.
2. Переведите курсор в заполняемое поле и нажмите **Вставка → Закладка** (Insert → Bookmark).
3. Выберите необходимый атрибут для подстановки (например, user_name).



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 примените ссылку на закладку (Bookmark):

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

user_name	
user_logonName	
user_email	
user_organization	
user_jobTitle	
{REF user_name}	{ }



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

Перед печатью заполненного документа обновите все поля (**Ctrl+A** + **F9**), чтобы подставить значения из ссылок на **Закладки** {Ref Bookmark name:}.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Печать сводных данных по нескольким СКЗИ или пользователям не предусмотрена.

Создание дополнительных полей

Вы можете создать дополнительные поля в документе, если в журнале учета СКЗИ вашей организации есть информация, которой нет в списке атрибутов Indeed CM.

Дополнительные поля задаются в **Мастере настройки Indeed CM** в разделе **Журнал учета СКЗИ**. Созданные поля 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 указать в поле **Имя закладки**: (Bookmark name:). Допустимы латинские имена.
   - **Атрибут** – отображаемое имя поля в журнале СКЗИ.

4. Для сохранения нажмите **Добавить**.

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

> **ПРИМЕЧАНИЕ**
>
> При добавлении дополнительных полей в документ необходимо указать **Имя закладки** формата `skzi_id`. Например, **Имя закладки** для поля customField1: `skzi_customField1`.

СКЗИ

В разделе **СКЗИ** задаются настройки средств криптографической защиты информации.

Нормативные документы

Вы можете определить шаблоны нумерации нормативных документов и выбрать шаблон печати для каждого типа СКЗИ в каждом его состоянии. Таким образом вы регулируете, по какому шаблону пользователь и оператор могут просмотреть и распечатать нормативные документы СКЗИ.

> **ПРИМЕЧАНИЕ**
>
> Пользователь может просмотреть и распечатать назначенные ему СКЗИ в Сервисе самообслуживания.
>
> Оператор может управлять СКЗИ в Консоли управления в разделе **СКЗИ** или в карточке пользователя.

Чтобы редактировать шаблон нормативного документа СКЗИ:

1. Перейдите в Консоль управления и откройте вкладку **Конфигурация** > **СКЗИ** > **Нормативные документы**.
2. Нажмите ✎ напротив выбранного акта и укажите:

- **Шаблон печати**
  Выберите один из шаблонов документов СКЗИ, загруженных в разделе **Шаблоны печати**.
- **Шаблон номера**
  Задайте полный формат номера документа согласно внутреннему документообороту компании. Этот номер будет отображаться в сформированном нормативном документе. Например, номер акта изготовления ключевого документа – *КД СЗ № $docNumber*, где $docNumber – текущий номер по порядку.
- **Текущий номер**
  Укажите внутренний порядковый номер документа. В Indeed CM ведется своя нумерация для каждого типа СКЗИ в каждом состоянии.

Если вы определили шаблон для одного типа СКЗИ в одном из его состояний, то при печати нормативный документ для этого типа СКЗИ в текущем состоянии сгенерируется именно по этому шаблону.

Если вы не определили такой шаблон, то при печати нормативного документа пользователь и оператор смогут выбрать любой из шаблонов, загруженных для этого типа СКЗИ в разделе **Шаблоны печати**.

Журналы учета

В разделе **Журналы учета** настраиваются справочники и шаблоны журналов.

Справочники

Справочник – это перечень значений, которые можно указать 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**.

Для редактирования созданного справочника и его значений нажмите ✎. Для удаления нажмите ✖.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Удалить используемый **Справочник** или используемое **Значение** невозможно.

Шаблоны журналов

Журнал учета – это набор полей с данными 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**.
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.

    1. Укажите **Имя** создаваемого поля.
    2. Выберите **Способ заполнения**:
        - **Вручную**;

- **Автоматически** (выберите **Выражение** из выпадающего списка подходящие для выбранного типа журнала);
- **Справочник** (выберите созданный справочник из выпадающего меню).

3. Выберите **Тип значения:**
   - **Текст**;
   - **Дата**.
4. 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** в Консоли управления).
5. Нажмите **Добавить**.

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

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> - 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 одно устройстве можно записать несколько сертификатов или на разные устройства можно записан **Общий сертификат**.
> - При редактировании уже добавленного поля вы можете изменить только его **Имя** и набор параметров: **Уникальное**, **Обязательное**, **Поиск**.

> ⓘ **ПРИМЕЧАНИЕ**
>
> 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**.

Для редактирования шаблона журнала выберите ,для удаления шаблона нажмите .

При редактировании созданного шаблона доступно следующее:

- изменить **Имя** шаблона;

- изменить **Политики**;
- добавить, удалить поля или отредактировать уже добавленные поля.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> При удалении поля в шаблоне оно удалится во всех записях в **Журнале учета**.

Консоль управления

Сводная информация

Просмотр сводной информации об Indeed CM

Карточка пользователя

Доступные действия в карточке пользователя

Устройства

Управление устройствами пользователей

Агенты

Работа с Indeed CM Agent

СКЗИ

Ведение журнала учета СКЗИ

Журналы учета

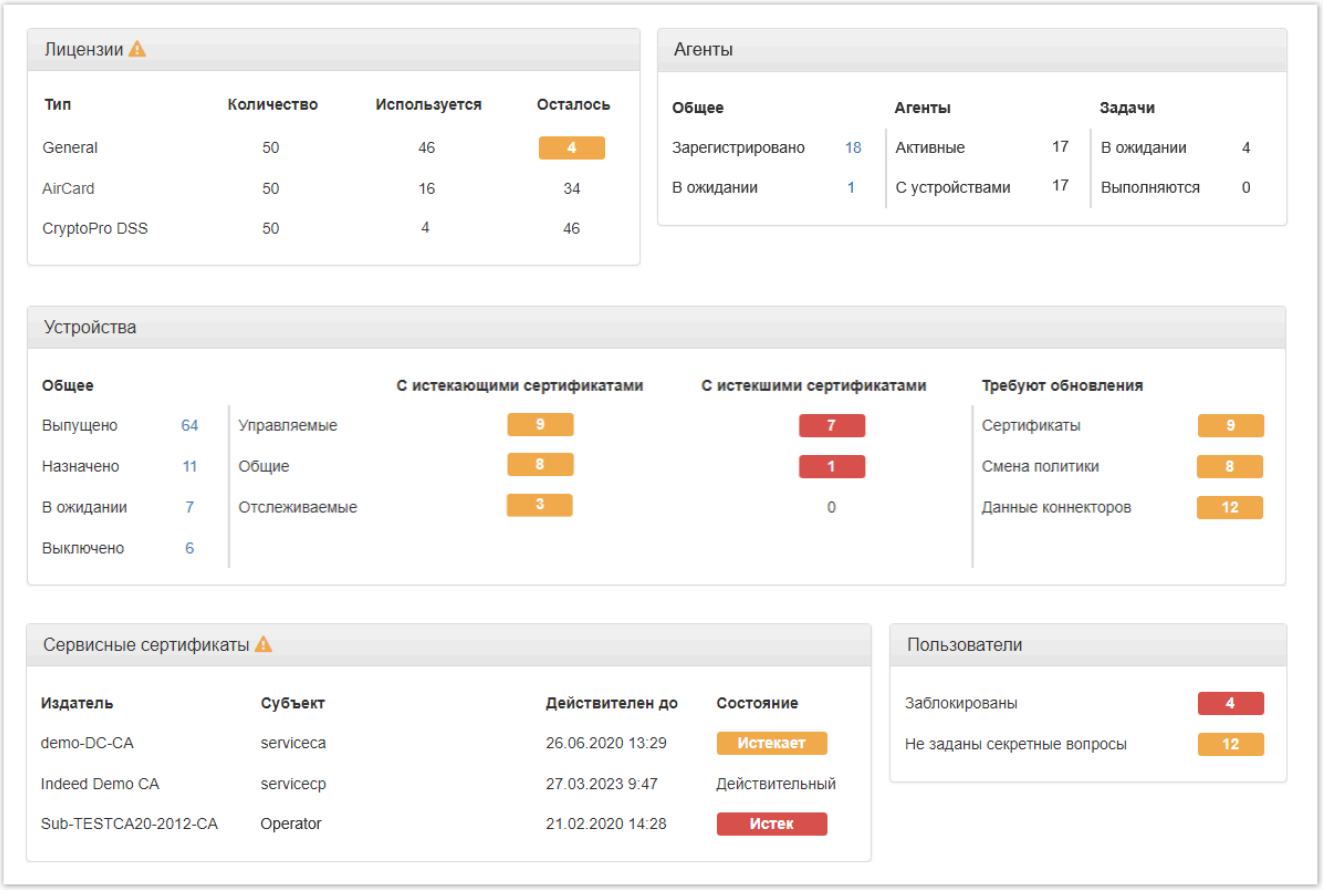
Просмотр журналов учета устройств и сертификатов

Журнал событий

Запись событий Indeed CM

Сводная информация

В разделе отображается сводная информация об Indeed CM:



Лицензии

- тип лицензий;
- общее количество;
- количество используемых лицензий;
- количество оставшихся лицензий.

ПОДСКАЗКА

Иконка предупреждения появляется, если:

- лицензии не добавлены в Indeed CM;
- осталось 10% от общего количества лицензий;
- все лицензии использованы.

Агенты

> **ПРИМЕЧАНИЕ**
>
> Поле **Агенты** отображается, если выполнена **настройка Indeed CM Agent**.

Количество агентов по их статусу:

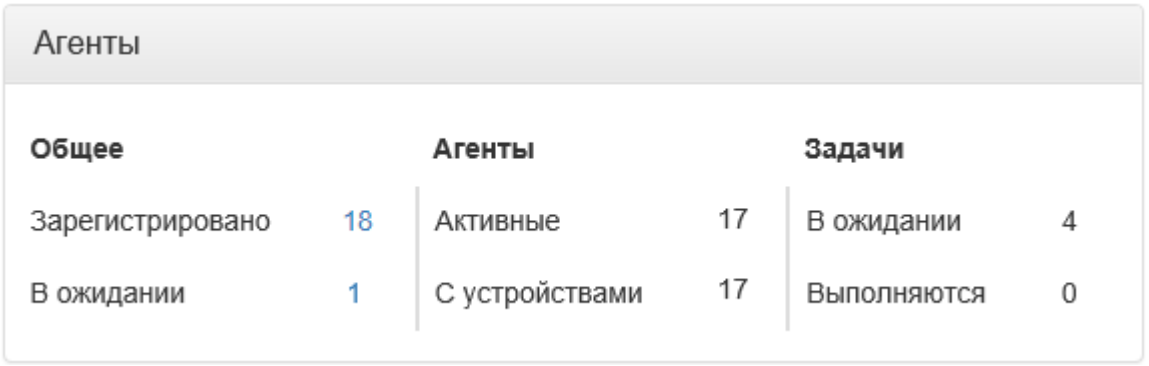
- зарегистрирован;
- ожидает регистрации.

По доступности связи с сервером Indeed CM:

- **активные** – агенты, которые обращались к серверу 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.



Устройства

Устройства по состояниям:

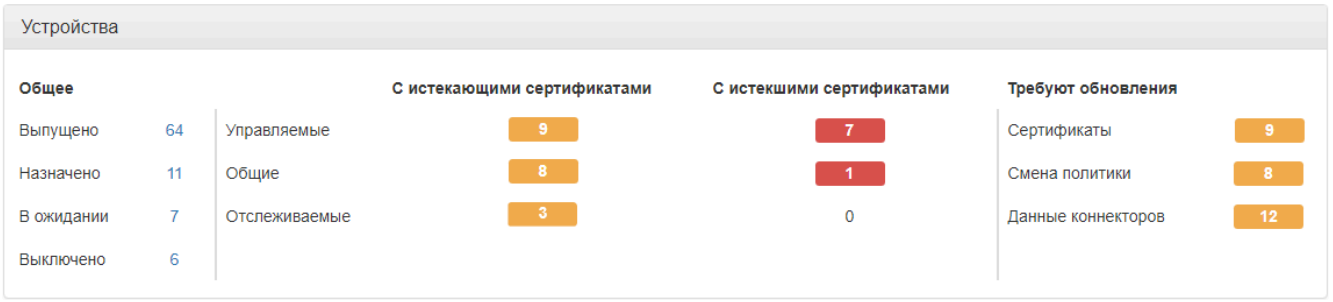
- выпущено;
- назначено;
- в ожидании;
- выключено.

Количество устройств по статусу содержимого (с истекающими и истекшими сертификатами):

- **управляемые** – сертификаты, выпущенные через Indeed CM.
- **общие** - сертификаты, добавленные в политику использования устройств в формате PFX и записанные на устройство.
- **отслеживаемые** – сертификаты, выпущенные и записанные на устройство вне Indeed CM.

Устройства, требующие обновления:

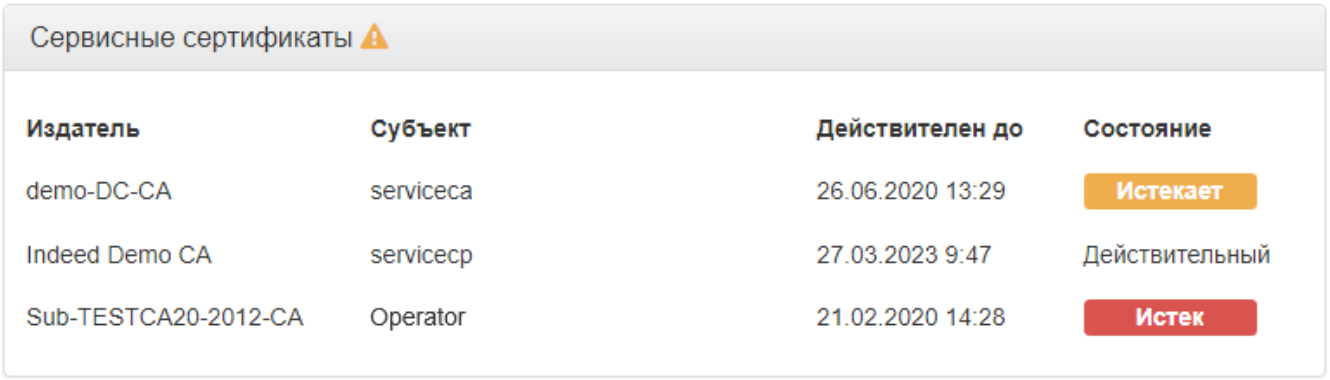
- **сертификаты** – в политике использования устройств изменился набор обязательных шаблонов сертификатов.
- **смена политики** – на пользователя, для которого было выпущено устройство, была назначена новая политика использования устройств.
- **данные коннекторов** – после выпуска устройства в действующей политике была включена/выключена интеграция с Indeed Access Manager и/или интеграция с Secret Net Studio.



Сервисные сертификаты

Сертификаты, выданные для сервисных учетных записей при настройке интеграции с удостоверяющими центрами: Microsoft CA, КриптоПро УЦ 2.0.

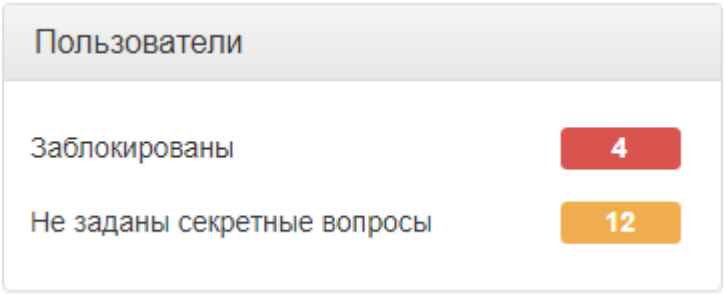
> **ПОДСКАЗКА**
>
> Иконка предупреждения отображается в случаях, если хотя бы один из сервисных сертификатов истекает (10% от срока действия) или истек.



Пользователи

Отображение количества пользователей по состоянию в базе данных системы с возможностью перехода в раздел расширенного поиска пользователей:

- **Заблокированы в системе** – пользователи, которые исчерпали попытки ответов на секретные вопросы при выполнении онлайн-разблокировки устройства, задачи на сброс PIN-кода пользователя на агенте или выполнении входа в Сервис удаленного самообслуживания.
- **Не заданы секретные вопросы** – пользователи, у которых не заданы ответы на секретные вопросы.



Карточка пользователя

Поиск

Простой и расширенный поиск пользователей Indeed CM

Загрузка фотографии

Параметры загрузки фотографии

Связь каталогов пользователей

Связь пользователя AD с пользователями КриптоПро УЦ 2.0 и КриптоПро DSS

Разблокировка пользователя

Как разблокировать учетную запись пользователя

Сброс ответов на секретные вопросы

Как сбросить ответы на секретные вопросы

Сброс пароля пользователя

Как сбросить доменный пароль

Выпуск устройства

Как записать сертификаты на устройство

Назначение устройства

Как закрепить устройство за пользователем

Сброс PIN-кода устройства

Как сбросить PIN-код устройства

Разблокировка устройства

Как разблокировать устройство в режиме онлайн или офлайн

Выключение и включение устройства

Как выключить и включить устройство

Отзыв устройства

Как отозвать устройство при его повреждении, утере, изъятии, обновлении

Изъятие устройства

Как изъять устройство у пользователя

Замена устройства

Временная или постоянная замена устройств пользователей

Обновление устройства

Как обновить содержимое устройства

Выпуск устройства с печатью

Как выпустить устройство с печатью

Массовый выпуск смарт-карт

Режим массового выпуска

Назначенные СКЗИ

Как настроить управление СКЗИ в карточке пользователя

Документы

Электронный документооборот

События пользователя

Информация о событиях Indeed CM

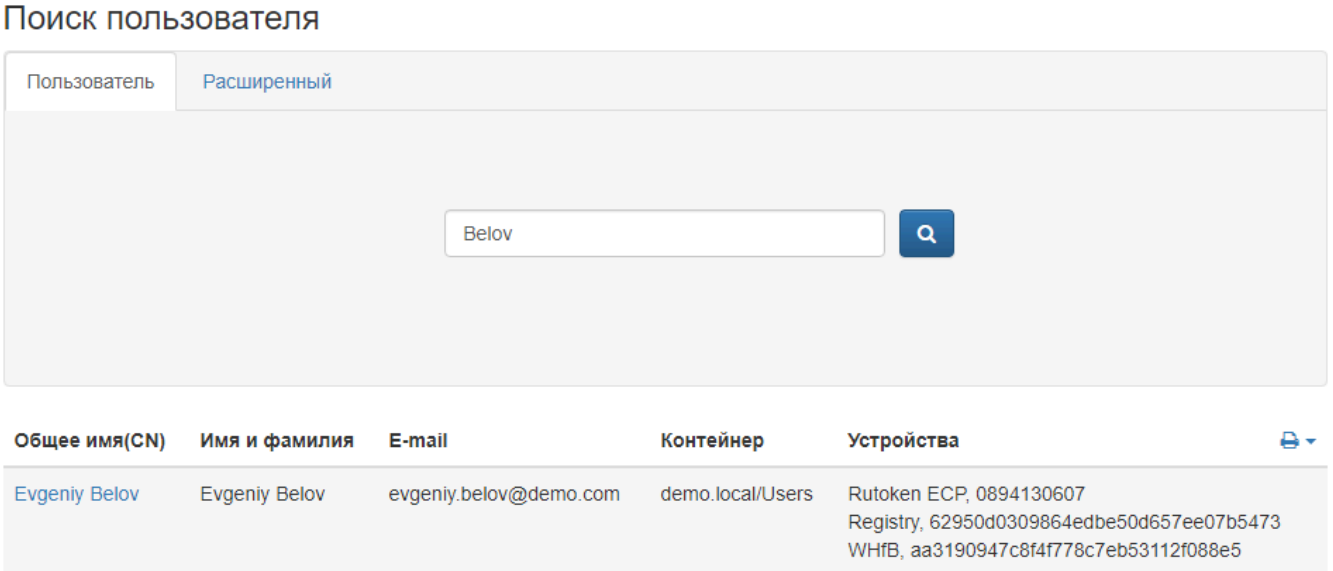
Поиск

Раздел **Пользователи** открывается автоматически при переходе на страницу Консоли управления. 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:

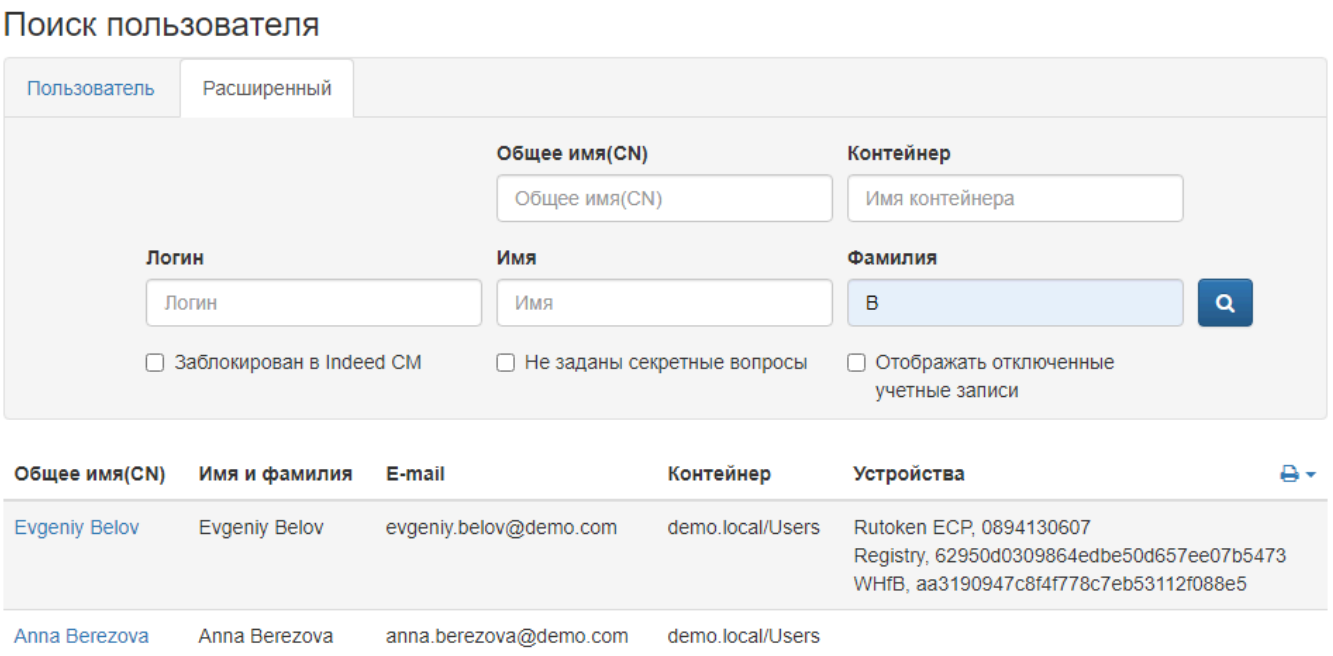
- Общее имя(CN)
- Имя и фамилия
- E-mail
- Контейнер
- Устройства



Чтобы перейти к карточке пользователя, нажмите на **Общее имя** (CN) пользователя в результатах поиска.

Расширенный поиск пользователей

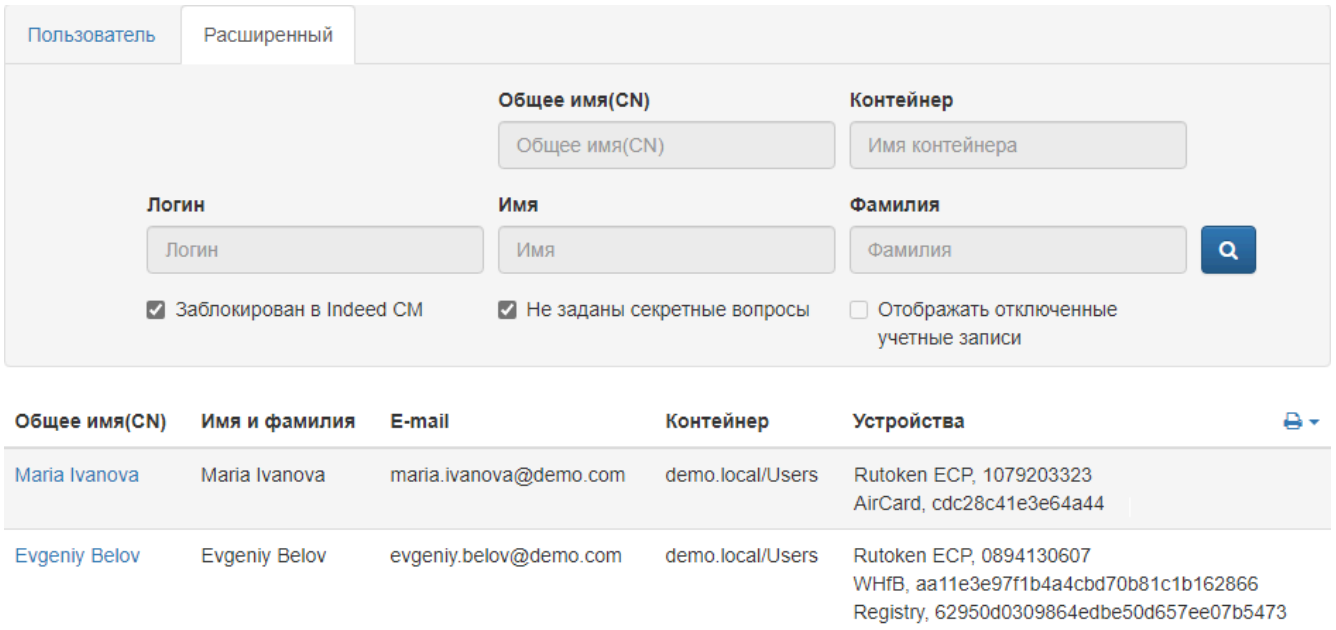
Расширенный поиск может выполняться по нескольким параметрам: логину (sAMAccountName), общему имени (Common name), имени, фамилии и контейнеру. Поиск может осуществляться как по одному параметру (например, фамилии) так и по нескольким (например, все пользователи с фамилией, начинающейся на *B*, находящиеся в указанном контейнере или подразделении).



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 системе** 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.



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.

Загрузка фотографии

Если профиль пользователя в Active Directory содержит фотографию, то она будет отображена в карточке пользователя. Для загрузки фотографии вручную нажмите **Загрузить фотографию**.

Параметры загрузки фотографии

- Фотография пользователя может быть записана в атрибуты `thumbnailPhoto` или `jpegPhoto`. Чтобы выбрать атрибут, откройте Мастер настройки Indeed CM и перейдите в раздел **Каталог пользователей → Active Directory → Расширенные настройки**.
- 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 100 КБ.

Связь каталогов пользователей

Если в используемой вами конфигурации каталог пользователей Indeed CM не совпадает с каталогом пользователей удостоверяющего центра (например, пользователям Active Directory необходимо выпускать сертификаты КриптоПро УЦ 2.0), то для выпуска устройства необходимо установить связь с каталогом нужного удостоверяющего центра.

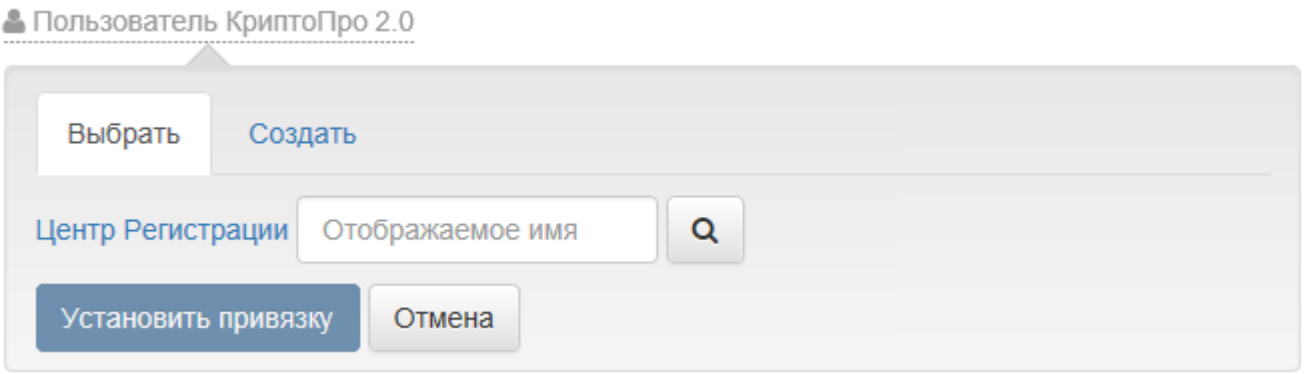
Необходимость привязки пользователя к каталогу удостоверяющего центра определяется опцией **Устанавливать привязку между пользователем УЦ и пользователем каталога** в разделе КриптоПро 2.0 политики использования устройств. Один и тот же пользователь Active Directory может быть связан с каталогами различных УЦ.

Пользователь Indeed CM (неважно, в каком каталоге он расположен: Active Directory или КриптоПро 2.0) может быть связан с любым пользователем удостоверяющего центра КриптоПро 2.0. Если каталог УЦ, с которым необходимо установить связь, не содержит пользователей, то при помощи Indeed CM их можно создать.

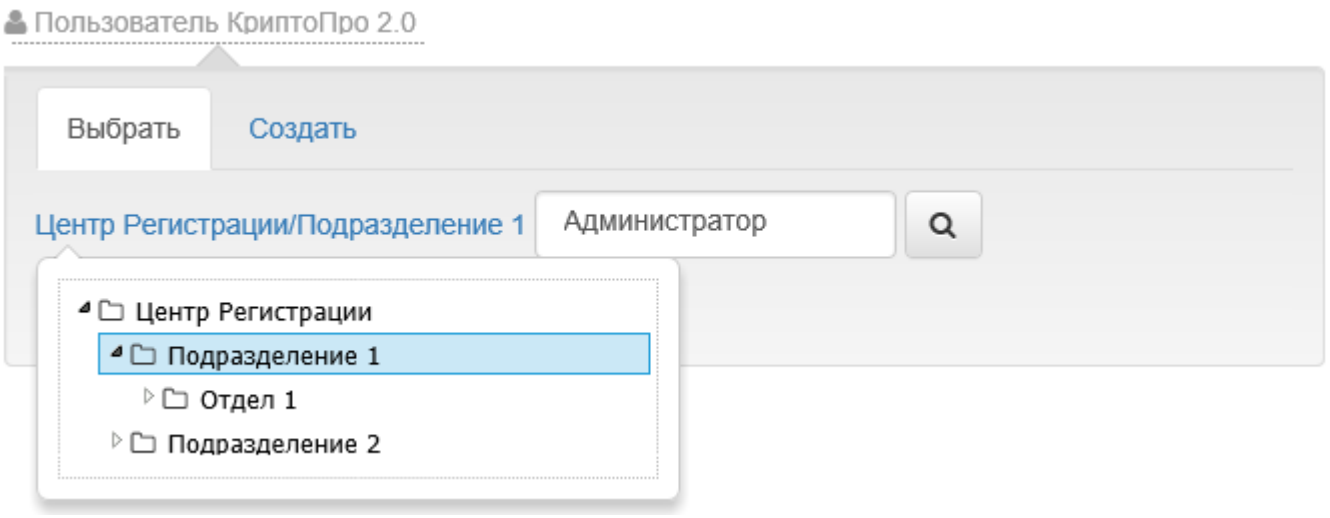
Связать пользователя Active Directory с пользователем КриптоПро УЦ 2.0 можно автоматически (см. опцию **Устанавливать привязку автоматически**) и в ручном режиме.

Для установки связи вручную:

1. Перейдите в карточку пользователя.
2. Нажмите **Пользователь КриптоПро 2.0**:

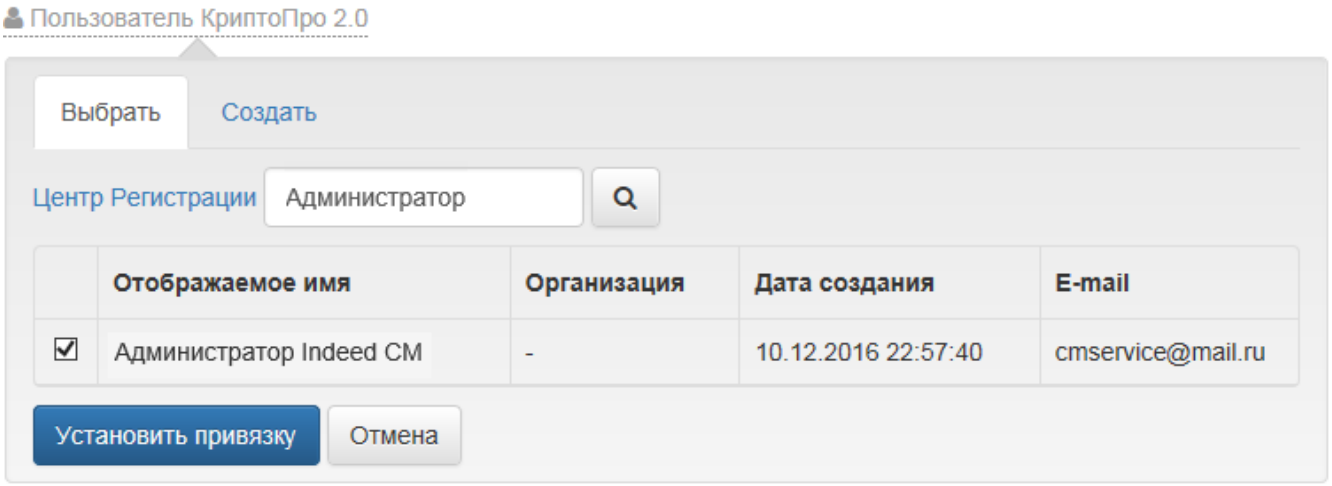


3. Введите имя пользователя центра регистрации КриптоПро УЦ 2.0 и укажите папку, в которой располагаются пользователи:

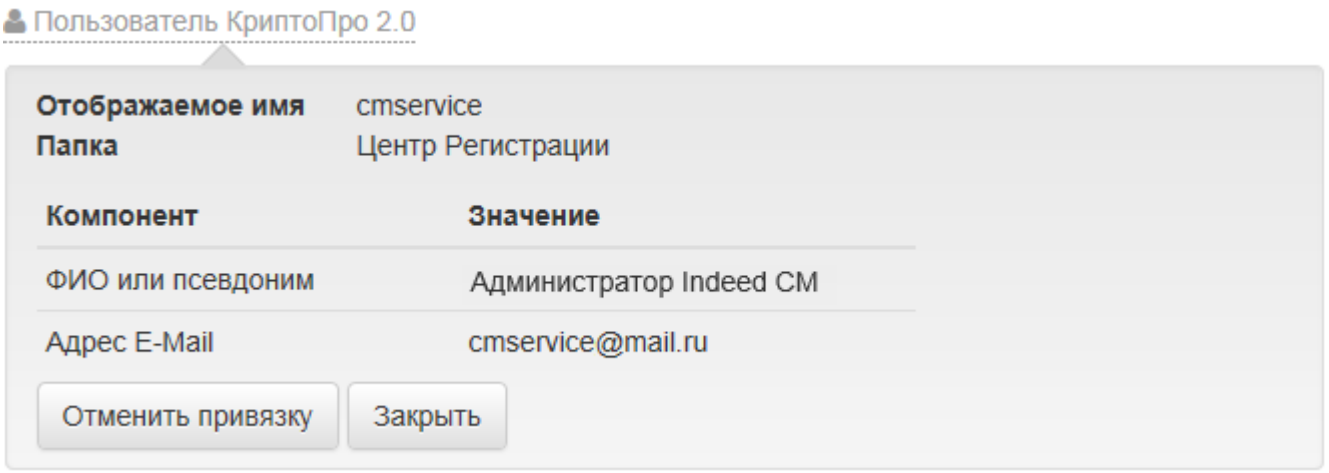


4. Нажмите кнопку поиска.

5. Отметьте нужного пользователя в результатах поиска и нажмите **Установить привязку**.

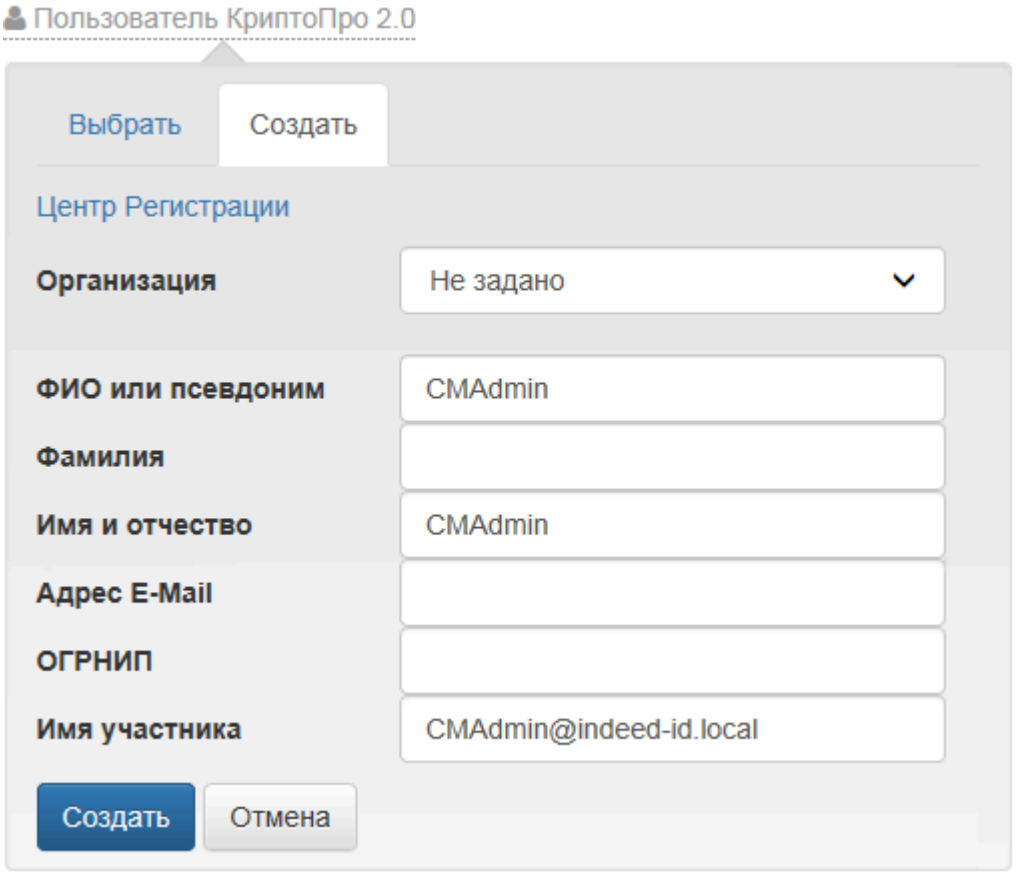


6. Установленную привязку можно отменить. Для этого нажмите **Пользователь КриптоПро 2.0** и затем **Отменить привязку**.



Для создания нового пользователя в каталоге КриптоПро УЦ 2.0:

1. Перейдите в карточку пользователя.
2. Нажмите **Пользователь КриптоПро 2.0** и перейдите на вкладку **Создать**. Вы можете отредактировать данные создаваемого пользователя. Перечень полей для редактирования зависит от настроек используемого удостоверяющего центра КриптоПро.



ПРИМЕЧАНИЕ

При создании пользователя КриптоПро УЦ 2.0 некоторые поля свойств могут быть заполнены автоматически. Например, имя пользователя, адрес электронной почты, город, страна, организация. Эти данные система получает из профиля пользователя Active Directory (см. раздел **Соответствия атрибутов** Мастера настройки Indeed CM).

Разблокировка пользователя

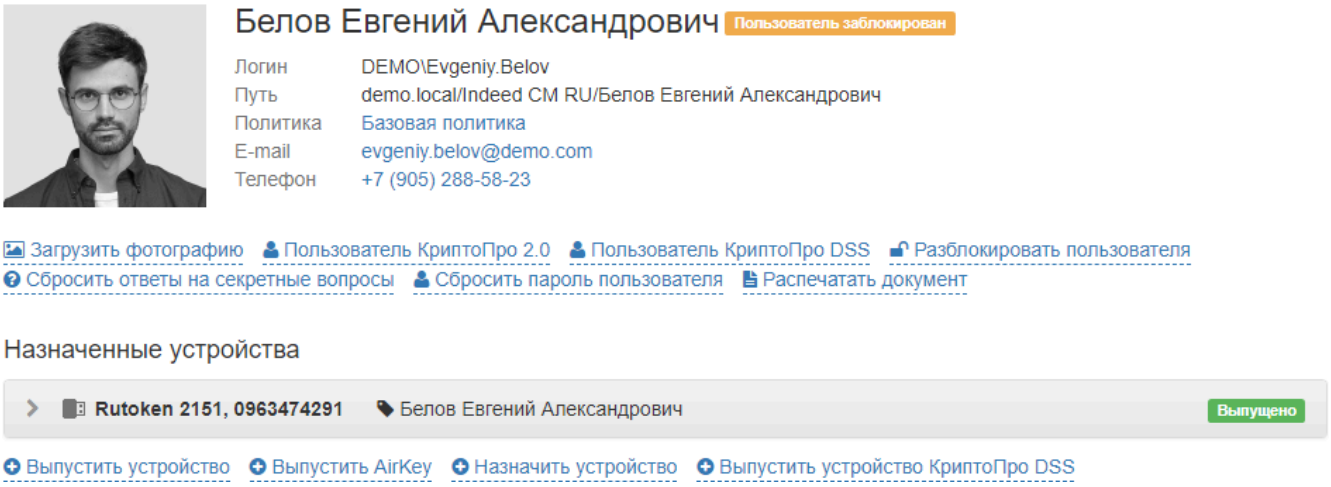
Помимо блокировки устройства пользователя в Indeed Certificate Manager реализован механизм блокировки учетной записи пользователя.

Учетная запись пользователя блокируется, если пользователь превысил количество попыток ввести ответы на секретные вопросы при онлайн-разблокировке устройства или при входе в Сервис удаленного самообслуживания.

Количество попыток задается в параметре **Максимальное количество попыток аутентификации** политики использования устройств.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Заблокированный пользователь не сможет войти в Сервис удаленного самообслуживания и разблокировать/выключить устройство с использованием Indeed CM Credential Provider.
>
> Если заблокированы и устройство, и пользователь, то оператор системы может разблокировать устройство без разблокировки пользователя, если отключить опцию **Проверять ответы на секретные вопросы** в разделе **Поведение** политики использования устройств.

Если учетная запись пользователя заблокирована, в журнал событий системы заносится запись, а в карточке пользователя появляется статус.

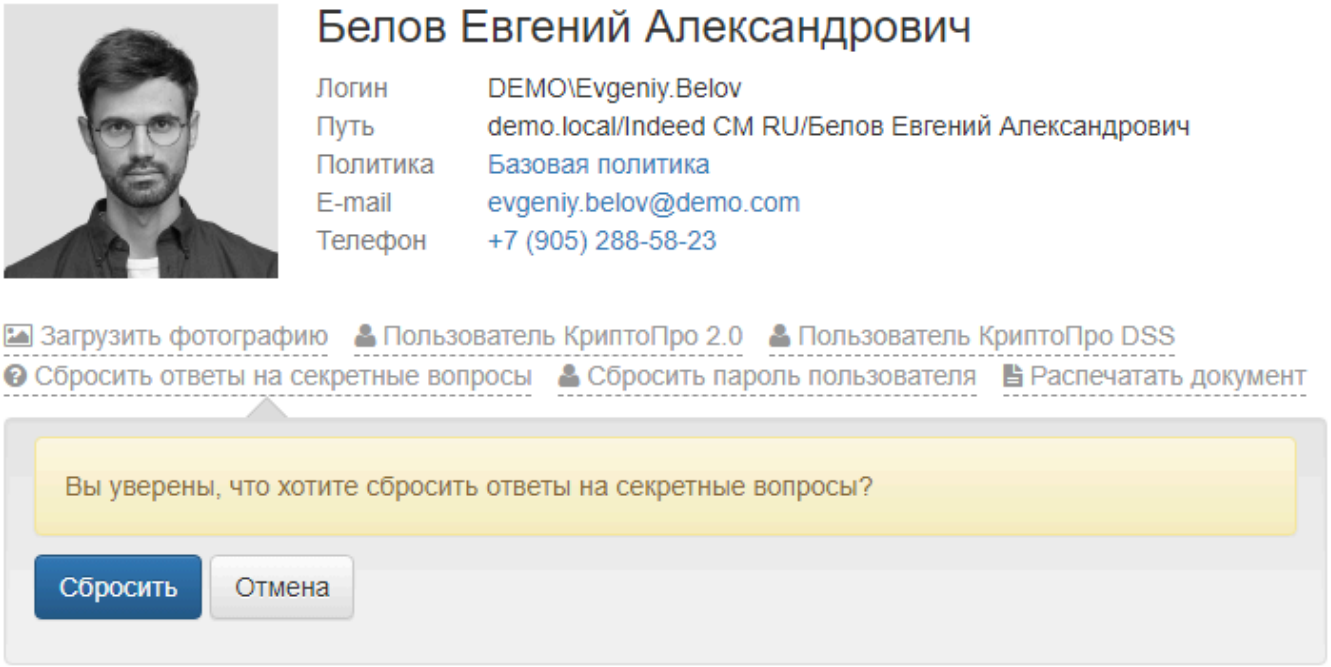


Для разблокировки пользователя нажмите **Разблокировать пользователя**.

Сброс ответов на секретные вопросы

Оператор Indeed Certificate Manager может сбросить секретные вопросы пользователя и указанные ответы. В этом случае пользователь должен будет установить новые вопросы и задать ответы в **Сервисе самообслуживания**.

Чтобы сбросить секретные вопросы пользователя, нажмите **Сбросить ответы на секретные вопросы** в карточке пользователя.



Сброс пароля пользователя

ПОДСКАЗКА

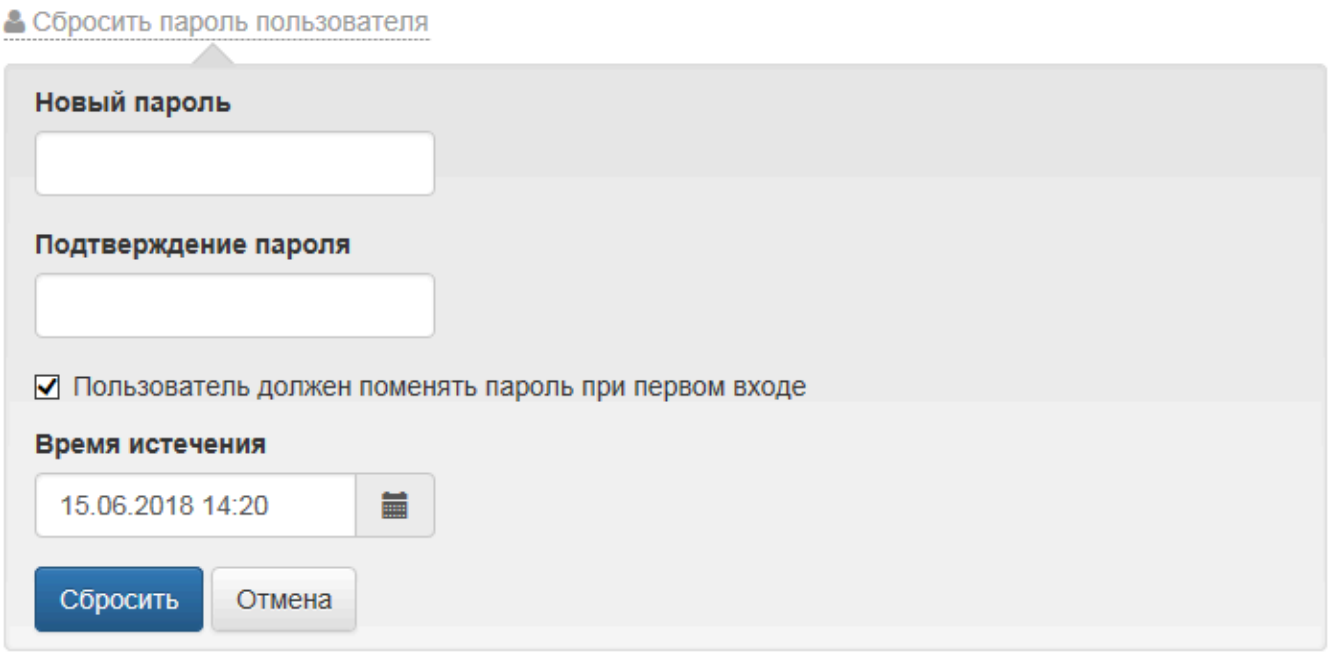
Сброс пароля доступен в карточке пользователя, если включить опцию **Сброс пароля пользователя в Active Directory** в разделе **Общие функции** Мастера настройки Indeed CM.

Оператор и администратор Indeed CM могут сбросить доменный пароля пользователя.

ПРИМЕЧАНИЕ

Сброс доменного пароля может использоваться, если пользователю необходимо войти 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.



> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> 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 – время, по истечении которого служба Card Monitor сбросит пароль на случайное значение.

Пароль будет состоять из:

- латинских строчных и прописных букв
- цифр
- 10 символов

> ⓘ **ПРИМЕЧАНИЕ**
>
> Установленный пароль не будет записан в хранилище данных Indeed CM.

Выпуск устройства

Во время процедуры выпуска устройство персонализируется для пользователя. В соответствии с настройками назначенной политики устройство инициализируется, генерируются ключевые пары, выпускаются сертификаты и записываются в память устройства.

Процесс получения сертификата включает следующие шаги:

1. Пользователь создает запрос на сертификат по заданному шаблону и генерирует на устройстве пару ключей (открытый и закрытый) с использованием криптопровайдера (CSP).
2. Пользователь формирует запрос на сертификат, в который записывается открытый ключ.
3. Пользователь подписывает запрос закрытым ключом.
4. Оператор удостоверяющего центра (УЦ) подписывает запрос ключом сервисной учетной записи с необходимыми правами, которыми владеет сервер Indeed CM.
5. Запрос отправляется в УЦ.
6. УЦ одобряет или отклоняет запрос. После одобрения в УЦ выпущенный сертификат записывается на носитель с помощью криптопровайдера.

Процедура выпуска

Чтобы выпустить устройство пользователю, выполните следующие действия:

1. Перейдите на вкладку **Пользователи** в Консоли управления и выполните поиск пользователя.

2. Нажмите на логин и перейдите в карточку пользователя.

3. Нажмите **Выпустить устройство**.

4. Выберите шаблоны, по которым будут сформированы сертификаты для записи на устройство. Обязательные сертификаты запишутся на устройство автоматически.

5. Если в политике использования устройств настроена **Интеграция со СМЭВ** и сертификат выпускается по шаблону для КриптоПро УЦ 2.0 или Валидата УЦ, отобразится форма проверки СМЭВ. Проверьте данные пользователя.

6. Подключите устройство к компьютеру и задайте следующие настройки:

Инициализировать устройство

Опция **Инициализировать устройство** позволяет отключить и включить инициализацию для конкретного устройства.

При выпуске устройства с инициализацией все данные на устройстве будут удалены.

Параметры инициализации настраиваются в разделе **Выпуск** политики использования устройств.

Имя устройства

Имя устройства выставится автоматически, если в разделе **Выпуск** политики использования устройств задана опция **Генерировать имя устройства автоматически**.

Комментарий к устройству

Указание комментария обязательно, если в разделе **Выпуск** политики использования устройств задана опция **Требовать указания комментария к устройству**.

Если в параметрах шаблона сертификата КриптоПро УЦ 2.0 включена опция **Использовать комментарий устройства в качестве комментария пользователя к запросу на сертификат**, то текст комментария будет добавлен в запрос.

Теги

Добавьте теги, если их создал администратор на вкладке **Конфигурация** в разделе **Теги**.

Добавление тегов обязательно, если в разделе **Выпуск** политики использования устройств задана опция **Требовать указания тегов к устройству**.

Номер и дата документа

Выставите данные о документе, на основании которого будет изготовлено СКЗИ с информацией об устройстве.

Поле **Номер и дата документа** отображается, если:

- устройство поддерживает аппаратную криптографию;
- устройство не добавлено в Indeed CM, и в разделе **Поведение** политики использования устройств задана опция **Добавлять устройство автоматически**.

7. Раздел **Дополнительно** отображается, если устройство не было ранее добавлено в Indeed CM. Введите нужный PIN-код в зависимости от настроек инициализации:

Выпуск с инициализацией

Устройство будет инициализировано, если задать опцию **Инициализировать устройство** (шаг 6) и настроить параметры инициализации при выпуске. Все данные на устройстве будут удалены.

1. Введите **PIN-код администратора**. Поле отображается, если устройство не добавлено в Indeed CM и в разделе **Поведение** политики использования устройств задана опция **Добавлять устройство автоматически**.

   > **ПРИМЕЧАНИЕ**
   >
   > Если поле **PIN-код администратора** оставить пустым, то установится значение, указанное в разделе **Типы устройств**.
   > Поддерживается ввод PIN-кодов для нескольких областей. Например, для PKI и ГОСТ на устройствах JaCarta.

2. Если вы выпускаете устройство eToken со встроенной защитой от форматирования, то укажите ключ инициализации.
3. Нажмите **Выпустить**.

Выпуск без инициализации

1. Введите **PIN-код пользователя**.
2. Введите **PIN-код администратора**. Поле отображается, если устройство не добавлено в Indeed CM и в разделе **Поведение** политики использования устройств задана опция **Добавлять устройство автоматически**.

   > **ПРИМЕЧАНИЕ**
   >
   > Если поля **PIN-код администратора** и **PIN-код пользователя** оставить пустыми, то установятся значения, указанные в разделе **Типы устройств**. Поддерживается ввод PIN-кодов для нескольких областей. Например, для PKI и ГОСТ на устройствах JaCarta.

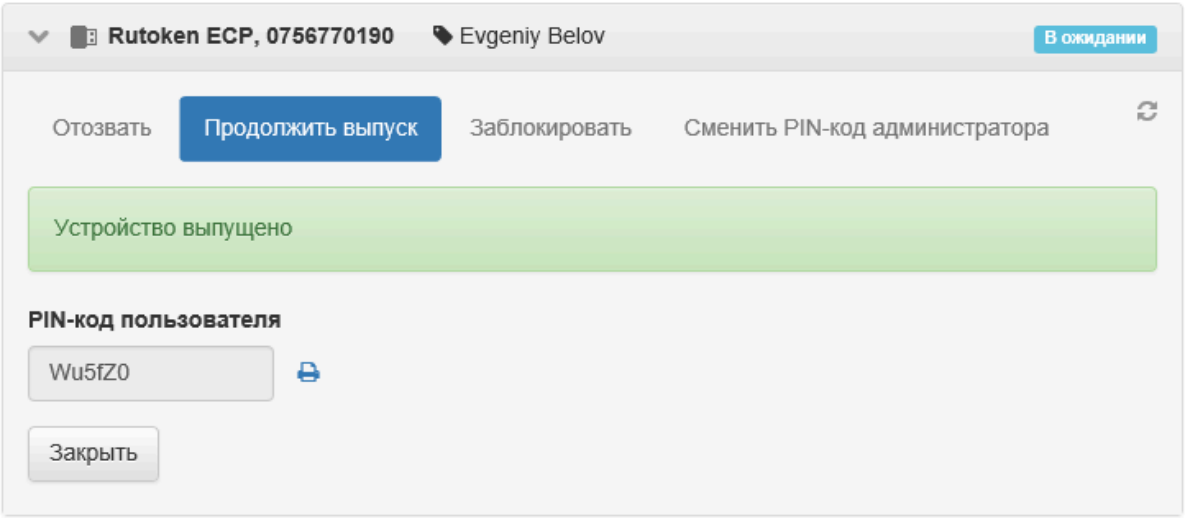
3. Нажмите **Выпустить**.
4. Если устройство содержит сторонние сертификаты, Indeed CM может их обнаружить и внести информацию о таких сертификатах в систему – отследить. Окно выбора сертификатов для отслеживания отображается, если в разделе **Поведение** политики использования устройств задана опция **Включить отслеживание сертификатов**.
   Выберите сертификаты для отслеживания, если они есть на устройстве, и нажмите **ОК**.

8. Если в разделе **Выпуск** политики использования устройств задана опция **Установить случайный PIN-код пользователя**, то после выпуска устройства отобразится PIN-код пользователя.

Как передать PIN-код пользователю

Если в разделе **Уведомления** настроена рассылка уведомлений по электронной почте, PIN-код можно отправить на электронную почту пользователя и его руководителя.

PIN-код можно распечатать и отправить в конверте. Нажмите . PIN-код будет сохранен в файле *PinEnvelope.pdf*.



ПРИМЕЧАНИЕ

Параметры печати содержатся в шаблоне *C:\inetpub\wwwroot\cm\mc\wwwroot\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*.

9. По завершении выпуска устройства нажмите **Закрыть**.

После выпуска устройства в разделе **Назначенные устройства** карточки пользователя отобразятся сведения об устройстве.

Контроль выпуска

Выпуск устройства можно приостановить, если регламент вашей организации предусматривает проверку запроса на сертификат в УЦ.

Чтобы настроить проверку запроса на сертификат в УЦ, перейдите в настройки шаблонов сертификатов используемых УЦ и отключите опцию **Автоматически одобрять запрос на сертификат**.

В окне выпуска устройства появится сообщение *Выпуск устройства ожидает решения*. Устройству присваивается статус **В ожидании**. Это означает, что запрос на выпуск устройства перешел в стадию рассмотрения.

Если запрос на сертификат одобрен в УЦ, то сертификат получает статус **Одобрен** и записывается на устройство. Нажмите **Продолжить выпуск устройства** в карточке устройства.

Если запрос отклонен в УЦ, отзовите и очистите устройство, после чего начните выпуск устройства заново.

Если в политике настроена автоматическая рассылка уведомлений по электронной почте, то вам придет уведомление о статусе одобрения. Если автоматическая рассылка уведомлений не настроена, дождитесь появления кнопки **Продолжить обновление устройства** в карточке устройства.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Если на устройство одновременно записываются несколько сертификатов, устройство можно выпустить, когда оба запроса на сертификат одобрены в УЦ.
> Если один из сертификатов был одобрен автоматически (статус **Действительный**), он будет записан на устройство вместе со вторым сертификатом.

Проверка данных пользователя в СМЭВ

> ⓘ **ПРИМЕЧАНИЕ**
>
> 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 в политике использования устройств настроена **Интеграция со СМЭВ** и требуется выпустить или обновить квалифицированный сертификат КриптоПро УЦ 2.0 или Валидата УЦ согласно политике использования устройств.

1. Выберите **Тип пользователя**, данные которого необходимо проверить в СМЭВ: физическое лицо, юридическое лицо или индивидуальный предприниматель.
2. Введите данные пользователя и нажмите **Далее**.
3. Проверка данных пользователя может занять несколько часов. Нажмите **Проверить повторно**, чтобы редактировать данные пользователя и проверить их повторно, или **Закрыть**, чтобы продолжить проверку в фоновом режиме. Данные, введенные при проверке, сохраняются.

Результат проверки отобразится при следующей попытке выпуска или обновления устройства. Результат можно проверить в **Журнале событий**.

Если проверка прошла успешно, выберите:

- **Проверить повторно**, чтобы повторно проверить данные пользователя в СМЭВ. Например, если паспортные данные пользователя изменились с момента последней проверки.
- **Далее**, чтобы продолжить выпуск/обновление устройства.
- **Отмена**, чтобы отменить выпуск/обновление устройства.

Если проверка завершилась ошибкой, выберите:

- **Проверить повторно**, чтобы редактировать данные пользователя и проверить их повторно.
- **Одобрить данные пользователя**, чтобы принудительно подтвердить корректность данных.
- **Отмена**, чтобы отменить выпуск/обновление устройства.

ПОДСКАЗКА

Выберите опцию **Одобрить данные пользователя**, если в СМЭВ еще не поступили недавно измененные персональные данные пользователя (например, при смене фамилии или замене паспорта).

Опция доступна для администраторов и операторов Indeed CM с привилегией **Одобрение данных запроса СМЭВ**. Привилегия назначается на вкладке **Конфигурация** в разделе **Роли**.

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. Если отзыв временный (после 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 (после отзыва или изъятия устройства), сертификат нельзя использовать.
Истекает	Срок действия сертификата скоро закончится. Обновите сертификат, если планируете его использовать.
Ключ истекает	Срок действия закрытого ключа сертификата КриптоПро УЦ скоро закончится. Обновите сертификат, если планируете его использовать. Закрытый ключ также будет обновлен.
Истек	Срок действия сертификата истек. Сертификат непригоден для использования. Срок действия сертификата можно продлить на период, равный сроку его действия, заданный в шаблоне сертификата на УЦ (см. раздел **Обновление устройства**).
Ошибка	Состояние сертификата не удалось определить. Возможно, центр сертификации недоступен. Сертификат непригоден для использования.
Одобрен	Администратор одобрил запрос на сертификат, но сертификат еще не выпущен пользователю.

Состояние сертификата	Описание
Отклонен	Администратор отклонил запрос на сертификат.
В ожидании	Запрос на сертификат ожидает рассмотрения оператором УЦ.

Публикация выпущенных сертификатов

Сертификаты, выпущенные и записанные на устройство, можно опубликовать в следующие хранилища:

- 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**.
- Единая система идентификации и аутентификации (ЕСИА). Опция **Публиковать сертификат в ЕСИА**.
- Файловое хранилище. Опция **Публиковать сертификат в файловое хранилище**.
- База приложений ЦФТ. Опция **Публиковать сертификат в ЦФТ**.

Печать персонального сертификата и запроса сертификата

Печатные формы запроса на сертификат, сертификата и запроса на отзыв сертификата можно сохранить в формате PDF и отправить пользователю по электронной почте.

Для печати нажмите , выберите нужную форму и сохраните файл.

Для изменения стандартных шаблонов печати, общих для всех шаблонов сертификатов, добавленных в политику использования устройств, отредактируйте в Консоли управления и в Сервисе самообслуживания следующие файлы:

Консоль управления:

- *C:\inetpub\wwwroot\cm\mc\wwwroot\content\request_ru.xsl* – шаблон печати запроса;
- *C:\inetpub\wwwroot\cm\mc\wwwroot\content\cert_ru.xsl* – шаблон печати сертификата;

- *C:\inetpub\wwwroot\cm\mc\wwwroot\content\revocationRequest_ru.xsl*– шаблон печати запроса на отзыв сертификата.

Сервис самообслуживания:

- *C:\inetpub\wwwroot\cm\ss\wwwroot\content\request_ru.xsl* – шаблон печати запроса;
- *C:\inetpub\wwwroot\cm\ss\wwwroot\content\cert_ru.xsl* – шаблон печати сертификата;
- *C:\inetpub\wwwroot\cm\ss\wwwroot\content\revocationRequest_ru.xsl* – шаблон печати запроса на отзыв сертификата.

Вы можете использовать разные шаблоны печати сертификата, запроса на сертификат или запроса на отзыв сертификата для шаблонов сертификатов, добавленных в политику выпуска устройств. Для этого отредактируйте шаблоны и загрузите их на вкладке **Конфигурация** Консоли управления в разделе **Шаблоны печати**, и выберите в **Настройках шаблонов сертификатов**.

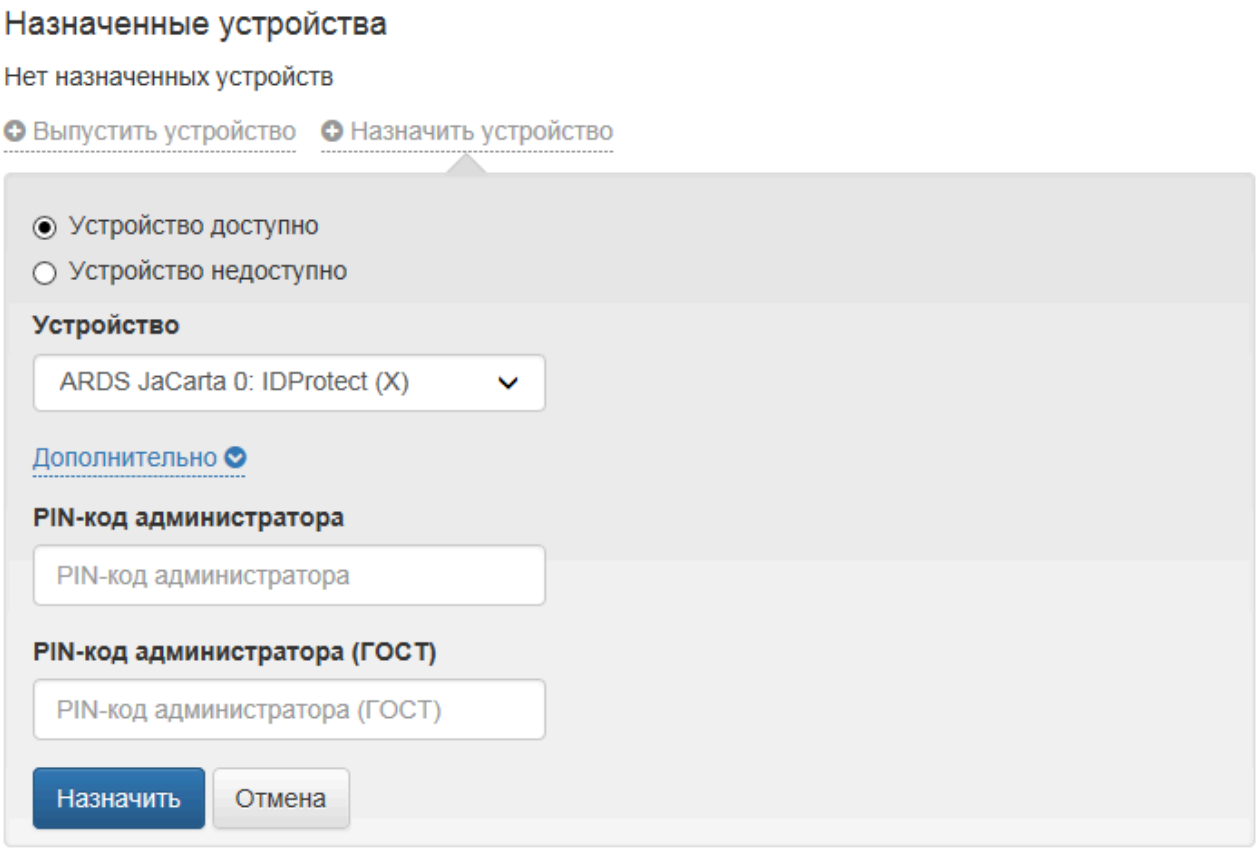
Назначение устройства

При назначении устройство закрепляется за пользователем, чтобы пользователь мог выпустить это устройство самостоятельно в Сервисе самообслуживания.

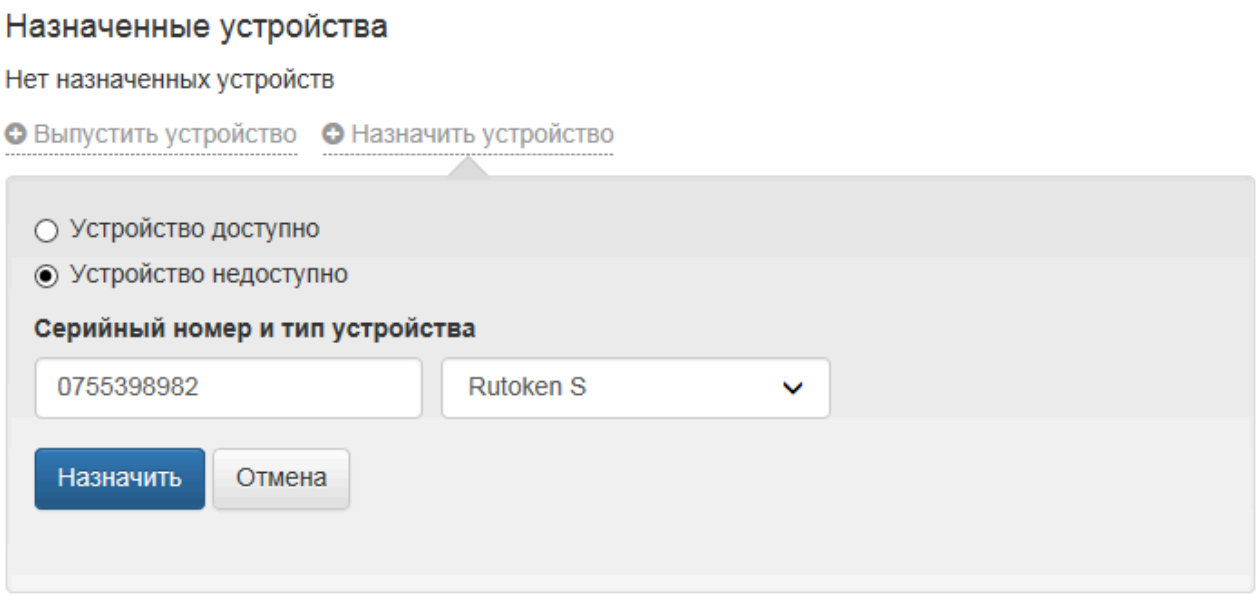
> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Одно устройство может одновременно принадлежать только одному пользователю. У одного пользователя может быть несколько устройств. Возможность пользователям самостоятельно назначать себе устройства в Сервисе самообслуживания задает администратор в разделе **Поведение** политики использования устройств, действующей на пользователя.

Чтобы назначить устройство 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**. Нажмите **Назначить**.



4. Если устройство недоступно, но известны его серийный номер и тип, укажите их и нажмите **Назначить**.



Назначенное устройство имеет статус **Назначено** в карточке пользователя.

Отмена назначения

Вы можете отозвать устройство, которое было назначено пользователю, но еще не выпущено.

Чтобы отменить назначение, перейдите в карточку пользователя, выберите назначенное устройство и нажмите **Отменить назначение**.

Если назначенное устройство поддерживает аппаратную криптографию и в системе ведется учет СКЗИ, то в поле **Номер и дата документа** автоматически выставятся номер и дата нормативного документа об изъятии по шаблону, заданному в разделе **Конфигурация → Нормативные документы**.

Информация об имеющихся в системе средств криптографической защиты информации находится в Консоли управления в разделе **Дополнительно → СКЗИ**.

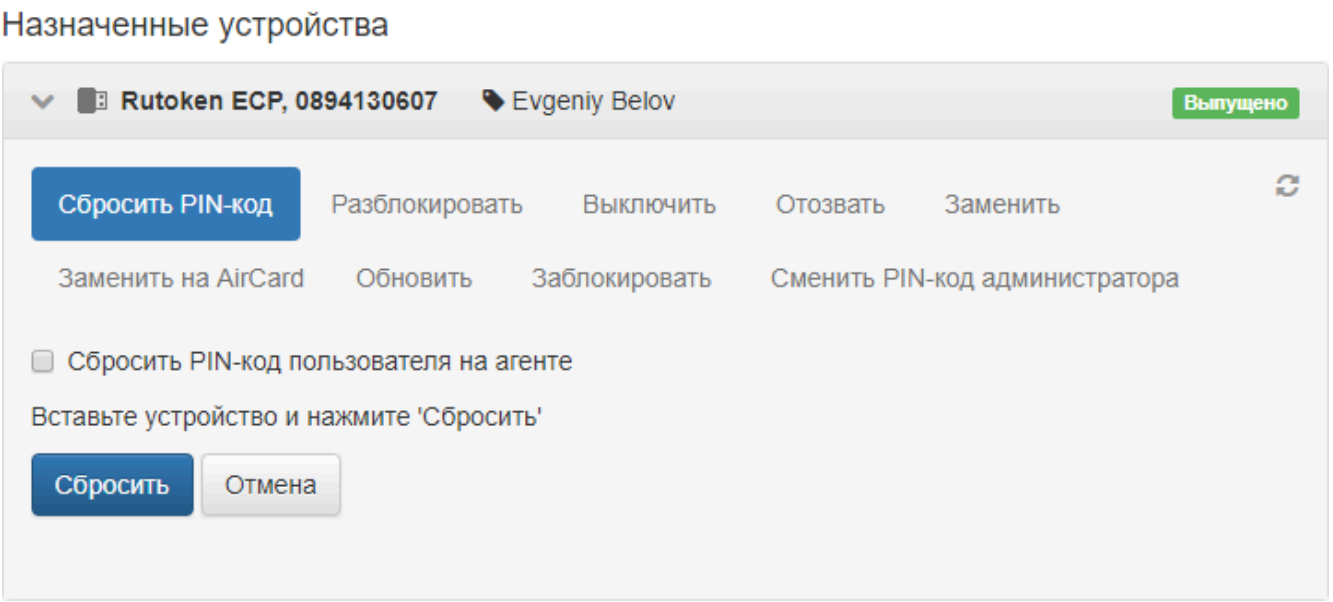
Сброс PIN-кода устройства

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**.

> **ПРИМЕЧАНИЕ**
>
> 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. Нажмите на логин и перейдите в карточку пользователя.
3. Выберите нужное устройство и раскройте информацию о нем.
4. Нажмите **Сбросить PIN-код:**.
5. Подключите устройство и нажмите **Сбросить**. Если устройство недоступно, выберите опцию **Сбросить PIN-код пользователя на агенте**, чтобы создать задачу для Indeed CM Agent.



Когда администратор сбросит PIN-код, пользователь сможет задать новый PIN-код самостоятельно в Сервисе самообслуживания.

Разблокировка устройства

Устройство блокируется, если пользователь ввел неверный PIN-код устройства больше определенного количества раз.

Максимальное количество попыток ввода PIN-кода пользователем задает администратор в разделе **Выпуск → Инициализация устройства** политики использования устройств.

Существует два режима разблокировки устройства пользователя: онлайн и офлайн.

Онлайн

Онлайн-разблокировка осуществляется пользователем в окне входа ОС Windows. Пользователь отвечает на секретные вопросы, задает и подтверждает новый PIN-код, после чего устройство разблокируется.

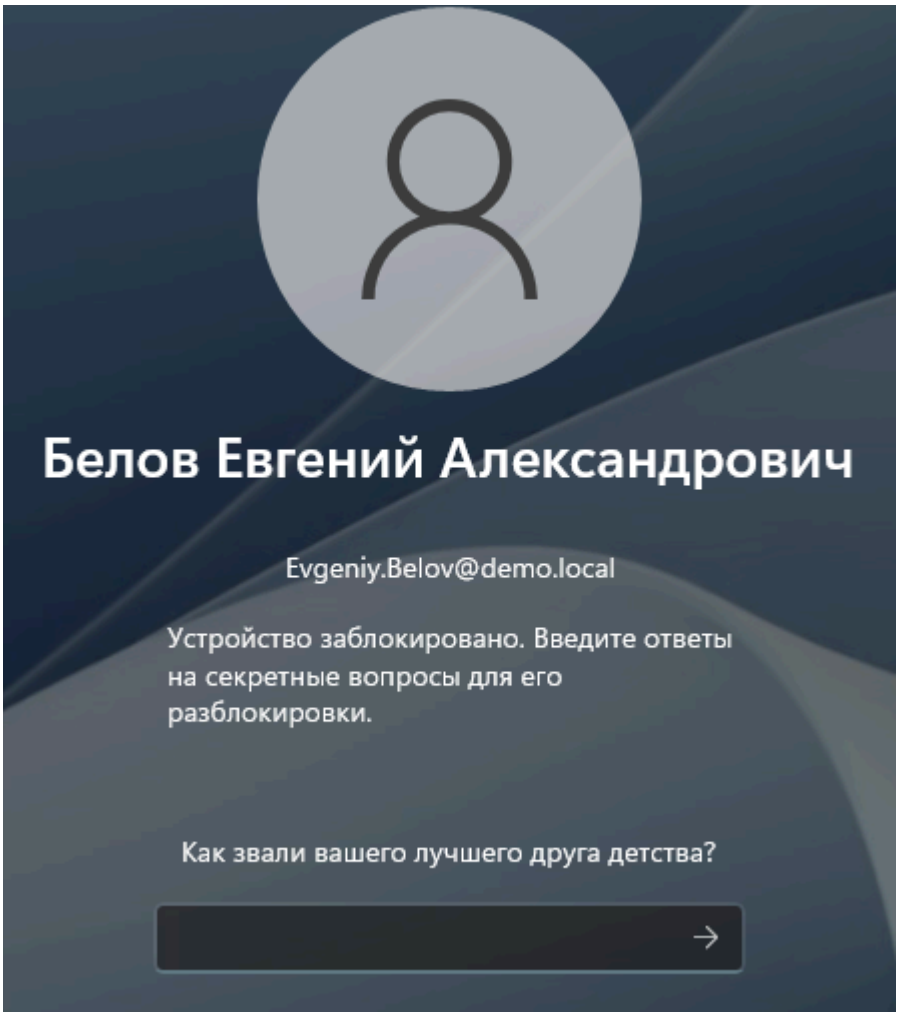
Обязательные условия для онлайн-разблокировки:

- Рабочая станция пользователя, к которой подключено заблокированное устройство, связана с сервером Indeed CM.
- Пользователь задал ответы на секретные вопросы в Сервисе самообслуживания.

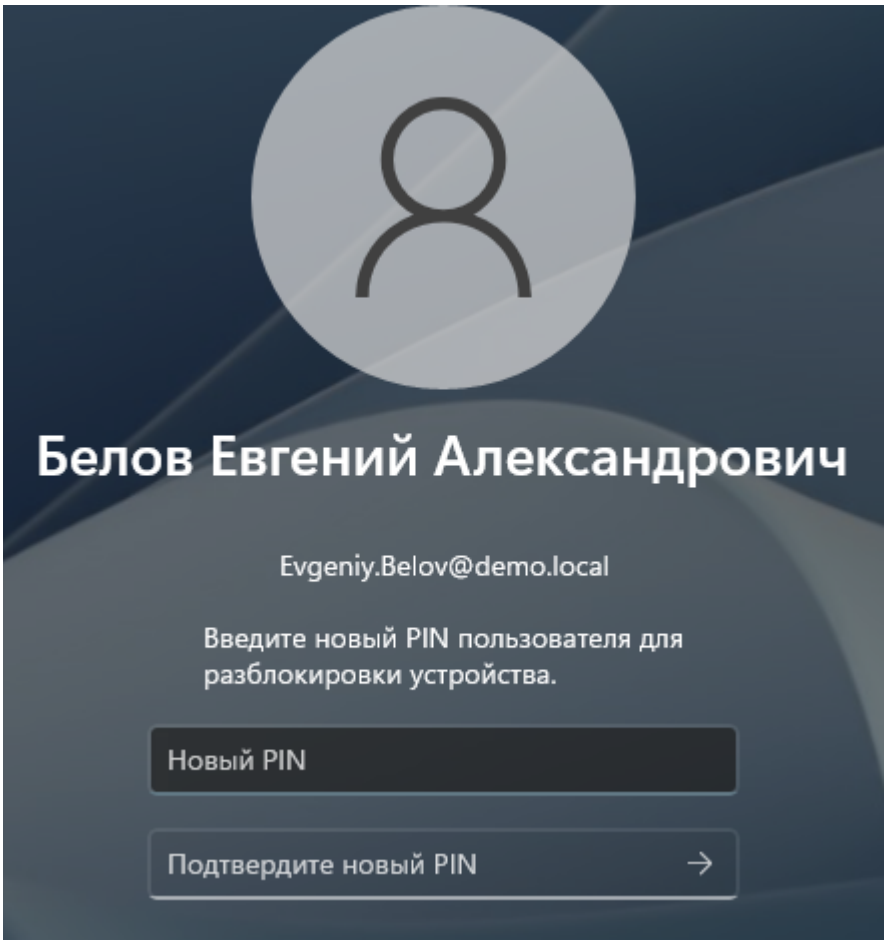
Если секретные вопросы пользователя не установлены, онлайн-разблокировка устройства будет недоступна. Разблокировать устройство можно в офлайн-режиме.

Пример онлайн-разблокировки устройства в окне входа ОС Windows 11

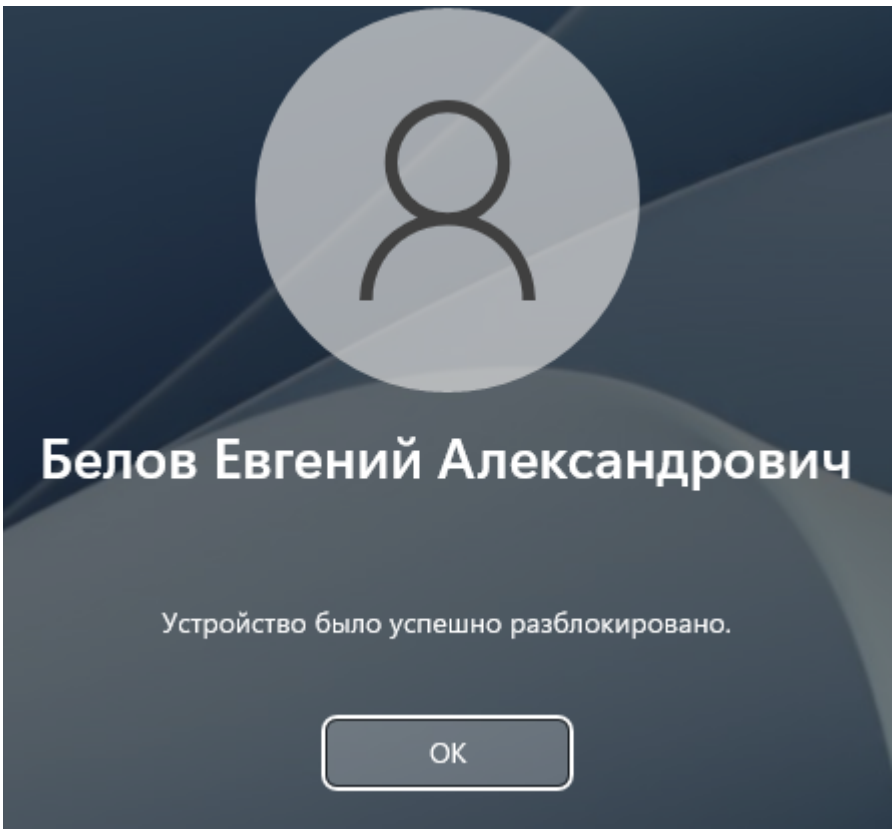
1. Введите ответы на секретные вопросы и нажмите  .



2. Введите **Новый PIN** и его **Подтверждение**.



3. В случае успешной разблокировки устройства появится сообщение.



Механизм разблокировки устройства в ОС Windows других версий выглядит похожим образом.

Офлайн

Разблокировать устройство офлайн можно в окне входа Windows или в Windows сессии.

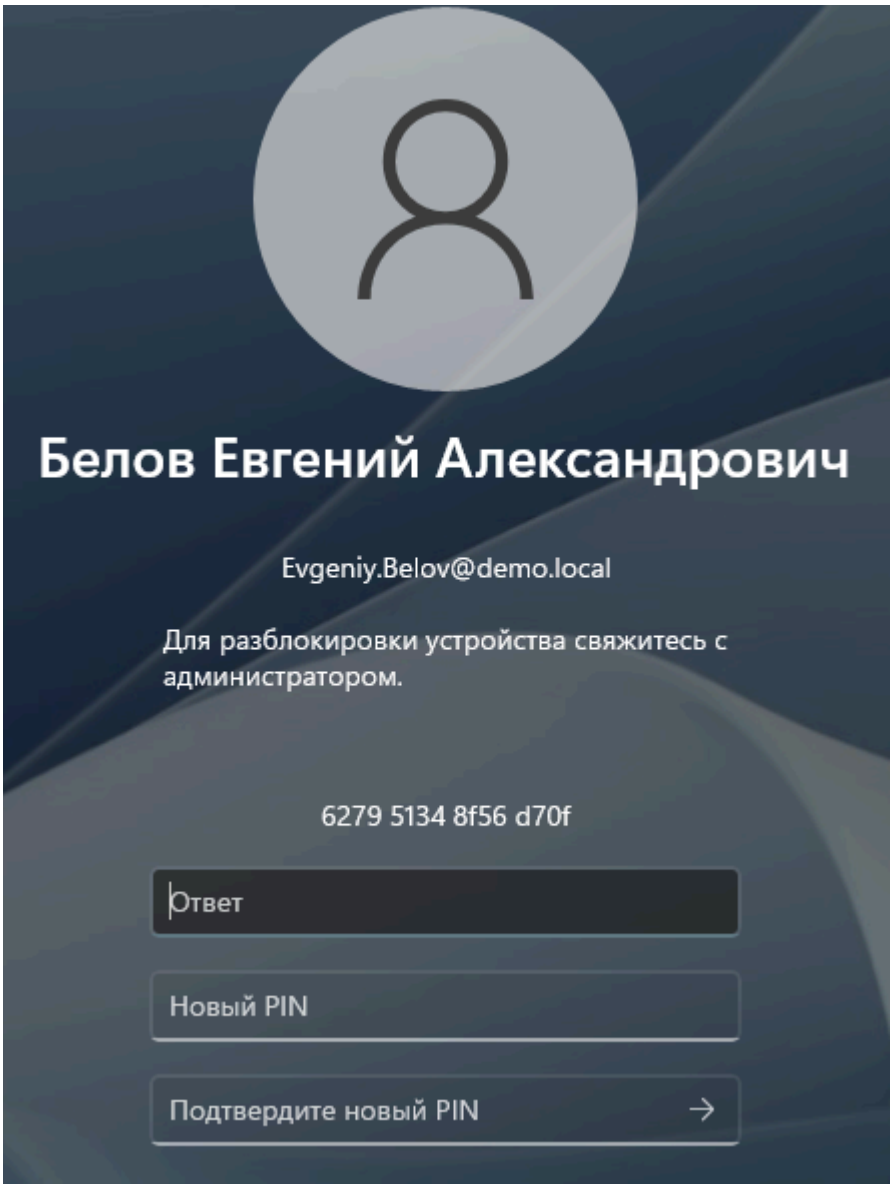
Окно входа

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Разблокировка устройства на экране входа в Windows не поддерживается при удаленном подключении через Remote Desktop.

Офлайн-разблокировка осуществляется оператором Indeed CM по принципу аутентификации вида запрос-ответ (challenge-response authentication mechanism).

При исчерпании заданного числа попыток ввода PIN-кода пользователь получает сообщение, что его устройство заблокировано. Вместе с сообщением пользователь получает уникальный код-запрос из 16 символов. Пользователю необходимо связаться с оператором системы (например, по телефону), подтвердить свою личность, ответив на секретные вопросы, и сообщить полученный код.

Пример экрана офлайн-разблокировки устройства в окне входа ОС Windows 11

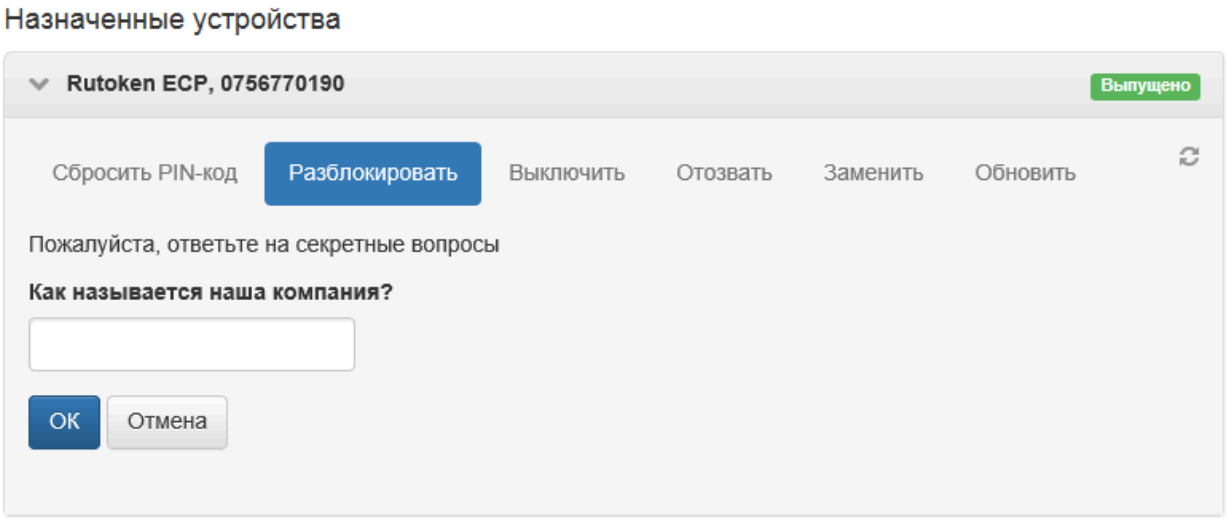


Оператор системы открывает карточку пользователя и в перечне действий над устройством выбирает пункт **Разблокировать**. Прежде чем выполнить генерацию ответного кода для разблокировки устройства, администратор системы задает секретный вопрос (или несколько вопросов, в зависимости от настроек политики использования устройств) и вводит полученный от пользователя ответ в соответствующую форму.

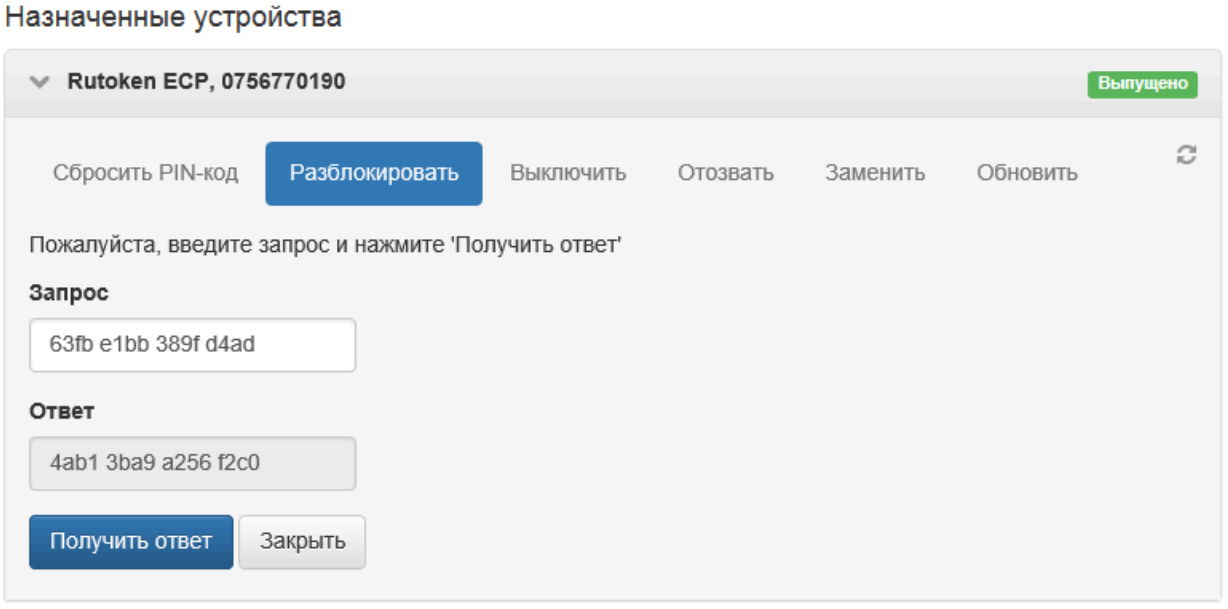
ПРИМЕЧАНИЕ

Опцию **Разрешить офлайновую разблокировку** можно отключить в разделе **Поведение** политики использования устройств. В этом случае кнопка **Разблокировать** в карточке устройства будет недоступна.

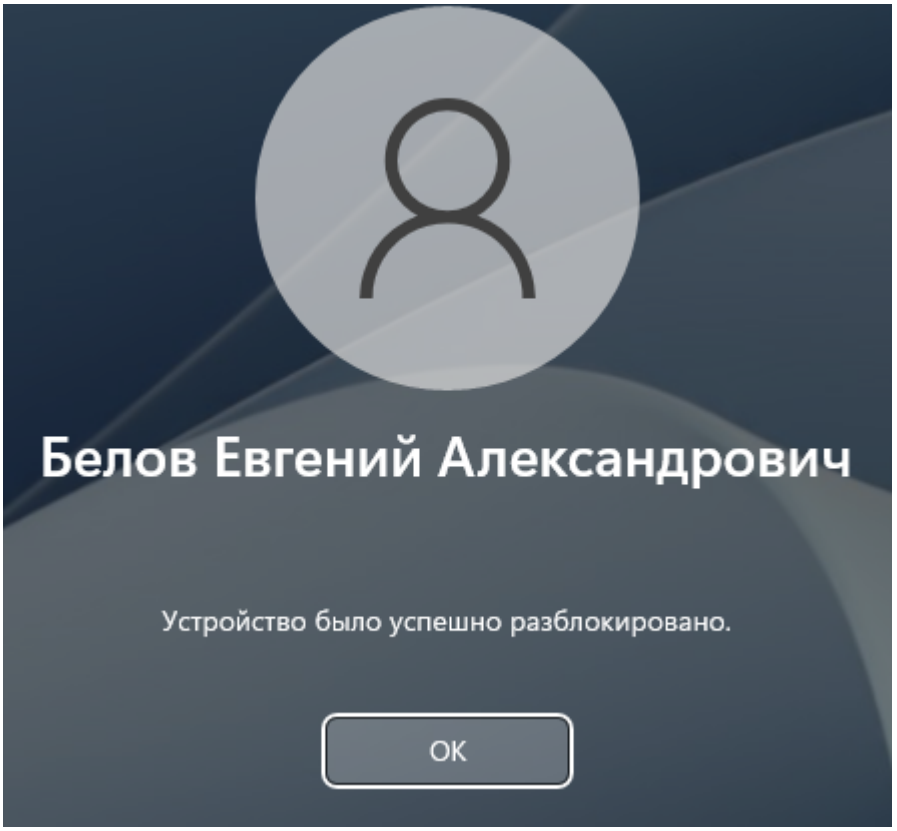
Необходимость проверки ответов на секретные вопросы при офлайн-разблокировке определяется опцией **Проверять ответы на секретные вопросыт** в разделе **Поведение** политики использования устройств.



Если ответы на все вопросы даны верно, то оператор вводит код, полученный от пользователя, и система генерирует ответный код, который оператор сообщает пользователю.



Пользователь вводит код, полученный от оператора, и задает новый PIN-код устройства. В случае успешной разблокировки отображается соответствующее сообщение.

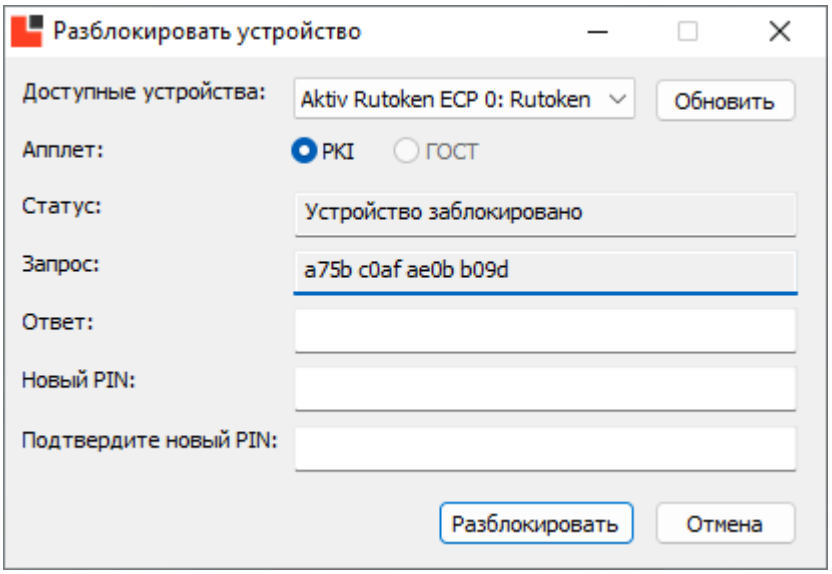


Механизм разблокировки устройства в ОС Windows других версий выглядит похожим образом.

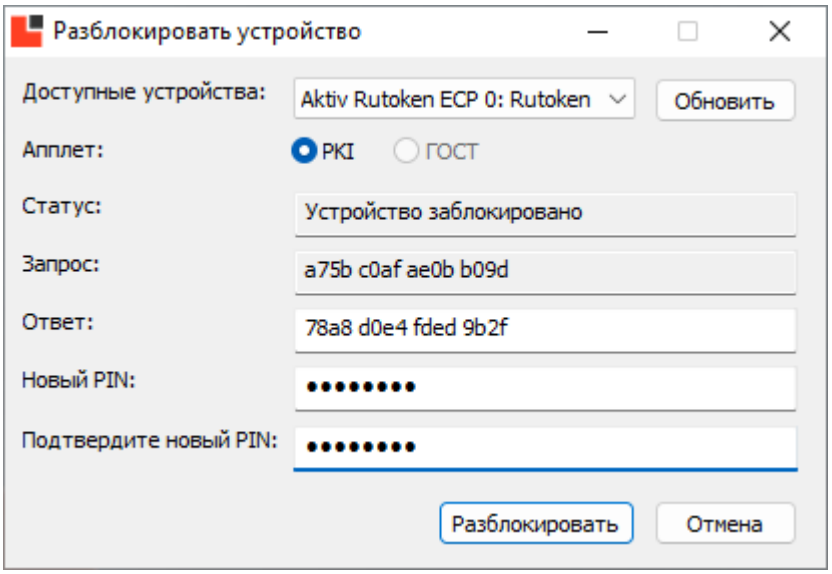
Сессия

Если устройство не используется для входа на рабочую станцию и было заблокировано, то для его разблокировки применяется утилита Indeed CM - Unblock (*Пуск – Все программы – Indeed*).

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 код в поле **Ответ** утилиты разблокировки, задайте новый PIN-код, подтвердите его и нажмите **Разблокировать**.



После этого устройство разблокируется, а PIN-код изменится на новый. Завершите работу с утилитой Indeed CM - Unblock.

Выключение и включение устройства

Устройство пользователя можно выключить на определенный промежуток времени и затем снова включено. Например, на период отпуска сотрудника.

> **ПРИМЕЧАНИЕ**
>
> Оператор может выключить и включить устройство без подключения устройства к рабочей станции.

Для выключения устройства пользователя выполните следующие действия:

1. Перейдите на вкладку **Пользователи** и выполните поиск пользователя.
2. Нажмите на логин и перейдите в карточку пользователя.
3. Выберите нужное устройство и раскройте информацию о нем.
4. Нажмите **Выключить**.

> **ПРЕДУПРЕЖДЕНИЕ**
>
> При выключении устройства Indeed Certificate Manager сможет отозвать все сертификаты, хранящиеся на нем. Для этого включите опцию **Отзывать сертификат при отзыве/выключении устройства** в политике использования устройств.
>
> Сертификаты будут отозваны с отметкой **Приостановка действия** (Certificate hold). Включите устройство, чтобы возобновить действие сертификатов.

При попытке использования выключенного устройства для аутентификации пользователь получит сообщение, что его сертификаты отозваны.

Для включения устройства пользователя выполните следующие действия:

1. Перейдите на вкладку **Пользователи** и выполните поиск пользователя.
2. Нажмите на логин и перейдите в карточку пользователя.
3. Выберите нужное устройство и раскройте информацию о нем.
4. Нажмите **Включить**.

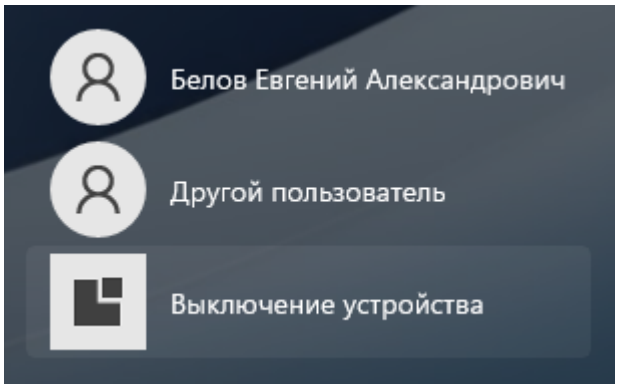
Выключение устройства без выполнения входа в систему

В экстренном случае пользователь может самостоятельно выключить устройство без выполнения входа в операционную систему.

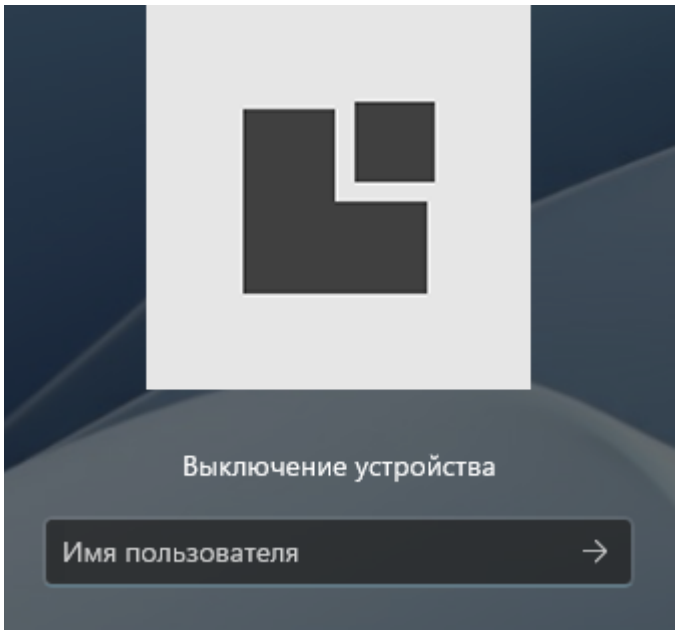
> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Выключение устройства доступно только в том случае, если у рабочей станции, с которой осуществляется операция, есть связь с сервером Indeed Certificate Manager, и у пользователя заданы ответы на секретные вопросы.
>
> Возможность выключения устройства можно отключить для определенных категорий пользователей (см. раздел **Настройка онлайн-разблокировки устройств**).

Для выключения устройства пользователя выполните следующие действия:

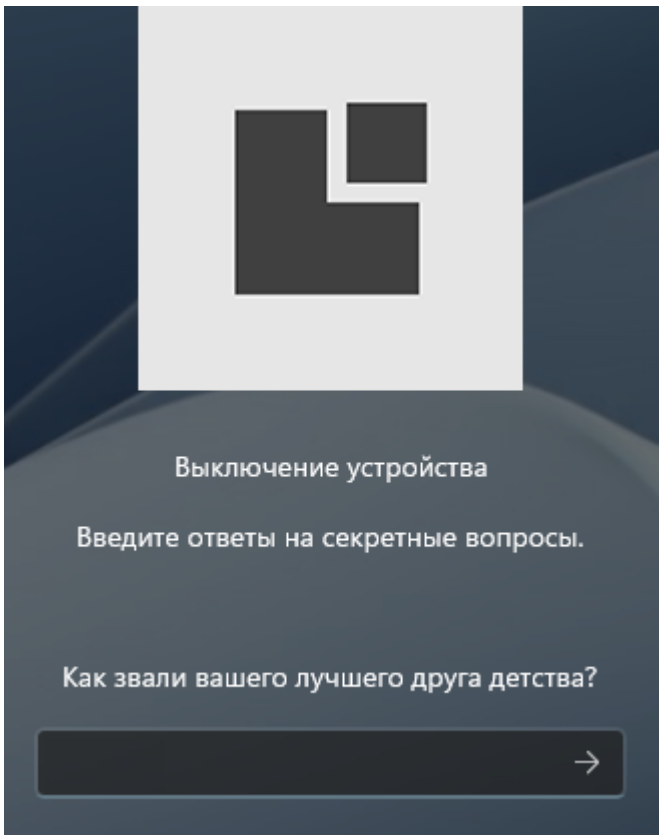
1. Выберите **Выключение устройства** на экране входа Windows. Пример для операционной системы Windows 11:



2. Укажите имя пользователя (логин или UPN), устройство которого необходимо выключить.



3. Введите ответы на секретные вопросы.



4. Выберите устройство из списка выпущенных устройств пользователя и нажмите .

Появится сообщение "Устройство было успешно выключено".

Отзыв устройства

Оператор или пользователь могут отозвать устройство, если оно повреждено, утеряно, изъято, или устройство нужно обновить.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Если в настройках шаблонов сертификатов включена опция **Отзывать сертификат при отзыве/выключении устройства**, то все сертификаты 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. Нажмите на логин и перейдите в карточку пользователя.
3. Выберите нужное устройство и раскройте информацию о нем.
4. Нажмите **Отозвать**.
5. Укажите **Причину отзыва**.

> ⓘ **ПРИМЕЧАНИЕ**
>
> Если устройство отзывается по причинам **Устройство утеряно** или **Компрометация устройства**, то все сертификаты на устройстве будут отозваны (даже если не была включена опция **Отзывать сертификат при отзыве/выключении устройства** в параметрах шаблонов сертификатов).

6. Нажмите **Отозвать**, если устройство доступно. Если устройство недоступно, создайте задачу на агенте - выберите опцию **Очистить устройство на агенте**.

Причина отзыва устройства отображается в карточке пользователя. При попытке использования отозванного устройства для аутентификации пользователь получит сообщение, что его сертификаты отозваны.

Изъятие устройства

Отозванное устройство пользователя остается закрепленным за ним. Такое устройство можно заменить (см. раздел **Замена устройства**) или изъять.

Для изъятия устройства пользователя выполните следующие действия:

1. Перейдите на вкладку **Пользователи** и выполните поиск пользователя.
2. Нажмите на логин и перейдите в карточку пользователя.
3. Выберите нужное устройство и раскройте информацию о нем.
4. Нажмите **Изъять**.
5. Выберите **Устройство недоступно (потеряно или повреждено)**, если у вас нет доступа к устройству. Нажмите **Изъять**.
6. Выберите **Устройство доступно**, если у вас есть доступ к устройству. Подключите его к рабочей станции и при необходимости выберите опции:

- **Очистить устройство**

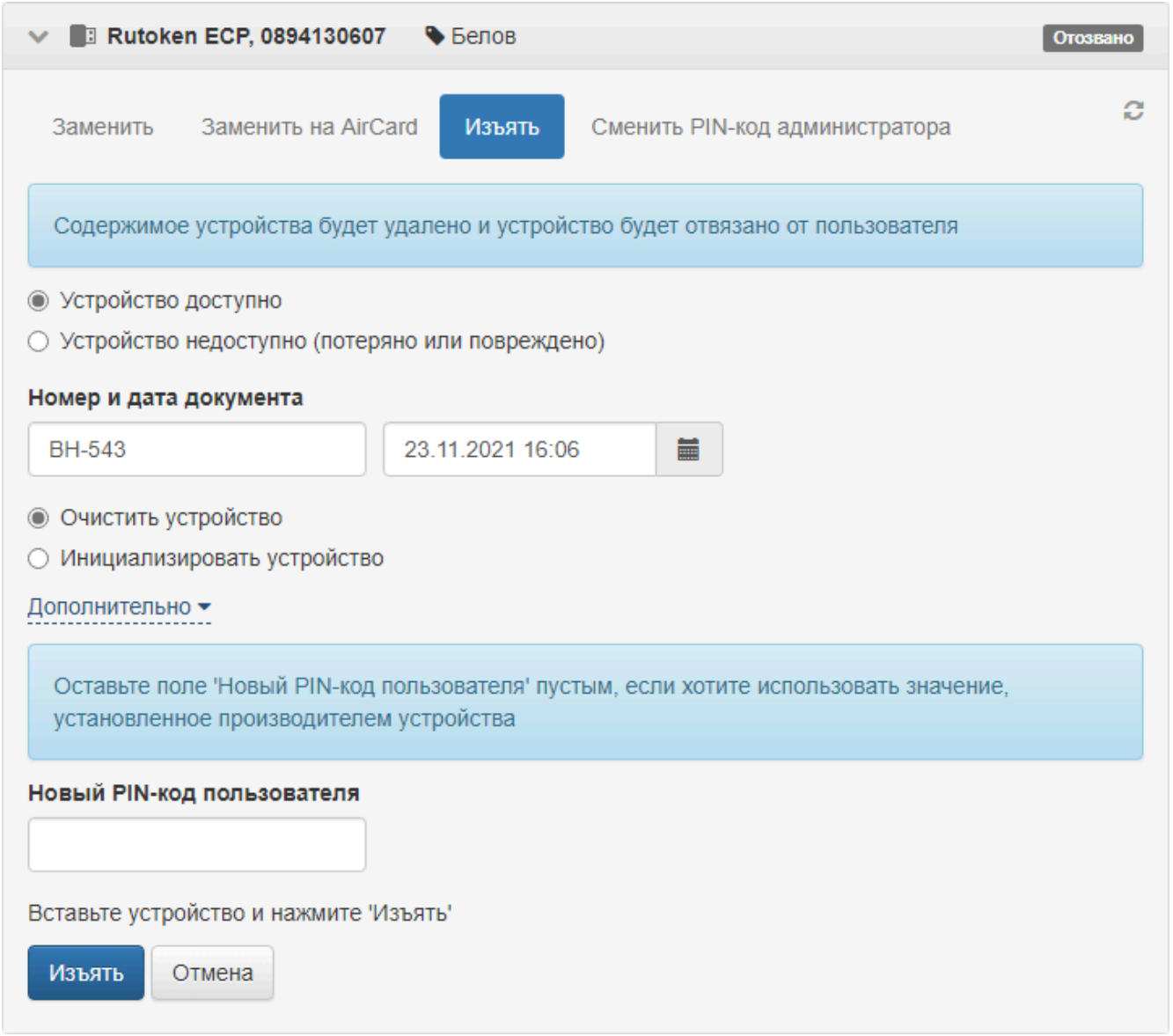
  После изъятия с устройства удалятся все сертификаты, записанные в Indeed CM. Сертификаты, запросы, ключи, записанные вне Indeed CM не будут удалены.
  Укажите **PIN-код пользователя**, который установится на устройстве после его изъятия. Если не задать PIN-код пользователя, то после изъятия устройства установится PIN-код, указанный в типе этого устройства.

> **ПРИМЕЧАНИЕ**
>
> PIN-код пользователя нужно установить, если PIN-код, 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**).

- **Инициализировать устройство**

  После изъятия с устройства удалятся все данные. Для инициализации использоуются такие же параметры, как при включении опции **Инициализировать устройство при добавлении** в разделе **Конфигурация → Типы устройств**.

6. Если при выпуске устройства было создано СКЗИ, то автоматически выставятся **Номер и дата документа**, на основании которого происходит уничтожение/изъятие СКЗИ в процессе изъятия.
7. 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.

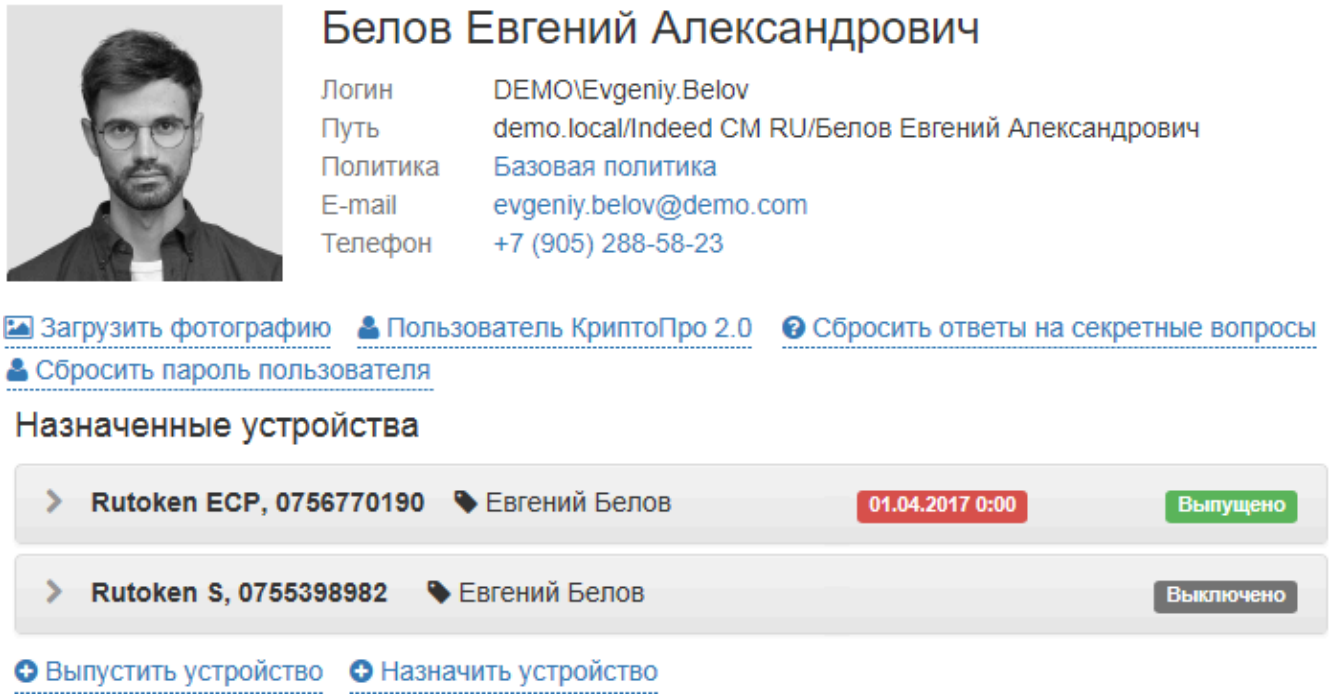
Временная замена

Новое устройство будет выдано на определенный срок. Например, сотрудник забыл свою смарт-карту дома. Для работы в офисе оператор выпускает ему новое устройство с заданным сроком действия.

В этом случае действие сертификатов на забытой карте сотрудника приостанавливается. Действительные сертификаты и ключи будут записаны на новое устройство.

В карточке пользователя отображаются два устройства:

- Основное устройство Rutoken S выключено. Действие всех сертификатов на устройстве приостановлено.
- Устройство-дубликат Rutoken ECP выпущено с ограниченным сроком действия.



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.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> При замене устройства PIN-код устройства не переносится на новое устройство. На устройство-дубликат PIN-код установится в соответствии с настройками политики использования устройств:
>
> - Установленный производителем по умолчанию
> - Заданный администратором в параметрах инициализации устройства
> - Случайный
>
> Пользователь может изменить PIN-код устройства в Сервисе самообслуживания, если определены соответствующие настройки в политике использования устройств.

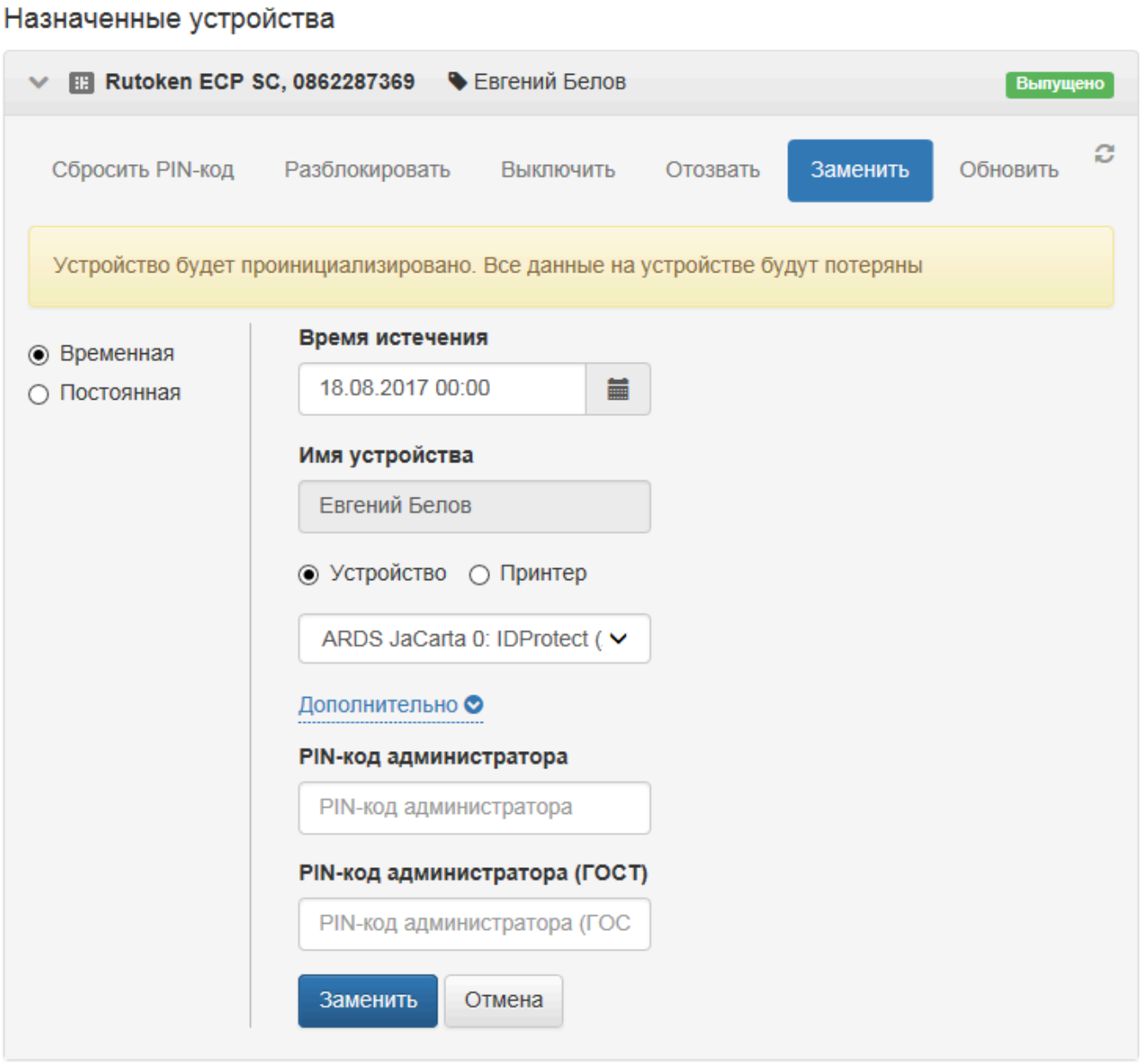
Для замены устройства пользователя выполните следующие действия:

1. Перейдите на вкладку **Пользователи** и выполните поиск пользователя.
2. Нажмите на логин и перейдите в карточку пользователя.
3. Выберите нужное устройство и раскройте информацию о нем.
4. Нажмите **Заменить**.
5. Укажите тип замены:

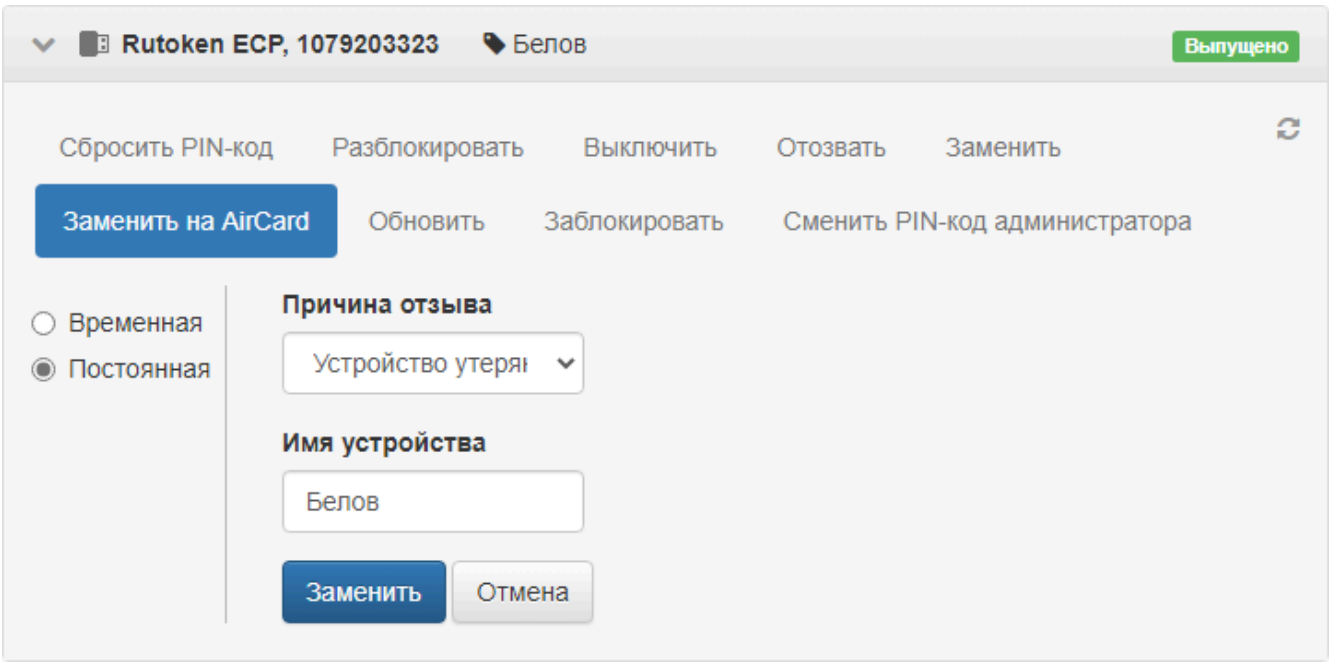
- **Временная**. Укажите срок окончания действия временного устройства.
- **Постоянная**. Укажите причину.

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. Нажмите **Заменить** для замены устройства или **Отмена** для возврата к карточке пользователя.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Если определены соответствующие настройки в политике использования устройств, то в процессе замены новое устройство будет инициализировано. Все данные, хранящиеся на устройстве будут удалены.



Если Indeed Certificate Manager интегрирован с Indeed AirCard Enterprise, то аппаратное устройство можно заменить на сетевую смарт-карту AirCard. Для замены устройства на AirCard нажмите **Заменить на AirCard** в панели доступных действий с устройством.


Rutoken ECP, 1079203323
Белов
Выпущено
Сбросить PIN-код
Разблокировать
Выключить
Отозвать
Заменить
Заменить на AirCard
Обновить
Заблокировать
Сменить PIN-код администратора
Временная
Постоянная
Причина отзыва
Устройство утеря
Имя устройства
Белов
Заменить
Отмена

Обновление устройства

Устройство необходимо обновить в следующих случаях:

- срок действия одного или нескольких сертификатов истек или истекает;
- администратор Indeed CM назначил пользователю новую политику;
- на устройство добавлены сертификаты вне Indeed CM;
- в политике использования устройств:
  - изменилось количество шаблонов сертификатов;
  - изменены отслеживаемые атрибуты пользователя в шаблонах сертификатов;
  - добавлены или удалены общие сертификаты;
  - настроен хотя бы один необязательный сертификат (для записи сертификата на устройство или удаления с устройства);
  - включена или отключена интеграция с Indeed Access Manager;
  - включена или отключена интеграция с Secret Net Studio.

> **ПРИМЕЧАНИЕ**
>
> Если вы назначили пользователю новую политику, то при обновлении устройства произойдет следующее:
>
> 1. С устройства удалятся сертификаты, которые есть в текущей политике, но отсутствуют в новой.
> 2. На устройство запишутся сертификаты, которые есть в новой политике, но отсутствуют в текущей.
> 3. Сертификаты, которые есть в обеих политиках, останутся без изменений.

Процедура обновления

Для обновления устройства выполните следующие действия:

1. Перейдите на вкладку **Пользователи** Консоли управления и выполните поиск пользователя.
2. Нажмите на логин и перейдите в карточку пользователя.
3. Выберите нужное устройство и нажмите **Обновить**.

ПОДСКАЗКА

Если у вас нет доступа к устройству пользователя, задайте опцию **Обновить устройство на агенте**. Клиентский агент, установленный на рабочей станции пользователя, выполнит задачу по обновлению.
Как создать задачу по обновлению на агенте Indeed CM

4. Подключите устройство к компьютеру.
5. Выберите шаблоны, по которым будут сформированы сертификаты для записи на устройство. Обязательные сертификаты запишутся на устройство автоматически.
6. Если в политике использования устройств настроена **Интеграция со СМЭВ** и сертификат выпускается по шаблону для КриптоПро УЦ 2.0 или Валидата УЦ, отобразится форма проверки СМЭВ.
   Проверьте данные пользователя.
7. Введите **PIN-код пользователя**.
8. Если на устройство были добавлены сторонние сертификаты, Indeed CM может их обнаружить и внести информацию о таких сертификатах в систему – отследить.
   Окно выбора сертификатов для отслеживания отображается, если в разделе **Поведение** политики использования устройств задана опция **Включить отслеживание сертификатов**.
   Выберите сертификаты для отслеживания, если они есть на устройстве, и нажмите **Ок**.
9. Нажмите **Обновить**.
10. По завершении обновления устройства нажмите **Закрыть**.

Контроль обновления

Обновление устройства можно приостановить, если регламент вашей организации предусматривает проверку запроса на обновление сертификата в УЦ.

Чтобы настроить проверку запроса на обновление сертификата в УЦ, перейдите в настройки шаблонов сертификатов используемых УЦ и отключите опцию **Автоматически одобрять подписанный запрос на обновление сертификата**.

В окне обновления устройства появится сообщение *Обновление устройства ожидает решения*. Устройству присваивается статус **В ожидании**. Это означает, что запрос на обновление перешел в стадию рассмотрения.

Если запрос на обновление сертификата одобрен в УЦ, то сертификат получает статус **Одобрен** и записывается на устройство. Нажмите **Продолжить обновление устройства** в карточке устройства.

Если запрос отклонен в УЦ:

- отзовите и очистите устройство, после чего выпустите устройство заново;
- отмените обновление устройства и обновите устройство заново.

Если в политике настроена автоматическая рассылка уведомлений по электронной почте, то вам придет уведомление о статусе одобрения – *Одобрение обновления устройства* или *Отклонение обновления устройства*. Если автоматическая рассылка уведомлений не настроена, дождитесь появления кнопки **Продолжить обновление устройства** в карточке устройства.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Настройки УЦ могут ограничивать автоматическое обновление сертификатов – обновлять только действующие сертификаты. В этом случае опция **Автоматически одобрять подписанный запрос на обновление сертификата** в Indeed CM не регулирует автоматическое обновление сертификатов.

Отмена обновления

Вы можете отменить обновление устройства на агенте, если в разделе **Поведение** политики использования устройств задана опция **Разрешить отмену обновления устройства**.

Чтобы отменить обновление устройства:

1. Нажмите **Отменить обновление** в карточке устройства.
2. Введите **PIN-код пользователя**.
3. Подключите устройство и нажмите **Отменить обновление**.

> 💡 **ПОДСКАЗКА**
>
> Если у вас нет доступа к устройству, задайте опцию **Отменить обновление на агенте**. Клиентский агент, установленный на рабочей станции пользователя, отменит задачу по обновлению.

Выпуск устройства с печатью

Если в политике использования устройств включена опция **Включить печать устройства**, то выпуск устройств в форм факторе смарт-карты в Indeed CM можно объединить с печатью изображения или текста на них.

В этом случае смарт-карта помещается в лоток подачи карт принтера, и в процессе выпуска на нее записываются сертификаты и наносится изображение в соответствии с заданным шаблоном печати.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Для печати на устройствах на рабочей станции должны быть установлены следующие компоненты:
>
> - Драйвера принтера EDISecure XID8300
> - Настроенное соединение с принтером в утилите EDI Secure Connect
> - Компонент поддержки принтера **IndeedCM.EdiSecure.Middleware**
> - Подключенный через интерфейс USB принтера XID8300
>
> Драйвера принтера EDISecure XID8300 и утилита EDI Secure Connect поставляются 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. Нажмите на логин и перейдите в карточку пользователя.
3. Нажмите **Выпустить устройство**.
4. Укажите **Имя устройства**. Имя устройства может быть подставлено автоматически (См. **Настройки выпуска устройства**).
5. Если политика использования устройств позволяет выбрать сертификаты, выберите нужные и нажмите **Далее**.
6. Укажите способ выпуска устройства **Принтер**. Имя подключенного принтера подставится автоматически.

7. Поместите карту в лоток подачи принтера.

8. Нажмите **Выпустить**.

Indeed CM позволяет наносить изображение на ранее выпущенные карты без использования принтера. 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. Нажмите на логин и перейдите в карточку пользователя.
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.

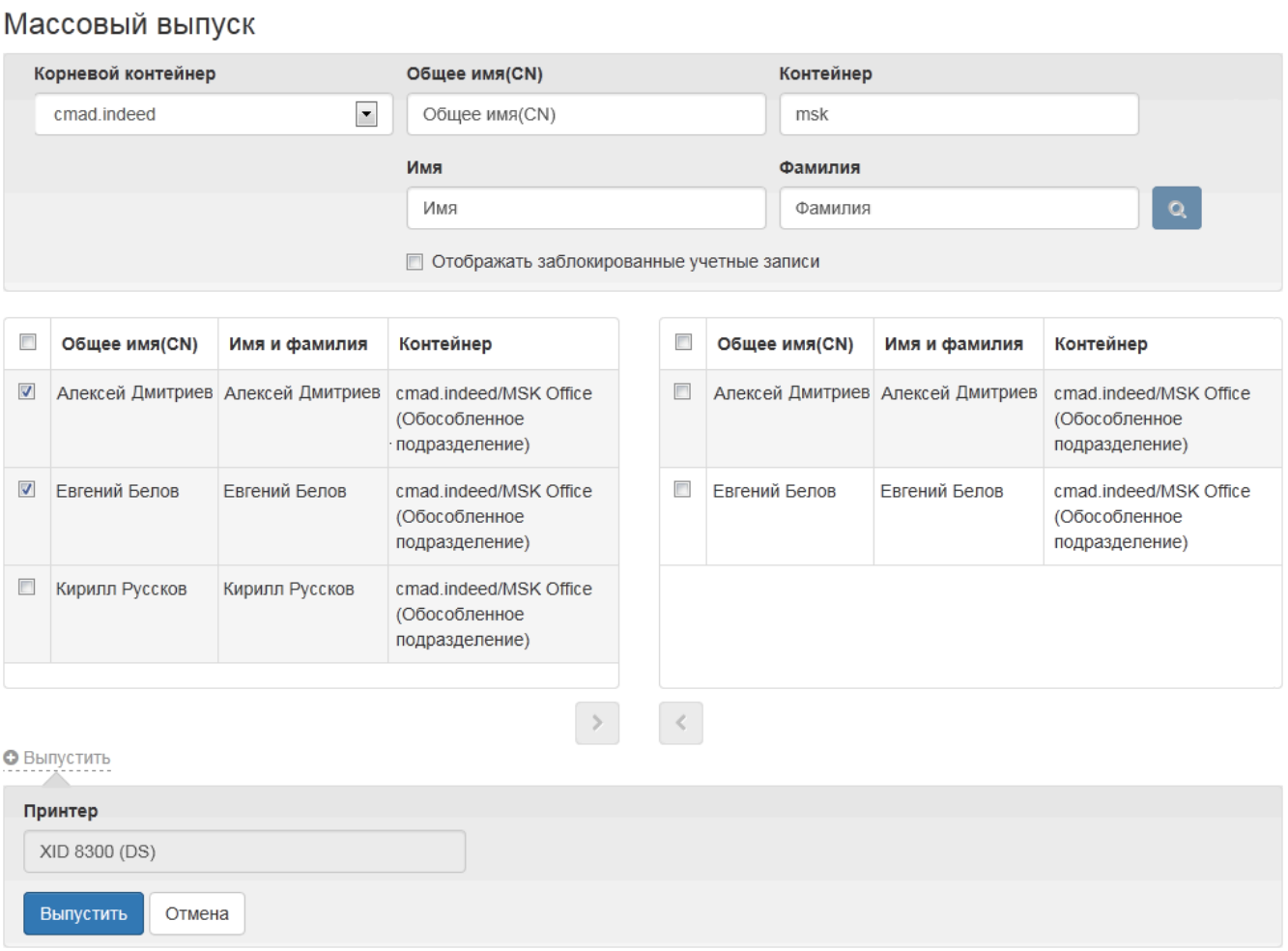
Режим массового выпуска имеет следующие особенности и ограничения:

- Отсутствует возможность выбора необязательных сертификатов. Будут выпущены только обязательные. Необязательные сертификаты можно выпустить для каждого пользователя отдельно через карточку пользователя или Сервис самообслуживания.
- Отсутствует возможность указания имя 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.

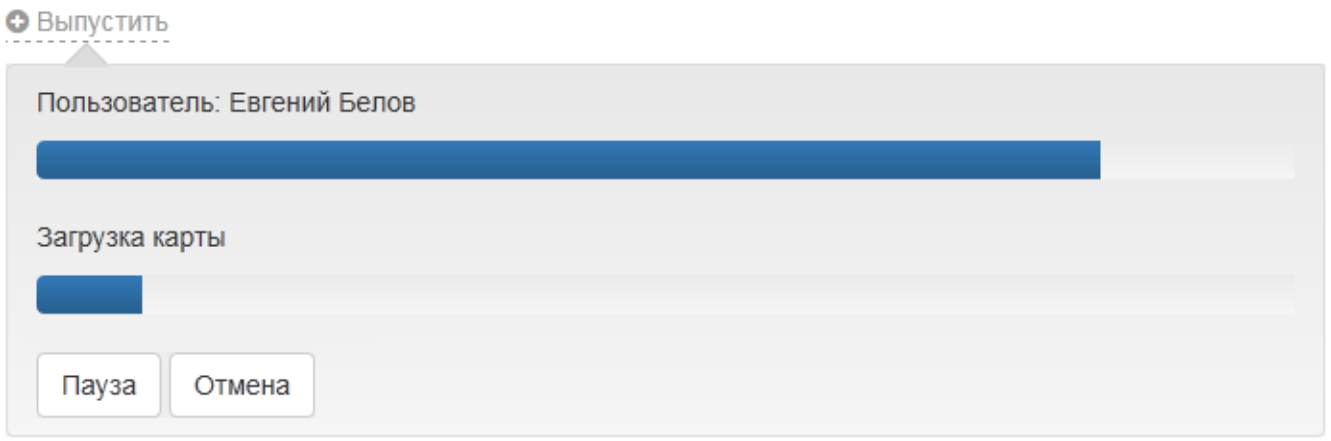
> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Для печати на устройствах на рабочей станции должны быть установлены следующие компоненты:
>
> - Драйвера принтера EDISecure XID8300
> - Настроенное соединение с принтером в утилите EDI Secure Connect
> - Компонент поддержки принтера **IndeedCM.EdiSecure.Middleware**
> - Подключенный через интерфейс USB принтера XID8300
>
> Драйвера принтера EDISecure XID8300 и утилита EDI Secure Connect поставляются производителем вместе с принтером. **IndeedCM.EdiSecure.Middleware** поставляется в составе дистрибутива Indeed CM.

Для массового выпуска устройств выполните следующие действия:

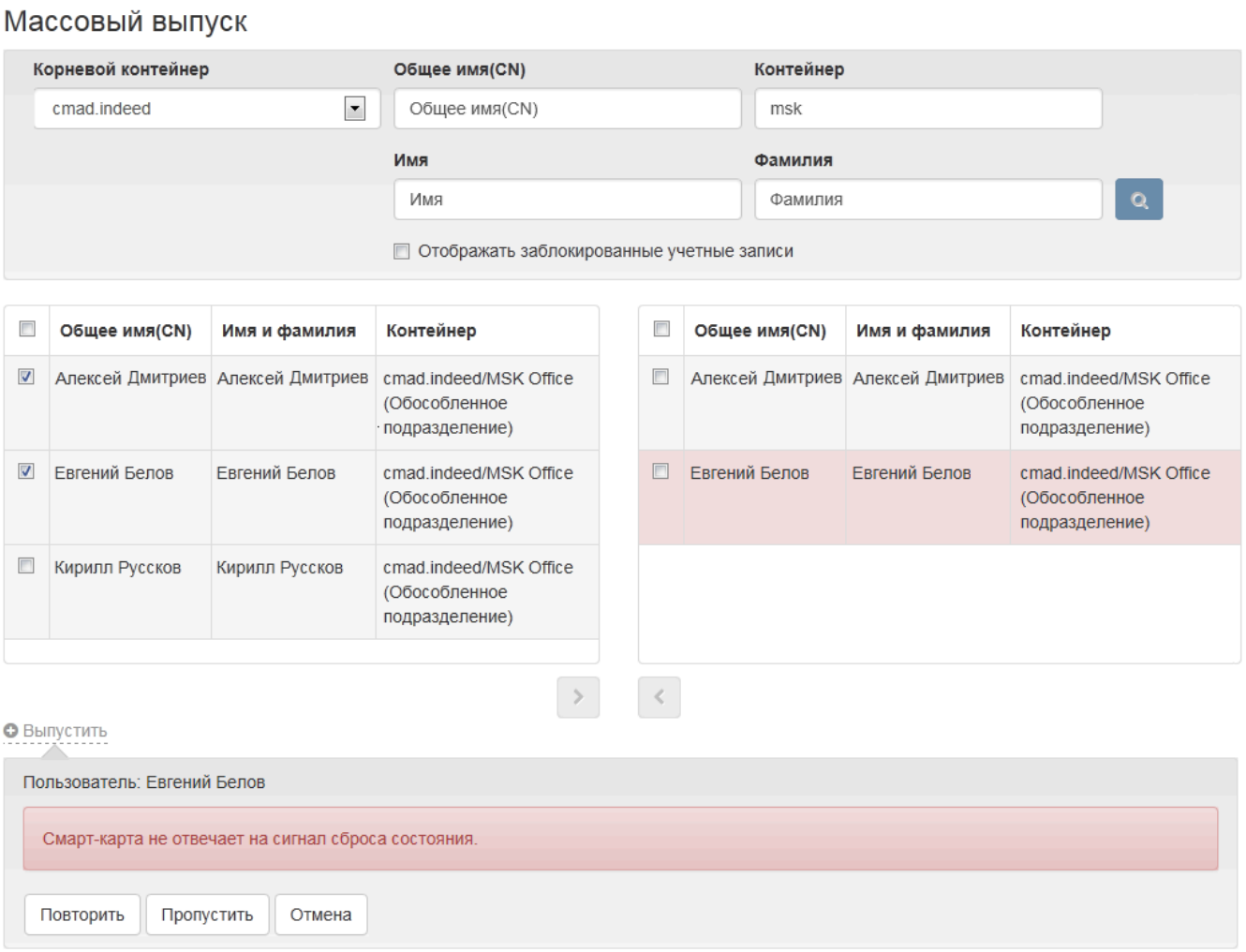
1. Перейдите на страницу сервиса *https://<FQDN сервера Indeed CM>/cm/mc/bulkissue*
2. Выполните поиск пользователей (например, по месту расположения). Результат поиска отобразится в таблице слева.
3. Отметьте среди найденных пользователей всех, кому необходимо выпустить смарт-карты и нажмите  .
4. Нажмите **Выпустить**. Имя будет подставлено автоматически.
5. Нажмите **Выпустить**.



Прогресс выпуска карты для каждого пользователя отображается в нижней части экрана. Выпуск карты можно приостановить или отменить.



Если при массовом выпуске возникла ошибка, пользователь, на котором произошла ошибка, выделяется красным, а в нижней части экрана отображается текст ошибки.



После устранения ошибки выпуск можно повторить. Для игнорирования ошибки и продолжения массового выпуска карт нажмите **Пропустить**. Для отмены массового выпуска для всех пользователей нажмите **Отмена**.

Назначенные СКЗИ

Назначенные СКЗИ отображаются в карточке пользователя и в Сервисе самообслуживания.

ПОДСКАЗКА

Чтобы настроить управление СКЗИ из карточки пользователя, выполните следующие действия:

1. Откройте Мастер настройки Indeed CM и перейдите в раздел **Функции системы → Журнал учета СКЗИ**.
2. Включите опцию **Вести журнал учета СКЗИ**.
3. Откройте Консоль управления Indeed CM и перейдите в раздел **Конфигурация → Роли**.
4. Задайте членам роли привилегии на действия с СКЗИ.

Чтобы разрешить пользователю просмотр и печать нормативных документов назначенных ему СКЗИ, включите опцию **Разрешить пользователю просмотр СКЗИ** в разделе **Поведение** политики использования устройств.

Добавление

СКЗИ можно назначить автоматически при его добавлении в карточке пользователя Indeed CM.

Чтобы создать новое СКЗИ и закрепить его за пользователем, нажмите **Добавить СКЗИ**,задайте значения параметров и нажмите **Добавить**.

Обязательные поля:

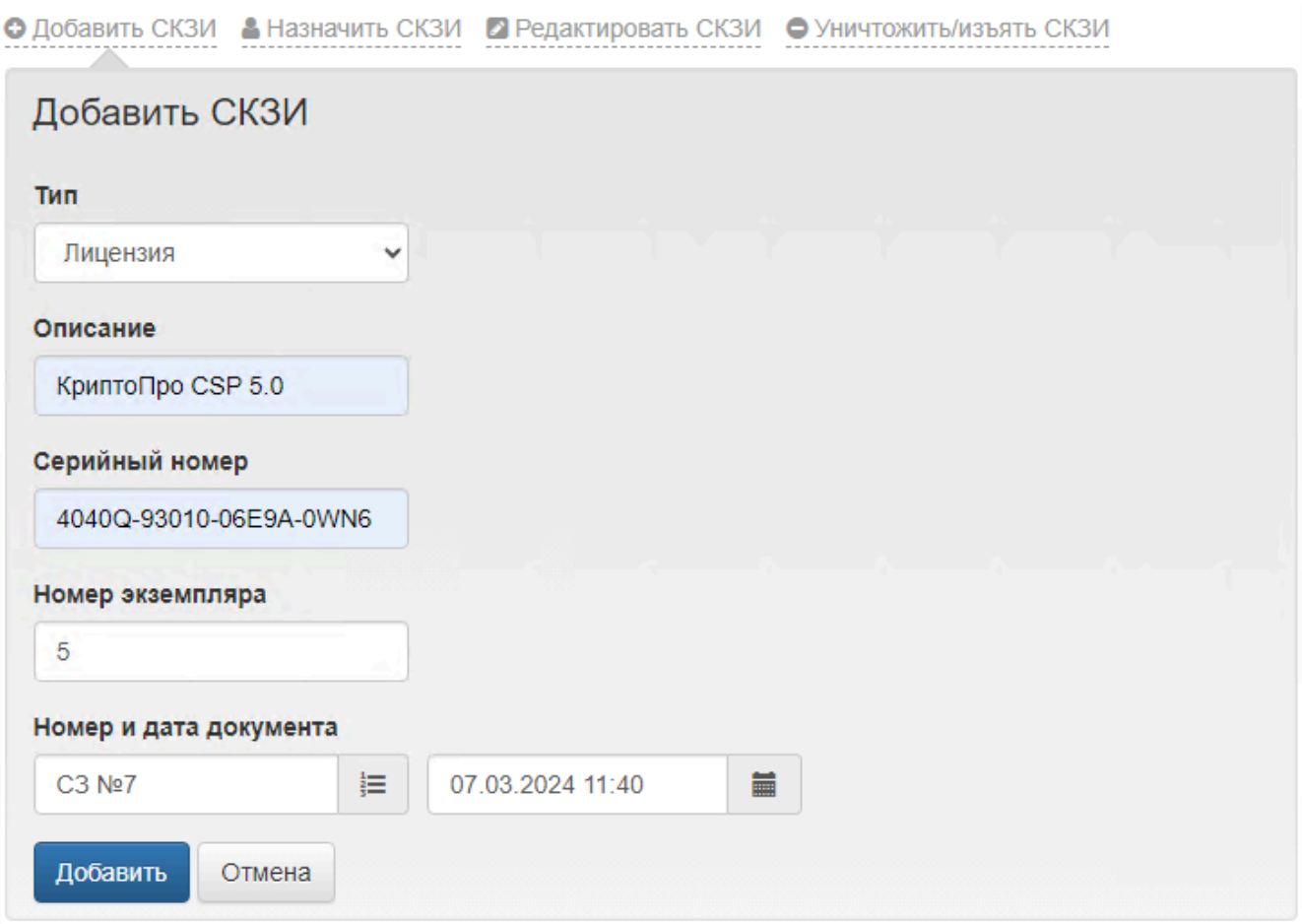
- **Тип** (дистрибутив, лицензия, документация, ключевой документ, ключевой носитель, пользовательский)
- **Описание**
- **Серийный номер**
- **Номер и дата документа**

ПОДСКАЗКА

Номер документа, на основании которого добавляется СКЗИ, можно указать вручную или выставить автоматически.

Нажмите , и номер документа выставится автоматически по шаблону нумерации, настроенному для документов этого типа СКЗИ в разделе **Нормативные документы**.

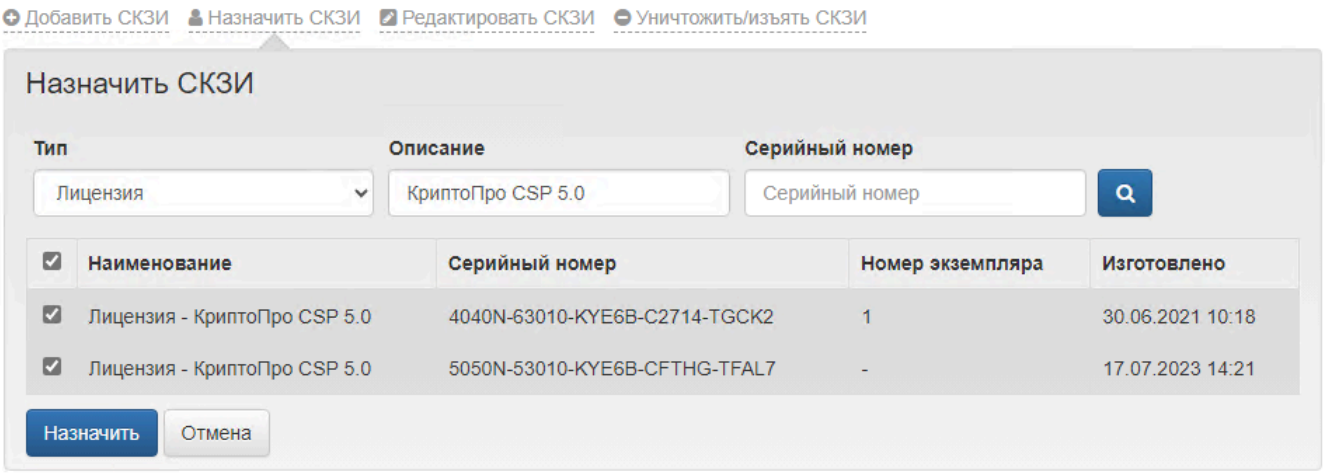
Необязательное поле: **Номер экземпляра**. Введите учетный номер экземпляра СКЗИ.



Назначение

Вы можете закрепить за пользователем СКЗИ, которые уже существуют в системе Indeed CM, не уничтожены/не изъяты и не назначены другому пользователю. Для этого:

1. Нажмите **Назначить СКЗИ** и задайте фильтры поиска: тип, описание, серийный номер.
2. Выберите одно или несколько СКЗИ.
3. Нажмите **Назначить.**



Редактирование

1. Выберите СКЗИ и нажмите **Редактировать СКЗИ**.
2. Внесите изменения и нажмите **Сохранить**.

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)

> **ПРИМЕЧАНИЕ**
>
> Перечень полей указан в соответствии с типовыми формами журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (для органа криптографической защиты информации и обладателя конфиденциальной информации), утвержденной Приказом ФАПСИ от 13 июня 2001 г. №152.

Уничтожение и изъятие

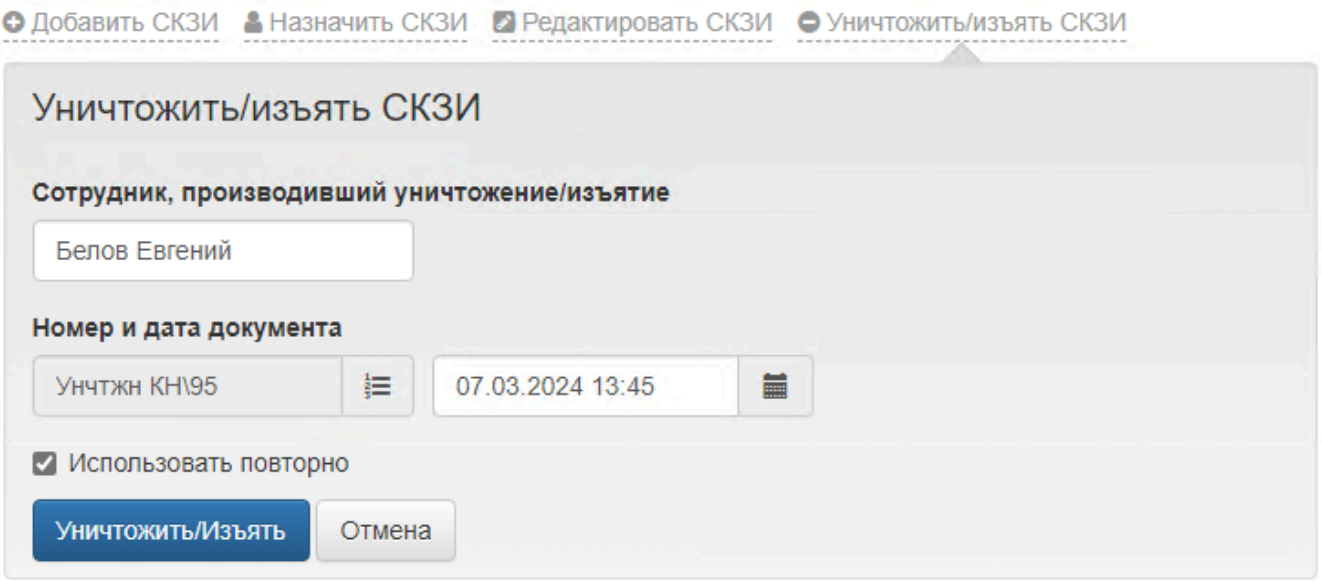
1. Выберите СКЗИ и нажмите **Уничтожить/изъять СКЗИ**.
2. Укажите имя сотрудника, который выполняет уничтожение/изъятие СКЗИ.

3. Укажите **Номер и дату документа**, на основании которого осуществляется уничтожение/изъятие.

> **ПОДСКАЗКА**
>
> Нажмите , и номер документа выставится автоматически по шаблону нумерации, настроенному для документов этого типа СКЗИ в разделе **Нормативные документы**.

4. Включите опцию **Использовать повторно**,если СКЗИ будет использоваться повторно (например, для другого сотрудника).

5. Нажмите **Уничтожить/Изъять**.



Печать

Документы СКЗИ можно распечатать по заранее настроенным шаблонам.

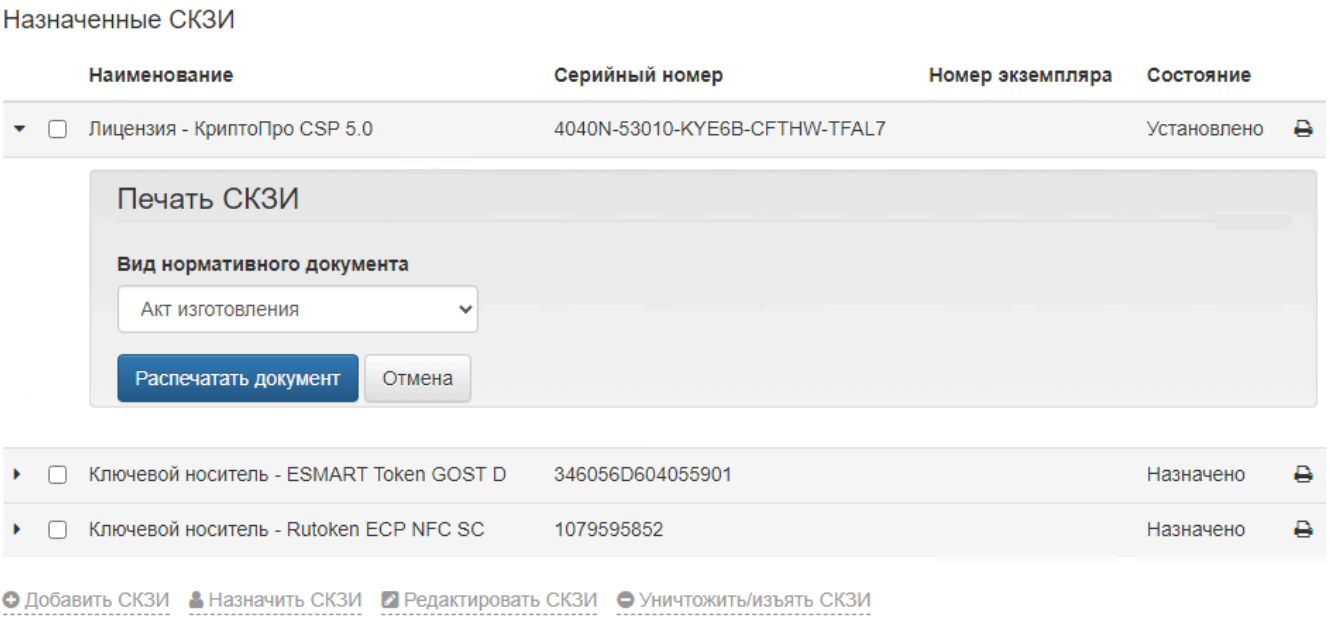
Чтобы распечатать документ СКЗИ:

1. Нажмите напротив выбранного СКЗИ.

2. Выберите вид нормативного документа или шаблон печати.

> **ПРИМЕЧАНИЕ**
>
> Выпадающий список **Вид нормативного документа** отображается, если вы определили шаблон печати для выбранного типа СКЗИ в текущем состоянии в разделе **Нормативные документы**.
>
> Выпадающий список **Шаблон печати** отображается, если вы не определили шаблон печати для выбранного типа СКЗИ в текущем состоянии. В этом случае вы можете выбрать любой из шаблонов, загруженных для этого типа СКЗИ в разделе **Шаблоны печати**.

3. Нажмите **Распечатать документ**.



Документы

Если в конфигурации настроена функция внутреннего электронного документооборота – **Indeed CM ЭДО**, пользователи и администраторы могут обмениваться документами для получения сертификата ключа проверки электронной подписи с помощью Indeed CM.

> **ПОДСКАЗКА**
>
> Если функция Indeed CM ЭДО не настроена, пользователь может отправить вам документы вне Indeed CM любым другим способом, принятым в вашей организации. Например, по электронной почте.

Вы можете управлять документами по получению сертификата в карточке пользователя в разделе **Документы**.

Пользователи могут добавить, подписать, скачать, редактировать и удалить документы в Сервисе самообслуживания в разделе **Ваши документы**.

> **ПРИМЕЧАНИЕ**
>
> Чтобы разрешить пользователю удалять документы в Сервисе самообслуживания, включите опцию **Разрешить пользователю удаление документа** в разделе **Поведение** политики использования устройств.

При добавлении документа пользователи могут подписать его электронной подписью, если:

- у пользователя есть устройство, которое содержит сертификат подписи;
- сертификат подписи имеет любой статус, кроме **Отозван**, **Истек**, **Ключ истек** и **Ошибка**;
- поле **Улучшенный ключ** сертификата содержит значения **Защита электронной почты** (Secure Email, OID 1.3.6.1.5.5.7.3.4) и **Подписание кода** (codeSigning, OID 1.3.6.1.5.5.7.3.3) согласно требованиям к электронной подписи (RFC 5280).

Подробнее о возможностях пользователя по работе с документами в Indeed CM

Контроль выпуска и обновления устройств

Indeed CM ЭДО позволяет дополнительно приостановить выпуск и обновление устройства пользователя. В этом случае документы пользователя проверяет не только удостоверяющий центр (УЦ), но и администратор или оператор Indeed CM.

Пользователь может продолжить выпуск или обновление устройства только после того, как предоставит на проверку администратору пакет необходимых документов – запрос на сертификат, форму сертификата или оба документа.

Устройству присваивается статус **В ожидании**. Это означает, что запрос пользователя на выпуск/обновление устройства перешел в стадию рассмотрения.

Чтобы управлять документами пользователей, назначьте администраторам или операторам Indeed CM нужные привилегии:

1. Перейдите в раздел **Конфигурация → Роли**.
2. Выберите роль и нажмите ✎.
3. Выберите привилегии в разделе **Документы** – добавление, изменение, удаление, одобрение.

Как настроить дополнительную проверку документов:

Запрос на сертификат

Вы можете проверить запрос на сертификат перед отправкой в УЦ, чтобы убедиться, что пользователь сформировал корректный запрос.

Чтобы настроить дополнительную проверку запроса на сертификат, перейдите в настройки шаблонов сертификатов используемых УЦ и отключите опцию:

- **Автоматически одобрять запрос на сертификат**, если пользователь выпускает устройство в первый раз;
- **Автоматически одобрять подписанный запрос на обновление сертификата**, если пользователь обновляет устройство.

Сертификат

После одобрения запроса в УЦ форма сертификата будет доступна пользователю в Сервисе самообслуживания. Пользователь может скачать и подписать форму сертификата и предоставить ее на проверку администратору/оператору.

Таким образом вы можете убедиться, что пользователь ознакомился с содержимым сертификата до записи сертификата на устройство.

Чтобы настроить дополнительную проверку формы сертификата, перейдите в настройки шаблонов сертификатов используемых УЦ и включите опцию **Требовать подписанный документ сертификата перед продолжением выпуска/обновления устройства**.

Запрос на сертификат и сертификат

Чтобы настроить дополнительную проверку запроса на сертификат и формы сертфиката:

1. Перейдите в настройки шаблонов сертификатов используемых УЦ.
2. Отключите опцию:
   - **Автоматически одобрять запрос на сертификат**, если пользователь выпускает устройство в первый раз;
   - **Автоматически одобрять подписанный запрос на обновление сертификата**, если пользователь обновляет устройство.
3. Включите опцию **Требовать подписанный документ сертификата перед продолжением выпуска/обновления устройства**.

Пользователь подпишет и загрузит документы в Сервисе самообслуживания. Документы будут автоматически доступны в карточке пользователя в Консоли управления, где администратор проверит документы и разрешит/отклонит выпуск или обновление устройства.

ПРИМЕЧАНИЕ

Если в политике использования устройств настроена автоматическая рассылка уведомлений по электронной почте, вы получите уведомление, когда пользователь загрузит документ. К уведомлению будет прикреплен документ в формате PDF.

Чтобы просмотреть и одобрить документ:

1. Перейдите на вкладку **Пользователи** Консоли управления и выполните поиск пользователя.
2. Нажмите на логин и перейдите в карточку пользователя. Загруженный документ появится в разделе **Документы**.
3. Скачайте  и проверьте документ.
4. Если документ прошел проверку, нажмите ?.
5. В окне одобрения документа необходимо установить связь между загруженным документом, шаблоном сертификата и устройством:

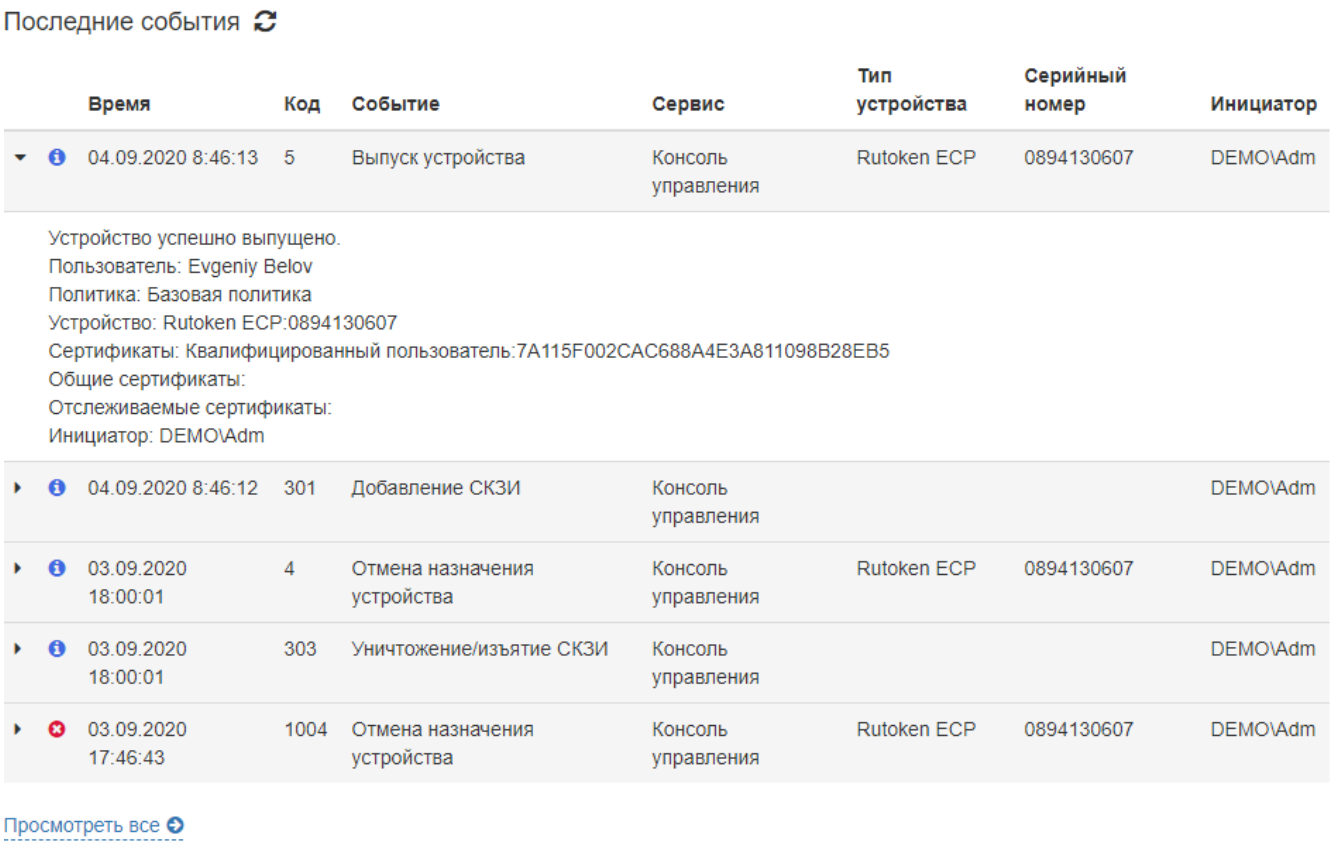
    1. В раскрывающемся списке **Сертификат** выберите шаблон сертификата, по которому выпускается сертификат.
    2. В раскрывающемся списке **Устройство** выберите устройство, на которое записывается сертификат.
    3. Нажмите **Одобрить**.

> **ПРИМЕЧАНИЕ**
>
> Вам не нужно одобрять документ, если пользователь предоставил документ через карточку устройства на вкладке **Содержимое**.

> **ПРЕДУПРЕЖДЕНИЕ**
>
> Если на устройство одновременно записываются несколько сертификатов, устройство можно выпустить, когда оба запроса на сертификат одобрены в УЦ.
> Если один из сертификатов был одобрен автоматически (статус **Действительный**), он будет записан на устройство вместе со вторым сертификатом.

События пользователя

В карточке пользователя отображается информация о пяти последних событиях в системе Indeed Certificate Manager для данного пользователя. Список событий можно обновить с помощью кнопки . 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

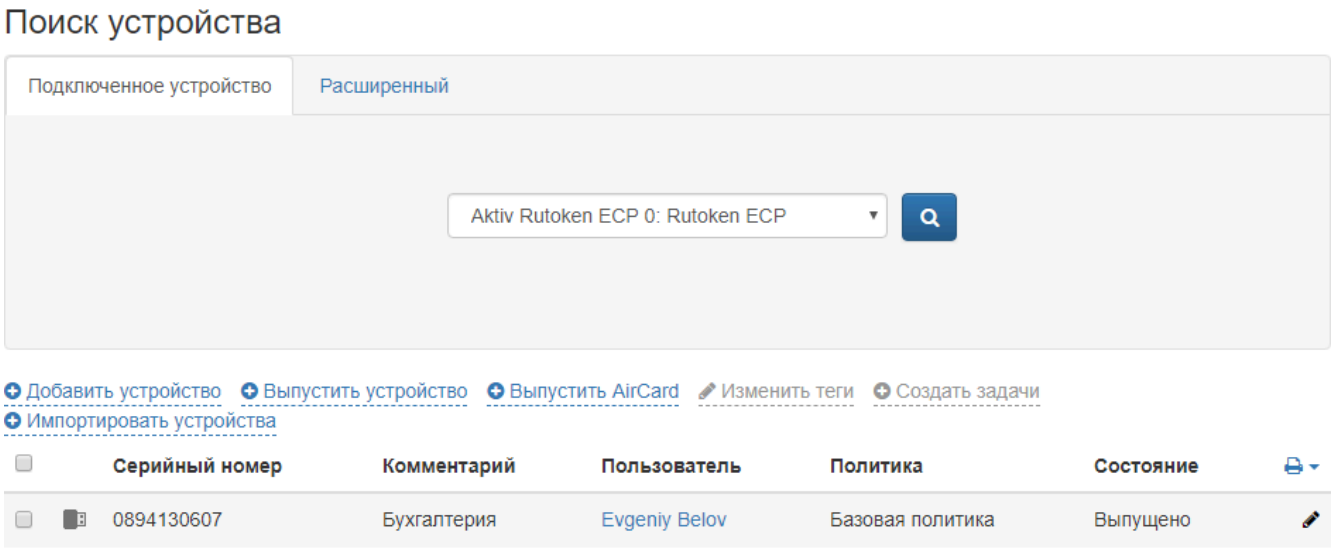
Для просмотра полного списка событий и перехода в раздел **Журнал** нажмите **Просмотреть все**.

Устройства

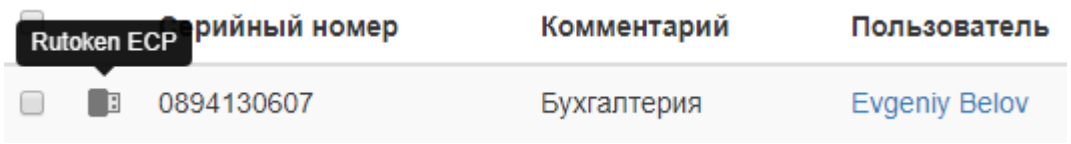
Подключенные устройства

Поиск по подключенному устройству применяется, 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  .



Чтобы просмотреть тип устройства, наведите указатель мыши на изображение устройства.



Расширенный поиск

Расширенный поиск применяется, 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 параметрам.

Чтобы выполнить поиск, укажите известные данные устройства и нажмите  .

ПОДСКАЗКА

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.

ПРИМЕЧАНИЕ

Для фильтрации устройств по статусу содержимого требуется настроенный по расписанию запуск службы Card Monitor в Мастере настройки Indeed CM.

Результаты поиска устройств можно сохранить в файл. Для создания файла нажмите и выберите формат (PDF или CSV). Сохраните полученный файл.

Для просмотра содержимого устройства нажмите . Для просмотра PIN-кода администратора нажмите .

Для изменения комментария или тегов нажмите в соответствующих полях.

ПРЕДУПРЕЖДЕНИЕ

Администраторы Indeed CM имеют доступ к PIN-кодам всех устройств, добавленных в систему. Администраторы отдельных политик имеют доступ к PIN-кодам устройств, назначенных/выпущенных пользователям этих политик.

Добавление

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 автоматически выставятся **Номер и дата документа** (приказа, распоряжения), в соответствии с которым будет изготовлено СКЗИ (Тип: Ключевой носитель). Информация об имеющихся в системе средствах криптографической защиты информации находится 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** и **Закрыть**.

Устройства можно добавлять автоматически, подключая их последовательно к одному и тому же считывателю.

> **ПРИМЕЧАНИЕ**
>
> При добавлении устройства PIN-код администратора заменяется на случайный или указанный в разделе **Типы устройств** конфигурации системы.

> **ПРЕДУПРЕЖДЕНИЕ**
>
> После добавления устройства с установкой случайного PIN-кода администратора вне Indeed CM будет невозможно разблокировать PIN-код пользователя и провести инициализацию отдельных видов устройств.

Выпуск

Выпуск устройств и виртуальных карт AirCard в разделе **Устройства** аналогичен выпуску из **Карточки пользователя**.

Удаление

Удалить устройство из Indeed Certificate Manager можно как при наличии устройства, так и без него.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> 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 ✖ .

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 устройство к компьютеру и нажмите **Удалить**.

Если устройство недоступно, нажмите **Удалить**.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> При включении опции **Инициализировать устройство** все содержимое (в том числе, сертификаты, записанные до ввода устройства в Indeed CM) будет удалено.

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.

> ⓘ **ПРИМЕЧАНИЕ**
>
> Операция **Инициализировать** доступна, если задана соответствующая привилегия в разделе **Роли**.

1. Выберите устройство и нажмите  для просмотра его содержимого.

2. Подключите устройство к рабочей станции и нажмите **Инициализировать**. Если устройство недоступно, создайте задачу на клиентском агенте - выберите опцию **Инициализировать устройство на агенте**.

- Если PIN-код администратора на устройстве совпадает с сохраненным в хранилище системы, нажмите **Инициализировать**. После инициализации PIN-код администратора на устройстве и в базе не изменится. PIN-код пользователя будет сброшен на значение, указанное в **Типе устройства**.

- 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.

> **ПРИМЕЧАНИЕ**
>
> Устройства Rutoken и eToken можно инициализировать 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.

> **ПОДСКАЗКА**
>
> Теги создает администратор на вкладке **Конфигурация** в разделе **Теги**.

Для добавления или удаления тегов перейдите в раздел **Устройства** на вкладку **Расширенный** поиск, выберите требуемые устройства и нажмите **Изменить теги**.

Укажите **Теги для добавления** или **Теги для удаления** и нажмите **Изменить**.

При успешном изменении тегов появится сообщение *Теги успешно изменены*.

Чтобы убедиться в изменении тегов, выберите устройство и нажмите ✎.

Для изменения уже назначенных тегов нажмите ✎ в поле **Теги**.

Пакетное добавление

Для пакетного добавления устройств на вкладке **Устройства** выполните следующие действия:

1. Нажмите **Импортировать устройства**.
2. Загрузите подготовленный **Файл устройств**.
3. Нажмите **Импортировать**.

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
```

Где:

- **Serial Number** - серийный номер устройства. Обязательный параметр.
- **Card Type** - тип устройства. Обязательный параметр. Укажите имя типа устройства в том виде, в котором он указан в разделе **Типы устройств**.
- **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: Тег1,Тег2.
- **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 находится в разделе **СКЗИ**.
- **Time Created** - время создания документа. Указывается в формате yyyyMMddHHmmss (UTC). Если значение не указано, то в качестве времени создания документа автоматически подставляется время импорта СКЗИ.

> **ПРИМЕЧАНИЕ**
>
> Если вместо поля **Serial Number** (Серийный номер) устройства прописано значение **default**, то значения оставшихся полей в строке 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.

> **ПРЕДУПРЕЖДЕНИЕ**
>
> Для импорта устройств JaCarta PKI (без ГОСТ области) необходимо выполнить разделение **JaCarta** по различным моделям и в файле импорта обязательно указать поле **Model**.

Пример файла устройств

```
default;Rutoken S;;UsbToken;87654321;;Московский офис;VPN,IT;;
0755398982
0756309531
default;Rutoken
ECP;;UsbToken;87654321;;Бухгалтерия;VPN;BH-169;20220412134200
0894130607
0894130536
default;Rutoken ECP SC;;;87654321;;;;BH-170;20220329111500
0862287268
0862287403
default;Rutoken 2151;;UsbToken;87654321;;;;BH-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;;;BH-172;
6082057494937678
4C54001522634C50
0B53001917347618;;JC305;SmartCard;;;;;BH-173;20220412145500
```

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 серийными номером: 01cec45d.
- 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.
- 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).

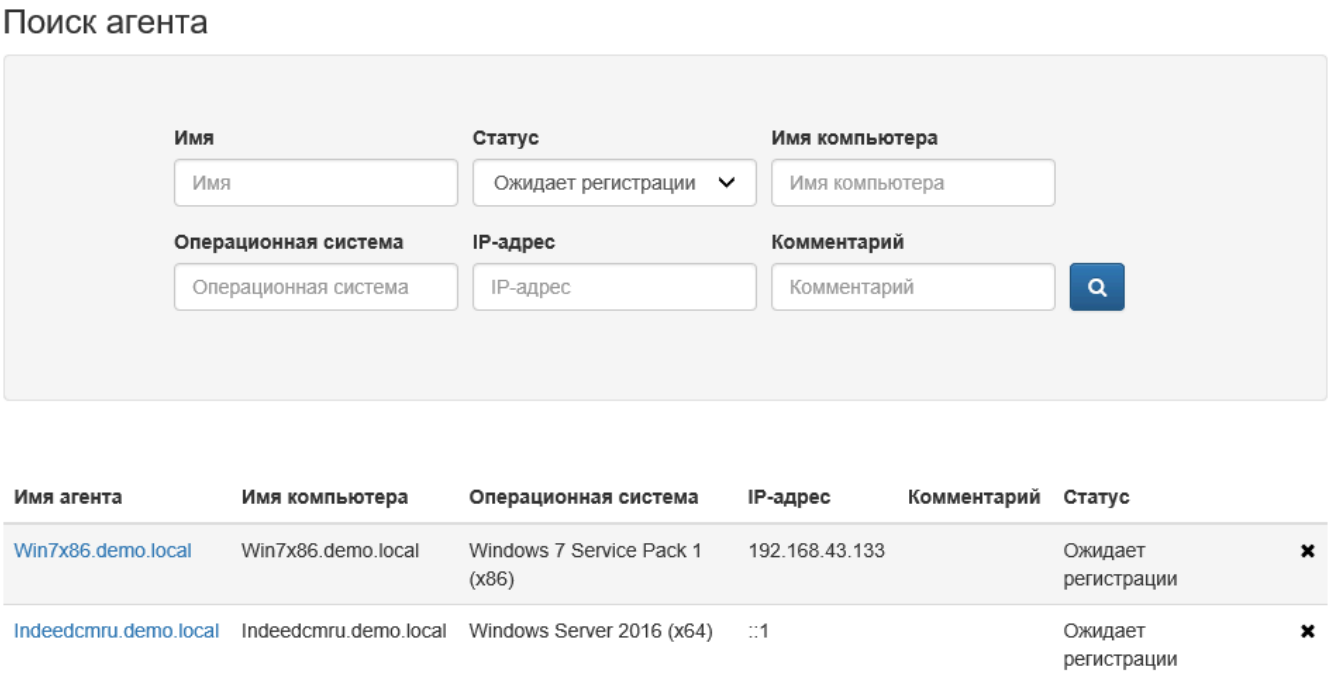
Агенты

ПОДСКАЗКА

Раздел доступен в Консоли управления на вкладке **Дополнительно**, если Indeed CM настроен для работы с клиентскими агентами (включена опция **Разрешить использование клиентских агентов** в разделе **Клиентский агент** Мастера настройки Indeed CM) и членам роли предоставлена привилегия **Просмотр репозитория агентов**.

ПРИМЕЧАНИЕ

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**.



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 учета статуса
  - Ожидает регистрации
  - Зарегистрирован
  - Отклонен

Поддерживаемые шаблоны поиска:

- Полное совпадение – **Win7x86.demo.local**
- Частичное совпадение –***86.demo.local** или ***demo***
- Все результаты – *****

Нажмите на имя Агента в результатах поиска, чтобы перейти в профиль Агента. Нажмите **Зарегистрировать** для подтверждения запроса на регистрацию или **Отклонить**, чтобы отклонить запрос.

В области уведомления Windows появится значок  .

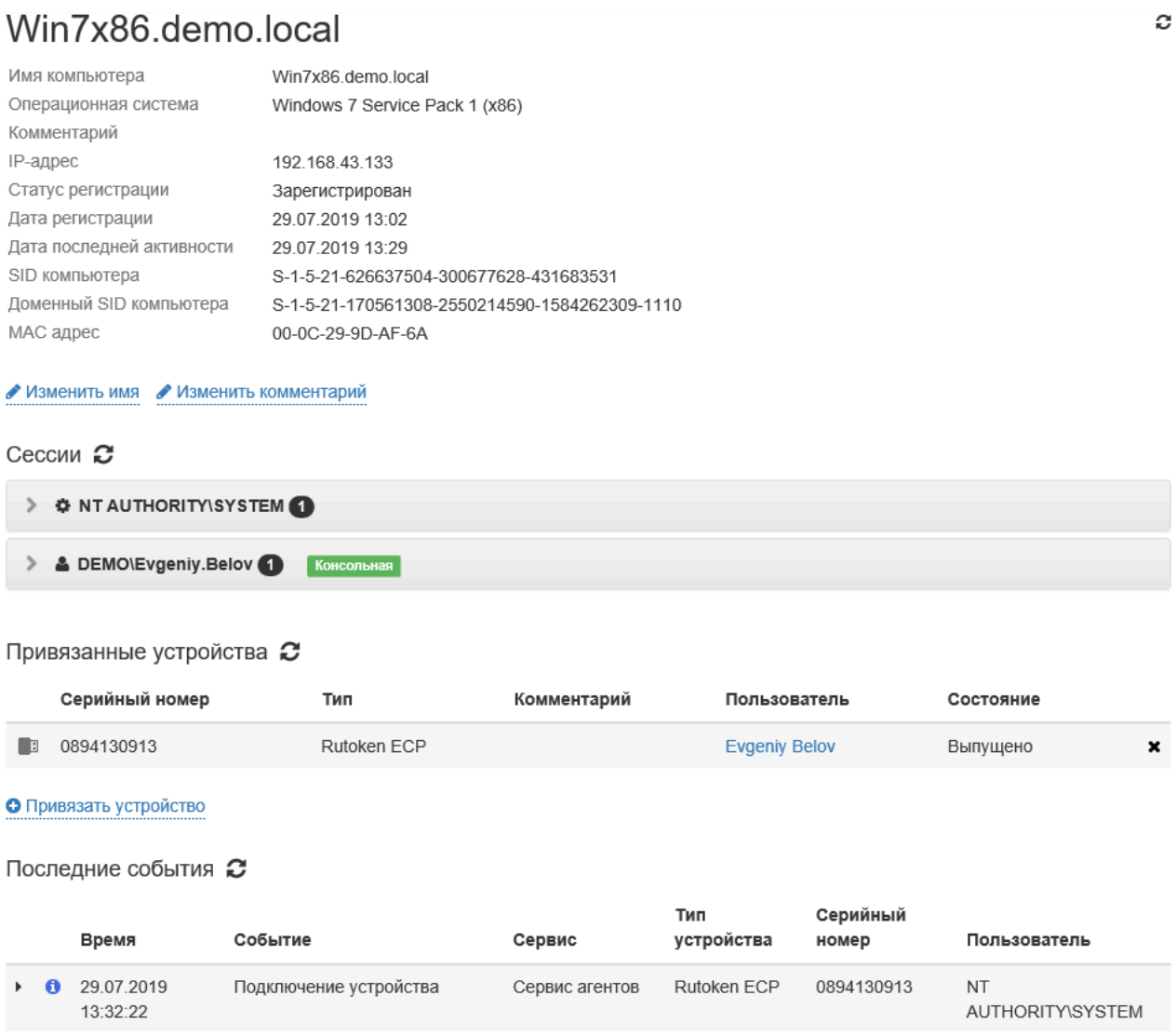
Профиль агента

В профиле содержится информация об Агенте, сессиях пользователей, привязанных устройствах и последних событиях, связанных с Агентом.

- **Имя Агента** – 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 (необязательно 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, которые администратор Indeed CM закрепил за Агентом.

- **Последние события** – последние пять событий, связанных с работой Агента.

Пример профиля Агента с сессиями и устройством пользователя



Назначение устройства

Агент Indeed CM автоматически определяет устройства, подключенные к рабочей станции, и запрашивает у сервера Indeed CM список 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**.
Если устройство недоступно, то укажите его серийный номер, тип и нажмите **Привязать**.

Устройство отобразится в разделе **Привязанные устройства** профиля Агента. Для отвязки устройства нажмите ✖ и затем **Отвязать**.

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, установленный на ней агент 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 агенту.
- **При нарушении условий привязки устройства и пользователя**. Например, пользователь выполнил вход на рабочую станцию по смарт-карте, привязанной к агенту, а затем сменил учетную запись в операционной системе.

> ⚠ **ДЛЯ ПОЛЬЗОВАТЕЛЕЙ СОСТАВНОГО КАТАЛОГА И КАТАЛОГА КРИПТОПРО УЦ 2.0**
>
> Привязка пользователя к Агенту не контролируется для пользователей составного каталога и каталога КриптоПро УЦ 2.0.

При обнаружении агентом одного из событий возможны следующие действия:

- Запись события в журнал системы
- 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 укажите **Таймаут до блокировки пользовательской сессии**, максимальное значение 5 секунд.

Чтобы агент отслеживал привязку сессии пользователя к подключенному устройству, включите опцию **Включить проверку привязки устройства к пользователю**. Если агенты и устройства будут использоваться на рабочих станциях, не входящих в домен вашей организации, то включите опцию **Проверять условия привязки устройства к пользователю на компьютерах, не включенных в домен**.

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 (Answer to reset) устройства
- {model} – вывод модели устройства
- {label} – вывод метки устройства

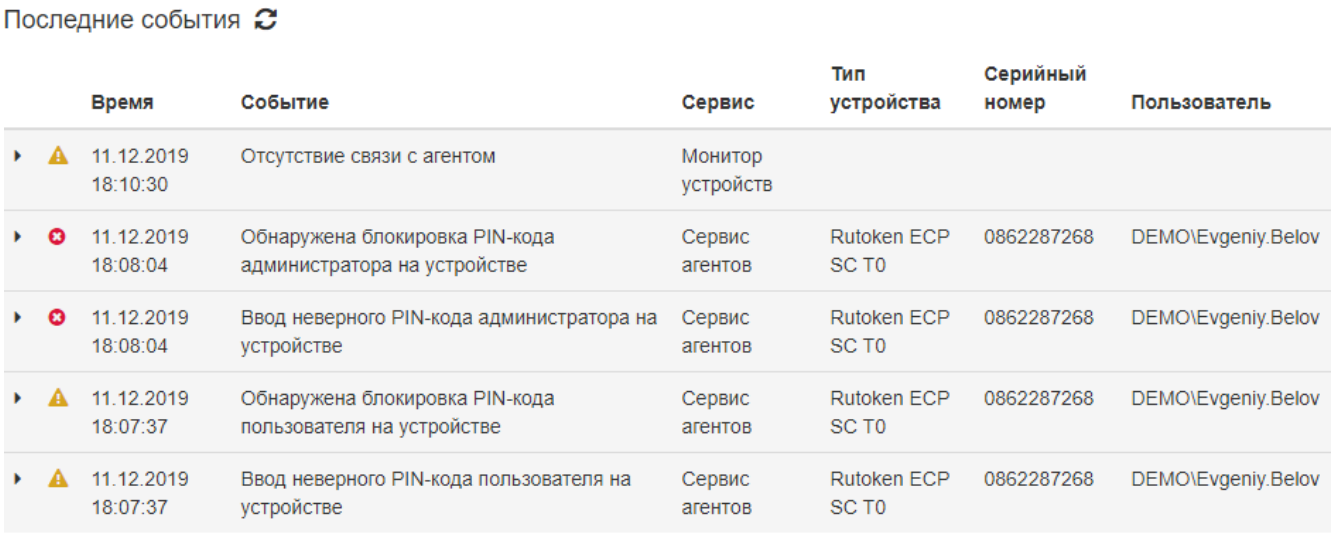
> **ПРИМЕР СООБЩЕНИЯ**
>
> "Подключенное устройство {model}: {sn} не соответствует сессии пользователя."

Мониторинг подключенных устройств

Клиентский агент проверяет все устройства, подключенные к рабочей станции пользователя, и фиксирует в системный **Журнал** следующие события:

- 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 служба Card Monitor фиксирует это событие в системный журнал. Период отсутствия связи агента с сервером задается в разделе **Служба Card Monitor** Мастера настройки Indeed CM.



Администратор Indeed CM может получать почтовые уведомления о следующих событиях на устройствах:

- 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.

Опция работает для устройств в состоянии *Выпущено*, *В ожидании*, *Отозвано*, *Выключено* и *Назначено*.

ПОДСКАЗКА

Создание уведомлений администратора и **Настройка шаблонов почтовых уведомлений** о данных событиях настраиваются в политике использования устройств.

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.

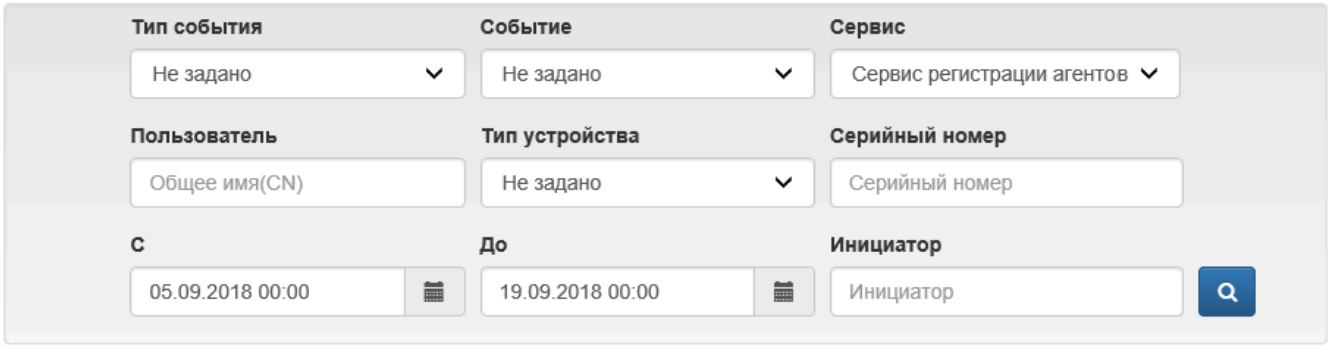
Производитель устройств	Список поддерживаемых событий
ISBC	Обнаружение блокировки PIN-кода пользователя/ администратора на устройстве.
Kaztoken	Обнаружение блокировки PIN-кода пользователя/ администратора на устройстве. Ввод неверного PIN-кода пользователя/администратора на устройстве.
Microsoft VSC (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

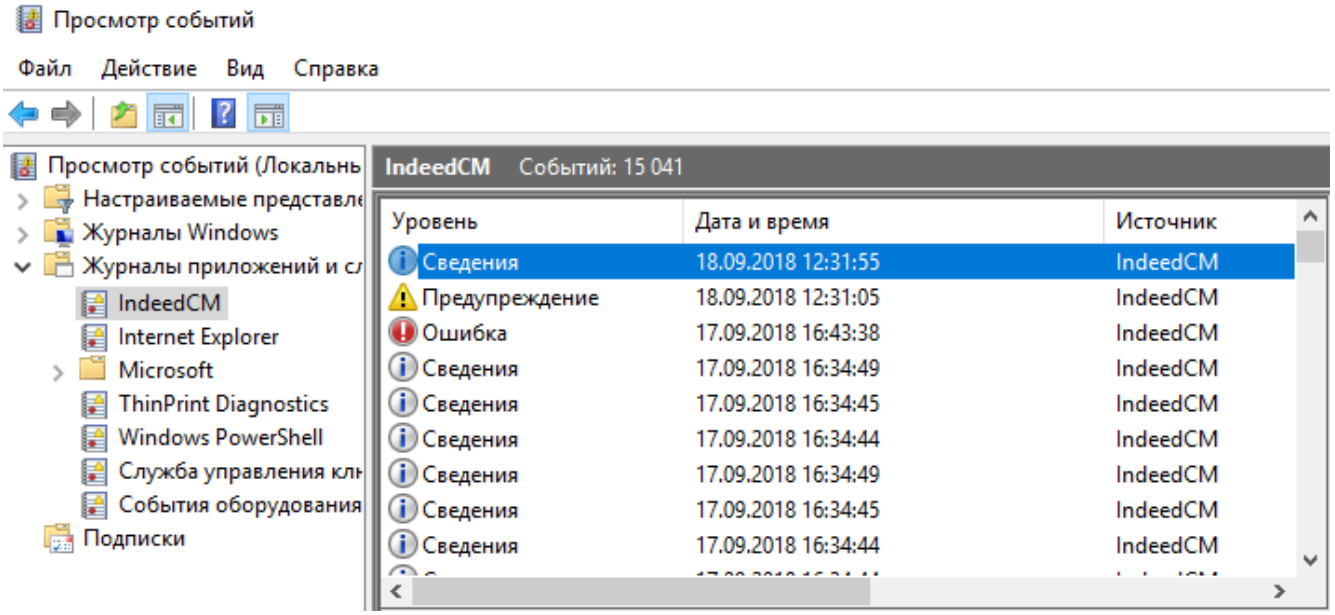
Сведения о работе Агентов Indeed Certificate Manager заносятся в журналы сервера и клиента. События Агентов фиксируют сервисы: **Сервис регистрации агентов**, **Сервис агентов** и **Монитор устройств**.

Для просмотра событий Агентов во вкладке **Журнал** Консоли управления Indeed CM отфильтруйте содержимое журнала по одному из сервисов или по событиям.

Журнал



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.



Назначение задач

Агенты позволяют управлять устройствами и их содержимым через задачи.

Если задача не требует действия от пользователя, то ее 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.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> 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 агент выволнит задачи, требующие действия от пользователя, 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 к рабочей станции ранее, то агент будет запрашивать список задач у сервера через заданный интервал времени. По умолчанию – каждые 30 секунд.

Задачи для агента назначаются в разделе **Устройства** или в карточке пользователя.

После назначения задача добавляется в раздел **Назначенные задачи** в карточке устройства и отображается до тех пор, пока не выполнится или не отменится.

В свойствах задачи отображаются **Тип**, **Комментарий**, **Дата создания**, **Статус**.

Статусы задачи

Ожидает выполнения – задача ожидает выполнения (включения рабочей станции с агентом, подключения устройства к рабочей станции или завершения выполнения предыдущей задачи).
Выполняется – агент 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 ее можно отменить. Для этого нажмите ✖ и подтвердите действие.

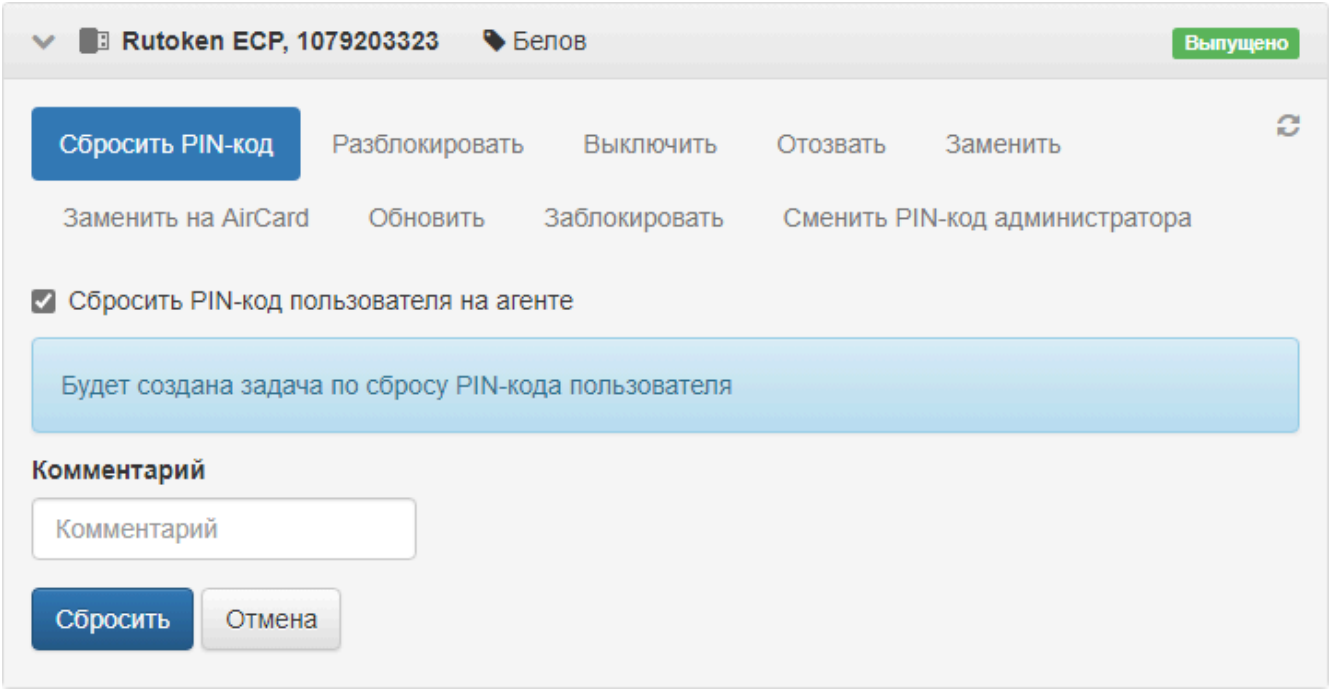
Агент Indeed CM может выполнить следующие задачи:

Сброс PIN-кода пользователя

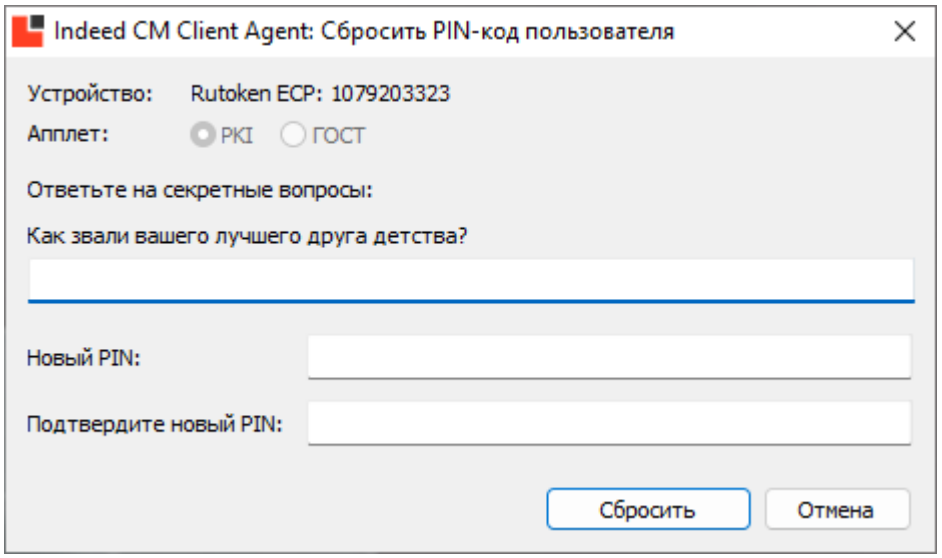
Если сбросить PIN-кода пользователя, устройство разблокируется.

Чтобы разблокировать устройство с помощью агента, нажмите **Сбросить PIN-код** в свойствах устройства и включите опцию **Сбросить PIN-код пользователя на агенте**. Укажите **Комментарий**, который отобразится в Журнале событий Indeed CM, и нажмите **Сбросить**.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> 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 Сервисе самообслуживания.



При выполнении задачи агент запустит на рабочей станции пользователя утилиту разблокировки. PIN-кода пользователя сбросится после того, как пользователь ответит на секретные вопросы, задаст новый PIN-код и нажмет **Сбросить**.



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.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Для разблокировки устройств с несколькими логическими областями (например, JaCarta PKI/ГОСТ) создайте две задачи для поочередного сброса PIN-кода каждой области.

Смена PIN-кода пользователя

Устройства Рутокен ЭЦП 3.0 и eToken 72K поддерживают аппаратное требование смены PIN-кода пользователя при первом подключении устройства к рабочей станции.

Требование о смене PIN-кода можно настроить в Консоли управления Indeed CM. Включите опцию **Пользователь должен поменять PIN-код при первом входе** в разделе **Конфигурация → Политики → Выпуск**.

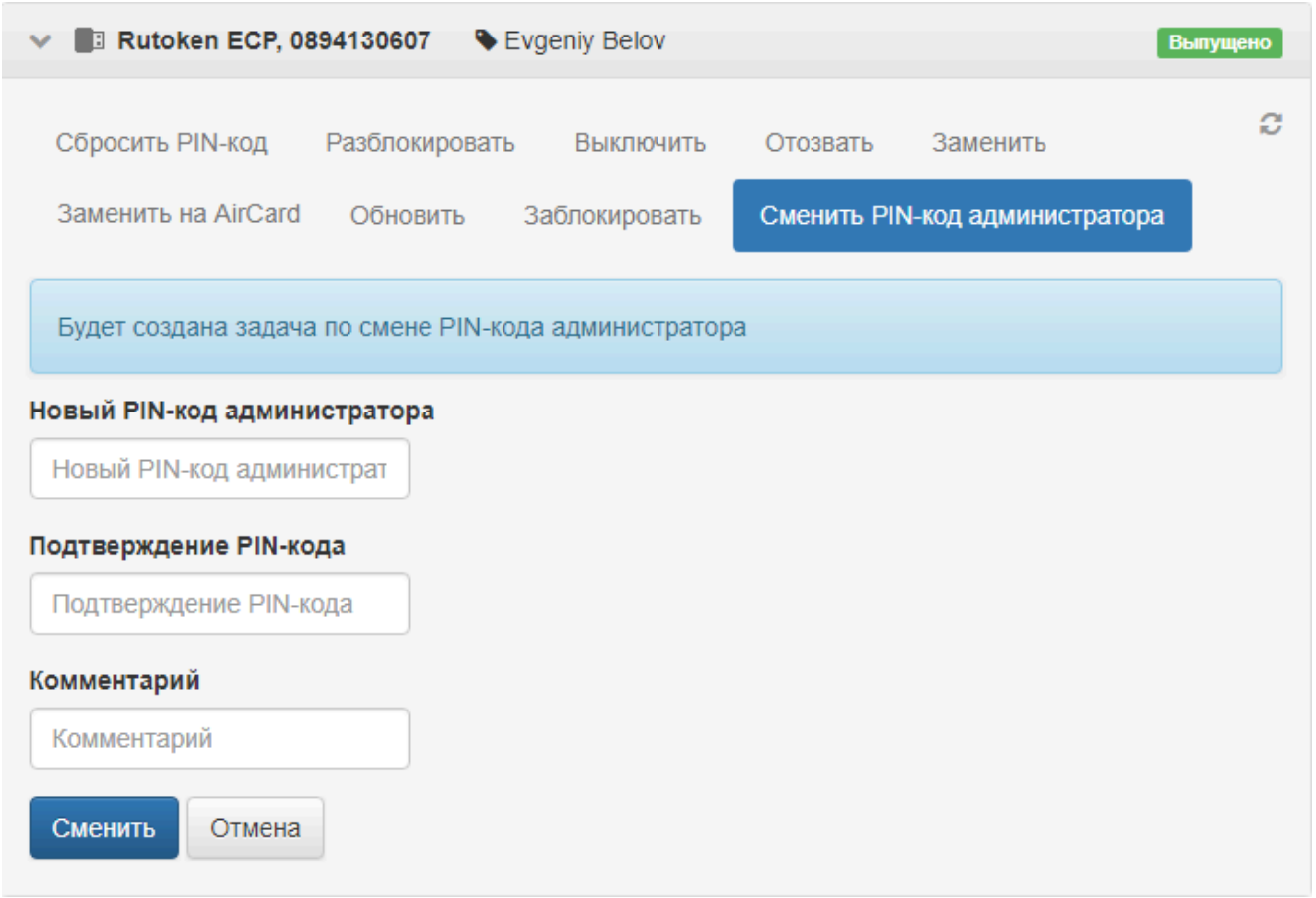
> ⓘ **ПРИМЕЧАНИЕ**
>
> Требование о смене PIN-кода можно настроить вне Indeed CM.

При подключении устройств Рутокен ЭЦП 3.0 и eToken 72K к рабочей станции клиентский агент Indeed CM создаст задачу **Смена PIN-кода пользователя**. Когда пользователь подключит устройство к рабочей станции, агент выполнит задачу. Откроется окно смены PIN-кода.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Задача создается только для устройств в состоянии **Выпущено**.

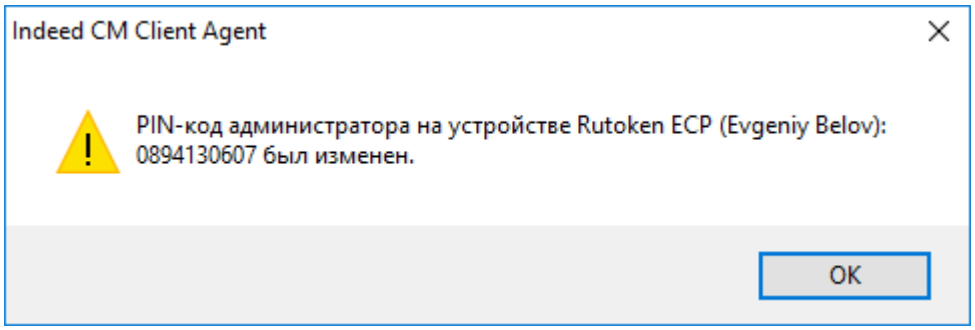
Смена PIN-кода администратора

Нажмите **Сменить PIN-код администратора** в свойствах устройства, задайте и подтвердите **Новый PIN-код администатора**. Укажите **Комментарий** при необходимости и нажмите **Сменить**.



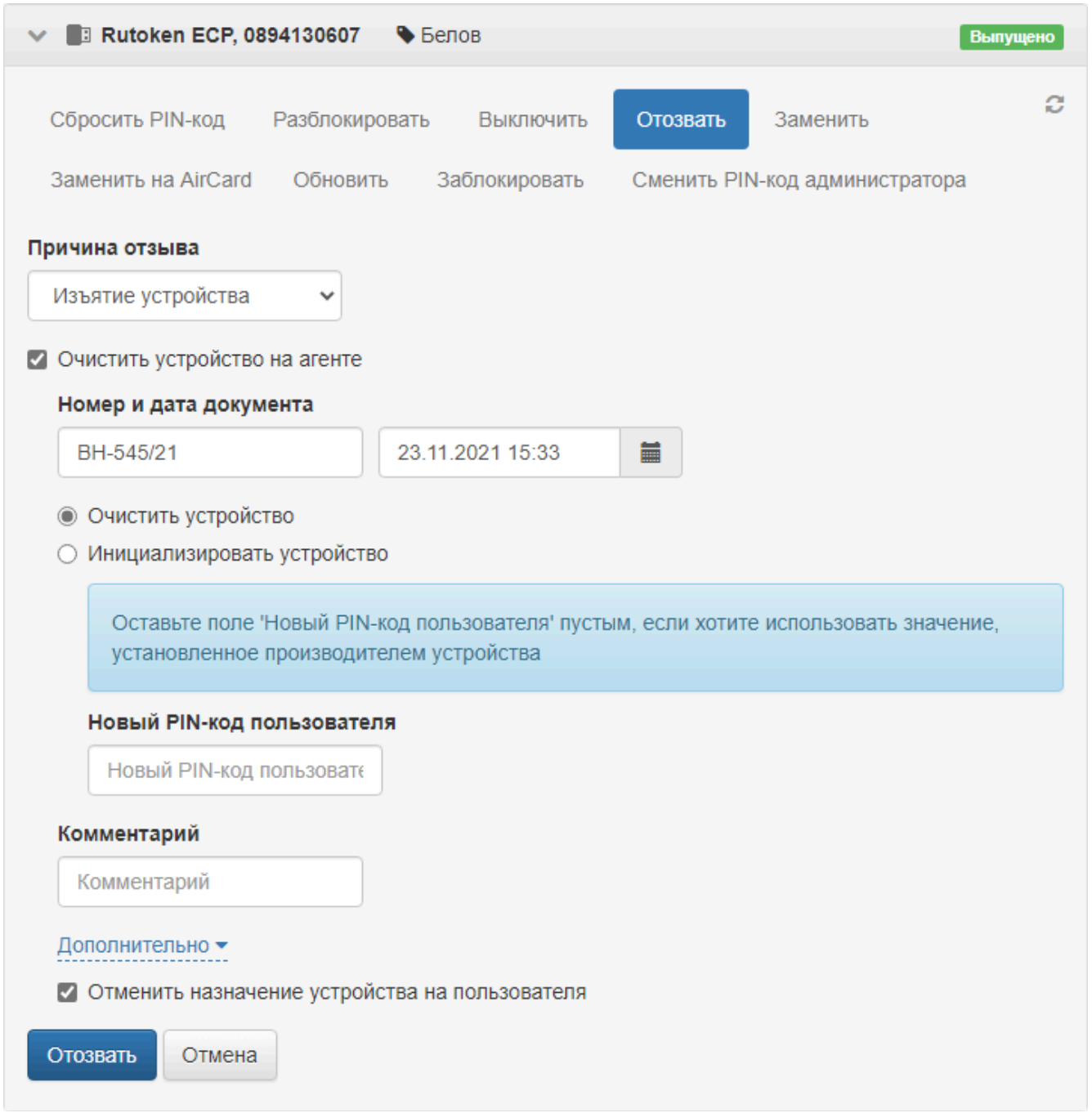
PIN-код администратора изменится автоматически при подключении устройства к рабочей станции с установленным агентом Indeed CM. Сведения о выполнении задачи с указанным комментарием запишутся в Журнал событий Indeed CM.

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 и инициализация устройства при его отзыве администратором

Нажмите **Отозвать** в карточке устройства, укажите **Причину отзыва** и включите опцию **Очистить устройство на агенте**.



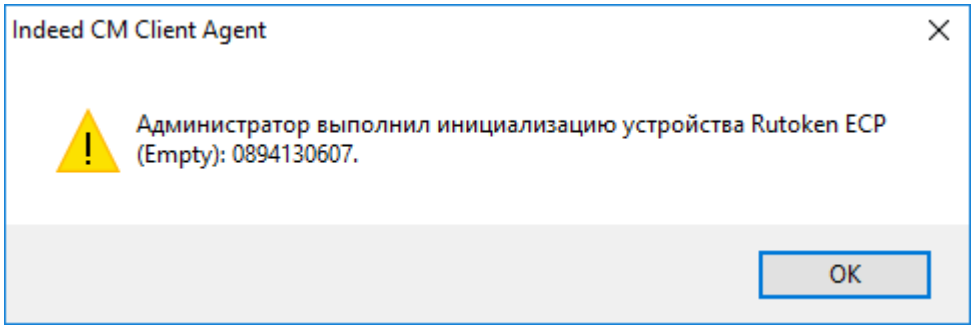
- Если при выпуске устройства было создано/назначено СКЗИ, то необходимо указать **Номер и дату документа**, на основании которого происходит уничтожение/изъятие СКЗИ .
- **Очистка устройства** предполагает удаление всех сертификатов, которые были записаны с помощью Indeed CM. Сертификаты и ключи, хранившиеся на устройстве до ввода в Indeed CM, не будут удалены.
- Укажите **Новый PIN-код пользователя**, который установится на устройстве после его изъятия. Если не задать PIN-код пользователя, то после изъятия устройства установится PIN-код, указанный в разделе **Типы устройств**.

> **ПРИМЕЧАНИЕ**
>
> PIN-код необходимо установить 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**).

- **Инициализация устройства** приведет к удалению всего содержимого, политики паролей (если она была на устройстве) и изменит имя 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.

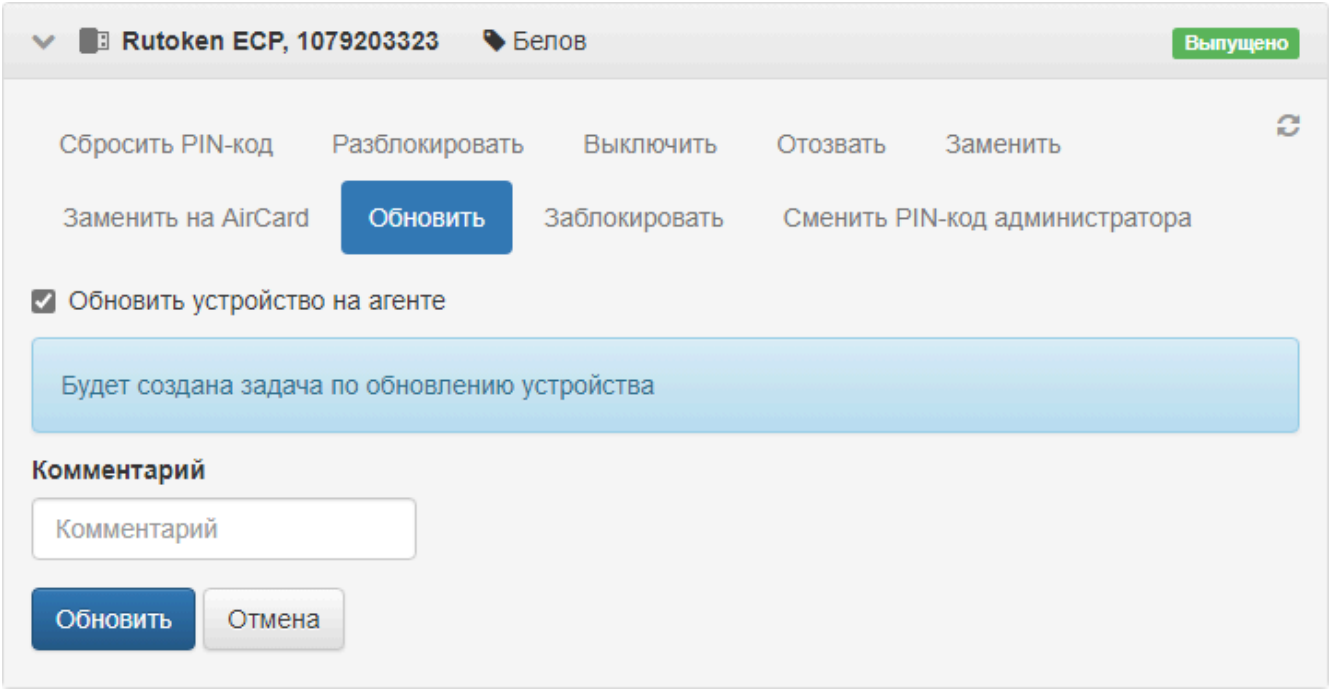
Для создания задачи нажмите **Отозвать**.

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.

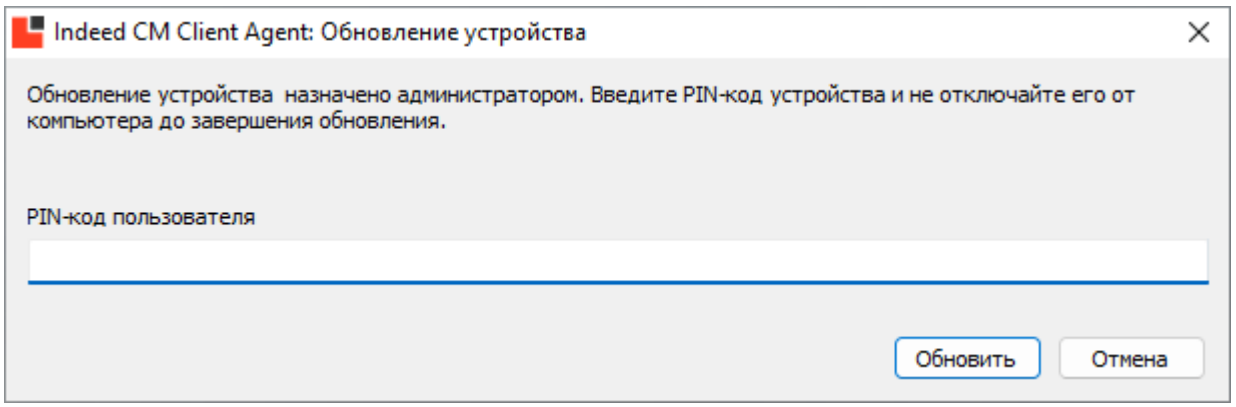


Обновление содержимого устройства

Нажмите **Обновить** в свойствах устройства, выберите сертификаты, если политика выпуска устройств это позволяет, включите опцию **Обновить устройство на агенте**, и укажите **Комментарий** при необходимости. Для создания задачи нажмите **Обновить**.

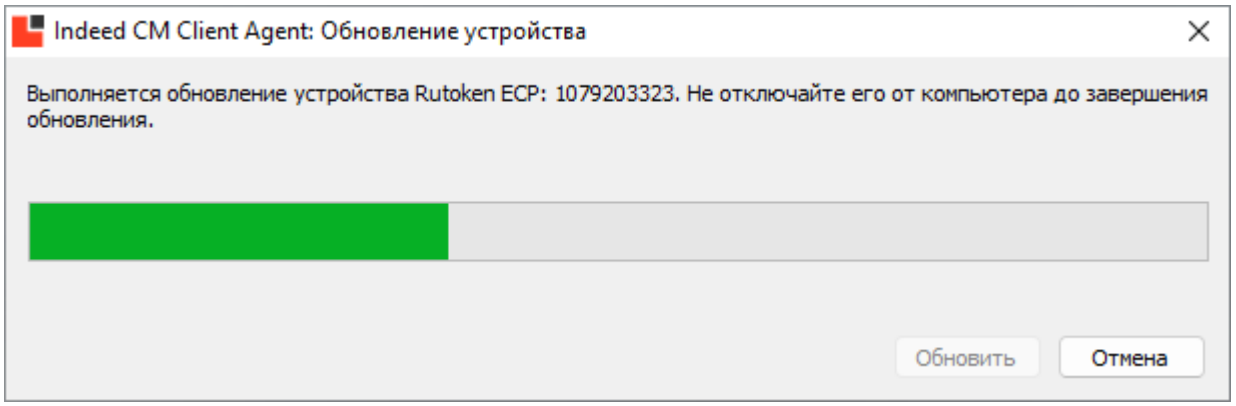


Для обновления содержимого агент запросит у пользователя PIN-код обновляемого устройства, когда оно будет подключено к рабочей станции пользователя. Введите PIN-код и нажмите **Обновить**.

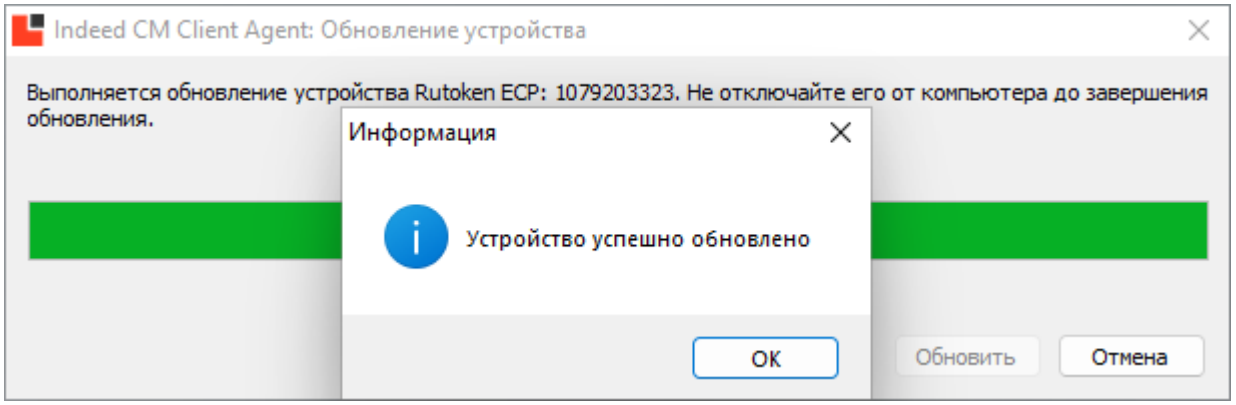


Если PIN-код неверный, отобразится соответствующее сообщение и обновление не будет выполнено.

Если введен верный PIN-код пользователя, то начнется обновление устройства.



После успешного завершения обновления отобразится соответствующее сообщение.



Отмена обновления

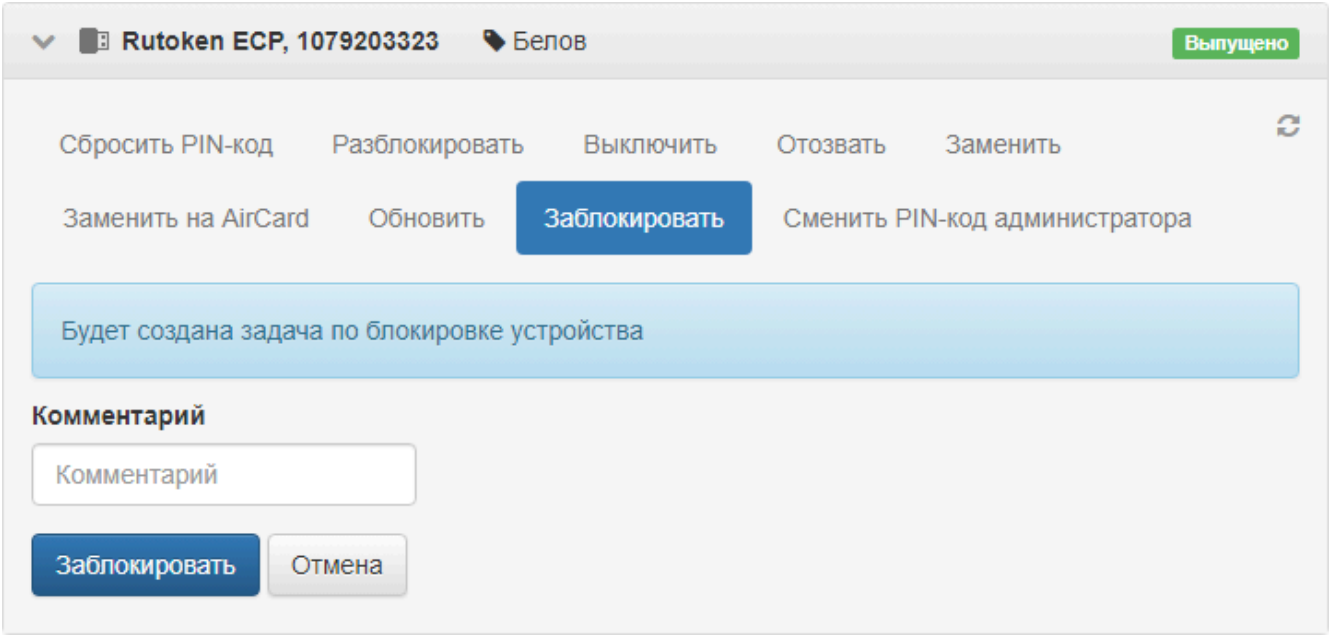
Вы можете отменить обновление устройства на агенте, если в разделе **Поведение** политики использования устройств задана опция **Разрешить отмену обновления устройства**.

Чтобы отменить обновление устройства:

1. Нажмите **Отменить обновление** в карточке устройства.
2. Введите **PIN-код пользователя**.
3. Задайте опцию **Отменить обновление на агенте**.
4. Нажмите **Отменить обновление**.

Блокировка устройства

Нажмите **Заблокировать** в свойствах устройства и укажите **Комментарий** при необходимости. Для создания задачи нажмите **Заблокировать**.

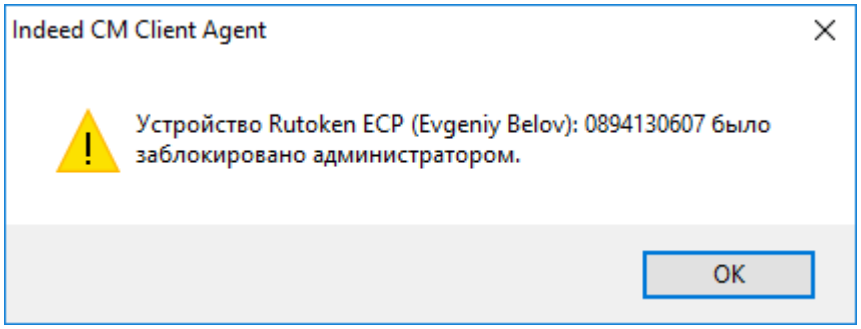


После выполнения задачи PIN-код пользователя заблокируется.

> **ПРИМЕЧАНИЕ**
>
> 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:

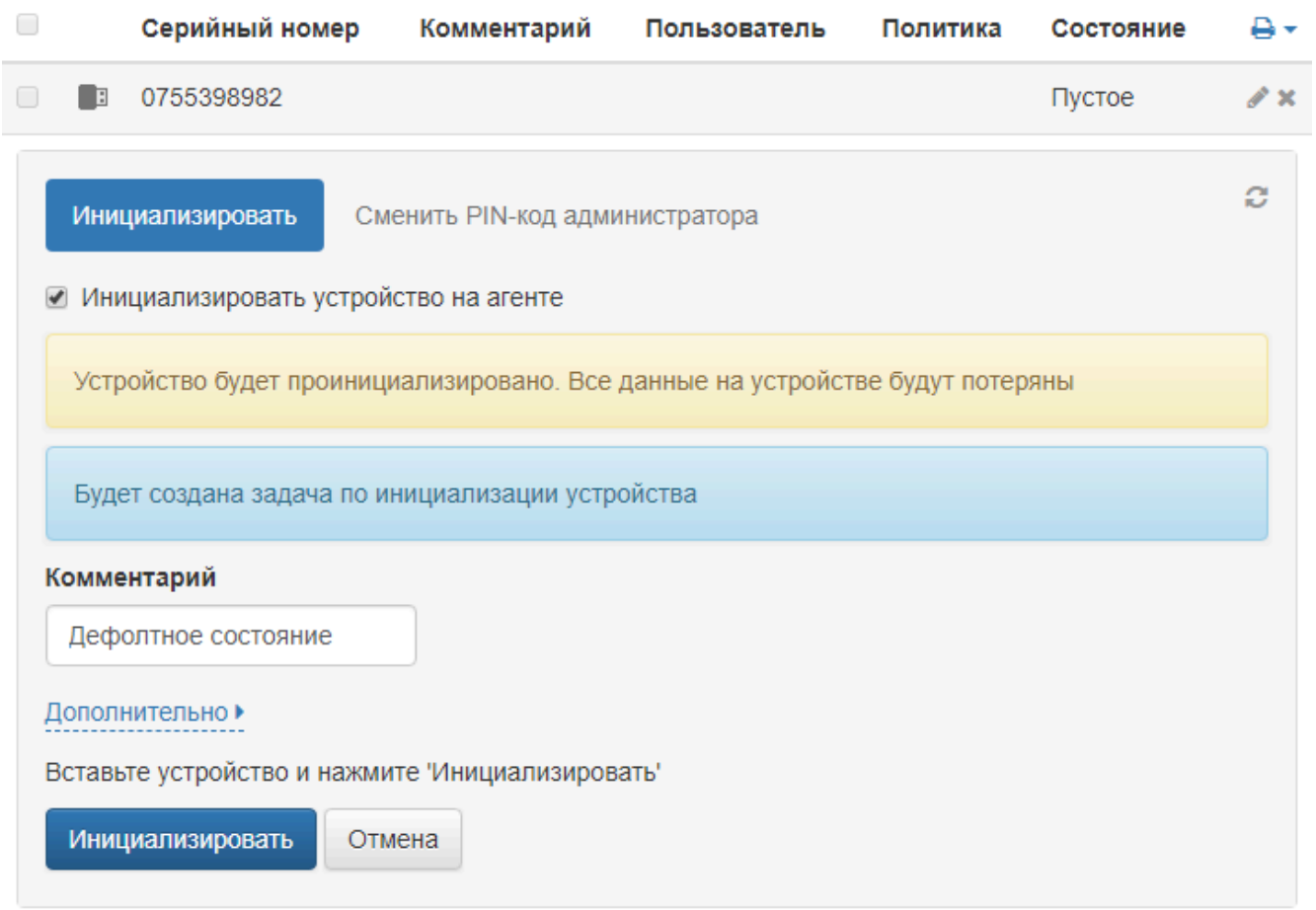


Инициализация устройства на агенте

Indeed CM позволяет выполнять инициализацию добавленных устройств на клиентском агенте, находящихся в состоянии **Пустое**.

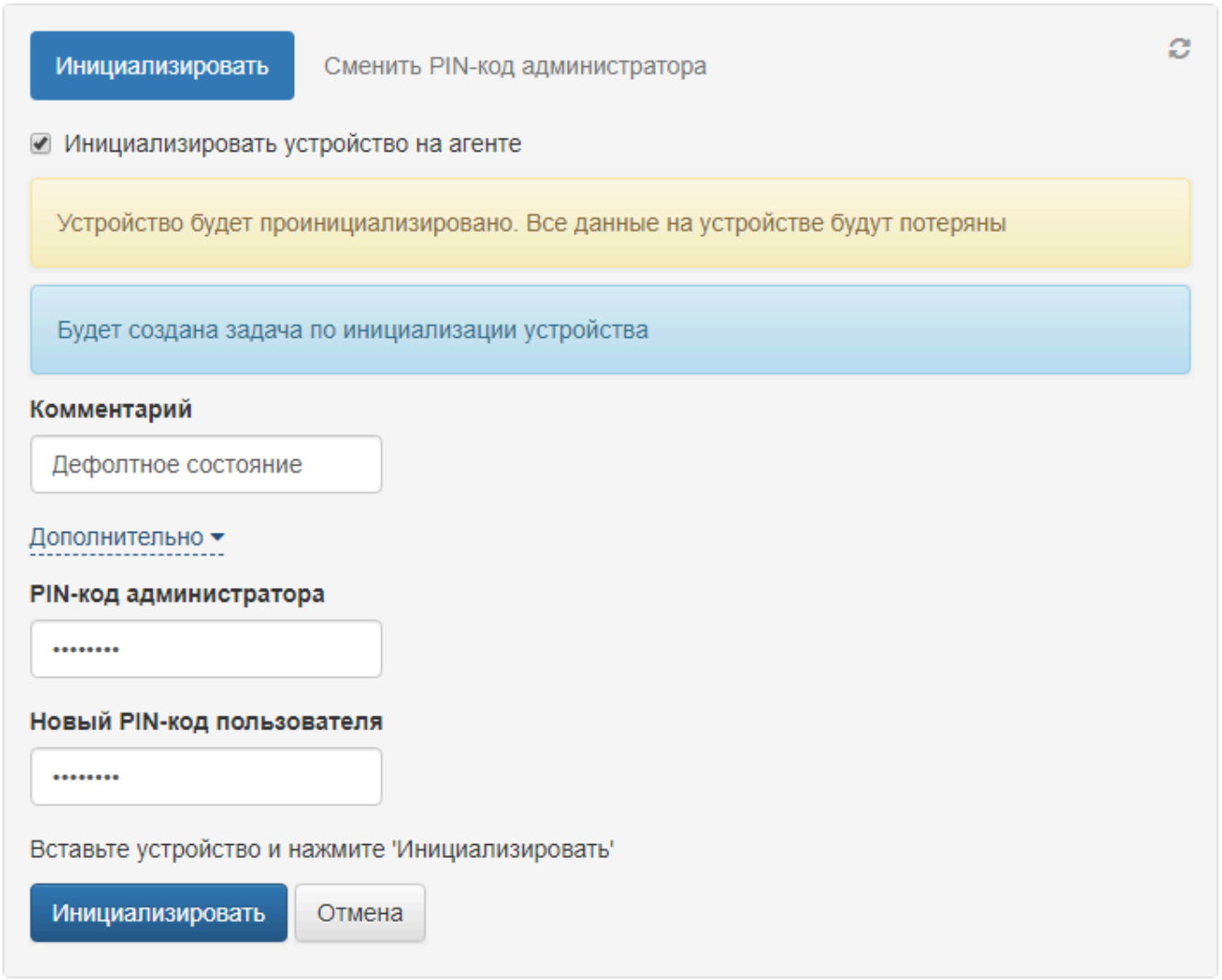
В карточке устройства нажмите **Инициализировать** и выберите опцию **Инициализировать устройство на агенте**:

1. 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**.



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.



ПРИМЕЧАНИЕ

Для устройств Рутокен 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.

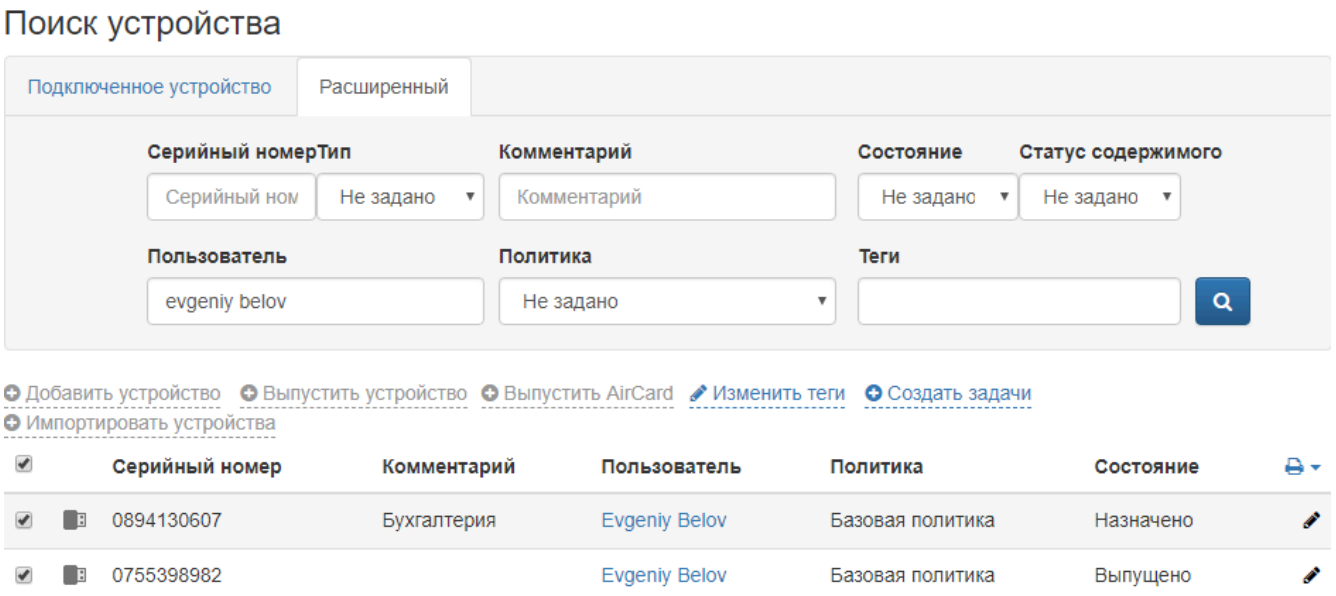
Массовые задачи

Массовые задачи – задачи, которые возможно назначить на несколько устройств сразу:

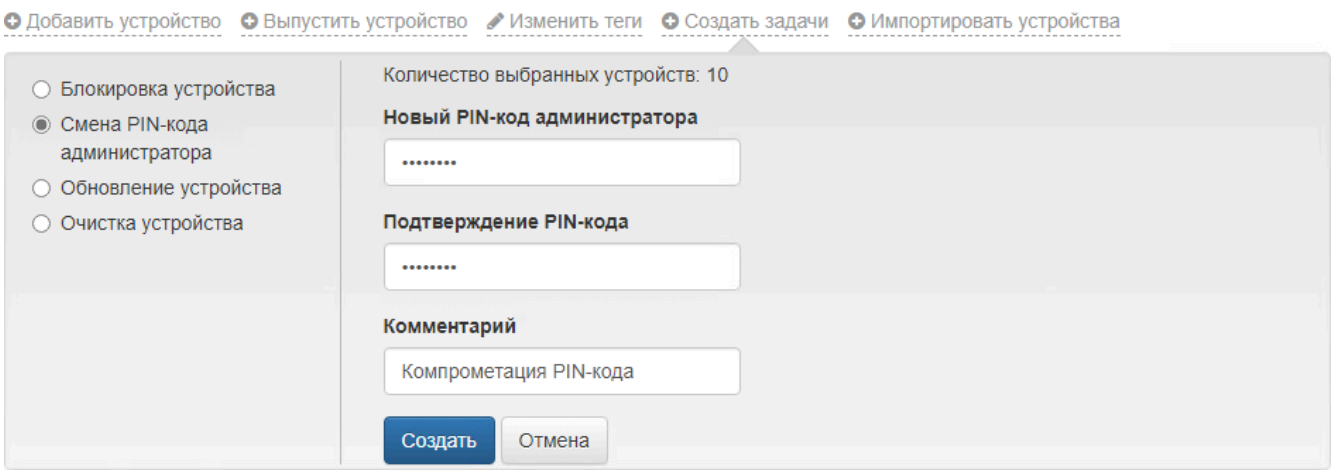
- Блокировка устройства - блокировка PIN-кода пользователя. Задача доступна для устройств в состояниях **Выпущено** или **В ожидании**.

- Смена PIN-кода администратора - задача доступна для всех состояний устройств в системе.
- Обновление устройства - задача по обновлению доступна для устройств в состоянии **Выпущено** и удовлетвореющим критериям обновления.
- Очистка устройства - очистка или инициализация устройства с возможностью отмены назначения (изъятия) устройства от пользователя. Задача доступна для устройств в состоянии **Отозвано**.

Массовые задачи назначаются на выбранные устройства и будут выполняться по мере подключения устройств к рабочим станциям, на которых установлен и настроен клиентский агент. Для создания массовой задачи перейдите на вкладку **Устройства**, выберите требуемые устройства и нажмите **Создать задачи**.



Выберите задачу, укажите параметры и нажмите **Создать**.



Задачи появятся в карточках устройств, а в разделе **Журнал** будут фиксироваться события о результатах выполнения задач на каждом агенте.

Рассылка сообщений пользователю

См. раздел **Сообщения пользователю**.

СКЗИ

> **ПОДСКАЗКА**
>
> Раздел доступен в Консоли управления на вкладке **Дополнительно**, если включена опция **Вести журнал учета СКЗИ** в разделе **Журнал учета СКЗИ** Мастера настройки Indeed CM и членам роли предоставлена привилегия на **Просмотр репозитория СКЗИ**.

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);
- **Дата** (за все время или за период).

Результаты поиска СКЗИ можно сохранить в файл в формате XLSX и распечатать.

Чтобы создать файл с результатами поиска, нажмите и выберите форму учета СКЗИ. Доступны следующие формы:

- типовая форма для органа криптографической защиты (ОКЗ);
- типовая форма для обладателя конфиденциальной информации (ОКИ);
- форма лицевого счета пользователя СКЗИ (доступна, если в условиях поиска выбрать конкретного пользователя);
- пользовательская форма.

Управление

Управлять СКЗИ можно в разделе **Дополнительно → СКЗИ** Консоли управления Indeed CM и в **карточке пользователя**.

Добавление

СКЗИ можно создать вручную или автоматически:

- при **добавлении устройства** с поддержкой аппаратной криптографии (тип: ключевой носитель);
- при **выпуске устройства**, если устройство не было предварительно добавлено в Indeed CM (тип: ключевой документ, ключевой носитель).

Нажмите **Добавить СКЗИ** и задайте значения параметров СКЗИ:

- **Тип** (дистрибутив, лицензия, документация, ключевой документ, ключевой носитель, пользовательский);
- **Описание**;
- **Серийный номер**;
- **Номер экземпляра** (необязательное поле);
- **Номер и дата документа**, на основании которого добавляется СКЗИ. Нажмите  , и номер документа выставится автоматически по шаблону нумерации, настроенному администратором Indeed CM для документов выбранного типа СКЗИ в разделе **Нормативные документы**.

Назначение

Изготовленные СКЗИ могут быть закреплены за пользователями.

1. Выберите изготовленные СКЗИ (одно или несколько), которые необходимо закрепить за пользователем и нажмите **Назначить СКЗИ**.
2. Выполните поиск пользователя, за которым необходимо закрепить выбранные СКЗИ, и нажмите **Выбрать**.
3. Нажмите **Назначить**. Состояние выбранных СКЗИ будет изменено с **Изготовлено** на **Назначено**. Закрепленные за пользователем СКЗИ будут доступны в его карточке в разделе **Назначенные СКЗИ**.

Редактирование

Отредактировать СКЗИ может уполномоченный сотрудник: оператор или администратор Indeed CM.

1. Выберите одно или несколько СКЗИ и нажмите **Редактировать 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).

2. Внесите изменения и нажмите **Сохранить**.

> **ПРИМЕЧАНИЕ**
>
> 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.

Уничтожение и изъятие

1. Выберите СКЗИ и нажмите **Уничтожить/изъять СКЗИ**.
2. Укажите имя сотрудника, выполняющего уничтожение/изъятие СКЗИ.
3. Укажте **Номер и дату документа**, на основании которого осуществляется уничтожение/изъятие.
4. Выберите опцию **Использовать повторно**, если СКЗИ будет использоваться повторно (например, при передаче лицензии или дистрибутива другому сотруднику).
5. Нажмите **Уничтожить/Изъять**.

Пакетный импорт

Поддерживается импорт СКЗИ 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`, где:

- `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 yyyyMMddHHmmss (UTC). Если значение не указано, то в качестве времени создания документа автоматически подставляется время импорта СКЗИ.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Serial Number, SKZI Type, Description и Document Number являются обязательными параметрами.
>
> Если вместо поля `Serial Number` 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**.

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
КС2 (исполнение 2-Base);СФ/124-3727 от 13.08.2019;20190813000000
```

В файл добавлены:

- Дистрибутив КриптоПро CSP 4.0 и его копия с серийным номером: 4040P-73010-04F65-67N08-637V1 по номеру документа ВН-337
- Дистрибутив КриптоПро CSP 5.0 и его копия с серийным номером: 4040Q-93010-04F65-UUZDG-E81NX по номеру документа ВН-338
- Лицензия КриптоПро CSP 4.0 с серийным номером: 4040Q-43010-KYE6B-C1857-0NKZH по номеру документа ВН-339
- Лицензия КриптоПро CSP 5.0 с серийным номером: 4040N-53010-KYE6B-CFTHW-TFAL7 по номеру документа ВН-339
- Документация Формуляр: ЖТЯИ.00102 01 30 01 КриптоПро CSP 5.0 КС2 (исполнение 2-Base) регистрационный номер СФ/124-3727 от 13.08.2019

Для пакетного импорта СКЗИ на вкладке **СКЗИ**:

1. Нажмите **Импортировать СКЗИ**.
2. Загрузите подготовленный файл СКЗИ.
3. Нажмите **Импортировать**.

Журналы учета

ПОДСКАЗКА

Раздел **Журналы учета** доступен в Консоли управления при включенной опции **Журнал учета устройств и сертификатов** в разделе **Общие функции** Мастера настройки Indeed CM и предоставленной привилегии **Просмотр журнала учета** членам роли.

Журналы учета содержат данные об устройствах и сертификатах, их владельцах и системах, в которых используются эти устройства и сертификаты.

Поля журналов учета настраиваются на вкладке **Конфигурация** → **Шаблоны журналов**.

Записи в журналы учета заносятся автоматически при выпуске, замене, изъятии или обновлении устройств (для журнала сертификатов) в Консоли управления или в Сервисе самообслуживания.

В разделе **Журналы учета** администратор или оператор Indeed CM могут выбрать созданный журнал и запросить необходимую информацию при помощи фильтров, настроенных для конкретного журнала.

Для добавления записи вручную нажмите **Добавить запись**, заполните **Обязательные поля** и нажмите **Добавить**.
Для редактирования 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 событий

Записи об операциях, совершенных во всех приложениях Indeed Certificate Manage, фиксируются в разделе **Журнал**.

По умолчанию в инсталляциях под управлением ОС Windows события хранятся в **Журнале Событий** (Event Viewer) на сервере Indeed CM, журнал **Indeed CM/Operational**.

Для просмотра событий установите параметры поиска:

- **Тип события** (информация, ошибка, предупреждение);
- **Событие**;
- **Сервис** (Консоль управления, Сервис самообслуживания, Монитор устройств, Credential provider, Сервис удаленного самообслуживания, API, AirCard Cleaner, утилита миграции, Сервис регистрации агентов, Сервис агентов);
- **Пользователь**;
- **Тип устройства**;
- **Серийный номер**;
- **Дата** (за период или за все время);
- **Инициатор**.

КАК ИЗМЕНИТЬ АТРИБУТ ИМЕНИ ПОЛЬЗОВАТЕЛЯ ДЛЯ ПОИСКА

Вы можете выбрать атрибут, по значению которого выполняется поиск пользователя в журнале событий. Для этого запустите Мастер настройки Indeed CM, перейдите на вкладку **Журнал событий** и выберите атрибут:

- **Общее имя** (CN) - значение по умолчанию;
- **sAMAccountName**;
- **userPrincipalName**;
- **Пользовательский**.

Для формирования отчета о событиях нажмите и выберите формат PDF или CSV.

Список событий

Основные события

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:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
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 учета	Запись успешно добавлена. Журнал учета: Поля: Инициатор:
1351	Ошибка	Изменение записи в журнале учета	Произошла ошибка при добавлении записи. Журнал учета: Поля: Инициатор: Сообщение об ошибке:
352	Информация	Изменение записи в журнале учета	Запись успешно изменена. Журнал учета: Поля: Новые поля: Инициатор:

Код	Тип	Событие	Описание
1352	Ошибка	Изменение записи в журнале учета	Произошла ошибка при изменении записи. Журнал учета: Поля: Новые поля: Инициатор: Сообщение об ошибке:
353	Информация	Изменение записи в журнале учета	Запись успешно удалена. Журнал учета: Поля: Инициатор:
1353	Ошибка	Изменение записи в журнале учета	Произошла ошибка при удалении записи. Журнал учета: Поля: Инициатор: Сообщение об ошибке:
1801	Ошибка	Отправка уведомления	Произошла ошибка при отправке уведомления. Сообщение об ошибке:

События клиентского агента

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:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
2723	Предупреждение	Ввод неверного PIN-кода пользователя на устройстве	Ввод неверного 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:

События журнала учета

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:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
351	Информация	Изменение записи в журнале учета	Запись успешно добавлена. Журнал учета: Поля: Инициатор:
1351	Ошибка	Изменение записи в журнале учета	Произошла ошибка при добавлении записи. Журнал учета: Поля: Инициатор: Сообщение об ошибке:
352	Информация	Изменение записи в журнале учета	Запись успешно изменена. Журнал учета: Поля: Новые поля: Инициатор:
1352	Ошибка	Изменение записи в журнале учета	Произошла ошибка при изменении записи. Журнал учета: Поля: Новые поля: Инициатор: Сообщение об ошибке:
353	Информация	Изменение записи в журнале учета	Запись успешно удалена. Журнал учета: Поля: Инициатор:

Код	Тип	Событие	Описание
1353	Ошибка	Изменение записи в журнале учета	Произошла ошибка при удалении записи. Журнал учета: Поля: Инициатор: Сообщение об ошибке:

События СКЗИ

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:

Код	Тип	Событие	Описание
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:

События КриптоПро DSS

Код	Тип	Событие	Описание
501	Информация	Выпуск устройства КриптоПро DSS	Устройство КриптоПро DSS успешно выпущено. Пользователь: Политика: Сертификаты: Инициатор:
1501	Ошибка	Выпуск устройства КриптоПро DSS	Произошла ошибка при выпуске устройства КриптоПро DSS. Пользователь: Политика: Инициатор: Сообщение об ошибке:
502	Информация	Включение устройства КриптоПро DSS	Устройство КриптоПро DSS успешно включено. Пользователь: Инициатор:
1502	Ошибка	Включение устройства КриптоПро DSS	Произошла ошибка при включении устройства КриптоПро DSS. Пользователь: Политика: Инициатор: Сообщение об ошибке:
503	Информация	Выключение устройства КриптоПро DSS	Устройство КриптоПро DSS успешно выключено. Пользователь: Инициатор:

Код	Тип	Событие	Описание
1503	Ошибка	Выключение устройства КриптоПро DSS	Произошла ошибка при выключении устройства КриптоПро DSS. Пользователь: Инициатор: Сообщение об ошибке:
504	Информация	Отзыв устройства КриптоПро DSS	Устройство КриптоПро DSS успешно отозвано. Пользователь: Причина: Сертификаты: Инициатор:
1504	Ошибка	Отзыв устройства КриптоПро DSS	Произошла ошибка при отзыве устройства КриптоПро DSS. Пользователь: Причина: Инициатор: Сообщение об ошибке:
505	Информация	Обновление устройства КриптоПро DSS	Устройство КриптоПро DSS успешно обновлено. Пользователь: Новые сертификаты: Обновленные сертификаты: Удаленные сертификаты: Новая политика: Инициатор:

Код	Тип	Событие	Описание
1505	Ошибка	Обновление устройства КриптоПро DSS	Произошла ошибка при обновлении устройства КриптоПро DSS. Пользователь: Инициатор: Сообщение об ошибке:
506	Информация	Удаление устройства КриптоПро DSS	Устройство КриптоПро DSS успешно удалено. Пользователь: Инициатор:
1506	Ошибка	Удаление устройства КриптоПро DSS	Произошла ошибка при удалении устройства КриптоПро DSS. Пользователь: Инициатор: Сообщение об ошибке:
507	Информация	Выпуск устройства КриптоПро DSS ожидает решения	Выпуск устройства КриптоПро DSS ожидает решения. Пользователь: Политика: Сертификаты: Инициатор:
508	Информация	Обновление устройства КриптоПро DSS ожидает решения	Обновление устройства КриптоПро DSS ожидает решения. Пользователь: Новые сертификаты: Обновленные сертификаты: Удаленные сертификаты: Новая политика: Инициатор:

Код	Тип	Событие	Описание
509	Информация	Отмена обновления устройства КриптоПро DSS	Обновление устройства КриптоПро DSS успешно отменено. Пользователь: Инициатор:
1509	Ошибка	Отмена обновления устройства КриптоПро DSS	Произошла ошибка при отмене обновления устройства КриптоПро DSS. Пользователь: Инициатор: Сообщение об ошибке:

События AirCard Enterprise

Код	Тип	Событие	Описание
401	Информация	Добавление AirCard к компьютеру	AirCard был добавлен к компьютеру. Устройство: Компьютер:
1401	Ошибка	Добавление AirCard к компьютеру	Произошла ошибка при добавлении AirCard к компьютеру. Устройство: Компьютер: Сообщение об ошибке:
402	Информация	Удаление AirCard от компьютера	AirCard был удален от компьютера. Устройство: Компьютер:
1402	Ошибка	Удаление AirCard от компьютера	Произошла ошибка при удалении AirCard от компьютера. Устройство: Компьютер: Сообщение об ошибке:
403	Информация	Создание кода подключения AirCard к компьютеру	Код подключения AirCard к компьютеру успешно создан. Устройство: Компьютер:

Код	Тип	Событие	Описание
1403	Ошибка	Создание кода подключения AirCard к компьютеру	Произошла ошибка при создании кода подключения AirCard к компьютеру. Устройство: Компьютер: Сообщение об ошибке:

Руководство пользователя

Пользователи Indeed CM могут управлять своими устройствами самостоятельно в Сервисе самообслуживания и в Сервисе удаленного самообслуживания.

Сервис самообслуживания

Сервис самообслуживания (Self-Service) — это веб-приложение, где пользователи Indeed Certificate Manager могут управлять своими устройствами самостоятельно. Доступен по адресу: *https://<FQDN сервера Indeed CM>/cm/ss*.

Настройки входа в приложение задаются в параметрах аутентификации.

В Сервисе самообслуживания пользователю доступна следующая информация:

- **О себе** – имя, логин, электронная почта, телефон и фото. Информация о пользователе (имя, имя для входа в домен, электронная почта, телефон и фото) добавляется в Indeed CM автоматически из профиля пользователя в Active Directory. Изменения в профиле пользователя в Active Directory отображаются в Сервисе самообслуживания.
- **Устройства** – список устройств, закрепленных за пользователем, и их содержимое.
- **СКЗИ** – список назначенных СКЗИ.
- **Документы** – список документов пользователя.

> **ПРИМЕЧАНИЕ**
>
> Список действий пользователя с устройствами определяет администратор в разделе **Конфигурация → Политики →** Поведение Консоли управления Indeed CM.

Операции, доступные пользователю в Сервисе самообслуживания:

Выпуск устройства

Как выпустить смарт-карту или USB-токен

Изменение ответов на секретные вопросы

Как изменить ответы на секретные вопросы

Обновление устройства

Как обновить содержимое устройства

Выключение и включение устройств

Как включить и выключить устройство

Выключение устройств без выполнения входа в систему

Как выключить устройство

Отзыв и очистка устройств

Как отозвать и очистить устройство

Сброс и изменение PIN-кода устройств

Как задать новый PIN-код

Просмотр содержимого устройства

Как просмотреть и распечатать содержимое устройства

СКЗИ

Как просмотреть и распечатать нормативные документы СКЗИ

Документы

Внутренний электронный документооборот

Клиентский агент Indeed CM

Удаленное управление устройствами пользователей

Загрузка файлов и ресурсов

Как просмотреть файлы и ресурсы в Indeed CM

Выгрузка сертификата DSS

Как установить сертификат DSS на рабочую станцию пользователя

Сервис удаленного самообслуживания

Сервис удаленного самообслуживания позволяет выполнять операции с устройствами без подключения к компьютеру, за исключением случая разблокировки устройства при помощи утилиты Indeed CM - Unblock.

Сервис удаленного самообслуживания доступен по адресу: *https://<FQDN сервера Indeed CM>/cm/rss*.

Для входа в Сервис удаленного самообслуживания введите **Имя пользователя**(логин) и символы с изображения.

Для доступа к карточке пользователя требуется аутентификация по секретным вопросам.

После входа 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

Изменить ответы на секретные вопросы Пользователь КриптоПро 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

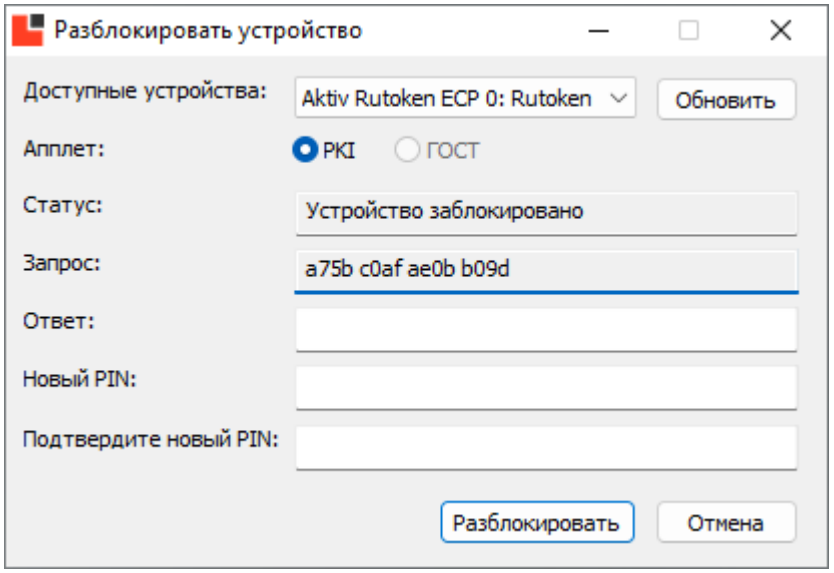
Изменить PIN-код устройства
Изменить PIN-код устройства, если вы предполагаете, что кто-либо другой узнал его

AirCard, f9a104e93d054e59 Evgeniy Belov Выпущено

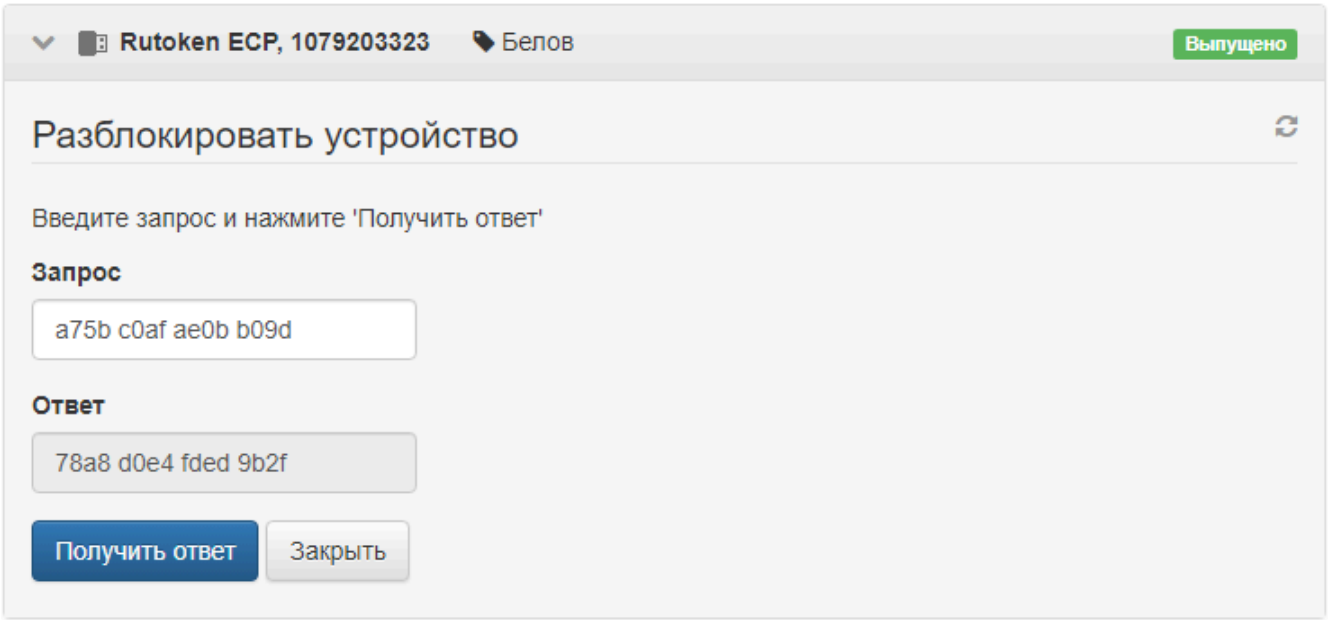
Операции выключения, включения и отзыва устройств производятся так же, как и в Сервисе самообслуживания.

Для разблокировки устройства используйте утилиту Indeed CM - Unblock.

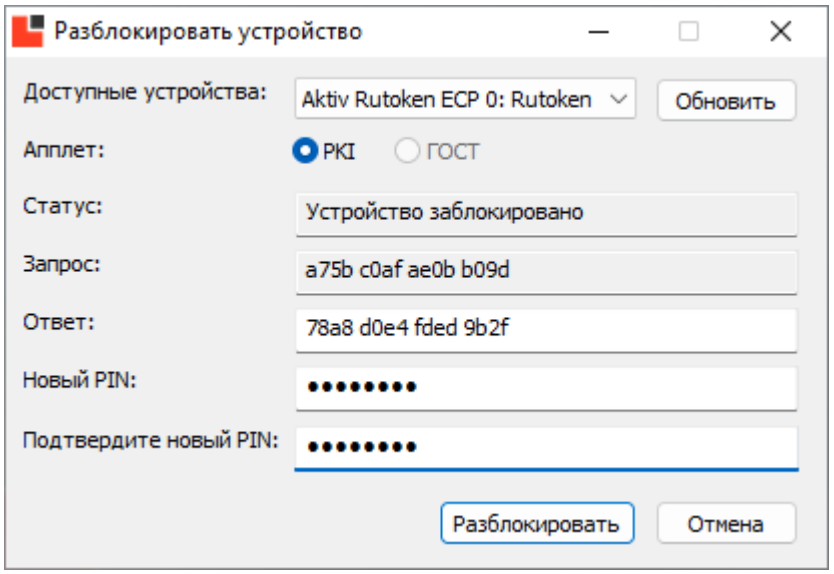
1. Запустите утилиту Indeed CM - Unblock (*Пуск – Все программы – Indeed*. Расположение по умолчанию: */IndeedCM/IndeedCM.Unblock.exe*).
2. Выберите устройство из списка в интерфейсе утилиты и скопируйте код разблокировки из поля **Запрос**.



3. Выберите нужное устройство и нажмите **Разблокировать устройство**, введите код разблокировки устройства из утилиты в поле **Запрос** и нажмите **Получить ответ**.



4. Введите полученный код ответа в поле **Ответ** утилиты разблокировки, ведите новый PIN-код, его подтверждение и нажмите **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

Выпуск устройства

Вы можете получить уже готовое к работе устройство или выпустить устройство самостоятельно, если администратор или оператор Indeed CM выдал вам пустое устройство.

Если вы получили готовое к работе устройство, то при входе в Сервис самообслуживания отобразится вся информация об этом устройстве.

Дополнительные опции:

- **Установить секретные вопросы и ответы на них**. Опция доступна при первом входе в Сервис самообслуживания перед выпуском устройства. Количество секретных вопросов и необходимость установки ответов задает администратор Indeed CM в разделах **Поведение** и **Аутентификация** политики использования устройств.

- **Выпустить устройство самостоятельно**. Опция доступна, если выпущенных устройств нет, и администратор разрешил вам выпускать устройства.

Процедура выпуска

1. Нажмите **Выпустить устройство**.

2. Если администратор задал опцию **Разрешить пользователю выбор необязательных сертификатов при выпуске устройства** в разделе **Поведение** политики использования устройств, отобразится окно выбора шаблонов сертификатов.
   Выберите шаблоны, по которым будут сформированы сертификаты для записи на устройство.

3. Если администратор настроил интеграцию в разделе **СМЭВ** политики использования устройств и сертификат выпускается по шаблону для КриптоПро УЦ 2.0 или Валидата УЦ, отобразится форма проверки СМЭВ.
   Вы можете проверить данные на соответствие и изменить их, если администратор задал опцию **Разрешить пользователю редактирование данных в форме проверки в СМЭВ** в разделе **Поведение**.

4. Если устройство поддерживает аппаратную криптографию, не добавлено в Indeed CM, и администратор включил опцию **Разрешить пользователю добавление устройства** в разделе **Поведение**, то в окне выпуска устройства отобразится поле **Номер и дата документа**.

Выставите данные о документе, на основании которого будет изготовлено СКЗИ с информацией об устройстве.

5. Если администратор задал опцию **Инициализировать устройство** в разделе **Выпуск** и настроил параметры инициализации в разделе **Инициализация устройства** политики использования устройств, устройство будет инициализировано.

Выпуск с инициализацией

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> При выпуске устройства с инициализацией все данные на устройстве будут удалены.

1. Введите **PIN-код администратора**. Поле отображается, если устройство не добавлено в Indeed CM и администратор включил опцию **Разрешить пользователю добавление устройства** в разделе **Поведение**.

   > ⓘ **ПРИМЕЧАНИЕ**
   >
   > Если поле **PIN-код администратора** оставить пустым, то установится значение, указанное администратором в разделе **Типы устройств**. Поддерживается ввод PIN-кодов для нескольких областей. Например, для PKI и ГОСТ на устройствах JaCarta.

2. Нажмите **Выпустить**.

Выпуск без инициализации

1. Введите **PIN-код пользователя**.
2. Введите **PIN-код администратора**. Поле отображается, если устройство не добавлено в Indeed CM и администратор включил опцию **Разрешить пользователю добавление устройства** в разделе **Поведение**.

> **ПРИМЕЧАНИЕ**
>
> Если поля **PIN-код администратора** и **PIN-код пользователя** оставить пустыми, то установятся значения, указанные администратором в разделе **Типы устройств**.
> Поддерживается ввод PIN-кодов для нескольких областей. Например, для PKI и ГОСТ на устройствах JaCarta.

3. Нажмите **Выпустить**.
4. Если устройство содержит сторонние сертификаты, Indeed CM может их обнаружить и внести информацию о таких сертификатах в систему – отследить.
   Окно выбора сертификатов для отслеживания отображается, если администратор задал опцию **Включить отслеживание сертификатов** в разделе **Поведение** политики использования устройств.
   Выберите сертификаты для отслеживания, если они есть на устройстве, и нажмите **Ок**.

6. Если администратор задал опцию **Установить случайный PIN-код пользователя** в разделе **Выпуск** политики использования устройств, то после выпуска устройства вы увидите свой PIN-код.
   Если администратор настроил рассылку уведомлений по электронной почте в разделе **Уведомления**, PIN-код можно отправить на вашу электронную почту или почту руководителя.

7. По завершении выпуска устройства нажмите **Закрыть**.

В Сервисе самообслуживания появится раздел **Ваши устройства**, где отображаются сведения о выпущенном устройстве – тип, серийный номер, имя, статус.

Если вы не задали секретные вопросы при выпуске, перейдите к их настройке.

Одобрение выпуска

Выпуск устройства может быть приостановлен, если регламент вашей организации предусматривает проверку документов для получения цифровых сертификатов – одобрение.

В окне выпуска устройства появится сообщение *Выпуск устройства ожидает решения*. Устройству присваивается статус **В ожидании**. Это означает, что ваш запрос на выпуск устройства перешел в стадию рассмотрения.

Отправьте документы для получения сертификата:

- с помощью Indeed CM, если настроена функция внутреннего электронного документооборота – **Indeed CM ЭДО**;
- вне Indeed CM любым другим способом, принятым в вашей организации. Например, по электронной почте.

Обмен документами в Indeed CM

Если в Indeed CM настроена функция внутреннего электронного документооборота – **Indeed CM ЭДО**,

> **ПОДСКАЗКА**
>
> Настройки одобрения задает администратор Indeed CM в разделе **Шаблоны** политики использования устройств.

В зависимости от настроек, заданных администратором Indeed CM, вам необходимо подписать и загрузить в Indeed CM следующие документы:

Запрос на сертификат

Предоставьте подписанную форму запроса на сертификат для одобрения в удостоверяющем центре (УЦ). Администратор Indeed CM может предварительно проверить запрос на сертификат перед отправкой запроса в УЦ.

Выполните следующие действия:

1. Загрузите подписанный запрос на сертификат в Indeed CM:
    1. Распечатайте запрос на сертификат. Перейдите на вкладку **Содержимое** в карточке устройства и нажмите  напротив шаблона сертификата.
    2. Подпишите запрос на сертификат и добавьте в Indeed CM. **Как подписать и загрузить документ в Indeed CM**
2. Дождитесь одобрения запроса на сертификат в УЦ. На вкладке **Содержимое** в карточке устройства можно проверить статус сертификата – **В ожидании**.
3. Если запрос на сертификат одобрен в УЦ, то сертификат получает статус **Одобрен** и записывается на устройство. Перейдите в карточку устройства и нажмите **Продолжить выпуск устройства**.
   Если запрос отклонен, отзовите и очистите устройство самостоятельно или обратитесь к администратору, после чего начните выпуск устройства заново.

> **ПРИМЕЧАНИЕ**
>
> Если администратор Indeed CM настроил автоматическую рассылку уведомлений пользователя по электронной почте, вы получите уведомление о статусе одобрения – *Одобрение документа*, *Одобрение выпуска устройства* или *Отклонение выпуска устройства*.
>
> Если автоматическая рассылка уведомлений не настроена, дождитесь появления кнопки **Продолжить выпуск устройства** в карточке устройства.

Сертификат

Если регламент получения сертификата проверки электронной подписи, принятый в вашей организации, предусматривает дополнительную проверку документа о сертификате, то администратор Indeed CM может проверить документ перед записью сертификата на устройство.

В этом сценарии УЦ одобряет сертификат автоматически. На вкладке **Содержимое** в карточке устройства можно проверить статус сертификата – **Действителен**. Это означает, что сертификат выпущен в УЦ, но еще не записан на устройство.

Выполните следующие действия:

1. Загрузите подписанную форму сертификата в Indeed CM:
    1. Распечатайте форму сертификата. Перейдите на вкладку **Содержимое** в карточке устройства, нажмите напротив шаблона сертификата и выберите **Сертификат**.
    2. Подпишите форму сертификата и добавьте в Indeed CM. **Как подписать и загрузить документ в Indeed CM**
2. Дождитесь одобрения документа от администратора Indeed CM.
3. Если администратор одобрил документ, то сертификат записывается на устройство. Перейдите в карточку устройства и нажмите **Продолжить выпуск устройства**.
   Если администратор отклонил документ, отредактируйте его, подпишите и заново загрузите в Indeed CM.

> **ПРИМЕЧАНИЕ**
>
> Если администратор Indeed CM настроил автоматическую рассылку уведомлений пользователя по электронной почте, то вы получите уведомление о статусе одобрения – *Одобрение документа*.
>
> Если автоматическая рассылка уведомлений не настроена, дождитесь появления кнопки **Продолжить выпуск устройства** в карточке устройства.

Запрос на сертификат и сертификат

Чтобы продолжить выпуск устройства и записать на него сертификат:

1. Предоставьте подписанную форму запроса на сертификат и дождитесь одобрения запроса в УЦ.
2. Предоставьте подписанную форму сертификата и дождитесь одобрения документа от администратора Indeed CM.

Выполните следующие действия:

1. Загрузите подписанную форму запроса на сертификат в Indeed CM:

    1. Распечатайте запрос на сертификат. Перейдите на вкладку **Содержимое** в карточке устройства и нажмите  напротив шаблона сертификата.
    2. Подпишите запрос на сертификат и добавьте в Indeed CM. **Как подписать и загрузить документ в Indeed CM**

2. Дождитесь одобрения запроса на сертификат в УЦ. На вкладке **Содержимое** в карточке устройства можно проверить статус сертификата – **В ожидании**.

3. Если запрос на сертификат одобрен в УЦ, то сертификат получает статус **Действителен**. Это означает, что сертификат выпущен в УЦ, но еще не записан на устройство. Загрузите подписанную форму сертификата в Indeed CM для проверки администратора:

    1. Распечатайте форму сертификата. Перейдите на вкладку **Содержимое** в карточке устройства, нажмите  напротив шаблона сертификата и выберите **Сертификат**.
    2. Подпишите форму сертификата и добавьте в Indeed CM.

    Если запрос отклонен в УЦ, отзовите и очистите устройство самостоятельно или обратитесь к администратору, после чего начните выпуск устройства заново.

4. Если администратор одобрил подписанную форму сертификата, то сертификат получает статус **Одобрен** и записывается на устройство. Перейдите в карточку устройства и нажмите **Продолжить выпуск устройства**.

Если администратор отклонил документ, отредактируйте его, подпишите и заново загрузите в Indeed CM.

> **ПРИМЕЧАНИЕ**
>
> Если администратор Indeed CM настроил автоматическую рассылку уведомлений пользователя по электронной почте, то вы получите уведомление о статусе одобрения – *Одобрение выпуска устройства*, *Одобрение документа* или *Отклонение выпуска устройства*.
>
> Если автоматическая рассылка уведомлений не настроена, дождитесь статуса сертификата **Одобрен**.

Обмен документами вне Indeed CM

Предоставьте документы администратору Indeed CM согласно регламенту получения сертификата проверки электронной подписи, принятому в вашей организации.

Выполните следующие действия:

1. Предоставьте администратору Indeed CM подписанную форму запроса на сертификат для одобрения в удостоверяющем центре (УЦ).
2. Дождитесь одобрения запроса на сертификат в УЦ. На вкладке **Содержимое** в карточке устройства можно проверить статус сертификата – **В ожидании**.
3. Если запрос на сертификат одобрен, то сертификат получает статус **Одобрен** и записывается на устройство. Перейдите в карточку устройства и нажмите **Продолжить выпуск устройства**.
   Если запрос отклонен, вам необходимо отозвать и очистить устройство самостоятельно или обратиться к администратору, после чего начать выпуск устройства заново.

ПРИМЕЧАНИЕ

Если администратор Indeed CM настроил автоматическую рассылку уведомлений пользователя по электронной почте, то вы получите уведомление о статусе одобрения – *Одобрение выпуска устройства* или *Отклонение выпуска устройства*.

Если автоматическая рассылка уведомлений не настроена, дождитесь появления кнопки **Продолжить выпуск устройства** в карточке устройства.

Выпуск специализированных устройств

В Indeed CM можно выпустить следующие специализированные устройства:

- Registry;
- TPM Virtual Smart Card (VSC);
- Windows Hello for Business;
- AirCard.

Registry

Инструкция для администратора Indeed CM по настройке выпуска устройств Registry

1. Настройте поддержку устройств Registry.
2. Добавьте тип устройства *Registry.xml* в конфигурацию Indeed CM.
3. Установите компонент IndeedCM.Registry.Middleware на рабочую станцию пользователя.

ОСОБЕННОСТИ ВЫПУСКА УСТРОЙСТВ REGISTRY

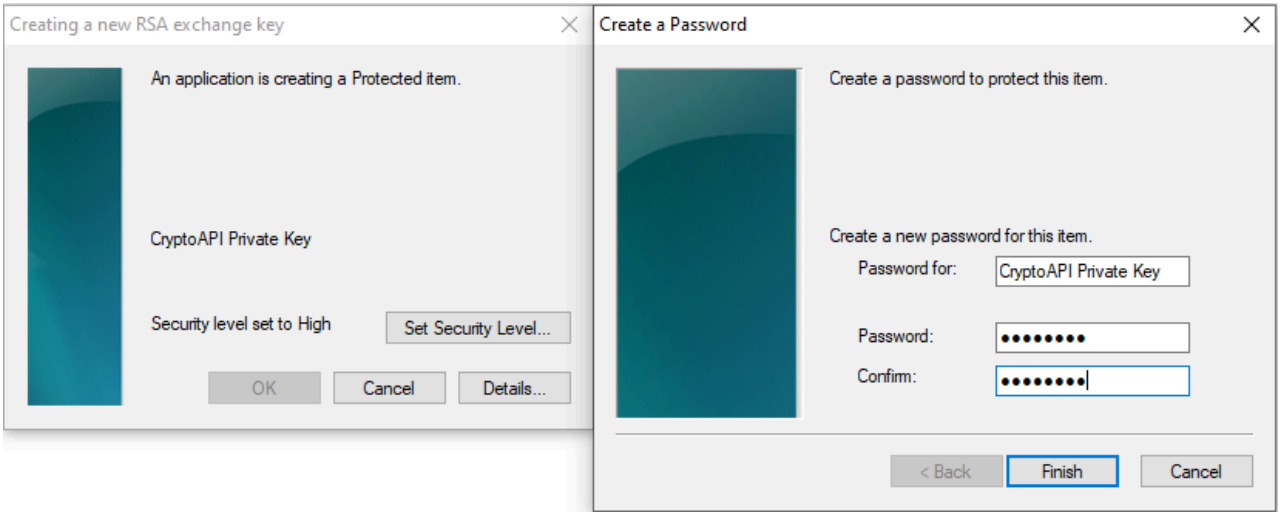
- поддерживается выпуск только RSA сертификатов;
- не поддерживается работа с PIN-кодами;
- не поддерживается инициализация устройства.

Чтобы выпустить устройство Registry, выполните следующие действия:

1. Нажмите **Выпустить устройство**.
2. Задайте имя устройства.
3. В поле **Устройство** выберите:
   - **Registry - Machine: Registry**, чтобы выпустить сертификат в хранилище сертификатов локального компьютера;
   - **Registry - User: Registry**, чтобы выпустить сертификат в хранилище сертификатов текущего пользователя.
4. Нажмите **Выпустить**. Indeed CM отправит запрос на сертификат в УЦ.
5. Создайте пароль для контейнера закрытого ключа в окне создания приватного RSA-ключа.

   Это необходимо, если в настройках шаблона сертификата в Microsoft CA администратор задал опцию **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).

   1. Нажмите **Выбор уровня безопасности..** (Set security Level..) и задайте пароль, удовлетворяющий требованиям безопасности вашей организации.
   2. Нажмите **Finish** и **ОК**.



Сертификаты с закрытыми ключами запишутся в хранилище сертификатов пользователя или компьютера.

⚠ **ПРЕДУПРЕЖДЕНИЕ**

Сбросить пароль на контейнер при его утере невозможно. Перевыпустите сертификат.

TPM Virtual Smart Card

Инструкция для администратора Indeed CM по настройке выпуска устройств TPM VSC

1. Запустите Мастер настройки Indeed CM, перейдите в раздел **Общие функции** и включите опцию **Работа с TPM Virtual Smart Card**.
2. Добавьте тип устройства *Tpm.xml* в конфигурацию Indeed CM.

⚠ **НАСТРОЙКИ РАЗБЛОКИРОВКИ УСТРОЙСТВ TPM**

Чтобы иметь возможность разблокировать устройство TPM, при добавлении типа устройства в Indeed CM PIN-код администратора должен меняться на случайный или на любой неслучайный Triple DES.

3. Установите Доверенный платформенный модуль 2.0 (Trusted Platform Module) на рабочую станцию пользователя.
4. Установите компонент IndeedCM.TPM.Middleware на рабочую станцию пользователя.

ⓘ **ОСОБЕННОСТИ ВЫПУСКА УСТРОЙСТВ TPM VSC**

- поддерживается выпуск только RSA сертификатов;
- не поддерживается инициализация устройства.

Чтобы выпустить устройство TPM VSC, выполните следующие действия:

1. Нажмите **Выпустить устройство**.
2. Задайте имя устройства.

3. Выберите **Создать виртуальное устройство TPM** или выберите уже созданное устройство.
4. Нажмите **Выпустить**.

Indeed CM создаст виртуальную карту. Виртуальную карту TPM можно использовать как аппаратное устройство на вашей рабочей станции. Например, для аутентификации в домене.

Windows Hello for Business

Инструкция для администратора Indeed CM по настройке выпуска устройств Windows Hello for Business

1. Разверните инфраструктуру Windows Hello for Business по инструкции Microsoft.
2. Запустите Мастер настройки Indeed CM, перейдите в раздел **Общие функции** и включите опцию **Работа с Windows Hello for Business**.
3. Добавьте тип устройства *Whfb.xml* в конфигурацию системы.
4. Установите Доверенный платформенный модуль 2.0 (Trusted Platform Module) на рабочую станцию пользователя.
5. Установите компонент IndeedCM.WHfB.Middleware на рабочую станцию пользователя.

ОСОБЕННОСТИ ВЫПУСКА УСТРОЙСТВ WINDOWS HELLO FOR BUSINESS

- 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 - 10;
- не поддерживается инициализация устройства.

Чтобы выпустить устройство Windows Hello for Business, выполните следующие действия:

1. Нажмите **Выпустить устройство**.
2. Задайте имя устройства.

3. Выберите **Настроить WHfB**.
4. Нажмите **Выпустить**.
5. Настройте PIN-код в окне настройки PIN-кода для Windows Hello:

    1. Нажмите **Задать PIN-код** (Set up PIN).
    2. Введите учетные данные для основной и пользовательской проверки подлинности (с помощью Indeed CM MFA адаптера) и нажмите **Submit**.
    3. Создайте PIN-код и нажмите **ОК**.

После создания PIN-кода Indeed CM продолжит выпуск устройства.

Windows Hello for Business может использоваться как аппаратное устройство на вашей рабочей станции пользователя. Например, для аутентификации в домене.

AirCard

Инструкция для администратора Indeed CM по настройке выпуска устройств AirCard

1. Задайте опцию **Разрешить пользователю выпуск AirCard устройств** в разделе **Поведение** политики использования устройств.
2. Добавьте тип устройства *AirCard.xml* в конфигурацию системы.
3. Установите компоненты IndeedCM.AirCard.Middleware и IndeedID.AirCard.Runtime на рабочую станцию пользователя.
4. Настройте сетевую доступность сервера Indeed AirCard Enterprise с рабочей станции пользователя.

> **ОСОБЕННОСТИ ВЫПУСКА УСТРОЙСТВ AIRCARD**
>
> Поддерживается выпуск только RSA сертификатов.

После установки Indeed AirCard Runtime в области уведомлений панели задач Windows появится индикатор подключенных устройств AirCard.

Чтобы выпустить виртуальную смарт-карту AirCard, выполните следующие действия:

1. Нажмите **Выпустить устройство**.
2. Задайте имя устройства.
3. Выберите **Создать новое устройство AirCard** или выберите уже созданное устройство.
4. Нажмите **Выпустить**.

После выпуска устройство AirCard автоматически привяжется к вашей рабочей станции. Список разрешенных компьютеров для подключения выпущенного устройства отображается в карточке устройства AirCard.

Покдлючение AirCard к рабочей станции

AirCard можно подключить двумя способами:

- автоматически в Indeed CM;
- вручную в панели управления Indeed AirCard Enterprise.

Indeed CM

После выпуска устройство AirCard автоматически подключится к разрешенным компьютерам, если они находятся в корпоративной сети предприятия.

Indeed AirCard Enterprise

Применяется, если устройство нельзя подключить автоматически (например, если компьютер находится за пределами корпоративной сети предприятия). В этом случае устройство может выпустить только администратор Indeed CM.

Добавьте устройство вручную в приложении Indeed AirCard Enterprise и подключите его к рабочей станции:

1. Откройте панель управления Indeed AirCard Enterprise.
2. Нажмите  и  .
3. В поле **Код** введите код, полученный от администратора, выпустившего устройство. Нажмите **Добавить**. Код действителен в течение часа, его можно использовать только один раз. Адрес сервера Indeed AirCard Enterprise подставляется автоматически.

После добавления устройство AirCard отобразится в панели управления. Для удаления устройства нажмите ✕.

В разделе **Активные смарт-карты** панели управления Indeed AirCard Enterprise можно просмотреть устройства, автоматически подключенные к рабочей станции. Для каждого устройства указан ID (серийный номер), который отображается в сервисах Indeed CM.

ПОДСКАЗКА

Индикатор подключенных устройств AirCard находится в области уведомлений панели задач Windows. Если к рабочей станции не подключено ни одного устройства, или связь с Indeed AirCard Enterprise Server не установлена, то индикатор будет серого цвета, если подключено хотя бы одно устройство – красного.

Изменение ответов на секретные вопросы

Чтобы изменить ответы на заданные секретные вопросы:

1. Нажмите **Изменить ответы на секретные вопросы** под информацией о пользователе.
2. Выберите вопрос из списка доступных и задайте ответ на вопрос.
3. Нажмите **ОК** для сохранения изменений.

> **ПРИМЕЧАНИЕ**
>
> Возможность изменения ответов на секретные вопросы настраивает администратор 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

Изменить ответы на секретные вопросы Пользователь КриптоПро 2.0

Секретные вопросы

Секретные вопросы необходимы для подтверждения операций с вашими устройствами

Секретный вопрос

Ваш любимый цвет?

Ответ

ОК Отмена

Обновление устройства

Если срок действия одного или нескольких сертификатов на вашем устройстве подходит к концу, или вам потребовался новый сертификат, то устройство необходимо обновить.

> **ПРИМЕЧАНИЕ**
>
> Вы можете обновить устройство, если администратор задал опцию **Разрешить пользователю обновление устройства** в разделе **Поведение** политики использования устройств.

Для обновления устройства выполните следующие действия:

1. Нажмите **Обновить содержимое устройства** и подключите устройство к компьютеру.
2. Если администратор задал опцию **Разрешить пользователю выбор необязательных сертификатов при обновлении устройства** в разделе **Поведение** политики использования устройств, отобразится окно выбора шаблонов сертификатов.
   Выберите шаблоны, по которым будут сформированы сертификаты для записи на устройство.
3. Если администратор настроил интеграцию в разделе **СМЭВ** политики использования устройств и сертификат выпускается по шаблону для КриптоПро УЦ 2.0 или Валидата УЦ, отобразится форма проверки СМЭВ.
   Вы можете проверить данные на соответствие и изменить их, если администратор задал опцию **Разрешить пользователю редактирование данных в форме проверки в СМЭВ** в разделе **Поведение**.
4. Введите **PIN-код пользователя**.
5. Если на устройство были добавлены сторонние сертификаты, Indeed CM может их обнаружить и внести информацию о таких сертификатах в систему – отследить.
   Окно выбора сертификатов для отслеживания отображается, если администратор задал опцию **Включить отслеживание сертификатов** в разделе **Поведение** политики использования устройств.
   Выберите сертификаты для отслеживания, если они есть на устройстве, и нажмите **Ок**.
6. Нажмите **Обновить**.

Контроль обновления устройства

Обновление устройства может быть приостановлено, если регламент вашей организации предусматривает проверку документов для обновления цифровых сертификатов.

В окне обновления устройства появится сообщение *Обновление устройства ожидает решения*. Устройству присваивается статус **В ожидании**. Это означает, что ваш запрос на обновление устройства перешел в стадию рассмотрения.

Отправьте документы для обновления сертификата:

- с помощью Indeed CM, если настроена функция внутреннего электронного документооборота – **Indeed CM ЭДО**;
- вне Indeed CM любым другим способом, принятым в вашей организации. Например, по электронной почте.

Отправить документы в Indeed CM

Если в Indeed CM настроена функция внутреннего электронного документооборота – **Indeed CM ЭДО**, вы можете подписать и отправить документы для обновления сертификата с помощью Indeed CM в разделе **Ваши документы**.

> **ПОДСКАЗКА**
>
> Настройки одобрения задает администратор Indeed CM в разделе **Шаблоны** политики использования устройств.

В зависимости от настроек, заданных администратором Indeed CM, вам необходимо подписать и загрузить в Indeed CM следующие документы:

Запрос на сертификат

Предоставьте подписанную форму запроса на сертификат для одобрения в удостоверяющем центре (УЦ). Администратор Indeed CM может предварительно проверить запрос на сертификат перед отправкой запроса в УЦ.

Выполните следующие действия:

1. Загрузите подписанный запрос на сертификат в Indeed CM:
    1. Распечатайте запрос на сертификат. Перейдите на вкладку **Содержимое** в карточке устройства и нажмите  напротив сертификата.
    2. Подпишите запрос на сертификат и добавьте в Indeed CM. **Как подписать и загрузить документ в Indeed CM**
2. Дождитесь одобрения запроса на сертификат в УЦ. На вкладке **Содержимое** в карточке устройства можно проверить статус сертификата – **В ожидании**.
3. Если запрос на сертификат одобрен в УЦ, то сертификат получает статус **Одобрен** и записывается на устройство. Перейдите в карточку устройства и нажмите **Продолжить обновление устройства**.
   Если запрос отклонен:
    - отзовите и очистите устройство, затем выпустите его заново;
    - обратитесь к администратору, чтобы отменить обновление устройства, затем начните обновление устройства заново.

> **ПРИМЕЧАНИЕ**
>
> Если администратор Indeed CM настроил автоматическую рассылку уведомлений пользователя по электронной почте, то вам придет уведомление о статусе одобрения – *Одобрение документа*, *Одобрение обновления устройства* или *Отклонение обновления устройства*.
>
> Если автоматическая рассылка уведомлений не настроена, дождитесь появления кнопки **Продолжить обновление устройства** в карточке устройства.

Сертификат

В этом сценарии УЦ одобряет сертификат автоматически. Сертификат записывается на устройство после того, как администратор Indeed CM одобрит подписанную форму сертификата, если дополнительная проверка предусмотрена по регламенту получения сертификата проверки электронной подписи.

Выполните следующие действия:

1. Загрузите подписанную форму сертификата в Indeed CM:
    1. Распечатайте форму сертификата. Перейдите на вкладку **Содержимое** в карточке устройства, нажмите напротив сертификата и выберите **Сертификат**.
    2. Подпишите форму сертификата и добавьте в Indeed CM. **Как подписать и загрузить документ в Indeed CM**
2. Дождитесь одобрения документа от администратора Indeed CM. На вкладке **Содержимое** в карточке устройства можно проверить статус сертификата – **Действителен**. Это означает, что сертификат проверен в УЦ, но ожидает проверки администратора.
3. Если администратор одобрил документ, то сертификат записывается на устройство. Перейдите в карточку устройства и нажмите **Продолжить обновление устройства**.
   Если администратор отклонил документ, отредактируйте его, подпишите и заново загрузите в Indeed CM.

> **ПРИМЕЧАНИЕ**
>
> Если администратор Indeed CM настроил автоматическую рассылку уведомлений пользователя по электронной почте, то вам придет уведомление о статусе одобрения – *Одобрение документа*.
>
> Если автоматическая рассылка уведомлений не настроена, дождитесь появления кнопки **Продолжить обновление устройства** в карточке устройства.

Запрос на сертификат и сертификат

Чтобы продолжить обновление устройства и записать на него сертификат:

1. Предоставьте подписанную форму запроса на сертификат и дождитесь одобрения запроса в УЦ.
2. Предоставьте подписанную форму сертификата и дождитесь одобрения документа от администратора Indeed CM.

Выполните следующие действия:

1. Загрузите подписанную форму запроса на сертификат в Indeed CM:

    1. Распечатайте запрос на сертификат. Перейдите на вкладку **Содержимое** в карточке устройства и нажмите напротив сертификата.
    2. Подпишите запрос на сертификат и добавьте в Indeed CM.**Как подписать и загрузить документ в Indeed CM**

2. Дождитесь одобрения запроса на сертификат в УЦ. На вкладке **Содержимое** в карточке устройства можно проверить статус сертификата – **В ожидании**.

3. Если запрос на сертификат одобрен в УЦ, то сертификат получает статус **Действителен**. Это означает, что сертификат проверен в УЦ и ожидает проверки администратора. Загрузите подписанную форму сертификата в Indeed CM:

    1. Распечатайте форму сертификата. Перейдите на вкладку **Содержимое** в карточке устройства, нажмите напротив сертификата и выберите **Сертификат**.
    2. Подпишите форму сертификата и добавьте в Indeed CM.

    Если запрос отклонен в УЦ:

    - отзовите и очистите устройство, затем выпустите его заново;
    - обратитесь к администратору, чтобы отменить обновление устройства, затем начните обновление устройства заново.

4. Если администратор одобрил подписанную форму сертификата, то сертификат получает статус **Одобрен** и записывается на устройство. Перейдите в карточку

устройства и нажмите **Продолжить обновление устройства**.
Если администратор отклонил документ, отредактируйте его, подпишите и заново загрузите в Indeed CM.

> **ПРИМЕЧАНИЕ**
>
> Если администратор Indeed CM настроил автоматическую рассылку уведомлений пользователя по электронной почте, то вам придет уведомление о статусе одобрения – *Одобрение обновления устройства*, *Одобрение документа* или *Отклонение обновления устройства*.
>
> Если автоматическая рассылка уведомлений не настроена, дождитесь статуса сертификата **Одобрен**.

Отправить документы вне Indeed CM

Предоставьте документы администратору Indeed CM согласно регламенту получения сертификата проверки электронной подписи, принятому в вашей организации.

Выполните следующие действия:

1. Предоставьте администратору Indeed CM подписанную форму запроса на сертификат для одобрения в удостоверяющем центре (УЦ).
2. Дождитесь одобрения запроса на сертификат в УЦ. На вкладке **Содержимое** в карточке устройства можно проверить статус сертификата – **В ожидании**.
3. Если запрос на сертификат одобрен, то сертификат получает статус **Одобрен** и записывается на устройство. Перейдите в карточку устройства и нажмите **Продолжить обновление устройства**.
   Если запрос отклонен:
   - отзовите и очистите устройство, затем выпустите его заново;
   - обратитесь к администратору, чтобы отменить обновление устройства, затем начните обновление устройства заново.

ПРИМЕЧАНИЕ

Если администратор Indeed CM настроил автоматическую рассылку уведомлений пользователя по электронной почте, то вам придет уведомление о статусе одобрения – *Одобрение обновления устройства* или *Отклонение обновления устройства*.

Если автоматическая рассылка уведомлений не настроена, дождитесь появления кнопки **Продолжить обновление устройства** в карточке устройства.

Выключение и включение устройств

Устройство пользователя можжно выключить на определенный промежуток времени (например, на период отпуска) и затем снова включить.

В зависимости от настроек политики использования устройств вам доступны следующие действия:

- выключение и включение устройства
- только выключение устройства
- только включение устройства

> **ПРИМЕЧАНИЕ**
>
> Чтобы выключить и включить устройство, его не нужно подключать к рабочей станции.

Для выключения устройства, нажмите **Временно выключить устройство** в меню устройства. Нажмите **Выключить**. Статус устройства изменится с **Выпущено** на **Выключено**.

Для включения устройства, нажмите **Включить устройство** в меню устройства. Нажмите **Включить**. Статус устройства изменится с **Выключено** на **Выпущено**.

> **ПРЕДУПРЕЖДЕНИЕ**
>
> 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.

Выключение устройств без выполнения входа в систему

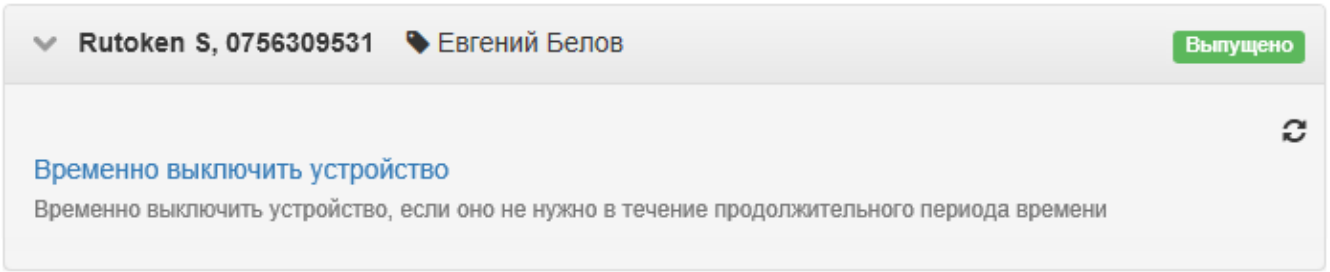
В экстренном случае пользователь может самостоятельно выключить устройство без входа в операционную систему, если администратор разрешил выключение устройства.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Выключение устройства доступно только в том случае, если у рабочей станции, с которой осуществляется операция, есть связь с сервером Indeed CM, и у пользователя настроены секретные вопросы.

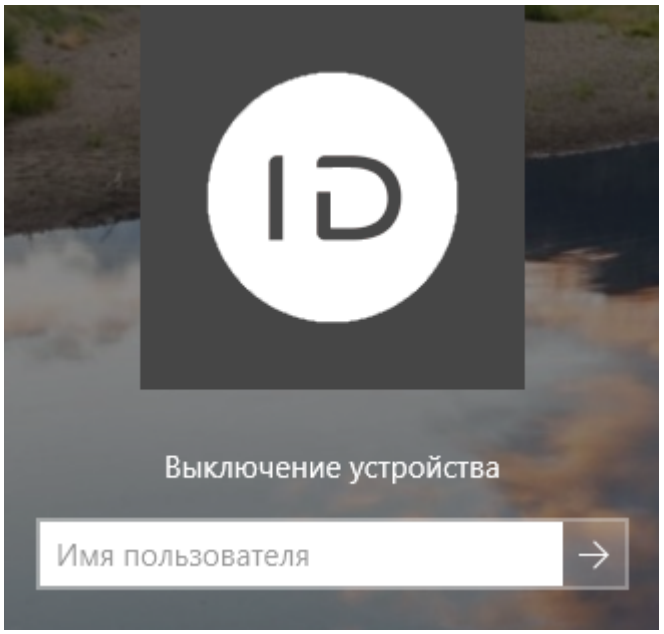
Ниже приведен пример выключения устройства для операционной системы Windows 10. Механизм выключения в операционных системах Windows 7 и Windows 8 выглядит похожим образом.

Чтобы выключить устройство:

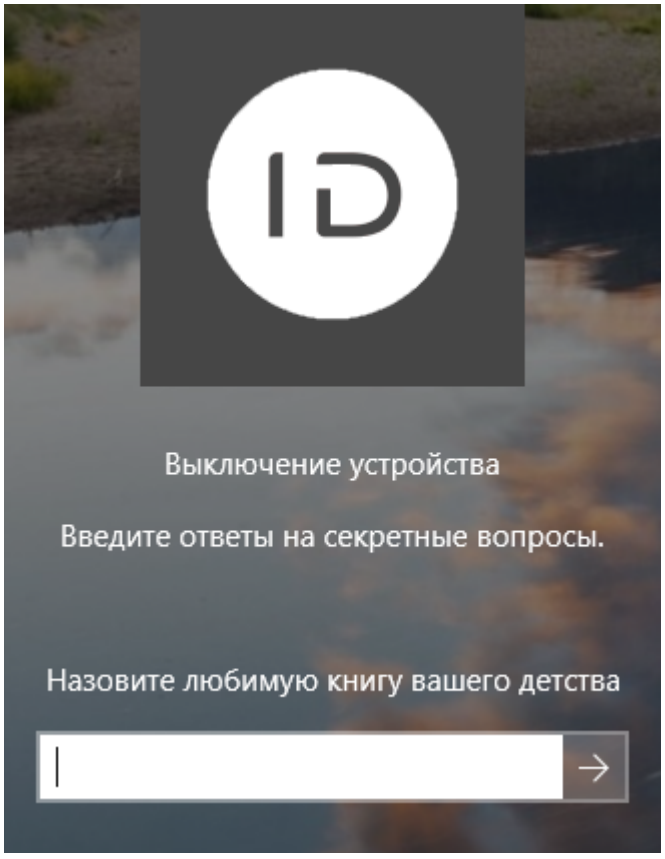
1. Выберите **Выключение устройства** на экране выбора пользователей.



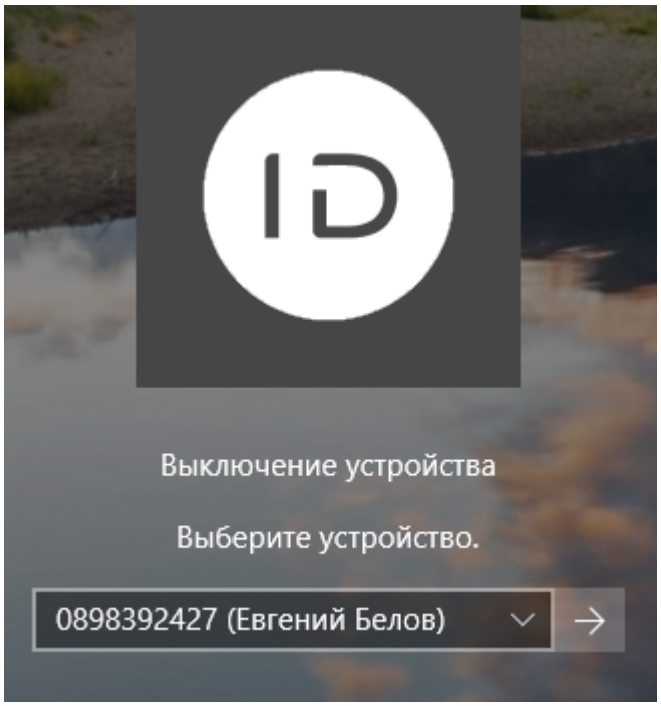
2. Укажите ваше имя пользователя и устройство, которое необходимо выключить.



3. Введите ответы на секретные вопросы.



4. Выберите устройство из списка выпущенных устройств пользователя и нажмите  .


Выключение устройства
Выберите устройство.
0898392427 (Евгений Белов)

Отзыв и очистка устройств

Устройство пользователя можно отозвать в случае его повреждения, утери или компрометации.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> 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 CM.

Для отзыва устройства выполните следующие действия:

1. Нажмите **Сообщить о том, что устройство неисправно, утеряно или скомпрометировано**.
2. Укажите причину отзыва:

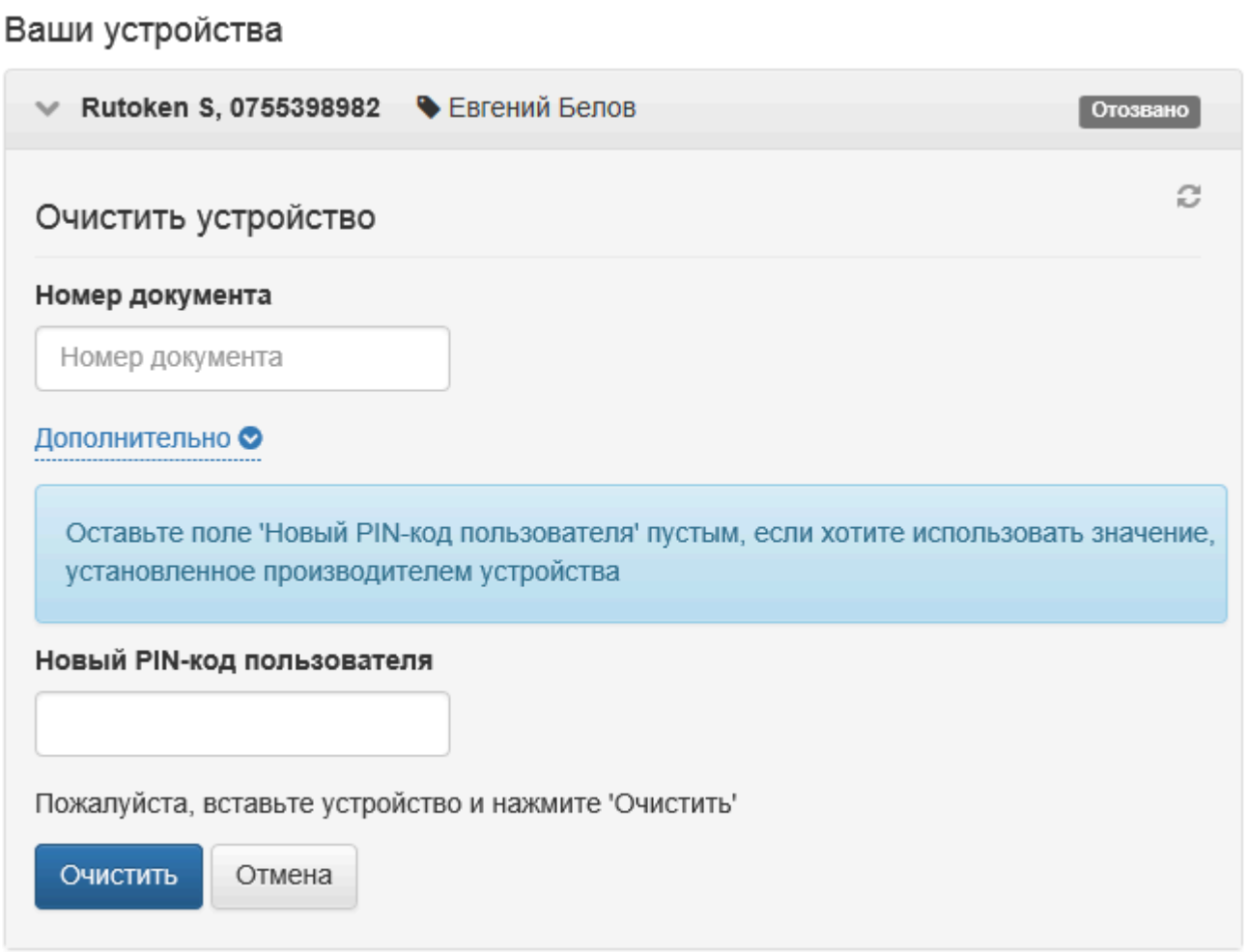
- устройство неисправно
- устройство утеряно
- компрометация устройства

3. Нажмите **Отозвать**.

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**.

> ⓘ **ПРИМЕЧАНИЕ**
>
> Для очистки и удаления устройств TPM, Registry, Windows Hello for Business нажмите **Удалить устройство**.



> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> При очистке устройства все данные, записанные на него в 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 можно изменить PIN-код пользователя. Indeed CM может изменить его на значение по умолчанию или на значение, соответствующее политике безопасности вашей компании (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. Нажмите **Очистить**.

После очистки устройство останется закрепленным за вами в Indeed CM, и его можно выпустить повторно (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, чтобы разблокировать устройство.

> **ПРИМЕЧАНИЕ**
>
> Возможность сброса PIN-кода настраивает администратор Indeed CM в политике использования устройств в разделе **Поведение**.

Сброс

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 **Закрыть**.

Изменение

Для изменения PIN-кода устройства выполните следующие действия:

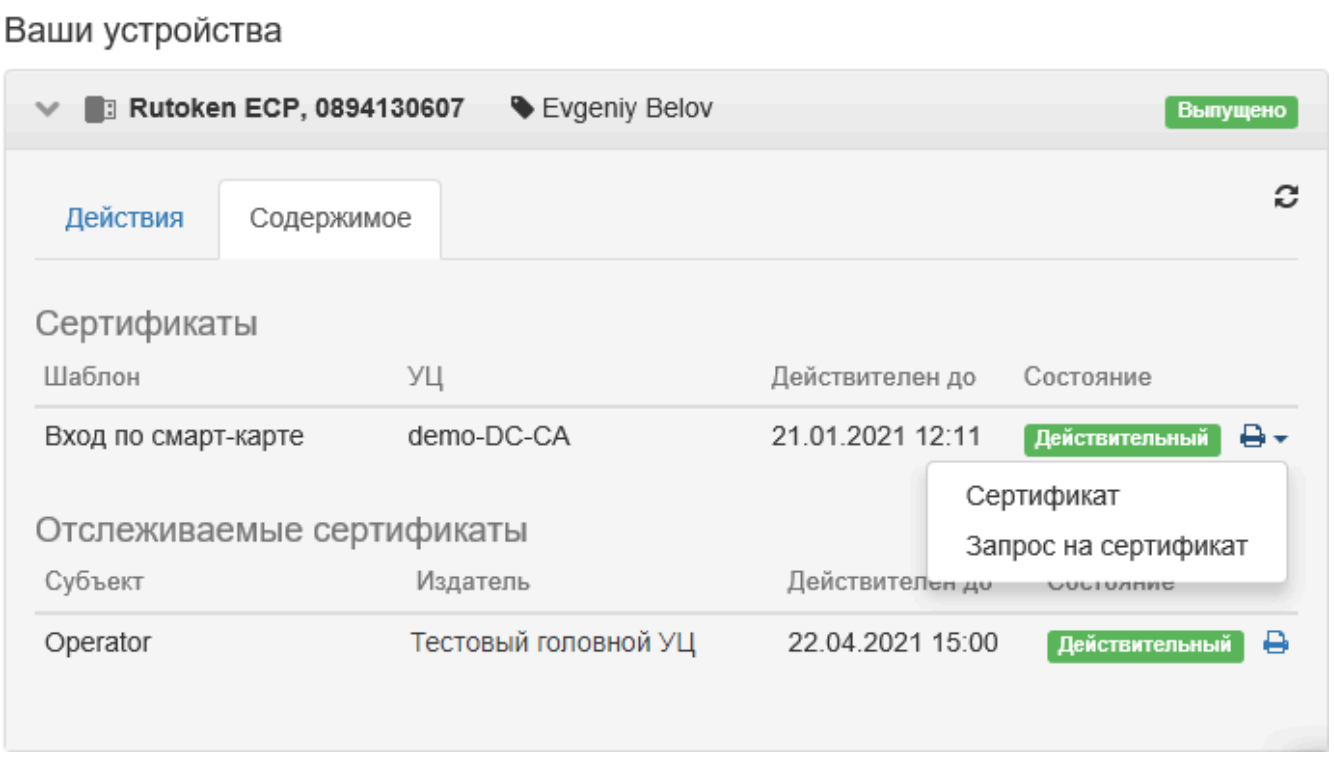
1. Нажмите **Изменить PIN-код устройства**.
2. Подключите устройство к компьютеру.
3. Введите текущий PIN-код, задайте новый PIN-код и подтвердите его.
4. Нажмите **Изменить**.
5. После того, как PIN-код будет изменен, нажмите **Закрыть**.

Просмотр содержимого устройства

Если в настройках системы разрешено отображение содержимого устройства в Сервисе самообслуживания, то в свойствах выпущенного устройства будет доступна вкладка **Содержимое** с информацией о сертификатах на устройстве.

> **ПОДСКАЗКА**
>
> Опцию **Просмотр содержимого устройства** включает администратор в разделе **Общие функции** Мастера настройки Indeed CM.

При необходимости пользователь может распечатать сведения о сертификате и его запросе. Для печати нажмите .



СКЗИ

В сервисе самообслуживания пользователь может просмотреть и распечатать нормативные документы назначенных ему СКЗИ.

> **ПОДСКАЗКА**
>
> Раздел **Ваши СКЗИ** доступен, если администратор включил опцию **Разрешить пользователю просмотр СКЗИ** в разделе **Поведение** политики использования устройств.

Чтобы распечатать документ СКЗИ:

1. Нажмите  напротив выбранного СКЗИ.
2. Выберите вид нормативного документа или шаблон печати.

> **ПОДСКАЗКА**
>
> Выпадающий список **Вид нормативного документа** отображается, если администратор определил шаблон печати для выбранного типа СКЗИ в текущем состоянии.
>
> Выпадающий список **Шаблон печати** отображается, если администратор не определил шаблон печати для выбранного типа СКЗИ в текущем состоянии. В этом случае вы можете выбрать любой из шаблонов, доступных для этого типа СКЗИ.

3. Нажмите **Распечатать документ**.

Документы

Если в конфигурации Indeed CM настроена функция внутреннего электронного документооборота – **Indeed CM ЭДО**, вы можете работать с документами по получению сертификата в Сервисе самообслуживания.

Поддерживаются документы следующих типов:

- **персональные данные** – копии документов, удостоверяющих личность: паспорт гражданина РФ, СНИЛС, ИНН;
- **запрос на сертификат** – подписанная копия заявления на создание сертификата ключа проверки электронной подписи;
- **сертификат** – подписанная копия сведений о сертификате ключа проверки электронной подписи;
- **запрос на отзыв сертификата** – подписанная копия заявления на прекращение действия сертификата ключа проверки электронной подписи;
- **пользовательские** – другие виды документов, например, подписанный регламент удостоверяющего центра.

Документы можно добавить, скачать, редактировать и удалить.

> **ПРИМЕЧАНИЕ**
>
> Удаление документов доступно, если администратор включил опцию **Разрешить пользователю удаление документа** в разделе **Поведение** Консоли управления Indeed CM.

При работе с документами в Indeed CM у вас есть следующие возможности:

- загрузить документ, подписанный на бумаге;
- загрузить документ и подписать его электронной подписью (ЭЦП), если у вас есть устройство с сертификатом ключа проверки электронной подписи (далее – сертификат подписи);
- открыть содержимое устройства, распечатать документ и подписать его электронной подписью.

Загрузка документа, подписанного на бумаге

Чтобы загрузить документ, подписанный на бумаге:

1. Нажмите **Добавить документ** в разделе **Ваши документы**.
2. Выберите тип документа.
3. Загрузите файл документа.
4. Заполните поле **Описание** (необязательно).
5. Нажмите **Добавить**.

Загрузка и подпись документа ЭЦП

При добавлении документа вы можете подписать его электронной подписью.

> ⚠ **ТРЕБОВАНИЯ ДЛЯ ПОДПИСИ ДОКУМЕНТОВ В INDEED CM**
>
> - у вас есть устройство, которое содержит сертификат подписи;
> - сертификат подписи имеет любой статус, кроме **Отозван**, **Истек** и **Ключ истек**.

Чтобы загрузить и подписать документ:

1. Нажмите **Добавить документ** в разделе **Ваши документы**.
2. Выберите тип документа и загрузите файл документа.
3. Заполните поле **Описание** (необязательно).
4. Включите опцию **Подписать документ**.
5. Подключите устройство с сертификатом подписи к рабочей станции и выберите его в выпадающем списке **Устройство**.
6. В выпадающем списке **Сертификат** выберите подходящий сертификат.
7. Введите PIN-код пользователя.
8. Нажмите **Добавить**.

Подпись документа ЭЦП без загрузки файла документа

Если на вашем устройстве уже есть документ, который нужно подписать, то вам не нужно загружать этот документ в Indeed CM. Вы можете найти документ в содержимом устройства и подписать его ЭЦП.

Поддерживаются следующие виды документов:

- сертификат;
- запрос на сертификат;
- запрос на отзыв сертификата.

Чтобы подписать документ:

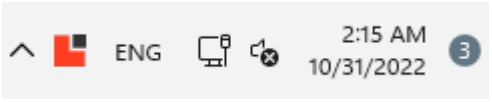
1. В разделе **Ваши устройства** выберите устройство, на котором содержится нужный сертификат, и перейдите на вкладку **Содержимое**.
2. Нажмите  напротив нужного сертификата и выберите документ: сертификат, запрос на сертификат или запрос на отзыв сертификата.
3. В открывшемся окне нажмите **Подписать документ** или **Скачать**.
4. Подключите устройство с сертификатом подписи к рабочей станции и выберите его в выпадающем списке **Устройство**.
5. В выпадающем списке **Сертификат** выберите подходящий сертификат.
6. Введите PIN-код пользователя.
7. Нажмите **Подписать**.

Подписанный документ автоматически появится в списке **Ваши документы**. В описании будет указан серийный номер устройства и название шаблона, по которому сформирован и подписан документ.

Клиентский агент Indeed CM

На рабочую станцию пользователя можно установить клиентский агент Indeed CM, который позволит администраторам назначать задачи для устройств пользователя и выполнять их в полностью автоматическом или полуавтоматическом режиме.

Агент запускается автоматически. В области уведомлений отображается логотип , когда агент активен.

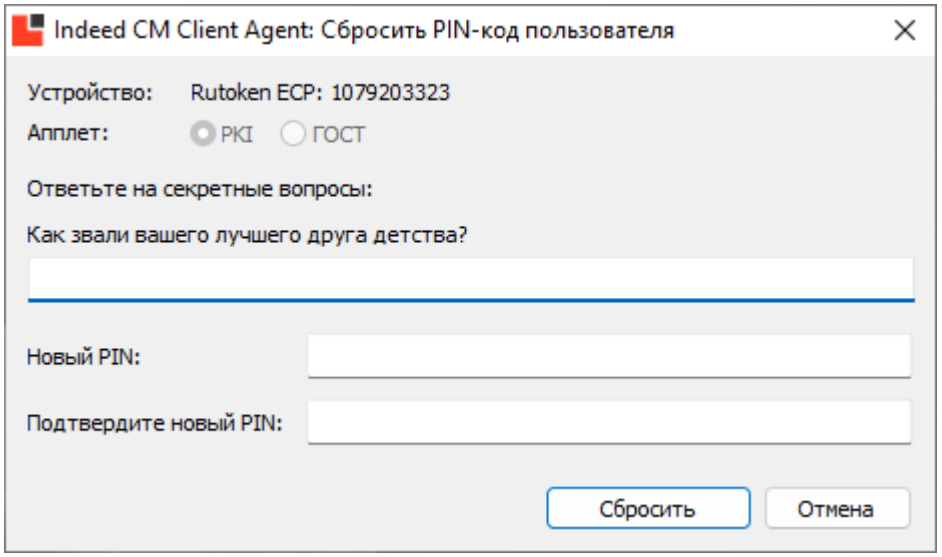


Задачи, требующие действия пользователя:

- сброс и разблокировка
- обновление содержимого устройства

Сброс и разблокировка PIN-кода

Если вы забыли PIN-код устройства или заблокировали его, сообщите об этом администратору. Он создаст задачу по сбросу PIN-кода для вашего устройства. Подключите его к компьютеру и дождитесь появления формы сброса PIN-кода.



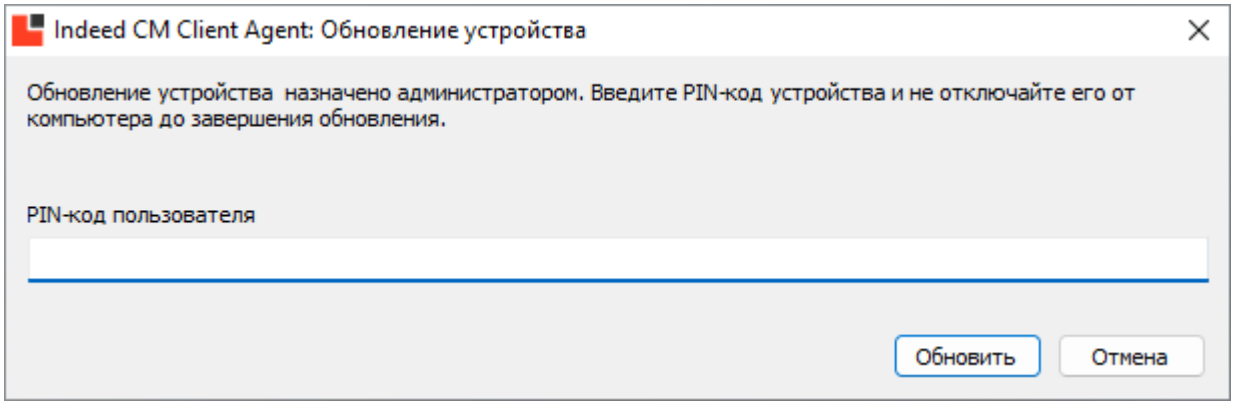
> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Для сброса PIN-кода у вас должны быть заданы ответы на секретные вопросы. Если вы не помните ответы, измените их в Сервисе самообслуживания.

Введите ответ на один или несколько секретных вопросов, задайте новый PIN-код, его подтверждение и нажмите **Сбросить**. В случае успешного сброса появится сообщение *PIN-код пользователя на устройстве успешно сброшен*.

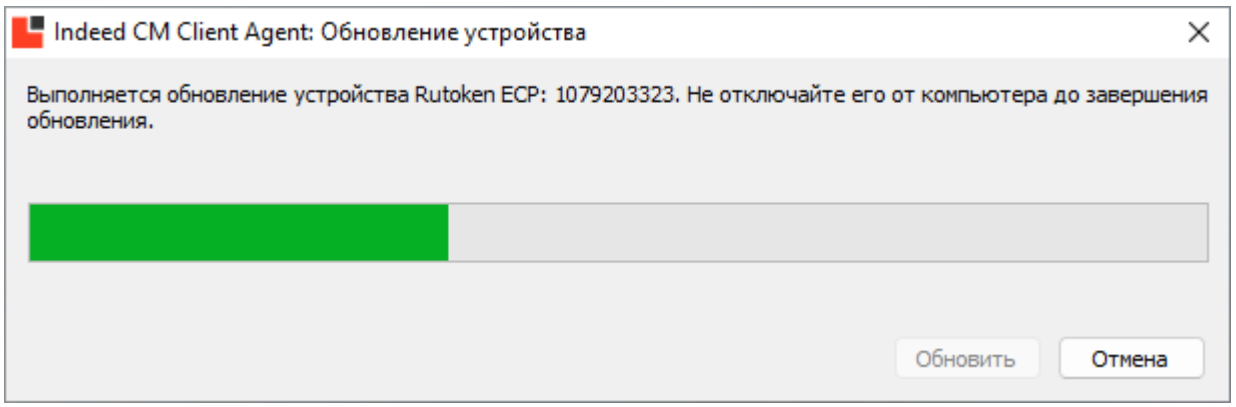
Обновление содержимого устройства

Обновление устройства может потребоваться, если срок действия одного или нескольких сертификатов на устройстве подходит к концу, или вам потребовался другой сертификат.

Администратор Indeed CM создаст задачу по обновлению содержимого вашего устройства. Подключите устройство к компьютеру, появится форма обновления.



Введите PIN-код и нажмите **Обновить**. После этого начнется процесс обновления содержимого устройства. Обновление может длиться несколько минут.



После успешного завершения обновления отобразится сообщение *Устройство успешно обновлено*.

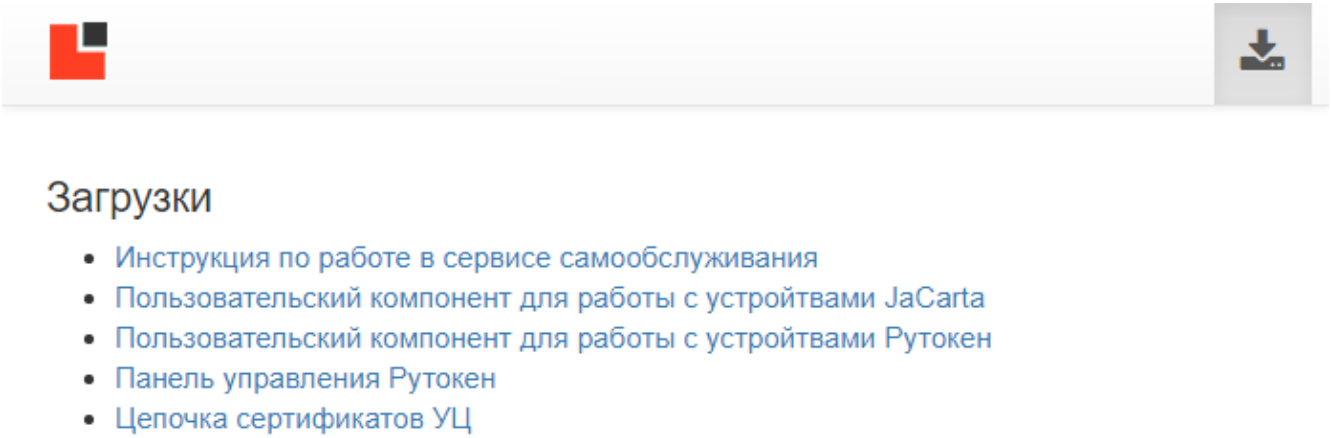
В случае ошибки обновления ее текст появится в информационном сообщении.

Загрузка файлов и ресурсов

Если при настройке системы администратор добавил файлы и/или ссылки для использования в Сервисе самообслуживания, то пользователь может найти их по ссылке *https://<FQDN сервера Indeed CM>/cm/ss/Downloads* или личном кабинете под кнопкой .

> **ПОДСКАЗКА**
>
> Опцию **Загрузка файлов и ресурсов** включает администратор в разделе **Общие функции** Мастера настройки Indeed CM.

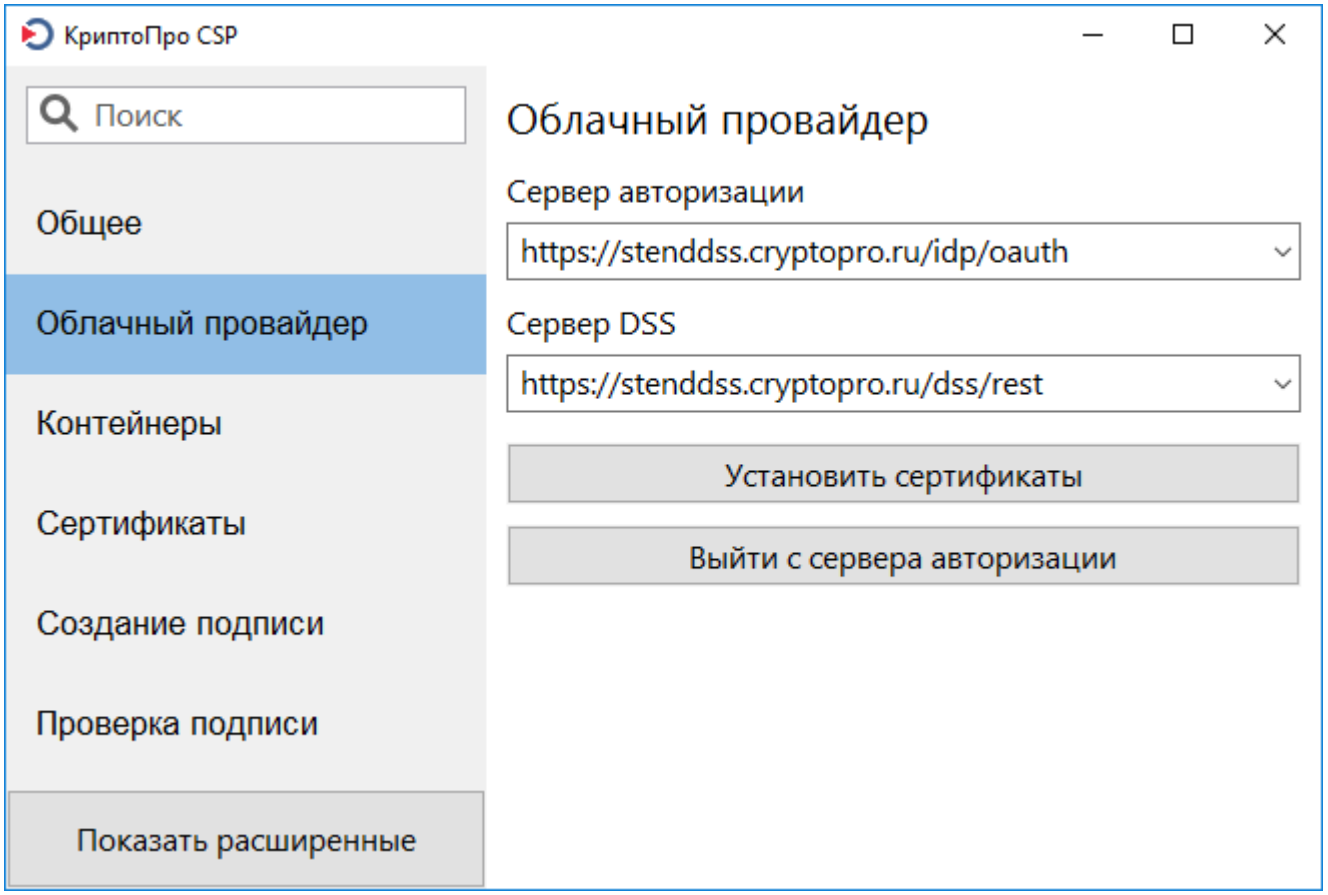
На странице **Загрузки** будут доступны ресурсы, добавленные администратором.



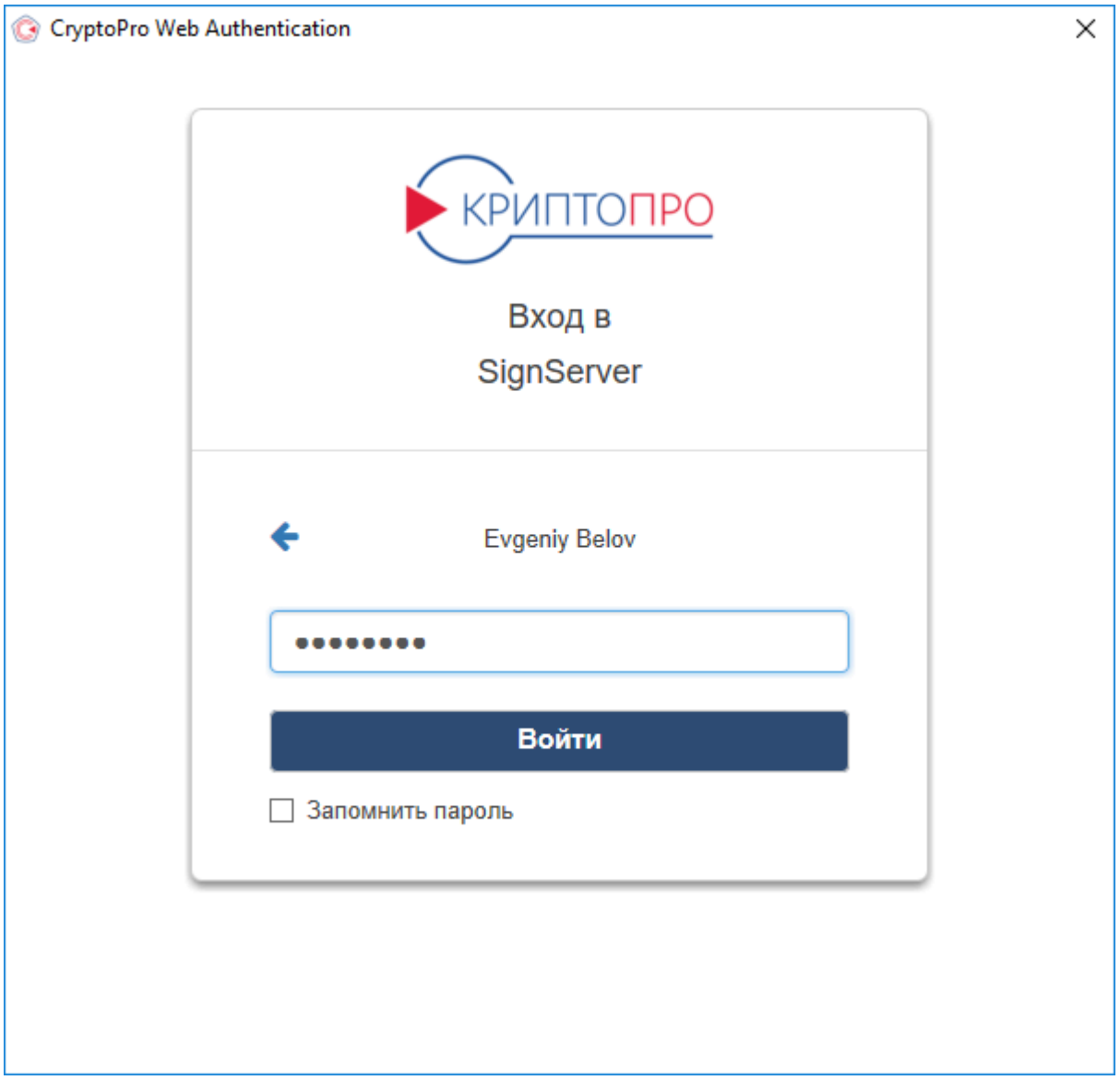
Если добавлен файл, то при нажатии на ссылку начнется его скачивание, если веб-страница - то она откроется в новой вкладке.

Выгрузка сертификата DSS

Для выгрузки сертификата из облачного хранилища запустите компонент **Инструменты КриптоПро** и перейдите в раздел **Облачный провайдер**, укажите URL-адрес для сервера авторизации и сервера DSS.



Нажмите **Установить сертификат**, введите логин и пароль от личного кабинета пользователя DSS, и нажмите **Войти**.


CryptoPro Web Authentication
КРИПТОПРО
Вход в
SignServer
Evgeniy Belov
Войти
Запомнить пароль

API

Набор API-функций позволяет управлять устройствами с помощью клиентских приложений.

Доступ к API-функциям осуществляется через веб-приложение **API**.

Приложение **API** входит в состав сервера Indeed Certificate Manager и доступно по адресу: *https://<FQDN сервера Indeed CM>/cm/api*.

Для взаимодействия с Indeed CM через API в разделе **Конфигурация** → **Роли** Консоли управления необходимо создать сервисную роль, включить в нее учетную запись, от имени которой будет производиться обращение по API, и определить для роли следующие привилегии:

- поиск пользователей;
- просмотр репозитория устройств;
- выключение устройства;
- включение устройства;
- обновление устройства;
- сброс PIN-кода;
- блокировка устройства;
- отзыв устройства;
- удаление задачи.

Cards

Получить список устройств, добавленных в Indeed CM.

Тип запроса: GET.

Параметры:

- без указания параметров;
- `offset` – сдвиг на указанное количество устройств;
- `count` – количество выводимых устройств;
- `serialNumber` – серийный номер устройства;
- `cardTypeName` – тип устройств;

- `userName` – имя пользователя устройства в форматах имени входа нижнего уровня (DOMAIN\LogonName) или имени участника-пользователя (UPN);
- `comment` – комментарий к устройствам;
- `tags` – теги устройств;
- `state` – состояние устройств:
  - clean – пустое;
  - assigned – назначено;
  - pending – в ожидании;
  - issued – выпущено;
  - disabled – выключено;
  - revoked – отозвано;
- `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 IDPrimeMD, 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;
- `userId` – идентификатор пользователя, на которого назначено устройство;
- `userName` – имя пользователя устройства в формате имени входа нижнего уровня (DOMAIN\LogonName);
- `policyId` – идентификатор политики использования устройства;
- `policyName` – название политики использования устройства;
- `certificates`:
  - type – тип сертификата;
  - serialNumber – серийный номер сертификата;
  - thumbprint – отпечаток сертификата;
  - subject – общее имя (CN) субъекта сертификата;
  - issuer – общее имя (CN) издателя сертификата;
  - validTo – срок действия сертификата в формате ISO 8601.

> **ПРИМЕР ВЫЗОВА**
>
> http://localhost/cm/api/Cards – вывод всех устройств;
> http://localhost/cm/api/Cards?offset=0&count=50 – вывод 50 устройств без сдвига.

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/cm/api/cards/1/revoke

Тело запроса: причина отзыва устройства. Например, { reason: 5 }.

Cards/{id}/Disable

Временно отключить устройство пользователя.

Тип запроса: POST.
Параметры: `id` – идентификатор устройства.
Возвращаемые значения: нет.

> **ПРИМЕР ВЫЗОВА**
>
> http://localhost/cm/api/cards/1/disable

Cards/{id}/Enable

Включить устройство пользователя.

Тип запроса: POST.
Параметры: `id` – идентификатор устройства.
Возвращаемые значения: нет.

ПРИМЕР ВЫЗОВА

http://localhost/cm/api/cards/1/enable

Cards/{id}/Preupdate

Отозвать неактуальный сертификат пользователя.

ПРЕДУПРЕЖДЕНИЕ

Метод **Preupdate** можно использовать 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 сертификат 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/cm/api/cards/1/preupdate

Перенос данных из сторонних систем

Aladdin JMS

Миграция данных из Aladdin JaCarta Management System в Indeed CM

SafeNet Authentication Manager

Миграция данных из SafeNet Authentication Manager в Indeed CM

Aladdin JMS

Миграция данных не затрагивает базу данных JMS — состояние и содержимое устройств остаются неизменными. После переноса в Indeed CM для всех перенесенных устройств и сертификатов доступны все возможные операции: выпуск, обновление содержимого, отзыв и другие.

Утилита миграции переносит в Indeed CM следующие 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

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Для JaCarta PKI/ГОСТ информация о приложении ГОСТ-апплете не импортируется. В Indeed CM возможны операции только с PKI-областью устройства.

В Indeed CM не переносятся следующие данные:

- Метки АМДЗ Аккорд
- Сертификаты Валидата УЦ
- Сертификаты КриптоПро УЦ

Если такие данные есть на устройстве, то они не отображаются в Indeed CM после переноса, но остаются на устройстве.

Предварительные настройки

Миграция данных возможна при соблюдении условий:

- У 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** Мастера настройки Indeed CM.
- В разделе **Конфигурация** → **Типы устройств** Indeed CM добавлены все типы устройств JaCarta, которые используются в JMS.
- В Indeed CM есть свободные лицензии: в разделе **Конфигурация** → **Лицензии** есть действующая лицензия на достаточное количество пользователей.
- На 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.

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 другие.

Каждая политика имеет область действия. Для каталога пользователей Indeed CM в Active Directory областью действия может быть:

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

Для всех пользователей в пределах области действия политики будут выпускаться устройства с параметрами, определенными в этой политике. Политика может распространяться как на весь объект целиком (домен, контейнер или подразделение), так и на отдельные группы пользователей внутри него. Если пользователь попадает под действие нескольких политик выпуска устройств (например, состоит в двух группах в одном подразделении), применяется политика с наивысшим приоритетом.

Перед миграцией данных из JMS заранее создайте одну или несколько политик использования устройств в Indeed CM. Настройте в политике 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.

Процесс миграции

1. Настройте файл конфигурации утилиты миграции.
2. Запустите утилиту миграции.

Настройка файла конфигурации утилиты миграции

Для работы утилиты заполните файл конфигурации *IndeedCM.Migrate.JMS.exe.config*, находящийся в каталоге с утилитой.

1. Заполните параметры в 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 установится на устройстве после его переноса в Indeed CM.
   - `issuedTokenAdminPin` — если ключевой носитель в JMS находится в любом другом состоянии и выпускался без инициализации, то в параметре задается PIN-код администратора, который установится на устройстве после его переноса в Indeed CM.
2. В секции `<sqlPersistenceSettings>` заполните параметры подключения к базе данных Indeed CM. Всю секцию можно перенести из файла конфигурации *Web.config* веб-приложения mc (Консоль управления).
3. В секции `<adUserCatalogSettings>` заполните параметры подключения к каталогу пользователей. Всю секцию можно перенести из файла конфигурации *Web.config* веб-приложения mc (Консоль управления).

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> 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 миграции

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 рабочей базы данных.

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]`.

SafeNet Authentication Manager

Предварительные настройки

Для миграции данных из SafeNet Authentication Manager в Indeed CM убедитесь, что выполнены следующие предварительные условия:

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

Процесс миграции

1. Настройте Indeed CM для работы с данными из SAM.
2. Создайте политики использования устройств.
3. Настройте утилиту миграции IndeedCM.Migrate.SAM:

    1. Заполните файл конфигурации *IndeedCM.Migrate.SAM.exe.config*.
    2. Заполните файл конфигурации *unity.config*.
    3. Запустите процесс миграции.

Настройка Indeed CM для работы с данными из SAM

Прежде чем приступить к выгрузке данных из SAM, подготовьте Indeed CM к приему данных. Убедитесь, что выполнены следующие условия:

1. Каталог пользователей Indeed CM совпадает с каталогом пользователей SAM. Путь к каталогу задается в Мастере настройки в разделе **Каталог пользователей**.

2. В разделе **Конфигурация → Лицензии** есть действующая лицензия на достаточное количество пользователей.
3. В разделе **Конфигурация → Типы устройств** добавлены все типы устройств eToken, которые используются в SAM.
4. Для всех пользователей, устройства которых будут переноситься из SAM, созданы и назначены политики использования устройств в Indeed CM.

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 другие.

Каждая политика имеет область действия. Для каталога пользователей Indeed CM в Active Directory областью действия может быть:

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

Для всех пользователей в пределах области действия политики будут выпускаться устройства с параметрами, определенными в этой политике. Политика может распространяться как на весь объект целиком (домен, контейнер или подразделение), так и на отдельные группы пользователей внутри него. Если пользователь попадает под действие нескольких политик выпуска устройств (например, состоит в двух группах в одном подразделении), применяется политика с наивысшим приоритетом.

Перед миграцией данных из SAM заранее создайте одну или несколько политик использования устройств в Indeed CM. Настройте в политике 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.

Утилита миграции

Данные из SAM переносятся с помощью утилиты *IndeedCM.Migrate.SAM.exe*, расположенной в дистрибутиве сервера Indeed Certificate Manager (каталог *Misc\SAMMigration*). Для работы

утилиты заполните файлы конфигурации *IndeedCM.Migrate.SAM.exe.config* и *IndeedCM.Migrate.SAM.unity.config*.

IndeedCM.Migrate.SAM.exe.config

Откройте файл *SAMMigration\IndeedCM.Migrate.SAM.exe.config* от имени администратора в текстовом редакторе и заполните следующие секции:

- `samSettings` – параметры подключения к хранилищу данных SAM.
- `MsCAConnectorId` – идентификатор коннектора к Microsoft CA. Значение параметра можно найти в файле XML коннектора в каталоге SAM.
  Путь по умолчанию:
  C:\ProgramFiles\SafeNet\Authentication\SAM\x64\Bin\MsCAConnectorDescriptor.xml.
  Значение по умолчанию: {1A30B883-CD69-4cbb-8D61-E72E9697D8B1}.
- `connectionString` - путь к файлу XML (в названии файла имя домена, в котором развернут SAM) с информацией для подключения к SAM серверу.
  Путь по умолчанию *C:\ProgramData\SafeNet\Authentication\SAM*.
- `migrateSAMSettings` – параметры переноса данных.
- `ignoreCMCertificateTemplateNotFoundError` – параметр импорта устройств. Процесс импорта карт не останавливается. Может иметь два значения:
  - `true` – из SAM импортируется устройство вместе с сертификатами, 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. Значение по умолчанию.
- `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 его переноса 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 его переноса 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).

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Значение ATR для каждого устройства можно получить у производителя или при помощи стороннего ПО, обратившись в службу технической поддержки компании Индид.
>
> 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 переносятся в хранилище Indeed CM, а утилита выводит соответствующую ошибку.

- `adPersistenceSettings` – параметры подключения к хранилищу данных Indeed CM в Active Directory. Содержимое секции должно полностью совпадать с содержимым одноименной секции файла конфигурации Консоли управления Indeed CM (*mc\Web.config*).
- `sqlPersistenceSettings` – параметры подключения к хранилищу данных Indeed CM в Microsoft SQL. По умолчанию секция закомментирована символами `<! - - . . . - - >`. Содержимое секции должно полностью совпадать с содержимым одноименной секции файла конфигурации Консоли управления Indeed CM (*mc\Web.config*).
- `adUserCatalogSettings` – параметры подключения к каталогу пользователей Indeed CM в Active Directory. Содержимое секции должно полностью совпадать с содержимым одноименной секции файла конфигурации Консоли управления Indeed CM (*mc\Web.config*).

Сохраните изменения.

Пример файла IndeedCM.Migrate.SAM.exe.config

```
<samSettings MsCAConnectorId="{1A30B883-CD69-4cbb-8D61-E72E9697D8B1}"
connectionString="C:\ProgramData\SafeNet\Authentication\SAM\demo.local
/>
<migrateSAMSettings ignoreCMCertificateTemplateNotFoundError="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 OS755"
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="11d2f5051684451860ad177ebc39b55cacaf2a0a843b05ddf273b955c93
/>
<adUserCatalogSettings>
<rootContainers>
<container path="LDAP://OU=SAM_USERS,DC=demo,DC=local"
userName="DEMO\cmadmin"
password="Password1" />
</rootContainers>
</adUserCatalogSettings>
```

IndeedCM.Migrate.SAM.unity.config

Откройте файл *SAMMigration\unity.config* от имени администратора в текстовом редакторе и заполните секцию `container`:

- Все строки до `<register type="ISAMDbContext". . . />` должны совпадать с теми, что указаны в файле конфигурации Консоли управления Indeed CM (*mc\unity.config*).

  > ⚠ **ПРЕДУПРЕЖДЕНИЕ**
  >
  > Добавлять секции, которых по умолчанию нет в *unity.config* утилиты миграции (но есть в *mc\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 файл CSV, созданный в папке расположения утилиты с именем *IndeedCM.Migrate.SAM.Report_dd-MM-yyyy_HH-mm-ss.csv*. По умолчанию отчет не создается.

- `<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 *`<! - - . . . - ->`.

  > ⚠ **ПРЕДУПРЕЖДЕНИЕ**
  >
  > 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 изменения.

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.Utils.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

Чтобы запустить процесс миграции данных:

1. Войдите на сервер SAM под сервисной учетной записью SAM (Service Account).
2. Запустите утилиту в тестовом режиме в командной строке Windows от имени администратора.

   ```
   IndeedCM.Migrate.SAM.exe /test
   ```

   Тестовый запуск утилиты требуется для генерации отчета об устройствах и сертификатах, которые будут перенесены в ходе миграции, а также для вывода информации по ошибкам. В этом режиме работы утилиты данные не переносятся с репозиториев, и не заносятся события в журнал.
3. Если в тестовом режиме не было критических ошибок, продолжите миграцию. Запустите утилиту *IndeedCM.Migrate.SAM.exe* в командной строке Windows от имени администратора.

В ходе работы утилита отображает выполняемые действия с устройствами и выводит сведения об ошибках.

Если в файле конфигурации *IndeedCM.Migrate.SAM.exe.config* включена опция ведения отчета, то в каталоге с утилитой миграции автоматически создается файл отчета *IndeedCM.Migrate.SAM.Report_dd-MM-yyyy_HH-mm-ss.csv*.

Пример содержимого файла отчета в 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').

Запись событий миграции в журнал

События успешности или ошибки переноса данных можно записать в журнал на сервере Indeed CM. Для записи событий используется компонент Indeed CM EventLog Proxy.

Чтобы настроить запись событий утилиты миграции данных в журнал событий сервера Indeed CM:

1. Откройте файл *SAMMigration\IndeedCM.Migrate.SAM.exe.config* от имени администратора в текстовом редакторе 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` файла *web.config* приложения Indeed CM EventLog Proxy).
   - `password` - пароль учетной записи, используемой для подключения к сервису.

   Пример заполненной секции

   ```
   <proxyServer url="https://server.demo.local/eventlogproxy"
   userName="DEMO\Administrator" password="P@ssw0rd" />
   ```

2. Сохраните изменения.

3. Установите компонент IndeedCM.EventLog.Proxy на сервер Indeed CM. Как установить Indeed CM EventLog Proxy.

4. Откройте файл *C:\inetpub\wwwroot\eventlogproxy\Web.config* от имени администратора в текстовом редакторе 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.

Дополнительные инструкции

Работа с ключевыми носителями

Использование устройств JaCarta, eToken и IDPrime MD в Indeed CM

Indeed CM Client Browser Extension

Поддержка множественных сессий пользователей на терминальном сервере

Indeed CM Card Template Designer

Утилита для создания шаблонов печати

Работа с ключевыми носителями

Данное руководство предназначено для администраторов предприятий и поможет ознакомиться с подготовкой и использованием устройств JaCarta, eToken и IDPrime MD в Indeed Certificate Manager.

Indeed CM взаимодействует с устройствами с помощью компонента IndeedCM.Middleware.

Для работы с ключевыми носителями установите на рабочие станции операторов и пользователей Indeed CM следующие компоненты:

- **Единый клиент JaCarta** для устройств JaCarta,
- **SafeNet Authentication Client** для устройств eToken.

Работа с устройствами JaCarta

Особенности работы с ГОСТ-областью

При использовании устройств **JaCarta с PKI/ГОСТ-областями** и **JaCarta-2 с PKI/ГОСТ1/ГОСТ2-областями** следует учитывать следующие особенности:

JaCarta PKI/ГОСТ

- PIN-код администратора области ГОСТ по умолчанию меняется на случайный после добавления устройства в Indeed Certificate Manager. При удалении устройства из Indeed CM с подключением устройства к рабочей станции случайный PIN-код администратора области ГОСТ меняется на значение, указанное в разделе **Конфигурация → Типы устройств**.
- PIN-код пользователя для области ГОСТ можно установить и изменить только при инициализации устройства после выпуска устройства.
- При изъятии у пользователя устройства с подключением к рабочей станции нужно 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. Чтобы выпустить такое устройство повторно, устройство нужно инициализировать, и будет задан новый PIN-код пользователя для области ГОСТ, известный пользователю и/или оператору.

- При разблокировке области ГОСТ PIN-код пользователя не меняется. На счетчике попыток ввода PIN-кода до блокировки устройства устанавливается 10 попыток.

Для PIN-кода пользователя области ГОСТ в политиках Indeed CM не поддерживаются следующие опции:

- 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 в политиках Indeed CM поддерживаются следующие опции:

- 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.

JaCarta-2 PKI/ГОСТ1/ГОСТ2

- 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).

- PIN-коды пользователя для обоих ГОСТ-областей можно установить или изменить только при инициализации устройства (при выпуске смарт-карты с включенной опцией **Инициализировать устройство**), при этом содержимое устройства для ГОСТ2-области не будет очищено. Новое значение PIN-кода необходимо указать в параметрах инициализации для устройств JaCarta-2.

- 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 нельзя, т.е. все устройства JaCarta-2 после добавления в Indeed CM будут иметь PIN-код администратора, заданный производителем (**1234567890**).

  Чтобы сменить PIN-код администратора ГОСТ1:

  - измените PUK-код через АРМ-администратора JaCarta (предоставляется разработчиком устройств JaCarta),
  - измените 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.

- 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

При добавлении в Indeed Certificate Manager устройства JaCarta не разделяются по моделям.

Чтобы разделить устройства по моделям и установить параметры инициализации для каждой модели, выполните следующие действия:

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>
```

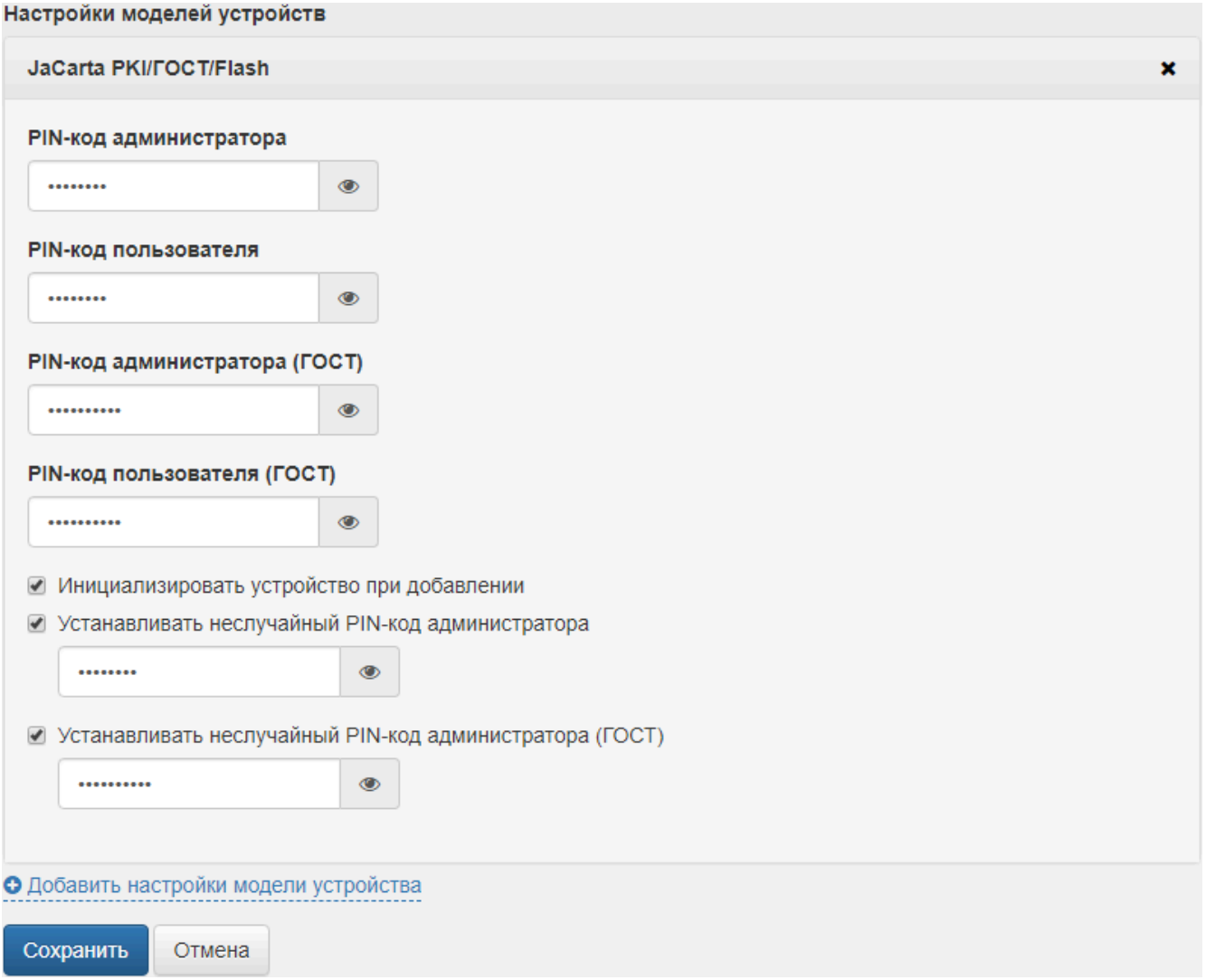
> **ПРИМЕЧАНИЕ**
>
> Обратитесь в службу технической поддержки компании Индид, если моделей устройств JaCarta, используемых в вашей организации, нет в списке.

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**.

6. Установите параметры для выбранной модели и нажмите **Сохранить**.



> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> 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 и IDPrime MD

При добавлении в Indeed Certificate Manager некоторые устройства eToken и IDPrime MD не разделяются по моделям, так как имеют общее свойство ATR (Answer-to-Reset).

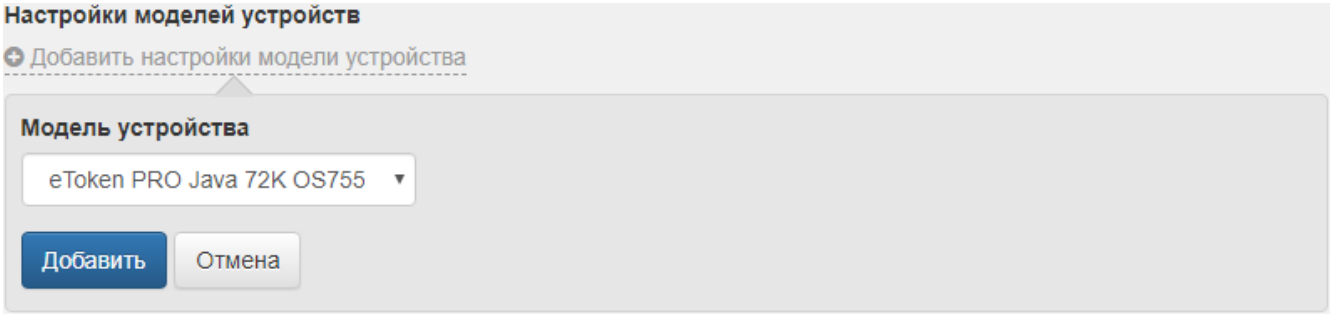
Вы можете разделить устройства по моделям и установить параметры инициализации для каждой модели. Для этого выполните следующие действия:

1. Откройте файл конфигурации *eTokenProJava72K.xml* и *IDPrimeMD.xml* из дистрибутива Indeed CM (\Misc\CardTypes) в текстовом редакторе, например, в Блокноте.
2. Удалите тег **<!- - ... - ->** из секции models и сохраните изменения.

```
eToken PRO Java 72K:
<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="IDCore 30B" rawModel="IDCore30B eToken 1.7.7" hasGostApplet="false" />
</models>

IDPrime MD:
<models>
    <model name="IDPrime MD 830-FIPS" rawModel="IDPrime MD 830-FIPS" hasGostApplet="false" />
    <model name="IDPrime MD 830-FIPS Rev B" rawModel="IDPrime MD 830-FIPS Rev B" hasGostApplet="false" />
    <model name="IDPrime MD 840 B" rawModel="IDPrime MD 840 B" hasGostApplet="false" />
    <model name="IDPrime MD 3810" rawModel="IDPrime MD 3810" hasGostApplet="false" />
    <model name="IDPrime MD 3811 Mifare-Desfire" rawModel="IDPrime MD 3811 Mifare-Desfire" hasGostApplet="false" />
</models>
```

3. Откройте Консоль управления Indeed CM и перейдите в раздел **Конфигурация → Типы устройств**.
4. Нажмите **Добавить тип устройства** и загрузите файлы *eTokenProJava72K.xml* и *IDPrimeMD.xml*. Включите опцию **Заменить существующий**, если устройства eToken или IDPrime MD уже использовались в Indeed CM.
5. Нажмите ✎ напротив добавленного типа устройства eToken или IDPrime MD.



6. Нажмите **Добавить настройки модели устройства**, выберите модель и нажмите **Добавить**.

7. Установите параметры для выбранной модели и нажмите **Сохранить**.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Чтобы устройства eToken или IDPrime MD фильтровались по моделям, удалите из системы Indeed CM все добавленные устройства eToken или IDPrime MD и добавьте их повторно. Если модель добавляемого устройства не найдена или настройки моделей отсутствуют, то устройство будет настроено по умолчанию.

Изменение иконок устройства

В Indeed Certificate Manager существует набор изображений, который отображает форм-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>...</models>>**

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> 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\mc\Content\images**
   - **C:\inetpub\wwwroot\mcremote\Content\images**
   - **C:\inetpub\wwwroot\mcservice\Content\images**

4. Откройте Консоль управления (Management Console) и перейдите в раздел **Устройства**.

	Серийный номер	Тип
	003bc82b	eToken PRO Java 72K (JC1.0b) (eToken PRO Java 72K OS755)
	0641367757	Rutoken S

Indeed CM Client Browser Extension

Компонент Indeed CM Client Browser Extension обеспечивает поддержку множественных сессий пользователей на терминальном сервере.

При подключении к терминальному серверу для каждого пользователя создается отдельная сессия с проброшенным устройством (смарт-картой, USB-токеном). Без поддержки множественных сессий пользователи видят устройство первого подключившегося пользователя.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Компонент Indeed CM Client Browser Extension поддерживается только в браузере Mozilla Firefox.

Установка и настройка

1. Выполните вход на терминальный сервер с правами локального администратора.
2. Установите **IndeedCM.Client.Browser.Extension-<*номер версии*>.ru-ru.msi** из каталога *IndeedCM.Client* дистрибутива системы.
3. Создайте файл REG реестра Windows со следующим содержимым:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\IndeedCM\Client\Server]
"MultipleServerMode"=dword:00000001
```

4. Сохраните созданный файл.
5. Примените значение файла реестра и перезагрузите службу **IndeedCM.Client.Server.Monitor**.
6. Настройте браузер Mozilla Firefox для работы Indeed CM Client Browser Extension.

Indeed CM Card Template Designer

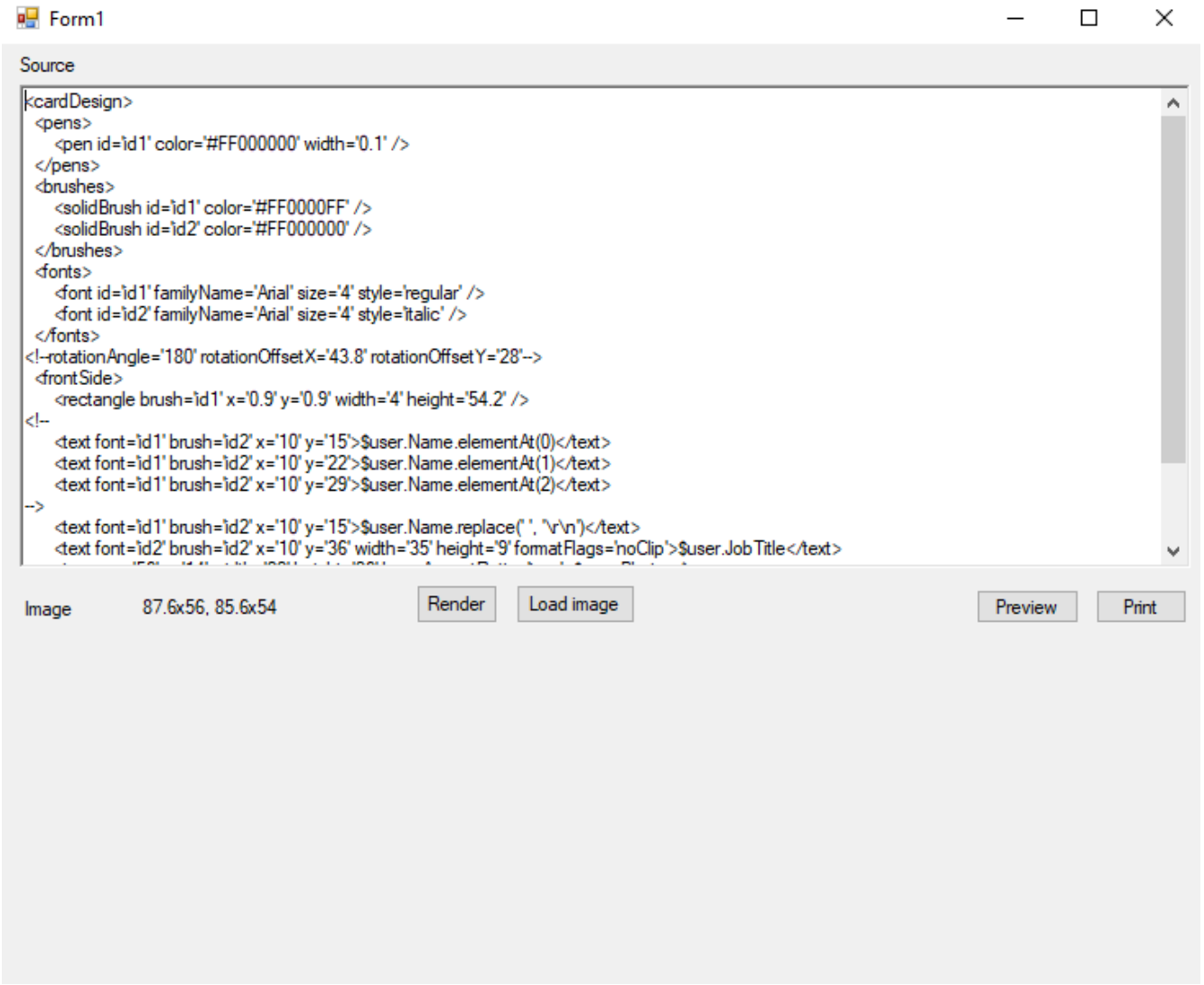
Утилита Indeed CM Card Template Designer позволяет создавать шаблоны печати на смарт-картах, которые используются с принтером **EDIsecure XID 8100\8300**.

Интеграция Indeed Certificate Manager с принтером позволяет выполнять следующие сценарии:

- выпускать смарт-карты с помощью считывателей принтера (контактного и бесконтактного) без печати,
- выпускать смарт-карты с печатью изображения или текста,
- печатать на смарт-картах изображение или текст без выпуска карты пользователям

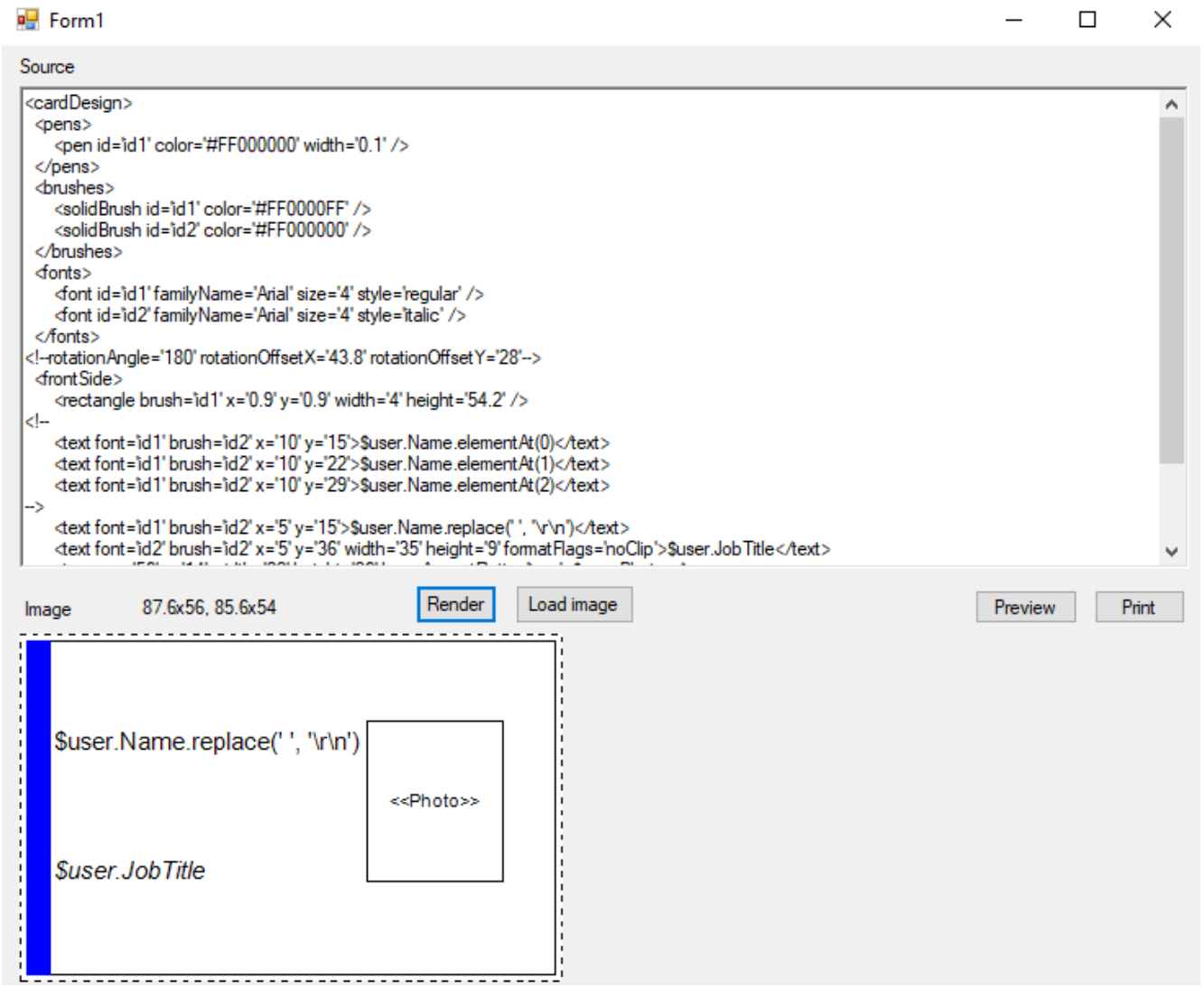
Утилита Indeed CM Card Template Designer предоставляется по запросу службой технической поддержки компании Индид.

Запустите приложение *cardTemplateDesigner.exe* из дистрибутива. После запуска в окне приложения загрузится 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>`.

Закомментированный текст внутри секций `<!- -... - ->` не учитывается при создании шаблона.

Параметры 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. Далее `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’ />

> **ПРЕДУПРЕЖДЕНИЕ**
>
> Для задания цвета используйте шестнадцатеричное значение и степень прозрачности. Например, **#FFA52A2A**, где **FF** – полная непрозрачность коричневого цвета **A52A2A** .

- **Кисть**. Задается в секции `<brushes>` с параметрами `brush id` и `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 `<fonts>` с параметрами `font id`, `familyName`, `size`, `style`

> **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. Далее `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
  - widht (опциональный)
  - heigth (опциональный)
  - horizontalAlignment: left, right, center (опциональный)
  - verticalAlignment: top, bottom, center (опциональный)
  - formatFlags (см. *подробное описание значений*)

> **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. 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 можно перенести 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:

ПРИМЕЧАНИЕ

<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)

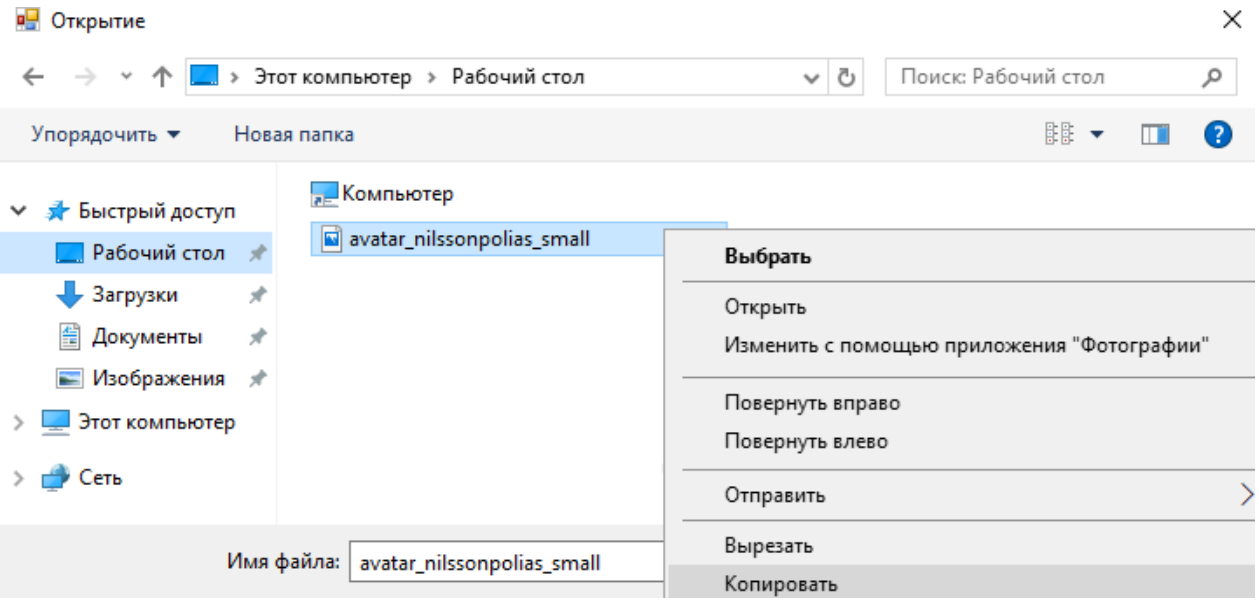
- **Изображение**. Задается в секции `<image>` с параметрами:
  - x
  - y
  - widht (опциональный)

- heigth (опциональный)
- keepAspectRatio (true или false)
- data (опциональный)

> **ПРИМЕР**
>
> <image x=’56’ y=’14’ width=’22’ height=’26’
> keepAspectRatio=’true’>$user.Photo</image>

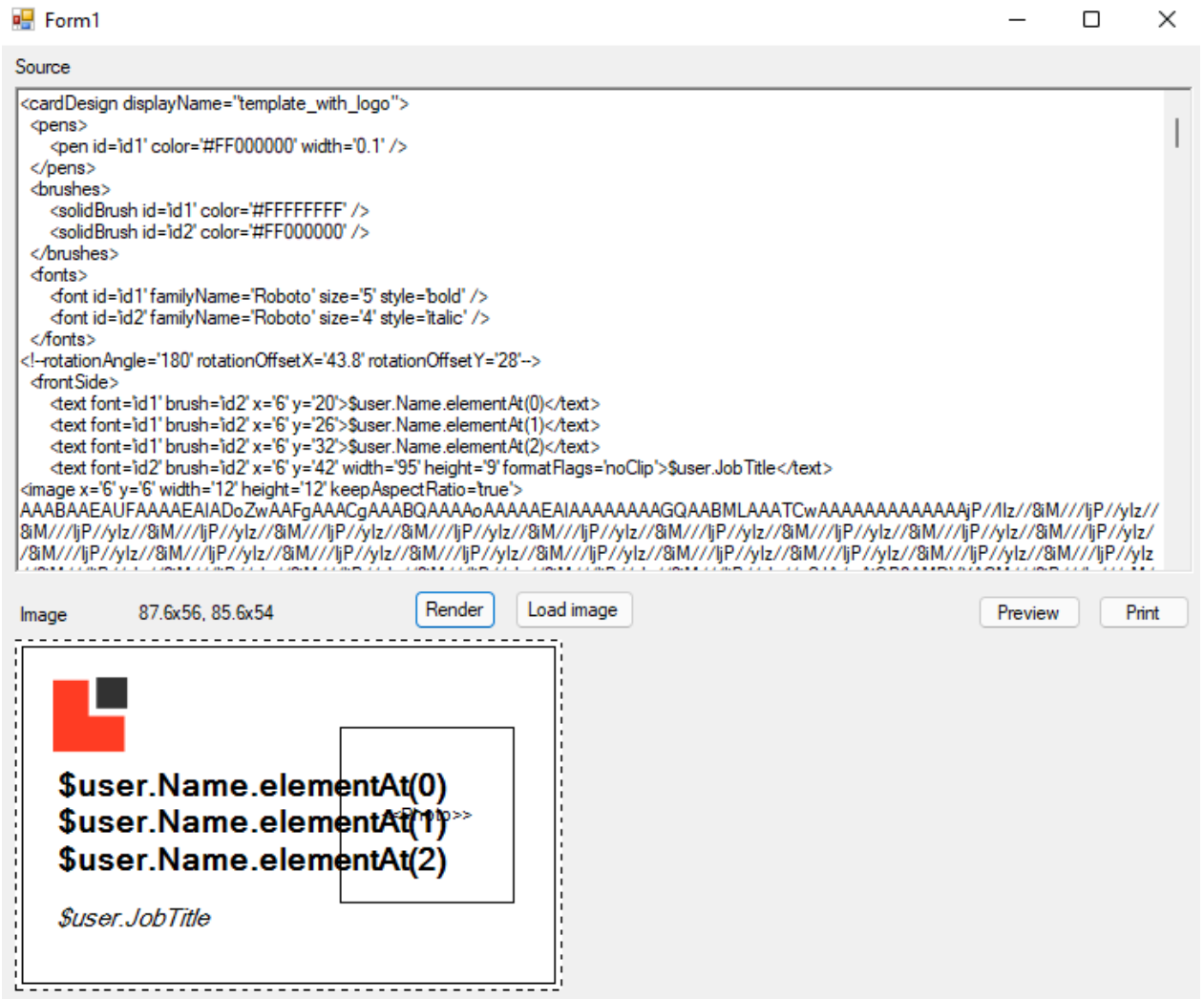
Описанная строка определяет положение, размер и следование пропорциям изображения, подставляемого из атрибута Active Directory (переменная `$user.Photo`). Помимо переменной можно подставить и изображение в кодировке base64 (например, для добавления в шаблон логотипа компании) и затем визуализировать 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. Нажмите 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.

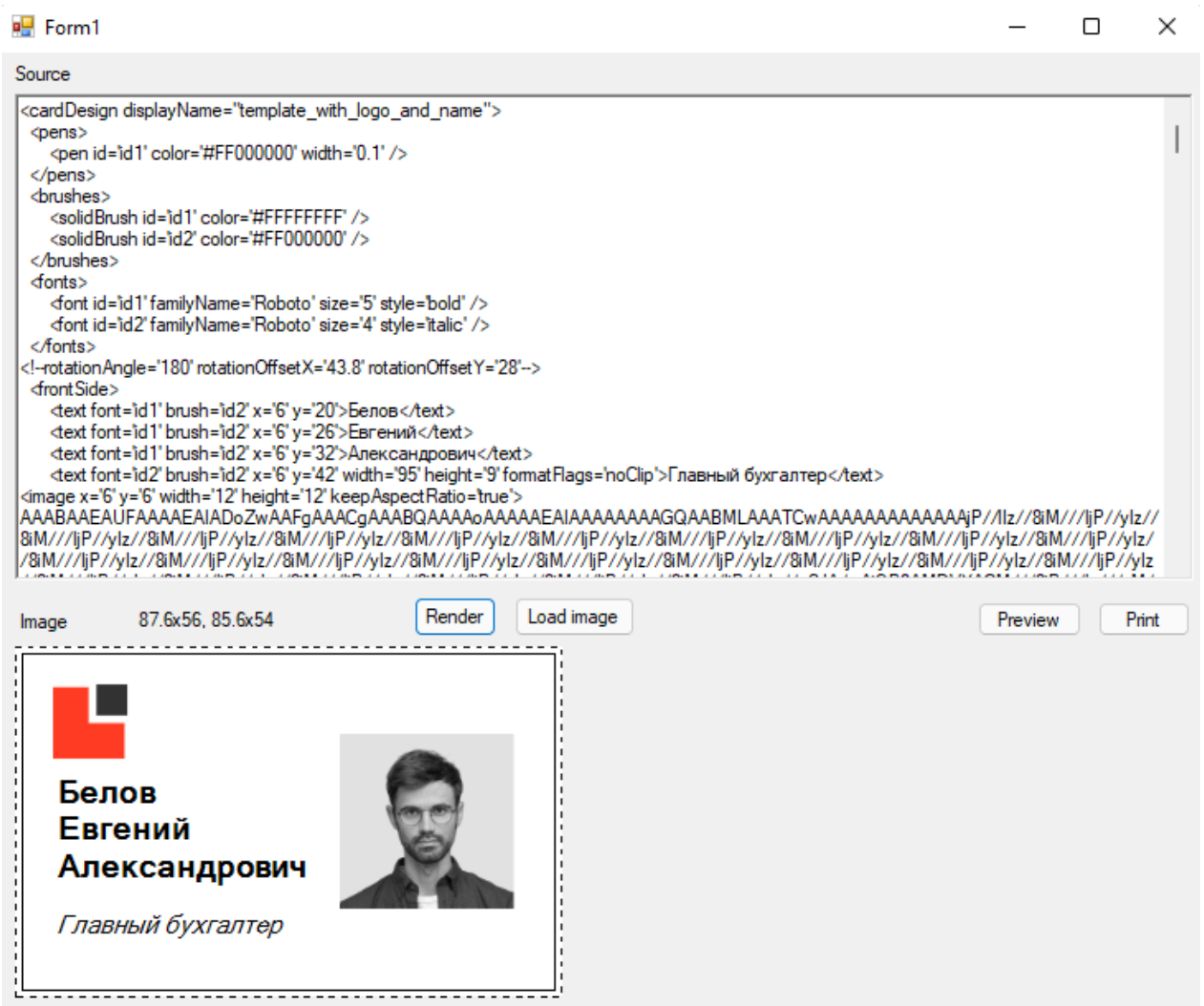


Ниже на рисунке приведен пример шаблона со статическим логотипом компании и подстановкой данных пользователя из Active Directory:

- ФИО с разбивкой по строкам, написанные жирным шрифтом,
- фотография,
- должность, написанная курсивом.



Далее приведен пример ожидаемого результата печати по шаблону. Для визуализации вместо переменных `$user.Name.elementAt`, `$user.JobTitle` и `$user.Photo` в шаблоне прописаны данные пользователя и загружена его фотография.



- **Прямоугольник**. Задается в секции **<rectangle>** с параметрами:
  - pen (опциональный)
  - brush (опциональный)
  - x
  - y
  - width (опциональный)
  - height (опциональный)
- **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`.

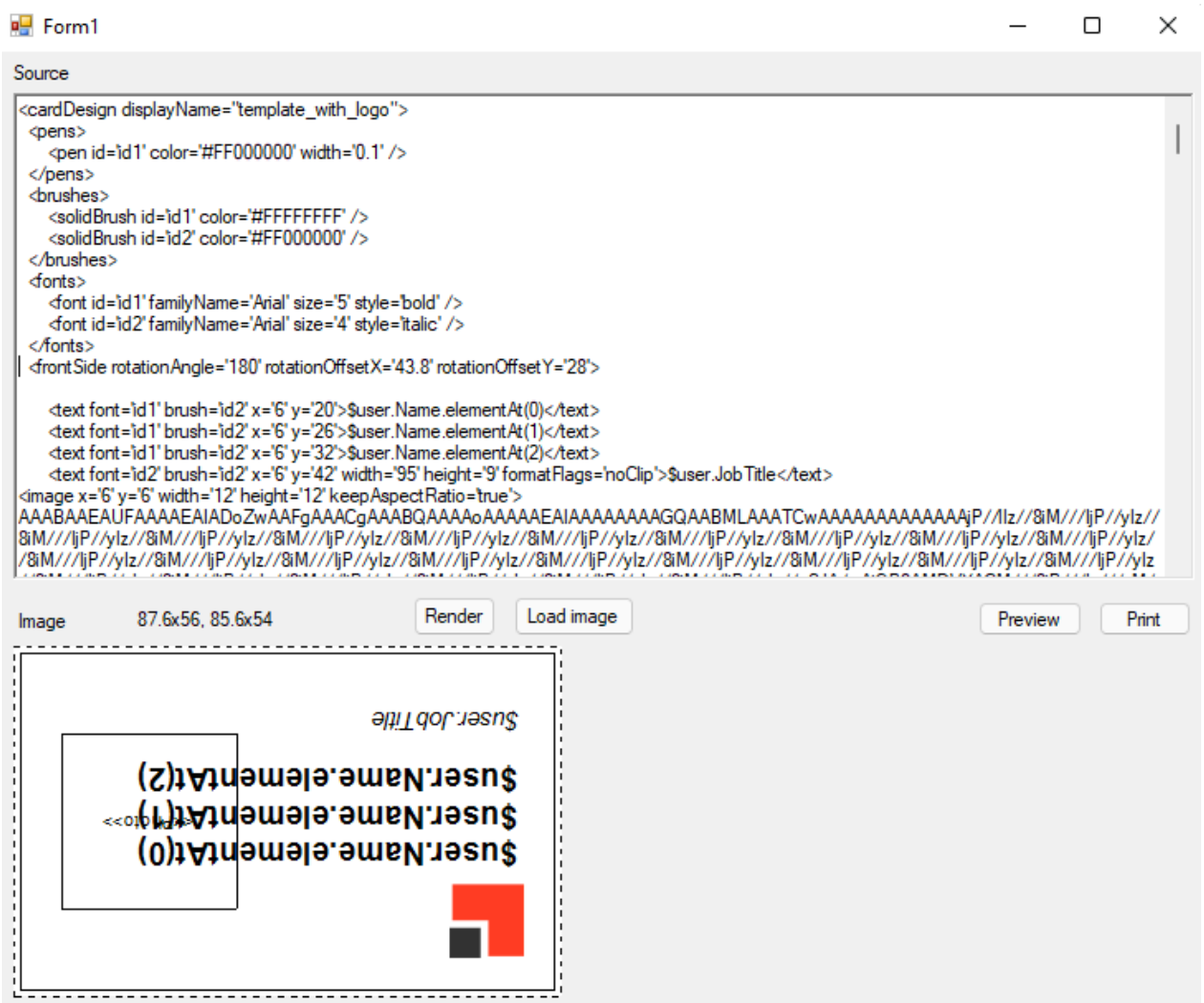
ПРИМЕР:

<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.



HEX-коды для настройки прозрачности цветов

#F0F8FF		#2F4F4F		#20B2AA		#FFDAB9	
#FAEBD7		#00CED1		#87CEFA		#CD853F	
#00FFFF		#9400D3		#778899		#FFC0CB	
#7FFFD4		#FF1493		#B0C4DE		#DDA0DD	
#F0FFFF		#00BFFF		#FFFFE0		#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		#FFFFF0		#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		#FFEFD5	
#483D8B		#FFB6C1		#DB7093		#FFA07A	

В таблице приведены HEX-коды процентного соотношения прозрачности. Где 100% – абсолютно непрозрачный цвет, 0% – абсолютно прозрачный.

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  :

100%  75%  50%  25% 

Решение проблем

Сбор логов

Как собрать логи компонентов Indeed CM

Контакты

Техническая поддержка и отдел по работе с клиентами

Сбор логов

Серверные компоненты

1. Перейдите в каталог сервиса, логи которого необходимо получить.

Расположение сервисов

Windows

Имя сервиса	Расположение
Служба Монитора устройств (Card Monitor)	%ProgramFiles%\Indeed CM\CardMonitor
Сервис регистрации агентов – веб-приложение agentregistrationapi	%SystemDrive%\inetpub\wwwroot\cm\agent\agentregistrationapi
Сервис агентов – веб-приложение agentserviceapi	%SystemDrive%\inetpub\wwwroot\cm\agent\agentserviceapi
Сервис API – веб-приложение api	%SystemDrive%\inetpub\wwwroot\cm\api
Сервис онлайн-разблокировки и выключения устройств – веб-приложение credprovapi	%SystemDrive%\inetpub\wwwroot\cm\credprovapi
Консоль управления (Management Console) – веб-приложение mc	%SystemDrive%\inetpub\wwwroot\cm\mc

Имя сервиса	Расположение
OpenID Connect Server – веб-приложение oidc	%SystemDrive%\inetpub\wwwroot\cm\oidc
Сервис удаленного обслуживания (Remote Self-Service) – веб-приложение rss	%SystemDrive%\inetpub\wwwroot\cm\rss
Сервис самообслуживания (Self-Service) – веб-приложение ss	%SystemDrive%\inetpub\wwwroot\cm\ss
Мастер настройки Indeed CM (Indeed CM Setup Wizard) – веб-приложение wizard	%SystemDrive%\inetpub\wwwroot\cm\wizard
Сервер Indeed AirCard Enterprise	%SystemDrive%\inetpub\wwwroot\Indeed.AirKey.EntServer

Linux

Имя сервиса	Расположение
Служба Card Monitor	/opt/indeed/cm/cardmonitor
Сервис регистрации агентов – веб-приложение agentregistrationapi	/opt/indeed/cm/agentregistrationapi

Имя сервиса	Расположение
Сервис агентов – веб-приложение agentserviceapi	/opt/indeed/cm/agentserviceapi
Сервис API – веб-приложение api	/opt/indeed/cm/api
Сервис онлайн-разблокировки и выключения устройств – веб-приложение credprovapi	/opt/indeed/cm/credprovapi
Консоль управления (Management Console) – веб-приложение mc	/opt/indeed/cm/mc
OpenID Connect Server – веб-приложение oidc	/opt/indeed/cm/oidc
Сервис удаленного обслуживания (Remote Self-Service) – веб-приложение rss	/opt/indeed/cm/rss
Сервис самообслуживания (Self-Service) – веб-приложение ss	/opt/indeed/cm/ss
Мастер настройки Indeed CM (Indeed CM Setup Wizard) – веб-приложение wizard	/opt/indeed/cm/wizard

2. Откройте файл *nlog.config* в текстовом редакторе, например, в Блокноте, запущенном от имени администратора, и измените значение параметра `minlevel` с **Off** на **Trace**:

```
<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, что в нем появились подкаталоги с файлами отладочной информации.

7. Пришлите каталог **logs** со всем его содержимым специалистам технической поддержки компании Индид с описанием проблемы.
8. Для отключения логирования измените значение параметра `minlevel` с **Trace** на **Off** и сохраните изменения в файле.

Клиентские компоненты

Windows

Приложение Indeed-Id GetLog предназначено для локального и удаленного сбора программных логов следующих компонентов:

- Indeed CM Middleware,
- Indeed CM Client Tools,
- Indeed CM Agent.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Для работы утилиты Indeed-Id GetLog необходимы права локального администратора. На операционных системах Windows Vista и выше утилита запускается от имени администратора (Run As Administrator).

Запустите приложение *IndeedID.GetLog.exe* из каталога *GetLog* дистрибутива Indeed Certificate Manager. Выполните следующие действия:

1. Подключитесь к компьютеру. Для этого введите *localhost* в поле **Computer** для подключения к локальному компьютеру или имя/IP-адрес удаленного компьютера для подключения к удаленному компьютеру. Нажмите **Connect**

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Для установки подключения к удаленному компьютеру под управлением Windows Vista и выше убедитесь, что на удаленном компьютере запущена и не заблокирована служба **Инструментарий управления Windows (WMI)** (Windows Management Instrumentation).

2. Нажмите **Enable Log**, чтобы включить логирование.

3. Воспроизведите проблему.
4. Нажмите **Disable Log**, чтобы отключить логирование.
5. Нажмите **Get Log...**, чтобы получить логи.
6. Укажите каталог для сохранения zip-архива и нажмите **Сохранить**.
7. Нажмите **Disconnect**, чтобы отключиться от компьютера.
8. Отправьте логи специалистам технической поддержки компании Индид. Подробно опишите действия пользователя и укажите точное время воспроизведения проблемы.

ПРИМЕЧАНИЕ

По умолчанию логи пишутся 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**.

Дополнительные настройки

В окне **Advanced Settings** доступны следующие настройки:

Настройка	Описание
Max. log size (bytes)	Максимальный размер в байтах всех файлов в каталоге. Значение по умолчанию – 1Гб. При достижении максимального размера 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 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. Перед началом записи логов клиентский компонент проверит, включено ли логирование на рабочей станции. По умолчанию интервал проверки составляет 1 минуту (60 000миллисекунд).

Настройка	Описание
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 старый файл удалится, и логи будут записываться в новый 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

- **при подключении к удаленному компьютеру:**

Ошибка	Причина	Решение
`0x800706BA The RPC server is unavailable`	На удаленном компьютере под управлением Windows Vista и выше остановлена или заблокирована служба **Инструментарий управления Windows** (WMI) (Windows Management Instrumentation).	Запустите службу WMI: 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`	Удаленный компьютер недоступен по сети.	Проверьте параметры сетевого подключения.

- **при подключении к локальному компьютеру:**

Ошибка	Причина	Решение
`0x80070005 Access is denied` или `The network path is not accessible. Access is denied`	У пользователя, под учетной записью которого запущен Indeed-Id GetLog, нет прав на чтение и/или изменение ветки реестра Windows с параметрами записи логов.	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. Нажмите **Применить** (Apply). Чтобы изменения в правах вступили в силу, пользователю необходимо выйти из системы и выполнить повторный вход.
	У пользователя нет прав на запись в каталог сохранения логов.	Предоставьте учетной записи пользователя необходимые права в указанном каталоге.

- **при сохранении логов:**

Ошибка	Причина	Решение
`0x80070035 The network path was not found`	Недоступен сетевой каталог, используемый для доступа к лог-файлам (по умолчанию используется каталог *ADMIN$\System32\LogFiles*).	Проверьте параметры доступа к сетевому каталогу.
`0x80070003 The system cannot find the file specified`	Неверно указан путь к сетевому каталогу для сохранения файлов.	Укажите правильный сетевой путь.

Linux

Логи Indeed CM Middleware, установленного на ОС Linux, записываются в каталог *tmp/cm/logs*.

Управление логированием

1. Откройте файл */etc/cm/logging.cfg* с правами администратора.
2. Измените значение параметра *enabled:*
   - значение *1* включает логирование,
   - значение *0* отключает логирование.
3. Сохраните файл.

Сбор логов

1. Очистите существующие логи Indeed CM Middleware в каталоге */tmp/cm/logs*.
2. Воспроизведите проблему.
3. Отправьте новые логи специалистам технической поддержки компании Индид. Подробно опишите действия пользователя и укажите точное время воспроизведения проблемы.

Инсталляторы

Все инсталляторы Indeed Certificate Manager для ОС Windows 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 отправьте файл с логами специалистам технической поддержки компании Индид с описанием проблемы.

Примеры запуска

```
msiexec /i IndeedCM.Client.Tools-<номер версии>.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-<номер
версии>.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.
```

Если вам необходимо собрать логи инсталлятора при установке компонента через групповые политики, и у вас нет возможности задать параметры командной строки, включите логи Windows Installer с помощью ключа в реестре.

- чтобы включить логирование, в ветке реестра *HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer* создайте ключ **Reg_SZ: Logging** с значением ***voicewarmupx***.
- чтобы выключить логирование, задайте пустое значение ключа **Logging**.

Включить и выключить отладочные логи инсталляторов Indeed CM можно с помощью файлов REG, которые входят в состав дистрибутива и находятся в папке *\GetLog\Regfiles* (файлы *MSI*

logs On.reg и *MSI logs Off.reg*).

- чтобы включить запись отладочных логов инсталляторов на рабочей станции, запустите файл *MSI logs On.reg*.
- чтобы выключить запись отладочных логов инсталляторов на рабочей станции, запустите файл *MSI logs Off.reg*.

Файл с логами 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 следующую команду:

```
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-company.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**

История версий

В этом разделе содержится краткое описание изменений и улучшений Indeed Certificate Manager по версиям.

7.2

- Реализована интеграция с удостоверяющими центрами Aladdin Enterprise CA и SafeTech CA для выпуска сертификатов с поддержкой алгоритмов шифрования RSA и ГОСТ.
- Реализована поддержка LDAP-каталогов пользователей Samba AD DC и РЕД АДМ.
- Добавлена поддержка Windows Server 2025 для серверных компонентов Indeed CM.
- Добавлена поддержка Альт 8 СП релиз 10 (c10f2) для серверных и клиентских компонентов Indeed CM.
- Оптимизировано определение параметров работы Indeed CM в Мастере настройки.
- Оптимизировано администрирование Indeed CM в Консоли управления.
- Расширена функциональность сервиса внутреннего электронного документооборота:
    - Реализована поддержка CAdES – стандарта, по которому формируется усовершенствованная электронная подпись с временным штампом.
    - В настройки политики добавлена возможность установить тип подписи, который разрешено использовать при подписи документов в Сервисе самообслуживания (CMS, CAdES-BES, CAdES-T, CAdES-X Long Type 1, CAdES-A).
- Исправлена ошибка при импорте корневых сертификатов Microsoft CA на устройство.
- Исправлена ошибка установки виртуальной смарт-карты AirCard на все разрешенные компьютеры.
- Исправлена ошибка прав доступа к ключу шифрования при работе Log Server в ОС Linux.

7.1

Интеграции

- Добавлена поддержка LDAP-каталогов FreeIPA и ALD Pro.
- Добавлена совместимость Indeed CM с новыми версиями удостоверяющего центра ПАК «КриптоПро УЦ» 2.0 (варианты исполнения 15, 16) и КриптоПро PKI-Кластером, которые доступны на ОС Astra Linux и Windows.

- Реализована интеграция Indeed CM с Рутокен Логон для настройки доменной аутентификации по сертификату в ОС Linux.
- Indeed CM интегрирован с Indeed Access Manager версии 8.2 и выше.
- Реализован аудит событий Indeed CM на ОС Linux через приложение Log Server.

Indeed CM Agent

- В массовые задачи агента добавлена функция смены PIN-кода пользователя.
- Автоматизирован процесс выпуска назначенных устройств – устройства можно добавлять, назначать и выпускать автоматически с помощью агента.
- В настройки работы агента добавлена возможность настроить временной период для принудительной смены PIN-кода пользователя на устройстве.
- Добавлено уведомление о подключении незарегистрированного устройства к рабочей станции с агентом.
- В раздел поиска агентов добавлена фильтрация по версии.

СКЗИ

- Внедрена возможность настроить внутренний каталог пользователей в базе данных Microsoft SQL или PostgreSQL, чтобы создавать пользователей в Консоли управления и назначать СКЗИ внешним пользователям.
- Реализована возможность контролировать допуск пользователей к самостоятельной работе с СКЗИ с помощью обучающих курсов.
- Добавлена возможность разделить СКЗИ по типам и настроить мониторинг сертификатов соответствия на СКЗИ и сертификатов технической поддержки.
- В Консоль управления и Сервис самообслуживания добавлена функциональность формирования и подписания нормативных документов СКЗИ электронной подписью.

Документы

- В Консоль управления добавлен раздел поиска документов по фильтрам.
- Реализована проверка наличия оригиналов документов и отслеживание неподписанных документов.

Сертификаты

- В Консоль управления добавлен раздел поиска сертификатов по фильтрам.
- Добавлена функция мониторинга сервисных сертификатов следующих типов: сертификаты операторов шлюза КриптоПро УЦ-СМЭВ, корневой сертификат сервисов агента,

сертификаты интегрированных УЦ.

Новые модели устройств

- Рутокен ЭЦП 3.0 3120, Рутокен ЭЦП 3.0 3220, Рутокен Lite 1010;
- ESMART Token USB 192k и ESMART Token CARD 192K;
- SafeNet eToken Fusion Series, SafeNet eToken 5300, SafeNet eToken 5110CC (940), IDPrime 940 и IDPrime 940B, IDPrime 3940 и IDPrime 3940 FIDO.

Дополнительные настройки уведомлений

- Добавлены уведомления об окончании срока действия лицензии и о нехватке свободных лицензий.
- Реализована возможность глобальной конфигурации почтового сервера.
- В шаблонах уведомлений переработаны переменные, значения которых автоматически подставляются в текст сообщения.

API

- Реализовано управление СКЗИ через API – получение списка СКЗИ по заданным фильтрам, поиск СКЗИ по идентификатору или типу, регистрация в Indeed CM, назначение на пользователя, смена состояния, уничтожение или изъятие.
- Расширены возможности управления устройствами через API:
  - В параметры запроса `GET/Cards` добавлены фильтры по дате выпуска, обновления и отзыва устройства, фильтр по модели устройства и политике, действующей на устройство. В возвращаемые значения добавлен параметр для выгрузки даты начала действия сертификата на устройстве.
  - Добавлен метод `GET/Cards/{Id}`, чтобы получить информацию о конкретном устройстве по идентификатору.
  - Добавлен метод `POST /Cards/{id}/Withdraw`, чтобы изъять отозванное устройство.

Отдельные изменения

- В функции службы Card Monitor добавлено автоматическое изъятие устройств у удаленных пользователей, чтобы освободить лицензии.
- Добавлены новые функции настройки PIN-кодов: возможность настроить отдельные параметры работы PIN-кода для каждой модели устройств Рутокен и новые параметры генерации случайных PIN-кодов.

- Усовершенствована функциональность ролевой модели.
- Добавлена расширенная проверка паспорта в СМЭВ, чтобы запретить выпуск квалифицированного сертификата для пользователя с недействительным паспортом.
- Реализована возможность принудительно подтвердить корректность данных пользователя при проверке в СМЭВ, если она длится более 15 минут.

7.0

Поддержка ОС Linux

- Добавлена поддержка ОС Linux для серверных компонентов Indeed CM.
- Реализовано управление ключевыми носителями семейств Рутокен, JaCarta, SafeNet eToken и ESMART на ОС Linux с помощью Indeed CM Middleware.
- Добавлена аутентификация с использованием протокола OpenID Connect в Консоли управления, Сервисе самообслуживания, Сервисе API и в Мастере настройки.

Indeed CM ЭДО

- Разработан сервис внутреннего электронного документооборота Indeed CM ЭДО для централизованного управления жизненным циклом сертификатов от выпуска до прекращения действия и для обмена документами между пользователями и администраторами.
- В Сервис самообслуживания добавлена возможность загружать документы для получения сертификата ключа проверки электронной подписи.
- В Консоли управления реализована возможность приостановить выпуск и обновление устройства для дополнительной проверки документов пользователей.

Управление СКЗИ

- Добавлена настройка шаблонов нумерации нормативных документов и возможность выбора шаблона печати для каждого типа СКЗИ в каждом его состоянии.
- Добавлена возможность сохранить результаты поиска СКЗИ в файл XLSX и распечатать по форме из приказа ФАПСИ №152 и по форме лицевого счета пользователя.
- Добавлена возможность указать имена одного или нескольких сотрудников, которые производили установку, изъятие/уничтожение СКЗИ.
- В Консоль управления добавлена функция назначения СКЗИ.
- В Сервис самообслуживания добавлена функция просмотра и печати СКЗИ.

Indeed CM Agent

- В массовые задачи Агента добавлена функция дистанционной очистки устройств.
- Реализована автоматическая отмена всех задач, назначенных на агент, при отзыве и изъятии устройства – обновление, сброс PIN-кода, блокировка и очистка.
- Добавлена поддержка аппаратной смены PIN-кода на ключевых носителях Рутокен ЭЦП 3.0 и eToken PRO Java 72K.
- Настроена функция удаления неактивных агентов по заданному расписанию.

Ведение журналов учета и управление сертификатами

- Настроена отправка информации об отслеживаемых сертификатах в журналы учета.
- Добавлена возможность регулировать выбор необязательных сертификатов при выпуске и обновлении устройства в Сервисе самообслуживания, а также задать сообщение, которое отображается в виде предупреждения в окне выбора необязательных сертификатов.
- Реализовано отслеживание сертификатов, выпущенных Валидата УЦ, и отправка уведомления, если срок действия сертификатов истекает.
- Добавлена возможность формировать запрос на сертификат Валидата УЦ в формате RTM.

Другие изменения

- Добавлена возможность назначить политику на несколько групп пользователей Microsoft Active Directory.
- В настройки выпуска устройств добавлена возможность указать, какие символы исключить при генерации случайного PIN-кода.
- Реализована проверка заполнения полей в параметрах Мастера настройки.
- Прекращена поддержка хранилища данных в Microsoft Active Directory.
- В возвращаемые значения API добавлена информация о пользователе, на которого назначено устройство, о действующей на устройство политике и о сертификатах на устройстве.
- В исполняемый файл добавлены атрибуты пользователя `sAMAccountName` (Logon name) и `userPrincipalName` (Principal Name).

Исправления

- Исправлена ошибка при попытке создать копию политики, действующей на устройство с сертификатом Валидата УЦ или КриптоПро УЦ 2.0.

- Исправлена ошибка при попытке зарегистрировать агент с неактуальным корневым сертификатом в хранилище.
- Исправлено отображение названий ОС на странице агентов.

6.6

- Добавлена поддержка PostgreSQL и Postgres Pro в качестве хранилища данных.
- Разработана утилита для миграции данных Indeed CM из Microsoft SQL в PostgreSQL и Postgres Pro.
- В Консоль управления добавлена опция проверки данных пользователя в СМЭВ.
- Добавлена возможность одобрить проверку данных пользователя в СМЭВ в Консоли управления как отдельная привилегия в разделе **Роли**.
- Уменьшен интервал времени, при котором не отправляются повторные запросы в КриптоПро Шлюз УЦ-СМЭВ.
- Добавлена печатная форма запроса на отзыв сертификата.
- Добавлена возможность просмотреть свойства сервисных сертификатов **Субъект** (Subject), **Издатель** (Issuer), **Действителен до** (Valid to) при настройке удостоверяющих центров в политике.
- Добавлена возможность одновременно установить опции **Устанавливать случайный PIN-код пользователя** и **Пользователь должен поменять PIN-код при первом входе** в параметрах выпуска устройств в Консоли управления.
- Добавлена поддержка аппаратных политик качества PIN-кодов для ключевых носителей Рутокен ЭЦП 3.0 NFC.
- Исправлена ошибка валидации СНИЛС в форме проверки в СМЭВ со значениями контрольных сумм больше 101, в которых остаток от деления 101 был равен 100.
- Устранена уязвимость в Сервисе самообслуживания, позволяющая выполнить код HTML/JavaScript в поле **Ответ** при задании ответов на секретные вопросы.
- Исправлена ошибка экспорта результатов поиска в разделе **Пользователи** в CSV.
- Исправлено отображение всплывающего сообщения при нарушении привязки устройства к агенту.
- Исправлено отображение информации о сессии пользователя в журнале событий при нарушении условий привязки устройства к агенту.
- Исправлена проблема с кодировкой в субъекте запроса на сертификат при использовании аппаратной криптографии с версиями Рутокен Панели выше 4.9.1.

- Добавлен параметр инициализации *Требуется соответствие уровню сложности: не менее 3 типов (3 из 4)* для ключевых носителей eToken PRO Java 72K.