Indeed Certificate Manager

Техническая документация

Версия: 7.3

Дата: 22.07.2026

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 и СКЗИ 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
- Биометрическая защита закрытого ключа сертификата на устройствах с поддержкой биометрии

Совместимость

Платформы	• ОС Windows • ОС Linux (в том числе Astra Linux и РЕД ОС, сертифицированные ФСТЭК)

Каталоги пользователей	• LDAP-каталоги – Active Directory, Samba AD DC, РЕД АДМ, Альт Домен, FreeIPA, ALD Pro, OpenLDAP • Центр Регистрации КриптоПро УЦ • Внутренний каталог в СУБД Microsoft SQL Server или PostgreSQL
Удостоверяющие центры	• Microsoft CA • Aladdin Enterprise CA • SafeTech CA • Dogtag CA • КриптоПро УЦ 2.0 (варианты исполнения 15 и 16 для ОС Astra Linux и Windows) 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.

- **Рутокен Логон**

  Рутокен Логон позволяет использовать схему двухфакторной аутентификации в Linux через устройство с сертификатом или зашифрованным паролем. Indeed CM выпускает такое устройство и записывает на него данные, необходимые для аутентификации.

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
- **Indeed CM Agent** (Клиентский агент) – сервис регистрации клиентских агентов и сервис для удаленного управления устройствами пользователей
- **Мастер настройки Indeed CM** (Indeed CM Configuration Wizard) – веб-консоль для настройки параметров работы 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 системы 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.Config.DataProtector** – утилита для шифрования файлов конфигурации сервисов 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 онлайн- и офлайн-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 выполнения блокировки, сброса PIN-кода пользователя, обновления содержимого устройства, очистки или инициализации устройства при его отзыве, смены PIN-кода администратора на устройствах пользователей.

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 2012–2025 Убедитесь, что в ОС Windows параметр **Язык программ, не поддерживающих Юникод** имеет значение **Русский (Россия)**. • Debian 10–13 • Astra Linux Special Edition 1.7–1.8 • Ubuntu 20.04 LTS–24.04 LTS • Red Hat Enterprise Linux 8–9 • CentOS Stream 8–9 • РЕД ОС 7.3–8 • Альт 8 СП релиз 10 (c10f2) • Альт 10–11 • Platform V SberLinux OS Server 9.6 и выше

Веб-сервер	• Internet Information Services (IIS) 7.0 и выше с компонентами **Компоненты IIS** ◦ 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) ◦ Авторизация URL-адреса (URL Authorization) ◦ Windows-проверка подлинности (Windows Authentication) ◦ Консоль управления службами IIS (IIS Management Console) • Nginx 1.22.1 и выше • Angie PRO 1.1.0 и выше • Apache 2.4.25 и выше
Дополнительные компоненты Microsoft	• Microsoft .NET 8.0.10 и выше • URL Rewrite (для работы приложения Log Server в ОС Windows)
Компоненты КриптоПро	• КриптоПро CSP 5.0 и выше для интеграции с КриптоПро DSS 2.0 • КриптоПро CSP 5.0 R3 и выше для ОС Linux Чтобы установить защищенное TLS-соединение между сервером Indeed CM и Центрами Регистрации КриптоПро УЦ 2.0 и Валидата УЦ, необходима серверная лицензия КриптоПро CSP. КриптоПро УЦ 2.0 и Валидата УЦ защищены в соответствии с государственными стандартами РФ.

Требования к окружению

Каталог пользователей	• LDAP-каталоги:
	  ◦ Active Directory
	  ◦ Samba AD DC 4.0 и выше
	  ◦ РЕД АДМ (промышленная редакция) 1.2.2, 2.0.2, 2.0.3
	  ◦ Альт Домен 10–11
	  ◦ FreeIPA 4.4 и выше
	  ◦ ALD Pro 2.4 и выше
	  ◦ OpenLDAP 2.4 и выше
	• Центр Регистрации КриптоПро УЦ 2.0
	• Внутренний каталог пользователей в базе данных Microsoft SQL или PostgreSQL

Центр сертификации	• Центр сертификации Microsoft (Microsoft Enterprise CA) на базе:
	  ◦ Windows Server 2008 (редакция Enterprise и выше)
	  ◦ Windows Server 2012/2012 R2
	  ◦ Windows Server 2016–2025
	  Microsoft Enterprise CA поддерживает использование КриптоПро CSP в качестве криптопровайдера для выпуска сертификатов.
	• Aladdin Enterprise CA версии 2.0.1, 2.2.0
	• SafeTech CA версии 2.0 и выше
	• Dogtag CA версии 11.4 и выше
	• КриптоПро УЦ 2.0:
	  ◦ Варианты исполнения 5, 6, 9, 10 для ОС Windows
	  ◦ Варианты исполнения 15, 16 для ОС Astra Linux и Windows
	• Валидата УЦ версий 3.1, 4.0

Хранилище данных	• Microsoft SQL Server 2012 SP2 и выше • PostgreSQL 14 и выше • Postgres Pro Standard, Postgres Pro Enterprise 14 и выше

Поставщики службы криптографии (CSP)	**RSA** • CSP производителя устройства (Aktiv ruToken CSP v1.0, eToken Base Cryptographic Provider) • Microsoft Base Smart Card Cryptographic Service Provider (если CSP не предоставляется производителем устройства) Microsoft Base Smart Card Cryptographic Service Provider также поддерживается в связке с КриптоПро УЦ 2.0. **ГОСТ Р34.10-2001/2012** • КриптоПро CSP 5.0 R2 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" Работа с ключами ГОСТ Р34.10-2001/2012 также поддерживается при использовании Microsoft Enterprise CA.

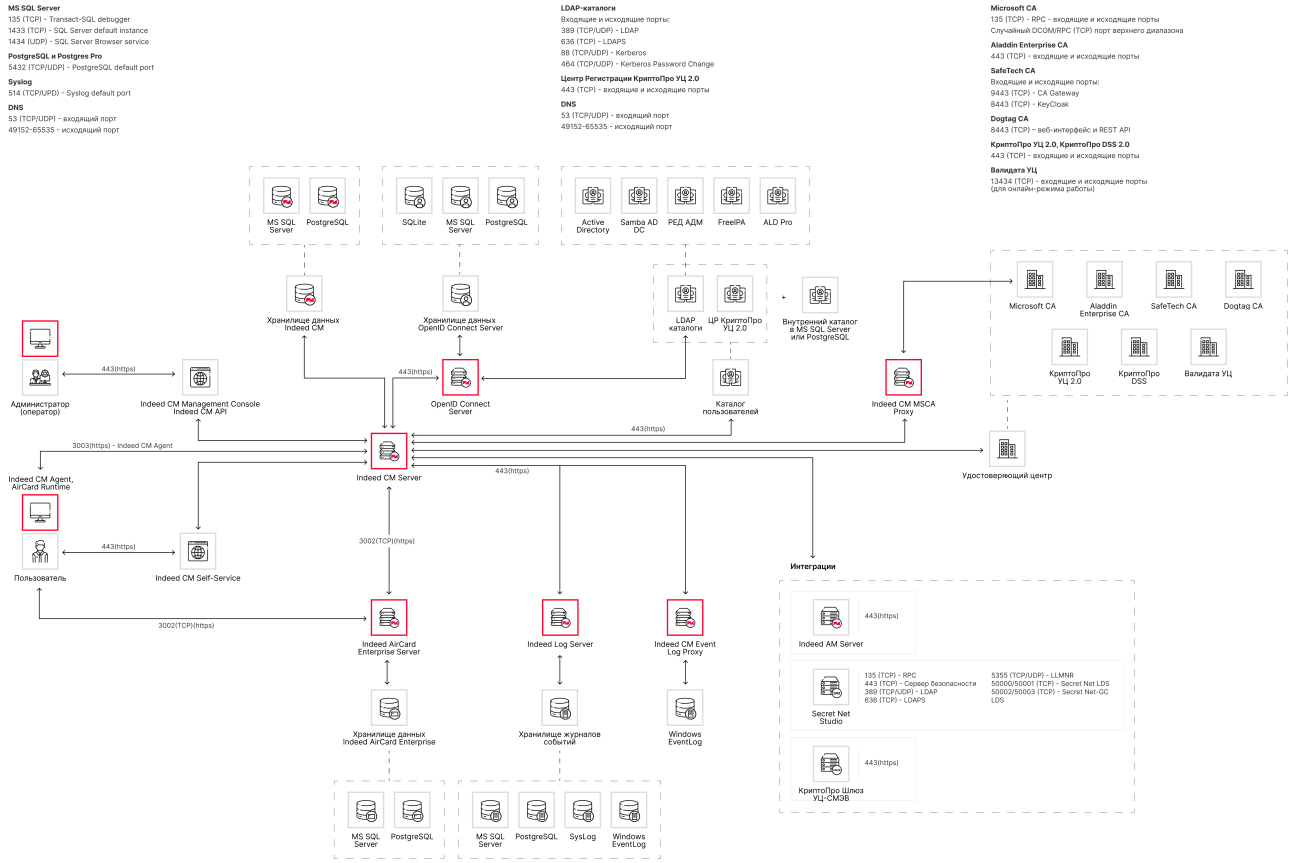
Клиентские компоненты

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

Аппаратные требования	Не менее 300 МБ свободного дискового пространства
Операционная система	• Windows 7–11 • Windows Server 2008 SP2 x86/x64 (с обновлением KB980368), R2 SP1 • Windows Server 2012–2025 • Debian 10–13 • Astra Linux Special Edition 1.7–1.8 • Astra Linux Common Edition 2.12 • Ubuntu 20.04 LTS–24.04 LTS • Red Hat Enterprise Linux 8–9 • CentOS Stream 8–9 • РЕД ОС 7.3–8 • Альт 8 СП релиз 10 (c10f2) • Альт 10–11
Требования к окружению	• Установленные драйверы (PKI-менеджеры) используемых смарт-карт и USB-токенов • Microsoft Edge 88.0.705.81 и выше • Google Chrome или Chromium 88.0.4324 и выше • Яндекс.Браузер 22.1.1 и выше • Mozilla Firefox 109.0.1 и выше • КриптоПро CSP 5.0 и выше для интеграции с КриптоПро DSS 2.0

Сетевое взаимодействие

На схеме представлена инфраструктура сетевого взаимодействия между компонентами Indeed CM.



Сервер

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 (исходящие подключения)	• 25 (TCP) • 465 (TCP) • 587 (TCP)

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 • 49152 - 65535 – случайный DCOM/RPC (TCP) порт верхнего диапазона Microsoft CA реализован с помощью технологии DCOM. По умолчанию приложения DCOM используют случайные номера TCP-портов верхнего диапазона, но есть возможность задать номер TCP-порта для удостоверяющего центра.
Aladdin Enterprise CA	443 (TCP)
SafeTech CA	• 9443 (TCP) – CA Gateway • 8443 (TCP) – KeyCloak
Dogtag CA	8443 (TCP) – веб-интерфейс и REST API
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

Устройства

В разделе перечислены устройства аутентификации и электронной подписи, которые поддерживаются в Indeed CM.

Windows

Производитель	Модель устройства
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 JaCarta-3 PKI/ГОСТ JaCarta-3 SE
Компания «Актив»	Рутокен PKI 1800 Рутокен Lite 1000 Рутокен Lite 1010 Рутокен S Рутокен ЭЦП Рутокен ЭЦП 2.0 2000 Рутокен ЭЦП 2.0 2100 Рутокен ЭЦП 2.0 3000 Рутокен ЭЦП 2.0 Flash 4500 Рутокен 2151 Рутокен ЭЦП 3.0 3100 Рутокен ЭЦП 3.0 NFC 3100 Рутокен ЭЦП 3.0 3100 SAM Рутокен ЭЦП 3.0 3120 Рутокен ЭЦП 3.0 3150 Рутокен ЭЦП 3.0 3220 Рутокен ЭЦП 3.0 3250 БИО

Производитель	Модель устройства
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
HID	Crescendo C1150 Series Crescendo C1300 Series Crescendo C2300 Series
ISBC	ESMART Token USB 64K ESMART Token USB 192K ESMART Token USB ГОСТ MS_KEY K-"Ангара" ESMART Token CARD 64K ESMART Token CARD 192K ESMART Token CARD ГОСТ
Kaztoken	Kaztoken Kaztoken SC
Microsoft	Реестр Локального компьютера Реестр Пользователя TPM Virtual Smart Card (Microsoft VSC) Windows Hello for Business (WHfB)
RSA	RSA SecurID 800

Производитель	Модель устройства
Thales (SafeNet и Gemalto)	SafeNet eToken PRO 32k SafeNet eToken PRO 64k eToken PRO Java 72K OS755 SafeNet eToken 5105 SafeNet eToken 5110 SafeNet eToken 5110 CC (940) IDCore30B eToken 1.7.7 SafeNet eToken 5300 SafeNet eToken Fusion SafeNet eToken Fusion CC IDPrime MD 830 FIPS IDPrime MD 830B FIPS IDPrime MD 840B IDPrime 930 IDPrime 930nc IDPrime 940 IDPrime 940B IDPrime MD 3810 IDPrime MD 3811 IDPrime 3930 IDPrime 3940 IDPrime 3940 FIDO
Yubico	YubiKey 5 Series

Linux

Производитель	Модель устройства
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 JaCarta-3 PKI/ГОСТ JaCarta-3 SE
Компания «Актив»	Рутокен PKI 1800 Рутокен ЭЦП Рутокен ЭЦП 2.0 2000 Рутокен ЭЦП 2.0 2100 Рутокен ЭЦП 2.0 3000 Рутокен ЭЦП 2.0 Flash 4500 Рутокен 2151 Рутокен ЭЦП 3.0 3100 Рутокен ЭЦП 3.0 NFC 3100 Рутокен ЭЦП 3.0 3100 SAM Рутокен ЭЦП 3.0 3120 Рутокен ЭЦП 3.0 3150 Рутокен ЭЦП 3.0 3220 Рутокен ЭЦП 3.0 3250 БИО
ISBC	ESMART Token USB 64K ESMART Token USB 192K ESMART Token USB ГОСТ ESMART Token CARD 64K ESMART Token CARD 192K ESMART Token CARD ГОСТ

Производитель	Модель устройства
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

ПРИМЕЧАНИЕ

Устройства Thales (SafeNet и Gemalto) поддерживают выпуск сертификатов только для ключей RSA.

Порядок установки

Подготовьте инфраструктуру для работы Indeed CM и установите серверные и клиентские компоненты.

Выберите инструкцию в зависимости от ОС рабочей станции, где вы планируете установить сервер Indeed CM.

Windows

Предварительные настройки инфраструктуры

1. Настройте каталог пользователей. 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.
3. Подготовьте удостоверяющий центр для работы с Indeed CM.
4. Выпустите SSL/TLS-сертификат для настройки защищенного соединения с сайтом Indeed CM.
5. Установите веб-сервер Internet Information Services (IIS).
6. Установите платформу .NET.

Установка и настройка Indeed CM

1. Установите сервер Indeed CM.
2. Настройте параметры работы Indeed CM в Мастере настройки.
3. Установите и настройте клиентские компоненты Indeed CM:
    1. Indeed CM Client Tools
    2. Indeed CM Middleware
4. Установите расширение Indeed CM Middleware в браузеры на рабочих станциях администраторов, операторов и пользователей.

Установка и настройка дополнительных компонентов

Кроме основных компонентов, для расширения функциональности Indeed CM доступны следующие компоненты:

- Indeed CM Event Log Proxy или Log Server для записи событий в единый журнал, если в инфраструктуре планируется развернуть несколько серверов Indeed CM.
- Indeed CM MS CA Proxy для подключения к центру сертификации Microsoft CA, если он находится за пределами домена сервера Indeed CM.
- Сервер OpenID Connect для настройки аутентификации в веб-сервисах Indeed CM по протоколу OpenID Connect.
- Indeed CM Agent – клиентский агент для управления устройствами на рабочих станциях пользователей. Агент лицензируется отдельно.

Linux

Предварительные настройки инфраструктуры

1. Настройте каталог пользователей. 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.
3. Подготовьте удостоверяющий центр для работы с Indeed CM. Для подключения к центру сертификации Microsoft CA установите компонент Indeed CM MS CA Proxy.
4. Выпустите SSL/TLS-сертификат для настройки защищенного соединения с сайтом Indeed CM.
5. Установите веб-сервер NGINX, Angie PRO или Apache HTTP Server и настройте в качестве обратного прокси-сервера.
6. Установите платформу .NET.

Установка и настройка Indeed CM

1. Установите и настройте серверные компоненты Indeed CM:
    1. Сервер Indeed CM

    2. Сервер OpenID Connect
    3. Indeed CM Event Log Proxy или Log Server для записи событий в единый журнал
2. Настройте параметры работы Indeed CM в Мастере настройки.
3. Установите и настройте клиентский компонент Indeed CM Middleware.
4. Установите расширение Indeed CM Middleware в браузеры на рабочих станциях администраторов, операторов и пользователей.

Установка и настройка дополнительных компонентов

Кроме основных компонентов, для расширения функциональности Indeed CM доступен Indeed CM Agent – клиентский агент для управления устройствами на рабочих станциях пользователей. Агент лицензируется отдельно.

Настройка окружения

Каталог пользователей

Настройка каталогов пользователей

Хранилище данных

Создание хранилища данных в Microsoft SQL, PostgreSQL и Postgres Pro

Удостоверяющие центры

Настройка удостоверяющих центров для интеграции с Indeed CM

Сервисные сертификаты

Подготовка SSL/TLS-сертификатов для настройки защищенного соединения с сервисами Indeed CM

Установка сертификатов в хранилище компьютера

Установка сертификатов RSA и ГОСТ на Windows и Linux

Веб-сервер

Настройка веб-сервера для работы серверных компонентов Indeed CM

Платформа .NET

Установка .NET для работы серверных компонентов Indeed CM

Каталог пользователей

Чтобы данные о пользователях появились в Indeed CM, настройте каталог пользователей.

Поддерживаются следующие службы каталогов:

LDAP

Active Directory, Samba AD DC, РЕД АДМ, Альт Домен, FreeIPA, ALD Pro, OpenLDAP

ЦР КриптоПро УЦ 2.0

Центр регистрации КриптоПро УЦ 2.0

Внутренний каталог пользователей

Внутренний каталог в базе данных Microsoft SQL или PostgreSQL

ПРИМЕЧАНИЕ

Внутренний каталог пользователей является дополнительным и использует хранилище базы данных Microsoft SQL или PostgreSQL.
Перед тем как подключить внутренний каталог, настройте основной каталог пользователей LDAP или в ЦР КриптоПро УЦ 2.0.

LDAP

Настройте каталог пользователей Indeed CM.

LDAP-каталог может быть составным. В этом случае пользователи расположены в разных контейнерах одного домена или в нескольких доменах.

Поддерживаются следующие службы LDAP-каталогов:

- Active Directory, Samba AD DC, РЕД АДМ, Альт Домен
- FreeIPA
- ALD Pro
- OpenLDAP

Active Directory, Samba AD DC, РЕД АДМ, Альт Домен

Подготовьте сервисную учетную запись для работы с Indeed CM.

Особенности настройки Samba AD DC, РЕД АДМ и Альт Домен

Samba AD DC, РЕД АДМ или Альт Домен могут быть настроены как дополнительный контроллер домена для Active Directory или как основной контроллер домена.

Существующая конфигурация

Если Indeed CM был ранее настроен на работу с каталогом пользователей в Active Directory и контроллер домена был перенастроен на Samba AD DC, РЕД АДМ или Альт Домен, то менять параметры каталога пользователей в Мастере настройки не требуется.

Новая конфигурация

При первой настройке подключения к каталогу пользователей выберите нужный тип каталога в Мастере настройки.

Создание сервисной учетной записи

В зависимости от используемой службы каталогов создайте сервисную учетную запись для чтения и записи атрибутов пользователей одним из следующих способов:

- В оснастке Active Directory (для Active Directory, Samba AD DC, РЕД АДМ и Альт Домен)
- С помощью инструмента командной строки samba-tool (для Samba AD DC, РЕД АДМ и Альт Домен)
- В веб-интерфейсе РЕД АДМ (только для РЕД АДМ)
- В оснастке ADMC (для Active Directory, Samba AD DC, РЕД АДМ и Альт Домен)

В оснастке Active Directory

1. Запустите оснастку **Active Directory — пользователи и компьютеры** (Active Directory Users and Computers).

2. Откройте контекстное меню объекта с конечными пользователями.
3. Выберите **Создать** (Create) → **Пользователь** (User).
4. Укажите имя сервисной учетной записи.
5. Заполните обязательные поля и нажмите **Готово**.

С помощью samba-tool

1. Выполните команду:

```
samba-tool user add <имя пользователя>
```

Пример

```
samba-tool user add servicecm
```

2. Если сервисная учетная запись будет использоваться для настройки ролей в Indeed CM, назначьте этой учетной записи атрибут UPN (User Principal Name):

```
sudo samba-tool user rename <имя пользователя> --upn=<UPN-имя пользователя>
```

Пример

```
sudo samba-tool user rename servicecm --upn=servicecm@domain.name
```

В веб-интерфейсе РЕД АДМ

1. Откройте веб-интерфейс РЕД АДМ и перейдите в раздел **Управление объектами домена** → **Пользователи**.
2. Нажмите **Создать**.
3. Укажите имя сервисной учетной записи.
4. Заполните обязательные поля и нажмите **Создать**.

В оснастке ADMC

1. Запустите модуль удаленного управления базой данных конфигурации (ADMC).
2. Откройте контекстное меню контейнера с конечными пользователями и выберите **Создать** → **Пользователь**.

3. Укажите имя сервисной учетной записи.
4. Заполните обязательные поля и нажмите **ОК**.

Настройка разрешений

Разрешения настраиваются для всех каталогов (Active Directory, Samba AD DC, РЕД АДМ, Альт Домен) в оснастке **Active Directory — пользователи и компьютеры** (Active Directory Users and Computers).

1. Запустите оснастку **Active Directory — пользователи и компьютеры** (ADUC).
2. Откройте свойство **Безопасность** (Security) объекта, где хранятся пользователи Indeed CM, и нажмите **Дополнительно** (Advanced). 3. 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 и нажмите **ОК**.
4. В выпадающем списке **Применяется к** (Applies to) выберите **Дочерние объекты: Пользователь** (Descendant User objects).
5. В списке **Разрешения** (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.
6. В списке **Свойства** (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.
   - **Запись: userAccountControl** (Write userAccountControl) для работы опции **Требовать логон по смарт-карте**.
   - **Запись: userCertificate** (Write userCertificate) для публикации сертификата КриптоПро УЦ 2.0, Aladdin eCA, SafeTech CA, Валидата УЦ в профиле пользователя в LDAP-каталоге.
7. Нажмите **ОК** и **Применить** (Apply).

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

Настройка прав на чтение данных

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. Права на чтение данных настраиваются для всех каталогов (Active Directory, Samba AD DC, РЕД АДМ, Альт Домен) в оснастке **Редактирование ADSI** (ADSI edit).

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 **Разрешения** (Permissions) отметьте **Список содержимого** (List contents).
    2. В списке **Свойства** (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 **Разрешения** (Permissions) отметьте **Список содержимого** (List contents).
    2. В списке **Свойства** (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)

Список атрибутов для работы с каталогом пользователей

В списке приведены отображаемые имена LDAP (LDAP Display Name).

> **ПРИМЕЧАНИЕ**
>
> Предоставление прав доступа к набору свойств значительно улучшает производительность и упрощает управление безопасностью (подробнее на сайте компании Microsoft).

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).
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).

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

FreeIPA

Подготовьте сервисную учетную запись для работы с каталогом пользователей Indeed CM.

1. Войдите в веб-версию FreeIPA под учетной записью администратора.
2. Создайте сервисную учетную запись для работы с каталогом пользователей:
    1. На вкладке **Идентификация** (Identity) → **Пользователи** (Users) нажмите **Добавить** (Add).
    2. Создайте пользователя. По умолчанию созданный пользователь состоит в служебной доменной группе ipausers.
3. Создайте разрешение для чтения и поиска данных в каталоге:
    1. На вкладке **IPA-сервер** (IPA Server) в выпадающем списке **Управление доступом на основе ролей** (Role-Based Access Control) выберите **Разрешения** (Permissions) и нажмите **Добавить** (Add).
    2. Укажите имя разрешения.
    3. В строке **Тип правила привязки** (Bind rule type) выберите **permission**.
    4. В строке **Предоставленные права** (Granted Rights) выберите `read`, `search`.
    5. В строке **Поддерево** (Subtree) введите имя домена в формате Distinguished name.
    6. Выберите **Действующие атрибуты** (Effective attributes): `entryUUID`.
4. Создайте разрешение для записи данных в каталог:
    1. На вкладке **IPA-сервер** (IPA Server) в выпадающем списке **Управление доступом на основе ролей** (Role-Based Access Control) выберите **Разрешения** (Permissions) и нажмите **Добавить** (Add).
    2. Укажите имя разрешения.
    3. В строке **Тип правила привязки** (Bind rule type) выберите **permission**.
    4. В строке **Предоставленные права** (Granted Rights) выберите `write`.
    5. В выпадающем списке **Тип** (Type) выберите **Пользователь**.
    6. Выберите **Действующие атрибуты** (Effective attributes):

    - `userPassword` для возможности сбросить пароль пользователя
    - `krbPasswordExpiration` для возможности указать срок действия пароля пользователя
    - `userCertificate` для публикации сертификата КриптоПро 2.0 в профиле пользователя
    - `jpegPhoto` для загрузки фотографии пользователя

5. В выпадающем списке **Управление доступом на основе ролей** (Role-Based Access Control) выберите **Привилегии** (Privileges) и нажмите **Добавить** (Add).
6. Создайте привилегию и добавьте в нее созданные разрешения.
7. В выпадающем списке **Управление доступом на основе ролей** (Role-Based Access Control) выберите **Роли** (Roles), нажмите **Добавить** (Add) и создайте роль.
8. В разделе **Роли** (Roles) перейдите на вкладку **Привилегии** (Privileges) и добавьте созданную привилегию в роль.
9. Назначьте роль на пользователя:
    1. В разделе **Роли** (Roles) выберите созданную роль.
    2. В открывшемся списке пользователей нажмите **Добавить** (Add) и выберите созданного пользователя.

Список атрибутов для работы с каталогом пользователей

Атрибут пользователя	Описание
entryUUID	Универсальный уникальный идентификатор записи
entryDN	Уникальное имя записи в каталоге
uid	Идентификатор пользователя
mail	Адрес электронной почты
telephoneNumber	Телефон
givenName	Имя
sn	Фамилия
cn	Общее имя
krbPrincipalName	Имя участника-пользователя Kerberos (UPN)
jpegPhoto	Фото
userPassword	Пароль

Атрибут пользователя	Описание
krbPasswordExpiration	Атрибут, хранящий дату и время истечения срока действия текущего пароля
userCertificate	Сертификат

ALD Pro

Подготовьте сервисную учетную запись для работы с каталогом пользователей Indeed CM.

1. Войдите в веб-версию ALD Pro под учетной записью администратора.
2. Создайте сервисную учетную запись для работы с каталогом пользователей и назначьте необходимые привилегии:
    1. Запустите оснастку ALD Pro **Пользователи и компьютеры**, в выпадающем меню выберите **Пользователи**.
    2. Нажмите **Новый пользователь** и создайте пользователя. По умолчанию созданный пользователь состоит в служебной доменной группе ipausers.
3. Чтобы создать разрешения, привилегии и роль для работы с каталогом пользователей, используйте оболочку FreeIPA в ALD Pro: в адресной строке замените `ad` на `ipa`. Например, `https://dc/ipa/ui/#/login`.
4. Создайте разрешение для чтения и поиска данных в каталоге:
    1. На вкладке **IPA-сервер** (IPA Server) в выпадающем списке **Управление доступом на основе ролей** (Role-Based Access Control) выберите **Разрешения** (Permissions) и нажмите **Добавить** (Add).
    2. Укажите имя разрешения.
    3. В строке **Тип правила привязки** (Bind rule type) выберите **permission**.
    4. В строке **Предоставленные права** (Granted Rights) выберите `read`, `search`.
    5. В строке **Поддерево** (Subtree) укажите имя объекта с пользователями или имя домена в формате Distinguished name.
    6. Выберите **Действующие атрибуты** (Effective attributes): `entryUUID`.
5. Создайте разрешение для записи данных в каталог:
    1. На вкладке **IPA-сервер** (IPA Server) в выпадающем списке **Управление доступом на основе ролей** (Role-Based Access Control) выберите **Разрешения** (Permissions) и нажмите **Добавить** (Add).
    2. Укажите имя разрешения.
    3. В строке **Тип правила привязки** (Bind rule type) выберите **permission**.
    4. В строке **Предоставленные права** (Granted Rights) выберите `write`.
    5. В выпадающем списке **Тип** (Type) выберите **Пользователь**.
    6. Выберите **Действующие атрибуты** (Effective attributes):
    - `userPassword` для возможности сбросить пароль пользователя

- `krbPasswordExpiration` для возможности указать срок действия пароля пользователя
- `userCertificate` для публикации сертификата КриптоПро 2.0 в профиле пользователя
- `jpegPhoto` для загрузки фотографии пользователя

6. В выпадающем списке **Управление доступом на основе ролей** (Role-Based Access Control) выберите **Привилегии** (Privileges) и нажмите **Добавить** (Add).
7. Создайте привилегию и добавьте в нее созданные разрешения.
8. В выпадающем списке **Управление доступом на основе ролей** (Role-Based Access Control) выберите **Роли** (Roles), нажмите **Добавить** (Add) и создайте роль.
9. В разделе **Роли** (Roles) перейдите на вкладку **Привилегии** (Privileges) и добавьте созданную привилегию в роль.
10. Назначьте роль на пользователя:
    1. В разделе **Роли** (Roles) выберите созданную роль.
    2. В открывшемся списке пользователей нажмите **Добавить** (Add) и выберите созданного пользователя.

Список атрибутов для работы с каталогом пользователей

Атрибут пользователя	Описание
entryUUID	Универсальный уникальный идентификатор записи
entryDN	Уникальное имя записи в каталоге
uid	Идентификатор пользователя
mail	Адрес электронной почты
telephoneNumber	Телефон
givenName	Имя
sn	Фамилия
cn	Общее имя

Атрибут пользователя	Описание
krbPrincipalName	Имя участника-пользователя Kerberos (UPN)
jpegPhoto	Фото
userPassword	Пароль
krbPasswordExpiration	Атрибут с датой и временем истечения срока действия текущего пароля
userCertificate	Сертификат

OpenLDAP

Подготовьте сервисную учетную запись для работы с каталогом пользователей Indeed CM. Во всех примерах файлов и команд указаны шаблонные значения. Замените их на реальные значения.

1. Создайте сервисную учетную запись. Например, с помощью файла LDIF.

    1. Создайте файл LDIF.

    Пример файла

    ```
    cat > create_service_user.ldif <<EOF
    dn: cn=servicecm,ou=users,dc=domain,dc=loc
    objectClass: inetOrgPerson
    objectClass: posixAccount
    objectClass: top
    uid: servicecm
    cn: Service Account
    sn: CM
    userPassword: {SSHA}XiU3Tq7V8fQzJm5nLoP9rStYw12AbCdE
    uidNumber: 900
    gidNumber: 900
    homeDirectory: /home/servicecm
    EOF
    ```

    2. Добавьте пользователя в каталог.

    Пример команды

    ```
    ldapadd -x -D "cn=admin,dc=domain,dc=loc" -W -f create_service_user.ldif
    ```

    3. Установите пароль для пользователя. Дважды введите пароль изменяемой записи, а затем — пароль записи `cn=admin,dc=domain,dc=loc`.

    Пример команды

    ```
    ldappasswd -xWD cn=admin,dc=domain,dc=loc -S cn=servicecm,ou=users,dc=domain,dc=loc
    ```

2. Выдайте созданному пользователю разрешения на чтение, поиск и запись данных в каталог.

1. Создайте файл LDIF для ACL базы данных с пользователями и группами. Например, *servicecm.acl.ldif*.

Пример файла

```
cat > servicecm.acl.ldif <<EOF
dn: olcDatabase={1}mdb,cn=config
changetype: modify
replace: olcAccess
olcAccess: {0}to *
  by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" manage
  by * break
olcAccess: {1}to attrs=userPassword
  by self write
  by anonymous auth
  by dn.base="cn=servicecm,ou=users,dc=domain,dc=loc" write
  by * none
olcAccess: {2}to attrs=jpegPhoto
  by self write
  by dn.base="cn=servicecm,ou=users,dc=domain,dc=loc" write
  by * read
olcAccess: {3}to *
  by self read
  by dn.base="cn=servicecm,ou=users,dc=domain,dc=loc" read
EOF
```

2. Примените изменения.

Пример команды

```
ldapmodify -x -D "cn=admin,cn=config" -W -f servicecm.acl.ldif
```

Список атрибутов для работы с каталогом пользователей

Атрибут пользователя	Описание
entryUUID	Универсальный уникальный идентификатор записи
entryDN	Уникальное имя записи в каталоге
uid	Идентификатор пользователя
mail	Адрес электронной почты

Атрибут пользователя	Описание
telephoneNumber	Телефон
givenName	Имя
sn	Фамилия
cn	Общее имя
jpegPhoto	Фото
userPassword	Пароль

ЦР КриптоПро УЦ 2.0

Чтобы настроить каталог пользователей:

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

Разрешение	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

Разрешение	Тип объекта	Комментарий
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 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.

Внутренний каталог пользователей

С помощью внутреннего каталога вы можете создавать в Indeed CM учетные записи для внешних пользователей. Внутренний каталог пользователей настраивается в базе данных Microsoft SQL или PostgreSQL.

Внутренний каталог является дополнительным. Перед тем как подключить внутренний каталог, настройте основной каталог пользователей LDAP или в ЦР КриптоПро УЦ 2.0.

Настройка базы данных

Чтобы настроить базу данных для внутреннего каталога пользователей:

1. Создайте базу данных.
2. Настройте сервисную учетную запись.
3. Используйте скрипт из дистрибутива Indeed CM, чтобы наполнить базу данных.

Microsoft SQL

База данных

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

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

Сервисная учетная запись

Используйте локальную учетную запись Microsoft SQL или учетную запись из поддерживаемого LDAP-каталога и наделите ее необходимыми правами для работы с созданной базой данных. Эта учетная запись используется для выполнения операций чтения и записи в базу данных.

1. Определите **Имя для входа** (Logins) для созданной базы.
2. Нажмите **Безопасность** (Security) → **Имя для входа** (Logins) и из списка выберите учетную запись.

3. Перейдите на вкладку **Сопоставление пользователей** (User Mapping).
4. Укажите разрешения **db_owner** и **public** и нажмите **ОК**.

Наполнение базы данных

В **Обозревателе объектов** (Object Explorer) выберите созданную базу данных и выполните скрипт *UserCatalog.sql*:

1. Выберите **Файл** (File) → **Открыть** (Open) → **Файл**...(File...), укажите путь к файлу *UserCatalog.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, или выберите базу данных в выпадающем списке.
3. Нажмите **Выполнить** (Execute).

PostgreSQL

Сервисная учетная запись

1. Откройте pgAdmin, укажите мастер пароль и подключитесь к серверу.
2. В разделе **Обозреватель** (Browser) правой кнопкой мыши нажмите на вкладку **Роли входа/группы** (Login/Group Roles).
3. Выберите **Создать** (Create) → **Роль входа/группы** (Login/Group Role…).
4. На вкладке **Общие** (General) в поле **Имя** (Name) укажите имя пользователя.
5. На вкладке **Определение** (Definition) в поле **Пароль** (Password) укажите пароль пользователя. Убедитесь, что в поле **Роль активна до** (Account Expires) указано значение **No Expiry**.
6. На вкладке **Права** (Privileges) включите параметр **Вход разрешен?** (Can Login?), оставьте остальные значения по умолчанию и нажмите **Сохранить** (Save).

База данных

Создайте базу данных в среде pgAdmin:

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

3. На вкладке **Общие** (General) укажите имя базы данных, в списке **Владелец** выберите созданную сервисную учетную запись и нажмите **Сохранить** (Save).

Наполнение базы данных

Выберите в **Обозревателе** (Browser) созданную базу данных, выполните скрипт *UserCatalog-Postgre.sql* и предоставьте сервисной учетной записи привилегии на таблицы базы данных:

1. Выберите **Инструменты** (Tools) → **Запросник** (Query Tool).
2. В меню запросника нажмите  и укажите путь к файлу *UserCatalog-Postgre.sql* (*IndeedCM.WindowsServer\Misc*). Нажмите **Выбрать** (Select).
3. В меню запросника нажмите **Выполнить** (Execute/Refresh)  .
4. Нажмите  и выберите **Clear Query**, чтобы очистить поле запроса к базе данных.
5. Введите текст запроса, указав в запросе имя учетной записи.

   Пример запроса

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

6. Нажмите **Выполнить** (Execute/Refresh)  .

Удаленное подключение к базе данных

1. Откройте конфигурационный файл *pg_hba.conf*.

Расположение файла *pg_hba.conf*

PostgreSQL

ОС Windows: *C:\Program Files\PostgreSQL\<номер версии>\data*
ОС Linux: */etc/postgresql/<номер версии>/main* или */var/lib/pgsql/<номер версии>/data*

Postgres Pro

ОС Linux: */var/lib/pgpro/<номер версии>/data*

2. Добавьте строку в следующем формате.

```
CONNECTIONTYPE DATABASE USER ADDRESS METHOD
```

Где:

- `CONNECTIONTYPE` – тип подключения. Укажите `host`, чтобы использовать подключение по TCP/IP.
- `DATABASE` – имя базы данных, для которой предоставляется доступ.
- `USER` – имя пользователя, для которого 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
```

Список атрибутов

Для работы с внутренним каталогом пользователей Indeed CM использует следующие атрибуты.

Основные атрибуты

Атрибут пользователя	Общее имя атрибута	Отображаемое имя атрибута
cn	Common Name	Общее имя
dn	Distinguished Name	Уникальное имя
givenName	First Name	Имя
sn	Last Name	Фамилия
sAMAccountName	Logon Name	Логин
email	E-mail	Адрес электронной почты

Дополнительные атрибуты

Атрибут пользователя	Отображаемое имя атрибута
telephoneNumber	Телефонный номер
countryName	Страна/регион
stateOrProvinceName	Область
localityName	Город
streetAddress	Адрес
organizationName	Организация
organizationUnitName	Подразделение
title	Должность

В Мастере настройки Indeed CM можно редактировать дополнительные атрибуты и добавить собственные.

Как настроить дополнительные атрибуты внутреннего каталога пользователей

Хранилище данных

Создайте основную базу данных для работы Indeed Certificate Manager. Дополнительно вы можете создать отдельные базы данных для сервера OIDC и для компонента Log Server.

Для подключения к каждой базе данных требуется сервисная учетная запись, от имени которой выполняются запросы на поиск, чтение и запись данных. Вы можете использовать отдельную учетную запись для каждой базы или общую учетную запись для всех баз данных.

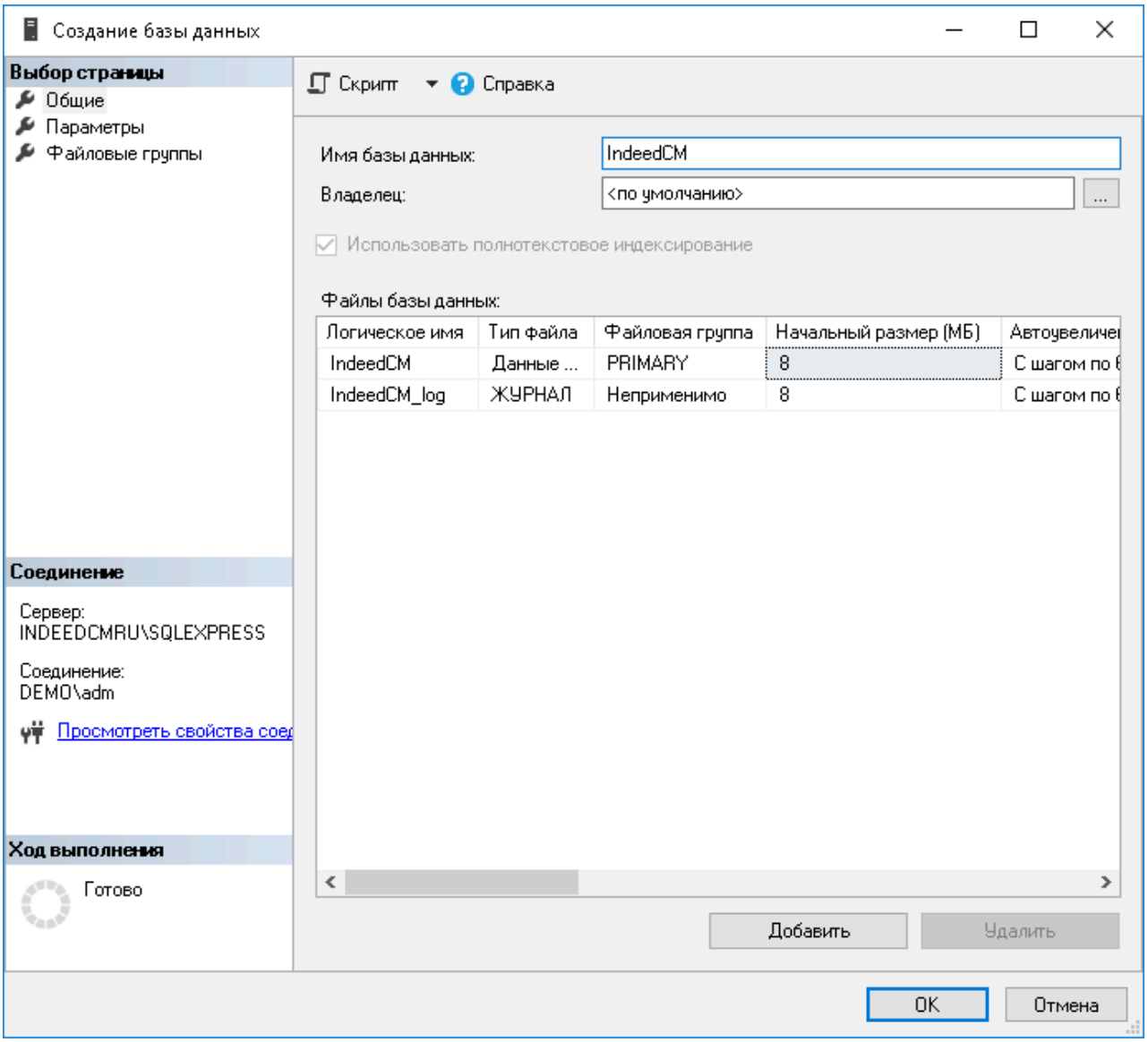
Indeed Certificate Manager поддерживает работу с базами данных Microsoft SQL Server, PostgreSQL и Postgres Pro.

Microsoft SQL

Создание базы данных

Создайте базу данных в среде SQL Server Management Studio.

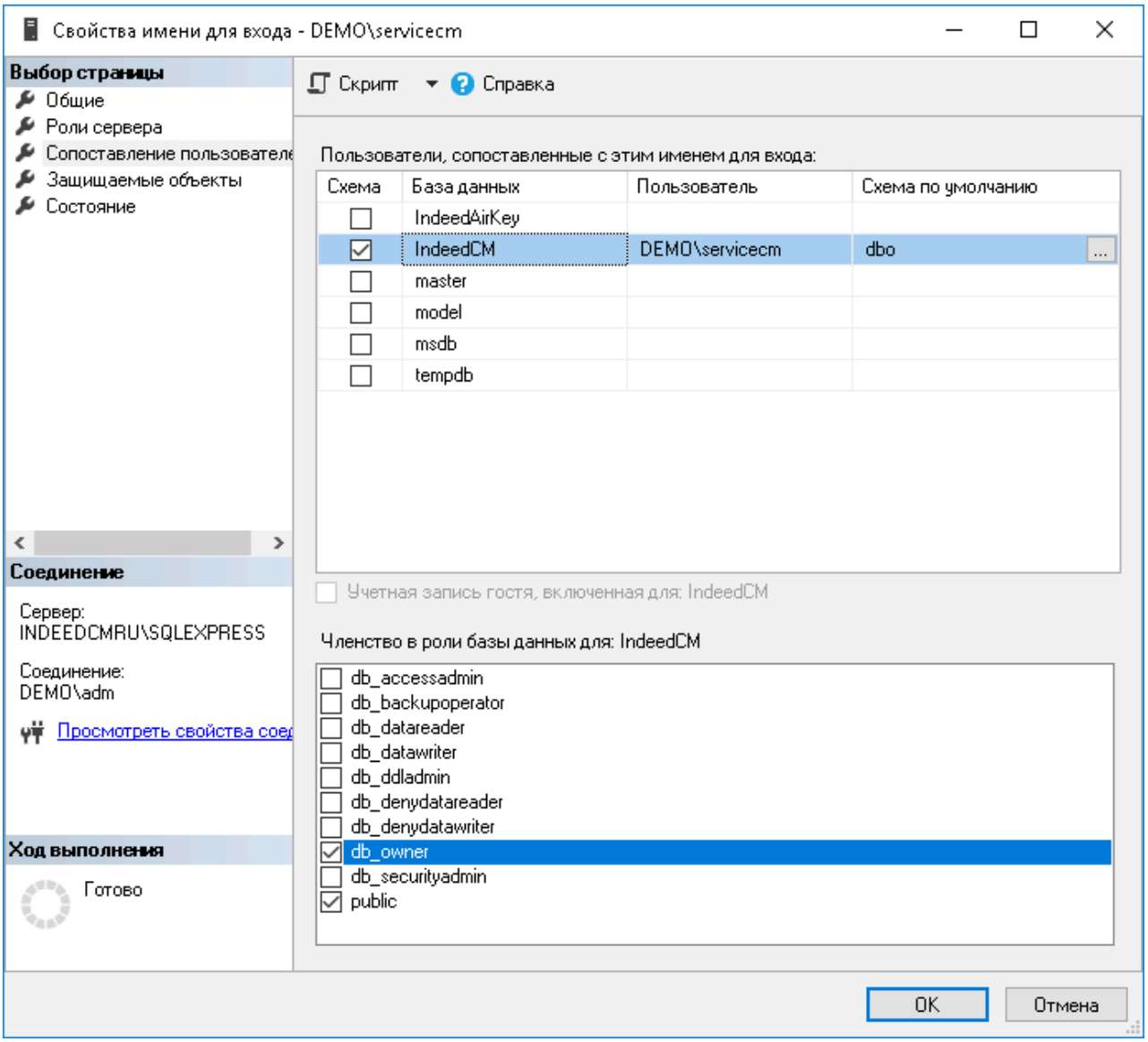
1. В окне **Обозреватель объектов** (Object Explorer) нажмите правой кнопкой мыши на **Базы данных** (Databases).
2. Выберите **Создать базу данных...** (New Database...).
3. Укажите **Имя базы данных:** (Database name:) и нажмите **OK**.



Настройка сервисной учетной записи

Используйте локальную учетную запись Microsoft SQL или учетную запись из поддерживаемого LDAP-каталога. Выдайте учетной записи права для работы с созданной базой данных. Эта учетная запись используется для выполнения операций чтения и записи в базу данных.

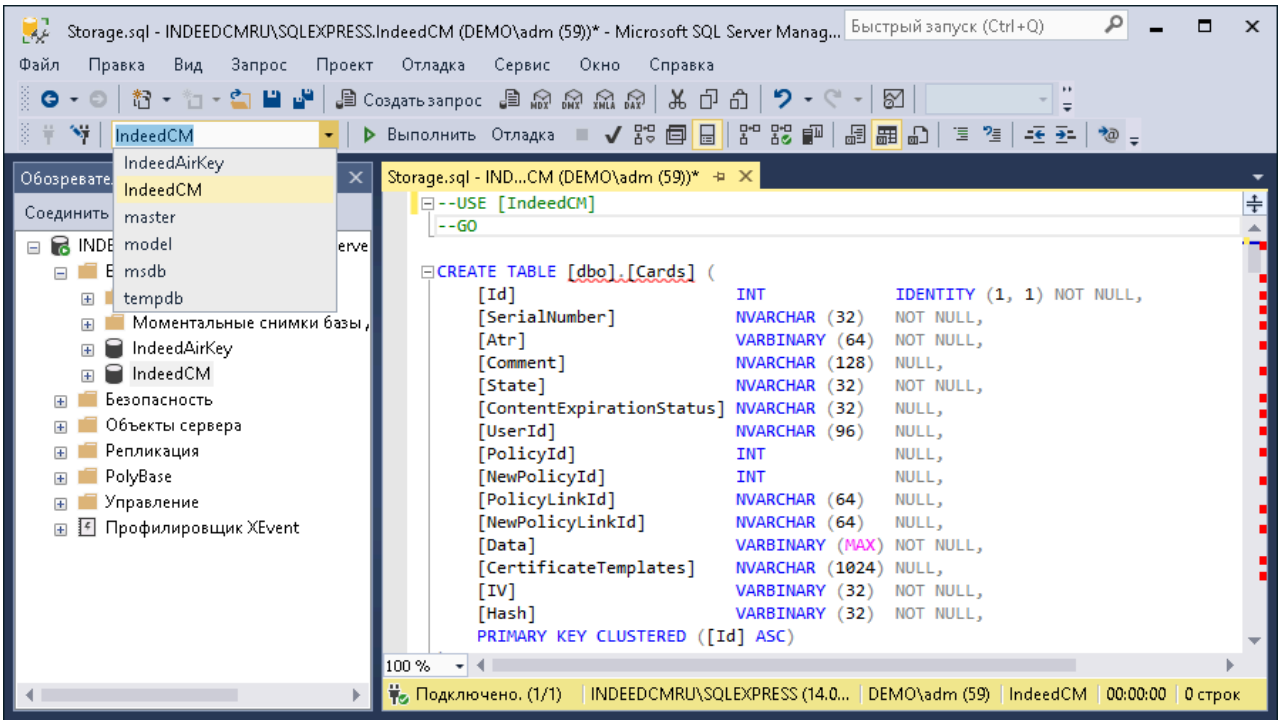
1. Определите **Имя для входа** (Logins) для созданной базы.
2. Нажмите **Безопасность** (Security) → **Имя для входа** (Logins), из списка выберите учетную запись.
3. Перейдите на вкладку **Сопоставление пользователей** (User Mapping).
4. Выдайте права на работу с базой для выбранного имени входа, укажите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



Наполнение базы данных

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: **--USE[Indeed CM]--GO**. Или выберите необходимую базу данных в выпадающем меню.
3. Нажмите **Выполнить** (Execute).



PostgreSQL и Postgres Pro

Настройте базу данных одним из следующих способов:

- В графическом интерфейсе pgAdmin
- С помощью командной строки psql

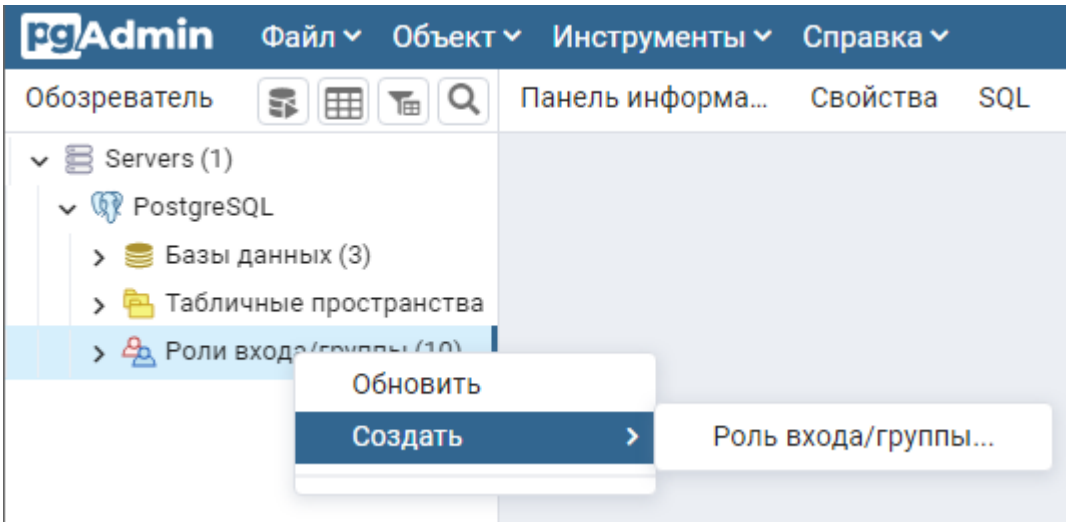
В качестве примера для имени сервисной учетной записи в инструкциях используется *servicepg*, для имени базы данных — *indeedstorage*.

pgAdmin

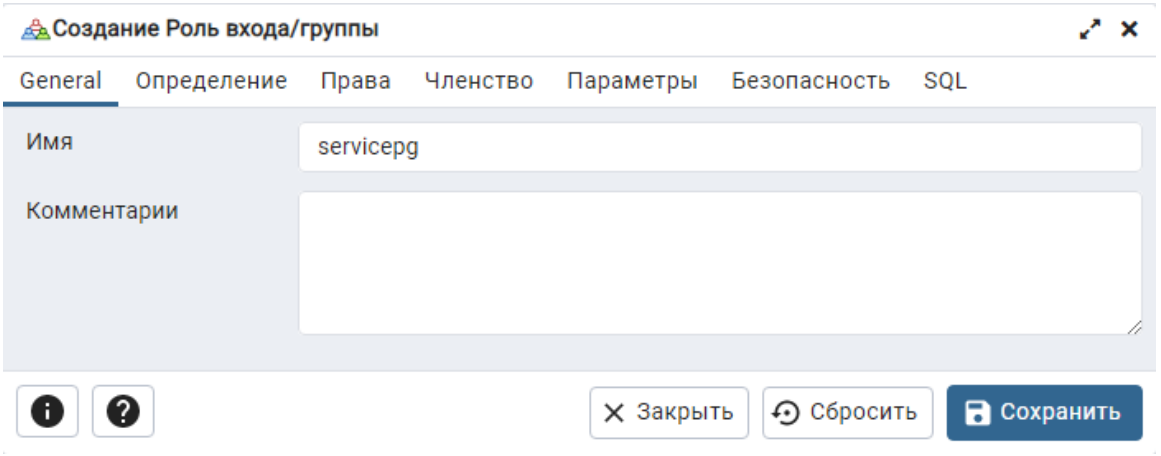
Создание сервисной учетной записи

1. Откройте pgAdmin, укажите мастер пароль и подключитесь к серверу.

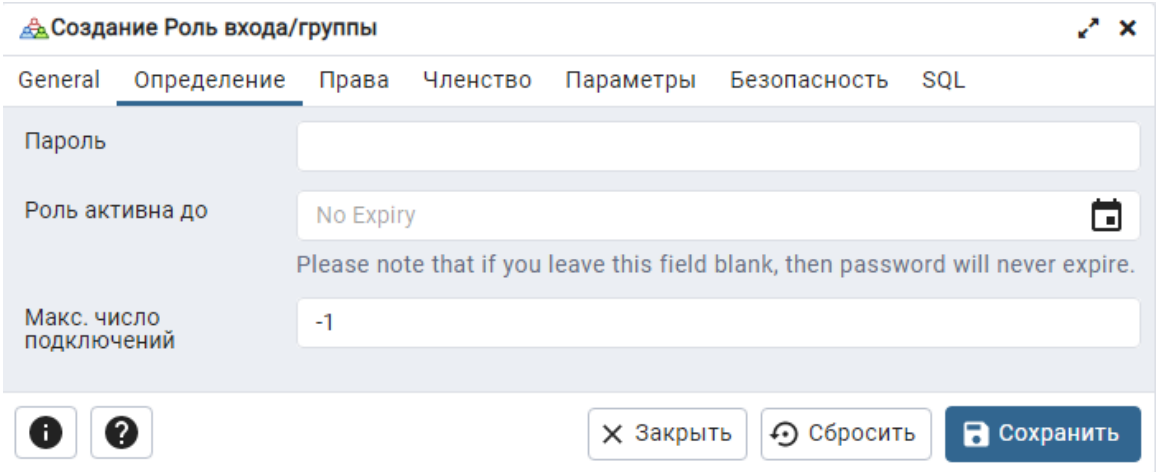
2. В разделе **Обозреватель** (Browser) правой кнопкой мыши нажмите по пункту меню **Роли входа/группы** (Login/Group Roles)и выберите **Создать** → **Роль входа/группы** (Create → Login/Group Role…).



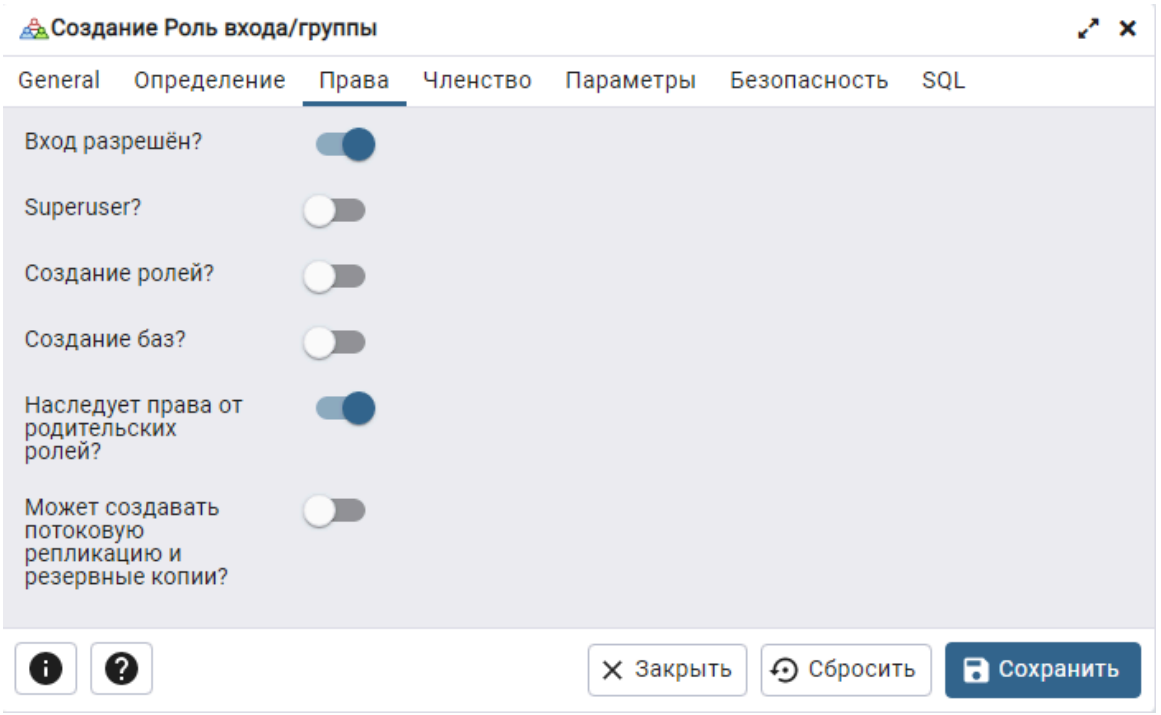
3. На вкладке **Общие** (General) укажите имя пользователя в поле **Имя** (Name).



4. Перейдите на вкладку **Определение** (Definition) и в поле **Пароль** (Password) укажите пароль пользователя. В поле **Роль активна до** (Account Expires) укажите значение **No Expiry**. При создании сервисной учетной записи требуется отключить срок действия пароля.

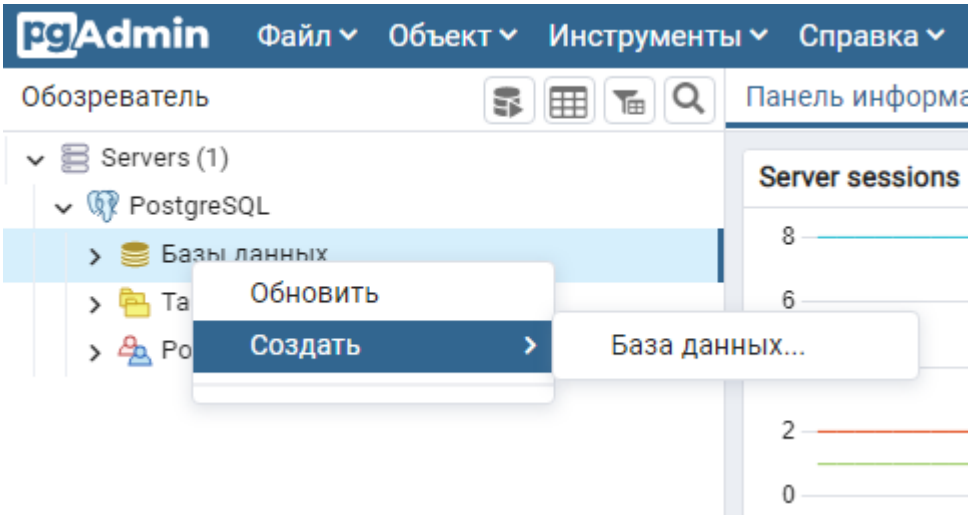


5. На вкладке **Права** (Privileges) включите параметр **Вход разрешен?** (Can Login?), оставьте остальные значения по умолчанию и нажмите **Сохранить** (Save).

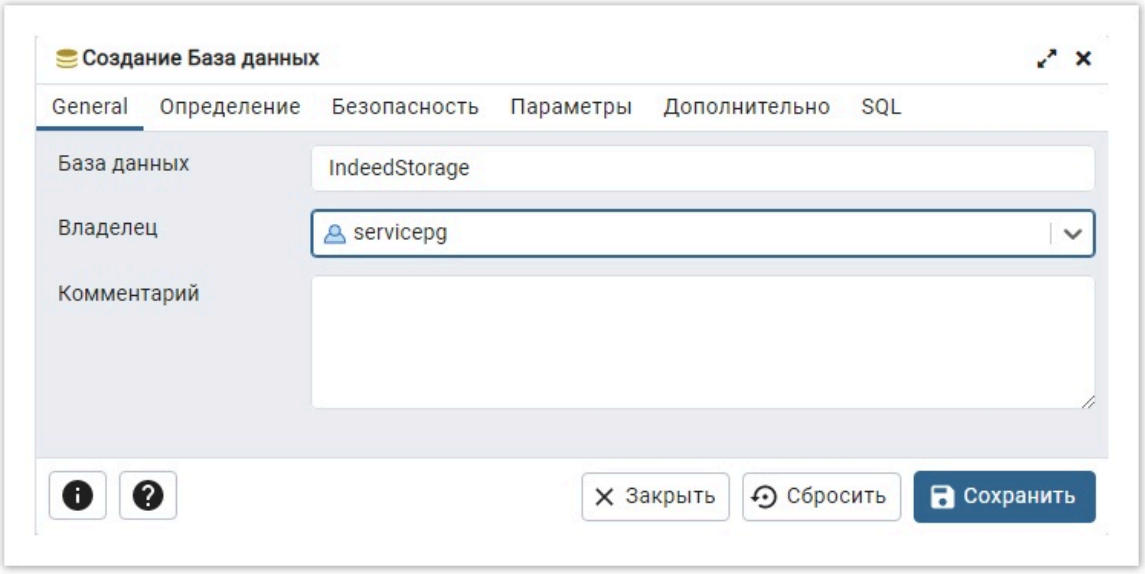


Создание и наполнение базы данных

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

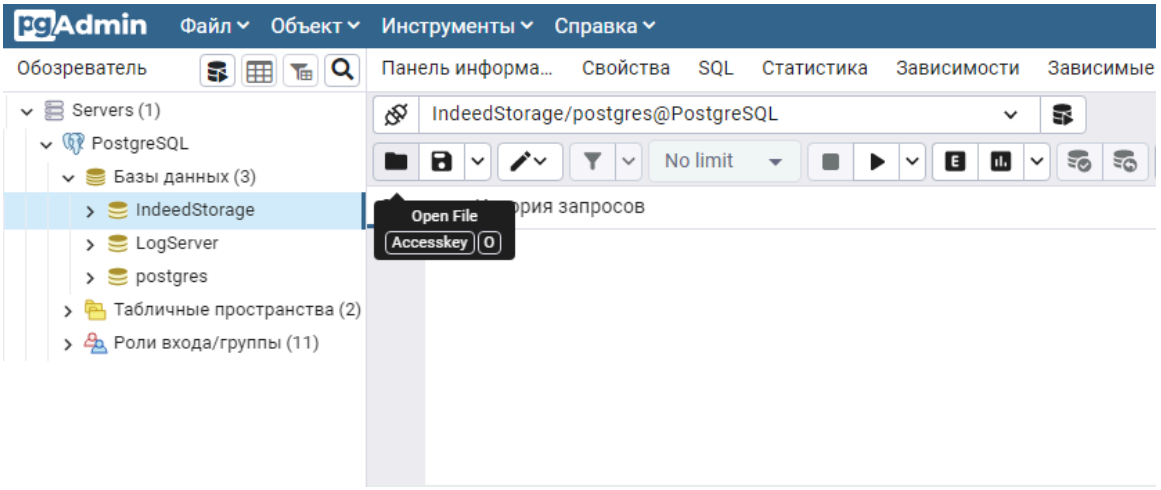


2. На вкладке **Общие** (General) укажите название базы данных в поле **База данных** (Database), в списке **Владелец** (Owner) выберите пользователя (сервисную учетную запись) и нажмите **Сохранить** (Save).

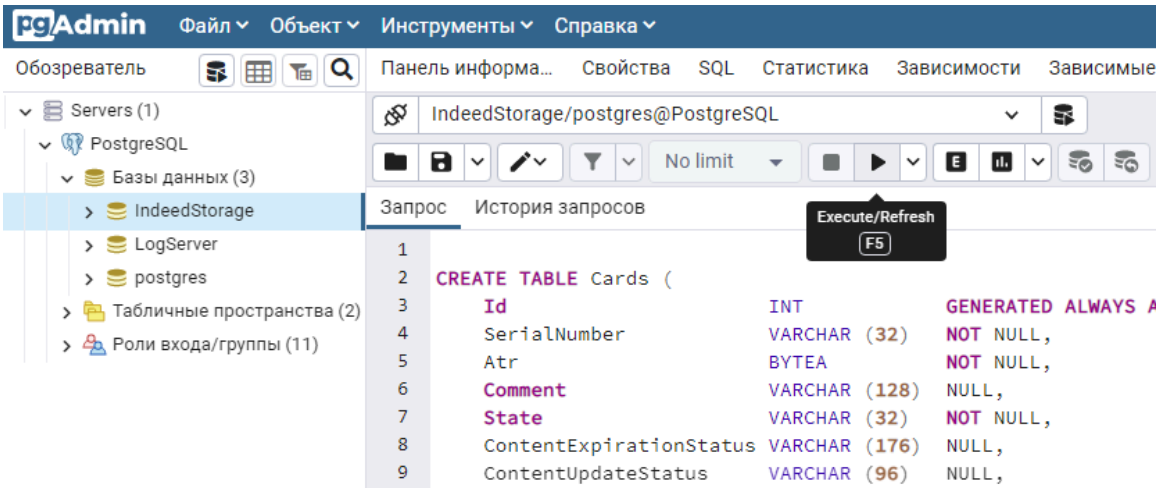


3. Выберите в **Обозревателе** (Browser) созданную базу данных и выполните скрипт *Storage-Postgre.sql*:

    1. Нажмите **Инструменты** (Tools) → **Запросник** (Query Tool).
    2. В меню запросника нажмите  и укажите путь к файлу *Storage-Postgre.sql* (*IndeedCM.Server\Misc*). Нажмите **Выбрать** (Select).

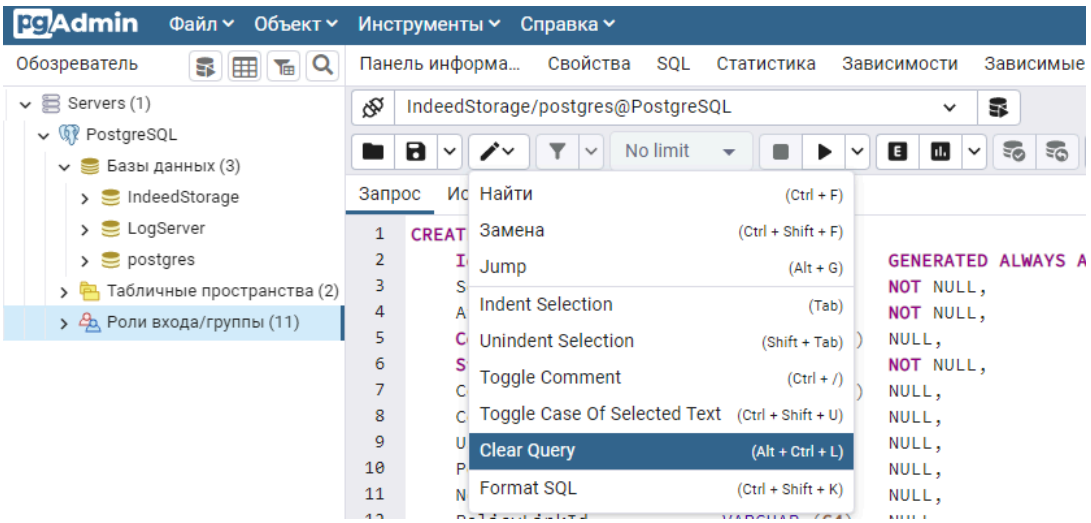


    3. Нажмите **Выполнить** (Execute/Refresh)  .



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

    1. В меню запросника нажмите  и выберите **Clear Query**, чтобы очистить поле запроса к базе данных.



    2. Введите текст запроса. В запросе укажите имя сервисной учетной записи.

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

    3. Нажмите **Выполнить** (Execute/Refresh)  .

Командная строка psql

1. Запустите командную строку от имени администратора.

2. Подключитесь к серверу PostgreSQL от имени пользователя postgres:

```
sudo -u postgres psql
```

3. Создайте сервисную учетную запись и установите пароль:

```
CREATE USER servicepg WITH PASSWORD 'password';
```

4. Создайте базу данных и назначьте сервисную учетную запись ее владельцем:

```
CREATE DATABASE indeedstorage OWNER servicepg;
```

5. Подключитесь к созданной базе данных:

```
\c indeedstorage
```

6. Наполните базу данных с помощью скрипта *Storage-Postgre.sql*. Файл скрипта находится в каталоге *Misc* дистрибутива Indeed CM.

```
\i IndeedCM.Linux-<номер версии>\IndeedCM.LinuxServer-<номер версии>\Misc\Storage-Postgre.sql
```

7. Предоставьте сервисной учетной записи доступ к базе данных:

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

Удаленное подключение к базе данных

Откройте конфигурационный файл *pg_hba.conf*.

Расположение файла *pg_hba.conf*

PostgreSQL

ОС Windows: *C:\Program Files\PostgreSQL\<номер версии>\data*
ОС Linux: */etc/postgresql/<номер версии>/main* или */var/lib/pgsql/<номер версии>/data*

Postgres Pro

ОС Linux: */var/lib/pgpro/<номер версии>/data*

Добавьте строку следующего формата:

```
CONNECTIONTYPE DATABASE USER ADDRESS METHOD
```

Где:

- `CONNECTIONTYPE` – тип подключения. Укажите `host`, чтобы использовать подключение по TCP/IP.
- `DATABASE` – имя базы данных, для которой предоставляется доступ.
- `USER` – имя пользователя, для которого 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
```

Удостоверяющие центры

Microsoft CA

Настройка Microsoft CA

Aladdin Enterprise CA

Настройка Aladdin Enterprise CA

SafeTech CA

Настройка SafeTech CA

Dogtag CA

Настройка Dogtag CA

КриптоПро УЦ 2.0

Настройка КриптоПро УЦ 2.0

КриптоПро DSS 2.0

Настройка КриптоПро DSS 2.0

Валидата УЦ

Настройка Валидата УЦ

Microsoft CA

Чтобы настроить работу Indeed CM с Microsoft Enterprise CA:

1. Создайте сервисную учетную запись.
2. Подготовьте шаблоны сертификатов.
3. Добавьте 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 MS CA Proxy, если:

- Microsoft Enterprise CA располагается за пределами домена, в котором находится сервер Indeed CM на ОС Windows.
- Сервер Indeed CM установлен на ОС Linux.

Создание сервисной учетной записи

Создайте сервисную учетную запись, от имени которой Indeed CM будет создавать запросы на сертификаты пользователей в Microsoft CA. Если вы планируете использовать Indeed CM с несколькими центрами сертификации (ЦС), сервисная учетная запись должна иметь одинаковый набор привилегий для всех ЦС.

1. Создайте учетную запись пользователя в Active Directory.
2. Откройте оснастку **Центр сертификации** (Certification Authority), выберите ЦС 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.
   Если вы планируете использовать Indeed CM с несколькими центрами сертификации (ЦС), сервисная учетная запись должна иметь одинаковый набор привилегий для всех ЦС.
5. Нажмите **ОК**.

ПОДСКАЗКА

Включите разрешение **Управлять ЦС** (Manage CA), чтобы иметь возможность **Публиковать список отозванных сертификатов** при настройке шаблонов сертификатов для Microsoft CA в Indeed CM.

Подготовка шаблонов сертификатов

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

Агент Регистрации

Сертификат **Агент регистрации** (Enrollment Agent) – это обязательный сертификат, который позволяет создавать запросы на 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.

Чтобы создать 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. В окне **Свойства нового шаблона** 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. Из списка политик применения выберите **Проверка подлинности клиента** (Client Authentication) и 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 и нажмите **ОК**.
    2. В разделе **Разрешения для группы** (Permissions for) установите **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) 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.

   Подробнее о минимальном размере ключа

   Минимальный размер ключа можно настроить 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. Включите опцию **Одобрения диспетчера сертификатов ЦС** (CA certificate manager approval).
   2. Включите опцию **Указанного числа авторизованных подписей** (This number of authorized signatures) и укажите число подписей, равное **1** (значение по умолчанию).
   3. Из списка **В подписи требуется указать тип политики** (Policy type required in signature) выберите **Политики применения** (Application Policy).
   4. Из списка **Политика применения** (Application Policy) выберите **Агент запроса сертификата** (Certificate Request Agent).
   5. В разделе **Требовать для повторной регистрации** (Require the following for reenrollment) выберите параметр **Тех же условий, что и для регистрации** (Same criteria as for enrollment).

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 этому 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. Из списка **Формат имени субъекта** (Subject name format) выберите **Полное различающееся имя** (Fully distinguished name).
2. Включите опцию **Имя субъекта-пользователя (UPN)** (User principal name (UPN)).
3. Если по этому шаблону будут выпускаться сертификаты для пользователей, у которых не указан адрес электронной почты в Active Directory, отключите опции **Включить имя электронной почты в имя субъекта** (Include e-mail name in subject name) и **Имя электронной почты** (E-mail name).

Предоставляется в запросе

Выберите **Предоставляется в запросе** (Supply in the request), если по этому 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 формируется 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 и нажмите **ОК**.
    2. В разделе **Разрешения для группы** (Permissions for) установите **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, чтобы от его имени Indeed CM создавал и подписывал запросы на сертификаты для всех остальных пользователей.

Сертификат можно создать следующими способами:

- С помощью утилиты Cm.CertEnroll.MsCA
- В оснастке **Сертификаты** (Certificates) пользователя (certmgr.msc)

Cm.CertEnroll.MsCA

1. Откройте консоль Powershell от имени администратора на сервере Indeed CM и перейдите в каталог *IndeedCM.WindowsServer\Misc\certenrollmsca*.

2. Запустите утилиту Cm.CertEnroll.MsCA.exe с параметрами `/e userName password` и `/t templateName`, где:

   - `userName` – имя сервисной учетной записи для работы с ЦС
   - `password` – пароль сервисной учетной записи
   - `templateName` – имя шаблона сертификата **Агент регистрации**. Убедитесь, что поле **Улучшенный ключ** (Extended Key Usage) сертификата содержит значение «Агент запроса сертификата» (Certificate Request Agent)

   Пример

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

   Результат работы утилиты

   ```
   CA: msca.domain.loc\Indeed-Demo-CA
   Certificate has been enrolled successfully.
   ```

3. Если запрос на сертификат должен одобрить оператор удостоверяющего центра (УЦ), то утилита предложит принять запрос и укажет порядковый номер запроса и имя ключевого контейнера.

   Пример

   ```
   CA: msca.domain.loc\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.
   ```

4. После одобрения запроса в УЦ установите сертификат в хранилище сертификатов компьютера: запустите утилиту Cm.CertEnroll.MsCA.exe с параметром `/i userName password requestId containerName`, где:

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

   Пример

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

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

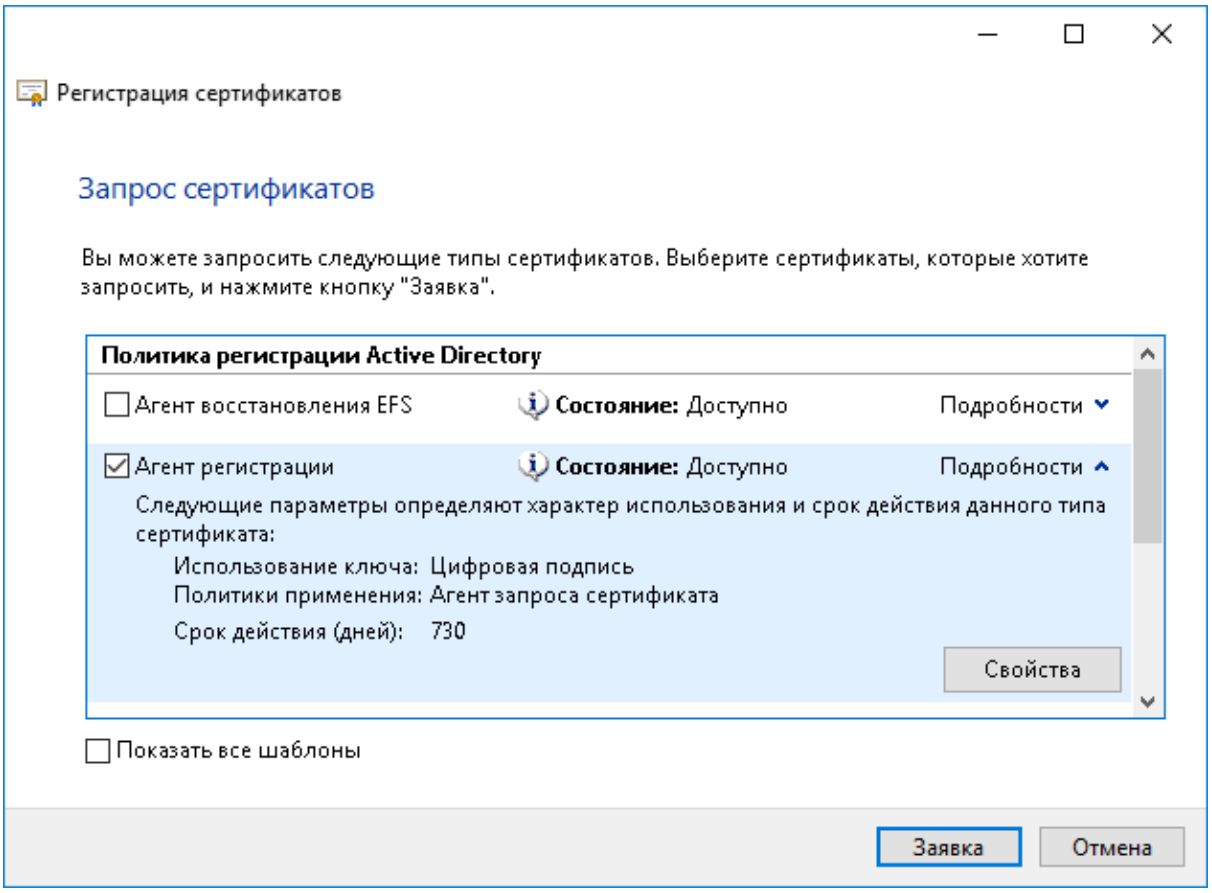
   - `CAMachineName` – DNS-имя сервера с ролью ЦС
   - `CAName` – имя ЦС

   Пример запуска утилиты с указанием ЦС

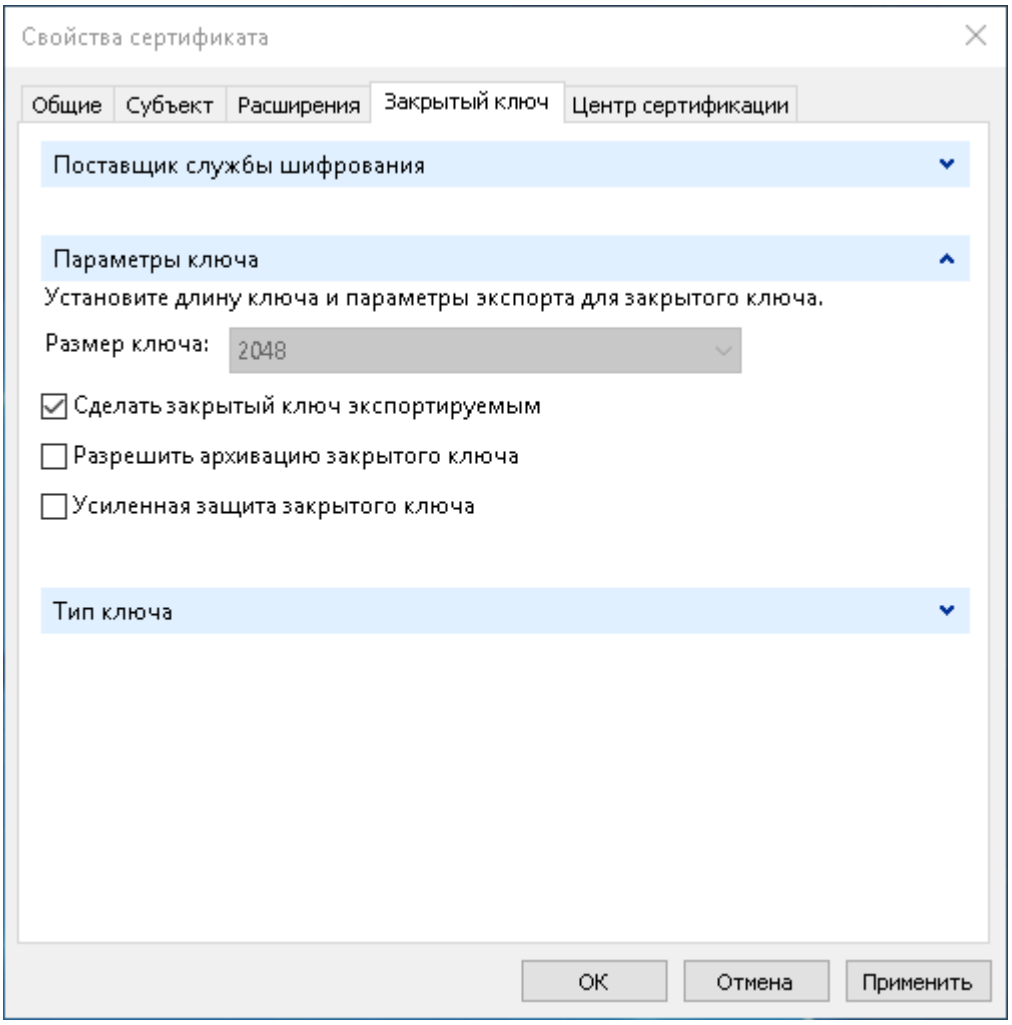
   ```
   Cm.CertEnroll.MsCA.exe /e serviceca p@ssw0rd /t=”IndeedEnrollmentAgent”
   /c=”msca.domain.loc\Indeed-Demo-CA”
   ```

Certmgr.msc

1. Войдите в систему от имени сервисной учетной записи и откройте оснастку **Сертификаты** (Certificates) пользователя: в меню **Пуск** выберите **Выполнить** (**Win+R**) и введите `certmgr.msc`.
2. Нажмите правой кнопкой мыши на хранилище **Личное** и выберите **Все задачи** → **Запросить новый сертификат**.
3. Два раза нажмите **Далее**.
4. Выберите тип сертификата **Агент регистрации** (Enrollment Agent), разверните окно **Подробности** (Details) и перейдите в **Свойства** (Properties).



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



6. Установите выпущенный сертификат и его закрытый ключ в хранилище сертификатов компьютера на сервере Indeed CM и выдайте сервисной учетной записи права на чтение закрытого ключа сертификата **Агент регистрации** (Enrollment Agent).
   Как установить сертификат и выдать права на чтение закрытого ключа

Подключение к Microsoft CA через Indeed CM MS CA Proxy

Indeed Certificate Manager может взаимодействовать с ЦС Microsoft, которые находятся за пределами домена сервера Indeed CM, с помощью компонента Indeed CM MS CA Proxy. При выпуске сертификата Indeed CM обращается к Indeed CM MS CA Proxy, который использует сертификат Агента Регистрации, чтобы передать запрос на целевой ЦС.

Примеры конфигурации:

- В инфраструктуре есть несколько независимых доменов с самостоятельными ЦС в каждом, и Indeed CM находится только в одном из этих доменов.
- Indeed CM находится на внедоменном сервере под управлением ОС Linux и используется для запроса и выпуска сертификатов в домене с Microsoft CA.

Приложение MS CA Proxy можно установить только на систему под управлением ОС Windows.
Системные требования

Установка и настройка Indeed CM MS CA Proxy

1. Создайте во внешнем для системы домене сервисную учетную запись для работы с Microsoft CA.

2. Создайте шаблон **Агент регистрации** и выпустите сертификат для сервисной учетной записи по этому шаблону. Убедитесь, что сертификат **Агент регистрации** установлен в хранилище **Локальный компьютер** (Local computer) рабочей станции, на которую устанавливается Indeed CM MS CA Proxy.

3. Установите Indeed CM MS CA Proxy на рабочую станцию в домене с внешним УЦ: откройте каталог *IndeedCM.Server* дистрибутива Indeed CM и запустите Мастер установки *IndeedCM.MSCA.Proxy-<номер версии>.x64.ru-ru.msi*.

4. В Мастере установки выберите способ аутентификации в зависимости от ОС, где установлен сервер Indeed CM, и укажите необходимые настройки в файлах конфигурации:

   Windows

   1. Выберите способ аутентификации Windows. По завершении установки нажмите **Готово** и закройте Мастер установки.
   2. Откройте файл *appsettings.json* (*C:\inetpub\wwwroot\cm\mscaproxy*) в редакторе Блокнот от имени администратора.
   3. В секции `caProxySettings` укажите:

   - `ca` – имя ЦС в формате `CAMachineName\CAName`, где `CAMachineName` – DNS-имя сервера с ролью ЦС, `CAName` – имя ЦС.
   - `userName` и `password` – логин и пароль учетной записи , обладающей сертификатом **Агент регистрации**.

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

Пример настроек

```
"caProxySettings": {
"ca": "servercm.external.com\\EXTERNAL-CA",
"userName": "EXTERNAL\\serviceca",
"password": "p@ssw0rd",
"enrollmentAgentCertificateThumbprint":
"dbd1859d27395860843643ebe17e2ee3fc463aba"
}
```

4. Сохраните изменения и закройте файл *appsettings.json*.

Linux

1. Выберите способ аутентификации по сертификату. По завершении установки нажмите **Готово** и закройте Мастер установки.
2. Откройте файл *appsettings.json* (*C:\inetpub\wwwroot\cm\mscaproxy*) в редакторе Блокнот от имени администратора.
3. В секции `caProxySettings` укажите:

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

Пример настроек

```
"caProxySettings": {
"ca": "servercm.external.com\\EXTERNAL-CA",
"userName": "EXTERNAL\\serviceca",
"password": "p@ssw0rd",
"enrollmentAgentCertificateThumbprint":
"dbd1859d27395860843643ebe17e2ee3fc463aba"
}
```

4. В секции `authSettings` в параметре `allowedCertificateThumbprints` укажите отпечаток клиентского сертификата, разрешенного к предъявлению сервером Indeed CM. Убедитесь, что поле **Улучшенный ключ** (Enhanced Key Usage) сертификата содержит значение «Проверка подлинности клиента» (Client Authentication), и сертификат установлен в хранилище сертификатов на сервере Indeed CM.
   Как установить сертификат

   Рекомендуется использовать один и тот же сертификат в качестве сертификата **Агент регистрации** и для клиентской аутентификации.

   ```
   "authSettings": {
   "authorizeByCertificate": "true",
   "allowedCertificateThumbprints": "dbd1859d27395860843643ebe17e2ee3fc463aba"
   }
   ```

5. Сохраните изменения и закройте файл *appsettings.json*.

5. 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).

Aladdin Enterprise CA

Чтобы настроить работу Indeed CM с Aladdin Enterprise CA (Aladdin eCA):

1. Создайте сервисную учетную запись.
2. Выпустите сертификат клиентской аутентификации и установите его в личное хранилище сертификатов на сервере Indeed CM.
3. Установите корневой сертификат Aladdin eCA в хранилище доверенных корневых сертификатов на сервере Indeed CM.
4. Создайте шаблоны сертификатов пользователей.
5. Настройте подключение к Aladdin eCA в Консоли управления Indeed CM.

Создание сервисной учетной записи

Создайте сервисную учетную запись, от имени которой Indeed CM будет создавать запросы на сертификаты пользователей в Aladdin eCA.

1. Откройте веб-интерфейс Центра сертификации Aladdin eCA и перейдите в раздел **Учетные записи**.
2. Нажмите **Создать** и выберите роль *Администратор*.
3. Заполните поля **Отображаемое имя** и **Логин**.
4. Нажмите **Создать**.

Выпуск сертификата клиентской аутентификации

Чтобы выпустить сертификат клиентской аутентификации для сервисной учетной записи, создайте шаблон и получите сертификат.

Создание шаблона сертификата

1. В веб-интерфейсе Aladdin eCA перейдите в раздел **Шаблоны**.
2. Создайте шаблон сертификата для Indeed CM на основе шаблона **ECA-User**: клонируйте шаблон и укажите имя нового шаблона. Откроется окно свойств шаблона.

3. При необходимости укажите **Период действия сертификата**.
4. Выберите Центр сертификации.
5. В выпадающем списке **Тип субъекта** выберите **Пользователь**.
6. В разделе **Шифрование** выключите опцию **ECDSA**. Indeed CM не поддерживает работу с сертификатами на основе алгоритма ECDSA.

> **АЛГОРИТМ ШИФРОВАНИЯ ДЛЯ ФОРМИРОВАНИЯ СЕРТИФИКАТА**
> Чтобы формировать сертификат с использованием ГОСТ-шифрования, включите только опцию **ГОСТ**. Если включены оба варианта – **ГОСТ** и **RSA**, то используется алгоритм RSA.

7. На вкладках **Расширения** и **Компоненты имени сертификата** оставьте параметры по умолчанию и нажмите **Сохранить**.

Получение сертификата

1. Перейдите в раздел **Учетные записи**.
2. В строке с созданной сервисной учетной записью нажмите **Создать сертификат** и выберите опцию **С закрытым ключом (PKCS#12)**.
3. Выберите шаблон и нажмите **Продолжить**.
4. При необходимости измените данные сервисной учетной записи и нажмите **Продолжить**.
5. Создайте пароль для защиты ключевого контейнера PKCS#12.
6. Выберите алгоритм и длину ключа или оставьте параметры по умолчанию.
7. Нажмите **Создать сертификат** и **Скачать**.

Файл сертификата скачивается в формате P12.

Установка сертификатов на сервер Indeed CM

Установите на сервер Indeed CM следующие сертификаты:

- Сертификат клиентской аутентификации в личное хранилище сертификатов компьютера

- Корневой сертификат Aladdin eCA в хранилище доверенных корневых сертификатов компьютера

Как установить сертификаты

> **УСТАНОВКА СЕРТИФИКАТА P12 В ОС LINUX**
>
> При установке сертификата в формате P12 на рабочую станцию под управлением ОС Linux, конвертируйте формат файла сертификата с P12 на PFX. Вместо `FILE` подставьте имя файла сертификата.
>
> ```
> sudo mv FILE.p12 FILE.pfx
> ```

Создание шаблонов сертификатов пользователей

1. В веб-интерфейсе Aladdin eCA перейдите в раздел **Шаблоны**.
2. Клонируйте нужный шаблон и укажите имя нового шаблона. Откроется окно свойств шаблона.
3. В окне свойств шаблона при необходимости укажите **Период действия сертификата**.
4. Выберите Центр сертификации.
5. В выпадающем списке **Тип субъекта** выберите **Пользователь**.
6. В разделе **Шифрование** выключите опцию **ECDSA**. Indeed CM не поддерживает работу с сертификатами на основе алгоритма ECDSA.
7. На вкладке **Расширения** укажите необходимые параметры.
8. На вкладке **Компоненты имени сертификата** выберите атрибуты для формирования отличительного и альтернативного имени субъекта сертификата.

> **ПРЕДУПРЕЖДЕНИЕ**
>
> Атрибут `Domain qualifier` не поддерживается как обязательный в имени субъекта сертификата, выпускаемого через Indeed CM.

9. Нажмите **Сохранить**.

SafeTech CA

Чтобы настроить работу Indeed CM с SafeTech CA:

1. Создайте сервисную учетную запись.
2. Настройте шаблоны сертификатов.
3. Установите корневой сертификат УЦ на сервер Indeed CM.
4. Настройте подключение к SafeTech CA в Консоли управления Indeed CM.

Создание сервисной учетной записи

Чтобы управлять пользователями, клиентами и группами, используйте сервис управления доступом Keycloak.

Создайте сервисную учетную запись, от имени которой Indeed CM будет отправлять запросы на сертификаты пользователей в SafeTech CA.

1. Откройте веб-консоль администратора Keycloak: `https://<имя сервера УЦ>:8443/`.
2. В основном меню перейдите в раздел **Manage realms** и выберите Realm (область) из списка. Realm по умолчанию для SafeTech CA – `st-ca`.
3. Используйте клиенты по умолчанию (CA Core и CA Gateway) или создайте новый клиент.

Как создать клиент в Keycloak

1. Перейдите в раздел **Clients** и нажмите **Create client**.
2. В разделе **General settings**:
    1. В выпадающем списке **Client type** выберите **OpenID Connect**.
    2. В поле **Client ID** введите идентификатор клиента.
3. Нажмите **Next**.
4. В разделе **Capability config**:
    1. Включите **Client Authentication**.
    2. В параметре **Authentication flow** включите опции **Standard flow**, **Implicit flow**, **Direct access grants**, **Service accounts roles**.
5. Нажмите **Next** и **Save**.
6. В меню управления клиентом назначьте созданному клиенту роль Оператора УЦ:
    1. Перейдите на вкладку **Service accounts roles** и нажмите **Assign role**.
    2. В фильтре выберите **Filter by realm roles**.
    3. Выберите роль **CaOperator** и нажмите **Assign**.
7. Настройте соответствие атрибута `instance_relation`, чтобы клиент имел доступ к нужному экземпляру SafeTech CA:
    1. Перейдите на вкладку **Client scopes** и нажмите **Add client scope**.
    2. Выберите scope `<имя_клиента>-dedicated`.
    3. Нажмите **Add mapper** → **By configuration** → **User Attibute**.
    4. Заполните поля:
        - **Name** – укажите произвольное имя соответствия атрибута
        - **User Attribute** – `instance_relation`
        - **Token Claim Name** – `instance_relation`
    5. Нажмите **Save**.

4. Создайте сервисную учетную запись и добавьте ее в группу доступа SafeTech CA.
    1. В разделе **Users** нажмите **Add user** и укажите **Username**.
    2. В поле **Groups** нажмите **Join Groups** и выберите группу **access-ST-CA-Root**.
    3. Нажмите **Create**. Появится меню управления пользователем.

5. Перейдите на вкладку **Credentials** и установите пароль для пользователя.

6. Назначьте пользователю роль Оператора УЦ:

    1. Перейдите на вкладку **Role mapping** и нажмите **Assign role**.
    2. В выпадающем списке выберите **Realm roles**.
    3. Выберите роль **CaOperator** и нажмите **Assign**.

Настройка шаблонов сертификатов

Выберите инструкцию в зависимости от используемой версии SafeTech CA.

3.1

1. Войдите в веб-интерфейс SafeTech CA от имени сервисной учетной записи, выберите нужный УЦ и нажмите **Работать с этим УЦ**.
2. Перейдите в раздел **Настройки** → **Шаблоны** и нажмите **Добавить шаблон**.
3. Укажите следующие параметры:
    - Наименование шаблона
    - Описание шаблона
    - Тип протокола – **ST_CA**
    - Максимальный срок действия сертификата в днях
    - Минимальная длина ключа
4. В разделе **Использование ключа**:
    1. Выберите как минимум одну политику использования ключа.
    2. Включите опцию **Использовать значения из шаблона**.
5. В разделе **Роли шаблона** для каждой роли задайте права на действия с шаблоном. Чтобы настроить права для роли Оператора:
    1. Нажмите **Добавить**.
    2. В выпадающем списке выберите **Оператор**.
    3. Выдайте права **Чтение** и **Выпуск**.
       Чтобы сертификаты выпускались автоматически, без ожидания одобрения запроса на сертификат в УЦ, дополнительно выдайте право **Автовыпуск**.
6. В разделе **Атрибуты сертификата** в выпадающем списке выберите **Enhanced Key Usage** и нажмите **Добавить**. Значение атрибута оставьте пустым.

7. В разделе **Расширения использования ключей (EKU)**:
    1. Нажмите **Добавить расширение**, выберите нужные расширения из списка и нажмите **Подтвердить**.
    2. Включите опцию **Использовать значения из шаблона**.
8. Нажмите **Создать**, затем нажмите **Сохранить на сервер**.

Опциональные настройки

Следующие настройки являются опциональными и не требуются для интеграции Indeed CM с SafeTech CA:

- Опция **Всегда проверять уникальность публичного ключа** в разделе **Использование ключа**
- Настройка обязательных имен субъекта сертификата

3.2 и выше

1. Войдите в веб-интерфейс SafeTech CA от имени сервисной учетной записи, выберите нужный УЦ и нажмите **Работать с этим УЦ**.
2. Перейдите в раздел **Настройки** → **Шаблоны** и нажмите **Добавить шаблон**.
3. Укажите следующие параметры:
    - Наименование шаблона
    - Описание шаблона
    - Тип протокола – **ST_CA**
    - Максимальный срок действия сертификата в днях
    - Минимальная длина ключа
4. В поле **Выпуск сертификата** в выпадающем списке **Сценарий выпуска** выберите **Стандартный**.
5. В поле **Настройка криптографии** включите опцию **Требуется настройка** и выберите алгоритм шифрования:
    - **RSA**

      В поле **Алгоритмы подписи** выберите **SHA256WITHRSA**. В поле **Длина ключа** выберите любое значение.

- **GOST**

  В поле **Алгоритмы подписи** выберите любое значение.

6. В разделе **Использование ключа**:
   1. Выберите как минимум одну политику использования ключа.
   2. Включите опцию **Использовать значения из шаблона**.
7. В разделе **Роли шаблона** задайте права на действия с шаблоном. Чтобы настроить права для роли Оператора:
   1. Нажмите **Добавить**.
   2. В выпадающем списке **Без роли** выберите **Оператор**.
   3. Выдайте права **Чтение** и **Выпуск**.

      Чтобы сертификаты выпускались автоматически, без ожидания одобрения запроса на сертификат в УЦ, дополнительно выдайте право **Автовыпуск**.
8. В разделе **Атрибуты сертификата** в выпадающем списке выберите **Enhanced Key Usage** и нажмите **Добавить**. Поле **Значение атрибута** оставьте пустым.
9. В разделе **Расширения использования ключей (EKU)**:
   1. Нажмите **Добавить расширение**.
   2. Выберите нужные расширения из списка и нажмите **Подтвердить**.
   3. Включите опцию **Использовать значения из шаблона**.
10. Нажмите **Создать**, затем нажмите **Сохранить на сервер**.

Опциональные настройки

Следующие настройки являются опциональными и не требуются для интеграции Indeed CM с SafeTech CA:

- Опция **Всегда проверять уникальность публичного ключа** в разделе **Использование ключа**
- Настройка обязательных альтернативных имен и обязательных имен субъекта сертификата
- Опции **Критичный** и **Включать SID в сертификат** в разделе **Атрибуты сертификата**

Dogtag CA

Чтобы настроить работу Indeed CM с Dogtag CA:

1. Создайте в Dogtag CA сервисную учетную запись для работы с Indeed CM.
2. Выпустите сертификат агента регистрации и установите его в личное хранилище сертификатов на сервере Indeed CM.
3. Установите корневой сертификат Dogtag CA в хранилище доверенных корневых сертификатов на сервере Indeed CM.
4. Создайте шаблоны сертификатов пользователей.
5. Настройте подключение к Dogtag CA в Консоли управления Indeed CM.

Создание сервисной учетной записи

Создайте сервисную учетную запись – агента, от имени которого Indeed CM будет отправлять запросы на сертификаты пользователей в Dogtag CA.

УЦ

1. Создайте пользователя от имени администратора Dogtag CA.

   ```
   pki -u <имя администратора> -w <пароль администратора> ca-user-add <имя пользователя>
   --fullName "<отображаемое имя пользователя>"
   ```

2. Добавьте пользователя в группу операторов **Certificate Manager Agents**, чтобы он мог управлять запросами на сертификаты.

   ```
   pki -u <имя администратора> -w <пароль администратора> ca-group-member-add
   "Certificate Manager Agents" <имя пользователя>
   ```

REST API

1. Выполните вход в Dogtag CA. Для аутентификации используйте сертификат администратора, который находится на сервере Dogtag CA по пути */root/ca-agent.p12*.

```
GET /ca/v2/account/login
```

2. Создайте пользователя.

```
POST /ca/v2/admin/users
```

```
{
    "id": "<имя пользователя>",
    "UserID": "<имя пользователя>",
    "FullName": "<отображаемое имя пользователя>"
}
```

3. Добавьте пользователя в группу операторов **Certificate Manager Agents**, чтобы он мог управлять запросами на сертификаты.

```
POST /ca/v2/admin/groups/Certificate Manager Agents/members
```

```
{
    "id": "<имя пользователя>",
    "groupID": "Certificate Manager Agents"
}
```

Выпуск сертификата агента регистрации

Выпустите сертификат агента регистрации для сервисной учетной записи.

УЦ

1. Подготовьте хранилище для закрытых ключей и сертификатов на сервере Dogtag CA.

```
pki client-init
```

2. Сгенерируйте ключевую пару и отправьте запрос на сертификат.

```
pki client-cert-request uid=<имя пользователя>
```

В результате создается запрос со статусом `pending`. Сохраните значение `requestID` из вывода команды.

3. Одобрите запрос на сертификат от имени администратора Dogtag CA.

```
pki -u <имя администратора> -w <пароль администратора> ca-cert-request-approve
<requestID>
```

Сохраните значение `certID` из вывода команды.

4. От имени администратора Dogtag CA назначьте полученный сертификат на сервисную учетную запись.

```
pki -u <имя администратора> -w <пароль администратора> ca-user-cert-add <имя
пользователя> --serial <certID>
```

5. Импортируйте сертификат в локальное хранилище.

```
pki client-cert-import <имя пользователя> --serial <certID>
```

6. Экспортируйте сертификат вместе с закрытым ключом в формат PKCS #12.

```
pki -u <имя администратора> -w <пароль администратора> pkcs12-export --pkcs12-file
<путь к файлу P12> --pkcs12-password <пароль от файла P12> "<имя пользователя>"
```

7. Скопируйте полученный файл с расширением P12 на сервер Indeed CM для последующей установки в хранилище сертификатов.

REST API

Требования к сертификату

- Поле **Субъект** (Subject) сертификата содержит атрибут `uid` с именем сервисной учетной записи для работы с Indeed CM.
- Поле **Улучшенный ключ** (Extended Key Usage) сертификата содержит значение «Проверка подлинности клиента» (Client Authentication, 1.3.6.1.5.5.7.3.2).

Выпуск сертификата

1. Создайте файл конфигурации *openssl.conf*.

```
nano openssl.conf
```

2. Укажите следующие параметры для генерации запроса на сертификат (CSR):

   - `CN` — имя пользователя
   - `email.1` — электронная почта пользователя
   - `otherName.1` — UPN-имя пользователя
   - `default_bits` — длина ключа шифрования (по умолчанию 2048)

   Пример файла конфигурации openssl.conf

```
[req]
default_bits = 2048
prompt = no
default_md = sha256
req_extensions = req_ext
distinguished_name = dn
[dn]
CN = <имя пользователя>
[req_ext]
subjectAltName = @alt_names
[alt_names]
email.1 = <email пользователя>
otherName.1 = 1.3.6.1.4.1.311.20.2.3;UTF8:<UPN-имя пользователя>
```

3. Сгенерируйте закрытый ключ и запрос на сертификат (CSR) с помощью утилиты openssl.

```
openssl req -new -nodes -out csr.pem -newkey rsa:2048 -keyout key.pem -config
openssl.conf
```

4. Выполните вход в Dogtag CA. Для аутентификации используйте сертификат администратора, который находится на сервере Dogtag CA по пути */root/ca-agent.p12*.

```
GET /ca/v2/account/login
```

5. Отправьте запрос на выпуск сертификата:

1. В поле `cert_request` передайте содержимое запроса на сертификат (CSR), полученное на шаге 2.
2. В поле `sn_uid` укажите имя сервисной учетной записи.

```
POST /ca/v2/certrequests
```

Пример запроса

```
{
    "ProfileID": "caUserCert",
    "Renewal": false,
    "Input": [
        {
            "id": "i1",
            "ClassID": "keyGenInputImpl",
            "Name": "Key Generation",
            "Attribute": [
                {
                    "name": "cert_request_type",
                    "Value": "pkcs10"
                },
                {
                    "name": "cert_request",
                    "Value": "<содержимое CSR>"
                }
            ]
        },
        {
            "id": "i2",
            "ClassID": "subjectNameInputImpl",
            "Name": "Subject Name",
            "Attribute": [
                { "name": "sn_uid", "Value": "<имя пользователя>" },
                { "name": "sn_cn", "Value": "" },
                { "name": "sn_o", "Value": "" },
                { "name": "sn_c", "Value": "" }
            ]
        },
        {
            "id": "i3",
            "ClassID": "submitterInfoInputImpl",
            "Name": "Requestor Information",
            "Attribute": [
                { "name": "requestor_name", "Value": "<имя заявителя>" },
                { "name": "requestor_email", "Value": "" }
            ]
        }
    ],
    "Output": [],
    "Attributes": {
        "Attribute": []
    }
}
```

Скопируйте значение поля `requestID` из ответа.

6. Получите данные запроса на сертификат. Подставьте значение поля `requestID`, полученное на шаге 4.

```
GET /ca/v2/agent/certrequests/<requestID>
```

Скопируйте ответ, чтобы одобрить запрос на следующем шаге.

7. Одобрите запрос на сертификат. Подставьте значение поля `requestID`, полученное на шаге 4, и передайте полный ответ, полученный на предыдущем шаге.

```
POST /ca/v2/agent/certrequests/<requestID>/approve
```

8. Получите идентификатор выпущенного сертификата.

```
GET /ca/v2/certrequests/<requestID>
```

Скопируйте значение поля `certID` из ответа.

9. Получите сертификат в формате Base64.

```
GET /ca/v2/agent/certs/<certID>
```

Скопируйте значение поля `Encoded` из ответа.

10. Назначьте сертификат на сервисную учетную запись для работы с Indeed CM. В поле `Encoded` передайте строку сертификата, полученную на предыдущем шаге.

```
POST /ca/v2/admin/users/<имя пользователя>/certs
```

```
{
    "Encoded": "-----BEGIN CERTIFICATE-----\n<содержимое сертификата в Base64>\r\n----
-END CERTIFICATE-----\n"
}
```

11. Сохраните сертификат, полученный на шаге 8, в файл *cert.pem*. Убедитесь, что сертификат содержит корректные данные.

```
openssl x509 -in cert.pem -noout -text
```

12. Объедините сертификат и закрытый ключ в файл PFX. Скопируйте файл на сервер Indeed CM для установки в хранилище сертификатов.

```
openssl pkcs12 -export -out cert.pfx -inkey key.pem -in cert.pem
```

Установка сертификатов на сервер Indeed CM

Установите на сервер Indeed CM следующие сертификаты:

- Сертификат агента регистрации, полученный на шаге Выпуск сертификата агента регистрации, в локальное хранилище компьютера
- Корневой сертификат Dogtag CA в хранилище доверенных корневых сертификатов компьютера

Чтобы получить корневой сертификат Dogtag CA:

1. На сервере Dogtag CA выполните команду:

   ```
   pki ca-cert-export -o <путь к файлу корневого сертификата>
   ```

2. Скопируйте полученный файл на сервер Indeed CM.

Как установить сертификаты

Создание шаблонов сертификатов пользователей

Подготовьте шаблоны сертификатов для назначений (политик применения), которые будут использоваться для выпуска сертификатов пользователей.

Indeed CM поддерживает работу с шаблонами (профилями) сертификатов Dogtag CA определенной структуры. Примеры подходящих шаблонов: `AdminCert`, `caUserCert`, `caOtherCert`, `caServerKeygen_UserCert`. Чтобы подготовить шаблоны сертификатов пользователей, отредактируйте шаблоны Dogtag CA.

Далее приведен пример создания шаблона **Вход со смарт-картой** (Smartcard Logon) на основе шаблона `caUserCert`.

УЦ

1. Отключите шаблон, который необходимо отредактировать.

```
pki -u <имя администратора> -w <пароль администратора> ca-profile-disable caUserCert
```

2. Экспортируйте параметры шаблона в файл для редактирования.

```
pki -u <имя администратора> -w <пароль администратора> ca-profile-show caUserCert --
raw --output <путь к файлу>
```

3. Внесите необходимые изменения в файл параметров шаблона, например, настройте расширения и атрибуты имени субъекта.

   Подробнее о настройке шаблонов в документации Dogtag CA

   > **ПРИМЕЧАНИЕ**
   >
   > Сертификат **Вход со смарт-картой** (Smartcard Logon) должен содержать атрибут UPN (User Principal Name) пользователя в расширении Subject Alternative Name (SAN). В шаблоне `caUserCert` атрибут UPN по умолчанию отсутствует — добавьте его в настройки SAN.

4. Загрузите отредактированный файл с параметрами шаблона в Dogtag CA.

```
pki -u <имя администратора> -w <пароль администратора> ca-profile-mod <путь к файлу>
```

5. Включите шаблон.

```
pki -u <имя администратора> -w <пароль администратора> ca-profile-enable caUserCert
```

При настройке шаблонов сертификатов в Консоли управления Indeed CM отображаются только видимые и включенные шаблоны. Убедитесь, что в параметрах шаблона в Dogtag CA параметры `visible` и `enable` имеют значение `true`.

REST API

1. Выполните вход в Dogtag CA. Для аутентификации используйте сертификат администратора, который находится на сервере Dogtag CA по пути */root/ca-agent.p12*.

```
GET /ca/v2/account/login
```

2. Отключите шаблон, который необходимо отредактировать.

```
POST /ca/v2/profiles/caUserCert/disable
```

3. Получите параметры шаблона в формате RAW.

```
GET /ca/v2/profiles/caUserCert/raw
```

4. Внесите необходимые изменения в параметры шаблона, например, настройте расширения и атрибуты имени субъекта.

   Подробнее о настройке шаблонов в документации Dogtag CA

   > **ПРИМЕЧАНИЕ**
   >
   > Сертификат **Вход со смарт-картой** (Smartcard Logon) должен содержать атрибут UPN (User Principal Name) пользователя в расширении Subject Alternative Name (SAN). В шаблоне `caUserCert` атрибут UPN по умолчанию отсутствует — добавьте его в настройки SAN.

5. Отправьте обновленные параметры.

```
POST /ca/v2/profiles/caUserCert/raw
```

6. Включите шаблон.

```
POST /ca/v2/profiles/caUserCert/enable
```

При настройке шаблонов сертификатов в Консоли управления Indeed CM отображаются только видимые и включенные шаблоны. Убедитесь, что в параметрах шаблона в Dogtag CA параметры `profileVisible` и `profileEnable` имеют значение `true`.

КриптоПро УЦ 2.0

Для настройки работы Indeed Certificate Manager с КриптоПро УЦ 2.0:

1. Создайте сервисную группу пользователей в Центре Регистрации.
2. Создайте сервисную учетную запись для работы с КриптоПро УЦ 2.0.
3. Выпустите сертификат агента подачи заявок и установите его в личное хранилище сертификатов на сервере Indeed CM.
4. Установите корневой сертификат КриптоПро УЦ 2.0 в хранилище доверенных корневых сертификатов на сервере Indeed CM.

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

Описанный далее вариант создания сервисной учетной записи является рекомендуемым, но не единственным. Вы можете создать учетную запись пользователя и выпустить сертификат в Центре Регистрации, затем экспортировать его, чтобы установить на сервер Indeed CM.

1. Запустите браузер от имени администратора на сервере Indeed CM.
2. Откройте веб-портал Центра Регистрации КриптоПро УЦ 2.0: `https://<имя сервера УЦ>/UI/`.
3. На начальной странице выберите **Регистрация**. Откроется форма регистрации пользователя.
4. Укажите **Имя** и **E-mail** сервисной учетной записи.
5. Сохраните выданный ЦР логин и временный пароль.
6. При необходимости укажите дополнительную информацию и завершите регистрацию.
7. В Консоли управления ЦР одобрите запрос на регистрацию нового пользователя.
8. Добавьте созданного пользователя в группу безопасности **Indeed CM Service Users**.

Выпуск сертификата агента подачи заявок для сервисной учетной записи

Чтобы выпустить сертификат агента подачи заявок, создайте шаблон и получите сертификат.

Создание шаблона сертификата

1. Запустите утилиту **Диспетчер УЦ**.
2. В разделе **Сервер ЦС** выберите **Шаблоны сертификатов**.
3. Создайте шаблон сертификата **Indeed CM Service User** на основе шаблона **Пользователь**. Откроется окно свойств шаблона.
4. При необходимости укажите **Срок действия** сертификата.
5. В разделе **Параметры создания ключа** выберите **Ключ принадлежит: Компьютеру** и убедитесь, что включена опция **Разрешить экспорт ключа**.
6. В разделе **Настройка расширений сертификата** выберите **Улучшенный ключ (2.5.29.37)** и нажмите **Изменить...**.
7. В окне **Настройки расширения** нажмите **Изменить...**.
8. Поставьте отметку напротив пункта **Агент запроса сертификата** и два раза нажмите **OK**.
9. Нажмите **Применить**.

Получение сертификата

1. На сервере Indeed CM войдите в личный кабинет пользователя КриптоПро УЦ по логину и временному паролю сервисной учетной записи.
2. Создайте запрос на сертификат.
    1. Откройте вкладку **Сертификаты**.
    2. В верхней панели меню выберите **Создать**. Откроется окно запроса на сертификат.
    3. Выберите шаблон сертификата **Indeed CM Service User**.
    4. Выберите криптопровайдер **Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider**. Также поддерживаются криптопровайдеры RSA.
    5. Нажмите **Создать**.
3. Дождитесь, когда Оператор Центра Регистрации одобрит запрос.
4. В личном кабинете пользователя КриптоПро перейдите в раздел **Запросы → Изготовление**. После выпуска сертификата статус запроса изменится на *Завершен*. Изготовленный сертификат отобразится на вкладке **Сертификаты → Действительные**.
5. Сохраните сертификат: выделите его и в правой части строки нажмите **Скачать**.

ДЛЯ ИНСТАЛЛЯЦИЙ С НЕСКОЛЬКИМИ СЕРВЕРАМИ INDEED CM

Если в инфраструктуре планируется несколько серверов Indeed CM, то сертификат сервисной учетной записи необходимо выпустить с экспортируемым закрытым ключом. Перенесите этот сертификат и его контейнер закрытого ключа на каждый сервер Indeed CM.

Установка сертификатов на сервер Indeed CM

Установите на сервер Indeed CM следующие сертификаты:

- Сертификат агента подачи заявок в личное хранилище сертификатов компьютера
- Сертификат корневого центра сертификации КриптоПро УЦ 2.0 в хранилище доверенных корневых сертификатов компьютера
- Список отозванных сертификатов (CRL) в хранилище промежуточных сертификатов компьютера

Как установить сертификаты

Настройка аутентификации в веб-сервисах Indeed CM по сертификатам

Чтобы настроить аутентификацию в веб-сервисах Indeed CM по сертификатам, получите сертификат аутентификации сервера КриптоПро УЦ 2.0 и установите его в личное хранилище сертификатов на сервере Indeed CM.

1. Зарегистрируйте нового пользователя КриптоПро УЦ. В качестве имени пользователя укажите FQDN сервера Indeed CM.
2. На рабочей станции, где установлен сервер Indeed CM, войдите в личный кабинет пользователя КриптоПро УЦ по идентификатору и временному паролю.
3. Создайте запрос на сертификат:
    1. Откройте вкладку **Сертификаты**.
    2. В верхней панели меню выберите **Создать**. Откроется окно запроса на сертификат.
    3. Выберите шаблон сертификата **Веб-сервер**.

    4. Выберите криптопровайдер **Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider**. Также поддерживаются криптопровайдеры RSA.
    5. В параметре **Ключ будет использоваться для** выберите **Подпись**.
    6. Нажмите **Создать**.
4. Дождитесь, когда Оператор Центра Регистрации одобрит запрос.
5. В личном кабинете пользователя КриптоПро перейдите в раздел **Запросы** → **Изготовление**. После выпуска сертификата статус запроса изменится на *Завершен*. Изготовленный сертификат отобразится на вкладке **Сертификаты** → **Действительные**.
6. Сохраните сертификат: выделите его и в правой части строки нажмите **Скачать**.
7. Установите сертификат в личное хранилище на сервере Indeed CM.

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 настройки

Для интеграции Indeed Certificate Manager с КриптоПро DSS настройте следующее:

- 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
- Интеграция КриптоПро УЦ 2.0 с КриптоПро DSS

Подробнее об интеграции КриптоПро УЦ 2.0 с КриптоПро DSS

Интеграция КриптоПро УЦ 2.0 и КриптоПро DSS необходима для управления пользователями и их сертификатами в удостоверяющем центре. КриптоПро DSS выступает в роли привилегированного пользователя в КриптоПро УЦ 2.0. Создание и обновление пользователей, запрос сертификатов и прочие действия в УЦ 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. Чтобы настроить работу Indeed CM с КриптоПро DSS 2.0:

1. Установите на сервер Indeed CM следующие сертификаты:

    - Сертификат Оператора DSS в личное хранилище сертификатов компьютера
    - Корневые сертификаты КриптоПро УЦ 2.0 и КриптоПро DSS 2.0 в хранилище доверенных корневых сертификатов компьютера

    Как установить сертификаты

2. Выдайте учетной записи Оператор DSS разрешения на папку с пользователями в КриптоПро УЦ 2.0.

    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** (Security) и добавьте созданную группу **DSS Operators**.
    3. Выдайте группе следующие разрешения.

Список разрешений

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 пользователя
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

Наименование разрешения	Тип объекта	Комментарий
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

3. Настройте подключение к КриптоПро DSS 2.0 в Консоли управления Indeed CM.

Валидата УЦ

Чтобы настроить работу Indeed CM с Валидата УЦ:

1. Настройте один из режимов работы с Валидата УЦ.
    - Офлайн – в УЦ обрабатываются запросы пользователей в формате PKCS#10, после чего сертификаты выдаются пользователям.
    - Онлайн – сервер Indeed CM заменяет АРМ Оператора ЦР Валидата.
2. Подготовьте шаблоны сертификатов пользователей.

Настройка режима работы

Офлайн

Чтобы настроить работу Indeed CM с Валидата УЦ в офлайн-режиме, предоставьте сервисной учетной записи права на чтение и запись файлов в каталоге для обмена файлами с Центром Регистрации Валидата УЦ. Убедитесь, что в каталоге содержится следующее:

- Корневой и промежуточные сертификаты Валидата УЦ
- Актуальный файл списка отозванных сертификатов (CRL)
- Подкаталог для входящих незащищенных запросов пользователей в формате PKCS#10
- Подкаталог сертификатов для выдачи конечным пользователям

> ⓘ **ПРИМЕЧАНИЕ**
> Запросы в формате PKCS#10 можно обработать только в ручном режиме на АРМ Администратора ЦР.

Онлайн

Чтобы настроить работу Indeed CM с Валидата УЦ в онлайн-режиме:

1. Предоставьте сервисной учетной записи права на чтение и запись файлов в каталоге для обмена файлами с Центром Сертификации Валидата УЦ.

2. Настройте 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 аутентификации по протоколу TLS, так и для подписания XML-шаблона на получение или отзыв сертификата ключа проверки электронной подписи пользователя. Убедитесь, что сертификат Оператора ЦР содержит значение **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).

Чтобы выпустить сертификат Оператора ЦР, используйте Валидата CSP или КриптоПро CSP.

Выпуск сертификата Оператора ЦР с помощью Валидата CSP

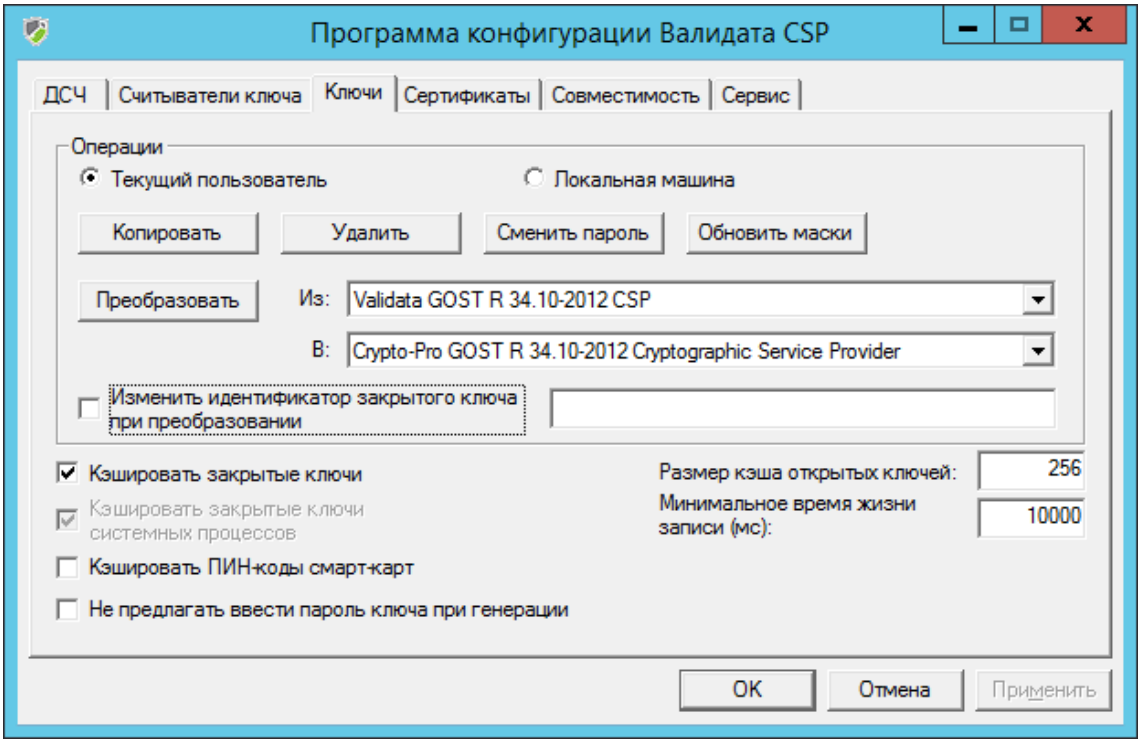
1. Чтобы создать шаблон сертификата, в основном меню АРМ Администратора ЦР выберите **Центр Регистрации** → **Сформировать запрос на сертификат абонента**.
2. Выберите шаблон и нажмите **Далее**.
3. Заполните атрибуты сертификата для построения **Имени Владельца сертификата**, при необходимости включите опцию **Разрешить генерацию ключа шифрования** и нажмите **Далее**.
4. Выберите области 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. При необходимости задайте атрибуты **Альтернативного имени Владельца сертификата** и нажмите **Готово**.

Преобразование закрытого ключа сертификата

Если вы выпустили сертификат с помощью Валидата CSP, преобразуйте его закрытый ключ из Validata GOST R 34.10-2012 CSP в Crypto-Pro GOST R 34.10-2012 CSP:

1. Запустите приложение Validata CSP от имени администратора.
2. Перейдите на вкладку **Ключи**. В поле **Преобразовать** выберите поля:

- **Из:** Validata GOST R 34.10-2012 CSP
- **В:** Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider.



3. Следуйте инструкциям мастера, чтобы преобразовать закрытый ключ сертификата Оператора ЦР в Crypto-Pro GOST R 34.10-2012 CSP.
4. Установите на сервер Indeed CM следующие сертификаты:
   - Преобразованный ключ и сертификат Оператора ЦР в локальное хранилище сертификатов компьютера
   - Сертификат корневого центра сертификации Валидата УЦ в хранилище доверенных корневых сертификатов компьютера
   - Сертификат промежуточного центра сертификации и список отозванных сертификатов (CRL) Валидата УЦ в хранилище промежуточных сертификатов компьютера

Как установить сертификаты

Подготовка шаблонов сертификатов пользователей

В Центре Регистрации Валидата УЦ подготовьте XML-шаблоны сертификатов, которые будут использоваться для выпуска сертификатов конечным пользователям.

Чтобы настроить шаблон сертификата пользователя в Центре Регистрации Валидата УЦ:

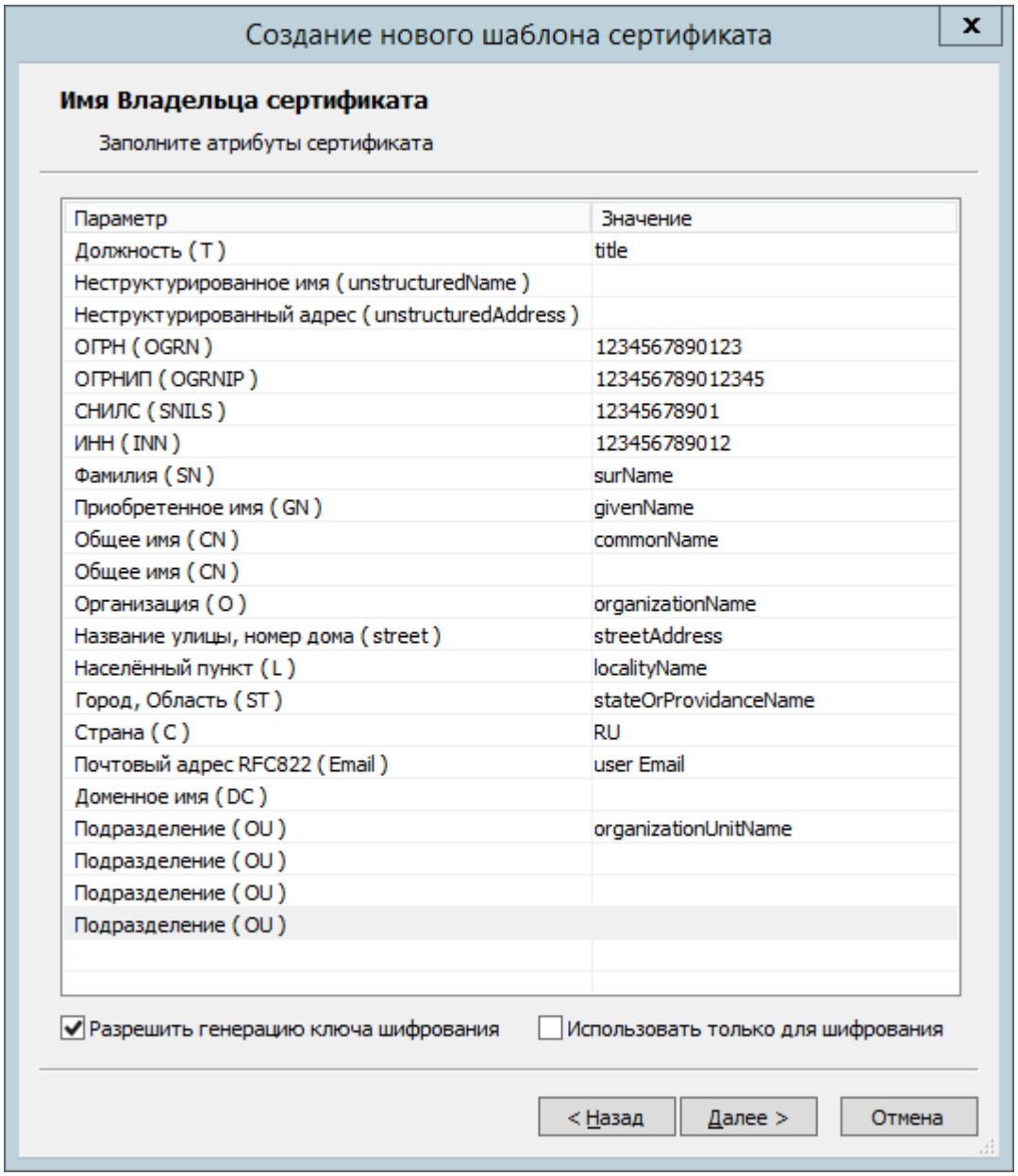
1. В основном меню АРМ Оператора или Администратора ЦР выберите **Центр Регистрации → Создать новый шаблон сертификата**.

2. Укажите **Наименование шаблона** и нажмите **Далее**.

3. Заполните атрибуты сертификата для построения **Имени Владельца сертификата**. При необходимости включите опцию **Разрешить генерацию ключа шифрования**, чтобы создать ключ шифрования для сертификата. Если опция не включена, то пользователю, для которого создается сертификат, 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. Установите время действия ключа ЭП и нажмите **Далее**.

5. Выберите область применения ключа и нажмите **Далее**.

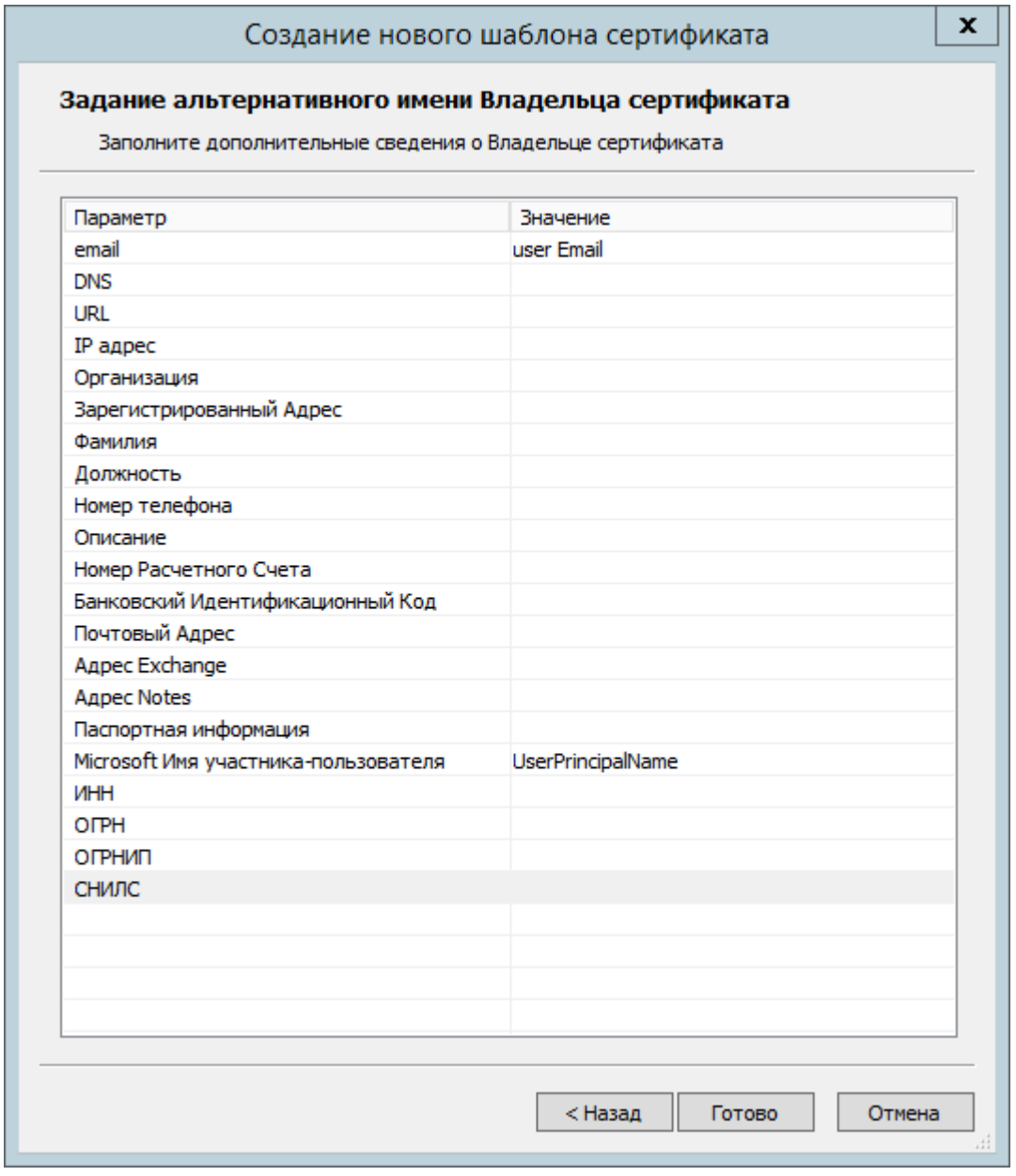
6. Выберите регламент для сертификата и нажмите **Далее**.

7. Выберите дополнения для сертификата и нажмите **Далее**.

8. Укажите альтернативное имя владельца сертификата и нажмите **Готово**.

Поддерживаемые атрибуты для построения альтернативного имени владельца сертификата

- Email
- Описание
- Имя участника-пользователя (User Principal Name)



9. Чтобы использовать созданный шаблон в Indeed CM, очистите значения заполненных атрибутов в текстовом редакторе и при сохранении шаблона перекодируйте его в UTF-8.

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>
```

Сервисные сертификаты

Для защищенного соединения с сервисами Indeed CM установите на сервер следующие SSL/TLS-сертификаты:

- Сертификат серверной аутентификации для веб-сервера и сервера OpenID Connect
- Сертификат клиентской аутентификации сервера Indeed CM для дополнительных сервисов Indeed CM MS CA Proxy, Indeed CM Event Log Proxy и Indeed AirCard Enterprise (сервер Indeed CM выступает клиентом для сервисов)

> **ПРИМЕЧАНИЕ**
>
> В разделе описывается настройка шаблонов и выпуск сертификатов в Microsoft CA. Инструкции для других поддерживаемых УЦ

Требования к сертификатам

Серверный сертификат

- **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.domain.loc*, или соответствующую запись с подстановочными знаками, например **.domain.loc* (Wildcard certificate).
- **Улучшенный ключ** (Enhanced Key Usage) сертификата содержит значение «Проверка подлинности сервера» (Server Authentication).

Клиентский сертификат

- **Субъект** (Subject) сертификата содержит FQDN сервера Indeed CM.
- **Улучшенный ключ** (Enhanced Key Usage) сертификата содержит значение «Проверка подлинности клиента» (Client Authentication).

Создание шаблона

Чтобы подготовить шаблон сертификата:

1. В оснастке управления УЦ certsrv нажмите правой кнопкой мыши на **Шаблоны сертификатов** (Certificate Templates) и выберите **Управление** (Manage).
2. Скопируйте предустановленный шаблон: нажмите правой кнопкой на название шаблона и выберите **Скопировать шаблон** (Duplicate Template). Откроется окно свойств нового шаблона.
    - Для серверного сертификата: **Веб-сервер** (Web Server)
    - Для клиентского сертификата: **Проверка подлинности рабочей станции** (Workstation Authentication)
3. На вкладке **Общие** (General) укажите имя шаблона сертификата. При необходимости укажите период действия сертификата и период обновления.
4. На вкладке **Обработка запроса** (Request Handling) включите опцию **Разрешить экспортировать закрытый ключ** (Allow private key to be exported).
5. На вкладке **Шифрование** (Cryptography) измените минимальный размер ключа при необходимости.
6. На вкладке **Безопасность** (Security) укажите имя сервера для запроса сертификата:
    1. Нажмите **Добавить** (Add) → **Типы объектов** (Object Types), включите опцию **Компьютеры** (Computers) и нажмите **ОК**.
    2. Введите имя сервера, где вы планируете установить Indeed CM, и нажмите **ОК**.
7. В списке разрешений напротив опции **Заявка** (Enroll) включите **Разрешить** (Allow), чтобы разрешить запрос сертификата.
8. Нажмите **Применить** (Apply) и **ОК**.
9. Опубликуйте созданный шаблон сертификата:
    1. Перейдите в оснастку управления УЦ certsrv.
    2. Нажмите правой кнопкой мыши на **Шаблоны сертификатов** (Certificate Templates) и выберите **Создать** (New) → **Выдаваемый шаблон сертификата** (Certificate Template to Issue).
    3. В окне **Включение шаблонов сертификатов** (Enable Certificate Templates) выберите созданный шаблон. Шаблон опубликуется в УЦ.
10. Закройте certsrv.

Выпуск

Выпустите сертификаты:

- Серверный — на имя рабочей станции с веб-сервером

- Клиентский — на имя рабочей станции с сервером Indeed CM

Сертификаты можно выпустить в УЦ или с помощью самоподписанного сертификата.

УЦ

1. Откройте оснастку certs и перейдите в раздел хранилища локального компьютера **Сертификаты (локальный компьютер)** (Certificates (Local Computer)).
2. Правой кнопкой мыши нажмите **Личное** (Personal).
3. Выберите **Все задачи** (All Tasks) → **Запросить новый сертификат** (Request New Certificate).
4. В окне **Регистрация сертификатов** (Certificate Enrollment) два раза нажмите **Далее** (Next) и активируйте чекбокс с названием шаблона сертификата.
5. Нажмите на ссылку **Требуется больше данных для подачи заявки на этот сертификат. Щелкните здесь для настройки параметров** (More information is required to enroll for this certificate. Click here to configure settings), чтобы указать дополнительную информацию для запроса сертификата. Откроется окно свойств сертификата.
6. На вкладке **Субъект** (Subject):
    1. В поле **Имя субъекта** (Subject name) в выпадающем списке **Тип** (Type) выберите **Общее имя** (Common name).
    2. Введите FQDN сервера Indeed CM и нажмите **Добавить** (Add).
    3. В поле **Дополнительное имя** (Alternative name) в выпадающем списке **Тип** (Type) выберите **DNS**.
    4. Введите FQDN сервера Indeed CM и нажмите **Добавить** (Add).
    5. При необходимости создайте маску имени домена для Wildcard-сертификатов, которые предъявляют серверы с различными именами. В поле **Дополнительное имя** (Alternative name) в выпадающем списке **Тип** (Type) выберите **DNS** и введите имя домена, например, `*.domain.loc`. Нажмите **Добавить** (Add).
7. Нажмите **OK**.
8. Перейдите на вкладку **Закрытый ключ** (Private Key) → **Параметры ключа** (Key Options) и убедитесь, что опция **Сделать закрытый ключ экспортируемым** (Make private key exportable) включена. Нажмите **OK**.

9. Нажмите **Заявка** (Enroll).

Самоподписанный сертификат

Самоподписанный корневой сертификат создается с помощью утилиты openssl.

1. Создайте закрытый ключ, а затем корневой сертификат с помощью сгенерированного ключа.

```
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.

```
nano SSL.conf
```

3. В параметрах `commonName` и `DNS.1` укажите DNS-имя рабочей станции, где вы планируете установить веб-сервер (для выпуска серверного сертификата) или сервер Indeed CM (для выпуска клиентского сертификата).

Пример содержимого файла *SSL.conf*

```
[ 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 = <FQDN сервера Indeed CM>
[ req_ext ]
subjectAltName = @alt_names
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
basicConstraints = CA:FALSE
extendedKeyUsage = serverAuth
[alt_names]
DNS.1 = <FQDN сервера Indeed CM>
```

4. Создайте запрос на сертификат и выпустите сертификат 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
```

Убедитесь, что сертификат выпущен и установлен в хранилище локального компьютера (**Сертификаты** (Certificates) → **Личное** (Personal) → **Сертификаты** (Certificates)).

Подробнее об установке сертификатов в хранилище компьютера

Установка сертификатов в хранилище компьютера

В разделе описывается, как установить сертификаты для сервисов и интеграций Indeed CM на рабочие станции под управлением ОС Windows или Linux.

Установите следующие сертификаты:

- На сервер Indeed CM:
  - Корневые сертификаты удостоверяющих центров (УЦ)
  - Список отозванных сертификатов (CRL)
  - SSL/TLS-сертификат для веб-сервера
  - Корневой сертификат УЦ для сертификатов агента
- На рабочие станции пользователей – корневые сертификаты УЦ и список отозванных сертификатов (CRL)

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Список отозванных сертификатов (CRL) содержит информацию о сертификатах, которые были отозваны в УЦ. Для проверки статуса корневых и промежуточных сертификатов убедитесь, что на рабочие станции пользователей и на сервер Indeed CM установлены актуальные списки отозванных сертификатов (CRL) от интегрированных УЦ.

Windows

Сертификаты можно установить следующими способами:

- Из файла
- В Диспетчере сертификатов (оснастка **Сертификаты**)
- С помощью КриптоПро CSP (для ГОСТ-сертификатов)

Файл

1. Откройте файл сертификата и нажмите **Установить сертификат...**.
2. В мастере импорта сертификатов выберите расположение хранилища **Текущий пользователь** или **Локальный компьютер** и нажмите **Далее**.

3. Выберите **Поместить все сертификаты в следующее хранилище**, нажмите **Обзор** и выберите:
    - **Личное** — для сертификатов пользователя или компьютера
    - **Доверенные корневые центры сертификации** — для корневых сертификатов УЦ
    - **Промежуточные центры сертификации** — для промежуточных сертификатов УЦ и списка отозванных сертификатов (CRL)
4. Нажмите **Далее** и **Готово**.

Выдача разрешений на чтение закрытого ключа сертификата

После установки сертификата выдайте системе разрешения на чтение закрытого ключа.

1. Откройте оснастку **Сертификаты** (Certificates).
2. Правой кнопкой мыши нажмите на сертификат и выберите **Все задачи** (All tasks) → **Управление закрытыми ключами...** (Manage Private Keys...).
3. Нажмите **Добавить** (Add).
4. В меню **Размещение** (Location) укажите сервер.
5. В поле **Введите имена выбранных объектов** (Enter the object names to select) укажите локальную группу **IIS_IUSRS** и нажмите **Проверить имена** (Check Names) и **ОК**.
6. Выставите разрешения **Полный доступ** (Full Control) и **Чтение** (Read).
7. Нажмите **Применить** (Apply).

Диспетчер сертификатов

1. Откройте оснастку **Сертификаты** (Certificates): в меню **Пуск** выберите **Выполнить** (**Win+R**) и введите:
    - `certmgr.msc`, чтобы открыть хранилище сертификатов текущего пользователя
    - `certlm.msc`, чтобы открыть хранилище сертификатов локального компьютера
2. Перейдите в нужное хранилище:
    - **Личное** — для сертификатов пользователя или компьютера
    - **Доверенные корневые центры сертификации** — для корневых сертификатов УЦ

- **Промежуточные центры сертификации** — для промежуточных сертификатов УЦ и списка отозванных сертификатов (CRL)

3. В верхнем меню оснастки **Сертификаты** выберите **Действие** → **Все задачи** → **Импорт**.
4. Следуйте инструкциям мастера импорта сертификатов.

Выдача разрешений на чтение закрытого ключа сертификата

После установки сертификата выдайте системе разрешения на чтение закрытого ключа.

1. Откройте оснастку **Сертификаты** (Certificates).
2. Правой кнопкой мыши нажмите на сертификат и выберите **Все задачи** (All tasks) → **Управление закрытыми ключами...** (Manage Private Keys...).
3. Нажмите **Добавить** (Add).
4. В меню **Размещение** (Location) укажите сервер.
5. В поле **Введите имена выбранных объектов** (Enter the object names to select) укажите локальную группу **IIS_IUSRS** и нажмите **Проверить имена** (Check Names) и **ОК**.
6. Выставите разрешения **Полный доступ** (Full Control) и **Чтение** (Read).
7. Нажмите **Применить** (Apply).

КриптоПро CSP

Для работы с ГОСТ-сертификатами установите приложение КриптоПро CSP версии 5.0 или выше.

Чтобы установить ГОСТ-сертификат:

1. Откройте КриптоПро CSP и перейдите на вкладку **Сервис**.
2. В разделе **Личный сертификат** нажмите **Установить личный сертификат...**. Откроется Мастер установки личного сертификата.
3. Укажите путь к файлу сертификата. Возможные форматы файла:
   - PFX, P12 — файл с закрытым ключом
   - CER, CRT — файл сертификата (требуется контейнер закрытого ключа)
4. Нажмите **Далее**.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Не устанавливайте пароль на контейнер закрытого ключа сертификата. Нажмите **Далее** без ввода пароля.

5. В окне контейнера закрытого ключа выберите:
   - **Найти контейнер автоматически** — КриптоПро CSP найдет контейнер по имени сертификата.
   - **Выбрать контейнер вручную** — выберите имя контейнера из списка.
6. В блоке **Введенное имя задает ключевой контейнер** выберите **Компьютера** и нажмите **Далее**.
7. Нажмите **Далее** и **Готово**.

Linux

Сертификат можно установить следующими способами:

- С помощью утилиты OpenSSL в командной строке
- С помощью утилиты certmgr.exe в командной строке
- В приложении Инструменты КриптоПро (cptools) (для ГОСТ-сертификатов)

Если сертификат выпущен на рабочей станции под управлением ОС Windows, экспортируйте сертификат и его закрытый ключ.

Как экспортировать сертификат

1. В оснастке **Сертификаты** правой кнопкой мыши нажмите на сертификат и выберите **Все задачи** (All Tasks) → **Экспорт** (Export). Откроется мастер экспорта сертификатов.
2. Нажмите **Далее** (Next), выберите **Да, экспортировать закрытый ключ** (Yes, export the private key) и два раза нажмите **Далее** (Next).
3. Установите пароль – включите опцию **Пароль** (Password), введите и подтвердите пароль. Нажмите **Далее** (Next).
4. Выберите папку для экспорта сертификата.
5. Нажмите **Готово** (Finish). В папке сохранится сертификат в формате PFX.
6. Перенесите сертификат на рабочую станцию под управлением ОС Linux и следуйте инструкциям, описанным далее.

OpenSSL

1. Войдите в систему с учетной записью, от имени которой будет запускаться Indeed CM. По умолчанию это пользователь www-data.

```
sudo su -s /bin/sh www-data
```

Как убедиться, что пользователь www-data существует

1. Проверьте наличие пользователя www-data.

```
cat /etc/passwd | grep www-data

#Пример вывода, если пользователь www-data существует
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
```

2. Если пользователя www-data не существует, создайте его.

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

2. Разделите файл PFX на файл сертификата и файл закрытого ключа. Вместо PFXFILE подставьте имя файла PFX.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> При выполнении команд утилита openssl предлагает установить пароль для файла закрытого ключа (.key). Оставьте файл без пароля: два раза нажмите Enter.

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

Файл сертификата *SSL.crt* должен содержать следующее:

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

3. Создайте поддиректорию домашнего каталога пользователя www-data.

```
sudo mkdir -p /var/www/.dotnet/corefx/cryptography/x509stores/my/
```

4. Объедините файл сертификата и файл ключа обратно в файл PFX. Поместите файл PFX в поддиректорию домашнего каталога пользователя.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> При выполнении команды утилита openssl предлагает установить пароль для файла PFX. Оставьте файл без пароля: два раза нажмите Enter.

```
sudo openssl pkcs12 -export -out
/var/www/.dotnet/corefx/cryptography/x509stores/my/PFXFILE.pfx -inkey SSL.key -in
SSL.crt
```

5. Настройте право доступа 600 к файлу PFX.

```
sudo chmod 600 /var/www/.dotnet/corefx/cryptography/x509stores/my/PFXFILE.pfx
```

6. Если вы устанавливаете корневой сертификат УЦ, добавьте его в список доверенных корневых сертификатов.

Debian-based

1. Поместите корневой сертификат в хранилище доверенных корневых сертификатов.

   ```
   sudo cp <путь к файлу CER или CRT> /usr/share/ca-certificates/
   ```

2. Перенастройте список доверенных корневых сертификатов.

   ```
   sudo dpkg-reconfigure ca-certificates
   ```

3. Перезапустите систему.

   ```
   sudo reboot
   ```

RHEL-based

1. Поместите корневой сертификат в хранилище доверенных корневых сертификатов.

   ```
   sudo cp <путь к файлу CER или CRT> /etc/pki/ca-trust/source/anchors/
   ```

2. Обновите хранилище доверенных корневых сертификатов.

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

3. Перезапустите систему.

   ```
   sudo reboot
   ```

Certmgr.exe

1. Войдите в систему с учетной записью, от имени которой будет запускаться Indeed CM. По умолчанию это пользователь www-data.

```
sudo su -s /bin/sh www-data
```

Как убедиться, что пользователь www-data существует

1. Проверьте наличие пользователя www-data.

```
cat /etc/passwd | grep www-data

#Пример вывода, если пользователь www-data существует
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
```

2. Если пользователя www-data не существует, создайте его.

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

2. Установите сертификат в формате PFX с помощью утилиты certmgr.exe.

Личный сертификат

```
# PFX
/opt/cprocsp/bin/amd64/certmgr -inst -pfx -file <путь к файлу PFX> -pin <пароль от файла PFX>
# CER
/opt/cprocsp/bin/amd64/certmgr -inst -file <путь к файлу CER> -cont <имя сертификата> -silent
```

Корневой сертификат

```
/opt/cprocsp/bin/amd64/certmgr -inst -store uRoot -file <путь к файлу CER или CRT>
```

Список отозванных сертификатов (CRL)

```
/opt/cprocsp/bin/amd64/certmgr -inst -crl -file <путь к файлу CRL>
```

3. Если вы устанавливаете корневой сертификат УЦ, добавьте его в список доверенных корневых сертификатов.

Debian-based

1. Поместите корневой сертификат в хранилище доверенных корневых сертификатов.

```
sudo cp <путь к файлу CER или CRT> /usr/share/ca-certificates/
```

2. Перенастройте список доверенных корневых сертификатов.

```
sudo dpkg-reconfigure ca-certificates
```

3. Перезапустите систему.

```
sudo reboot
```

RHEL-based

1. Поместите корневой сертификат в хранилище доверенных корневых сертификатов.

```
sudo cp <путь к файлу CER или CRT> /etc/pki/ca-trust/source/anchors/
```

2. Обновите хранилище доверенных корневых сертификатов.

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

3. Перезапустите систему.

```
sudo reboot
```

Инструменты КриптоПро

В приложении Инструменты КриптоПро можно установить только ГОСТ-сертификаты.

1. Войдите в систему с учетной записью, от имени которой будет запускаться Indeed CM. По умолчанию это пользователь www-data.

```
sudo su -s /bin/sh www-data
```

Как убедиться, что пользователь www-data существует

1. Проверьте наличие пользователя www-data.

```
cat /etc/passwd | grep www-data

#Пример вывода, если пользователь www-data существует
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
```

2. Если пользователя www-data не существует, создайте его.

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

2. Запустите cptools.

```
/opt/cprocsp/bin/amd64/cptools
```

3. Перейдите на вкладку **Сертификаты**.

4. В выпадающем списке хранилищ сертификатов выберите:

   - **Личное** — для сертификатов пользователя или компьютера
   - **Доверенные корневые центры сертификации** — для корневых сертификатов УЦ
   - **Промежуточные центры сертификации** — для промежуточных сертификатов УЦ и списка отозванных сертификатов (CRL)

5. Нажмите **Установить сертификаты**, выберите файл сертификата и нажмите **Открыть**.

Если сертификат установлен, в нижней части окна появится сообщение *Установка завершена*.

Веб-сервер

Для работы серверных компонентов Indeed CM на ОС Windows установите веб-сервер Internet Information Services (IIS), для ОС Linux – веб-сервер Apache или Nginx.

Прежде чем приступить к установке веб-сервера, создайте и выпустите SSL/TLS-сертификат для настройки защищенного соединения с веб-сайтом, где будет расположен Indeed CM.

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 на ОС Windows установите и настройте веб-сервер Internet Information Services (IIS).

Установка веб-сервера

Установите веб-сервер 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)
- Авторизация URL-адреса (URL Authorization)
- Windows-проверка подлинности (Windows Authentication)
- Консоль управления службами IIS (IIS Management Console)

> **ПОДСКАЗКА**
>
> Для быстрой установки IIS с требуемыми модулями используйте скрипт PowerShell из каталога *\IIS.Setup.Scripts* дистрибутива Indeed CM.
> После установки и настройки компонентов IIS установите Microsoft .NET.

Установка TLS-сертификата

Привяжите TLS-сертификат к сайту Indeed CM. Как создать TLS-сертификат для веб-сервера

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**.

NGINX

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

1. Установите nginx.
2. Установите SSL/TLS-сертификат.
3. Настройте конфигурационный файл *nginx.conf*.

Выберите инструкцию в зависимости от ОС рабочей станции, где вы устанавливаете nginx.

Debian-based

Установка nginx

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. Подключите apt-репозиторий.

   ```
   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. Установите nginx.

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

Документация по установке на другие ОС доступна на сайте NGINX.

Установка SSL/TLS-сертификата

Как создать SSL/TLS-сертификат

Чтобы установить SSL/TLS-сертификат на веб-сервер:

1. 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/
   ```

2. 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
   ```

3. Сделайте сертификат доверенным в домене, например, с помощью групповых политик.
4. Выдайте учетной записи www-data права на чтение файлов сертификата.

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 *nginx.conf* находится 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`
	`proxy_buffers`	`8 4k|8 8k`	`4 16k`
	`types_hash_max_size`	`1024`	`4096`
	`client_max_body_size`	`1m`	`10m`
	`large_client_header_buffers`	`4 8k`	`4 16k`

Контекст	Директива	Значение по умолчанию	Рекомендуемое значение
server	listen	80	443 ssl
			3003 ssl
	ssl_certificate	–	/etc/ssl/private/SSL.crt
	ssl_certificate_key	–	/etc/ssl/private/SSL.key
	ssl_verify_client	off	optional_no_ca

Контекст	Директива	Значение по умолчанию	Рекомендуемое значение
`location`	`proxy_pass`	–	*
	`include`	–	`/etc/nginx/conf.d/proxy.conf`
	`proxy_http_version`	`1.0`	`1.1`
	`proxy_cache_bypass`	–	`$http_upgrade`

Контекст	Директива	Значение по умолчанию	Рекомендуемое значение
	`proxy_set_header`	`—`	`Upgrade $http_upgrade`
			`Connection keep-alive`
			`Host $host`
			`X-Real-IP $remote_addr`
			`X-Forwarded-For $proxy_add_x_forwarded_for`
			`X-Forwarded-Proto $scheme`
	`fastcgi_buffers`	`8 4k|8k`	`16 16k`
	`fastcgi_buffer_size`	`4k|8k`	`32k`

Контекст	Директива	Значение по умолчанию	Рекомендуемое значение
	`proxy_set_header`	–	`x-ssl-client-cert $ssl_client_escaped_cert`

Из-за многократного описания контекстов `location` определенный набор директив повторяется. Для удобства конфигурации вынесите этот набор директив в отдельный файл и включите директивы из этого файла в описание контекста (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. Убедитесь, что имена контекстов `location` совпадают 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;

 large_client_header_buffers 4 16k;

 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. Чтобы применить изменения в конфигурационном файле, перезагрузите конфигурацию или перезапустите nginx.

```
sudo nginx -s reload
```

RHEL-based

Установка nginx

Для установки nginx убедитесь, что на рабочей станции подключен и настроен репозиторий пакетов nginx. При необходимости добавьте репозиторий вручную.

Чтобы добавить репозиторий пакетов nginx вручную:

1. Установите пакеты для подключения yum-репозитория.

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

2. Создайте файл */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/$releasever/$basearch/
gpgcheck=1
enabled=0
gpgkey=https://nginx.org/keys/nginx_signing.key
module_hotfixes=true
```

3. Установите nginx.

```
sudo yum install nginx
```

Если система запросит подтвердить GPG-ключ, проверьте, что отпечаток ключа совпадает с *573B FD6B 3D8F BC64 1079 A6AB ABF5 BD82 7BD9 BF62*, и подтвердите GPG-ключ.

Документация по установке на другие ОС доступна на портале NGINX.

Установка SSL/TLS-сертификата

Как создать SSL/TLS-сертификат

Чтобы установить SSL/TLS-сертификат на веб-сервер:

1. 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/
```

2. 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
```

3. Сделайте сертификат доверенным в домене, например, с помощью групповых политик.
4. Выдайте учетной записи nginx права на чтение файлов сертификата.

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 *nginx.conf* находится 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`
	`proxy_buffers`	`8 4k|8 8k`	`4 16k`
	`types_hash_max_size`	`1024`	`4096`
	`client_max_body_size`	`1m`	`10m`
	`large_client_header_buffers`	`4 8k`	`4 16k`

Контекст	Директива	Значение по умолчанию	Рекомендуемое значение
server	listen	80	443 ssl
			3003 ssl
	ssl_certificate	–	/etc/ssl/private/SSL.crt
	ssl_certificate_key	–	/etc/ssl/private/SSL.key
	ssl_verify_client	off	optional_no_ca

Контекст	Директива	Значение по умолчанию	Рекомендуемое значение
`location`	`proxy_pass`	–	*
	`include`	–	`/etc/nginx/conf.d/proxy.conf`
	`proxy_http_version`	`1.0`	`1.1`
	`proxy_cache_bypass`	–	`$http_upgrade`

Контекст	Директива	Значение по умолчанию	Рекомендуемое значение
	`proxy_set_header`	`—`	`Upgrade $http_upgrade`
			`Connection keep-alive`
			`Host $host`
			`X-Real-IP $remote_addr`
			`X-Forwarded-For $proxy_add_x_forwarded_for`
			`X-Forwarded-Proto $scheme`
	`fastcgi_buffers`	`8 4k|8k`	`16 16k`
	`fastcgi_buffer_size`	`4k|8k`	`32k`

Контекст	Директива	Значение по умолчанию	Рекомендуемое значение
	`proxy_set_header`	–	`x-ssl-client-cert $ssl_client_escaped_cert`

Из-за многократного описания контекстов `location` определенный набор директив повторяется. Для удобства конфигурации вынесите этот набор директив в отдельный файл и включите директивы из этого файла в описание контекста (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. Убедитесь, что имена контекстов `location` совпадают с путем к проксируемому сервису.

Пример файла *nginx.conf* для работы с Indeed CM

```
user nginx;
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;

 large_client_header_buffers 4 16k;

 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. Чтобы применить изменения в конфигурационном файле, перезагрузите конфигурацию или перезапустите nginx.

```
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 Apache.
2. Установите SSL/TLS-сертификат.
3. Настройте модули и конфигурацию.
4. Настройте сайт Apache.

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 сайте Apache.

Установка SSL/TLS-сертификата

Как создать SSL/TLS-сертификат для веб-сервера

Чтобы установить SSL/TLS-сертификат на веб-сервер:

1. Скопируйте файлы сертификата и ключа в папки для хранения сертификатов и закрытых ключей.

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

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

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

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

Настройка модулей и конфигурации

Apache имеет модульную архитектуру: ядро обеспечивает базовую функциональность, а расширенные возможности подключаются через отдельные модули.

1. Для работы системы включите следующие 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 этом месте и далее замените *SERVER_FQDN* на имя сервера, на который вы устанавливаете Apache.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> При установке Apache в ОС Astra Linux вам может потребоваться отключить параметр AstraMode в файле *apache2.conf*. Подробнее на сайте 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

        #ProxyPass /api http://localhost:5010/api
        #ProxyPassReverse /api http://localhost:5010/api

</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
```

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 сайте Apache.

Установка SSL/TLS-сертификата

Как создать SSL/TLS-сертификат для веб-сервера

Чтобы установить SSL/TLS-сертификат на веб-сервер:

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

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

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

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

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

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 этом месте и далее замените *SERVER_FQDN* на имя сервера, на который вы устанавливаете Apache.

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 logs/error.log
   CustomLog logs/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

       #ProxyPass /api http://localhost:5010/api
       #ProxyPassReverse /api http://localhost:5010/api

</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 logs/error.log
   CustomLog logs/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
```

Платформа .NET

Для работы серверных компонентов установите платформу .NET версии 8.0.10 и выше.

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

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

Windows

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

Чтобы установить .NET:

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 на ОС Linux требуется учетная запись с правами суперпользователя.

Чтобы установить .NET:

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-8.0.22-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:

```
dotnet --info
```

Установка и настройка серверных компонентов

1. Установите сервер Indeed CM.
2. Для инсталляций на ОС Linux настройте сервер авторизации пользователей OpenID Connect.
3. Для инсталляций на ОС Linux или конфигураций с несколькими серверами настройте единый журнал событий.
4. Если используется конфигурация с Indeed CM Agent, то выполните его установку и настройку.
5. Настройте параметры работы Indeed CM в Мастере настройки.

Indeed CM Server

Установка сервера Indeed CM

Сервер OpenID Connect

Настройка сервера OpenID Connect

Мастер настройки

Настройка файлов конфигурации сервисов Indeed CM в Мастере настройки

Единый журнал событий

Настройка записи событий в общий журнал

Indeed CM Agent

Настройка клиентского агента

Indeed CM Server

Indeed CM Server — основной серверный компонент Indeed Certificate Manager, который позволяет управлять жизненным циклом устройств и сертификатов пользователей.

Сервисы

Indeed CM состоит из набора сервисов. Каждый сервис имеет собственные файлы конфигурации и настройки доступа.

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

Установка сервера

Системные требования

Выберите инструкцию в зависимости от ОС рабочей станции, на которой вы планируете установить сервер Indeed CM.

Windows

1. В дистрибутиве Indeed CM перейдите в каталог *IndeedCM.WindowsServer* и выполните файл *IndeedCM.Server-<номер версии>.x64.ru-ru.msi*. Откроется Мастер установки сервера Indeed CM.

2. Выберите способ контроля доступа для приложений Indeed CM: аутентификация Windows, OpenID Connect или по персональным сертификатам пользователей.

   > ⚠ **ПРЕДУПРЕЖДЕНИЕ**
   >
   > Выберите тот же способ аутентификации при настройке контроля доступа к веб-приложениям Indeed CM в Мастере настройки.

   Параметры контроля доступа настраиваются автоматически. После установки сервера параметры SSL для каждого приложения можно изменить вручную в Диспетчере служб IIS (Internet Information Services (IIS) Manager).

Параметры контроля доступа

В зависимости от выбранного способа контроля доступа в Диспетчере служб IIS (Internet Information Services (IIS) Manager) автоматически устанавливаются следующие параметры:

Аутентификация Windows

- **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 разблокировки и выключения устройств (`credprovapi`)
    Сервисы клиентских агентов (`agentregistrationapi`, `agentserviceapi`)
  - **Анонимная проверка подлинности** (Anonymous Authentication) и **Проверка подлинности с помощью форм** (Forms Authentication) для Сервиса 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 и выключения устройств (`credprovapi`)
      Сервис API (`api`)
      Сервис регистрации клиентских агентов (`agentregistrationapi`)
    - **Требовать** (Require) для Сервиса агентов (`agentserviceapi`).

Аутентификация OpenID Connect

- **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 Сервиса 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 и выключения устройств (`credprovapi`)
      Сервис API (`api`)
      Сервис регистрации клиентских агентов (`agentregistrationapi`)
    - **Требовать** (Require) для Сервиса агентов (`agentserviceapi`).

Аутентификация по сертификату

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> Если в качестве каталога пользователей используется LDAP-каталог, то сертификаты, используемые для аутентификации, должны содержать значение UPN (User Principal Name). Администраторы и пользователи не смогут войти в веб-приложения Indeed CM по сертификату, если он не содержит UPN.

- **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 Сервиса 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 и выключения устройств (`credprovapi`)
      Сервис регистрации клиентских агентов (`agentregistrationapi`)
    - **Требовать** (Require) для следующих веб-приложений:
      Консоль управления (`mc`)
      Сервис самообслуживания (`ss`)
      Сервис API (`api`)
      Сервис агентов (`agentserviceapi`)

3. Выпустите SSL/TLS-сертификат для защищенного подключения к веб-приложениям Indeed CM.

   ▼ **Требования к SSL/TLS-сертификату для IIS**

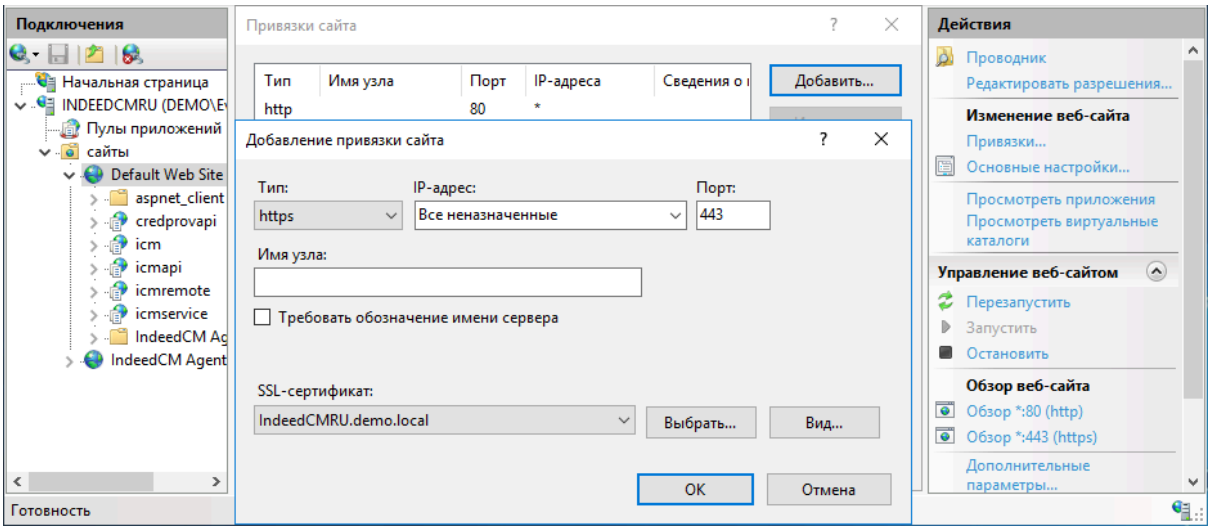
   Субъект (Subject) сертификата должен содержать атрибут **Общее имя** (Common Name) (FQDN сервера Indeed CM).

   Дополнительное имя субъекта (Subject Alternative Name) сертификата должно содержать атрибут **DNS-имя** (DNS Name) (FQDN сервера Indeed CM). Например, *server.domain.loc* или соответствующую запись с подстановочными знаками, например: **. domain.loc* (Wildcard certificate).

   Улучшенный ключ (Enhanced Key Usage) сертификата должен содержать значение «Проверка подлинности сервера» (Server Authentication).

4. Добавьте SSL/TLS-сертификат 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**.



Linux

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Для установки и настройки сервера Indeed CM на Linux нужны права суперпользователя.

1. Перейдите в каталог с дистрибутивом Indeed CM и установите пакет с сервером через пакетный менеджер.

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

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

2. Установите TrueType шрифты Windows для корректной работы Сервиса удаленного самообслуживания.

```
#Создание папки для шрифтов
sudo mkdir -p /usr/share/fonts/truetype/msttcorefonts

#Распаковка архива со шрифтами из дистрибутива Indeed CM
sudo tar -xzf msttcorefonts.tar.gz -C /usr/share/fonts/truetype/

#Обновление кеша шрифтов
sudo fc-cache -fv
```

3. Настройте запуск сервисов Indeed CM.

При установке сервера в каталоге */etc/systemd/system/* автоматически создаются файлы служб systemd. По умолчанию службы запускаются от имени учетной записи www-data.

Настройка учетной записи в RHEL и производных дистрибутивах

В RHEL и производных дистрибутивах учетной записи www-data нет. Создайте ее или укажите другую учетную запись, от имени которой будут запускаться сервисы Indeed CM.

Чтобы создать учетную запись www-data, используйте утилиту useradd:

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

Чтобы указать другую учетную запись:

1. Перейдите в каталог */etc/systemd/system/*.
2. В файлах служб *cm-<имя сервиса>.service* в директиве `User=` замените www-data на имя своей учетной записи.

Пример файла службы с учетной записью 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 запустить службы, выполните:

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

4. Настройте параметры работы Indeed CM в Мастере настройки (рекомендуется) или вручную.

5. Для безопасной работы с других рабочих станций настройте веб-сервер.

Сервер 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. Установите сервер OpenID Connect до установки сервера Indeed CM.

> **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).

Выберите инструкцию в зависимости от ОС рабочей станции, где вы планируете установить сервер Indeed CM.

Windows

1. Установите сервер OIDC из дополнительного пакета *IndeedCM.Oidc.Server-<номер версии>.x64.ru-ru.msi*.
2. Установите сервер Indeed CM и в Мастере установки сервера выберите способ контроля доступа Аутентификация OpenID Connect.
3. Подготовьте сертификат подписи JWT-токенов по инструкции ниже.
4. Настройте параметры взаимодействия Indeed CM с сервером OIDC в Мастере настройки в разделе **Контроль доступа** → OpenID Connect.
5. Примените настройки на сервере Indeed CM.

Подготовка сертификата подписи JWT-токенов

В качестве сертификата подписи используйте сертификат и закрытый ключ, созданные для веб-сервера.

Чтобы подготовить сертификат подписи:

1. Поместите сертификат подписи в хранилище *Локальный компьютер – Личное*.

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

Изменение настроек базы данных

По умолчанию сервер OIDC использует локальную базу данных SQLite. База данных SQLite используется для инсталляций с одним сервером Indeed CM. Данные сервера OIDC хранятся в каталоге *C:\inetpub\wwwroot\cm\oidc\data*.

Помимо SQLite, вы можете использовать базу данных Microsoft SQL или PostgreSQL. Чтобы настроить подключение к Microsoft SQL или PostgreSQL, внесите изменения в конфигурационный файл сервера OIDC *appsettings.json* вручную. Файл *appsettings.json* находится в каталоге *C:\inetpub\wwwroot\cm\oidc*.

Microsoft SQL

1. Создайте базу данных в SQL Server Management Studio.
2. Откройте конфигурационный файл сервера OIDC *appsettings.json* и измените секции `defaultConnection` и `provider`. В примере для подключения к базе данных используется SQL аутентификация.

    Пример подключения к Microsoft SQL

```
"connectionStrings": {
  "defaultConnection": "Data Source=MSSQL\SQLEXPRESS;Initial Catalog=oidcdb;Persist
Security Info=True;User
ID=servicesql;Password=p@ssw0rd;TrustServerCertificate=True"
},
"database": {
  "provider": "mssql"
},
```

3. Перезапустите пул приложения IndeedCM OIDC, 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 OIDC и в правом меню нажмите **Перезапуск** (Recycle).

PostgreSQL

1. Создайте базу данных в PostgreSQL.
2. Откройте конфигурационный файл сервера OIDC *appsettings.json* и измените секции `defaultConnection` и `provider`. Если вы используете файл PGPASS, не включайте директиву `Password` в строку подключения.

    Пример подключения к PostgreSQL

    ```
    "connectionStrings": {
      "defaultConnection":
    "Host=172.17.0.11;Port=5432;Database=oidcdb;Username=servicepg;Password=p@ssw0rd"
    },
    "database": {
      "provider": "pgsql"
    },
    ```

3. Перезапустите пул приложения IndeedCM OIDC, 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 OIDC и в правом меню нажмите **Перезапуск** (Recycle).

Linux

1. Установите сервер Indeed CM. Сервер OIDC является частью дистрибутива Indeed CM и устанавливается вместе с сервером Indeed CM.
2. Подготовьте сертификат подписи JWT-токенов по инструкции ниже.
3. Настройте параметры взаимодействия Indeed CM с сервером OIDC в Мастере настройки в разделе Контроль доступа.
4. Примените настройки на сервере Indeed CM.

Подготовка сертификата подписи JWT-токенов

В качестве сертификата подписи используйте сертификат и закрытый ключ, созданные для веб-сервера.

Чтобы подготовить сертификат подписи:

1. Создайте поддиректорию в домашнем каталоге пользователя, от имени которого запускается сервер OIDC (по умолчанию – www-data).

```
sudo mkdir -p /var/www/.dotnet/corefx/cryptography/x509stores/my/
```

Как проверить наличие пользователя www-data

1. Чтобы проверить наличие пользователя www-data, выполните:

```
/etc/passwd | grep www-data
```

Пример вывода, если пользователь www-data существует

```
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
```

2. Если пользователя www-data не существует, вы можете его создать или сменить пользователя, от имени которого запускаются сервисы Indeed CM.

   Чтобы создать пользователя www-data и войти от его имени, выполните:

```
sudo useradd -m -d /var/www -s /usr/sbin/nologin www-data
sudo su -s /bin/sh www-data
```

   Чтобы сменить пользователя, выполните следующую команду и укажите имя пользователя в директиве `User`.

```
/etc/systemd/system/cm-<имя сервиса>.service
```

2. Объедините файл сертификата и файл ключа в файл PFX. Поместите файл PFX в поддиректорию домашнего каталога пользователя.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> При выполнении команды утилита openssl предлагает установить пароль для файла PFX. Оставьте файл PFX без пароля: два раза нажмите Enter.

```
sudo openssl pkcs12 -export -out
/var/www/.dotnet/corefx/cryptography/x509stores/my/PFXFILE.pfx -inkey SSL.key -in
SSL.crt
```

3. Настройте право доступа 600 к файлу PFX.

```
sudo chmod 600 /var/www/.dotnet/corefx/cryptography/x509stores/my/PFXFILE.pfx
```

4. Получите отпечаток сертификата подписи.

```
sudo openssl x509 -fingerprint -in SSL.crt -noout | tr -d ':'
```

Пример вывода отпечатка сертификата

```
SHA1 Fingerprint=ADB613EC1A1692310D83C81F269C098A3DBD4EE0
```

Изменение настроек базы данных

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 сохраняются в каталоге */opt/indeed/cm/oidc/data*.

Помимо SQLite, вы можете использовать базу данных Microsoft SQL или PostgreSQL. Чтобы настроить подключение к Microsoft SQL или PostgreSQL, внесите изменения в конфигурационный файл сервера OIDC *appsettings.json* вручную. Файл *appsettings.json* находится в каталоге */opt/indeed/cm/oidc*.

Microsoft SQL

1. Создайте базу данных в SQL Server Management Studio.
2. Откройте конфигурационный файл сервера OIDC *appsettings.json* и измените секции `defaultConnection` и `provider`. В примере для подключения к базе данных используется SQL аутентификация.

   Пример подключения к Microsoft SQL

   ```
   "connectionStrings": {
     "defaultConnection": "Data Source=MSSQL\SQLEXPRESS;Initial
   Catalog=oidcdb;Persist Security Info=True;User
   ID=servicesql;Password=p@ssw0rd;TrustServerCertificate=True"
   },
   "database": {
     "provider": "mssql"
   },
   ```

3. Перезагрузите сервис OIDC, чтобы применить изменения.

```
sudo systemctl restart cm-oidc.service
```

PostgreSQL

1. Создайте базу данных в PostgreSQL.
2. Откройте конфигурационный файл сервера OIDC *appsettings.json* и измените секции `defaultConnection` и `provider`. Если вы используете файл PGPASS, не включайте директиву `Password` в строку подключения.

   Пример подключения к PostgreSQL

   ```
   "connectionStrings": {
     "defaultConnection":
   "Host=172.17.0.11;Port=5432;Database=oidcdb;Username=servicepsql;Password=p@ssw0rd"
   },
   "database": {
     "provider": "pgsql"
   },
   ```

3. Перезагрузите сервис OIDC, чтобы применить изменения.

   ```
   sudo systemctl restart cm-oidc.service
   ```

Мастер настройки

Мастер настройки позволяет автоматически заполнить файлы конфигурации для каждого сервиса 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

1. Установите Мастер настройки.

   Debian

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

RHEL

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

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.log* 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, используйте 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.domain.loc/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, используйте 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.domain.loc/ls/api` для ОС Windows, `https://server.domain.loc/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 интеграцию с удостоверяющими центрами:

- Microsoft Enterprise CA
- Aladdin Enterprise CA
- SafeTech CA
- Dogtag CA
- КриптоПро УЦ 2.0
- КриптоПро DSS
- Валидата УЦ

Для КриптоПро УЦ 2.0 доступна опция **Публиковать сертификаты пользователей КриптоПро УЦ 2.0 в базе приложений ЦФТ**. Укажите строку подключения к 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**.

AirCard Enterprise

Настройте интеграцию с Indeed AirCard Enterprise:

1. Включите опцию **Включить интеграцию с Indeed AirCard Enterprise**.
2. Введите URL подключения к серверу AirCard Enterprise, например, `https://aircard.domain.loc: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. Инструкция по установке 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

Чтобы сменить стратегию генерации идентификатора агента после первоначальной настройки Indeed CM:

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. В выпадающем списке **Уровень журналирования событий агентом** выберите, какие события агента попадают в журнал событий – все, только ошибки, только предупреждения и ошибки.

7. Заполните поля **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. Вы можете подключить несколько каталогов пользователей.

LDAP

Нажмите **Добавить** и выберите тип каталога пользователей.

Active Directory, Samba AD DC, РЕД АДМ, Альт Домен

1. Укажите данные учетной записи, у которой есть права на доступ к каталогу пользователей: имя в формате DOMAIN\UserName или UserName@DNSDomainName и пароль.

   Как настроить сервисную учетную запись для работы с каталогом пользователей

2. Укажите NetBIOS-имя домена и DNS-имя домена или контроллера домена.

   > **КАК НАЙТИ DNS-ИМЯ И NETBIOS-ИМЯ ДОМЕНА**
   >
   > Выполните в командной строке:
   >
   > `set USERDNSDOMAIN`, чтобы узнать DNS-имя домена.
   > `set USERDOMAIN`, чтобы узнать NetBIOS-имя домена.

3. Укажите путь к контейнеру с пользователями в формате Distinguished Name. Для работы со всеми пользователями выберите корень домена.

4. Если вы используете протокол LDAPS для доступа к каталогам, включите опцию **Использовать LDAPS**.

5. Чтобы отображать фотографию пользователя в интерфейсе Indeed CM или напечатать ее на смарт-карте, выберите атрибут, который содержит фотографию пользователя.

6. Нажмите **Сохранить**.

> ⚠ **ДЛЯ СУЩЕСТВУЮЩЕЙ КОНФИГУРАЦИИ INDEED CM**
>
> Если Indeed CM был ранее настроен на работу с каталогом пользователей в Active Directory, и контроллер домена был перенастроен с Active Directory на Samba AD DC, РЕД АДМ или Альт Домен, то параметры конфигурации каталога пользователей менять не нужно.

FreeIPA, ALD Pro, OpenLDAP

1. Укажите данные учетной записи, у которой есть права на доступ к каталогу пользователей: имя в формате Distinguished Name и пароль.

   Как настроить сервисную учетную запись для работы с каталогом пользователей

2. Укажите NetBIOS-имя домена и DNS-имя домена или контроллера домена.

   > 💡 **КАК НАЙТИ DNS-ИМЯ И NETBIOS-ИМЯ ДОМЕНА**
   >
   > Выполните в командной строке:
   >
   > `set USERDNSDOMAIN`, чтобы узнать DNS-имя домена.
   > `set USERDOMAIN`, чтобы узнать NetBIOS-имя домена.

3. Укажите путь к объекту с пользователями в формате Distinguished Name. Для FreeIPA и ALD Pro рекомендуем указать корень домена или каталог accounts.

4. Если вы используете протокол LDAPS для доступа к каталогам, включите опцию **Использовать LDAPS**.

5. Нажмите **Сохранить**.

ЦР КриптоПро УЦ 2.0

Как настроить каталог пользователей в ЦР 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. Выберите тип интеграции API с каталогом пользователей ЦР КриптоПро УЦ 2.0: REST или SOAP.
4. Укажите отпечаток сертификата сервисной учетной записи, который будет использоваться для подключения к ЦР КриптоПро УЦ 2.0 для просмотра списка пользователей.
5. Укажите URL подключения к Центру Регистрации. Например, `https://cryptopro.domain.loc/RA/RegAuthLegacyService.svc`.
6. Нажмите **Сохранить**.

Внутренний каталог

Как настроить внутренний каталог пользователей

В качестве внутреннего каталога пользователей используйте базу данных Microsoft SQL или PostgreSQL.

1. Нажмите **Добавить**.
2. Выберите тип хранилища.
3. Настройте подключение к хранилищу. Введите имя сервера, имя экземпляра (для Microsoft SQL), номер порта и имя базы данных.
4. 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.
5. Нажмите **Сохранить**.

Дополнительные атрибуты внутреннего каталога

Чтобы настроить дополнительные атрибуты внутреннего каталога пользователей:

1. Нажмите **Добавить**.

2. Введите имя атрибута в каталоге пользователей и отображаемое имя атрибута.
3. Чтобы атрибут отображался при создании и редактировании пользователя в Indeed CM, включите опцию **Отображать в форме создания/редактирования пользователя**.
4. Чтобы сделать атрибут обязательным для заполнения при создании и редактировании пользователя в Indeed CM, включите опцию **Обязательный для заполнения**.
5. Выберите тип атрибута:

- **Текст**
  Для текстового атрибута укажите следующие настройки:
  - Максимальная длина текста – максимальное количество символов.
  - Формат текста – регулярное выражение, с помощью которого будет проверяться корректность текстового значения атрибута. Например, проверка корректности ввода отчества, при которой допустимы русские буквы, пробел и дефис: `^[А-ЯЁ][а-яё]{0,30}(( |-)([а-яё]{0,30})){0,2}$`.
  - Сообщение о неверном формате – текст сообщения, который будет отображаться при вводе текстового значения, не отвечающего требованиям регулярного выражения.

- **Целочисленный**
  Укажите минимальное и максимальное значение. Например, для ввода информации о возрасте.
- **Логический**
  Атрибут может принимать значение `true` или `false`.
- **Справочник значений**
  Укажите справочник, который будет использоваться при выборе значений атрибута. Формат: `<значение атрибута #1>, <отображаемое значение атрибута #1>; <значение атрибута #2>, <отображаемое значение атрибута #2>;...`. Например, `red, Красный цвет; green, Зеленый цвет`.

6. Нажмите **Сохранить**.

Соответствия атрибутов

Вы можете настроить соответствие атрибутов удостоверяющего центра (УЦ) с атрибутами пользователей, чтобы корректно передавать данные пользователя из каталога в запрос на сертификат. Для КриптоПро УЦ 2.0 соответствие атрибутов дополнительно используется, чтобы зарегистрировать пользователя в Центре Регистрации (ЦР) или обновить его данные – как вручную, так и автоматически при выпуске устройства в Indeed CM.

Большинство соответствий атрибутов настроены по умолчанию. При необходимости отредактируйте атрибуты пользователя или добавьте собственные настройки соответствия атрибутов.

Обновляемые атрибуты

Вы можете настроить список атрибутов каталога пользователей, при изменении которых сертификат на устройстве нужно обновить. Отслеживать можно только атрибуты из полей **Субъект** (Subject) и **Дополнительное имя субъекта** (Subject Alternative Name) сертификата. По умолчанию отслеживаются атрибуты Общее имя, E-mail и UPN-имя пользователя.

> **ПРИМЕЧАНИЕ**
>
> Отслеживание атрибутов не поддерживается для КриптоПро DSS.

Чтобы добавить настройки отслеживания атрибута:

1. Нажмите **Добавить**.
2. Укажите параметры:
   - **Атрибут пользователя** – имя атрибута в каталоге пользователей.
   - **Отображаемое имя атрибута** – имя атрибута пользователя для отображения в интерфейсе Indeed CM.
   - **X.500 имя или OID атрибута сертификата** – по указанному значению выполняется поиск атрибута в сертификате.
3. 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 или Linux.

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

Настройка аутентификации OpenID Connect

1. Укажите следующие настройки:
   - URL подключения к серверу OpenID Connect.
   - Полное доменное имя (FQDN) сервера Indeed CM. Для конфигурации с несколькими серверами укажите их полные доменные имена через запятую.
   - Отпечаток сертификата подписи.

2. При необходимости сгенерируйте клиентские секреты.

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 в зависимости от окружения, в котором развернут Indeed CM: 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. Укажите учетную запись, от имени которой будет запускаться служба Card Monitor, в формате DOMAIN\UserName или UserName@DNSDomainName. Требования к учетной записи:
   - Входит в каталог пользователей Indeed CM
   - Состоит в группе Администраторов (Administrators) на сервере Indeed CM
   - 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** можно настроить следующее:

- **Выключить устройства отключенных 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.
- **Настроить фильтр поведения отключенных пользователей как удаленных**. 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=domain,DC=loc`.
- **Изъять устройства у удаленных пользователей**. Устройства у удаленных пользователей изымаются и переходят в состояние *Пустое*. При изъятии устройство не очищается.

4. В разделе **Операции с агентами** можно настроить следующее:
   - **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.

> **ПРИМЕЧАНИЕ**
> 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

Сервис регистрации агентов	`AgentRegistrationApi`
Сервис агентов	`AgentServiceApi`
Сервис очистки AirCard	`AirKeyCleaner`
Сервис API	`Api`
Служба Card Monitor	`CardMonitor`
Служба разблокировки и выключения устройств	`CredentialProvider`
Консоль управления	`ManagementConsole`
Компонент MS CA Proxy	`MsCaProxy`
Сервер OpenID Connect	`Oidc`
Сервис удаленного самообслуживания	`RemoteService`
Сервис самообслуживания	`SelfService`

- 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

Сервис регистрации агентов	`AgentRegistrationApi`
Сервис агентов	`AgentServiceApi`
Сервис очистки AirCard	`AirKeyCleaner`
Сервис API	`Api`
Служба Card Monitor	`CardMonitor`
Служба разблокировки и выключения устройств	`CredentialProvider`
Консоль управления	`ManagementConsole`
Компонент MS CA Proxy	`MsCaProxy`
Сервер OpenID Connect	`Oidc`
Сервис удаленного самообслуживания	`RemoteService`
Сервис самообслуживания	`SelfService`

- 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

Сервис регистрации агентов	`AgentRegistrationApi`
Сервис агентов	`AgentServiceApi`
Сервис очистки AirCard	`AirKeyCleaner`
Сервис API	`Api`
Служба Card Monitor	`CardMonitor`
Служба разблокировки и выключения устройств	`CredentialProvider`
Консоль управления	`ManagementConsole`
Сервер OpenID Connect	`Oidc`
Сервис удаленного самообслуживания	`RemoteService`
Сервис самообслуживания	`SelfService`

- 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"
```

4. После шифрования конфигурации перезапустите сервисы Indeed CM:

```
systemctl restart cm-*
```

Расшифровка

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

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

```
dotnet Cm.Config.DataProtector.dll unprotect
```

- Расшифровка файлов конфигурации отдельных компонентов:

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

Пример команды

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

Названия компонентов Indeed CM

Сервис регистрации агентов	`AgentRegistrationApi`
Сервис агентов	`AgentServiceApi`
Сервис очистки AirCard	`AirKeyCleaner`
Сервис API	`Api`
Служба Card Monitor	`CardMonitor`
Служба разблокировки и выключения устройств	`CredentialProvider`
Консоль управления	`ManagementConsole`
Сервер OpenID Connect	`Oidc`
Сервис удаленного самообслуживания	`RemoteService`
Сервис самообслуживания	`SelfService`

- Расшифровка файла конфигурации, расположенного вне стандартной директории:

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

Пример команды

```
dotnet Cm.Config.DataProtector.dll unprotect --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 Диспетчер служб IIS (Internet Information Services Manager) и в левом меню выберите **Пул приложений IIS** (Application pools).
2. Выберите приложение IndeedCM Wizard и в правом меню нажмите **Остановить** (Stop).

Linux

1. Откройте эмулятор терминала.
2. Выполните команду:

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

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 Log Server.

Indeed CM Event Log Proxy

Приложение Indeed CM Event Log Proxy позволяет записывать события с одного или нескольких серверов Indeed Certificate Manager в единый журнал Windows Event Log. Indeed CM Event Log Proxy можно установить только на рабочую станцию под управлением ОС Windows.

Системные требования

Чтобы установить и настроить Indeed CM Event Log Proxy:

1. Выполните вход на рабочую станцию с правами локального администратора.
2. Откройте каталог *IndeedCM.Server* дистрибутива системы и запустите Мастер установки *IndeedCM.EventLog.Proxy-<номер версии>.x64.ru-ru.msi*.
3. В Мастере установки выберите способ аутентификации в зависимости от ОС, где установлен сервер Indeed CM, и укажите необходимые настройки в файлах конфигурации.

   Windows

   1. Выберите способ аутентификации Windows.
   2. По завершении установки нажмите **Готово** и закройте Мастер установки.
   3. Откройте файл *web.config* (*C:\inetpub\wwwroot\cm\eventlogproxy*) в редакторе Блокнот от имени администратора.
   4. В параметре `allow users` укажите учетную запись из домена, где установлен Event Log Proxy. Например, сервисную учетную запись для работы с каталогом пользователей.

Пример

```
<authorization>
     <clear />
     <add accessType="Allow" users="DOMAIN\servicecm" />
</authorization>
```

5. Сохраните изменения и закройте файл *web.config*.

Linux

1. Выберите способ аутентификации по сертификату. По завершении установки нажмите **Готово** и закройте Мастер установки.

2. Откройте файл *appsettings.json* (*C:\inetpub\wwwroot\cm\eventlogproxy*) в редакторе Блокнот от имени администратора.

3. В секции `authSettings` в параметре `allowedCertificateThumbprints` укажите отпечаток клиентского сертификата, разрешенного к предъявлению сервером Indeed CM. Убедитесь, что поле **Улучшенный ключ** (Enhanced Key Usage) сертификата содержит значение «Проверка подлинности клиента» (Client Authentication), и сертификат установлен в хранилище сертификатов сервера Indeed CM.
   Как выпустить клиентский сертификат

   Пример

   ```
   "authSettings":{
   "authorizeByCertificate": "true",
   "allowedCertificateThumbprints": "aba8b93d73343f2182e3c1c40482b2ae2d75b6ec"
   }
   ```

4. Сохраните изменения и закройте файл *appsettings.json*.

4. 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 Indeed CM Event Log Proxy и в правом меню нажмите **Перезапуск** (Recycle).

Log Server

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.

Системные требования

Log Server можно установить на рабочую станцию под управлением ОС Windows или Linux.

Windows

Установка

Перед установкой Log Server установите платформу .NET версии 8.0 и модуль URL Rewrite.

Чтобы установить Log Server:

1. Выполните вход на рабочую станцию с правами локального администратора.
2. Запустите *LogServer-<номер версии>.x64.ru-ru.msi* из каталога *Log.Server* дистрибутива Indeed CM и следуйте указаниям мастера.
3. Из каталога *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

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

Вы можете настроить чтение и запись событий в хранилища Windows Event Log, Microsoft SQL, PostgreSQL, Syslog.

Windows Event Log

1. Перейдите в каталог *C:\inetpub\wwwroot\ls* и отредактируйте файл *clientApps.config*.
   - В секции `Applications` добавьте следующие параметры.

```
<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.

Microsoft SQL Server

1. Создайте базу данных и сервисную учетную запись в SQL Server Management Studio.

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

   - `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.
   - `TrustServerCertificate` – настройка доверия сертификату сервера. Установите значение `True`.

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

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

   - В секции `Application` добавьте следующие параметры.

```
<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

1. Создайте базу данных и сервисную учетную запись в PostgreSQL.
2. Создайте расширение uuid-ossp, которое предоставляет функции для генерации Universally Unique Identifiers (UUID).

   1. Введите текст запроса в поле ввода Запросника.

```
CREATE EXTENSION IF NOT EXISTS "uuid-ossp";
```

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

3. Перейдите в каталог *C:\inetpub\wwwroot\ls\targetConfigs* и отредактируйте файл *cmPgSqlTarget.config*. В секции `<ConnectionString>…</ConnectionString>` заполните следующие параметры:

- `Host` - имя сервера PostgreSQL Server.
- `Port` - порт для подключения к PostgreSQL. Значение по умолчанию — 5432.
- `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=P@ssw0rd</Connect
</Settings>
```

4. 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

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*. В секции `<ConnectionString>…</ConnectionString>` заполните следующие параметры:

    - `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 Log Server и в правом меню нажмите **Перезапуск** (Recycle).

Linux

Установка

1. Установите Log Server.

   Debian

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

   RHEL

   ```
   sudo rpm -i indeed.logserver-<номер версии>.x86_64.rpm
   ```

2. Из каталога *Log.Server* скопируйте файл *cmSchema.config* в каталог */opt/indeed/ls*.

   ```
   sudo cp ./cmSchema.config /opt/indeed/ls/
   ```

Настройка чтения и записи событий

Log Server поддерживает чтение событий только из одного хранилища (`ReadTargetId`). Запись событий возможна одновременно в несколько хранилищ (`WriteTargets`).

Вы можете настроить чтение и запись событий в хранилища Microsoft SQL, PostgreSQL и Syslog.

Microsoft SQL

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

1. Создайте базу данных в среде SQL Server 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:).
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 Microsoft SQL или учетную запись из поддерживаемого LDAP-каталога пользователей. Например, сервисную учетную запись для работы Indeed CM.
>
> После создания базы данных указанная учетная запись будет обладать правами *db_owner, public*. Indeed CM будет использовать эту учетную запись для чтения/записи в базу данных.

2. Перейдите в каталог */opt/indeed/ls/targetConfigs* и отредактируйте файл *cmMsSqlTarget.config*. В секции `<Settings>…</Settings>` заполните следующие параметры:

   - `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.
   - `TrustServerCertificate` – настройка доверия сертификату сервера. Установите значение True.

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

3. Перейдите в каталог */opt/indeed/ls* и отредактируйте файл *clientApps.config*.

   - В секции `Application` добавьте следующие параметры.

```
<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>
```

PostgreSQL

База для хранения данных 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), выберите из списка **Владелец** (Owner) сервисную учетную запись, которая будет использоваться для подключения к базе данных.
    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).
    2. Введите текст запроса, указав в запросе имя учетной записи.

```
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA public TO <имя сервисной учетной записи>;
```

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

3. Создайте расширение uuid-ossp, которое предоставляет функции для генерации Universally Unique Identifiers (UUID):

    1. Очистите поле ввода Запросника.
    2. Введите текст запроса.

```
CREATE EXTENSION IF NOT EXISTS "uuid-ossp";
```

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

4. По умолчанию в PostgreSQL разрешены только локальные подключения к базам данных. Для работы между различными серверами настройте удаленное подключение к базе данных.

    1. В каталоге PostgreSQL откройте конфигурационный файл *pg_hba.conf*. Файл находится в каталоге */etc/postgresql/<номер версии>/main*.
    2. В конце файла добавьте строку следующего типа.

```
CONNECTIONTYPE DATABASE USER ADDRESS METHOD
```

    Где:

    - `CONNECTIONTYPE` – тип подключения. Чтобы использовать подключение по TCP/IP, укажите `host`.
    - `DATABASE` – имя базы данных, для которой предоставляется доступ. Для доступа ко всем базам данных укажите `ALL`.
    - `USER` – имя пользователя, для которого будет доступно подключение. Для доступа всех пользователей укажите `ALL`.
    - `ADDRESS` – IP-адрес удаленного сервера Indeed CM. Для доступа с любых адресов укажите `0.0.0.0/0`.
    - `METHOD` – метод аутентификации пользователя. Например, `md5`, `scram-sha-256`.

Пример

```
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
```

5. В каталоге */opt/indeed/ls/targetConfigs* отредактируйте файл *cmPgSqlTarget.config*. В секции `<ConnectionString>…</ConnectionString>` заполните следующие параметры:

   - `Host` – имя сервера PostgreSQL Server.
   - `Port` – порт для подключения к PostgreSQL. Значение по умолчанию — 5432.
   - `Database` – имя 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=P@ssw0rd</Connect
</Settings>
```

6. Перейдите в каталог */opt/indeed/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

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

1. В каталоге */opt/indeed/ls/targetConfigs* отредактируйте файл *cmSysLogTarget.config*. В секции `<ConnectionString>…</ConnectionString>` заполните следующие параметры:

   - `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 */opt/indeed/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>
```

Применение настроек

1. Откройте конфигурационный файл веб-сервера nginx или Apache и раскомментируйте строки обработки приложения api.

Пример для nginx

```
 location /api
{  include /etc/nginx/conf.d/proxy.conf;   proxy_pass http://localhost:5010/api;   }
```

Пример для Apache

```
ProxyPass /api http://localhost:5010/api
ProxyPassReverse /api http://localhost:5010/api
```

2. Перезапустите веб-сервер.
3. Перезапустите сервис Log Server.

```
sudo systemctl restart indeed-ls.service
```

Настройка Indeed CM для работы с единым журналом событий

1. Настройте подключение к журналу событий в Мастере настройки.
2. Проверьте работу журнала событий. Перейдите в Консоль управления, откройте раздел **Журнал** и выполните поиск событий.

Ожидаемый результат: отсутствие 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

Клиентский агент Indeed CM Agent – дополнительный компонент, который позволяет удаленно управлять устройствами пользователей (USB-токенами, смарт-картами). Indeed CM Agent устанавливается на рабочие станции пользователей после настройки серверных компонентов Indeed CM.

С помощью агента на рабочих станциях пользователей выполняются следующие операции:

- Добавление и назначение устройства
- Выпуск пустого или назначенного устройства
- Продолжение выпуска и обновления устройства в состоянии *В ожидании*
- Запрос смены PIN-кода пользователя по расписанию
- 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

Установка и настройка

Установите Indeed CM Agent вместе с Indeed CM Middleware на рабочие станции, к которым подключаются устройства.

1. Подготовьте сертификаты для работы агента.
2. Настройте защищенное соединение с сайтом агента.
3. Откройте Мастер настройки Indeed CM и укажите параметры для работы с агентами.
4. Установите и настройте агенты на рабочих станциях.

Подготовка сертификатов агента

Для работы агента создайте следующие сертификаты:

Сертификат УЦ	Используется для выдачи сертификатов рабочим станциям пользователей, на которых устанавливаются агенты.
Сертификат проверки подлинности	Используется для установки двустороннего защищенного соединения между сервером Indeed CM и рабочей станцией с установленным агентом. Подписывается сертификатом УЦ. Выдается на имя рабочей станции, на которой установлен сервер Indeed CM.
Сертификат агента	Выдается автоматически при регистрации агента. Подписывается сертификатом УЦ. Обращаясь к серверу, клиентская рабочая станция предоставляет свой сертификат, а сервер Indeed CM проверяет его подлинность. После проверки сервер добавляет клиентскую рабочую станцию в список доверенных и может передавать на нее задачи.

Подготовьте сертификаты одним из способов:

- С помощью утилиты Cm.Agent.Cert.Generator

  Выпустите самоподписанный сертификат УЦ и сертификат проверки подлинности с помощью утилиты Cm.Agent.Cert.Generator.

- В удостоверяющем центре (УЦ)

  Заполните файлы конфигурации сервисов агента (**agentregistrationapi** и **agentserviceapi**) для автоматического выпуска сертификатов агента (поддерживаются сертификаты, выпущенные в SafeTech CA).

Cm.Agent.Cert.Generator

Параметры утилиты Cm.Agent.Cert.Generator

Параметры генерации самоподписанного сертификата УЦ и SSL-сертификата

Параметр	Описание
`/root`	Генерация самоподписанного сертификата УЦ.
`/rootKeySize`	Опциональный параметр. Размер закрытого ключа самоподписанного сертификата УЦ. По умолчанию генерируется закрытый ключ размером 4096 бит. Возможный диапазон – от 512 до 8192 бит.
`/sn <DNS-имя сервера>`	Генерация SSL-сертификата сайта агента на указанное DNS-имя сервера.
`/csn`	Генерация SSL-сертификата сайта агента на имя сервера, на котором запущена утилита Cm.Agent.Cert.Generator.
`/sslKeySize`	Опциональный параметр. Размер закрытого ключа SSL-сертификата сайта агента. По умолчанию генерируется закрытый ключ размером 2048 бит. Возможный диапазон – от 512 до 4096 бит.
`/pwd`	Опциональный параметр. Пароль SSL-сертификата сайта агента.
`/installToStore`	Опциональный параметр. Публикация SSL-сертификата сайта агента, выпущенного утилитой, в хранилище **Личных** сертификатов рабочей станции, на которой установлен сервер Indeed CM.

Параметры генерации SSL-сертификата с помощью самоподписанного сертификата УЦ

Параметр	Описание
`/rootKey`	Путь до файла самоподписанного сертификата УЦ.
`/ssl`	Генерация SSL-сертификата сайта агента.
`/sn <DNS-имя сервера>`	Генерация SSL-сертификата сайта агента на указанное DNS-имя сервера.
`/csn`	Генерация SSL-сертификата сайта агента на имя сервера, на котором запущена утилита Cm.Agent.Cert.Generator.
`/pwd`	Опциональный параметр. Пароль SSL-сертификата сайта агента.
`/sslKeySize`	Опциональный параметр. Размер закрытого ключа SSL-сертификата сайта агента. По умолчанию генерируется закрытый ключ размером 2048 бит. Возможный диапазон – от 512 до 4096 бит.

Выберите инструкцию в зависимости от операционной системы, где установлен сервер Indeed CM.

Windows

Чтобы создать сертификаты 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 следующие файлы:

   - *agent_root_ca.json* – самоподписанный сертификат УЦ с закрытым ключом в формате JSON
   - *agent_root_ca.cer* – самоподписанный сертификат УЦ

- *agent_root_ca.key* – закрытый ключ самоподписанного сертификата УЦ
- *agent_ssl_cert.cer* – SSL-сертификат сайта агента
- *agent_ssl_cert.key* – закрытый ключ SSL-сертификата сайта агента
- *agent_ssl_cert.pfx* – SSL-сертификат сайта агента с закрытым ключом в формате PFX

3. Поместите сертификат *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 выпустите SSL-сертификат сайта агента для каждого сервера с помощью сертификата УЦ. Используйте один и тот же сертификат УЦ на всех серверах.

Чтобы создать SSL-сертификат дополнительного сервера или обновить истекший сертификат:

1. Перенесите на сервер каталог с утилитой Cm.Agent.Cert.Generator и сертификат УЦ с закрытым ключом в формате JSON (*agent_root_ca.json*).

2. Выполните команду:

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

Пример

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

Linux

Чтобы создать сертификаты агента:

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

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

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

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

   В каталоге с утилитой появятся следующие файлы:

   - *agent_root_ca.json* – самоподписанный сертификат УЦ с закрытым ключом в формате JSON
   - *agent_root_ca.cer* – самоподписанный сертификат УЦ
   - *agent_root_ca.key* – закрытый ключ самоподписанного сертификата УЦ
   - *agent_ssl_cert.cer* – SSL-сертификат сайта агента
   - *agent_ssl_cert.key* – закрытый ключ SSL-сертификата сайта агента
   - *agent_ssl_cert.pfx* – SSL-сертификат сайта агента с закрытым ключом в формате PFX

3. Поместите сертификат *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 выпустите SSL-сертификат сайта агента для каждого сервера с помощью сертификата УЦ. Используйте один и тот же сертификат УЦ на всех серверах.

Чтобы создать SSL-сертификат дополнительного сервера или обновить истекший сертификат:

1. Перенесите на сервер каталог с утилитой Cm.Agent.Cert.Generator и сертификат УЦ с закрытым ключом в формате JSON (*agent_root_ca.json*).

2. Выполните команду:

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

   Пример

```
dotnet Cm.Agent.Cert.Generator.dll /rootKey ./agent_root_ca.json /ssl /sn
domain.loc1
```

SafeTech CA

Настройка автоматического выпуска сертификатов агента в УЦ

Внесите изменения в файлы конфигурации *appsettings.json* сервисов агента:

- agentregistrationapi
- agentserviceapi

1. Создайте шаблон сертификата в SafeTech CA.

Как создать шаблон сертификата в SafeTech CA

1. Войдите в веб-интерфейс SafeTech CA от имени сервисной учетной записи, выберите нужный УЦ и нажмите **Работать с этим УЦ**.
2. Перейдите в раздел **Настройки** → **Шаблоны** и нажмите **Добавить шаблон**
3. Укажите следующие параметры:
   - Наименование шаблона
   - Описание шаблона
   - Тип протокола: **ST_CA**
   - Максимальный срок действия сертификата в днях
   - Минимальная длина ключа: выберите любое значение из предложенных
4. Установите следующие параметры выпуска сертификата:
   - Сценарий выпуска: **Стандартный**
   - Настройка криптографии: включите опцию **Требуется настройка** и выберите алгоритм шифрования **RSA**
   - Алгоритмы подписи: **SHA256WITHRSA**
   - Длина ключа: выберите любое значение из предложенных
5. В разделе **Использование ключа** выберите **Подпись** и включите опцию **Использовать значения из шаблона**.
6. В разделе **Роли шаблона** задайте права на действия с шаблоном. Администратор по умолчанию обладает всеми правами. Чтобы настроить права для роли Оператора:
   1. Нажмите **Добавить**.
   2. В выпадающем списке выберите **Оператор**.
   3. Выдайте необходимые права.
7. В разделе **Атрибуты сертификата** в выпадающем списке выберите **Enhanced Key Usage** и нажмите **Добавить**. Поле **Значение атрибута** оставьте пустым.
8. В разделе **Расширения использования ключей (EKU)**:
   1. Нажмите **Добавить расширение**, выберите **Client Authentication** и нажмите **Подтвердить**.

2. Включите опцию **Использовать значения из шаблона**.

9. Нажмите **Создать**, затем нажмите **Сохранить на сервер**.

2. Откройте файл конфигурации *appsettings.json* сервиса регистрации агентов **agentregistrationapi**. Расположение файла:

   - Windows: *C:\inetpub\wwwroot\cm\agent\agentregistrationapi*
   - Linux: */opt/indeed/cm/agentregistrationapi*

3. В секции `agentCertificateSettings` настройте параметры выпуска сертификатов агента в УЦ.

▼ `agentCertificateSettings`

`checkCertificateRevocationStatus`	Проверка статуса отзыва сертификата агента в УЦ. Допустимые значения: • `true` – включить проверку. Если сертификат агента приостановлен или отозван, статус агента изменится на *Отозван*, и агент не будет выполнять задачи. • `false` – отключить проверку. Значение по умолчанию.
`certificateKeyLength`	Минимальная длина ключа сертификата агента. Значение по умолчанию – 2048 бит.
`caType`	Тип УЦ, в котором будут выпускаться сертификаты агента. Укажите значение `SafeTech`.

4. В секции `safeTechCaSettings` настройте параметры подключения к SafeTech CA. Подробнее в инструкции по настройке SafeTech CA

▼ `safeTechCaSettings`

`serviceUrl`	URL-адрес веб-службы CA Gateway. Например, `https://<имя сервера УЦ>:9443/ca-core/api/v1`.
`authServiceUrl`	URL-адрес веб-службы авторизации – адрес Realm (области) Keycloak, в которой находятся клиенты и пользователи (st-ca по умолчанию). Например, `https://<имя сервера УЦ>:8443/realms/st-ca`.
`clientId`	Идентификатор клиента — значение параметра `Client ID` в Keycloak. Например, `ca-gateway`. Убедитесь, что у клиента есть роль Администратора или Оператора УЦ.
`clientSecret`	Значение параметра `Client Secret` в Keycloak. Например, `vtG4VuWYbG6t4SxbIzsTCyxpMmqr4RPy`.
`userName`	Имя сервисной учетной записи.
`password`	Пароль сервисной учетной записи.
`certificateTemplate`	Название шаблона сертификата в УЦ, по которому будут выпускаться сертификаты для агентов.

5. Сохраните изменения в файле *appsettings.json* сервиса регистрации агентов **agentregistrationapi**.

6. Откройте файл конфигурации *appsettings.json* сервиса агентов для удаленного выполнения задач **agentserviceapi**. Расположение файла:

   - Windows: *C:\inetpub\wwwroot\cm\agent\agentserviceapi*
   - Linux: */opt/indeed/cm/agentserviceapi*

7. В секции `agentCertificateSettings` настройте параметры выпуска сертификатов агента в УЦ. Используйте те же параметры и значения, что и в файле конфигурации **agentregistrationapi** (шаг 3).

8. В секции `safeTechCaSettings` настройте параметры SafeTech CA. Используйте те же параметры и значения, что и в файле конфигурации **agentregistrationapi** (шаг 4).

9. Сохраните изменения в файле *appsettings.json* сервиса агентов для удаленного выполнения задач **agentserviceapi**.

При регистрации агента на клиентской рабочей станции сервер Indeed CM автоматически устанавливает два сертификата:

- Корневой сертификат УЦ – в доверенные корневые центры сертификации компьютера
- Сертификат агента – в личное хранилище службы CM Agent Service

В Консоли управления в разделе **Сводная информация** → Сервисные сертификаты доступна информация о корневом сертификате УЦ, который выдает сертификаты рабочим станциям с установленными агентами.

> ⓘ **ПРИМЕЧАНИЕ**
>
> Убедитесь, что корневой сертификат УЦ установлен на сервере Indeed CM.

Подготовка SSL-сертификата

В качестве SSL-сертификата можно использовать RSA-сертификат, выпущенный с любого доверенного УЦ на имя сервера Indeed CM.

Убедитесь, что сертификат соответствует следующим требованиям:

- **Субъект** (Subject) сертификата содержит атрибут **Общее имя** (Common Name) (FQDN сервера Indeed CM).
- **Дополнительное имя субъекта** (Subject Alternative Name) сертификата содержит атрибут **DNS-имя** (DNS Name) (FQDN сервера Indeed CM). Например, `server.domain.loc` или соответствующую запись с подстановочными знаками: `*.domain.loc` (Wildcard certificate).
- **Улучшенный ключ** (Enhanced Key Usage) сертификата содержит значение «Проверка подлинности сервера» (Server Authentication).

Настройка защищенного соединения с сайтом сервисов агента

Windows

1. Откройте 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**.

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

4. Нажмите **Изменить...** (Edit...).
5. В поле **SSL-сертификат** выберите SSL/TLS сертификат, выпущенный с любого доверенного УЦ на имя сервера Indeed CM, и нажмите **OK**.

Linux

Выберите инструкцию в зависимости от операционной системы, где установлен сервер Indeed CM.

Debian-based

1. Скопируйте SSL-сертификат сайта агента и закрытый ключ сертификата в соответствующие хранилища на сервере Indeed CM.

```
#Копировать сертификат в хранилище сертификатов
sudo cp ./agent_ssl_cert.cer /etc/ssl/certs/

#Копировать закрытый ключ в хранилище закрытых ключей
sudo cp ./agent_ssl_cert.key /etc/ssl/private/
```

2. Скопируйте сервисный сертификат агента в хранилище доверенных корневых сертификатов и конвертируйте его формат в CRT.

```
sudo cp ./agent_root_ca.cer /usr/local/share/ca-certificates/agent_root_ca.crt
```

3. Обновите хранилище доверенных корневых сертификатов.

```
sudo update-ca-certificates -f
```

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

RHEL-based

1. Скопируйте SSL-сертификат сайта агента и закрытый ключ сертификата в хранилище */etc/ssl/* на сервере Indeed CM.

```
sudo cp ./agent_ssl_cert.cer /etc/ssl/
sudo cp ./agent_ssl_cert.key /etc/ssl/
```

2. Скопируйте сервисный сертификат агента в хранилище доверенных корневых сертификатов.

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

3. Обновите хранилище доверенных корневых сертификатов.

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

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

Пример конфигурационного файла веб-сервера NGINX

```
server {
        listen              3003 ssl;
        server_name         server.domain.loc;

        ssl_certificate     "/etc/ssl/certs/agent_ssl_cert.cer";
        ssl_certificate_key "/etc/ssl/private/agent_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/agent_ssl_cert.cer
    SSLCertificateKeyFile /etc/apache2/ssl/agent_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 logs/error.log
    CustomLog logs/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. Убедитесь, что порт открыт для входящих подключений в брандмауэре.

Установка и настройка клиентских компонентов

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 управления устройствами

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.

Установка

Установите компонент Indeed CM Client Tools на рабочую станцию каждого пользователя, которому требуется разблокировка устройства с помощью Indeed CM.

1. В дистрибутиве Indeed CM перейдите в каталог *CM.Client*.
2. Запустите файл *Cm.Client.Tools-<номер версии>.ru-ru.msi*.
3. Следуйте указаниям мастера установки.

Режимы разблокировки устройств

Разблокировка устройств реализована в двух режимах: онлайн и офлайн.

Онлайн-разблокировка

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-разблокировка

В офлайн-режиме оператор Indeed CM разблокирует устройство по принципу аутентификации вида запрос-ответ (challenge-response authentication mechanism).

Если допустимое число попыток ввода PIN-кода исчерпано, устройство блокируется. На экране пользователя отображается сообщение о блокировке и уникальный 16-символьный код-запрос. Пользователю необходимо связаться с оператором Indeed CM и сообщить код.

Подробнее о разблокировке устройств

Настройка онлайн-разблокировки устройств

Настройте онлайн-разблокировку устройств на рабочих станциях пользователей одним из способов:

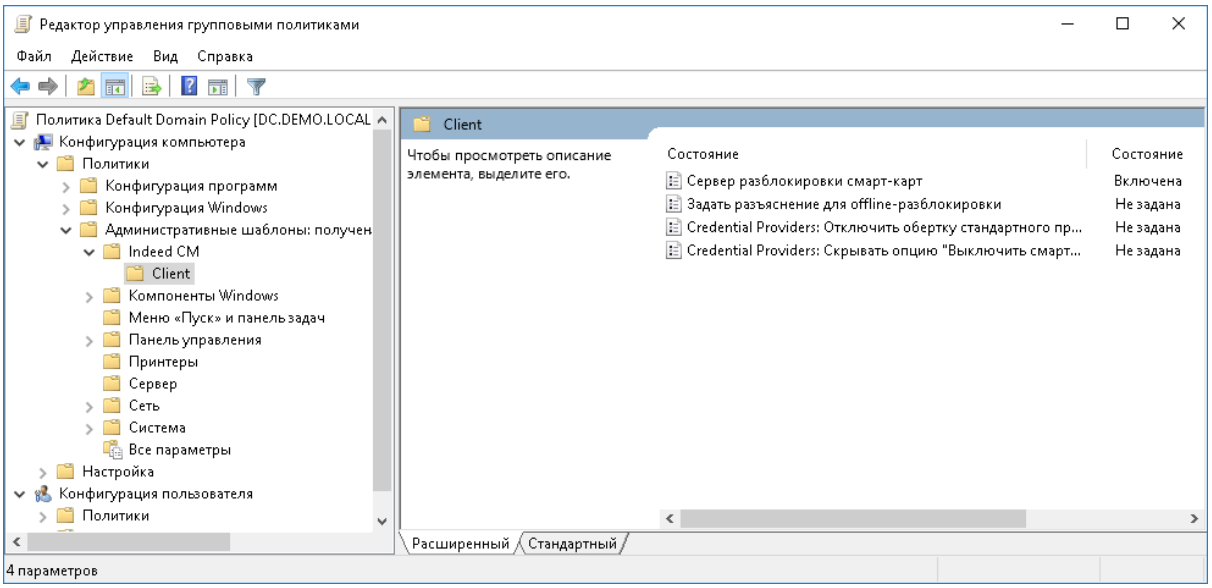
- Групповые политики — для рабочих станций в домене Windows
- Реестр Windows — для рабочих станций вне домена Windows

Групповые политики

Настройте онлайн-разблокировку устройств через групповую политику с административными шаблонами Indeed CM:

1. Добавьте административные шаблоны Indeed CM: скопируйте содержимое каталога *CM.Client\Misc* в центральное хранилище ADMX-файлов контроллера домена *C:\Windows\SYSVOL\domain\Policies\PolicyDefinitions*.
   Если ADMX-файлы хранятся локально, поместите шаблоны в каталог *C:\Windows\PolicyDefinitions*.
2. Откройте консоль **Управление групповой политикой** (Group Policy Management).
3. В дереве консоли создайте новый объект групповой политики или выберите существующий.
4. Нажмите правой кнопкой мыши на объект групповой политики и выберите **Изменить** (Edit). Откроется окно **Редактор управления групповыми политиками** (Group Policy Management Editor).
5. 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:
   1. В параметре **URL сервиса** (Service URL) укажите ссылку на компонент credprovapi, размещенный на сервере Indeed CM: `https://<FQDN сервера Indeed CM>/cm/credprovapi`.
   2. В параметре **Проверять сертификат сервера** (Verify server certificate) установите значение **Да**, чтобы проверять подлинность 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 Indeed CM.
8. Нажмите **Применить** (Apply).
9. Обновите политики одним из следующих способов:
    - Перезагрузите рабочую станцию
    - В терминале выполните команду `gpupdate /force`
10. (Опционально) Настройте дополнительные политики, определяющие работу сервиса разблокировки.

Дополнительные политики сервиса разблокировки

Политика	Параметры
Задать разъяснение для offline-разблокировки (Set explanations for offline unlocking)	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 отображается текст разъяснения, указанный в политике. Например, контактный телефон администратора Indeed CM.
Credential Providers: Отключить обертку стандартного провайдера смарт-карт (Credential Providers: Disable smart card standard provider wrapping)	Если политика выключена или не определена, пользователь может разблокировать смарт-карту в стандартном интерфейсе входа в ОС Windows по смарт-карте. Если политика включена, то отдельная опция для разблокировки смарт-карты отображается на экране входа в ОС. Настройка применяется, если стороннее ПО на рабочей станции не позволяет разблокировать смарт-карту через стандартный Credential Provider.
Credential Providers: Скрывать опцию "Выключить смарт-карту" (Credential Providers: Hide the "Disable the smart card" option)	Если политика выключена или не определена, пользователь может выключить смарт-карту в интерфейсе входа в ОС Windows. Если политика включена, то опция для выключения смарт-карты не отображается на экране входа в ОС.

Реестр Windows

Настройте онлайн-разблокировку устройств в реестре каждой клиентской рабочей станции:

1. Создайте файл реестра с расширением .reg со следующими параметрами:

   - `CredProvAPIURL` — адрес приложения credprovapi на сервере Indeed CM
   - `AdminDetails` — текст сообщения для пользователя
   - `DisableServerCertificateChecking` — проверка подлинности серверного сертификата Indeed CM:
     - `dword:00000000` — проверка включена (по умолчанию)
     - `dword:00000001` — проверка выключена
   - `DisableSuspendCP` — отображение опции **Выключение смарт-карты** в интерфейсе входа в ОС:
     - `dword:00000000` — опция отображается (по умолчанию)
     - `dword:00000001` — опция скрыта
   - `DisableWrapperCP` — способ разблокировки смарт-карты на экране входа в ОС Windows:
     - `dword:00000000` — через стандартный интерфейс входа по смарт-карте (стандартный Credential Provider, по умолчанию)
     - `dword:00000001` — через отдельный Credential Provider

   Пример файла реестра

   ```
   Windows Registry Editor Version 5.00

   [HKEY_LOCAL_MACHINE\SOFTWARE\Policies\CM\Client]
   "CredProvAPIURL"="https://server.domain.loc/cm/credprovapi"
   "AdminDetails"="Свяжитесь с администратором по внутреннему номеру 1607"
   "DisableServerCertificateChecking"=dword:00000000
   "DisableSuspendCP"=dword:00000001
   "DisableWrapperCP"=dword:00000001
   ```

2. Примените файл реестра на каждой клиентской рабочей станции.

3. Перезагрузите рабочие станции, чтобы применить изменения.

Indeed CM Middleware

Indeed CM Middleware — клиентский компонент, необходимый для работы с устройствами (USB-токенами и смарт-картами).

> **ПРИМЕЧАНИЕ**
>
> Для работы Indeed CM Middleware установите на рабочие станции пользователей драйверы и сервисные утилиты для используемых устройств и считывателей. Драйверы и утилиты не входят в дистрибутив Indeed CM.

Установка Middleware

Windows

1. В дистрибутиве Indeed CM перейдите в каталог *CM.Client*.
2. Запустите файл *Cm.<имя типа устройства>.Middleware-<номер версии>.ru-ru.msi*. Для разных типов устройств предусмотрены разные файлы Indeed CM Middleware.
3. Следуйте указаниям мастера установки.

Таблица соответствия производителей, моделей устройств и файлов Indeed CM 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 JaCarta-3 PKI/ГОСТ JaCarta-3 SE	*IndeedCM.JaCarta.Middleware-<номер версии>.ru-ru.msi*

Производитель	Модели устройств	Middleware
Компания «Актив»	Рутокен PKI 1800 Рутокен Lite 1000 Рутокен Lite 1010 Рутокен S Рутокен ЭЦП Рутокен ЭЦП 2.0 2000 Рутокен ЭЦП 2.0 2100 Рутокен ЭЦП 2.0 3000 Рутокен ЭЦП 2.0 Flash 4500 Рутокен 2151 Рутокен ЭЦП 3.0 3100 Рутокен ЭЦП 3.0 NFC 3100 Рутокен ЭЦП 3.0 3100 SAM Рутокен ЭЦП 3.0 3120 Рутокен ЭЦП 3.0 3150 Рутокен ЭЦП 3.0 3220 Рутокен ЭЦП 3.0 3250 БИО	*IndeedCM.Rutoken.Middleware-<номер версии>.ru-ru.msi*
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*

Производитель	Модели устройств	Middleware
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*
ISBC	ESMART Token USB 64K ESMART Token USB 192K ESMART Token USB ГОСТ ESMART Token CARD 64K ESMART Token CARD 192K ESMART Token CARD ГОСТ	*IndeedCM.ESMART.Middleware-<номер версии>.ru-ru.msi*

Производитель	Модели устройств	Middleware
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*
	TPM Virtual Smart Card (Microsoft VSC)	*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*

Производитель	Модели устройств	Middleware
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 FIPS IDPrime MD 830B FIPS IDPrime MD 840B IDPrime 930 IDPrime 930nc IDPrime 940 IDPrime 940B IDPrime MD 3810 IDPrime MD 3811 IDPrime 3930 IDPrime 3940 IDPrime 3940 FIDO SafeNet eToken 5300 SafeNet eToken Fusion SafeNet eToken Fusion CC SafeNet eToken 5110 CC (940)	*IndeedCM.IDPrime.Middleware-<номер версии>.ru-ru.msi*

Производитель	Модели устройств	Middleware
Yubico	YubiKey 5 Series	*IndeedCM.YubiKey.Middleware-<номер версии>.ru-ru.msi*

Linux

В Indeed CM для ОС Linux поддерживаются устройства Рутокен, JaCarta, ESMART и SafeNet eToken. Для всех типов устройств предусмотрен единый Indeed CM Middleware.

Таблица моделей устройств, поддерживаемых Indeed CM в 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 JaCarta-3 PKI/ГОСТ JaCarta-3 SE
Компания «Актив»	Рутокен PKI 1800 Рутокен ЭЦП Рутокен ЭЦП 2.0 2000 Рутокен ЭЦП 2.0 2100 Рутокен ЭЦП 2.0 3000 Рутокен ЭЦП 2.0 Flash 4500 Рутокен 2151 Рутокен ЭЦП 3.0 3100 Рутокен ЭЦП 3.0 NFC 3100 Рутокен ЭЦП 3.0 3100 SAM Рутокен ЭЦП 3.0 3120 Рутокен ЭЦП 3.0 3150 Рутокен ЭЦП 3.0 3220 Рутокен ЭЦП 3.0 3250 БИО
ISBC	ESMART Token USB 64K ESMART Token USB 192K ESMART Token USB ГОСТ ESMART Token CARD 64K ESMART Token CARD 192K ESMART Token CARD ГОСТ

Производитель	Модели устройств
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

Чтобы установить Indeed CM Middleware:

1. Выберите дистрибутив Indeed CM Middleware в зависимости от версии OpenSSL в операционной системе:

   - OpenSSL 3.x — *IndeedCM.Client-v<номер версии>-linux*
   - OpenSSL 1.1.1 — *IndeedCM.Client-v<номер версии>-linux-openssl-1.1*

   Чтобы проверить версию OpenSSL, в терминале выполните команду `openssl version`.

2. Выполните команду установки:

   Debian-based

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

   RHEL-based

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

Установка браузерного расширения

Для доступа к веб-приложениям Indeed CM установите расширение Indeed CM Middleware в браузеры на рабочих станциях администраторов, операторов и пользователей.

Google Chrome, Chromium, Яндекс.Браузер

Расширение можно установить следующими способами:

- Через интернет-магазин Chrome
- Через файл CRX из каталога *CM.Client*

Чтобы установить расширение через файл CRX:

1. Запустите браузер и откройте страницу со списком расширений:
   - `chrome://extensions` для Google Chrome и Chromium
   - `browser://extensions` для Яндекс.Браузера
2. Откройте каталог *CM.Client-v<номер версии>\cm.middleware.chrome.extension*.
3. Перетащите файл CRX на страницу браузера со списком расширений.
4. Во всплывающем окне нажмите **Установить расширение**.

Mozilla Firefox

1. Запустите браузер и откройте страницу со списком расширений `about:addons`.
2. Нажмите  и выберите **Установить дополнение из файла…**.
3. Выберите файл *cm.middleware-1.0.xpi* из каталога *CM.Client-v<номер версии>\cm.middleware.chrome.extension* и нажмите **Открыть**.
4. Во всплывающем окне нажмите **Добавить**.

Работа с устройствами в ОС Astra Linux SE в режиме ЗПС

Indeed CM поддерживает работу с устройствами в ОС Astra Linux SE в режиме замкнутой программной среды (ЗПС). Для поддержки режима ЗПС исполняемые файлы компонента Indeed CM Middleware подписаны встроенной подписью.

Предварительные настройки

Для работы с устройствами в режиме ЗПС установите следующие компоненты:

- Indeed CM Middleware для ОС Linux
- Подписанные версии драйверов и сервисных утилит устройств и считывателей

Проверка подписи

Чтобы подпись прошла проверку для работы в режиме ЗПС, установите открытый ключ Indeed CM Middleware:

1. Установите пакет *cm.digsig.key_1.0.0-1_all.deb*.

   ```
   sudo dpkg -i cm.digsig.key_1.0.0-1_all.deb
   ```

   После установки пакета ключ находится по пути */etc/digsig/keys*.

2. Чтобы ключ стал доверенным, перезагрузите операционную систему.

Поддержка устройств Registry

Чтобы пользователи могли выпускать устройства Registry, настройте поддержку устройств Registry одним из способов:

- Групповые политики — для рабочих станций в домене Windows
- Реестр Windows — для рабочих станций вне домена Windows

Групповые политики

Настройте возможность выпуска устройств Registry через групповую политику с административными шаблонами Indeed CM:

1. Добавьте административные шаблоны Indeed CM: скопируйте содержимое каталога *CM.Client\Misc* в центральное хранилище ADMX-файлов контроллера домена *C:\Windows\SYSVOL\domain\Policies\PolicyDefinitions*.
   Если ADMX-файлы хранятся локально, поместите шаблоны в каталог *C:\Windows\PolicyDefinitions*.

2. Откройте консоль **Управление групповой политикой** (Group Policy Management).

3. В дереве консоли создайте новый объект групповой политики или выберите существующий.

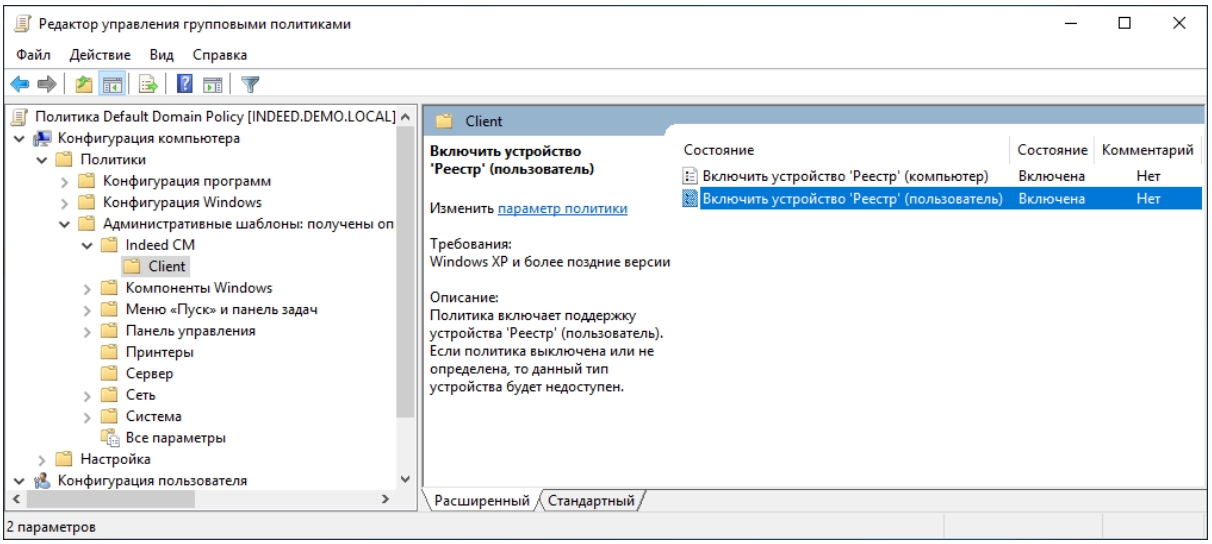
4. Нажмите правой кнопкой мыши на объект групповой политики и выберите **Изменить** (Edit). Откроется окно **Редактор управления групповыми политиками** (Group Policy Management Editor).

5. 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)), чтобы выпускать сертификаты в локальное хранилище рабочей станции.
   - **Включить устройство 'Реестр' (пользователь)** (Enable 'Registry' card (User)), чтобы выпускать сертификаты в хранилище пользователя.



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

8. Нажмите **Применить** (Apply).

9. Обновите политики одним из следующих способов:

   - Перезагрузите рабочую станцию
   - В терминале выполните команду `gpupdate /force`

Реестр Windows

Настройте возможность выпуска устройств Registry в реестре каждой клиентской рабочей станции:

1. Создайте файл реестра с расширением .reg со следующими параметрами:

   - `MachineRegistryCardEnabled` — установите значение `dword:00000001`, чтобы выпускать сертификаты в локальное хранилище рабочей станции.

- `UserRegistryCardEnabled` — установите значение `dword:00000001`, чтобы выпускать сертификаты в хранилище пользователя.

Пример файла реестра

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\CM\Client]
"MachineRegistryCardEnabled"=dword:00000001
"UserRegistryCardEnabled"=dword:00000001
```

2. Примените файл реестра на каждой клиентской рабочей станции.

3. Перезагрузите рабочие станции, чтобы применить изменения.

Indeed CM Agent

Indeed CM Agent (клиентский агент Indeed CM) позволяет удаленно управлять устройствами пользователей.

Установка

Установите Indeed CM Agent вместе с Indeed CM Middleware на рабочие станции пользователей Indeed CM:

1. В дистрибутиве Indeed CM перейдите в каталог *CM.Client*.
2. Запустите файл *Cm.Agent-<номер версии>.ru-ru.msi*.
3. Следуйте указаниям мастера установки. Агент запустится автоматически.

Настройка подключения к серверу Indeed CM

Настройте подключение агентов к серверу Indeed CM одним из способов:

- Групповые политики
- Реестр Windows

Групповые политики

Настройте подключение агентов к серверу Indeed CM через групповую политику с административными шаблонами Indeed CM:

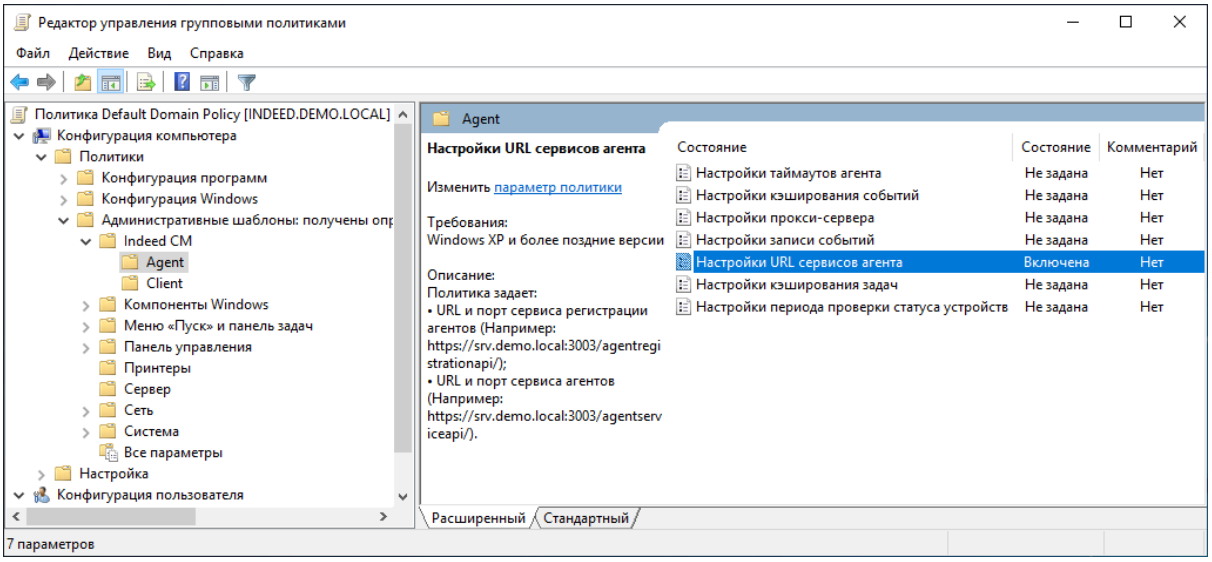
1. Добавьте административные шаблоны Indeed CM: скопируйте содержимое каталога *CM.Client\Misc* в центральное хранилище ADMX-файлов контроллера домена *C:\Windows\SYSVOL\domain\Policies\PolicyDefinitions*.
   Если ADMX-файлы хранятся локально, поместите шаблоны в каталог *C:\Windows\PolicyDefinitions*.
2. Откройте консоль **Управление групповой политикой** (Group Policy Management).
3. В дереве консоли создайте новый объект групповой политики или выберите существующий.
4. Нажмите правой кнопкой мыши на объект групповой политики и выберите **Изменить** (Edit). Откроется окно **Редактор управления групповыми политиками**

(Group Policy Management Editor).

5. Выберите **Конфигурация компьютера** (Computer Configuration) → **Политики** (Policies) → **Административные шаблоны** (Administrative Templates) → **CM** → **Agent**.

6. Включите политику **Настройка URL сервисов агентов** (Agent's URL Settings) и укажите ее значения:

    1. В параметре **URL сервиса регистрации агентов** (Agents registration service URL) укажите веб-адрес и порт подключения к приложению agentregistrationapi на сервере Indeed CM.
    Например, `https://server.domain.loc:3003/agentregistrationapi/`.
    2. В параметре **URL сервиса агентов** (Agents service URL) укажите веб-адрес и порт сервиса agentserviceapi.
    Например, `https://server.domain.loc:3003/agentserviceapi/`.



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

8. Нажмите **Применить** (Apply).

9. Обновите политики одним из следующих способов:

    - Перезагрузите рабочую станцию
    - В терминале выполните команду `gpupdate /force`

10. (Опционально) Настройте 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 или PIN-кода администратора • Попытки ввода неверного PIN-кода пользователя или PIN-кода администратора

Реестр Windows

Настройте подключение агентов к серверу Indeed CM в реестре каждой клиентской рабочей станции:

1. Создайте файл реестра с расширением .reg со следующими параметрами подключения:
   - `AgentRegistrationServiceUrl` — адрес и порт приложения agentregistrationapi
   - `AgentServiceUrl` — адрес и порт приложения agentserviceapi
2. Если на рабочих станциях с клиентским агентом используется прокси-сервер, дополнительно задайте параметры `ProxyEnable` и `ProxyServer`:
   - `ProxyEnable` — установите значение `dword:00000001`, чтобы использовать прокси-сервер для подключения к серверу Indeed CM.

- `ProxyServer` — оставьте пустым (`""`), чтобы использовать системные настройки, или укажите URL прокси-сервера.

Пример файла реестра

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\CM\Agent]
"AgentRegistrationServiceUrl"="https://server.domain.loc:3003/agentregistrationapi/"
"AgentServiceUrl"="https://server.domain.loc:3003/agentserviceapi/"
"ProxyEnable"=dword:00000001
"ProxyServer"="https://192.168.10.10:443"
```

> **ПРИМЕЧАНИЕ**
> Для 32-разрядных ОС параметры настраиваются в ветке *[HKEY_LOCAL_MACHINE\SOFTWARE\CM\Agent]*.

3. Примените файл реестра на каждой клиентской рабочей станции.
4. Чтобы применить изменения, перезагрузите рабочие станции или перезапустите службу CM Agent Service.

Руководство администратора

Начало работы

Вход в Консоль управления Indeed CM

Конфигурация

Настройка параметров Indeed Certificate Manager

Консоль управления

Управление пользователями, устройствами и сертификатами

Начало работы

Администраторы и операторы могут управлять Indeed Certificate Manager в веб-приложении Консоль управления (Management Console).

Вход

Консоль управления доступна по ссылке `https://<FQDN сервера Indeed CM>/cm/mc`.

Доступ к Консоли управления определяется настройками аутентификации, заданными при установке сервера Indeed CM.

Настройка Консоли управления

1. Запустите Консоль управления от имени учетной записи, которая указана в Мастере настройки в разделе **Контроль доступа** → **Администратор ролей**.

   > ⚠ **ПРЕДУПРЕЖДЕНИЕ**
   >
   > При первом входе в Консоль управления доступен только раздел **Конфигурация** → **Роли** и только для администратора ролей.

2. В разделе **Конфигурация** → Роли добавьте текущего пользователя в роль **Администратор**. Настройте роли и привилегии администраторов и операторов.

3. Выполните настройку в следующих разделах:

   - Лицензии — загрузите файл лицензии.
   - Типы устройств — загрузите файлы типов устройств.
   - Политики — настройте политики использования устройств.
   - Назначения политик — назначьте политики на пользователей.

Конфигурация

Политики

Создание и редактирование политик использования устройств

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

Настройка полномочий администраторов и операторов

Теги

Настройка тегов для гибкого учета устройств в организации

Шаблоны печати

Настройка шаблонов документов

СКЗИ

Управление средствами криптографической защиты информации

Уведомления

Настройки почтовых уведомлений об изменениях в настройках Indeed CM

Журналы учета

Настройка справочников и шаблонов журналов

Политики

Политики определяют разрешенные и запрещенные действия пользователей при использовании устройств.

Создание

1. В Консоли управления перейдите в раздел **Конфигурация** → **Политики**.
2. Нажмите **Создать политику**.
3. Укажите отображаемое имя политики в поле **Имя** или скопируйте параметры ранее созданной политики в поле **Копировать из**.
4. Нажмите **Создать**.

После создания политики откроются ее настройки. В разделе **Общие** отображается имя политики, которое можно изменить.

Удаление

1. В Консоли управления перейдите в раздел **Конфигурация** → **Политики**.
2. Выберите политику в списке и нажмите ✖ .
3. Нажмите **Удалить**.

Политику можно удалить только в том случае, если в Indeed CM нет ни одного устройства, выпущенного с применением этой политики.

Назначения политик

Настройте назначения, чтобы централизованно применять политики к объектам или пользователям.

Политики распространяются на следующие объекты:

- **LDAP-каталог пользователей**: Домен (Domain), Контейнер (Container), Подразделение (Organizational Unit)
- **КриптоПро УЦ 2.0**: часть существующей в Центре Регистрации структуры контейнеров (папок) или весь Центр Регистрации (ЦР)
- **Организационная структура Indeed CM**, в узлы которой могут входить:

- Домен (Domain), Контейнер (Container), Подразделение (Organization Unit), пользователи или группы каталога пользователей
- Часть существующей в Центре Регистрации структуры контейнеров (папок) или весь ЦР, пользователи или группы безопасности ЦР
  Подробнее об организационной структуре

> **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 LDAP-каталог пользователей или каталог Центра Регистрации КриптоПро УЦ 2.0 имеют приоритет над политиками, действующими на Организационную структуру Indeed CM.

Чтобы назначить политику на объект:

1. Перейдите в раздел **Конфигурация** → **Назначения политик**.
2. Нажмите **Создать назначение политики**.
3. В выпадающем списке **Политика** выберите нужную политику.
4. Определите следующие параметры:
   - **Контейнер** – область действия политики. Контейнером может быть подразделение каталога пользователей, 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 каталога.
   - **Приоритет** – значение, которое определяет, какая из политик действует на пользователя, если пользователь попадает в область действия нескольких политик одновременно. Например, когда пользователь состоит в двух группах, расположенных в одном Подразделении (Organizational Unit).
   - **Роли** – локальные роли, которым выдаются права на управление политикой.
5. Нажмите **Создать**

Назначение политики можно изменить  или удалить  .

Настройки политики

Настройки PKI

Настройки входа в систему и подключение удостоверяющих центров

Indeed Access Manager

Настройка интеграции с Indeed AM

Secret Net Studio

Настройка интеграции с Secret Net Studio

Рутокен Логон

Настройка интеграции с Рутокен Логон

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

В разделе **Настройки PKI** вы можете определить параметры входа пользователей в операционную систему. Выберите:

- **Импортировать сертификаты УЦ**

  При выпуске на устройство записывается корневой сертификат или цепочка сертификатов удостоверяющего центра (УЦ). Такие сертификаты не удаляются с устройства, когда оно изымается из Indeed CM.

  > **ПРИМЕЧАНИЕ**
  > Убедитесь, что устройство поддерживает запись корневого сертификата или цепочки сертификатов.

- **Требовать логон по смарт-карте**

  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).

Предварительные настройки для работы опции Требовать логон по смарт-карте

- Сервисная учетная запись для работы с каталогом пользователей должна обладать правами на **Запись:userAccountControl** (Write userAccountControl) в Active Directory. Подробнее о настройке 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.

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

Параметры работы с Microsoft CA

Aladdin Enterprise CA

Параметры работы с Aladdin Enterprise CA

SafeTech CA

Параметры работы с SafeTech CA

Dogtag CA

Параметры работы с Dogtag CA

КриптоПро УЦ 2.0

Параметры работы с КриптоПро УЦ 2.0

КриптоПро DSS 2.0

Параметры работы с КриптоПро DSS 2.0

Валидата УЦ

Параметры работы с Валидата УЦ

Общие сертификаты

Настройка общих сертификатов

Microsoft CA

Настройте подключение к Microsoft CA и создайте шаблоны сертификатов, которые будут выпускаться в этом УЦ.

Предварительные настройки

Чтобы разрешить доступ к разделу **Microsoft CA**:

1. Запустите Мастер настройки.
2. Перейдите в раздел **Удостоверяющие центры**.
3. Включите интеграцию с Microsoft Enterprise CA.

Добавить УЦ

Выберите инструкцию в зависимости от ОС, где установлен сервер Indeed CM.

Windows

1. Нажмите **Добавить УЦ**.
2. В поле **Адрес сервера** укажите адрес УЦ, если он не определился автоматически.
3. Укажите учетные данные пользователя с сертификатом **Агент регистрации** (Enrollment Agent): логин в формате *DOMAIN\Username* и пароль.
4. Нажмите **Добавить**.

> ⚠ **АГЕНТ РЕГИСТРАЦИИ**
> Для работы Indeed CM с УЦ требуется пользователь с сертификатом **Агент регистрации** (Enrollment Agent). От его имени Indeed CM отправляет запросы на выпуск сертификатов пользователей в УЦ. Учетные данные агента регистрации можно изменить при редактировании настроек УЦ.

Добавить УЦ, расположенный вне домена пользователей Indeed CM

1. Нажмите **Добавить УЦ**.
2. В поле **Адрес** укажите:

- URL-адрес приложения Indeed CM MSCA Proxy — если УЦ находится в другом лесу доменов или вне домена с пользователями Indeed CM.
- Имя УЦ — если Indeed CM и УЦ находятся в одном лесу доменов.

3. Укажите учетные данные пользователя с сертификатом **Агент регистрации** (Enrollment Agent) для внедоменного УЦ: логин в формате *DOMAIN\Username* и пароль.

4. Включите опцию **Выпускать сертификаты для пользователей из внешнего сопоставленного каталога**.

5. В поле **Путь (LDAP)** укажите путь к каталогу пользователей внешнего домена.

   Пример работы с каталогом пользователей внешнего домена

   Indeed CM установлен в домене domain.loc и использует УЦ в domain.loc для выпуска сертификатов. Вы можете подключить УЦ из другого домена — например, external.com. При добавлении УЦ укажите путь к каталогу пользователей в external.com. Убедитесь, что выполнены следующие условия:

   - У пользователей есть учетные записи в обоих доменах.
   - Атрибут соответствия совпадает в обоих каталогах (например, адрес электронной почты в domain.loc и external.com).

   УЦ из external.com будет выпускать сертификаты на учетные записи пользователей в external.com. На одно устройство можно записать сертификаты от УЦ из обоих доменов.

6. В поле **Имя пользователя** укажите логин в формате *DOMAIN\Username*. Учетная запись должна иметь права на чтение свойств пользователей во внешнем домене. Можно использовать учетную запись агента регистрации, указанную на шаге 3.

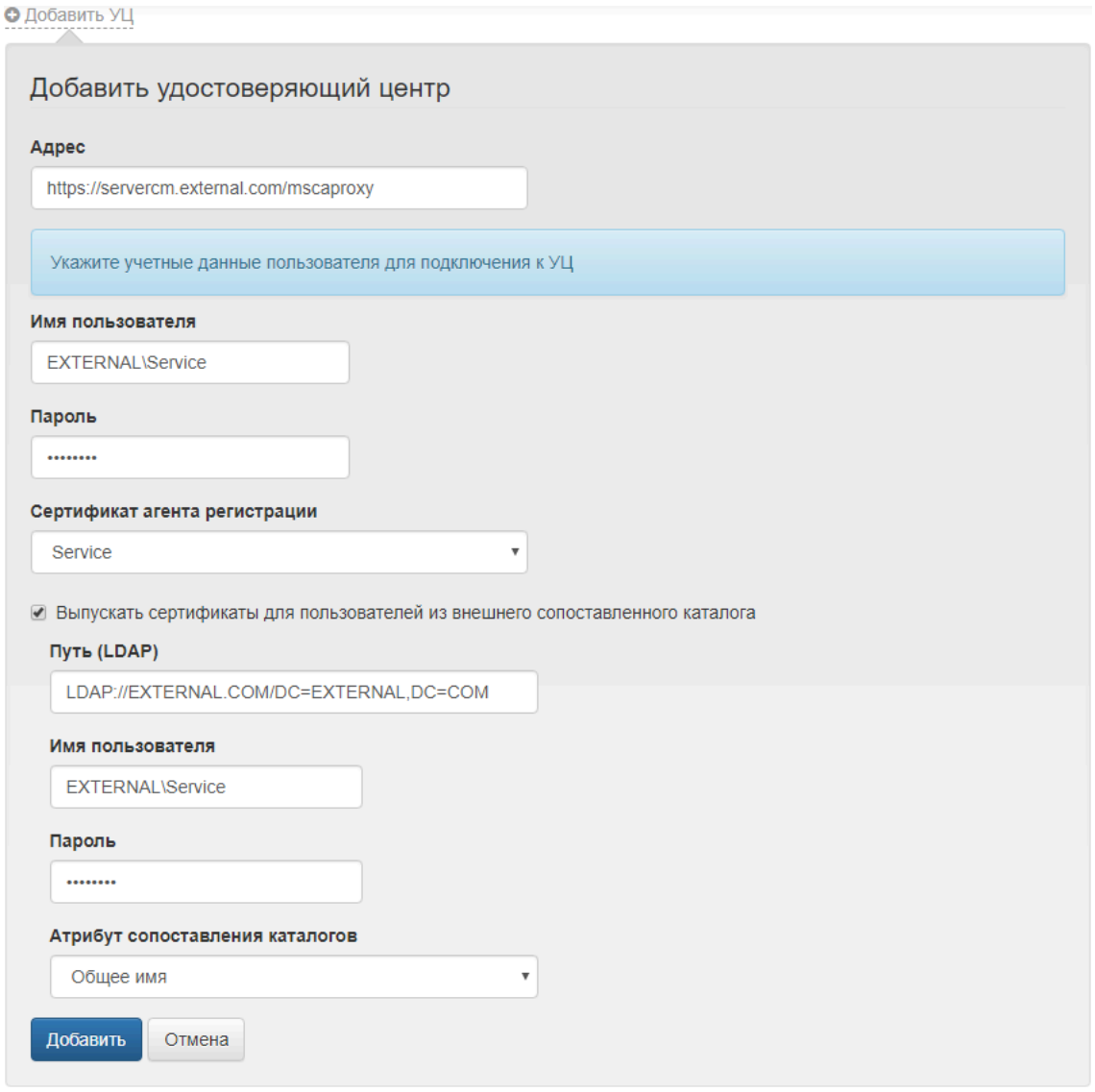
   ПОДСКАЗКА

   Чтобы настроить разрешение на чтение только необходимого набора свойств, перейдите в Active Directory и настройте свойства в списке **Разрешения** (Permissions) указанной учетной записи.

7. В поле **Атрибут сопоставления каталогов** укажите атрибут, по которому Indeed CM определяет уникальность пользователя, для которого созданы учетные записи в

каждом домене. Можно выбрать один из атрибутов – Общее имя, E-mail или Логин (sAMAccountName).

Пример настроек для внешнего Microsoft CA с опцией выпуска сертификатов для пользователей сопоставленного каталога



Linux

1. Нажмите **Добавить УЦ**.
2. В поле **Адрес** укажите URL-адрес приложения Indeed CM MS CA Proxy.
3. В поле **Клиентский сертификат** выберите сертификат клиентской аутентификации для подключения к Indeed CM MS CA Proxy.
4. Нажмите **Добавить**.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Сертификат клиентской аутентификации необходим для работы Indeed CM с Microsoft CA для инсталляций на ОС Linux.
>
> Как получить сертификат

Добавить УЦ, расположенный вне 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 работы с каталогом пользователей внешнего домена

   Indeed CM установлен в домене domain.loc и использует УЦ в domain.loc для выпуска сертификатов. Вы можете подключить УЦ из другого домена — например, external.com. При добавлении УЦ укажите путь к каталогу пользователей в external.com. Убедитесь, что выполнены следующие условия:

   - У пользователей есть учетные записи в обоих доменах.
   - Атрибут соответствия совпадает в обоих каталогах (например, адрес электронной почты в domain.loc и external.com).

   УЦ из external.com будет выпускать сертификаты на учетные записи пользователей в external.com. На одно устройство можно записать сертификаты от УЦ из обоих доменов.
3. В поле **Имя пользователя** укажите логин учетной записи в формате *DOMAIN\Username*. Учетная запись должна иметь права на чтение свойств пользователей во внешнем домене. Можно использовать учетную запись агента регистрации, указанную на шаге 3.

   > 💡 **ПОДСКАЗКА**
   >
   > Чтобы настроить разрешение на чтение только необходимого набора свойств, перейдите в Active Directory и настройте свойства в списке **Разрешения** (Permissions) указанной учетной записи.

4. В поле **Атрибут сопоставления каталогов** укажите атрибут (Общее имя, E-mail или Логин (sAMAccountName)), по которому Indeed CM будет определять уникальность пользователя, для которого созданы учетные записи в каждом домене.

Создать шаблоны сертификатов

Перед началом работы убедитесь, что шаблоны сертификатов настроены и добавлены в Microsoft CA.
Как настроить и добавить шаблоны сертификатов в Microsoft CA

Чтобы настроить шаблон сертификата:

1. Перейдите в раздел **Шаблоны**.
2. Нажмите **Создать шаблон сертификата**.
3. Заполните параметры и нажмите **Создать**.

Параметр	Описание
Имя	Имя шаблона сертификата
УЦ	Имя удостоверяющего центра
Шаблон сертификата УЦ	Загружается из удостоверяющего центра
Префикс имени ключа	Произвольная строка, которая добавляется в начало имени контейнера, содержащего ключевую пару. Если префикс не указан, имя контейнера формируется случайным образом. Имя контейнера с префиксом отображается в Indeed CM (имя контейнера в разделе СКЗИ) и в стороннем ПО для работы с контейнерами закрытого ключа (КриптоПро CSP, клиенты устройств). Некоторые устройства могут не поддерживать отображение имени контейнера с префиксом.

Параметр	Описание
Включить в имя субъекта	Выберите атрибуты для формирования имени субъекта (Subject) сертификата. **Список атрибутов** • Полное различающееся имя (значение по умолчанию) • Общее имя • Имя • Фамилия • Инициалы • E-mail • Должность • Подразделение • Организация • Адрес • Город • Область • Страна **ДЛЯ КАТАЛОГОВ ПОЛЬЗОВАТЕЛЕЙ ALD PRO И FREEIPA** Выберите атрибуты **Общее имя**, **Имя**, **Фамилия** для корректного формирования имени субъекта (Subject) сертификата.

Параметр	Описание
Включить в альтернативное имя субъекта	Выберите атрибуты для формирования альтернативного имени субъекта (Subject Alternative Name) сертификата. **Список атрибутов** • E-mail • Дополнительные e-mail адреса • UPN-имя пользователя Атрибут пользователя Active Directory, из которого вычитываются дополнительные e-mail адреса, указывается в Мастере настройки в разделе. Атрибут по умолчанию: proxyAddresses.
Защищать ключ биометрией, если поддерживается	Опция поддерживается только для устройств Рутокен ЭЦП 3.0 3250 БИО (Рутокен БИО). При выпуске сертификата контейнер закрытого ключа защищается биометрическими данными пользователя (отпечатками пальцев), хранящимися на устройстве. Для доступа к ключу необходимо ввести PIN-код пользователя и пройти биометрическую аутентификацию. Изменить значение опции при редактировании шаблона нельзя. Подробнее о работе с устройствами Рутокен БИО
Создавать резервную копию ключа	Когда на устройстве генерируется ключевая пара, ее резервная копия сохраняется на сервере Indeed CM. Копию ключевой пары можно сохранить только один раз. Если опция выключена, ключевая пара генерируется сразу на устройстве.
Записывать копию ключа при временной замене устройства	Копии сертификатов и закрытых ключей записываются на устройство при временной замене.
Использовать ключи повторно	При обновлении сертификатов, записанных на устройство, существующий ключ шифрования используется повторно.

Параметр	Описание
Импортировать сертификат, если существует	Indeed CM использует сертификат с устройства вместо выпуска нового сертификата (для указанного пользователя, УЦ и шаблона). Если устройство инициализируется перед выпуском, сертификат удаляется.
Не удалять сертификат при обновлении/очистке устройства	При обновлении или очистке устройства истекающий/истекший сертификат не удаляется с устройства и не отзывается в УЦ. В процессе обновления запрашивается новый сертификат с новым закрытым ключом и записывается на устройство. Если включена опция **Использовать ключи повторно**, то при обновлении устройства истекающий/истекший сертификат удаляется с устройства. На устройство записывается новый сертификат со старым закрытым ключом. Истекающий/истекший сертификат удаляется, если устройство изъято с инициализацией.
Отзывать сертификат при отзыве или выключении устройства	Сертификаты пользователя отзываются при выключении или отзыве устройства.
Устанавливать сертификат в локальное хранилище	При выпуске и обновлении устройства через Сервис самообслуживания записанные на него сертификаты добавляются в локальное хранилище пользователя на рабочей станции.
Публиковать сертификат в файловое хранилище	Выпущенный сертификат публикуется в сетевом хранилище. При отзыве устройства сертификаты из хранилища не удаляются. Опция доступна, если в Мастере настройки в разделе **Общие функции** включена опция **Публикация сертификатов в файловое хранилище**.
Публиковать список отозванных сертификатов	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.

Параметр	Описание
Автоматически одобрять запрос на сертификат	Запрос на сертификат одобряется автоматически. Если опция выключена, для завершения выпуска необходимо дождаться, когда УЦ одобрит запрос.
Автоматически одобрять подписанный запрос на обновление сертификата	Запрос на обновление сертификата одобряется автоматически. Если опция выключена, для обновления сертификата необходимо дождаться, когда УЦ одобрит запрос.
Требовать подписанный документ сертификата перед продолжением выпуска/обновления устройства	Сертификат записывается 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 требуется обновить сертификат. **Список атрибутов** • Общее имя • 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.

Параметр	Описание
Шаблоны печати запроса на сертификат, сертификата, запроса на отзыв сертификата	Загрузите шаблоны документов сертификата в разделе **Конфигурация** → **Шаблоны печати**. Если шаблонов нет, используются стандартные шаблоны печати.
Использовать по умолчанию	Сертификат используется по умолчанию для входа в стороннее ПО.
Необязательный сертификат	При выпуске и обновлении устройства появится возможность выбрать, какие сертификаты из списка необязательных, записать на устройство. Если опция выключена, сертификат записывается на устройство по умолчанию.

Aladdin Enterprise CA

Настройте подключение к Aladdin Enterprise CA (Aladdin eCA) и настройте шаблоны сертификатов, которые будут выпускаться в этом УЦ.

Предварительные настройки

Чтобы разрешить доступ к разделу **Aladdin Enterprise CA**:

1. Запустите Мастер настройки.
2. Перейдите в раздел **Удостоверяющие центры**.
3. Включите интеграцию с Aladdin Enterprise CA.

Добавить УЦ

1. Нажмите **Добавить УЦ**.
2. В поле **Адрес сервера** введите URL-адрес сервера Aladdin eCA. Например, `https://<имя сервера УЦ>`.
3. В поле **Клиентский сертификат** выберите сертификат клиентской аутентификации для подключения к УЦ.
4. Нажмите **Добавить**.

Создать шаблоны сертификатов

Перед началом работы убедитесь, что шаблоны сертификатов настроены в Aladdin eCA.
Как настроить шаблоны сертификатов в Aladdin eCA

Чтобы создать шаблон сертификата:

1. Перейдите в раздел **Шаблоны**.
2. Нажмите **Создать шаблон сертификата**.
3. Заполните параметры и нажмите **Создать**.

Параметр	Описание
Имя	Имя шаблона сертификата

Параметр	Описание
УЦ	Имя удостоверяющего центра
Шаблон сертификата Aladdin eCA	Шаблон сертификата, автоматически загруженный из Aladdin eCA
Префикс имени ключа	Произвольная строка, которая добавляется в начало имени контейнера, содержащего ключевую пару. Если префикс не указан, имя контейнера формируется случайным образом. Имя контейнера с префиксом отображается в Indeed CM (имя контейнера в разделе СКЗИ) и в стороннем ПО для работы с контейнерами закрытого ключа (КриптоПро CSP, клиенты устройств). Некоторые устройства могут не поддерживать отображение имени контейнера с префиксом.
Использовать аппаратную криптографию, если поддерживается	Опция отображается, если добавленный УЦ является ГОСТ-экземпляром Aladdin eCA. Изменить значение опции при редактировании шаблона нельзя. При выпуске сертификата ключевая пара создается с использованием криптографических алгоритмов, поддерживаемых устройством. Если устройство не поддерживает аппаратную криптографию, то используется КриптоПро CSP, установленный на рабочей станции, к которой подключено устройство.

Параметр	Описание
Защищать ключ биометрией, если поддерживается	Опция поддерживается только для устройств Рутокен ЭЦП 3.0 3250 БИО (Рутокен БИО). При выпуске сертификата контейнер закрытого ключа защищается биометрическими данными пользователя (отпечатками пальцев), хранящимися на устройстве. Для доступа к ключу необходимо ввести PIN-код пользователя и пройти биометрическую аутентификацию. Изменить значение опции при редактировании шаблона нельзя. Подробнее о работе с устройствами Рутокен БИО
Создавать резервную копию ключа	Когда на устройстве генерируется ключевая пара, ее резервная копия сохраняется на сервере Indeed CM. Копию ключевой пары можно сохранить только один раз. Если опция выключена, ключевая пара генерируется сразу на устройстве.
Записывать копию ключа при временной замене устройства	Копии сертификатов и закрытых ключей записываются на устройство при временной замене.
Импортировать сертификат, если существует	Indeed CM использует сертификат с устройства вместо выпуска нового сертификата (для указанного пользователя, УЦ и шаблона). Если устройство инициализируется перед выпуском, сертификат удаляется.
Не удалять сертификат при обновлении/очистке устройства	При обновлении или очистке устройства истекающий/истекший сертификат не удаляется с устройства и не отзывается в УЦ. В процессе обновления запрашивается новый сертификат с новым закрытым ключом и записывается на устройство. Истекающий/истекший сертификат удаляется, если устройство изъято с инициализацией.
Отзывать сертификат при отзыве/выключении устройства	Сертификаты пользователя отзываются при выключении или отзыве устройства.

Параметр	Описание
Устанавливать сертификат в локальное хранилище	При выпуске и обновлении устройства через Сервис самообслуживания записанные на него сертификаты добавляются в локальное хранилище пользователя на рабочей станции.
Публиковать сертификат в каталоге пользователей	Выпущенный сертификат опубликуется в профиле пользователя в каталоге. Сервисная учетная запись для работы с каталогом пользователей должна иметь права на запись.
Удалять опубликованный сертификат при отзыве устройства	При отзыве устройства сертификат удаляется из профиля пользователя в каталоге.
Публиковать список отозванных сертификатов	При выключении, включении и отзыве устройств список отозванных сертификатов (CRL) опубликуется вне очереди. Пользователь не сможет подписывать документы отозванным сертификатом.
Требовать подписанный документ сертификата перед продолжением выпуска/ обновления устройства	Сертификат записывается 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 требуется обновить сертификат. **Список атрибутов** • Общее имя • E-mail • UPN-имя пользователя Дополнительный список отслеживаемых атрибутов пользователей задается в Мастере настройки в разделе Обновляемые атрибуты.
Шаблоны печати запроса на сертификат, сертификата, запроса на отзыв сертификата	Загрузите шаблоны документов сертификата в разделе **Конфигурация** → **Шаблоны печати**. Если шаблонов нет, используются стандартные шаблоны печати.
Период обновления (дней)	Период времени, в течение которого сертификат и закрытый ключ можно обновить. Значение по умолчанию – 30 дней.
Необязательный сертификат	При выпуске и обновлении устройства появится возможность выбрать, какие сертификаты из списка необязательных записать на устройство. Если опция выключена, сертификат записывается на устройство по умолчанию.

SafeTech CA

Настройте подключение к SafeTech CA и создайте шаблоны сертификатов, которые будут выпускаться в этом УЦ.

Предварительные настройки

Чтобы разрешить доступ к разделу **SafeTech CA**:

1. Запустите Мастер настройки.
2. Перейдите в раздел **Удостоверяющие центры**.
3. Включите интеграцию с SafeTech CA.

Добавить УЦ

1. Нажмите **Добавить УЦ**.
2. В поле **Адрес веб-службы CA Gateway** введите URL-адрес веб-службы CA Gateway. Например, `https://<имя сервера УЦ>:9443/ca-core/api/v1`.
3. Укажите данные для получения токена доступа в сервисе авторизации:
   - **Адрес веб-службы авторизации** — URL-адрес Realm (области) Keycloak, в которой находятся клиенты и пользователи (`st-ca` по умолчанию). Например, `https://<имя сервера УЦ>:8443/realms/st-ca`.
   - **Идентификатор клиента** — значение параметра **Client ID**. Например, `ca-gateway`. Убедитесь, что у клиента есть роль Администратора или Оператора УЦ. Как создать клиент в KeyCloak
   - **Клиентский секрет** — значение параметра **Client Secret**. Например, `vtG4VuWYbG6t4SxbIzsTCyxpMmqr4RPy`.

     Как найти Client ID и Client Secret в KeyCloak

     Client ID доступен в параметрах клиента на вкладке **Settings** в разделе **General settings**.
     Client Secret доступен в параметрах клиента на вкладке **Credentials**.

- **Имя пользователя** — имя сервисной учетной записи. Как создать сервисную учетную запись
- **Пароль** — пароль сервисной учетной записи.

4. Нажмите **Добавить**.

Создать шаблоны сертификатов

Перед началом работы убедитесь, что шаблоны сертификатов настроены в SafeTech CA. Как настроить шаблоны сертификатов в SafeTech CA

Чтобы создать шаблон сертификата:

1. Перейдите в раздел **Шаблоны**.
2. Нажмите **Создать шаблон сертификата**.
3. Заполните параметры и нажмите **Создать**.

Имя	Имя шаблона сертификата
УЦ	Имя удостоверяющего центра
Шаблон сертификата SafeTech CA	Шаблон сертификата, автоматически загруженный из SafeTech CA
Алгоритм ключа	Настройка алгоритма ключа отображается, если добавленный УЦ является ГОСТ-экземпляром ST CA. Выберите алгоритм, по которому формируется ключ шифрования: • ГОСТ-2012 (256) • ГОСТ-2012 (512) • RSA Длина RSA-ключа настраивается в шаблоне сертификата SafeTech CA в поле **Минимальная длина ключа**.

Префикс имени ключа	Произвольная строка, которая добавляется в начало имени контейнера, содержащего ключевую пару. Если префикс не указан, имя контейнера формируется случайным образом. Имя контейнера с префиксом отображается в Indeed CM (имя контейнера в разделе **СКЗИ**) и в стороннем ПО для работы с контейнерами закрытого ключа (КриптоПро CSP, клиенты устройств). Некоторые устройства могут не поддерживать отображение имени контейнера с префиксом.
Использовать аппаратную криптографию, если поддерживается	Опция отображается, если: 1. Добавленный УЦ является ГОСТ-экземпляром ST CA. 2. В настройке **Алгоритм ключа** выбран алгоритм ГОСТ-2012 (256) или ГОСТ-2012 (512). При выпуске сертификата ключевая пара создается с использованием криптографических алгоритмов, поддерживаемых устройством. Если устройство не поддерживает аппаратную криптографию, то используется КриптоПро CSP, установленный на рабочей станции, к которой подключено устройство. Изменить значение опции при редактировании шаблона нельзя.
Защищать ключ биометрией, если поддерживается	Опция поддерживается только для устройств Рутокен ЭЦП 3.0 3250 БИО (Рутокен БИО). При выпуске сертификата контейнер закрытого ключа защищается биометрическими данными пользователя (отпечатками пальцев), хранящимися на устройстве. Для доступа к ключу необходимо ввести PIN-код пользователя и пройти биометрическую аутентификацию. Изменить значение опции при редактировании шаблона нельзя. Подробнее о работе с устройствами Рутокен БИО

Включить в имя субъекта	Выберите атрибуты для формирования имени субъекта (Subject) сертификата. **Список атрибутов** • Полное различающееся имя (значение по умолчанию) • Общее имя • Имя • Фамилия • Инициалы • E-mail • Должность • Подразделение • Организация • Адрес • Город • Область • Страна Если добавленный УЦ является ГОСТ-экземпляром ST CA, вы можете дополнительно выбрать следующие атрибуты: • СНИЛС • ИНН • ИНН ЮЛ • ОГРН • ОГРНИП **ДЛЯ КАТАЛОГОВ ПОЛЬЗОВАТЕЛЕЙ ALD PRO И FREEIPA** Выберите атрибуты **Общее имя**, **Имя**, **Фамилия** для корректного формирования имени субъекта (Subject) сертификата.

Включить в альтернативное имя субъекта	Выберите атрибуты для формирования альтернативного имени субъекта (Subject Alternative Name) сертификата. **Список атрибутов** • E-mail • Дополнительные e-mail адреса • UPN-имя пользователя
Создавать резервную копию ключа	Когда на устройстве генерируется ключевая пара, ее резервная копия сохраняется на сервере Indeed CM. Копию ключевой пары можно сохранить только один раз. Если опция выключена, ключевая пара генерируется сразу на устройстве.
Записывать копию ключа при временной замене устройства	Копии сертификатов и закрытых ключей записываются на устройство при временной замене.
Импортировать сертификат, если существует	Indeed CM использует сертификат с устройства вместо выпуска нового сертификата (для указанного пользователя, УЦ и шаблона). Если устройство инициализируется перед выпуском, сертификат удаляется.
Не удалять сертификат при обновлении/очистке устройства	При обновлении или очистке устройства истекающий/истекший сертификат не удаляется с устройства и не отзывается в УЦ. В процессе обновления запрашивается новый сертификат с новым закрытым ключом и записывается на устройство. Истекающий/истекший сертификат удаляется, если устройство изъято с инициализацией.
Отзывать сертификат при отзыве или выключении устройства	Сертификаты отзываются при отзыве или выключении устройства.
Устанавливать сертификат в локальное хранилище	При выпуске и обновлении устройства в Сервисе самообслуживания записанные на устройство сертификаты добавляются в локальное хранилище пользователя на рабочей станции.

Публиковать сертификат в каталоге пользователей	Выпущенный сертификат публикуется в каталоге пользователей. При отзыве устройства сертификаты не удаляются из каталога.
Удалять опубликованный сертификат при отзыве устройства	При отзыве устройства из каталога пользователей удаляется опубликованный сертификат.
Публиковать список отозванных сертификатов	При выключении, включении и отзыве устройства 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 SafeTech CA имеет разрешение на управление УЦ.
Требовать подписанный документ сертификата перед продолжением выпуска/ обновления устройства	Сертификат записывается 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 требуется обновить сертификат. **Список атрибутов** • Общее имя • E-mail • UPN-имя пользователя Изменение e-mail приводит к обновлению сертификата, если этот атрибут выбран в опции **Включить в альтернативное имя субъекта**. Дополнительный список отслеживаемых атрибутов пользователей задается в Мастере настройки в разделе Обновляемые атрибуты.

Шаблоны печати запроса на сертификат, сертификата, запроса на отзыв сертификата	Загрузите шаблоны документов сертификата в разделе **Конфигурация** → **Шаблоны печати**. Если шаблонов нет, используются стандартные шаблоны печати.
Период обновления (дней)	Период времени, в течение которого сертификат и закрытый ключ можно обновить. Значение по умолчанию – 30 дней.
Необязательный сертификат	При выпуске устройства появится возможность выбрать, какие сертификаты из списка необязательных записать на устройство. Если опция выключена, сертификат записывается на устройство по умолчанию.

Dogtag CA

Настройте подключение к Dogtag CA и создайте шаблоны сертификатов, которые будут выпускаться в этом УЦ.

Предварительные настройки

Чтобы разрешить доступ к разделу **Dogtag CA**:

1. Запустите Мастер настройки.
2. Перейдите в раздел **Удостоверяющие центры**.
3. Включите интеграцию с Dogtag CA.

Добавить УЦ

1. Нажмите **Добавить УЦ**.
2. В поле **Адрес сервера** введите URL-адрес сервера Dogtag CA. Например, `https://<имя сервера УЦ>:8443`.
3. В поле **Клиентский сертификат** выберите сертификат агента регистрации для подключения к УЦ.
   Как выпустить сертификат агента регистрации
4. Нажмите **Добавить**.

Создать шаблоны сертификатов

Перед началом работы убедитесь, что шаблоны сертификатов пользователей настроены в Dogtag CA.
Как настроить шаблоны сертификатов в Dogtag CA

Чтобы создать шаблон сертификата:

1. Перейдите в раздел **Шаблоны**.
2. Нажмите **Создать шаблон сертификата**.
3. Заполните параметры и нажмите **Создать**.

Параметр	Описание
Имя	Имя шаблона сертификата
УЦ	Имя удостоверяющего центра
Шаблон сертификата Dogtag CA	Шаблон сертификата, автоматически загруженный из Dogtag CA
Размер ключа	Размер RSA-ключа. Если шаблон сертификата Dogtag CA имет поддерживаемую структуру, список доступных значений загружается автоматически.
Префикс имени ключа	Произвольная строка, которая добавляется в начало имени контейнера, содержащего ключевую пару. Если префикс не указан, имя контейнера формируется случайным образом. Имя контейнера с префиксом отображается в Indeed CM и в стороннем ПО для работы с контейнерами закрытого ключа (КриптоПро CSP, клиенты устройств). Некоторые устройства могут не поддерживать отображение имени контейнера с префиксом.

Параметр	Описание
Включить в имя субъекта	Выберите атрибуты для формирования имени субъекта (Subject) сертификата. **Список атрибутов** • Полное различающееся имя (значение по умолчанию) • Общее имя • Имя • Фамилия • Инициалы • E-mail • Должность • Подразделение • Организация • Адрес • Город • Область • Страна
Включить в альтернативное имя субъекта	Выберите атрибуты для формирования альтернативного имени субъекта (Subject Alternative Name) сертификата. **Список атрибутов** • E-mail • Дополнительные e-mail адреса • UPN-имя пользователя

Параметр	Описание
Защищать ключ биометрией, если поддерживается	Опция поддерживается только для устройств Рутокен ЭЦП 3.0 3250 БИО (Рутокен БИО). При выпуске сертификата контейнер закрытого ключа защищается биометрическими данными пользователя (отпечатками пальцев), хранящимися на устройстве. Для доступа к ключу необходимо ввести PIN-код пользователя и пройти биометрическую аутентификацию. Изменить значение опции при редактировании шаблона нельзя. Подробнее о работе с устройствами Рутокен БИО
Создавать резервную копию ключа	Когда на устройстве генерируется ключевая пара, ее резервная копия сохраняется на сервере Indeed CM. Копию ключевой пары можно сохранить только один раз. Если опция выключена, ключевая пара генерируется сразу на устройстве.
Записывать копию ключа при временной замене устройства	Копии сертификатов и закрытых ключей записываются на устройство при временной замене.
Импортировать сертификат, если существует	Indeed CM использует сертификат с устройства вместо выпуска нового сертификата (для указанного пользователя, УЦ и шаблона). Если устройство инициализируется перед выпуском, сертификат удаляется.
Не удалять сертификат при обновлении/очистке устройства	При обновлении или очистке устройства истекающий/истекший сертификат не удаляется с устройства и не отзывается в УЦ. В процессе обновления запрашивается новый сертификат с новым закрытым ключом и записывается на устройство. Истекающий/истекший сертификат удаляется, если устройство изъято с инициализацией.
Отзывать сертификат при отзыве или выключении устройства	Сертификаты отзываются при отзыве или выключении устройства.

Параметр	Описание
Устанавливать сертификат в локальное хранилище	При выпуске и обновлении устройства в Сервисе самообслуживания записанные на устройство сертификаты добавляются в локальное хранилище пользователя на рабочей станции.
Публиковать сертификат в каталоге пользователей	Выпущенный сертификат публикуется в каталоге пользователей. При отзыве устройства сертификаты не удаляются из каталога.
Удалять опубликованный сертификат при отзыве устройства	При отзыве устройства из каталога пользователей удаляется опубликованный сертификат.
Публиковать сертификат в файловое хранилище	Выпущенный сертификат публикуется в сетевом хранилище. При отзыве устройства сертификаты из хранилища не удаляются. Опция доступна, если в Мастере настройки в разделе **Общие функции** включена опция **Публикация сертификатов в файловое хранилище**.
Автоматически одобрять запрос на сертификат	Запрос на сертификат одобряется автоматически. Если опция выключена, для завершения выпуска необходимо дождаться, когда оператор УЦ одобрит запрос.
Требовать подписанный документ сертификата перед продолжением выпуска/ обновления устройства	Сертификат записывается 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 требуется обновить сертификат. **Список атрибутов** • Общее имя • E-mail • UPN-имя пользователя Дополнительный список отслеживаемых атрибутов пользователей задается в Мастере настройки в разделе Обновляемые атрибуты.
Шаблоны печати запроса на сертификат, сертификата, запроса на отзыв сертификата	Загрузите шаблоны документов сертификата в разделе **Конфигурация** → **Шаблоны печати**. Если шаблонов нет, используются стандартные шаблоны печати.
Период обновления (дней)	Период времени, в течение которого сертификат и закрытый ключ можно обновить. Значение по умолчанию – 30 дней.
Необязательный сертификат	При выпуске и обновлении устройства появится возможность выбрать, какие сертификаты из списка необязательных записать на устройство. Если опция выключена, сертификат записывается на устройство по умолчанию.

КриптоПро УЦ 2.0

Настройте подключение к КриптоПро УЦ 2.0 и создайте шаблоны сертификатов, которые будут выпускаться в этом УЦ.

Предварительные настройки

Чтобы разрешить доступ к разделу **КриптоПро УЦ 2.0**:

1. Запустите Мастер настройки.
2. Перейдите в раздел **Удостоверяющие центры**.
3. Включите интеграцию с КриптоПро УЦ 2.0.

Добавить УЦ

1. Нажмите **Добавить УЦ**.
2. Выберите тип API в зависимости от используемого варианта исполнения КриптоПро УЦ 2.0:
   - SOAP для вариантов исполнений 5, 6, 9, 10 для ОС Windows
   - REST для вариантов исполнений 15, 16 для ОС Windows и ОС Astra Linux SE
3. Введите **Адрес сервера ЦР**. 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>
```

4. Оставьте пустым поле **Имя ЦС**, если на рабочей станции развернута только одна роль Центра Сертификации (ЦС). Имя определяется автоматически. Если ролей ЦС несколько, укажите имя ЦС, к которому необходимо подключиться.

5. В поле **Адрес прокси-сервера** укажите имя сервера и порт, если для соединения с УЦ используется прокси-сервер. Например, `http://proxy.company.com:8080`.

6. В поле **Клиентский сертификат** выберите сертификат клиентской аутентификации для подключения к УЦ (Indeed CM Service User). Как получить сертификат

7. Для вариантов исполнений 15, 16 в поле **Сертификат подписи** выберите сертификат для подписи запросов в УЦ.

8. Чтобы установить связь между пользователями УЦ и пользователями каталога Indeed CM, включите опцию **Устанавливать привязку между пользователем УЦ и пользователем каталога**.

Подробнее о работе опции

Установите связь между пользователями УЦ и пользователями каталога Indeed CM, если они не совпадают. Такая ситуация может быть в следующих сценариях использования:

- Indeed CM работает с пользователями домена Windows и запрашивает для них сертификаты КриптоПро УЦ. В КриптоПро УЦ есть свой каталог пользователей, который не связан с каталогом пользователей Indeed CM.
- Indeed CM работает с пользователями КриптоПро УЦ, но этим пользователям необходимо выдавать сертификаты других УЦ, кроме сертификатов собственного УЦ.

При необходимости определите следующие параметры работы с УЦ:

- **Устанавливать привязку автоматически**
  Если в каталоге УЦ есть пользователь, для которого выпускается устройство, связь устанавливается автоматически.
- **Создавать пользователя УЦ, если он не существует**
  Если в каталоге УЦ нет пользователя, для которого выпускается устройство с сертификатом, пользователь создается автоматически. По умолчанию пользователи создаются в корневом каталоге Центра Регистрации. Чтобы создавать пользователей во вложенной папке, укажите имя папки.
- **Обновлять учетные данные пользователя УЦ**
  Если в профиле пользователя в каталоге изменились данные, они обновятся автоматически в каталоге УЦ.
  Чтобы данные обновились, пользователь каталога должен быть связан с пользователем Центра Регистрации. Если привязка не установлена, в каталоге ЦР создается новый пользователь.

9. Нажмите **Добавить**.

Создать шаблоны сертификатов

1. Перейдите в раздел **Шаблоны**.
2. Нажмите **Создать шаблон сертификата**.
3. Заполните параметры и нажмите **Создать**.

Параметр	Описание
Имя	Имя шаблона сертификата
УЦ	Имя удостоверяющего центра
Шаблон сертификата КриптоПро УЦ 2.0	Шаблон сертификата, автоматически загруженный из КриптоПро УЦ 2.0
Префикс имени ключа	Произвольная строка, которая добавляется в начало имени контейнера, содержащего ключевую пару. Если префикс не указан, имя контейнера формируется случайным образом. Имя контейнера с префиксом отображается в Indeed CM (имя контейнера в разделе СКЗИ) и в стороннем ПО для работы с контейнерами закрытого ключа (КриптоПро CSP, клиенты устройств и пр.). Некоторые устройства могут не поддерживать отображение имени контейнера с префиксом.
Использовать аппаратную криптографию, если поддерживается	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
Защищать ключ биометрией, если поддерживается	Опция поддерживается только для устройств Рутокен ЭЦП 3.0 3250 БИО (Рутокен БИО). При выпуске сертификата контейнер закрытого ключа защищается биометрическими данными пользователя (отпечатками пальцев), хранящимися на устройстве. Для доступа к ключу необходимо ввести PIN-код пользователя и пройти биометрическую аутентификацию. Изменить значение опции при редактировании шаблона нельзя. Подробнее о работе с устройствами Рутокен БИО
Создавать резервную копию ключа	Когда на устройстве генерируется ключевая пара, ее резервная копия сохраняется на сервере Indeed CM. Копию ключевой пары можно сохранить только один раз. Если опция выключена, ключевая пара генерируется сразу на устройстве.
Записывать копию ключа при временной замене устройства	Копии сертификатов и закрытых ключей записываются на устройство при временной замене.
Импортировать сертификат, если существует	Indeed CM использует сертификат с устройства вместо выпуска нового сертификата (для указанного пользователя, УЦ и шаблона). Если устройство инициализируется перед выпуском, сертификат удаляется.
Не удалять сертификат при обновлении/очистке устройства	При обновлении или очистке устройства истекающий/истекший сертификат не удаляется с устройства и не отзывается в УЦ. В процессе обновления запрашивается новый сертификат с новым закрытым ключом и записывается на устройство. Истекающий/истекший сертификат удаляется, если устройство изъято с инициализацией.

Параметр	Описание
Отзывать сертификат при отзыве или выключении устройства	Сертификаты пользователя отзываются при выключении или отзыве устройства.
Устанавливать сертификат в локальное хранилище	При выпуске и обновлении устройства в Сервисе самообслуживания записанные на него сертификаты сохраняются в локальное хранилище пользователя на рабочей станции.
Публиковать сертификат в каталоге пользователей	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	Выпущенный квалифицированный сертификат будет зарегистрирован в Единой системе идентификации и аутентификации (ЕСИА). Опция доступна, если в Мастере настройки в разделе **Общие функции** включена **Интеграция со СМЭВ**.
Публиковать сертификат в файловое хранилище	Выпущенный сертификат сохраняется в сетевом хранилище (папке). При отзыве устройства сертификаты не удаляются из хранилища. Опция доступна, если в Мастере настройки в разделе **Общие функции** включена **Публикация сертификатов в файловое хранилище**.

Параметр	Описание
Публиковать сертификат в ЦФТ	Выпущенный сертификат сохраняется в базе приложений ЦФТ. При отзыве устройства сертификаты не удаляются из базы приложений ЦФТ. Опция доступна, если в Мастере настройки в разделе **Удостоверяющие центры** включена опция **Публиковать сертификаты пользователей КриптоПро УЦ 2.0 в базе приложений ЦФТ**.
Публиковать список отозванных сертификатов	При выключении, включении и отзыве устройств список отозванных сертификатов (CRL) опубликуется вне очереди. Пользователь не сможет подписывать документы отозванным сертификатом.
Использовать комментарий устройства в качестве комментария пользователя к запросу на сертификат	В поле **Заметки пользователя** запроса сертификата отображается текст комментария устройства.
Автоматически одобрять запрос на сертификат	Запросы на сертификат одобряются автоматически. Если опция выключена, для завершения выпуска необходимо дождаться одобрения запроса на УЦ.
Автоматически одобрять подписанный запрос на обновление сертификата	Запрос на обновление сертификата одобряется автоматически. Если опция выключена, для обновления сертификата необходимо дождаться одобрения запроса на УЦ.
Требовать подписанный документ сертификата перед продолжением выпуска/ обновления устройства	Сертификат запишется 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 требуется обновить сертификат: Общее имя, E-mail, UPN-имя пользователя. Дополнительный список отслеживаемых атрибутов пользователей задается в разделе **Обновляемые атрибуты** Мастера настройки Indeed CM.
Шаблон печати запроса на сертификат, сертификата, запроса на отзыв сертификата	Загрузите шаблоны документов сертификата в разделе **Конфигурация → Шаблоны печати**. Если шаблонов нет, используются стандартные шаблоны печати.
Период обновления (дней)	Период времени, в течение которого сертификат и закрытый ключ можно обновить. Значение по умолчанию – 30 дней.
Необязательный сертификат	При выпуске и обновлении устройства появится возможность выбрать, какие сертификаты из списка необязательных, записать на устройство. Если опция выключена, сертификат записывается на устройство по умолчанию.

КриптоПро DSS 2.0

Настройте подключение к КриптоПро DSS и создайте шаблоны сертификатов, которые будут выпускаться в этом УЦ.

Предварительные настройки

Чтобы разрешить доступ к разделу **КриптоПро DSS**:

1. Запустите Мастер настройки.
2. Перейдите в раздел **Удостоверяющие центры**.
3. Включите интеграцию с КриптоПро DSS.

Добавить УЦ

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

1. Перейдите в раздел **КриптоПро DSS** → **Серверы**.
2. Нажмите **Добавить сервер**, чтобы добавить удостоверяющий центр.
3. Укажите параметры подключения:
   - **Имя** – произвольное имя добавляемого сервера.
   - **Адрес веб-службы СЭП** – адрес службы электронной подписи DSS.
4. Укажите данные для получения токена доступа в сервисе авторизации:
   - **Адрес веб-службы ЦИ** – адрес центра идентификации DSS.
   - **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** – 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.

5. Чтобы установить связь между пользователями КриптоПро DSS и пользователями каталога Indeed CM, включите опцию **Устанавливать привязку между пользователем DSS и пользователем каталога**.

   Подробнее о работе опции

   Установите связь между пользователями УЦ и пользователями каталога Indeed CM, если они не совпадают. Такая ситуация может быть в следующих сценариях использования:

   - Indeed CM работает с пользователями домена Windows и запрашивает для них сертификаты КриптоПро DSS. В КриптоПро DSS есть свой каталог пользователей, который не связан с каталогом пользователей Indeed CM.
   - Indeed CM работает с пользователями КриптоПро DSS, но этим пользователям необходимо выдавать сертификаты других УЦ, кроме сертификатов собственного УЦ.

   При необходимости определите следующие параметры работы с УЦ:

   - **Устанавливать привязку автоматически**
     Если в каталоге УЦ есть пользователь, для которого выпускается устройство, связь устанавливается автоматически.
   - **Создавать пользователя УЦ, если он не существует**
     Если в каталоге УЦ нет пользователя, для которого выпускается устройство с сертификатом, пользователь создается автоматически. По умолчанию пользователи создаются в корневом каталоге Центра Регистрации. Чтобы создавать пользователей во вложенной папке, укажите имя папки.
   - **Обновлять учетные данные пользователя УЦ**
     Если в профиле пользователя в каталоге изменились данные, они обновятся автоматически в каталоге УЦ.
     Чтобы данные обновились, пользователь каталога должен быть связан с пользователем Центра Регистрации. Если привязка не установлена, в каталоге ЦР создается новый пользователь.

6. Нажмите **Добавить**.

Создать шаблоны сертификатов

1. Перейдите в раздел **Шаблоны**.
2. Нажмите **Создать шаблон сертификата**.
3. Заполните параметры и нажмите **Создать**.

Параметр	Описание
Имя	Имя шаблона сертификата
Сервер	Имя сервера DSS
УЦ	Имя удостоверяющего центра
Шаблон сертификата КриптоПро DSS	Шаблон сертификата, автоматически загруженный из КриптоПро DSS
Импортировать сертификат, если существует	Indeed CM использует сертификат с устройства вместо выпуска нового сертификата (для указанного пользователя, УЦ и шаблона). Если устройство инициализируется перед выпуском, сертификат удаляется.
Отзывать сертификат при отзыве или выключении устройства	Сертификаты пользователя отзываются при выключении или отзыве устройства.
Публиковать сертификат в каталоге пользователей	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	Запрос на сертификат одобряется автоматически. Если опция выключена, для завершения выпуска необходимо дождаться одобрения запроса на УЦ.

Параметр	Описание
Требовать подписанный документ сертификата перед продолжением выпуска/ обновления устройства	Сертификат запишется 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	При выпуске и обновлении устройства появится возможность записать на устройство сертификаты из списка необязательных. Если опция выключена, сертификат записывается на устройство по умолчанию.

Валидата УЦ

Настройте подключение к Валидата УЦ и создайте шаблоны сертификатов, которые будут выпускаться в этом УЦ.

Предварительные настройки

Чтобы разрешить доступ к разделу **Валидата УЦ**:

1. Запустите Мастер настройки.
2. Перейдите в раздел **Удостоверяющие центры**.
3. Включите интеграцию с Валидата УЦ.

Добавить УЦ

Офлайн-режим

1. Нажмите **Добавить УЦ**.
2. В поле **Каталог для обмена файлами с ЦР/ЦС** укажите каталог для обмена файлами Indeed CM с Центром Регистрации. Каталог должен содержать цепочку сертификатов Валидата УЦ и актуальный список отозванных сертификатов X.509 (CRL или COC).
3. В полях **Имя пользователя** и **Пароль** укажите учетные данные сервисной учетной записи для подключения к каталогу.
4. В поле **Подкаталог для запросов** укажите подкаталог для входящих незащищенных запросов пользователей в формате PKCS#10. Обработка запросов в формате PKCS#10 выполняется в ручном режиме на АРМ Администратора ЦР.
5. В поле **Подкаталог для сертификатов** укажите подкаталог сертификатов для выдачи конечным пользователям.
6. Нажмите **Добавить**.

Онлайн-режим

В онлайн-режиме Indeed CM заменяет АРМ Оператора ЦР Валидата. Убедитесь, что в настройках Центра Регистрации включена опция **Разрешить удаленное подключение к**

сервису для работы в онлайн-режиме.

1. Нажмите **Добавить УЦ**.
2. В поле **Адрес сервера ЦР** укажите адрес и порт RPC сервера Центра Регистрации.

   ```
   ncacn_ip_tcp:<ip>[<port>]
   ```

3. В выпадающем списке **Клиентский сертификат** выберите сертификат Оператора Центра Регистрации.

   > **ПРИМЕЧАНИЕ**
   >
   > Убедитесь, что поле **Улучшенный ключ** сертификата содержит 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).
   >
   > Клиентский сертификат используется:
   >
   > - При подключении к сервису ЦР, чтобы выполнить аутентификацию по протоколу TLS
   > - Для подписания XML-шаблона на получение или отзыв сертификата ключа проверки ЭП пользователя

4. В поле **Каталог для обмена файлами с ЦР/ЦС** укажите каталог для обмена файлами Indeed CM с Центром Регистрации. Каталог должен содержать цепочку 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 каталогу.
6. В поле **Подкаталог для запросов** укажите подкаталог запросов, обработанных Оператором ЦР, в формате CMS/PKCS#7 для Центра Сертификации.
7. В поле **Подкаталог для сертификатов** укажите подкаталог сертификатов, обработанных Центром Сертификации, в формате CMS/PKCS#7.
8. Нажмите **Добавить**.

Создать шаблоны сертификатов

Перед началом работы убедитесь, что шаблоны сертификатов настроены и добавлены в Валидата УЦ.
Как настроить шаблоны сертификатов в Валидата УЦ

1. Перейдите в раздел **Шаблоны**.
2. Нажмите **Создать шаблон сертификата**.
3. Заполните параметры и нажмите **Создать**.

Параметр	Описание
Имя	Имя шаблона сертификата
УЦ	Имя удостоверяющего центра
Шаблон сертификата Валидата УЦ	Загрузите файл шаблона сертификата.
Префикс имени ключа	Произвольная строка, которая добавляется в начало имени контейнера, содержащего ключевую пару. Если префикс не указан, имя контейнера формируется случайным образом. Имя контейнера с префиксом отображается в Indeed CM (имя контейнера в разделе **СКЗИ**) и в стороннем ПО для работы с контейнерами закрытого ключа (КриптоПро CSP, клиенты устройств и пр.). Некоторые устройства могут не поддерживать отображение имени контейнера с префиксом.
Использовать аппаратную криптографию, если поддерживается	При выпуске и обновлении сертификата ключевая пара создается с использованием криптографических алгоритмов, поддерживаемых устройством. Если устройство не поддерживает аппаратную криптографию, то используется КриптоПро CSP, установленный на рабочей станции, к которой подключено устройство. Изменить значение опции при редактировании шаблона нельзя.

Параметр	Описание
Защищать ключ биометрией, если поддерживается	Опция поддерживается только для устройств Рутокен ЭЦП 3.0 3250 БИО (Рутокен БИО). При выпуске сертификата контейнер закрытого ключа защищается биометрическими данными пользователя (отпечатками пальцев), хранящимися на устройстве. Для доступа к ключу необходимо ввести PIN-код пользователя и пройти биометрическую аутентификацию.
Изменить значение опции при редактировании шаблона нельзя. Подробнее о работе с устройствами Рутокен БИО	
Создавать резервную копию ключа	Когда на устройстве генерируется ключевая пара, ее резервная копия сохраняется на сервере Indeed CM. Копию ключевой пары можно сохранить только один раз. Если опция выключена, ключевая пара генерируется сразу на устройстве.
Записывать копию ключа при временной замене устройства	Копии сертификатов и закрытых ключей записываются на устройство при временной замене.
Импортировать сертификат, если существует	Indeed CM использует сертификат с устройства вместо выпуска нового сертификата (для указанного пользователя, УЦ и шаблона). Если устройство инициализируется перед выпуском, сертификат удаляется.
Не удалять сертификат при обновлении/очистке устройства	При обновлении или очистке устройства истекающий/истекший сертификат не удаляется с устройства и не отзывается в УЦ. В процессе обновления запрашивается новый сертификат с новым закрытым ключом и записывается на устройство. Истекающий/истекший сертификат удаляется, если устройство изъято с инициализацией.

Параметр	Описание
Отзывать сертификат при отзыве/выключении устройства	Сертификаты пользователя отзываются при выключении или отзыве устройства.
Устанавливать сертификат в локальное хранилище	При выпуске и обновлении устройства в Сервисе самообслуживания записанные на него сертификаты добавляются в локальное хранилище пользователя на рабочей станции.
Публиковать сертификат в каталоге пользователей	Выпущенный сертификат опубликуется в профиле пользователя в каталоге. Чтобы удалять сертификат из профиля, включите опцию **Удалять опубликованный сертификат при отзыве устройства**. Убедитесь, что сервисная учетная запись для работы с каталогом пользователей имеет привилегию **Запись: userCertificate** (Write userCertificate).
Публиковать сертификат в ЕСИА	Выпущенный квалифицированный сертификат регистрируется в Единой системе идентификации и аутентификации (ЕСИА). Опция доступна, если в Мастере настройки в разделе **Общие функции** включена **Интеграция со СМЭВ**.
Отслеживаемые атрибуты пользователя	Укажите атрибуты пользователя, при изменении которых требуется обновить сертификат: Общее имя, E-mail, UPN-имя пользователя. Дополнительный список отслеживаемых атрибутов пользователей задается в Мастере настройки Indeed CM в разделе **Обновляемые атрибуты**.
Шаблон печати запроса на сертификат, сертификата, запроса на отзыв сертификата	Загрузите шаблоны документов сертификата в разделе **Конфигурация → Шаблоны печати**. Если шаблонов нет, используются стандартные шаблоны печати.
Период обновления (дней)	Период времени, в течение которого сертификат и закрытый ключ можно обновить. Значение по умолчанию – 30 дней.

Параметр	Описание
Необязательный сертификат	При выпуске устройства появится возможность выбрать, какие сертификаты из списка необязательных записать на устройство. Если опция выключена, сертификат записывается на устройство по умолчанию.

Общие сертификаты

Общий сертификат – это сертификат, выпущенный в стороннем УЦ и общий для нескольких пользователей. Indeed CM позволяет записать общий сертификат и его закрытый ключ на устройства нескольких пользователей одновременно.

Особенности

Особенности работы Indeed CM с общими сертификатами:

- Поддерживаются сертификаты с ключами RSA и ГОСТ.
- Для записи ГОСТ-сертификатов нужно установить КриптоПро CSP на сервер Indeed CM и на рабочую станцию к которой подключено устройство.
- Общие сертификаты нельзя приостановить и отозвать, но можно обновить – удалить старый файл PFX и добавить новый.
- Общие сертификаты нельзя опубликовать в каталоге пользователей, файловом хранилище, базе приложений ЦФТ и в хранилище сертификатов пользователя.

Добавление

Чтобы добавить общий сертификат в Indeed CM:

1. Перейдите в настройки политики использования устройств в раздел **Настройки PKI** → **Общие сертификаты**.
2. Нажмите **Добавить общий сертификат**.
3. Выберите файл PFX.
4. Введите пароль для доступа к содержимому файла.
5. Нажмите **Добавить**.

Общий сертификат записывается на устройство при его выпуске или обновлении.

Необязательный сертификат

Вы можете настроить возможность выбора общего сертификата для записи на устройство. Включите опцию **Необязательный сертификат**.

Если опция **Необязательный сертификат** не включена, то общий сертификат считается обязательным и записывается на устройство при его выпуске или обновлении.

Уведомление об истекающих сертификатах

Чтобы отправить уведомление администраторам об истечении срока действия общих сертификатов:

1. Перейдите в настройки политики использования устройств в раздел **Уведомления**.
2. Создайте уведомление о событии *Общие сертификаты истекают*.

Уведомления о сертификатах, которые уже истекли, не отправляются.

Indeed Access Manager

В Indeed Certificate Manager реализована интеграция с Indeed Access Manager (Indeed AM) версии 6.x и 8.2 и выше.

Возможности интеграции

Интеграция позволяет объединить следующие операции:

- Выпуск устройства
- Запрос сертификата
- Запись сертификата на устройство
- Регистрация способа входа «Смарт-карта или USB-ключ + PIN» пользователя Indeed AM

Когда устройство выпускается в Indeed CM, в Indeed AM регистрируется способ входа «Смарт-карта или USB-ключ + PIN», и на устройство записывается сертификат. Выпущенное устройство можно использовать для аутентификации в домене и SSO-приложениях, для цифровой подписи и доступа к ресурсам по персональным сертификатам.

При изъятии и отзыве устройства удаляется и аутентификатор, и сертификаты, которые содержатся на устройстве. При выключении устройства аутентификатор становится неактивным, при включении – активным.

Предварительные настройки

Чтобы разрешить доступ к разделу **Indeed AM**:

1. Запустите Мастер настройки.
2. Перейдите в раздел **Общие функции**.
3. Включите опцию **Интеграция с Indeed Access Manager**.

Настройка интеграции

Выберите инструкцию в зависимости от версии Indeed AM.

Indeed AM 6
Чтобы настроить интеграцию Indeed CM с Indeed AM 6:

1. Установите и настройте следующие компоненты Indeed AM:
    - Indeed Administration Tools (или Indeed Admin Pack) на каждый сервер Indeed CM
    - Indeed Extended Security Provider на каждый сервер Indeed AM
    - Indeed AM Smart Card + PIN Provider на каждый сервер Indeed AM и на пользовательские рабочие станции

    > **ПОДСКАЗКА**
    > Indeed Administration Tools входит в состав дистрибутива Indeed AM 6. Чтобы получить компоненты Indeed Extended Security Provider и Indeed AM Smart Card + PIN Provider, обратитесь в службу технической поддержки компании Индид.

2. Настройте Extended Security Provider:
    1. Создайте группу безопасности Indeed-ID Enrollment Admins.
    2. Добавьте сервисную учетную запись в группы безопасности Indeed-ID User Admins и Indeed-ID Enrollment Admins.
3. В Консоли управления Indeed CM откройте раздел **Конфигурация**.
4. Перейдите в настройки политики использования устройств в раздел **Indeed AM**.
5. Включите опцию **Включить интеграцию с Indeed AM** и выберите **Indeed AM 6**.
6. Настройте параметры.

Параметр	Описание
Использовать прокси-сервер Indeed AM	Indeed CM обращается к прокси-серверу Indeed AM, который направляет запрос на серверы Indeed AM. Используйте прокси-сервер, если серверы Indeed CM находятся за пределами домена, в котором установлен Indeed AM.
URL-адрес прокси-сервера	Адрес, по которому доступен Indeed AM Proxy Server.

Параметр	Описание
Имя пользователя **Пароль**	Логин и доменный пароль пользователя, входящего в группы безопасности Indeed-ID User Admins и Indeed-ID Enrollment Admins.
Разрешить использование Indeed AM Windows Logon	При выпуске устройства в Indeed CM пользователь может аутентифицироваться в домене с помощью провайдера Indeed AM Windows Logon.
Разрешить использование Indeed AM Enterprise Single Sign-On	При выпуске устройства в Indeed CM пользователь может аутентифицироваться в приложениях с помощью провайдера Indeed AM Enterprise SSO Agent.
Генерировать случайный пароль учетной записи Windows	При выпуске устройства в Indeed CM для пользователя генерируется случайный доменный пароль. Когда срок действия пароля истекает, генерируется новый пароль. Новый пароль известен только системе Indeed AM.

⚠ **ПРЕДУПРЕЖДЕНИЕ**

Если удалить последний зарегистрированный аутентификатор пользователя, то выключатся разрешения на использование Indeed AM Windows Logon, Indeed AM Enterprise Single Sign-On и генерацию случайного пароля.

ⓘ **ПРИМЕР РАБОТЫ ИНТЕГРАЦИИ**

Если у пользователя нет 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 способ входа в Indeed AM – «Смарт-карта или USB-ключ + PIN».
- Одно устройство в Indeed CM. Например, eToken.

Indeed AM 8.2

Чтобы настроить интеграцию Indeed CM с Indeed AM 8.2 и выше:

1. Установите и настройте компонент Indeed AM Smart Card + PIN Provider на каждом сервере Indeed AM и на пользовательских рабочих станциях, с которых будут выпускаться устройства.
2. В Консоли управления Indeed CM откройте раздел **Конфигурация**.
3. Перейдите в настройки политики использования устройств в раздел **Indeed AM**.
4. Включите опцию **Включить интеграцию с Indeed AM** и выберите **Indeed AM 8.2**.
5. В поле **Адрес сервера** введите адрес сервера Indeed AM. Например, `https://server.domain.loc/am/core`.
6. Для подключения к серверу Indeed AM введите UPN-имя учетной записи пользователя (например, `admin@domain.loc`) и пароль.

   > **ПРИМЕЧАНИЕ**
   > Indeed CM и Indeed AM должны быть подключены к одному каталогу пользователей.
   > Учетная запись должна состоять в группе локальных или глобальных администраторов Indeed AM и иметь следующие привилегии:
   >
   > - Регистрация любого аутентификатора
   > - Включение аутентификатора
   > - Отключение аутентификатора
   > - Удаление аутентификатора

7. Нажмите **Сохранить**. Выполнится проверка подключения к серверу.

Secret Net Studio

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

Интеграция позволяет:

- Добавить устройство в базу данных SNS при его выпуске в Indeed CM. Пользователю присваивается персональный идентификатор SNS, который записывается на устройство.
- Добавить устройство в базу данных SNS при его замене в Indeed CM. Новое устройство присваивается пользователю, если в базе данных SNS содержалась информация о заменяемом устройстве. Если в базе данных SNS не было информации о заменяемом устройстве, то персональный идентификатор SNS можно записать на устройство при новом выпуске или обновлении устройства.
- Удалить устройство из базы данных SNS при его отзыве у пользователя в Indeed CM. При этом присвоение персонального идентификатора SNS пользователю отменяется.

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».

Предварительные настройки

Чтобы разрешить доступ к разделу **Secret Net Studio**:

1. Запустите Мастер настройки.
2. Перейдите в раздел **Общие функции**.
3. Включите опцию **Интеграция с Secret Net Studio**.

Настройка интеграции

1. Для подключения к базе данных SNS установите SNS клиент с базовой функциональностью на сервер Indeed CM.
2. Установите SNS клиент на клиентские рабочие станции, с которых будут выпускаться устройства.
3. Откройте раздел **Конфигурация** Консоли управления Indeed CM, перейдите в настройки политики использования устройств и выберите раздел **Secret Net Studio**.
4. Включите опцию **Включить интеграцию с Secret Net Studio**.
5. В поле **Имя пользователя** укажите учетную запись, входящую в группу администраторов безопасности SNS.
6. Чтобы записать идентификатор SNS с режимом хранения доменного пароля пользователя на устройство при выпуске, включите опцию **Включить режим хранения пароля пользователя**.
7. Нажмите **Сохранить**.

Рутокен Логон

Indeed Certificate Manager поддерживает интеграцию с Рутокен Логон – программным продуктом компании «Актив», который позволяет использовать схему двухфакторной аутентификации пользователей в ОС Linux с помощью защищенного устройства. Рутокен Логон поддерживает следующие механизмы аутентификации:

- Аутентификация по клиентскому сертификату
- Аутентификация по сложному паролю

Возможности интеграции

Интеграция Indeed CM с Рутокен Логон позволяет выпустить устройство, на котором содержится сертификат или сложный пароль, для доменной аутентификации в ОС Linux через окно входа Рутокен Логон.

Процесс аутентификации происходит следующим образом:

1. Пользователь подключает устройство к рабочей станции с установленным Рутокен Логон и вводит PIN-код устройства.
2. Рутокен Логон считывает данные с устройства и аутентифицирует пользователя в домене без ввода доменного пароля.

Особенности управления сложным паролем

При выпуске устройства

Генерируется сложный пароль — случайное значение из 72 ASCII-символов. Доменный пароль пользователя заменяется на сложный. На устройство записываются объекты с зашифрованными данными, подтверждающими владение паролем.

При изъятии устройства

Объекты данных, подтверждающих владение паролем, автоматически удаляются. Аутентификация с помощью этого устройства невозможна. Доменный пароль остается случайным и неизвестным, пользователь не сможет войти в домен по паролю.

Чтобы восстановить возможность входа по паролю, администратор может сбросить доменный пароль пользователя через Indeed CM. Подробнее о функции сброса пароля

пользователя

Предварительные настройки

Подготовка Рутокен Логон

Перед настройкой интеграции с Рутокен Логон в Indeed CM убедитесь, что Рутокен Логон настроен на доменный режим работы.

Настройка интеграции в Мастере настройки

Чтобы настроить доступ к разделу **Рутокен Логон** в политике:

1. Запустите Мастер настройки.
2. Перейдите в раздел **Общие функции**.
3. Включите опцию **Интеграция с Рутокен Логон**.
4. Примените настройки на сервере Indeed CM.

В политике появится раздел **Рутокен Логон**.

Требования для сброса пароля пользователя

Если вы планируете выпускать устройства для аутентификации в домене по сложному паролю, выполните следующие действия, чтобы иметь возможность сбросить доменный пароль пользователя:

1. Запустите Мастер настройки, перейдите в раздел **Каталог пользователей** и убедитесь, что в настройках каталога пользователей включена опция **Использовать LDAPS**.
2. Убедитесь, что сервисная учетная запись для работы с каталогом пользователей обладает правами **Сброс пароля** (Reset password) и **Запись: pwdLastSet** (Write pwdLastSet).
3. Откройте Консоль управления, перейдите в раздел **Конфигурация** → **Роли** и убедитесь, что операторы, которые выпускают устройства в Консоли управления, обладают привилегией *Сброс пароля пользователя*.

Настройка интеграции

1. Откройте Консоль управления и перейдите в раздел **Конфигурация**.
2. Выберите политику и перейдите в раздел **Рутокен Логон**.
3. Нажмите **Включить интеграцию с Рутокен Логон**.
4. Выберите тип аутентификации пользователей при входе в ОС с помощью Рутокен Логон:
   - **Сертификат** для аутентификации по сертификату.
     В выпадающем списке **Шаблон сертификата** выберите шаблон, на основе которого формируется сертификат. Шаблоны сертификатов задаются в настройках политики в разделе **Удостоверяющие центры → Шаблоны**.
   - **Сложный пароль** для аутентификации по сложному паролю.
5. При необходимости отключите опцию **Блокировать пользовательскую сессию при отключении устройства**.
   Если опция включена, сессия пользователя блокируется при отключении устройства от рабочей станции.
   Рекомендуется оставить опцию включенной для защиты от несанкционированного доступа.
6. Нажмите **Сохранить**.

СМЭВ

Indeed Certificate Manager можно интегрировать с Системой межведомственного электронного взаимодействия (СМЭВ) через КриптоПро Шлюз УЦ-СМЭВ версии 1.0.7374.2300 и выше.

Возможности интеграции

Интеграция позволяет объединить в единый процесс следующие операции:

- Выпуск и обновление устройства
- Проверка данных пользователя в СМЭВ
- Запрос квалифицированного сертификата
- Регистрация квалифицированного сертификата в Единой системе идентификации и аутентификации (ЕСИА)
- Запись квалифицированного сертификата на устройство

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.

Виды проверок данных пользователя

В зависимости от типа пользователя в СМЭВ отправляются запросы на получение следующей информации:

- Для физических лиц:
  - Предоставление сведений о соответствии фамильно-именной группы и СНИЛС
  - Предоставление сведений о соответствии паспортных данных и ИНН физического лица
  - Проверка действительности паспорта (расширенная)

- Для юридических лиц:
  - Получение данных юридического лица из ЕГРЮЛ по ОГРН
  - Предоставление сведений о соответствии фамильно-именной группы и СНИЛС
  - Предоставление сведений о соответствии паспортных данных и ИНН физического лица
  - Проверка действительности паспорта (расширенная)

- Для индивидуальных предпринимателей:
  - Получение данных индивидуального предпринимателя из ЕГРИП по ИНН
  - Предоставление сведений о соответствии фамильно-именной группы и СНИЛС
  - Предоставление сведений о соответствии паспортных данных и ИНН физического лица
  - Проверка действительности паспорта (расширенная)

Предварительные настройки

Настройка доступа к разделу СМЭВ

Настройте доступ к разделу **СМЭВ**:

1. Запустите Мастер настройки.
2. Перейдите в раздел **Общие функции**.
3. Включите опцию **Интеграция со СМЭВ**.

Установка сертификата оператора шлюза КриптоПро УЦ-СМЭВ

Установите сертификат оператора шлюза КриптоПро УЦ-СМЭВ и его контейнер закрытого ключа в локальное хранилище сертификатов компьютера на сервере Indeed CM.

Как установить сертификат

Настройка интеграции

1. Откройте Консоль управления и перейдите в раздел **Конфигурация**.
2. Выберите политику и перейдите в раздел **СМЭВ**.
3. Включите опцию **Включить интеграцию со СМЭВ**.
4. В поле **Адрес шлюза КриптоПро УЦ-СМЭВ** укажите URL шлюза КриптоПро УЦ-СМЭВ.
5. Выберите сертификат оператора шлюза СМЭВ. Убедитесь, что сертификат оператора шлюза КриптоПро УЦ-СМЭВ и его контейнер закрытого ключа установлены в локальное хранилище сертификатов на сервере Indeed CM.
6. Чтобы проводить проверку сведений о соответствии фамильно-именной группы, даты рождения, пола и СНИЛС, убедитесь, что включена опция **Проверять соответствие фамильно-именной группы и СНИЛС**.
7. Чтобы проводить расширенную проверку паспорта, убедитесь, что включена опция **Проверять действительность паспорта**.

Через КриптоПро Шлюз УЦ-СМЭВ отправляется дополнительный запрос в МВД, чтобы получить сведения о действительности паспорта. Проверяется ФИО, серия и номер паспорта.

8. Нажмите **Сохранить**.

После настройки интеграции Indeed CM со СМЭВ в Консоли управления в разделе **Сводная информация** отображаются данные о сертификате оператора шлюза КриптоПро УЦ-СМЭВ – субъект сертификата, издатель, дата окончания срока действия, состояние и политики.

Поведение

В разделе **Поведение** задаются настройки, которые определяют доступные операции для администраторов и операторов в Консоли управления и для пользователей в Сервисе самообслуживания.

Общие разрешения

Автоматически добавлять устройства при выпуске или назначении	В момент выпуска или назначения устройства автоматически добавляются в Indeed CM. Если опция выключена, нельзя выпускать или назначать устройства, которые подключены к компьютеру, но не добавлены в Indeed CM.
Разрешить пользователю добавлять устройства при выпуске	Пользователь может выпускать устройства, которые не были добавлены в Indeed CM. Устройства добавляются автоматически в процессе выпуска.
Искать сертификаты при выпуске/обновлении устройства для отслеживания срока действия	При выпуске/обновлении устройства Indeed CM проверяет наличие сторонних сертификатов и закрытых ключей и регистрирует такие сертификаты, чтобы отслеживать их срок действия. Поддерживается отслеживание сертификатов, выпущенных в Microsoft CA, КриптоПро УЦ 2.0, ViPNet УЦ 4, Валидата УЦ, Safetech CA, Aladdin Enterprise CA, Dogtag CA. Подробнее об отслеживаемых сертификатах
Записывать отслеживаемые сертификаты в журналы учета	Данные по отслеживаемым сертификатам попадают в журналы учета. Опция доступна, если в Мастере настройки в разделе **Общие функции** включена опция **Журнал учета устройств и сертификатов**.
Разрешить пользователю выбирать отслеживаемые сертификаты	При выпуске/обновлении устройства в Сервисе самообслуживания отображается список сторонних сертификатов. Пользователь может выбрать, какие сертификаты отслеживать.

Разрешения администратора

Сбрасывать PIN-код пользователя	В карточке устройства доступна опция **Сбросить PIN-код**. Если пользователь забыл или заблокировал PIN-код своего устройства, администратор может его сбросить.
Разблокировать устройство офлайн	В карточке устройства доступна опция **Разблокировать**. Администратор может разблокировать устройство в режиме офлайн (запрос-ответ), даже если между рабочей станцией пользователя и сервером Indeed CM нет соединения.
Проверять ответы на секретные вопросы	Чтобы администратор мог разблокировать устройство в режиме офлайн, он должен получить от пользователя верные ответы на секретные вопросы. Подробнее об офлайн-разблокировке
Отменять обновление устройства	В карточке устройства доступна опция **Отменить обновление**. Если пользователь начал обновлять устройство по ошибке, администратор может отменить обновление.

ПРИМЕЧАНИЕ

Убедитесь, что члены роли имеют привилегии для отмены обновления устройства, сброса PIN-кода и разблокировки устройства. Привилегии настраиваются в разделе **Конфигурация → Роли**.

Разрешения пользователя

Общие разрешения

Требовать установку ответов на секретные вопросы при входе в сервис самообслуживания	При входе в Сервис самообслуживания пользователь должен выбрать секретные вопросы и установить ответы на них. Чтобы иметь возможность аутентифицироваться в Сервисе удаленного самообслуживания, пользователь должен ввести ответы на секретные вопросы. Если опция выключена, форма настройки секретных вопросов и ответов не отображается при входе в Сервис самообслуживания. Пользователь может настроить секретные вопросы и ответы в любой момент.
Изменять ответы на секретные вопросы	Пользователь может редактировать ответы на секретные вопросы. Если опция выключена, редактировать ответы на секретные вопросы нельзя. Администратор может сбросить ответы на секретные вопросы, чтобы пользователь установил их заново.
Отображать привязку пользователя к КриптоПро УЦ	В Сервисе самообслуживания отображается информация о связи пользователя с каталогом КриптоПро УЦ 2.0.
Отображать привязку пользователя к КриптоПро DSS	В Сервисе самообслуживания отображается информация о связи пользователя с каталогом КриптоПро DSS.
Редактировать данные в форме проверки СМЭВ	Пользователь может редактировать данные в форме проверки СМЭВ при выпуске устройства. Если опция выключена, редактировать пользовательские данные в форме проверки СМЭВ может только администратор и оператор.
Выпускать AirCard	Пользователь может самостоятельно выпускать устройство AirCard. Выпуск устройств AirCard возможен только при настроенной интеграции с Indeed AirCard Enterprise.

Выпускать устройство КриптоПро DSS	Пользователь может самостоятельно выпускать устройства КриптоПро DSS. Если опция выключена, то выпускать устройство КриптоПро DSS может только администратор или оператор.

Действия при выпуске устройства

Назначать	Когда пользователь выпускает устройство в состоянии *Пустое* (не назначенное на пользователя), оно назначается автоматически. Если опция выключена, и устройство не назначено на пользователя, то он не сможет выпустить устройство в Сервисе самообслуживания.
Выбирать необязательные сертификаты при выпуске	При выпуске устройства отображается список шаблонов для необязательных сертификатов. Пользователь может выбрать, какие сертификаты записать на устройство. В поле **Сообщение пользователю** можно указать информацию, которая отобразится в виде предупреждения для пользователя.

Действия с выпущенным устройством

Просматривать содержимое	В карточке устройства в Сервисе самообслуживания доступна вкладка **Содержимое**, где отображаются все сертификаты, которые хранятся на устройстве.
Обновлять	В карточке устройства в Сервисе самообслуживания доступна опция **Обновить содержимое устройства**. Пользователь может обновить сертификаты, хранящиеся на устройстве, если их срок действия истек или истекает.

Выбирать необязательные сертификаты при обновлении	При обновлении устройства отображается список шаблонов для необязательных сертификатов. Пользователь может выбрать, какие сертификаты добавить или удалить. В поле **Сообщение пользователю** можно указать информацию, которая отобразится в виде предупреждения для пользователя.
Сбрасывать PIN-код пользователя	В карточке устройства в Сервисе самообслуживания доступна опция **Сбросить PIN-код устройства**. Если пользователь забыл или заблокировал PIN-код своего устройства, его можно сбросить.
Включать	В карточке устройства в Сервисе самообслуживания доступна опция **Включить устройство**, если устройство было выключено.
Выключать	В карточке устройства в Сервисе самообслуживания доступна опция **Временно выключить устройство**. Пользователь может выключить устройство, чтобы временно заблокировать доступ к нему.
Отзывать	В карточке устройства в Сервисе самообслуживания доступна опция **Сообщить о том, что устройство неисправно, утеряно или скомпрометировано**. Пользователь может отозвать устройство.
Очищать	После того как устройство было отозвано, в карточке устройства в Сервисе самообслуживания доступна опция **Очистить устройство**. Пользователь может очистить устройство – удалить его содержимое. После очистки устройство остается назначенным на пользователя.

Удалять устройства КриптоПро DSS	Пользователь может самостоятельно отзывать и удалять устройства DSS. Если опция выключена, то отзывать и удалять устройства DSS может только администратор и оператор.

Действия с документами

Использовать тип подписи	Пользователи могут подписывать документы в Сервисе самообслуживания подписью того типа, который выбрал администратор. Доступные типы подписи: • CMS • CAdES-BES • CAdES-T • CAdES-X Long Type 1 • CAdES-A Подробнее о поддержке электронной подписи
Удалять	Пользователи могут удалять документы в Сервисе самообслуживания в разделе **Ваши документы**.

Действия с СКЗИ

Просматривать	В Сервисе самообслуживания отображается раздел **Ваши СКЗИ** со списком экземпляров СКЗИ и обучающих курсов.
Отменять обучение	В Сервисе самообслуживания в разделе **Ваши СКЗИ** → **Обучающие курсы** доступна опция **Отменить обучение**. Пользователь может отменить обучение в состоянии *В процессе* и *Ожидание одобрения*. Подробнее об обучающих курсах СКЗИ

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	Устройство инициализируется перед выпуском. В результате инициализации все данные, хранящиеся на устройстве, удаляются. В процессе выпуска устройства вы можете включить или отключить инициализацию для конкретного устройства.

Опция	Описание
Устанавливать случайный PIN-код пользователя	В процессе выпуска устройства генерируется случайный PIN-код пользователя. Случайный PIN-код формируется из неповторяющихся символов. Настройте **Параметры генерации PIN-кода пользователя.** **Параметры генерации PIN-кода пользователя** 1. Выберите минимум одну группу символов, которые будут использованы при генерации PIN-кода: • цифры • буквы верхнего регистра • буквы нижнего регистра • специальные символы 2. При необходимости укажите до 16 запрещенных символов. 3. Задайте длину PIN-кода. Минимальная длина – 4 символа, максимальная – 31. Максимальная длина PIN-кода также зависит от выбранных групп символов. 4. Чтобы администратор мог посмотреть установленный PIN-код в карточке устройства в Консоли управления, включите опцию **Отображать установленный PIN-код администратору в Консоли управления**. 5. Чтобы пользователь мог посмотреть установленный PIN-код в карточке устройства в Сервисе самообслуживания, включите опцию **Отображать установленный PIN-код пользователю в Сервисе самообслуживания.**. Случайный PIN-код пользователя можно отправить пользователю или его руководителю в почтовом уведомлении.
Пользователь должен поменять PIN-код при первом входе	При первом подключении устройства к рабочей станции пользователь должен сменить PIN-код устройства. Опция поддерживается только для устройств eToken, IDPrime и Рутокен ЭЦП 3.0.

Опция	Описание
Блокировать устройство	Устройство заблокируется после выпуска. Перед использованием устройства пользователь должен его разблокировать и установить новый PIN-код.
Генерировать имя устройства автоматически	В качестве имени устройства можно использовать одно из значений из свойств пользователя – Общее имя, логин, фамилия, e-mail, подразделение, заданная строка. Выбранное значение автоматически подставляется в имя устройства в окне выпуска. При включенной опции **Разрешить редактирование имени устройства** пользователь может изменить имя устройства перед выпуском.
Требовать указания комментария к устройству	При выпуске устройства в Консоли управления администратор или оператор системы должен задать комментарий к устройству.
Требовать указания тегов к устройству	При выпуске устройства в Консоли управления администратор или оператор системы должен задать теги для устройства.
Отображать установленный пароль пользователя КриптоПро DSS администратору	При создании пользователя КриптоПро DSS и выпуске сертификата администратор может посмотреть пароль в карточке пользователя.
Отображать установленный пароль пользователя КриптоПро DSS пользователю	При создании пользователя КриптоПро DSS и выпуске сертификата пользователь может посмотреть пароль 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**

Инициализация устройства

Набор параметров инициализации зависит от типа устройства. Если в политике не настроены параметры инициализации для выпускаемых устройств, установятся параметры по умолчанию из файлов типов устройств, загруженных в разделе **Конфигурация** → Типы устройств.

Политики сложности PIN-кода, заданные в Indeed CM, распространяются на устройство при выпуске с инициализацией и сохраняются на устройстве до следующей инициализации.

Чтобы задать параметры инициализации устройств:

1. Нажмите **Добавить параметры инициализации**.
2. Выберите тип устройства и нажмите **ОК**.
3. Установите параметры инициализации.
4. Нажмите **Добавить**.

Параметры инициализации можно редактировать или удалить .

> **ПРИМЕЧАНИЕ**
>
> Если в разделах **Выпуск** и **Инициализация устройства** указаны разные значения длины PIN-кода, то в процессе выпуска устройства используется большее значение.

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 .

> **ПРИМЕЧАНИЕ**
>
> Если устройства были выпущены в рамках политики и отсутствуют в списке разрешенных, операции с устройствами остаются доступными.

Аутентификация

В разделе **Аутентификация** 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.

Секретные вопросы

Пользователи аутентифицируются по секретным вопросам в следующих случаях:

- Самостоятельная разблокировка устройства
- Выключение устройства без выполнения входа в ОС
- Доступ в Сервис удаленного самообслуживания
- Выполнение задачи по сбросу PIN-кода пользователя на клиентском агенте

Чтобы создать секретный вопрос:

1. Перейдите на вкладку **Секретные вопросы**.
2. Нажмите **Создать секретный вопрос**.
3. Введите вопрос.
4. Установите минимальную длину ответа. Значение по умолчанию – 3 символа.
5. Нажмите **Создать**.

> **ПРИМЕЧАНИЕ**
> Если секретные вопросы не созданы, то у пользователя нет возможности указать ответы на секретные вопросы в Сервисе самообслуживания.

Вопросы можно изменить или удалить .

> **ПРЕДУПРЕЖДЕНИЕ**
> Секретный вопрос можно удалить только в том случае, если его не использует ни один пользователь Indeed CM.

Агенты

Клиентский агент Indeed CM позволяет контролировать использование устройств на рабочих станциях пользователей.

В разделе **Агенты** можно задать настройки использования устройств, указать сообщения пользователю после успешного выполнения задач, определить доступные автоматические операции и задать PIN-коды администратора для разных типов устройств.

Настройки контроля использования устройства

Сообщение при нарушении условий привязки устройства к агенту	Введите сообщение, которое получит пользователь при подключении устройства к рабочей станции, не одобренной администратором.
Действие, выполняемое при нарушении условий привязки устройства к агенту	Выберите действие, которое выполнит агент, если пользователь подключит устройство к рабочей станции, не одобренной администратором: • запись события • блокировка пользовательской сессии • блокировка устройства • блокировка пользовательской сессии и устройства
Включить проверку привязки устройства к пользователю	При подключении устройства к рабочей станции агент проверит, принадлежит ли устройство пользователю, который выполняет подключение.
Сообщение при нарушении условий привязки устройства к пользователю	Введите сообщение, которое получит пользователь при подключении устройства к рабочей станции в сессии другого пользователя.

Действие, выполняемое при нарушении условий привязки устройства к пользователю	Выберите действие, которое выполнит агент, если пользователь подключит устройство к рабочей станции с сессией другого пользователя: • запись события • блокировка пользовательской сессии • блокировка устройства • блокировка пользовательской сессии и устройства
Таймаут до блокировки пользовательской сессии (сек.)	Установите период времени, после которого сессия пользователя будет заблокирована, если блокировка выбрана как действие, которое агент выполнит при нарушении правил использования устройства. Возможный интервал – от 0 до 5 секунд.

Сообщения пользователю

Агент может уведомить пользователей о выполнении следующих операций с устройствами:

- Блокировка устройства
- Смена PIN-кода администратора на устройстве
- Очистка устройства
- Обнаружение незарегистрированного устройства
- Разблокировка биометрической аутентификации на устройстве

По умолчанию сообщения не заданы и не выводятся пользователю. Чтобы сообщение приходило пользователю, введите текст в нужном поле. Когда пользователь подключит устройство к рабочей станции, сообщение отобразится во всплывающем окне.

Поведение

Задайте настройки, которые определяют доступные операции для агентов, установленных на рабочих станциях пользователей.

Подробнее об автоматических задачах агента Indeed CM

Добавлять устройство

Если к рабочей станции подключается устройство, не зарегистрированное в Indeed CM, агент добавляет его автоматически. Устройство привязывается к агенту рабочей станции, на которой оно добавлено.

При добавлении устройства агент проходит аутентификацию – вводит PIN-код администратора, чтобы получить доступ к устройству. Агент автоматически подставляет значение PIN-кода администратора, указанное для данного типа устройства в политике в разделе **Агенты** → **Поведение** → **PIN-коды администратора**.

> **ПРИМЕЧАНИЕ**
> Если PIN-код администратора не задан в политике, агент подставляет значение, указанное при редактировании типа устройства в разделе **Конфигурация** → **Типы устройств**.

Агент может добавить устройство и поменять PIN-код администратора или добавить устройство без PIN-кода администратора.

Добавить устройство и поменять PIN-код

Если предоставленное значение PIN-кода администратора верное, агент добавляет устройство и устанавливает новый PIN-код администратора.

PIN-код меняется на случайный или на указанный в опции **Устанавливать неслучайный PIN-код администратора** в разделе **Конфигурация** → **Типы устройств**.

Если PIN-код неверный, PIN-код администратора может заблокироваться. Чтобы не допустить блокировку PIN-кода администратора, не выключайте дополнительную опцию **Добавлять устройство без PIN-кода администратора, если предоставленный PIN-код недействителен**. В этом случае агент добавляет устройство в Indeed CM без PIN-кода администратора.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> У каждого устройства есть счетчик неудачных попыток ввода PIN-кода администратора. Например, на устройствах Рутокен по умолчанию установлено 10 попыток ввода PIN-кода администратора. Если на устройстве, которое добавляется в Indeed CM, осталась одна попытка, и введен неверный PIN-код, то PIN-код администратора заблокируется.
>
> На некоторых устройствах разблокировать PIN-код администратора невозможно. В случае блокировки PIN-кода администратора устройство можно инициализировать, но при этом все данные, хранящиеся на нем, удаляются.

Добавить устройство без PIN-кода

Если предоставленное значение PIN-кода администратора неверное, устройство можно добавить в Indeed CM без PIN-кода администратора. Для этого не выключайте дополнительную опцию **Добавлять устройство без PIN-кода администратора, если предоставленный PIN-код недействителен**.

Если предоставленное значение PIN-кода администратора верное, агент добавляет устройство и устанавливает новый PIN-код администратора.

Вы можете установить PIN-код администратора с помощью следующих настроек:

- Вручную в карточке устройства, если в разделе **Конфигурация** → **Роли** администратору назначена привилегия **Задание PIN-кода администратора**.
- Автоматически при выпуске устройства с инициализацией.
- С помощью задачи **Сменить PIN-код администратора**, которую выполняет агент, установленный на рабочей станции пользователя.

Назначать устройство

Агент автоматически назначит устройство на пользователя при добавлении. Устройство назначится на пользователя, в активной сессии которого оно добавляется.

Назначенные устройства можно выпустить автоматически с помощью опции **Выпускать назначенное устройство**.

Выпускать пустое устройство

Опция подходит для случаев, когда вам необходимо массово выпустить много новых устройств.

Если к рабочей станции подключить устройство в состоянии *Пустое*, т.е. не назначенное пользователю, то агент выпускает такое устройство. Настройки выпуска устройства определяет политика, действующая на пользователя.

После того как все устройства выпустятся, отключите опцию **Выпускать пустое устройство**. Это необходимо, чтобы устройство не выпускалось повторно в процессе своего жизненного цикла, например, после изъятия.

> **ПОДСКАЗКА**
> Рекомендуем настроить автоматический выпуск только назначенных устройств с помощью опции **Выпускать назначенное устройство**.

Выпускать назначенное устройство

Если пользователь подключает устройство к рабочей станции, агент проверяет, назначено ли это устройство этому пользователю, и выпускает такое устройство автоматически.

Настройки выпуска устройства определяет политика, действующая на пользователя.

Продолжать выпуск устройства

Агент автоматически продолжает выпуск устройства в состоянии *В ожидании*.

Устройство переходит в состояние *В ожидании*, если выпуск устройства приостановлен для проверки документов. Агент продолжает выпуск, если администратор одобрил документы пользователя.

Подробнее о контроле выпуска устройств

Продолжать обновление устройства

Агент автоматически продолжает обновление устройства в состоянии *В ожидании*.

Устройство переходит в состояние *В ожидании*, если обновление устройства приостановлено для проверки документов. Агент продолжает обновление, если администратор одобрил документы пользователя.

Подробнее о контроле обновления устройств

Запрашивать смену PIN-кода пользователя по истечении (дней)

Укажите срок действия PIN-кода пользователя. По истечении этого времени служба Card Monitor создает задачу **Смена PIN-кода пользователя** на агенте, к которому привязано устройство. Когда пользователь подключает устройство к рабочей станции, агент открывает окно смены PIN-кода.

> **ПРИМЕЧАНИЕ**
> Задача создается только для устройств в состоянии *Выпущено*.

PIN-коды администратора

Задайте PIN-коды администратора для типов используемых устройств. При добавлении устройства агент подставляет PIN-код, указанный для типа устройства, в качестве текущего PIN-кода администратора.

Чтобы добавить PIN-код администратора:

1. Нажмите **Добавить PIN-код администратора**.
2. Выберите тип устройства и нажмите **ОК**.
3. Введите значение в поле **PIN-код администратора**.
4. Нажмите **Добавить**.

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

Доступны следующие настройки принтера смарт-карт:

Включить поддержку принтера смарт-карт	При выпуске устройства доступен выбор считывателя, к которому подключена смарт-карта – считыватель рабочей станции или считыватель принтера.
Читать RFID-метку устройства	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	При выпуске устройства через принтер на нем напечатается изображение или текст по загруженному шаблону печати.

Чтобы загрузить шаблон печати:

1. Перейдите на вкладку **Шаблон устройства** и нажмите **Загрузить шаблон устройства**.
2. Выберите файл и нажмите **Загрузить**.

Шаблон представляет собой файл XML, который содержащий данные о том, что необходимо выводить на печать.

Чтобы получить файл шаблона печати, обратитесь в службу технической поддержки компании Индид.

Уведомления

В разделе **Уведомления** в параметрах политики вы можете настроить отправку уведомлений на почту администраторам и пользователям о событиях, которые относятся к этой политике – локальных событиях.

События администратора

- 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 документа
- Добавление AirCard к компьютеру
- Добавление СКЗИ
- Задача выполнена
- Замена устройства
- Замена устройства ожидает решения
- Изменение документа
- 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 биометрии
- 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 документа
- 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 биометрии
- Разблокировка пользователя

- Разблокировка устройства
- Регистрация биометрии
- Сброс ответов на секретные вопросы
- Сброс пароля пользователя
- Сброс PIN-кода
- Содержимое устройства КриптоПро DSS истекает
- Создание кода подключения AirCard к компьютеру
- Удаление документа
- Удаление AirCard от компьютера
- Удаление устройства КриптоПро DSS
- Уничтожение/изъятие СКЗИ
- Управляемые сертификаты истекают

События пользователя

- Атрибуты пользователя были изменены
- Аутентификация
- Блокировка пользователя
- Включение устройства
- Включение устройства КриптоПро DSS
- Выключение устройства
- Выключение устройства КриптоПро DSS
- Выпуск сертификата
- Выпуск сертификата КриптоПро DSS
- Выпуск устройства
- Выпуск устройства КриптоПро DSS
- Выпуск устройства КриптоПро DSS ожидает решения
- Выпуск устройства ожидает решения
- Добавление документа
- Добавление AirCard к компьютеру
- Добавление СКЗИ
- Замена устройства
- Замена устройства ожидает решения
- Изменение документа
- Изменение PIN-кода
- Изменение ответов на секретные вопросы
- Назначение СКЗИ
- Назначение устройства
- Обновление биометрии
- 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 документа
- 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 биометрии
- Разблокировка пользователя
- Разблокировка устройства
- Регистрация биометрии
- 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 документа
- Удаление AirCard от компьютера
- Удаление устройства КриптоПро DSS

- Уничтожение/изъятие СКЗИ
- Установка пароля пользователя КриптоПро DSS
- Установка PIN-кода

Чтобы настроить отправку уведомлений:

1. Настройте почтовый сервер.
2. Определите группы получателей уведомлений.
3. Создайте уведомления о событиях для администраторов и пользователей.
4. При необходимости настройте индивидуальный шаблон уведомления для каждого события.

Почтовый сервер

Для настройки почтового сервера можно использовать глобальные настройки или настроить подключение для политики.

Чтобы настроить подключение для политики:

1. Выберите опцию **Настроить подключение**.
2. Укажите настройки почтового сервера и нажмите **Сохранить**.
3. Нажмите **Отправить тестовое сообщение**, чтобы проверить работу почтового сервера.
4. Укажите адрес электронной почты получателя и нажмите **Отправить**.

Если тестовое сообщение не пришло, проверьте настройки почтового сервера и отправьте сообщение повторно.

Группы получателей

Настройте группы получателей уведомлений администраторов.

Для глобальных администраторов можно выбрать общие группы получателей, настроенные в разделе **Конфигурация** → **Уведомления** → Группы получателей. Для локальных администраторов можно создать отдельные группы получателей уведомлений о событиях, которые относятся к определенной политике.

Чтобы создать группу получателей:

1. Нажмите **Создать группу**.
2. Укажите имя группы.
3. Введите адреса получателей.
4. Нажмите **Создать**.

Группы получателей можно изменить  или удалить  .

> ⚠ **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. В выпадающем списке **Событие** выберите событие, о котором необходимо уведомить администратора.
3. Укажите тип события – информация, ошибка или предупреждение.
4. Выберите получателей:
   - **Группа получателей** – группа, созданная в разделе Группы получателей
   - **Группа безопасности** – группа безопасности в каталоге пользователей
5. Нажмите **Создать**.

Периодичность повторной отправки (в днях)

В поле **Периодичность повторной отправки (в днях)** можно указать интервал времени до повторной отправки уведомления.

Поле доступно для следующих событий:

- Атрибуты пользователя были изменены
- Общие сертификаты истекают
- Одобрение выпуска устройства
- Одобрение выпуска устройства КриптоПро DSS
- Одобрение замены устройства
- Одобрение обновления устройства
- Одобрение обновления устройства КриптоПро DSS
- Отклонение выпуска устройства
- Отклонение выпуска устройства КриптоПро DSS
- Отклонение замены устройства
- Отклонение обновления устройства
- Отклонение обновления устройства КриптоПро DSS
- Отслеживаемые сертификаты истекают
- Политика была обновлена
- Политика пользователя была изменена
- Политика пользователя устройства КриптоПро DSS была изменена
- Политика устройства КриптоПро DSS была обновлена
- Управляемые сертификаты истекают
- Управляемые сертификаты КриптоПро DSS истекают

Уведомления можно изменить или удалить .

Уведомления пользователя

Настройте почтовые уведомления для пользователей Indeed CM. Убедитесь, что в свойствах учетных записей пользователей в каталоге указан адрес электронной почты.

1. Нажмите **Создать уведомление**.

2. В выпадающем списке **Событие** выберите событие, о котором необходимо уведомить пользователя.
3. Укажите тип события – информация, ошибка или предупреждение.
4. Чтобы отправить копию уведомления руководителю сотрудника, включите опцию **Отправлять копию менеджеру**. Опция доступна для пользователей, расположенных в Active Directory. Адрес электронной почты руководителя указывается на вкладке **Организация** (Organization) свойств пользователя Active Directory в разделе **Руководитель** (Manager).
5. Нажмите **Создать**.

Периодичность повторной отправки (в днях)

В поле **Периодичность повторной отправки (в днях)** можно указать таймаут до отправки повторного уведомления.

Поле доступно для следующих событий:

- Атрибуты пользователя были изменены
- Общие сертификаты истекают
- Одобрение выпуска устройства
- Одобрение выпуска устройства КриптоПро DSS
- Одобрение замены устройства
- Одобрение обновления устройства
- Одобрение обновления устройства КриптоПро DSS
- Отклонение выпуска устройства
- Отклонение выпуска устройства КриптоПро DSS
- Отклонение замены устройства
- Отклонение обновления устройства
- Отклонение обновления устройства КриптоПро DSS
- Отслеживаемые сертификаты истекают
- Политика была обновлена
- Политика пользователя была изменена
- Политика пользователя устройства КриптоПро DSS была изменена
- Политика устройства КриптоПро DSS была обновлена
- Управляемые сертификаты истекают
- Управляемые сертификаты КриптоПро DSS истекают

Уведомления можно изменить или удалить .

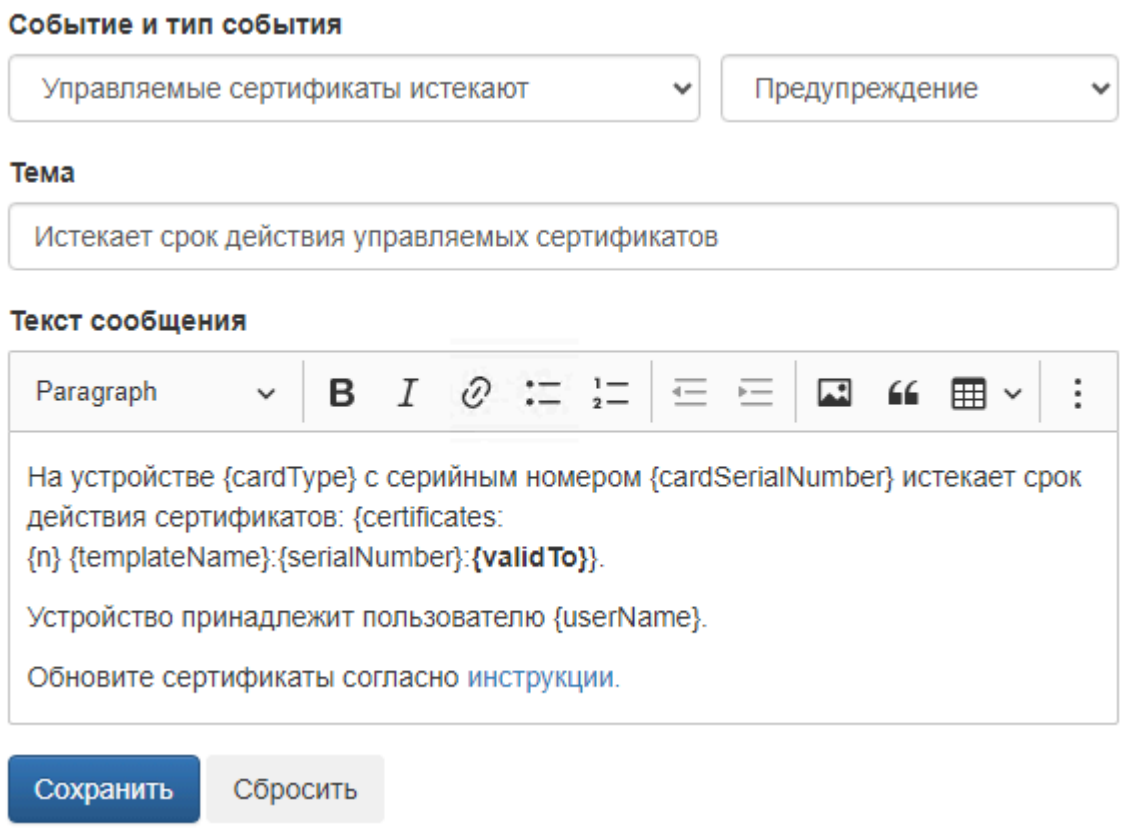
Шаблоны уведомлений

На вкладках **Шаблоны администратора** и **Шаблоны пользователя** можно настроить шаблоны почтовых уведомлений. Используйте базовые шаблоны, установленные по умолчанию, или редактируйте шаблоны, чтобы создать персонализированные уведомления.

Для каждого события в базовый шаблон встроен набор объектов с параметрами, значения которых подставляются в текст уведомления при отправке. В тексте уведомления можно использовать только те параметры, которые встроены в шаблон – новые добавлять нельзя. Вы можете удалить параметры, которые вам не нужны.

Чтобы создать персонализированное уведомление, внесите изменения и нажмите **Сохранить**. Чтобы вернуться к базовому шаблону, нажмите **Сбросить**.

Пример персонализированного шаблона уведомления для администратора



Пример персонализированного шаблона уведомления для пользователя

Событие и тип события

Установка PIN-кода | Информация

Тема

Установка PIN-кода

Текст сообщения

Paragraph

Уважаемый {userName}!

Ваше персональное устройство аутентификации **{cardType}** с серийным номером **{cardSerialNumber}** успешно выпущено в системе Indeed Certificate Manager.

PIN-код устройства: {userPin}

Никому не передавайте устройство и не сообщайте PIN-код!

Для получения дополнительной информации обратитесь к своему руководителю.

Инициатор: {initiator}

Сохранить | Сбросить

Лицензии

Подробнее о лицензиях Indeed Certificate Manager можно узнать в разделе Лицензирование.

Чтобы получить лицензии:

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 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:

1. Нажмите **Добавить лицензию**.
2. Выберите файл лицензии.
3. Нажмите **Добавить**.

Чтобы удалить лицензию, выберите ее в списке и нажмите ✖ .

Типы устройств

Indeed Certificate Manager поддерживает работу с USB-токенами, смарт-картами и комбинированными устройствами.

Список устройств, которые поддерживаются в Indeed CM

> **ПРИМЕЧАНИЕ**
>
> Поддерживайте список типов и моделей устройств в Indeed CM в актуальном состоянии. Если в вашей организации появились новые типы и модели устройств, или какие-то модели больше не используются, внесите изменения в Indeed CM.

В разделе **Конфигурация** → **Типы устройств** вы можете управлять настройками каждого типа устройств:

- Просмотреть PIN-коды администратора и пользователя, установленные на устройстве по умолчанию
- Настроить новые PIN-коды по умолчанию в соответствии с политиками безопасности, принятыми в вашей организации
- Указать новый PIN-код администратора, который автоматически установится вместо PIN-кода по умолчанию при добавлении устройства в Indeed CM
- Настроить параметры инициализации устройства при добавлении
- Настроить параметры моделей устройств

> **ПОДСКАЗКА**
>
> Файлы типов устройств находятся в дистрибутиве сервера Indeed CM в каталоге *\Misc\CardTypes*.

Список файлов для типов и моделей устройств

Производитель	Модель устройства	Файл типа устройства
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 JaCarta-3 PKI/ГОСТ JaCarta-3 SE	JaCarta-pin.xml

Производитель	Модель устройства	Файл типа устройства
Компания «Актив»	Рутокен Lite 1000 Рутокен Lite 1010	RutokenLite.xml
	Смарт-карта Рутокен Lite 1000	RutokenLiteSC.xml
	Рутокен S	RutokenS.xml
	Рутокен PKI 1800 Рутокен ЭЦП Рутокен ЭЦП 2.0 2000 Рутокен ЭЦП 2.0 2100 Рутокен ЭЦП 2.0 3000 Рутокен ЭЦП 2.0 Flash 4500 Рутокен ЭЦП 2.0 Flash 4500 Рутокен ЭЦП 3.0 NFC 3100 Рутокен ЭЦП 3.0 3120 Рутокен ЭЦП 3.0 3150 Рутокен ЭЦП 3.0 3220 Рутокен ЭЦП 3.0 3250 БИО	RutokenECP.xml
	Смарт-карты: Рутокен PKI 1800 Рутокен ЭЦП 2.0 2100	RutokenECPSC.xml
	Смарт-карты: Рутокен ЭЦП 3.0 NFC 3100 Рутокен ЭЦП 3.0 3100 Рутокен ЭЦП 3.0 3100 SAM 3100	RutokenECPNFCSC.xml
	Рутокен 2151	Rutoken2151.xml
	Смарт-карта Рутокен 2151	Rutoken2151SC.xml
Компания Индид	AirCard	AirCard.xml
ACS	ACOS5-64	Acos5-64.xml

Производитель	Модель устройства	Файл типа устройства
Avest	Avest Key 256A	AvestKey-256-A.xml
Bit4id	ID-One Cosmo	Bit4Id.xml
CRYPTAS	TicTok V2	TicTok_v2.xml
	TicTok V3	TicTok_v3.xml
Cryptovision	ePasslet Suite v3.0, JCOP V3.0	cv-ePassletSuite3.0-JCOP3.0.xml
Feitian	ePass2003 (A1+, A2) BioPass2003	ePass2003.xml
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

Производитель	Модель устройства	Файл типа устройства
Microsoft	Реестр Локального компьютера Реестр Пользователя	Registry.xml
	TPM Virtual Smart Card (Microsoft VSC)	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
	SafeNet eToken PRO Java 72K OS755 SafeNet eToken 5105 SafeNet eToken 5110 IDCore30B eToken 1.7.7	eTokenProJava72K.xml
	SafeNet eToken 5300 SafeNet eToken Fusion SafeNet eToken Fusion CC	eToken 5300.xml
	IDPrime MD 830 FIPS IDPrime MD 830B FIPS IDPrime MD 840B IDPrime 940 IDPrime 940B IDPrime MD 3810 IDPrime MD 3811 IDPrime 3930 IDPrime 3940	IDPrimeMD T=0.xml
	SafeNet eToken 5110 CC (940)	IDPrimeMD T=1.xml
	IDPrime 930 IDPrime 930nc	IDPrimeMD v2 T=0.xml
	IDPrime 3940 FIDO	IDPrimeMD Fido T=1.xml
Yubico	YubiKey 5 Series	YubiKey5.xml

Добавление типа устройства

1. В разделе **Конфигурация** → **Типы устройств** нажмите **Добавить тип устройства** и выберите файл.
   Файлы типов устройств находятся по пути *\Misc\CardTypes* в дистрибутиве сервера Indeed CM.
2. (Опционально) Чтобы заменить файл типа устройства, включите опцию **Заменить существующий**.
3. Нажмите **Добавить**.

Удаление типа устройства

1. В разделе **Конфигурация** → **Типы устройств** выберите тип устройства в списке и нажмите ✖ .
2. Нажмите **Удалить**.

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

Редактирование типов устройств

Файл типа устройства содержит PIN-коды администратора и пользователя, установленные на устройстве по умолчанию, в том числе и для ГОСТ-области. Наличие ГОСТ-области зависит от производителя и модели устройства.

> **ПРИМЕЧАНИЕ**
> При удалении устройства из Indeed CM PIN-код администратора сбрасывается на значение, указанное в файле типа устройства.
> При изъятии устройства у пользователя PIN-код пользователя сбрасывается на значение, указанное в файле типа устройства.

Чтобы редактировать тип устройства, в разделе **Конфигурация** → **Типы устройств** нажмите ✎ напротив нужного типа.

Просмотр и изменение PIN-кодов администратора и пользователя

Чтобы просмотреть PIN-коды администратора и пользователя, установленные на устройстве по умолчанию, нажмите 👁.

Чтобы настроить новые PIN-коды по умолчанию, введите новые значения и нажмите **Сохранить**.

Настройки добавления устройств

Indeed CM позволяет установить отдельные параметры для добавления устройств различных типов.

Инициализировать устройство при добавлении	Если опция включена, то при добавлении устройства устанавливаются следующие настройки: • Устройство очищается – удаляются сертификаты, добавленные с помощью Indeed CM • Имя устройства меняется на Empty • PIN-код администратора меняется на случайное значение, известное только Indeed CM, или на PIN-код, указанный в опции **Установить неслучайный PIN-код администратора** • Устанавливается 3 попытки ввода PIN-кода администратора до его блокировки • PIN-код пользователя, минимальная длина PIN-кода и количество попыток ввода до блокировки меняются на значения, указанные в файле типа устройства
Устанавливать неслучайный PIN-код администратора	Если опция включена, то при добавлении устройства PIN-код администратора меняется на значение, указанное в поле внутри опции. Если опция выключена, то при добавлении устройства PIN-код администратора меняется на случайное значение, известное только Indeed CM.

Устанавливать неслучайный PIN-код администратора (ГОСТ)	Если опция включена, то при добавлении устройства PIN-код администратора для ГОСТ-области меняется на значение, указанное в поле внутри опции. Если опция выключена, то при добавлении устройства PIN-код администратора для ГОСТ-области меняется на случайное значение, известное только Indeed CM.

> **ИНИЦИАЛИЗИРОВАТЬ УСТРОЙСТВО ETOKEN**
>
> Устройства eToken поддерживают инициализацию с любым состоянием и значением PIN-кода администратора.

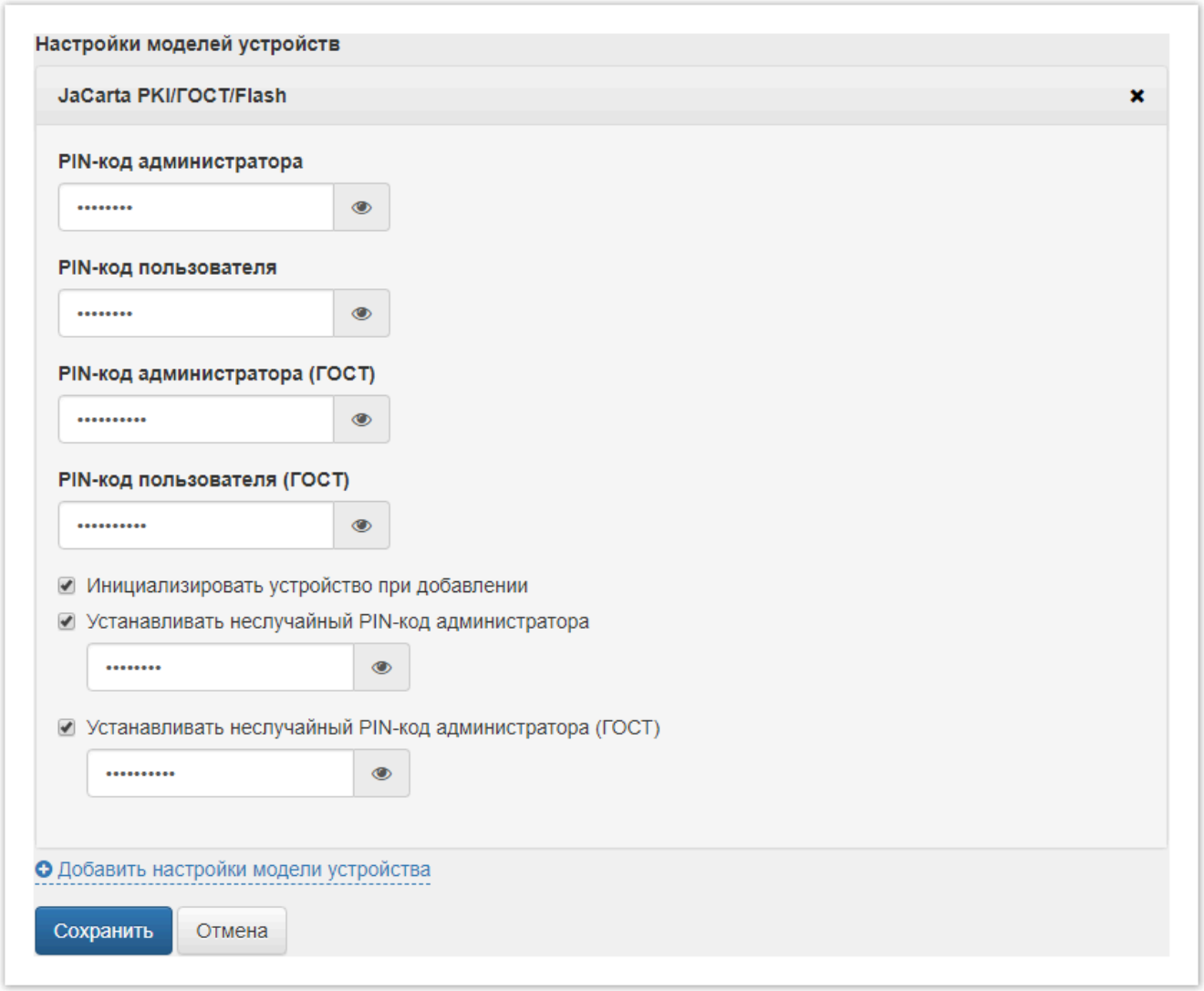
Настройки моделей устройств

Indeed CM позволяет установить отдельные параметры для добавления устройств различных моделей. Функциональность поддерживается для устройств Рутокен, JaCarta, eToken PRO Java 72K и IDPrime MD.

> **ПРИМЕЧАНИЕ**
>
> Если модель устройства не определилась или настройки моделей не заданы, то устройство настраивается по умолчанию.

Чтобы добавить настройки моделей устройств:

1. Выберите нужный тип устройства в списке и нажмите .
2. Нажмите **Добавить настройки модели устройства** в нижней части окна редактирования.
3. Выберите нужную модель в выпадающем списке и нажмите **Добавить**. Откроются настройки модели.
4. Установите параметры инициализации и PIN-кодов и нажмите **Сохранить**.



Настройки PIN-кодов для моделей устройств JaCarta с приложением ГОСТ

В зависимости от версии приложения ГОСТ (апплета) на моделях устройств JaCarta различаются PIN-коды по умолчанию.

Версия приложения ГОСТ	PIN-код пользователя	PIN-код администратора	PUK-код
2.5.3 – 2.5.9 (апплет Криптотокен 2 ЭП)	1234567890	—	0987654321
2.5.13 и выше (апплет ВПО JaCarta-3)	1234567890	0987654321	—

⚠ **ПРЕДУПРЕЖДЕНИЕ**

На моделях устройств JaCarta с версией приложения ГОСТ 2.5.3 – 2.5.9 (апплет Криптотокен 2 ЭП) могут быть установлены PIN-коды «наоборот»:

- PIN-код пользователя: 0987654321
- PIN-код администратора: 1234567890

Версию приложения ГОСТ можно узнать в ПК «Единый клиент JaCarta».

Подробнее об управлении устройствами JaCarta с приложением ГОСТ

Организационная структура

Устройства в Indeed CM 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.

Предварительные настройки

Чтобы разрешить доступ к разделу **Организационная структура**:

1. Запустите Мастер настройки и перейдите в раздел **Общие функции**.
2. Включите опцию **Организационная структура**.
3. Откройте Консоль управления и перейдите в раздел **Конфигурация** → **Роли**.
4. Предоставьте членам роли привилегии для работы с организационной структурой: просмотр и изменение организационной структуры.

Управление

Чтобы добавить новый узел:

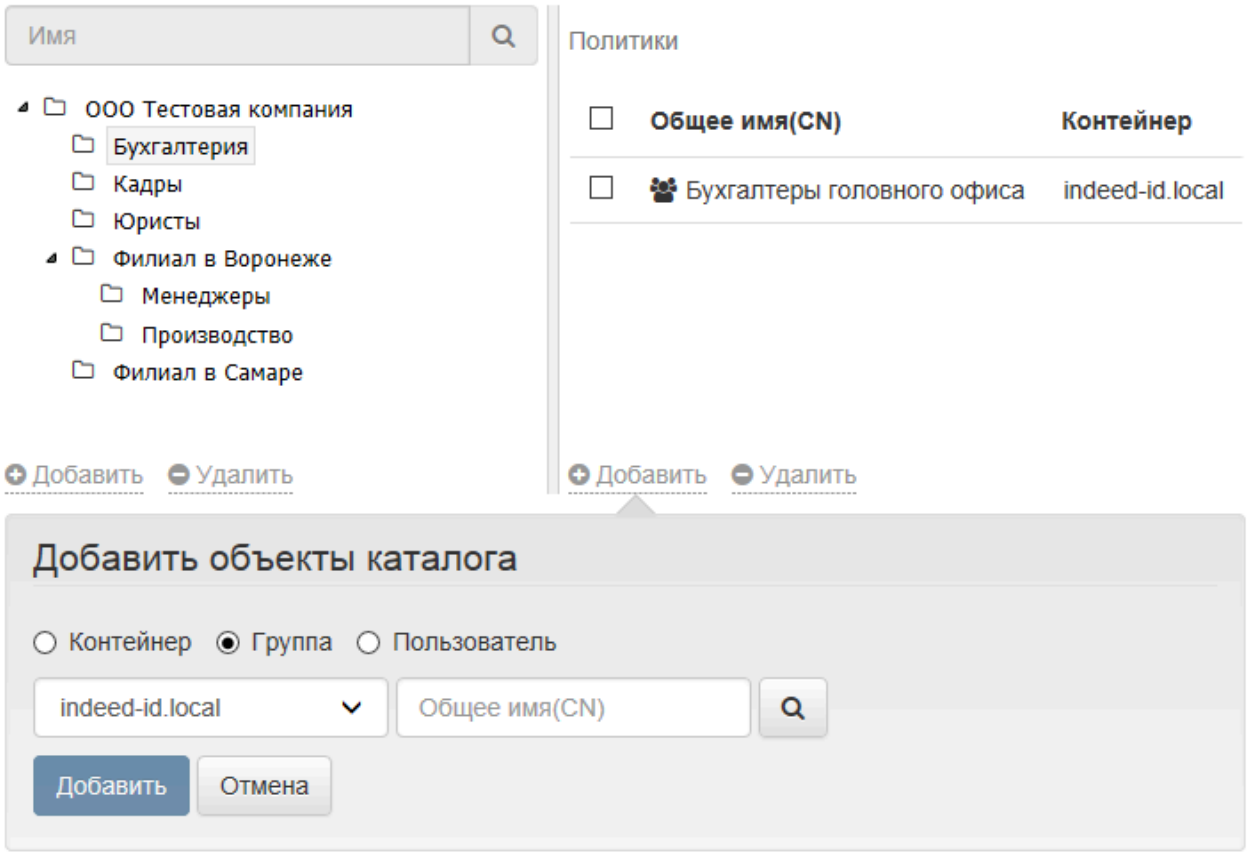
1. Нажмите **Добавить**.
2. Введите имя узла.

Чтобы удалить узел:

1. Выберите узел.
2. Нажмите **Удалить**.

Чтобы добавить объекты в узел, в правой части окна редактирования организационной структуры нажмите **Добавить**. При создании структуры используются объекты каталога пользователей.

Пример организационной структуры



Роли

Ролевая модель в Indeed CM позволяет гибко управлять доступом администраторов и операторов к функциям Консоли управления. Каждой роли назначается набор привилегий, которые определяют, какие действия могут выполнять члены роли.

Роли и привилегии настраиваются в разделе **Конфигурация** → **Роли**. Пока роли не назначены, все действия запрещены.

Предварительные настройки

При первоначальной настройке Indeed CM доступ к Консоли управления есть только у специальной учетной записи администратора ролей. Администратор ролей назначается в Мастере настройки в разделе **Контроль доступа** → Администратор ролей.

> **ПРИМЕЧАНИЕ**
> Учетная запись администратора ролей должна иметь атрибут User Principal Name (UPN) и входить в каталог пользователей.

Для первоначальной настройки прав доступа используйте администратора ролей, чтобы предоставить права управления Indeed CM другим пользователям:

1. Войдите в Консоль управления под учетной записью администратора ролей.
2. Перейдите в раздел **Конфигурация** → **Роли**.
3. Нажмите ✎ напротив роли **Администратор**.
4. В параметре **Состав роли** нажмите **Добавить**.
5. Добавьте всех сотрудников, которые должны иметь полный доступ к функциям Консоли управления, в том числе к управлению ролями. Выберите:
   - **Группа**, чтобы добавить группу пользователей. В поисковой строке введите **Общее имя** группы, чтобы найти группу пользователей.
   - **Пользователь**, чтобы добавить определенного пользователя. В поисковой строке введите **Общее имя** или **Логин**, чтобы найти пользователя.
6. Нажмите **Сохранить**.

Все пользователи с ролью **Администратор** могут управлять ролевой моделью Indeed CM – создавать новые роли, назначать привилегии и добавлять пользователей в роли.

Роли по умолчанию

По умолчанию в Indeed CM установлены роли **Администратор** и **Оператор**.

Администратор	• Максимальный набор привилегий • Доступ ко всем разделам Роль предназначена для специалистов, которые отвечают за конфигурацию и общее функционирование Indeed CM.
Оператор	• Ограниченный набор привилегий • Нет доступа к изменению параметров в разделе **Конфигурация** Роль предназначена для специалистов, которые отвечают за управление объектами Indeed CM.

Список привилегий

Привилегия	Администратор	Оператор
Пользователь		
Поиск пользователей	✓	✓
Просмотр пользователя	✓	✓
Разблокировка пользователя	✓	✓
Сброс ответов на секретные вопросы	✓	✓
Загрузка фото	✓	✓
Сброс пароля пользователя	✓	✓
Просмотр комментария о пользователе	✓	✓
Изменение комментария о пользователе	✓	✓
Одобрение данных запроса СМЭВ	✓	✓
Назначение пользователя УЦ	✓	✓
Назначение обучающих курсов	✓	✗
Завершение обучающих курсов	✓	✗
Одобрение завершения обучающих курсов	✓	✗
Отмена обучающих курсов	✓	✗

Привилегия	Администратор	Оператор
Конфигурация		
Просмотр политики	✓	✗
Создание политики	✓	✗
Изменение политики	✓	✗
Удаление политики	✓	✗
Просмотр назначения политики	✓	✗
Создание назначения политики	✓	✗
Изменение назначения политики	✓	✗
Удаление назначения политики	✓	✗
Просмотр лицензии	✓	✗
Добавление лицензии	✓	✗
Удаление лицензии	✓	✗
Просмотр типа устройства	✓	✗
Добавление типа устройства	✓	✗
Изменение типа устройства	✓	✗
Удаление типа устройства	✓	✗

Привилегия	Администратор	Оператор
Просмотр организационной структуры	✓	✗
Изменение организационной структуры	✓	✗
Просмотр роли	✓	✗
Создание роли	✓	✗
Изменение роли	✓	✗
Удаление роли	✓	✗
Просмотр тега	✓	✗
Создание тега	✓	✗
Изменение тега	✓	✗
Удаление тега	✓	✗
Просмотр шаблона печати	✓	✗
Добавление шаблона печати	✓	✗
Изменение шаблона печати	✓	✗
Удаление шаблона печати	✓	✗
Просмотр типа СКЗИ	✓	✗
Добавление типа СКЗИ	✓	✗

Привилегия	Администратор	Оператор
Изменение типа СКЗИ	✓	✗
Удаление типа СКЗИ	✓	✗
Просмотр шаблона нормативных документов	✓	✗
Изменение шаблона нормативных документов	✓	✗
Просмотр обучающих курсов	✓	✗
Создание обучающих курсов	✓	✗
Изменение обучающих курсов	✓	✗
Удаление обучающих курсов	✓	✗
Просмотр настроек почтового сервера	✓	✗
Редактирование настроек почтового сервера	✓	✗
Просмотр групп получателей	✓	✗
Добавление групп получателей	✓	✗
Изменение групп получателей	✓	✗
Удаление групп получателей	✓	✗
Просмотр уведомлений администратора	✓	✗
Добавление уведомлений администратора	✓	✗

Привилегия	Администратор	Оператор
Изменение уведомлений администратора	✓	✗
Удаление уведомлений администратора	✓	✗
Просмотр шаблонов администратора	✓	✗
Изменение шаблонов администратора	✓	✗
Просмотр справочника журнала учета	✓	✗
Создание справочника журнала учета	✓	✗
Изменение справочника журнала учета	✓	✗
Удаление справочника журнала учета	✓	✗
Просмотр шаблона журнала учета	✓	✗
Создание шаблона журнала учета	✓	✗
Изменение шаблона журнала учета	✓	✗
Удаление шаблона журнала учета	✓	✗
Журнал событий		
Просмотр журнала событий	✓	✓
Сводная информация		✓
Просмотр сводной информации	✓	✓

Привилегия	Администратор	Оператор
Устройства		
Просмотр репозитория устройств	✓	✓
Просмотр информации об устройстве	✓	✓
Добавление устройства	✓	✓
Изменение комментария устройства	✓	✓
Изменение тегов устройства	✓	✓
Просмотр PIN-кода администратора	✓	✗
Изменение PIN-кода администратора	✓	✗
Задание PIN-кода администратора	✓	✗
Инициализация устройства	✓	✓
Назначение устройства	✓	✓
Выпуск устройства	✓	✓
Включение устройства	✓	✓
Выключение устройства	✓	✓
Обновление устройства	✓	✓
Отмена обновления устройства	✓	✓

Привилегия	Администратор	Оператор
Замена устройства	✓	✓
Сброс PIN-кода	✓	✗
Изменение PIN-кода	✓	✗
Блокировка устройства	✓	✗
Разблокировка устройства	✓	✓
Разблокировка биометрии	✓	✓
Регистрация биометрии	✓	✓
Обновление биометрии	✓	✓
Печать устройства	✓	✓
Отзыв устройства	✓	✓
Очистка устройства	✓	✓
Отмена назначения устройства	✓	✓
Удаление устройства	✓	✓
Сертификаты		
Просмотр репозитория сертификатов	✓	✓
Устройства AirCard		

Привилегия	Администратор	Оператор
Изменение привязки AirCard	✓	✓
Удаление AirCard	✓	✓
Агенты		
Просмотр репозитория агентов	✓	✓
Изменение привязки устройства к агенту	✓	✓
Обновление статуса агента	✓	✓
Удаление агента	✓	
Обновление имени агента	✓	✓
Обновление комментария агента	✓	✓
Удаление задачи	✓	✓
СКЗИ		
Просмотр репозитория СКЗИ	✓	✓
Добавление СКЗИ	✓	✓
Назначение СКЗИ	✓	✓
Обновление СКЗИ	✓	✓
Уничтожение/изъятие СКЗИ	✓	✓
Документы		

Привилегия	Администратор	Оператор
Просмотр репозитория документов	✓	✓
Добавление документа	✓	✓
Изменение документа	✓	✓
Удаление документа	✓	✓
Одобрение документа	✓	✓
Журналы учета		
Просмотр журнала учета	✓	✓
Добавление записи в журнал учета	✓	✓
Изменение записи в журнале учета	✓	✓
Удаление записи из журнала учета	✓	✓

Типы роли

Глобальная	Права распространяются на все политики использования устройств.
Локальная	Права распространяются только на конкретные политики, к которым эта роль привязана. Члены локальной роли могут управлять только теми пользователями, которые попадают в область действия определенной политики.

ПРИМЕЧАНИЕ

Тип роли нельзя изменить после того, как роль уже создана.

Создание роли

Глобальная

Чтобы создать глобальную роль:

1. В разделе **Роли** нажмите **Создать роль**.
2. Укажите имя роли.
3. Выберите тип роли **Глобальная**.
4. Чтобы добавить членов роли, в параметре **Состав роли** нажмите **Добавить**.
5. Выберите:
   - **Группа**, чтобы добавить группу пользователей. В поисковой строке введите **Общее имя** группы, чтобы найти группу пользователей.
   - **Пользователь**, чтобы добавить определенного пользователя. В поисковой строке введите **Общее имя** или **Логин**, чтобы найти пользователя.
6. Нажмите **Добавить**.
7. Назначьте привилегии членам роли.
8. Нажмите **Создать**.

Локальная

Чтобы создать локальную роль:

1. В разделе **Роли** нажмите **Создать роль**.
2. Укажите имя роли.
3. Выберите тип роли **Локальная**.
4. Назначьте привилегии членам роли.
5. Нажмите **Создать**.
6. Чтобы добавить членов роли, перейдите в раздел **Конфигурация** → **Назначения политик**.
7. Нажмите напротив политики, для которой вы хотите предоставить доступ членам локальной роли.
8. В параметре **Роли** нажмите **Добавить роль**.
9. Выберите созданную локальную роль и нажмите **Добавить**.
10. Нажмите **Сохранить**.

Подробнее о назначении политик

Роль для 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 назначьте следующие привилегии:

- Выключение устройства
- Обновление устройства
- Отмена обновления устройства
- Отзыв устройства
- Очистка устройства
- Отмена назначения устройства
- Удаление устройства
- Удаление агента
- Удаление задачи
- Удаление записи из журнала учета

Если в Indeed CM настроена интеграция с КриптоПро DSS и Indeed AirCard Enterprise, назначьте следующие привилегии:

- Выключение устройства КриптоПро DSS
- Обновление устройства КриптоПро DSS
- Отмена обновления устройства КриптоПро DSS
- Отзыв устройства КриптоПро DSS
- Удаление устройства КриптоПро DSS
- Удаление AirCard

Подробнее о работе службы Card Monitor

Card Monitor – служба для контроля использования устройств, которая 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

Теги

Теги необходимы для более гибкого учета устройств в организации и помогают при поиске устройств в Консоли управления в разделе **Устройства** → **Расширенный поиск**.

Чтобы создать тег:

1. Нажмите **Создать тег**.
2. Укажите имя тега.
3. Нажмите **Создать**.

Созданные теги можно назначить на устройство:

- При пакетном добавлении устройств
- При выпуске устройства
- При просмотре содержимого устройства
- При изменении тегов в разделе **Устройства**
- В карточке пользователя

Шаблоны печати

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

Добавление шаблона печати

1. Нажмите **Добавить шаблон печати**.
2. Укажите название шаблона в поле **Имя**.
3. Выберите тип документа:
    - **СКЗИ** – дистрибутив, лицензия, документация, ключевой документ, ключевой носитель, пользовательский
    - **Сертификат** – запрос на сертификат, сертификат, запрос на отзыв сертификата
    - **Пользователь** – пользовательский документ
4. Загрузите файл шаблона печати.
5. 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 можно загрузить в настройках политики в разделе **Удостоверяющие центры** → **Шаблоны**.

Шаблоны можно редактировать и удалять .

Редактирование файлов стандартных шаблонов печати

Вы можете редактировать файлы стандартных шаблонов печати, общих для всех шаблонов сертификатов.

Где найти файлы шаблонов печати

Windows

Компонент	Документ	Путь к файлу шаблона
Консоль управления	Запрос на сертификат	*C:\inetpub\wwwroot\cm\mc\wwwroot\content\request_*
	Сертификат	*C:\inetpub\wwwroot\cm\mc\wwwroot\content\cert_ru.x*
	Запроса на отзыв сертификата	*C:\inetpub\wwwroot\cm\mc\wwwroot\content\revocatio*
Сервис самообслуживания	Запрос на сертификат	*C:\inetpub\wwwroot\cm\ss\wwwroot\content\request_r*
	Сертификат	*C:\inetpub\wwwroot\cm\ss\wwwroot\content\cert_ru.xs*
	Запрос на отзыв сертификата	*C:\inetpub\wwwroot\cm\ss\wwwroot\content\revocatio*

Linux

Компонент	Документ	Путь к файлу шаблона
Консоль управления	Запрос на сертификат	*/opt/indeed/cm/mc/wwwroot/content/request_ru.xsl*
	Сертификат	*/opt/indeed/cm/mc/wwwroot/content/cert_ru.xsl*
	Запрос на отзыв сертификата	*/opt/indeed/cm/mc/wwwroot/content/revocationReque*

Сервис самообслуживания	Запрос на сертификат	*/opt/indeed/cm/ss/wwwroot/content/request_ru.xsl*
	Сертификат	*/opt/indeed/cm/ss/wwwroot/content/cert_ru.xsl*
	Запрос на отзыв сертификата	*/opt/indeed/cm/ss/wwwroot/content/revocationReques*

Для каждой политики использования устройств можно использовать разные шаблоны печати:

1. Отредактируйте шаблоны.
2. Загрузите шаблоны в разделе **Конфигурация** → **Шаблоны печати**.
3. Откройте раздел **Конфигурация** и перейдите в настройки политики.
4. Откройте раздел **Удостоверяющие центры** → **Шаблоны**.
5. Нажмите **Создать шаблон сертификата**.
6. Выберите загруженные шаблоны.

Шаблоны печати нормативных документов СКЗИ

Шаблоны печати нормативных документов СКЗИ настраиваются в текстовом редакторе. Поддерживаются шаблоны в формате RTF. Печать сводных данных по нескольким объектам СКЗИ или пользователям не предусмотрена.

Настройка шаблона

Чтобы настроить шаблон печати нормативного документа СКЗИ, воспользуйтесь демонстрационным шаблоном. В левом столбце указаны имена атрибутов, в правом – параметры атрибутов в формате `${имя атрибута}`. Значения атрибутов подставляются автоматически из журнала СКЗИ.

Скачать демонстрационный шаблон

Описание атрибутов

Информация о пользователе

Атрибут	Описание атрибута
`user_name`	Общее имя пользователя
`user_logonName`	Логин пользователя
`user_email`	Email пользователя
`user_organization`	Организация
`user_jobTitle`	Должность

Информация об СКЗИ

Атрибут	Описание атрибута
`skzi_timeCreated`	Время добавления СКЗИ в Indeed CM
`skzi_skziType`	Тип СКЗИ
`skzi_objectType`	Тип объекта СКЗИ
`skzi_serialNumber`	Серийный номер СКЗИ
`skzi_instanceNumber`	Номер экземпляра СКЗИ
`skzi_creationData_creator`	Имя изготовителя СКЗИ
`skzi_creationData_timeCreated`	Время изготовления СКЗИ
`skzi_creationData_docNumber`	Номер документа об изготовлении СКЗИ
`skzi_sendingData_recipient`	Имя сотрудника, который подтверждает получение СКЗИ
`skzi_sendingData_timeSent`	Время передачи СКЗИ

Атрибут	Описание атрибута
`skzi_sendingData_docNumber`	Номер сопроводительного письма при передаче СКЗИ
`skzi_sendingData_timeConfirmed`	Время подтверждения получения СКЗИ
`skzi_sendingData_confirmationDocNumber`	Номер документа о подтверждении получения СКЗИ
`skzi_returnData_timeReturned`	Время возврата СКЗИ
`skzi_returnData_docNumber`	Номер сопроводительного письма при возврате СКЗИ
`skzi_returnData_timeConfirmed`	Время подтверждения возврата СКЗИ
`skzi_returnData_confirmationDocNumber`	Номер документа о подтверждении возврата СКЗИ
`skzi_issueData_timeIssued`	Время выдачи СКЗИ
`skzi_issueData_docNumber`	Номер сопроводительного письма при выдаче СКЗИ
`skzi_installationData_installer`	Ф.И.О. сотрудников органа криптографической защиты, пользователей СКЗИ, производивших установку СКЗИ
`skzi_installationData_timeInstalled`	Время установки СКЗИ
`skzi_installationData_docNumber`	Номер документа об установке СКЗИ
`skzi_installationData_hardwareId`	Номер аппаратного средства, на котором установлено или к которому подключено СКЗИ
`skzi_installationData_location`	Место установки СКЗИ

Атрибут	Описание атрибута
`skzi_destructionData_destructor`	Ф.И.О. сотрудников органа криптографической защиты, пользователей СКЗИ, производивших уничтожение/изъятие СКЗИ
`skzi_destructionData_timeDestructed`	Время уничтожения/изъятия СКЗИ
`skzi_destructionData_docNumber`	Номер акта или расписки об уничтожении СКЗИ
`skzi_comment`	Примечание

Чтобы настроить шаблон печати нормативного документа СКЗИ:

1. Откройте шаблон печати документа в текстовом редакторе.
2. Откройте демонстрационный шаблон печати СКЗИ и скопируйте параметры атрибутов.
3. Подставьте параметры атрибутов в шаблон печати документа.

Дополнительные поля журнала учета СКЗИ

Если в журнале учета СКЗИ вашей организации есть информация, которой нет в списке атрибутов Indeed CM, то в журнал учета можно добавить дополнительные поля. Атрибуты дополнительных полей можно использовать в шаблонах печати нормативных документов.

Дополнительные поля доступны при редактировании СКЗИ.

Чтобы создать дополнительные поля:

1. Запустите Мастер настройки на сервере Indeed CM.
2. Перейдите в раздел **Журнал учета СКЗИ**.
3. Нажмите **Добавить** и укажите:
   - **Идентификатор атрибута** – имя атрибута, которое подставляется в шаблоны печати нормативных документов. Допустимы только латинские буквы.
   - **Атрибут** – отображаемое имя поля в журнале СКЗИ.
4. Нажмите **Добавить**.

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

Чтобы добавить дополнительный атрибут в шаблон печати документа, укажите атрибут в формате `${skzi_<id>}`, где `id` – идентификатор атрибута. Например, чтобы добавить дополнительный атрибут *demo*, в шаблоне документа укажите `${skzi_demo}`.

Шаблон документа о прохождении обучения по работе с СКЗИ

Вы можете настроить шаблон заключения о прохождении обучения по работе с СКЗИ.
Подробнее об обучающих курсах

Скачать шаблон документа о прохождении обучения

Описание атрибутов

Информация о пользователе

Атрибут	Описание атрибута
`user_name`	Общее имя пользователя
`user_logonName`	Логин пользователя
`user_email`	Email пользователя
`user_organization`	Организация
`user_jobTitle`	Должность

Информация об обучении по работе с СКЗИ

Атрибут	Описание атрибута
`training_courseName`	Название обучающего курса.
`training_initiator`	Имя оператора, заполнившего номер заключения и одобрившего прохождение обучения, в формате Common name.
`training_initiator_logonName`	Имя оператора, заполнившего номер заключения и одобрившего прохождение обучения, в формате Logon name.
`training_certificateNumber`	Номер заключения о прохождении обучения.
`training_completionDate`	Время завершения обучения в сокращенном формате – дата.
`training_completionDate_full`	Время завершения обучения в полном формате – дата и время.

Примеры готовых шаблонов печати нормативных документов СКЗИ

Акт передачи средства электронной подписи

Акт установки средства электронной подписи

Акт уничтожения средства криптографической защиты информации

Заключение о прохождении обучения по работе с СКЗИ

СКЗИ

В разделе **СКЗИ** задаются настройки использования средств криптографической защиты информации (СКЗИ).

Предварительные настройки

Чтобы настроить управление СКЗИ в разделе **Конфигурация**:

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. Предоставьте членам роли привилегии для управления настройками использования СКЗИ.

Список привилегий

Привилегии для управления типами СКЗИ

- Просмотр типа СКЗИ
- Добавление типа СКЗИ
- Изменение типа СКЗИ
- Удаление типа СКЗИ

Привилегии для управления нормативными документами СКЗИ

- Просмотр шаблона нормативных документов
- Изменение шаблона нормативных документов

Привилегии для управления обучающими курсами по работе с СКЗИ

- Просмотр обучающих курсов
- Создание обучающих курсов
- Изменение обучающих курсов
- Удаление обучающих курсов

Типы СКЗИ

В разделе **Типы СКЗИ** можно создать справочник типов СКЗИ и добавить информацию о сертификатах соответствия на СКЗИ и сертификатах технической поддержки. Справочник позволяет отслеживать срок действия сертификатов для своевременного обращения к поставщику СКЗИ за обновленными сертификатами.

Добавление

Чтобы добавить тип СКЗИ:

1. Перейдите в раздел **Конфигурация** → **Типы СКЗИ**.
2. Нажмите **Добавить тип СКЗИ**.
3. В поле **Наименование** введите название типа СКЗИ. Например, КриптоПро CSP 5.0 R2 КС1.
4. В поле **Семейство** выберите семейство СКЗИ – программный, аппаратный или аппаратно-программный.
5. Чтобы добавить в Indeed CM информацию о сертификате соответствия и о сертификате технической поддержки:
    1. Включите опции **Сертификат соответствия** и **Сертификат технической поддержки**.
    2. Заполните поля **Номер**, **Дата выдачи**, **Срок действия (до)**.
6. Доступны следующие настройки в зависимости от выбранного семейства СКЗИ:

Программный

При автоматическом создании программного СКЗИ Indeed CM сопоставляет наименование экземпляра СКЗИ с наименованием типа СКЗИ. Если в Indeed CM нет типа СКЗИ, соответствующего этому экземпляру, то назначается тип по умолчанию.

Чтобы использовать тип СКЗИ в качестве типа по умолчанию, включите опцию **Использовать по умолчанию**. Тип по умолчанию отображается в списке типов СКЗИ со значком ✔.

Тип СКЗИ, используемый по умолчанию, нельзя удалить или архивировать. Чтобы удалить или архивировать такой тип, сначала выберите другой тип по умолчанию:

1. Нажмите напротив названия типа СКЗИ.
2. Включите опцию **Использовать по умолчанию** в нижней части окна редактирования.
3. Нажмите **Сохранить**.

Аппаратный

В Indeed CM типы аппаратных СКЗИ связаны с конкретными типами устройств. При добавлении типа устройства в разделе **Конфигурация** → **Типы устройств** для этого типа устройства автоматически создается тип аппаратных СКЗИ.

СКЗИ Рутокен и JaCarta можно дополнительно связать с моделями устройств. Чтобы связать СКЗИ Рутокен и JaCarta с моделями устройств, создайте отдельный тип СКЗИ для конкретной модели:

1. В выпадающем списке **Тип устройства** выберите тип.
2. В выпадающем списке **Модель устройства** выберите модель.

Аппаратно-программный

Вы можете создать аппаратно-программный тип СКЗИ для добавления экземпляров СКЗИ, которые не являются аппаратными или программными. Например, пользовательские СКЗИ ПАК С-Терра, ПАК ViPNet SIES, Континент TLS Сервер.

7. Нажмите **Добавить**.

Удаление

Тип программных и аппаратно-программных СКЗИ можно удалить ✖, если в Indeed CM нет зарегистрированных экземпляров СКЗИ этих типов.

Тип аппаратных СКЗИ можно удалить, если в Indeed CM нет зарегистрированных экземпляров СКЗИ этого типа и в разделе **Конфигурация** → **Типы устройств** нет типов устройств, связанных с этим типом СКЗИ.

Вместо удаления тип СКЗИ можно архивировать.

Архивация

Если определенные экземпляры СКЗИ больше не используются в вашей организации, или истек срок действия сертификата соответствия на СКЗИ или сертификата технической поддержки, вы можете архивировать тип, к которому относятся такие экземпляры СКЗИ, и вывести их из обращения.

> ⓘ **ПРИМЕЧАНИЕ**
> Тип программных СКЗИ, используемый по умолчанию, нельзя архивировать. Чтобы архивировать тип программных СКЗИ, используйте другой тип по умолчанию – нажмите ✎ напротив названия типа СКЗИ, включите опцию **Использовать по умолчанию** и нажмите **Сохранить**.

Чтобы архивировать тип СКЗИ:

1. Выберите нужный тип и нажмите ✎.
2. Включите опцию **Архивный** в нижней части окна редактирования.

3. Нажмите **Сохранить**.

Чтобы убрать тип СКЗИ из списка архивных:

1. Выберите нужный тип и нажмите  .
2. Выключите опцию **Архивный** в нижней части окна редактирования.
3. Нажмите **Сохранить**.

Архивные типы СКЗИ отображаются в конце списка типов СКЗИ со значком  . Информация об СКЗИ, которые относятся к архивному типу, сохраняется в журнале учета СКЗИ.

> **ПРИМЕЧАНИЕ**
> В Indeed CM нельзя создать СКЗИ, которое относится к архивному типу.
> После архивации типа СКЗИ рекомендуем вывести из обращения (уничтожить) все СКЗИ, которые относятся к этому типу.

Настройка уведомлений

Чтобы получать информацию об истечении срока действия сертификатов соответствия и сертификатов технической поддержки, настройте уведомления:

1. Откройте раздел **Конфигурация** → Уведомления администратора.
2. Нажмите **Создать уведомление**.
3. Выберите событие **Сертификаты соответствия истекают** и **Сертификаты технической поддержки истекают**.
4. Выберите тип события и получателей.
5. Нажмите **Создать**.

Нормативные документы

Вы можете настроить шаблоны нумерации нормативных документов и выбрать шаблон печати для каждого объекта СКЗИ в каждом его состоянии. Таким образом вы регулируете, по каким шаблонам формируются нормативные документы СКЗИ.

> **ПРИМЕЧАНИЕ**
>
> Пользователи могут управлять нормативными документами СКЗИ в Сервисе самообслуживания в разделе Ваши СКЗИ, администраторы – в Консоли управления в разделе СКЗИ или в карточке пользователя.

Чтобы редактировать шаблон нормативного документа СКЗИ:

1. Перейдите в Консоль управления и откройте раздел **Конфигурация** → **СКЗИ** → **Нормативные документы**.
2. Нажмите ✎ напротив нужного документа и настройте:

- **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 внутренняя нумерация для каждого типа СКЗИ в каждом состоянии.

Если вы настроили шаблон для одного объекта СКЗИ в одном из его состояний, то при печати нормативный документ для этого объекта СКЗИ в этом состоянии сформируется по этому шаблону.

Если вы не настроили такой шаблон, то при печати нормативного документа пользователи и администраторы смогут выбрать любой из шаблонов, загруженных для этого объекта СКЗИ в разделе Шаблоны печати.

Обучающие курсы

В разделе **Обучающие курсы** вы можете создать обучающие курсы, чтобы контролировать допуск пользователей к работе с СКЗИ.

Администраторы и операторы могут управлять обучением в карточке пользователя в Консоли управления, пользователи – в Сервисе самообслуживания.

Создание обучающих курсов

Чтобы создать обучающий курс:

1. Нажмите **Создать обучающий курс**.
2. Заполните поле **Имя** и **Описание**.
3. В поле **План обучения** укажите ссылку на курс и опишите план обучения.
4. В поле **Политики** выберите политики, которые определят, какие пользователи получат доступ к обучающему курсу. По умолчанию выбраны все политики.
5. Нажмите **Создать**.

Чтобы редактировать обучающий курс, нажмите  . Чтобы удалить обучающий курс, нажмите  .

Уведомления

В разделе **Конфигурация** → **Уведомления** вы можете настроить отправку уведомлений на почту администраторам о глобальных событиях Indeed CM:

- Подключение незарегистрированного устройства
- Свободные лицензии заканчиваются
- Свободные лицензии исчерпаны
- Сертификаты соответствия истекают (если в Indeed CM ведется учет СКЗИ)
- Сертификаты технической поддержки истекают (если в Indeed CM ведется учет СКЗИ)
- Срок действия лицензии истек
- Срок действия лицензии истекает

> **ПРИМЕЧАНИЕ**
>
> Вы можете задать отдельные настройки для отправки уведомлений администраторам и пользователям о событиях, которые относятся к этой политике – локальных событиях. Локальные настройки уведомлений можно задать в параметрах политики в разделе **Уведомления**.

Чтобы настроить отправку уведомлений:

1. Настройте почтовый сервер.
2. Определите группы получателей уведомлений.
3. Создайте уведомления о событиях.
4. При необходимости настройте индивидуальный шаблон уведомления для каждого события.

Предварительные настройки

Чтобы настроить доступ к управлению уведомлениями:

1. Перейдите в раздел **Конфигурация** → **Роли**.
2. Предоставьте членам роли привилегии для управления настройками уведомлений.

Список привилегий

- Просмотр настроек почтового сервера
- Изменение настроек почтового сервера
- Просмотр групп получателей
- Добавление групп получателей
- Изменение групп получателей
- Удаление групп получателей
- Просмотр уведомлений администратора
- Добавление уведомлений администратора
- Изменение уведомлений администратора
- Удаление уведомлений администратора
- Просмотр шаблонов администратора
- Изменение шаблонов администратора

Почтовый сервер

Настройте почтовый сервер для отправки уведомлений:

1. Откройте раздел **Конфигурация** → **Уведомления** → **Почтовый сервер**.
2. Укажите настройки почтового сервера и нажмите **Сохранить**.
3. Чтобы проверить работу почтового сервера, нажмите **Отправить тестовое сообщение**.
4. Укажите адрес электронной почты получателя.
5. Нажмите **Отправить**.

Если тестовое сообщение не пришло, проверьте настройки почтового сервера и отправьте сообщение повторно.

Группы получателей

Чтобы создать группу получателей:

1. Нажмите **Создать группу**.
2. Укажите имя группы.

3. Введите адреса получателей.
4. Нажмите **Создать**.

Группы получателей можно изменить  или удалить  .

> ⚠ **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. В выпадающем списке **Событие** выберите событие, о котором необходимо уведомить администратора.
3. Укажите тип события – информация, ошибка или предупреждение.
4. Выберите получателей:
   - **Группа получателей** – группа, созданная в разделе Группы получателей
   - **Группа безопасности** – группа безопасности Active Directory
5. Нажмите **Создать**.

Уведомления можно изменить  или удалить  .

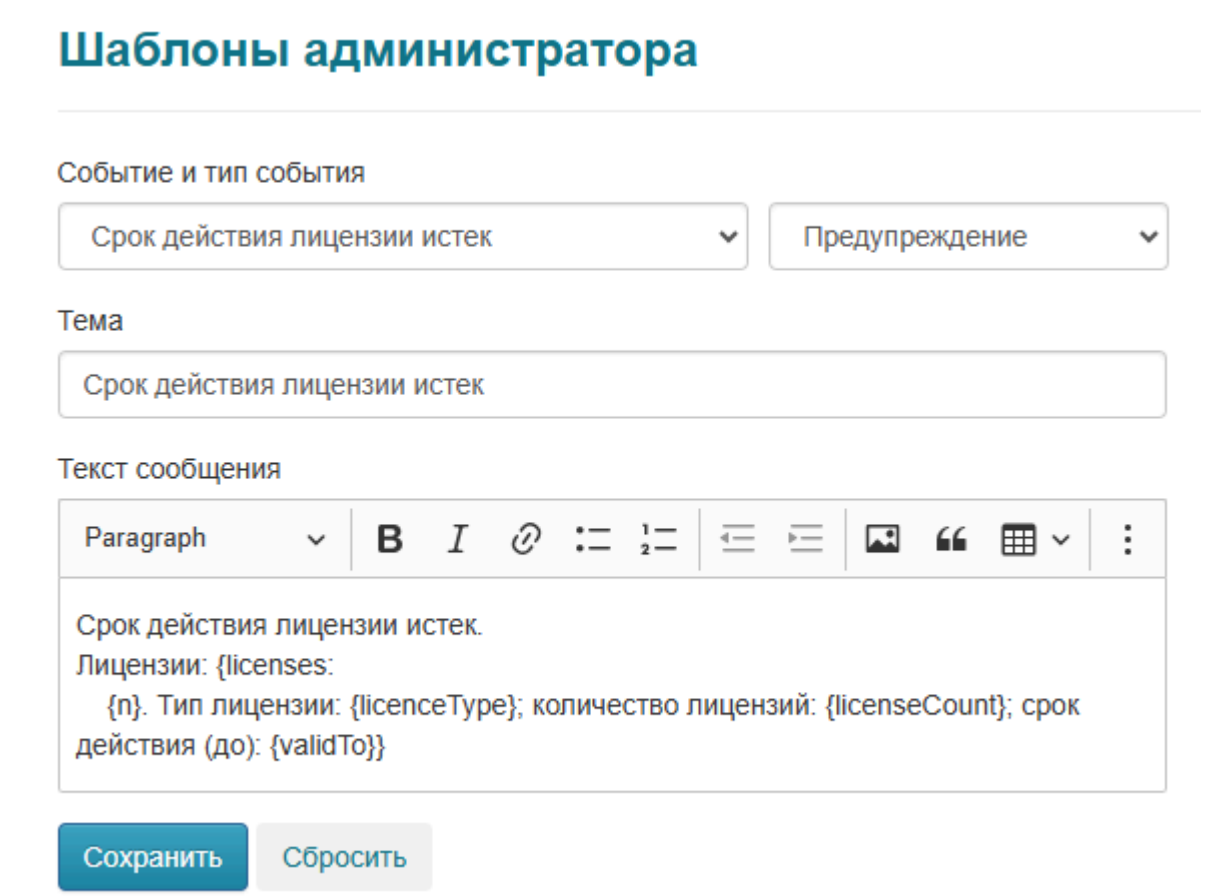
Шаблоны администратора

В разделе **Шаблоны администратора** можно настроить шаблоны почтовых уведомлений. Используйте базовые шаблоны, установленные по умолчанию, или редактируйте шаблоны, чтобы создать персонализированные уведомления.

Для каждого события в базовый шаблон встроен набор объектов с параметрами, значения которых подставляются в текст уведомления при отправке. В тексте уведомления можно использовать только те параметры, которые встроены в шаблон – новые добавлять нельзя. Вы можете удалить параметры, которые вам не нужны.

Например, в шаблон уведомления *Срок действия лицензии истек* встроен объект `licenses` с параметрами `licenseType`, `licenseCount`, `validTo`.

Пример шаблона уведомления



Чтобы создать персонализированное уведомление, внесите изменения и нажмите **Сохранить**. Чтобы вернуться к базовому шаблону, нажмите **Сбросить**.

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**.

Чтобы создать справочник:

1. Нажмите **Создать справочник**.
2. В поле **Имя** укажите название справочника.
3. Добавьте значения.
4. Нажмите **Создать**.

Справочник и его значения можно редактировать  и удалить .

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Нельзя удалить справочник или значение, которые уже используются.

Шаблоны журналов

Журнал учета – это набор полей с данными об устройствах и сертификатах, их владельцах и системах, в которых используются эти устройства и сертификаты.

Чтобы создать шаблон журнала учета:

1. Нажмите **Создать шаблон журнала**.
2. В поле **Имя** укажите название шаблона журнала.
3. В выпадающем списке **Тип объекта** выберите, какие объекты учитываются в журнале.
4. В выпадающем списке **Политики** выберите политики, для которых создается журнал учета.
5. Создайте поля журнала учета. Вы можете создать произвольные поля или использовать предустановленные поля.

6. Чтобы добавить предустановленные поля, нажмите **Добавить типовые поля**. Типовые поля предустановлены для типов объектов **Устройство** и **Сертификат**.
7. Чтобы добавить произвольное поле, нажмите **Добавить поле**.
8. Укажите имя поля.
9. В выпадающем списке **Способ заполнения** выберите, как заполняется поле:
    - **Вручную**

      Выберите формат заполнения поля – текст или дата.
    - **Автоматически**

      Выберите значение, подходящее для выбранного типа объекта.
    - **Справочник**

      Выберите справочник.

10. Задайте параметры поля:
    - **Уникальное**

      В поле есть уникальные значения.
    - **Обязательное**

      Поле обязательно к заполнению при редактировании журнала учета.
    - **Поиск**

      По полю доступен поиск в разделе **Журналы учета**

11. Нажмите **Добавить** и **Создать**.

> ⓘ **ПРИМЕЧАНИЕ**
>
> - Для типа объекта **Устройство** обязательным и уникальным полем является **Серийный номер устройства**.
> - Для типа объекта **Сертификат** обязательными полями являются **Серийный номер сертификата** и **Серийный номер устройства**. Эти поля не являются уникальными, так как на одно устройство можно записать несколько сертификатов или на разные устройства можно записать общий сертификат.
> - При редактировании уже добавленного поля вы можете изменить только его имя и набор параметров **Уникальное**, **Обязательное**, **Поиск**.
> - При удалении поля в шаблоне оно удалится во всех записях в **Журнале учета**.

Шаблон журнала учета можно редактировать ✎ или удалить ✖ .

Консоль управления

Сводная информация

Просмотр сводной информации об Indeed CM

Пользователи

Управление пользователями Indeed CM

Устройства

Управление устройствами пользователей

Сертификаты

Управление сертификатами пользователей

Журнал событий

Запись событий Indeed CM

Агенты

Работа с Indeed CM Agent

Журнал учета СКЗИ

Ведение журнала учета СКЗИ

Журнал учета устройств и сертификатов

Просмотр журналов учета устройств и сертификатов

Документы

Управление документами пользователей

Сводная информация

В разделе отображается сводная информация об Indeed CM.

Лицензии

- **Тип** – вид лицензии в зависимости от функциональности
- **Количество** – общее количество лицензий
- **Используется** – количество лицензий, занятых пользователями
- **Осталось** – количество свободных лицензий

> **ПОДСКАЗКА**
>
> Иконка предупреждения отображается в следующих случаях:
>
> - Лицензии не добавлены в Indeed CM
> - Осталось 10% от общего количества лицензий
> - Все лицензии использованы

Агенты

Информация об агентах отображается, если работа с агентами настроена в Мастере настройки Indeed CM в разделе **Функции системы** → Клиентский агент.

Количество агентов по их статусу:

- **Зарегистрировано** – агенты, которые прошли регистрацию
- **В ожидании** – агенты в ожидании регистрации
- **Отклонено** – агенты, регистрация которых была отклонена

Количество агентов по доступности связи с сервером Indeed CM:

- **Активные** – агенты, которые обращались к серверу за последние 5 минут
- **С устройствами** – агенты, в сессии которых подключено хотя бы одно устройство

Количество задач, назначенных на агенты, по статусу 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

Пользователи

Количество пользователей по состоянию в базе данных Indeed CM:

- **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

Нажмите на кнопку с количеством пользователей, чтобы перейти в раздел **Пользователи**.

Устройства

Количество устройств по состоянию:

- **Выпущено** – устройства, выпущенные в Indeed CM и готовые к работе
- **Назначено** – устройства, которые были назначены на пользователей, но еще не выпущены
- **В ожидании** – устройства в ожидании выпуска или обновления
- **Выключено** – выключенные устройства, которые можно включить, заменить или отозвать

Количество устройств с сертификатами, которые истекают или истекли:

- **Управляемые** – сертификаты, выпущенные в 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 по следующим причинам:

- **Сертификаты** – в политике использования устройств изменился набор обязательных шаблонов сертификатов

- **Смена политики** – на пользователя, для которого выпущено устройство, назначена новая политика использования устройств
- **Данные коннекторов** – после выпуска устройства в действующей политике была включена или выключена интеграция с Indeed Access Manager, Secret Net Studio, Рутокен Логон или СМЭВ

Сервисные сертификаты

Информация о сервисных сертификатах:

- Сертификаты, выданные для сервисных учетных записей при настройке интеграции с удостоверяющими центрами
- Сертификаты операторов КриптоПро УЦ-СМЭВ Шлюза, выбранные при настройке интеграции со СМЭВ

> **ПОДСКАЗКА**
> Иконка предупреждения отображается, если хотя бы один из сервисных сертификатов истекает (10% от срока действия) или истек.

Типы СКЗИ

Информация о сроке действия сертификатов соответствия на СКЗИ и сертификатов технической поддержки. Срок действия сертификатов указывается в разделе **Конфигурация** → Типы СКЗИ.

Отображается информация о типах СКЗИ, для которых был указан срок действия сертификатов. Информация о типах СКЗИ, которые были архивированы, не отображается.

Пользователи

В разделе **Пользователи** вы можете управлять пользователями Indeed CM.

Карточка пользователя

Доступные действия в карточке пользователя

Карточка устройства

Работа с устройствами пользователей

Управление СКЗИ

Работа с СКЗИ в карточке пользователя

Управление документами

Работа с документами в карточке пользователя

Поиск

Простой поиск

Чтобы найти пользователя:

1. Выберите каталог, где находится пользователь.
2. В строке поиска укажите Общее имя (Common Name), фамилию, логин (sAMAccountName) или адрес электронной почты пользователя.
   Чтобы найти всех пользователей каталога, введите `*`.
3. Нажмите  или Enter.

Расширенный поиск

Расширенный поиск позволяет найти пользователей по нескольким фильтрам:

- Корневой контейнер
- Общее имя (Common Name)
- Контейнер
- Логин (sAMAccountName)
- Имя
- Фамилия

Дополнительно можно установить следующие фильтры:

- **Заблокирован в системе**, чтобы найти пользователей, которые исчерпали попытки ответов на секретные вопросы и были заблокированы.
- **Не заданы секретные вопросы**, чтобы найти пользователей, у которых не заданы ответы на секретные вопросы.
- **Отображать отключенные учетные записи**, чтобы найти пользователей с активными и отключенными учетными записями каталога пользователей.

Результаты поиска пользователей можно сохранить в файл. Нажмите  и выберите формат PDF или CSV.

Работа с пользователями внутреннего каталога

Если в Мастере настройки Indeed CM в разделе **Каталог пользователей** настроено подключение к внутреннему каталогу пользователей, вы можете создавать контейнеры и учетные записи для внешних пользователей.

Убедитесь, что члены роли имеют привилегии для управления пользователями внутреннего каталога:

1. Перейдите в раздел **Конфигурация** → **Роли** и выберите нужную роль.
2. Проверьте следующие привилегии:
    - Создание пользователей
    - Редактирование пользователей
    - Удаление пользователей
    - Создание контейнеров
    - Редактирование контейнеров

Чтобы начать работу с пользователями внутреннего каталога, перейдите в раздел **Пользователи** и в выпадающем списке каталогов выберите корневой контейнер внутреннего каталога.

Создание пользователя

Вы можете создать пользователей вручную или импортировать файл с пользователями.

Чтобы создать пользователя вручную:

1. Нажмите **Создать пользователя** и выберите контейнер, в котором пользователь будет храниться.
2. Введите данные пользователя.
3. Нажмите **Создать**.

Импорт пользователей

Поддерживается файл в формате TXT (UTF-8) или CSV с набором строк следующего формата:

```
Container;CN;FirstName;LastName;LogonName;Email
```

Поле	Обязательно/ необязательно	Описание
Container	Необязательно	Путь к контейнеру, в котором создается пользователь. Если значение не указано, пользователь будет создан в корневом контейнере.
CN	Необязательно	Имя пользователя в формате CommonName. Если значение не указано, имя пользователя формируется из значений `LastName` и `FirstName`.
FirstName	Обязательно	Имя пользователя.
LastName	Обязательно	Фамилия пользователя.
LogonName	Обязательно	Логин пользователя в формате Domain\UserName.
Email	Необязательно	Адрес электронной почты пользователя.

Дополнительные атрибуты

Дополнительно можно использовать атрибуты внутреннего каталога, указанные в Мастере настройки Indeed CM в разделе **Дополнительные атрибуты**:

- telephoneNumber
- countryName
- stateOrProvinceName
- localityName
- streetAddress
- organizationName
- organizationUnitName
- title

При необходимости создайте дополнительные атрибуты. Например, `ageGroup` для указания возраста.

Пример содержимого файла импорта

```
CN;FirstName;LastName;LogonName;Email
Evgeniy Belov;Евгений;Белов;Demo\user1;evgeniy.belov@demo.com
Alexander Ponomarev;Александр;Пономарев;Demo\user2;alexander.ponomarev@demo.com
;Артем;Алексеев;Demo\user3
```

Чтобы импортировать пользователей:

1. Нажмите **Импортировать пользователей**.
2. Загрузите файл.
3. Выберите действие, если пользователь уже существует в Indeed CM – **Пропустить** или **Обновить данные**.
4. При необходимости включите опцию **Игнорировать ошибки**, чтобы загрузить файл с ошибками импорта.

Создание и редактирование контейнера

Чтобы создать контейнер:

1. Нажмите **Создать контейнер**.
2. Выберите родительский контейнер.
3. Введите имя контейнера.
4. Нажмите **Создать**.

Вы можете переместить созданный контейнер в другой родительский контейнер и изменить его имя:

1. Нажмите **Редактировать контейнер**.
2. Нажмите **Переместить** и выберите новый родительский контейнер.
3. Введите новое имя контейнера.
4. Нажмите **Сохранить**.

Карточка пользователя

В карточке пользователя вы можете управлять данными пользователя, его устройствами, сертификатами, документами и СКЗИ.

Чтобы перейти в карточку пользователя, найдите нужного пользователя в разделе **Пользователи** Консоли управления и нажмите на его логин.

Комментарий

В поле **Комментарий** вы можете добавить дополнительную информацию о пользователе — например, служебные заметки.

Чтобы добавить, редактировать или удалить комментарий, нажмите  .

Комментарий доступен только членам роли с привилегией *Просмотр комментария о пользователе*. Добавлять, редактировать и удалять комментарии могут только члены роли с привилегией *Изменение комментария о пользователе*.

> **ПРИМЕЧАНИЕ**
>
> Чтобы настроить привилегии, перейдите в раздел **Конфигурация** → **Роли**.

Загрузка фотографии

Фотография отображается в карточке пользователя, если она есть в профиле пользователя в каталоге.

Чтобы добавить фотографию, нажмите **Загрузить фотографию**.

Параметры загрузки фотографии

- Фотографию пользователя можно записать в атрибуты `thumbnailPhoto` или `jpegPhoto`.

  Выбор атрибута доступен для пользователей каталогов Active Directory, Samba AD DC, РЕД АДМ и Альт Домен. Чтобы выбрать атрибут, перейдите в Мастер настройки в раздел **Каталог пользователей**.

- Сервисная учетная запись для работы с каталогом пользователей должна обладать правами на запись для выбранного атрибута.
- Размер фотографии не должен превышать 100 КБ.

Связь каталогов пользователей

Если в вашей 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 политике использования устройств в разделе КриптоПро 2.0. Один и тот же пользователь может быть связан с каталогами различных УЦ.

Вне зависимости от каталога, где расположен пользователь, вы можете установить связь с любым пользователем КриптоПро УЦ 2.0. Если каталог УЦ, с которым необходимо установить связь, не содержит пользователей, то можно их создать с помощью Indeed CM.

Связать пользователя каталога с пользователем КриптоПро УЦ 2.0 можно автоматически через опцию **Устанавливать привязку автоматически** в политике или вручную.

Чтобы установить связь вручную:

1. Перейдите в карточку пользователя.
2. Нажмите **Пользователь КриптоПро 2.0**.
3. Введите имя пользователя 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**.

Чтобы отменить привязку, нажмите **Пользователь КриптоПро 2.0** и **Отменить привязку**.

Чтобы создать 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. Эти данные система получает из профиля пользователя Active Directory.

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 в политике использования устройств.

> **ПРЕДУПРЕЖДЕНИЕ**
>
> Заблокированный пользователь не сможет войти в Сервис удаленного самообслуживания и разблокировать/выключить устройство с помощью Indeed CM Credential Provider.
>
> Если заблокированы и устройство, и пользователь, то оператор Indeed CM 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 Indeed CM заносится запись, а в карточке пользователя появляется статус *Пользователь заблокирован*.

Чтобы разблокировать пользователя, откройте его карточку и нажмите **Разблокировать пользователя**.

Сброс ответов на секретные вопросы

В карточке пользователя можно сбросить секретные вопросы пользователя и указанные ответы. В этом случае пользователь должен 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

Вы можете сбросить доменный пароль, 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.

Требования для сброса пароля пользователя:

- В разделе **Каталог пользователей** Мастера настройки Indeed CM в настройках каталога пользователей включена опция **Использовать LDAPS**.
- Сервисная учетная запись для работы с каталогом пользователей обладает правами на **Сброс пароля** (Reset password) и на **Запись: pwdLastSet** (Write pwdLastSet).

Чтобы сбросить пароль пользователя:

1. В карточке пользователя нажмите **Сбросить пароль пользователя**.
2. Задайте новый пароль.
3. При необходимости включите опцию **Пользователь должен поменять пароль при первом входе**.
4. Задайте срок действия пароля. По истечении срока действия значение пароля сменится на случайное. Смену пароля выполняет служба Card Monitor.

Как запустить службу Card Monitor

Служба Card Monitor запускается ежедневно автоматически по расписанию, заданному в Мастере настройки в разделе **Card Monitor**.

Чтобы запустить Card Monitor вручную:

- **ОС Windows**
  Откройте консоль Powershell от имени администратора на сервере Indeed CM и запустите:

```
C:\Program Files\Indeed CM\CardMonitor\Cm.CardMonitor.exe
```

- **ОС Linux**
  Откройте терминал от имени администратора на сервере Indeed CM и запустите:

```
cd /opt/indeed/cm/cardmonitor && ./Cm.CardMonitor
```

ПРИМЕЧАНИЕ

Установленный пароль не записывается в хранилище данных Indeed CM.

Просмотр событий пользователя

В карточке пользователя отображается информация о пяти последних событиях в Indeed CM для данного пользователя.

Список событий можно обновить . Чтобы посмотреть расширенную информацию о событии, нажмите ▶. Чтобы просмотреть полный список событий и перейти в раздел **Журнал**, нажмите **Просмотреть все**.

Карточка устройства

Администраторы и операторы Indeed CM могут управлять устройствами пользователя в его карточке в разделе **Назначенные устройства**.

Операции с устройствами

Выпуск

Как записать сертификаты на устройство

Назначение

Как закрепить устройство за пользователем

Сброс PIN-кода

Как сбросить PIN-код устройства

Разблокировка устройства

Как разблокировать устройство в режиме онлайн или офлайн

Разблокировка биометрии

Как разблокировать биометрическую аутентификацию на устройстве Рутокен БИО

Выключение и включение

Как выключить и включить устройство

Отзыв

Как отозвать устройство при его повреждении, утере, изъятии, обновлении

Изъятие

Как изъять устройство у пользователя

Замена

Временная или постоянная замена устройств пользователей

Обновление

Как обновить содержимое устройства

Обновление биометрии

Как обновить зарегистрированные отпечатки пальцев на устройстве Рутокен БИО

Выпуск с печатью

Как выпустить смарт-карту с печатью изображения или текста

Содержимое устройства

В карточке устройства отображается следующая информация:

- Состояние устройства
- Комментарий
- Политика, действующая на устройство
- Причина отзыва, если устройство было изъято
- Агент, к которому привязано устройство
- PIN-код администратора
- Теги
- Сертификаты, которые хранятся на устройстве – управляемые, отслеживаемые, общие

Просмотр содержимого устройства в Сервисе самообслуживания

Вы можете разрешить или запретить пользователям доступ к просмотру содержимого устройства. Если у пользователей есть доступ, они могут просмотреть сертификаты, которые хранятся на устройстве, и распечатать документы сертификатов.

Чтобы разрешить доступ:

1. Перейдите в настройки политики использования устройств.
2. Перейдите в раздел **Поведение** → **Разрешения пользователя** → **Действия с выпущенным устройством**.
3. Включите опцию **Просматривать содержимое**.

Типы сертификатов

Управляемые

Это сертификаты, которые формируются по шаблонам, настроенным для интегрированных удостоверяющих центров (УЦ), и выпускаются в УЦ через Indeed CM. Шаблоны сертификатов настраиваются в политике использования устройств в разделе Настройки PKI.

Управляемые сертификаты можно выпускать, обновлять, отзывать, отслеживать их срок действия и состояние. Indeed CM получает информацию о состоянии сертификата или запроса на сертификат из УЦ.

Отслеживаемые

Это записанные на устройство сторонние сертификаты, информацию о которых можно внести в Indeed CM. Сертификаты, выпущенные в сторонних УЦ, нельзя выпускать, обновлять и отзывать, но можно проверить информацию об издателе сертификата и срок действия.

Настройка отслеживания

Чтобы в карточке устройства отображалась информация о сторонних сертификатах, хранящихся на устройстве, настройте отслеживание сторонних сертификатов:

1. Перейдите в настройки политики использования устройств в раздел **Поведение** → **Общие разрешения**.
2. Включите опцию **Искать сертификаты при выпуске/обновлении устройства для отслеживания срока действия**.

Уведомление об истечении срока действия

Чтобы отправить уведомление администраторам и пользователям об истечении срока действия отслеживаемых сертификатов:

1. Перейдите в настройки политики использования устройств в раздел **Уведомления**.
2. Создайте уведомление о событии *Отслеживаемые сертификаты истекают*.

Печать

Отслеживаемые сертификаты можно распечатать в Консоли управления и в Сервисе самообслуживания по стандартному шаблону печати сертификата.

Общие

Это сторонние сертификаты, общие для нескольких пользователей.

Общий сертификат записывается на устройство при его выпуске или обновлении. Чтобы записать общий сертификат на устройства нескольких пользователей, перейдите в настройки политики использования устройств в раздел **Настройки PKI** → Общие сертификаты и нажмите **Добавить общий сертификат**.

Уведомление об истечении срока действия

Чтобы отправить уведомление администраторам об истечении срока действия общих сертификатов:

1. Перейдите в настройки политики использования устройств в раздел **Уведомления**.
2. Создайте уведомление о событии *Общие сертификаты истекают*.

Состояния сертификата

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 не пригоден для использования. Срок действия сертификата можно продлить на период, равный сроку его действия, заданный в шаблоне сертификата на УЦ. Подробнее об обновлении сертификатов
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.
Отклонен	Администратор отклонил запрос на сертификат.
В ожидании	Запрос на сертификат ожидает рассмотрения оператора УЦ или форма сертификата ожидает рассмотрения администратора Indeed CM.

Экспорт документов 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  и выберите документ. Для отправки по электронной почте нажмите  и выберите документ.

Выпуск

При выпуске устройство персонализируется для конкретного пользователя в соответствии с настройками назначенной политики использования устройств. По каждому шаблону сертификата Indeed CM генерирует на устройстве ключевую пару, формирует подписанный запрос на сертификат и отправляет его в удостоверяющий центр (УЦ). После одобрения запроса в УЦ сертификат записывается на устройство.

Предварительные настройки

Параметры выпуска устройства задаются в политике использования устройств. Перед началом работы проверьте настройки следующих разделов политики:

- Выпуск — общие настройки процесса выпуска устройства.
- Инициализация устройства — параметры инициализации, заданные отдельно для каждого типа устройств.
- Настройки PKI — настройки УЦ и шаблонов сертификатов.
- Поведение — разрешения для администраторов/операторов и пользователей.

Процесс выпуска

1. Откройте окно выпуска устройства одним из способов:

    - В разделе **Пользователи** найдите пользователя, откройте его карточку и нажмите **Выпустить устройство**.
    - В разделе **Устройства** нажмите **Выпустить устройство**, найдите пользователя и нажмите **Выбрать**.

2. Выберите шаблоны, по которым формируются сертификаты для записи на устройство. Обязательные сертификаты записываются на устройство автоматически.

3. Если в политике настроена интеграция со СМЭВ и сертификат выпускается по шаблону для КриптоПро УЦ 2.0 или Валидата УЦ, отобразится форма проверки СМЭВ. Проверьте данные пользователя.
   Подробнее о проверке в СМЭВ

4. (Опционально) Включите опцию **Инициализировать устройство**. При инициализации все данные на устройстве удаляются. Параметры инициализации настраиваются в политике в разделе Выпуск и Инициализация устройства.

5. Заполните форму выпуска устройства:

   - **Имя устройства**

     Имя устройства, которое отображается в Indeed CM. Поле заполняется автоматически, если в политике в разделе **Выпуск** включена опция **Генерировать имя устройства автоматически**.

   - **Комментарий к устройству**

     Произвольный комментарий. Обязательное поле, если в политике в разделе **Выпуск** включена опция **Требовать указания комментария к устройству**.
     Для шаблонов сертификатов КриптоПро УЦ 2.0 комментарий попадает в запрос на сертификат, если в параметрах шаблона включена опция **Использовать комментарий устройства в качестве комментария пользователя к запросу на сертификат**.

   - **Теги**

     Теги из списка, заданного в разделе **Конфигурация → Теги**. Обязательное поле, если в политике в разделе **Выпуск** включена опция **Требовать указания тегов к устройству**.

   - **Номер и дата документа**

     Реквизиты документа, на основании которого изготавливается СКЗИ.
     Поле отображается, если устройство поддерживает аппаратную криптографию, не добавлено в Indeed CM и в политике в разделе **Поведение → Общие разрешения** включена опция **Автоматически добавлять устройства при выпуске или назначении**.

6. Подключите устройство к рабочей станции. Подключенное устройство автоматически отображается в поле **Устройство**.

7. Если устройство еще не добавлено в Indeed CM и в политике в разделе **Поведение → Общие разрешения** включена опция **Автоматически добавлять устройства при выпуске или назначении**, отобразится раздел **Дополнительно**. При необходимости введите PIN-коды устройства.

Раздел Дополнительно

Введите PIN-коды в зависимости от настроек инициализации (шаг 4):

- При выпуске с инициализацией введите PIN-код администратора.
- При выпуске без инициализации введите PIN-код пользователя и PIN-код администратора.

Для устройств с несколькими областями (например, PKI и ГОСТ на JaCarta) введите PIN-код для каждой области. Для устройств eToken со встроенной защитой от форматирования укажите ключ инициализации.

Если поля PIN-кодов оставить пустыми, Indeed CM подставит значения из файла типа устройства (раздел **Конфигурация** → **Типы устройств**).

8. Нажмите **Выпустить**. Дальнейшие действия зависят от настроек политики и типа устройства.

Отслеживание сторонних сертификатов при выпуске без инициализации

Если в политике в разделе **Поведение** → **Общие разрешения** включена опция **Искать сертификаты при выпуске/обновлении устройства для отслеживания срока действия** и на устройстве найдены сторонние сертификаты, отобразится их список.

Отметьте сертификаты, которые нужно отслеживать, и нажмите **OK**.

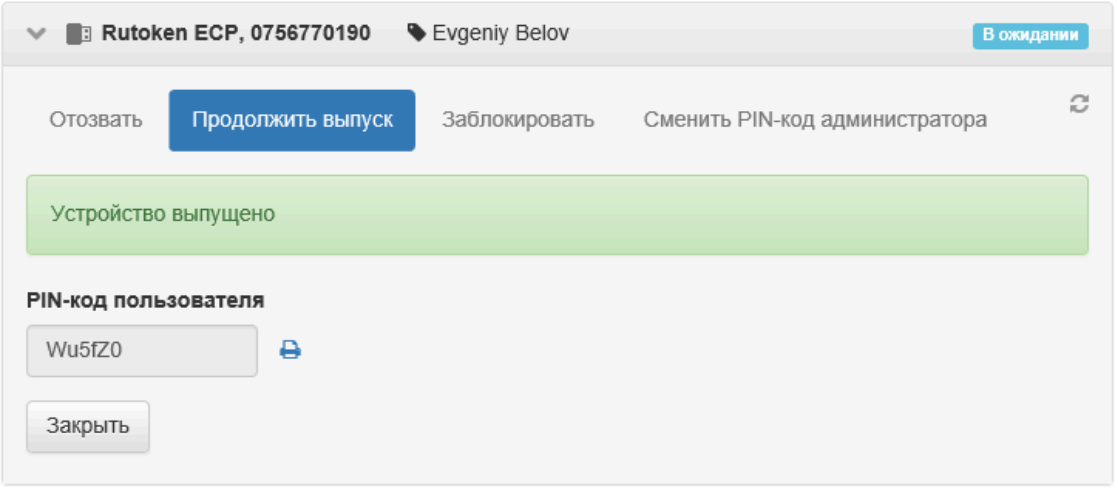
Подробнее об отслеживаемых сертификатах

PIN-код пользователя

Если в политике в разделе **Выпуск** включена опция **Устанавливать случайный PIN-код пользователя**, после выпуска устройства отображается сгенерированный PIN-код. Сохраните его и передайте пользователю одним из способов:

- По электронной почте
  Доступно, если в разделе **Уведомления** настроена рассылка уведомлений по электронной почте.

- В печатном виде
  Нажмите , и PIN-код сохранится в файл *PinEnvelope.pdf*.
  Параметры печати настраиваются в шаблоне *C:\inetpub\wwwroot\cm\mc\wwwroot\content\pinenvelope.xsl*. По умолчанию выводятся имя и e-mail пользователя, тип, серийный номер устройства и PIN-код пользователя.



Информация об устройстве появится в карточке пользователя в разделе **Назначенные устройства**.

ОСОБЕННОСТИ ВЫПУСКА УСТРОЙСТВ РУТОКЕН БИО

Если вы выпускаете устройство Рутокен ЭЦП 3.0 3250 БИО (Рутокен БИО), на которое записывается сертификат с биометрической защитой, в процессе выпуска откроется окно биометрической аутентификации. Пользователь должен пройти биометрическую аутентификацию, чтобы подтвердить выпуск сертификата.

Если биометрия на устройстве еще не зарегистрирована, перед аутентификацией откроется окно регистрации биометрии.

Подробнее о работе с устройствами Рутокен БИО

Проверка запроса на сертификат в УЦ

Если в шаблоне сертификата отключена автоматическая обработка запроса в УЦ, выпуск устройства приостанавливается до решения УЦ. В окне выпуска устройства появляется сообщение *Выпуск устройства ожидает решения*. Устройство переходит в состояние *В ожидании*.

Как настроить проверку запроса на сертификат в УЦ

1. В разделе **Конфигурация** перейдите в настройки политики.
2. В разделе **Настройки PKI** выберите УЦ и перейдите в раздел **Шаблоны**.
3. Выберите шаблон, нажмите ✎ и отключите опцию **Автоматически одобрять запрос на сертификат**.

Когда УЦ обработает запрос:

- Если запрос одобрен, сертификат получает статус *Одобрен* и записывается на устройство. В карточке устройства нажмите **Продолжить выпуск устройства**.
- Если запрос отклонен, отзовите и очистите устройство, затем начните выпуск заново.

> ⚠ **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 и имеет статус *Действительный*, он будет записан на устройство вместе со вторым сертификатом.

Вы можете настроить рассылку уведомлений по электронной почте, чтобы получать уведомления о статусе проверки.

Проверка подписанной формы сертификата

Если в шаблоне сертификата включена опция **Требовать подписанный документ сертификата перед продолжением выпуска/обновления устройства**, выпуск приостанавливается. Сертификат записывается на устройство только после того, как пользователь предоставит вам подписанную форму сертификата.

Подробнее о проверке документов

Проверка данных пользователя в СМЭВ

Вы можете настроить проверку данных пользователя в системе межведомственного электронного взаимодействия (СМЭВ) при выпуске или обновлении квалифицированного сертификата КриптоПро УЦ 2.0 или Валидата УЦ.
Как настроить интеграцию со СМЭВ

Данные можно проверить в СМЭВ при выпуске или обновлении устройства и в карточке пользователя. Чтобы проверить данные в карточке пользователя:

1. Нажмите **Проверить пользователя в СМЭВ** в меню действий с пользователем.
2. Выберите **Тип пользователя**: физическое лицо, юридическое лицо или индивидуальный предприниматель.
   Подробнее о проверке разных типов пользователей
3. Введите данные пользователя и нажмите **Далее**.
4. Проверка данных пользователя может занять несколько часов. Выберите опцию:
   - **Проверить повторно**, чтобы редактировать данные пользователя и проверить их повторно.

- **Одобрить данные пользователя**, чтобы принудительно подтвердить корректность данных.
- **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.

Одобрение данных пользователя

Опция **Одобрить данные пользователя** позволяет принудительно подтвердить корректность данных, когда в СМЭВ еще не поступили недавно измененные персональные данные пользователя – например, при смене фамилии или замене паспорта.

Опция появляется, если проверка занимает больше 15 минут или завершилась с ошибкой.

> ⓘ **ПРИМЕЧАНИЕ**
>
> Опция **Одобрить данные пользователя** доступна для членов роли с привилегией **Одобрение данных запроса СМЭВ**. Привилегии настраиваются в разделе **Конфигурация → Роли**.

Публикация выпущенных сертификатов

При выпуске устройства вы можете опубликовать сертификаты в различные хранилища.

Чтобы настроить публикацию сертификатов в хранилища:

1. В разделе **Конфигурация** перейдите в настройки политики.
2. В разделе **Настройки PKI** выберите УЦ и перейдите в раздел **Шаблоны**.
3. Выберите шаблон и нажмите ✎.
4. Включите нужные опции:
   - **Устанавливать сертификат в локальное хранилище**
   - **Публиковать сертификат в каталоге пользователей**
   - **Публиковать сертификат в ЕСИА**
   - **Публиковать сертификат в файловое хранилище**
   - **Публиковать сертификат в ЦФТ**

Назначение

При назначении устройство закрепляется за пользователем, чтобы он мог выпустить это устройство самостоятельно в Сервисе самообслуживания.

Одно устройство может одновременно принадлежать только одному пользователю. У одного пользователя может быть несколько устройств.

Чтобы назначить устройство:

1. Перейдите в карточку пользователя.
2. Нажмите **Назначить устройство**.
3. В в зависимости от того, есть ли у вас доступ к устройству, выберите опцию:
    - Устройство доступно
    - Устройство недоступно

Устройство доступно

Выберите инструкцию в зависимости от того, добавлено ли устройство в Indeed CM.

Устройство добавлено

1. Подключите его к рабочей станции.
2. Выберите в выпадающем списке **Устройство**. Нажмите **Назначить**.

Устройство не добавлено

Устройство можно добавить автоматически при назначении. Чтобы настроить возможность добавить устройство при назначении:

1. Перейдите в настройки политики использования устройств.
2. Перейдите в раздел **Поведение** → **Общие разрешения**
3. Включите опцию **Автоматически добавлять устройства при выпуске или назначении**.

Чтобы добавить и назначить устройство:

1. Подключите устройство к рабочей станции.
2. Выберите его в выпадающем списке **Устройство** в окне назначения устройства.

Если устройство поддерживает аппаратную криптографию и в Indeed CM ведется учет средств криптографической защиты информации (СКЗИ), то при добавлении устройства формируется нормативный документ СКЗИ. В окне назначения устройства отобразится поле **Номер и дата документа**.

При добавлении устройства Indeed CM автоматически подставит значение PIN-кода администратора, указанное для данного типа устройства в разделе **Конфигурация** → Типы устройств. Если PIN-код администратора отличается от значения, указанного в разделе **Типы устройств**, вы можете ввести его в разделе **Дополнительно**. Нажмите **Назначить**.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Если PIN-код администратора неверный, он может заблокироваться.
>
> ▼ **Подробнее о блокировке PIN-кода администратора**
>
> У каждого устройства есть счетчик неудачных попыток ввода PIN-кода администратора. Например, на устройствах Рутокен по умолчанию установлено 10 попыток ввода PIN-кода администратора. Если на устройстве, которое добавляется в Indeed CM, осталась одна попытка, и введен неверный PIN-код, то PIN-код администратора заблокируется.
>
> На некоторых устройствах разблокировать PIN-код администратора невозможно. В случае блокировки PIN-кода администратора необходимо инициализировать устройство, но при этом все данные, хранящиеся на нем, будут удалены.

Устройство недоступно

Устройство можно назначить пользователю удаленно, если оно было ранее добавлено в Indeed CM. Найдите нужное устройство с помощью фильтров поиска – серийный номер, тип, комментарий, теги. Нажмите **Назначить**.

Назначение в Сервисе самообслуживания

Вы можете разрешить или запретить пользователям назначать устройства самостоятельно в Сервисе самообслуживания. Чтобы настроить разрешение:

1. Перейдите в настройки политики использования устройств.
2. Перейдите в раздел **Поведение** → **Разрешения пользователя** → **Действия при выпуске устройства**.
3. Включите опцию **Назначать**.

Отмена назначения

Вы можете отменить назначение устройства, которое еще не было выпущено.

Чтобы отменить назначение, перейдите в карточку пользователя, выберите назначенное устройство и нажмите **Отменить назначение**.

Сброс PIN-кода

Если пользователь забыл или заблокировал PIN-код своего устройства, вы можете сбросить PIN-код пользователя. PIN-код поменяется на значение, указанное в разделе Типы устройств.

> **ПРИМЕЧАНИЕ**
>
> Если в разделе **Выпуск** политики использования устройств включена опция **Инициализировать устройство**, то PIN-код пользователя изменится на значение, указанное в параметрах инициализации типа устройства.

Чтобы сбросить PIN-код пользователя:

1. Перейдите в раздел **Пользователи** и выполните поиск пользователя.
2. Нажмите на логин и перейдите в карточку пользователя.
3. В карточке устройства выберите действие **Сбросить PIN-код**.
4. Если устройство доступно, подключите его к рабочей станции и нажмите **Сбросить**.
   Если устройство недоступно, создайте задачу для агента, установленного на рабочей станции пользователя:
   1. Включите опцию **Сбросить PIN-код пользователя на агенте**.
   2. (Опционально) Заполните поле **Комментарий**.
   3. Нажмите **Сбросить**.
      Подробнее о сбросе PIN-кода пользователя на агенте

После сброса PIN-кода пользователь может задать новый PIN-код в Сервисе самообслуживания.

Сброс PIN-кода в Сервисе самообслуживания

Вы можете разрешить или запретить пользователям сбрасывать PIN-код самостоятельно в Сервисе самообслуживания. Чтобы настроить разрешение:

1. Перейдите в настройки политики использования устройств.
2. Перейдите в раздел **Поведение** → **Разрешения пользователя** → **Действия с выпущенным устройством**.
3. Включите опцию **Сбрасывать PIN-код пользователя**.

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.

Вы можете разблокировать устройство пользователя. Существует два режима разблокировки: 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.

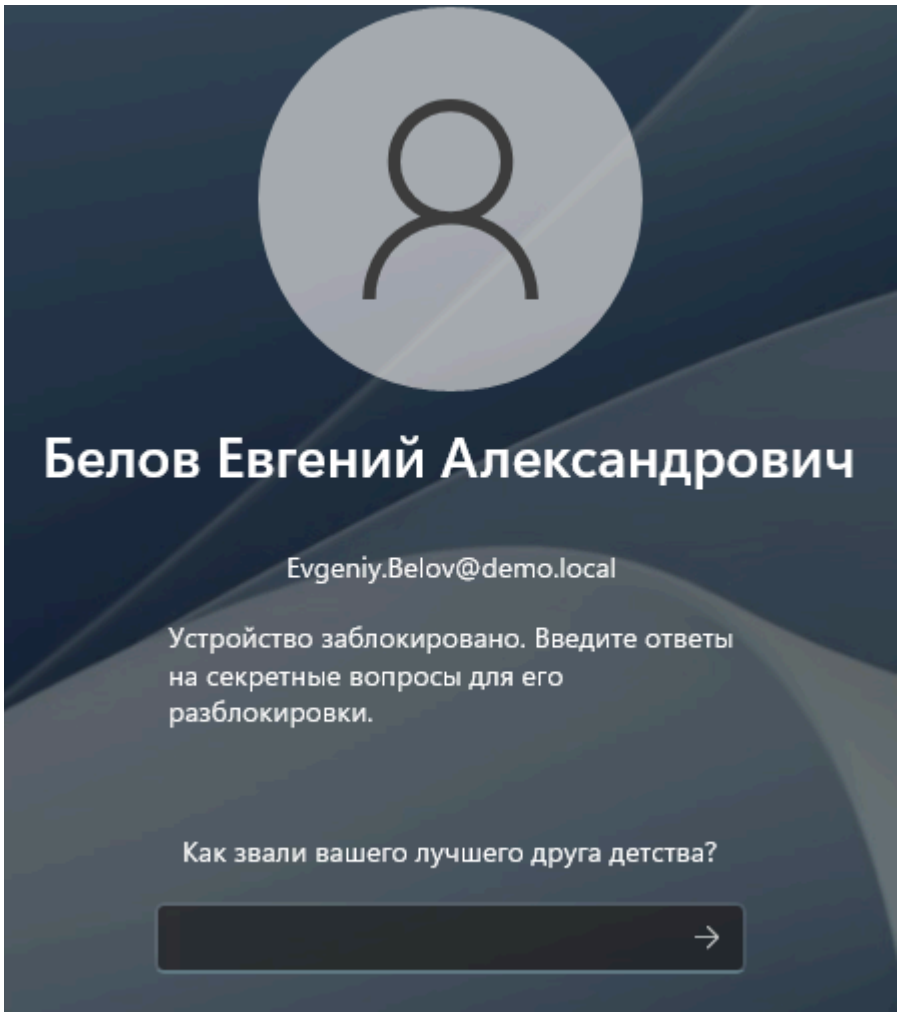
Обязательные условия для онлайн-разблокировки:

- Рабочая станция пользователя, к которой подключено заблокированное устройство, связана с сервером Indeed CM.
- Пользователь установил ответы на секретные вопросы в Сервисе самообслуживания.

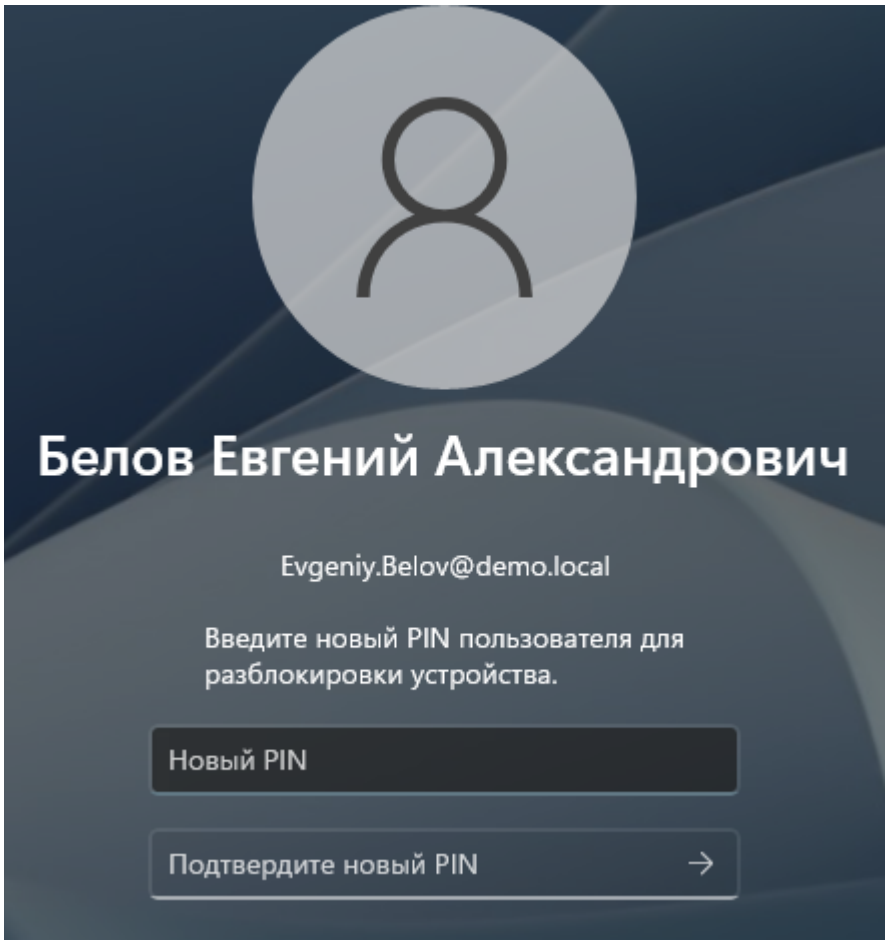
Если секретные вопросы пользователя не установлены, онлайн-разблокировка устройства недоступна. Разблокировать устройство можно только в офлайн-режиме.

Пример онлайн-разблокировки устройства в окне входа ОС Windows 11

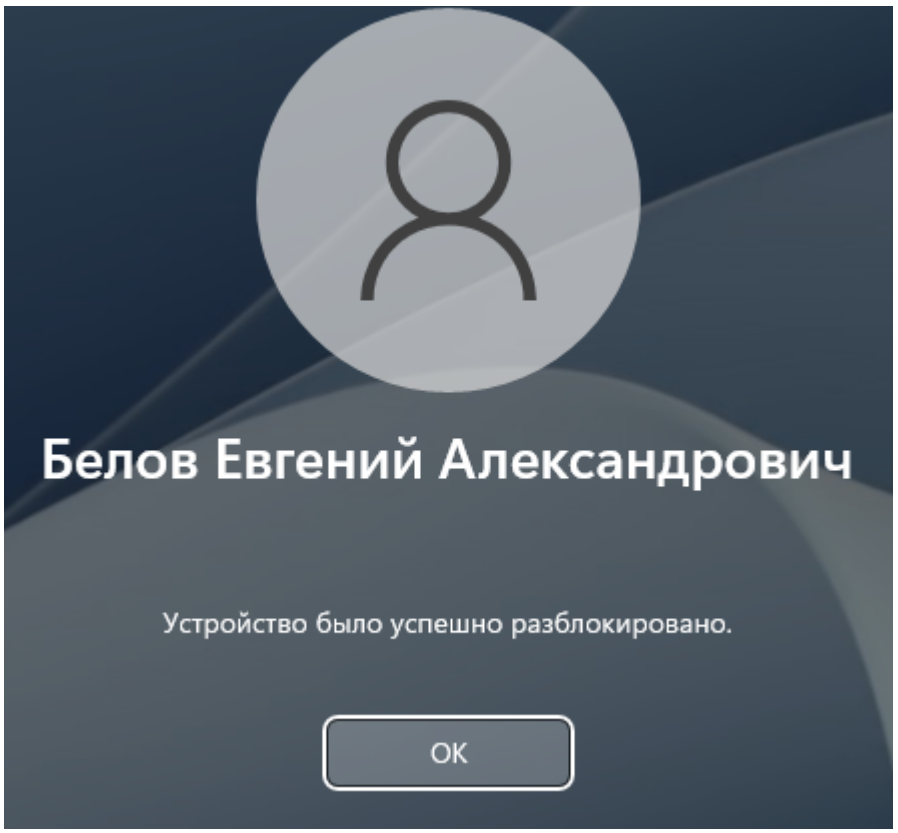
1. Введите ответы на секретные вопросы и нажмите  .



2. Введите **Новый PIN** и **Подтверждение**.



3. В случае успешной разблокировки устройства появится сообщение.



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.

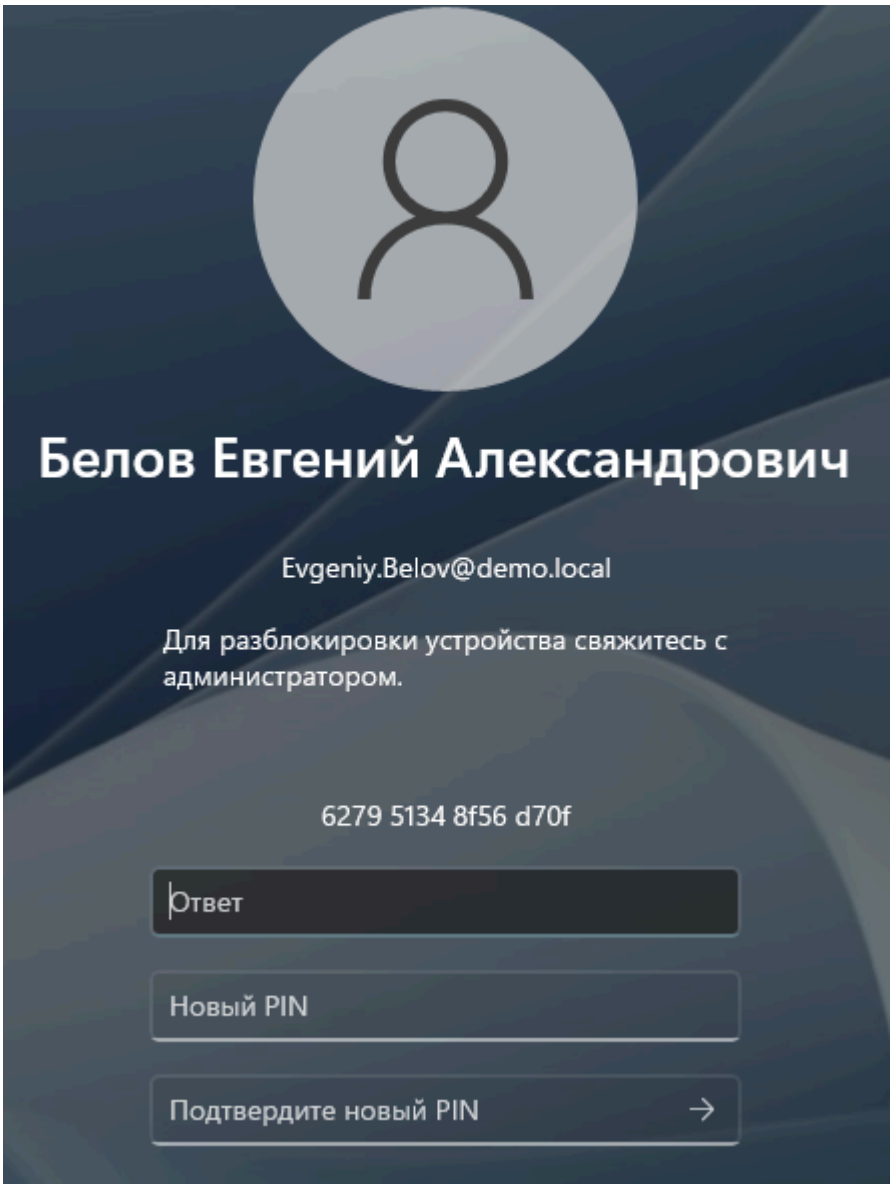
Офлайн-разблокировка осуществляется оператором Indeed CM по принципу аутентификации вида запрос-ответ (challenge-response authentication mechanism).

Процесс разблокировки

1. Когда число попыток ввода PIN-кода исчерпано, пользователь получает сообщение, что его устройство заблокировано. Вместе с сообщением пользователь получает уникальный код-запрос из 16 символов.

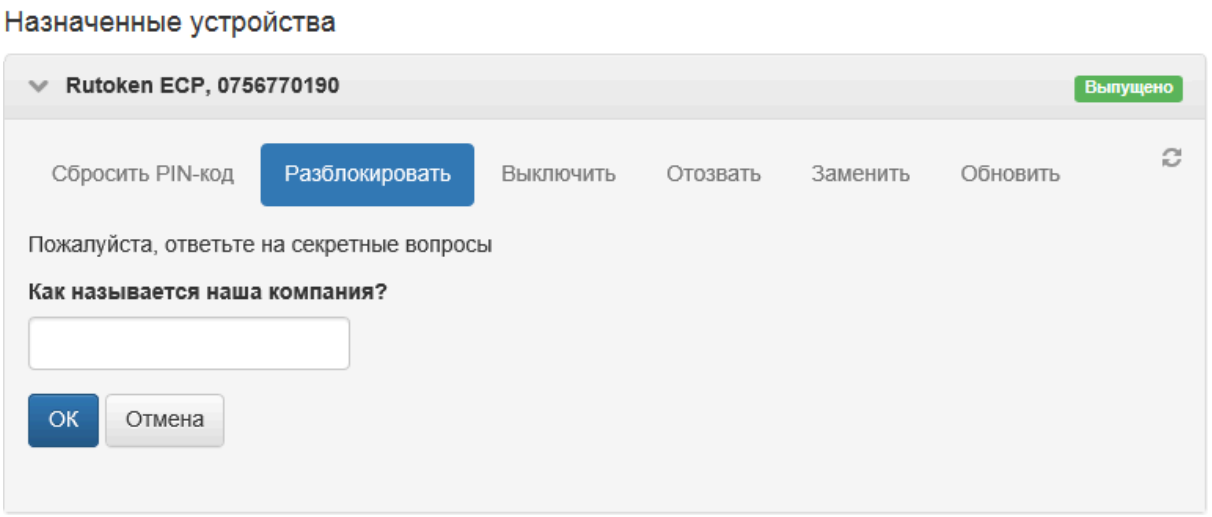
2. Пользователь связывается с оператором (например, по телефону), отвечает на секретные вопросы и сообщает полученный код-запрос.

   Пример экрана офлайн-разблокировки устройства в окне входа ОС Windows 11



3. Оператор открывает карточку устройства пользователя и выбирает пункт **Разблокировать**.

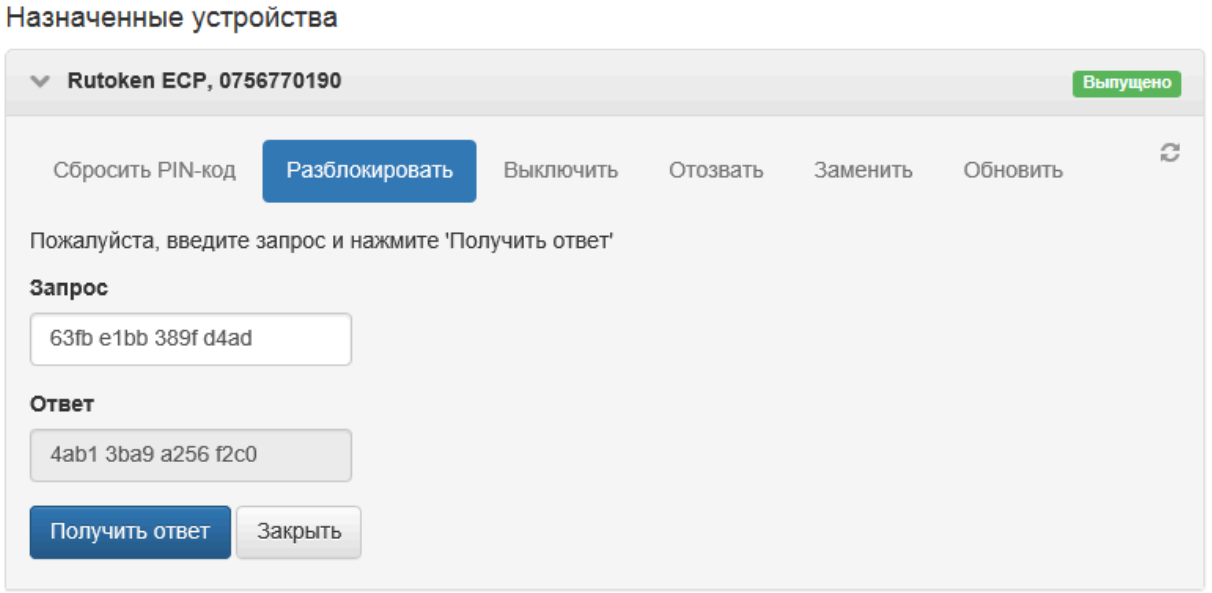
4. Прежде чем сгенерировать ответный код для разблокировки устройства, оператор задает секретный вопрос (или несколько вопросов, в зависимости от настроек политики использования устройств) и вводит полученный от пользователя ответ.



5. Если пользователь верно ответил на секретные вопросы, оператор вводит код, полученный от пользователя.

6. Indeed CM генерирует ответный код.

7. Оператор сообщает код пользователю.



8. Пользователь вводит полученный код и задает новый PIN-код устройства.

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*).

1. Подключите устройство к компьютеру и запустите утилиту Indeed CM Unblock.

2. Выберите устройство из списка и апплет PKI или ГОСТ.
3. В поле **Запрос** появится код разблокировки устройства. Сообщите код оператору Indeed CM. Оператор может запросить ответы на секретные вопросы для подтверждения личности и сообщит код ответа.
4. 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 утилиты Indeed CM Unblock.

ПРИМЕЧАНИЕ

Возможность офлайн-разблокировки устройства можно отключить:

1. Перейдите в настройки политики использования устройств.
2. Перейдите в раздел **Поведение** → **Разрешения администратора**.
3. Отключите опцию **Разблокировать устройство офлайн**. Кнопка **Разблокировать** в карточке устройства будет недоступна.

Необходимость проверки ответов на секретные вопросы при офлайн-разблокировке определяется опцией **Проверять ответы на секретные вопросы** в разделе **Поведение**.

Разблокировка биометрии

Биометрическая аутентификация на устройстве Рутокен БИО блокируется, если пользователь не прошел проверку отпечатка пальца пять раз подряд. Вы можете разблокировать биометрию, счетчик попыток аутентификации при этом сбрасывается.

Подробнее о работе с устройствами Рутокен БИО

Предварительные настройки

Действие **Разблокировать биометрию** доступно в карточке устройства членам роли с привилегией *Разблокировка биометрии*. Чтобы настроить привилегии, перейдите в раздел **Конфигурация** → **Роли**.

Процесс разблокировки биометрии

1. Перейдите в раздел **Пользователи** и выполните поиск пользователя.
2. Нажмите на логин и перейдите в карточку пользователя.
3. В карточке устройства Рутокен БИО выберите действие **Разблокировать биометрию**.
4. Подключите устройство и нажмите **Разблокировать**.
   Если устройство недоступно, создайте задачу для агента, установленного на рабочей станции пользователя:
   1. Включите опцию **Разблокировать биометрию на агенте**.
   2. (Опционально) Заполните поле **Комментарий**.
   3. Нажмите **Разблокировать**.

Биометрия разблокируется автоматически, как только пользователь подключит устройство к рабочей станции с агентом.

Сообщение пользователю

Вы можете настроить сообщение, которое увидит пользователь, когда подключит устройство к рабочей станции с агентом после разблокировки биометрии. Чтобы настроить сообщение:

1. В разделе **Конфигурация** перейдите в настройки политики.
2. Перейдите в раздел **Агенты** → **Сообщения пользователю**.
3. В поле **Разблокировка биометрической аутентификации на устройстве** введите текст сообщения.

4. Нажмите **Сохранить**.

Выключение и включение

Устройство пользователя можно выключить, например, на время отпуска сотрудника, и затем снова включить. Чтобы выключить или включить устройство, его не нужно подключать к рабочей станции.

Выключение

Чтобы выключить устройство пользователя:

1. Перейдите в раздел **Пользователи** и выполните поиск пользователя.
2. Нажмите на логин и перейдите в карточку пользователя.
3. В карточке устройства выберите действие **Выключить**.

При попытке использования выключенного устройства для аутентификации пользователь получит сообщение, что его сертификаты отозваны.

Приостановка действия сертификатов

Вы можете настроить временную приостановку действия сертификатов при выключении устройства:

1. Перейдите в настройки политики в раздел **Настройки PKI**.
2. Откройте раздел **Шаблоны** используемого УЦ.
3. Нажмите ✎ напротив нужного шаблона сертификата.
4. В параметрах шаблона включите опцию **Отзывать сертификат при отзыве/выключении устройства**.
5. Нажмите **Сохранить**.

Сертификаты будут отозваны с отметкой **Приостановка действия** (Certificate hold). Включите устройство, чтобы возобновить действие сертификатов.

Выключение устройства без выполнения входа в систему

В экстренном случае пользователь может самостоятельно выключить устройство без выполнения входа в операционную систему.

> **ПРИМЕЧАНИЕ**
>
> Устройство можно выключить только в том случае, если у рабочей станции есть связь с сервером Indeed CM, и у пользователя заданы ответы на секретные вопросы.
>
> Для определенных категорий пользователей можно запретить выключать устройства. Подробнее в настройках онлайн-разблокировки устройств

Чтобы выключить устройство пользователя:

1. Выберите **Выключение устройства** на экране входа Windows.
2. Укажите имя пользователя (логин или UPN).
3. Введите ответы на секретные вопросы.
4. Выберите устройство из списка выпущенных устройств и нажмите  .

Появится сообщение *Устройство было успешно выключено*.

Включение

Чтобы включить устройство пользователя:

1. Перейдите в раздел **Пользователи** и выполните поиск пользователя.
2. Нажмите на логин и перейдите в карточку пользователя.
3. В карточке устройства выберите действие **Включить**.

Выключение и включение устройств в Сервисе самообслуживания

Вы можете разрешить или запретить пользователям выключать и включать устройства самостоятельно в Сервисе самообслуживания. Чтобы настроить разрешение:

1. Перейдите в настройки политики использования устройств.
2. Перейдите в раздел **Поведение** → **Разрешения пользователя** → **Действия с выпущенным устройством**.
3. Включите опции **Выключать** и **Включать**.

Отзыв

Вы можете отозвать устройство, если оно повреждено, утеряно, изъято или нуждается в обновлении. После отзыва устройство можно заменить или изъять.

Особенности отзыва сертификатов

Если в параметрах шаблонов сертификатов используемого УЦ включена опция **Отзывать сертификат при отзыве/выключении устройства**, все сертификаты на устройстве отзываются без возможности восстановления.

При отзыве устройства по причинам **Устройство утеряно** или **Компрометация устройства** все сертификаты отзываются независимо от опции **Отзывать сертификат при отзыве/выключении устройства**.

Процесс отзыва устройства

1. Перейдите в раздел **Пользователи** и выполните поиск пользователя.
2. Нажмите на логин и перейдите в карточку пользователя.
3. В карточке устройства выберите действие **Отозвать**.
4. Выберите причину отзыва:
   - **Устройство неисправно** — техническая неисправность или физическое повреждение.
   - **Устройство утеряно** — устройство утеряно или украдено. Все сертификаты отзываются.
   - **Обновление устройства** — замена устройства на новое.
   - **Изъятие устройства** — удаление устройства из Indeed CM, например, при увольнении сотрудника.
   - **Компрометация устройства** — подозрение на компрометацию ключа. Все сертификаты отзываются.
5. Подключите устройство и нажмите **Отозвать**.
   Если устройство недоступно, включите опцию **Очистить устройство на агенте**, чтобы создать задачу для агента, установленного на рабочей станции пользователя.
   Подробнее об очистке устройства на агенте

Причина отзыва устройства отображается в карточке пользователя. При попытке использования отозванного устройства пользователь получит сообщение, что его сертификаты отозваны.

> **ОСОБЕННОСТИ ОТЗЫВА УСТРОЙСТВ РУТОКЕН БИО С ОЧИСТКОЙ НА АГЕНТЕ**
>
> Для устройства Рутокен ЭЦП 3.0 3250 БИО (Рутокен БИО), содержащего сертификат, защищенный биометрией, при отзыве с очисткой на агенте доступна только инициализация. При инициализации с устройства удаляются все данные, включая биометрию пользователя.
>
> Подробнее о работе с устройствами Рутокен БИО

Отзыв устройств в Сервисе самообслуживания

Вы можете разрешить или запретить пользователям отзывать устройства самостоятельно в Сервисе самообслуживания. Чтобы настроить разрешение:

1. Перейдите в настройки политики использования устройств.
2. Перейдите в раздел **Поведение** → **Разрешения пользователя** → **Действия с выпущенным устройством**.
3. Включите опцию **Отзывать**.

Изъятие

После отзыва устройство можно заменить или изъять. При изъятии устройство отвязывается от пользователя и имеет статус *Пустое*.

Чтобы изъять устройство:

1. В Консоли управления перейдите в раздел **Пользователи** и выполните поиск пользователя.
2. Нажмите на логин и перейдите в карточку пользователя.
3. В карточке устройства выберите действие **Изъять**.
4. Укажите, есть ли у вас доступ к устройству:
   - **Устройство доступно** — содержимое удаляется, устройство отвязывается от пользователя.
   - **Устройство недоступно (потеряно или повреждено)** — содержимое не удаляется, устройство только отвязывается от пользователя. Перейдите к шагу 6.
5. Подключите устройство к рабочей станции и выберите действие:
   - **Очистить** — с устройства удаляется только управляемое содержимое: данные, записанные через Indeed CM (сертификаты и ключи, аутентификаторы Indeed AM, идентификаторы SNS, сложный пароль Рутокен Логон). Данные, записанные на устройство вне Indeed CM, сохраняются.
   - **Инициализировать** — с устройства удаляются все данные.
6. В разделе **Дополнительно** в поле **Новый PIN-код пользователя** укажите PIN-код, который установится на устройстве после изъятия.

   Если поле **Новый PIN-код пользователя** оставить пустым, установится PIN-код из настроек типа устройства (**Конфигурация** → **Типы устройств**). Обязательно укажите PIN-код, если значение из настроек типа устройства не соответствует требованиям инициализации в политике (**Выпуск** → **Инициализация**).
7. Для устройств с СКЗИ заполните поля:
   - **Номер и дата документа** — заполняются автоматически на основании документа, по которому происходит уничтожение/изъятие СКЗИ.

- **Пользователь, производивший уничтожение/изъятие** — через запятую укажите ФИО сотрудников органа криптографической защиты или пользователей СКЗИ, выполнивших уничтожение/изъятие.

8. Нажмите **Изъять**.

> **ОСОБЕННОСТИ ИЗЪЯТИЯ УСТРОЙСТВ РУТОКЕН БИО**
>
> - При изъятии с очисткой на устройстве остаются биометрические данные пользователя. Устройство можно выпустить тому же пользователю без повторной регистрации биометрии.
> - Если при изъятии с очисткой с устройства удаляется управляемый сертификат, защищенный биометрией, пользователь должен пройти биометрическую аутентификацию, чтобы подтвердить удаление сертификата. Подтверждение не нужно, если в параметрах шаблона сертификата используемого УЦ включена опция **Не удалять сертификат при обновлении/очистке устройства**.
> - При изъятии с инициализацией удаляются все данные, включая биометрические данные пользователя.
>
> Подробнее о работе с устройствами Рутокен БИО

Замена

Indeed CM позволяет заменить устройство пользователя. Есть два вида замены:

- **Временная**
  Если сотрудник забыл свое устройство дома, оператор может выпустить для него новое устройство с ограниченным сроком действия для работы в офисе. Основное устройство выключается, а на замену ему выпускается временное устройство. Когда истекает срок действия временного устройства, оно отзывается, а основное устройство возобновляет работу.
- **Постоянная**
  Если устройство неисправно, утеряно или компрометировано, оператор может заменить его на новое. Старое устройство отзывается, а новое становится основным.

Состояние сертификатов при замене устройства

Состояние сертификатов при замене устройства зависит от настроек в шаблонах сертификатов УЦ.

Как настроить параметры шаблонов сертификатов УЦ

1. Перейдите в раздел **Конфигурация** и откройте настройки политики использования устройств.
2. В разделе **Настройки PKI** выберите нужный УЦ и перейдите в раздел **Шаблоны**.
3. Нажмите ✎ напротив нужного шаблона сертификата.

Резервная копия ключевой пары

Наличие резервной копии ключевой пары в базе данных Indeed CM определяет два сценария работы с сертификатами при замене устройства:

- Резервная копия ключевой пары сохранена – при выпуске нового устройства (временного или постоянного) на него переносится исходный сертификат с сохранением ключевой пары.
- Резервной копии ключевой пары нет – при выпуске нового устройства формируется новый сертификат с новой ключевой парой.

Чтобы сохранить резервную копию ключевой пары и записать ее на новое устройство при замене, в параметрах шаблона сертификата УЦ включите опции **Создавать резервную копию ключа** и **Записывать копию ключа при временной замене устройства**.

Отзыв сертификата при отзыве или выключении устройства

Состояние сертификатов при замене устройства дополнительно зависит от опции **Отзывать сертификат при отзыве/выключении устройства**, которая настраивается в параметрах шаблона сертификата УЦ:

- Включена – срок действия сертификатов приостанавливается в УЦ при отзыве или выключении устройства.
- Выключена – сертификаты остаются действительными.

> **ПРИМЕЧАНИЕ**
> При наличии резервной копии ключевой пары сертификат остается действительным независимо от состояния опции **Отзывать сертификат при отзыве/выключении устройства**. Сертификат переносится на новое устройство.

Временная замена

Как происходит временная замена:

1. Основное устройство выключается. Выпускается временное устройство.

	Состояние сертификата
С резервной копией ключевой пары	Сертификат остается действительным и переносится на временное устройство, если в шаблоне сертификата включена опция **Записывать копию ключа при временной замене устройства**
Без резервной копии ключевой пары	Срок действия сертификата на основном устройстве приостанавливается в УЦ, если в шаблоне сертификата включена опция **Отзывать сертификат при отзыве/выключении устройства**. На временное устройство записывается новый сертификат с новой ключевой парой

2. Заканчивается срок действия временного устройства или сотрудник получает доступ к основному устройству. После запуска службы Card Monitor временное устройство

отзывается, основное – включается.

Состояние сертификата	
С резервной копией ключевой пары	Сертификат остается действительным
Без резервной копии ключевой пары	Сертификат на временном устройстве отзывается. Сертификат на основном устройстве возобновляет работу

Как запустить службу Card Monitor

Служба Card Monitor запускается ежедневно автоматически по расписанию, заданному в Мастере настройки в разделе **Card Monitor**.

Чтобы запустить Card Monitor вручную:

- **ОС Windows**
  Откройте консоль Powershell от имени администратора на сервере Indeed CM и запустите:
  ```
  C:\Program Files\Indeed CM\CardMonitor\Cm.CardMonitor.exe
  ```
- **ОС Linux**
  Откройте терминал от имени администратора на сервере Indeed CM и запустите:
  ```
  cd /opt/indeed/cm/cardmonitor && ./Cm.CardMonitor
  ```

Постоянная замена

Старое устройство отзывается, вместо него выпускается новое устройство.

Состояние сертификата	
С резервной копией ключевой пары	Сертификат остается действительным и переносится на новое устройство

Состояние сертификата	
Без резервной копии ключевой пары	Сертификат на старом устройстве отзывается в УЦ, если в шаблоне сертификата включена опция **Отзывать сертификат при отзыве/ выключении устройства**. На новое устройство записывается новый сертификат с новой ключевой парой

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> PIN-код устройства не переносится на новое устройство. PIN-код устанавливается в соответствии с настройками политики использования устройств.

Замена устройства в карточке пользователя

Чтобы заменить устройство пользователя:

1. Перейдите в раздел **Пользователи** и выполните поиск пользователя.
2. Нажмите на логин и перейдите в карточку пользователя.
3. В карточке устройства выберите действие **Заменить**.
4. Выберите вид замены:
   - **Временная**. Укажите срок окончания действия временного устройства.
   - **Постоянная**. Укажите причину.
5. Введите имя временного устройства.
6. Подключите новое устройство к рабочей станции.
7. Укажите PIN-код администратора в разделе **Дополнительно**, если новое устройство не добавлено в Indeed CM.
8. Нажмите **Заменить**.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Если в политике использования устройств настроена инициализация устройства при замене, то новое устройство инициализируется. Все данные на устройстве удаляются.

При временной замене в карточке пользователя отображаются два устройства: основное устройство выключено, новое устройство выпущено на определенный срок.

Белов Евгений Александрович

Логин DEMO\Evgeniy.Belov
Путь demo.local/Indeed CM RU/Белов Евгений Александрович
Политика Базовая политика
E-mail
Телефон

Загрузить фотографию | Пользователь КриптоПро 2.0 | Сбросить ответы на секретные вопросы | Сбросить пароль пользователя

Назначенные устройства

Rutoken ECP, 0756770190	Евгений Белов	01.04.2017 0:00	Выпущено
Rutoken S, 0755398982	Евгений Белов		Выключено

Выпустить устройство | Назначить устройство

Замена на AirCard

Если Indeed CM интегрирован с Indeed AirCard Enterprise, то аппаратное устройство можно заменить на сетевую смарт-карту AirCard.

Чтобы заменить устройство на AirCard, в карточке устройства нажмите **Заменить на AirCard**.

Обновление

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

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.

Процесс обновления

1. Перейдите в раздел **Пользователи** и выполните поиск пользователя.
2. Нажмите на логин и перейдите в карточку пользователя.
3. В карточке устройства выберите действие **Обновить**.
4. Введите PIN-код пользователя.
   Если поле оставить пустым, Indeed CM подставит значение из настроек типа устройства (**Конфигурация** → **Типы устройств**).
5. Подключите устройство и нажмите **Обновить**.
   Если устройство недоступно, включите опцию **Обновить устройство на агенте**, чтобы

создать задачу для агента, установленного на рабочей станции пользователя. Опция недоступна, если содержимое устройства защищено биометрией.
Подробнее об обновлении устройства на агенте

6. Выберите шаблоны, по которым формируются сертификаты для записи на устройство. Обязательные сертификаты запишутся на устройство автоматически.
7. Если в политике настроена интеграция со СМЭВ и сертификат выпускается по шаблону для КриптоПро УЦ 2.0 или Валидата УЦ, отобразится форма проверки СМЭВ. Проверьте данные пользователя.
Подробнее о проверке в СМЭВ
8. Если в политике настроено отслеживание сторонних сертификатов и на устройстве найдены такие сертификаты, отобразится их список.
Отметьте сертификаты, которые нужно отслеживать, и нажмите **OK**.
Подробнее об отслеживаемых сертификатах
9. Нажмите **Обновить**.

ОСОБЕННОСТИ ОБНОВЛЕНИЯ УСТРОЙСТВ РУТОКЕН БИО

Если вы обновляете устройство Рутокен ЭЦП 3.0 3250 БИО (Рутокен БИО) и в процессе обновления записывается или удаляется сертификат, защищенный биометрией, откроется окно биометрической аутентификации. Пользователь должен пройти биометрическую аутентификацию, чтобы подтвердить обновление или удаление сертификата. Аутентификация может потребоваться несколько раз — например, при создании нового защищенного сертификата и удалении старого.

Подтверждение не требуется, если в параметрах шаблона сертификата включена опция **Не удалять сертификат при обновлении/очистке устройства**.

Подробнее о работе с устройствами Рутокен БИО

Проверка запроса на обновление сертификата в УЦ

Если в шаблоне сертификата отключена автоматическая обработка запроса на обновление, обновление устройства приостанавливается до решения УЦ. В окне обновления устройства появляется сообщение *Обновление устройства ожидает решения*. Устройство переходит в состояние *В ожидании*.

Как настроить проверку запроса на обновление сертификата в УЦ

1. В разделе **Конфигурация** перейдите в настройки политики.
2. В разделе **Настройки PKI** выберите УЦ и перейдите в раздел **Шаблоны**.
3. Выберите шаблон, нажмите ✎ и отключите опцию **Автоматически одобрять подписанный запрос на обновление сертификата**.

Когда УЦ обработает запрос:

- Если запрос одобрен, сертификат получает статус *Одобрен* и записывается на устройство. В карточке устройства нажмите **Продолжить обновление устройства**. Если устройство недоступно, включите опцию **Продолжить обновление на агенте** — опция недоступна, если содержимое устройства защищено биометрией.
- Если запрос отклонен — отзовите и очистите устройство и выпустите его заново, либо отмените обновление и обновите устройство заново.

> ⚠ **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.

Вы можете настроить рассылку уведомлений по электронной почте, чтобы получать уведомления о статусе проверки.

Отмена обновления

Вы можете отменить обновление устройства, если в политике использования устройств в разделе **Поведение** → **Разрешения администратора** включена опция **Отменять обновление устройства**.

Чтобы отменить обновление устройства:

1. В карточке устройства выберите действие **Отменить обновление**.
2. Введите PIN-код пользователя.

3. Подключите устройство и нажмите **Отменить обновление**.

   Если устройство недоступно, включите опцию **Отменить обновление на агенте**, чтобы создать задачу для агента, установленного на рабочей станции пользователя.

   Подробнее об отмене обновления на агенте

> **ОСОБЕННОСТИ ОТМЕНЫ ОБНОВЛЕНИЯ УСТРОЙСТВ РУТОКЕН БИО**
>
> Отмена обновления на агенте недоступна для устройства Рутокен ЭЦП 3.0 3250 БИО (Рутокен БИО), которое содержит сертификат, защищенный биометрией.
>
> Подробнее о работе с устройствами Рутокен БИО

Обновление устройств в Сервисе самообслуживания

Вы можете разрешить или запретить пользователям обновлять устройства самостоятельно в Сервисе самообслуживания. Чтобы настроить разрешение:

1. Перейдите в настройки политики использования устройств.
2. Перейдите в раздел **Поведение** → **Разрешения пользователя** → **Действия с выпущенным устройством**.
3. Включите опцию **Обновлять**.

Обновление биометрии

Вы можете обновить биометрию (отпечатки пальцев), зарегистрированную на устройстве Рутокен ЭЦП 3.0 3250 БИО (Рутокен БИО), при личном присутствии пользователя.

Подробнее о работе с устройствами Рутокен БИО

Предварительные настройки

Действие **Обновить биометрию** доступно в карточке устройства для членов роли с привилегией *Обновление биометрии*. Чтобы настроить привилегии, перейдите в раздел **Конфигурация** → **Роли**.

Процесс обновления биометрии

1. Перейдите в раздел **Пользователи** и выполните поиск пользователя.
2. Нажмите на логин и перейдите в карточку пользователя.
3. В карточке устройства Рутокен БИО выберите действие **Обновить биометрию**.
4. Подключите к рабочей станции устройство Рутокен БИО и сканер отпечатков пальцев.
5. Нажмите **Обновить**. Откроется окно биометрической аутентификации.
6. Пользователь прикладывает палец к сканеру, чтобы подтвердить обновление биометрии.
7. В окне обновления биометрии пользователь регистрирует от одного до трех отпечатков пальцев, последовательно прикладывая пальцы к сканеру.
8. Нажмите **Продолжить**.
9. Когда обновление биометрии завершится, нажмите **Закрыть**.

Выпуск 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.

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.

Предварительные настройки

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.

Выпуск смарт-карты с печатью

1. Перейдите в раздел **Пользователи** и выполните поиск пользователя.
2. Нажмите на логин и перейдите в карточку пользователя.
3. Нажмите **Выпустить устройство**.
4. Укажите **Имя 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 нанести изображение на ранее выпущенные карты без использования принтера. Для печати на ранее выпущенной карте:

1. Поместите карту в лоток принтера.
2. Перейдите в раздел **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**.

Управление СКЗИ

Назначенные СКЗИ отображаются в карточке пользователя и в Сервисе самообслуживания.

Предварительные настройки

Чтобы настроить управление СКЗИ из карточки пользователя, выполните следующие действия:

1. Запустите 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.

Список привилегий

Привилегии для управления СКЗИ

- Просмотр репозитория СКЗИ
- Добавление СКЗИ
- Назначение СКЗИ
- Обновление СКЗИ
- Уничтожение/изъятие СКЗИ

Привилегии для управления обучающими курсами по работе с СКЗИ

- Завершение обучений СКЗИ
- Отмена обучений СКЗИ
- Одобрение завершения обучения СКЗИ

Чтобы разрешить пользователю просмотр и печать нормативных документов СКЗИ:

1. Перейдите в настройки политики в раздел **Поведение** → **Разрешения пользователя** → **Действия с СКЗИ**.
2. Включите опцию **Просматривать**.

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**, заполните поля и нажмите **Добавить**.

Обязательные поля:

- **Тип объекта**
- **Тип СКЗИ**
- **Описание**
- **Серийный номер**
- **Номер и дата документа**. 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 объекта 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 Indeed CM, не уничтожены/не изъяты и не назначены другому пользователю. Для этого:

1. Нажмите **Назначить СКЗИ** и задайте фильтры поиска.
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. Нажмите  , и номер документа выставится автоматически по шаблону нумерации, настроенному для документов данного объекта 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.

Выпадающий список **Вид нормативного документа** отображается, если вы настроили шаблон печати для данного объекта СКЗИ в текущем состоянии в разделе Нормативные документы.
Если вы не настроили шаблон печати, отображается выпадающий список **Шаблон печати**, где можно выбрать любой из шаблонов, загруженных для данного объекта СКЗИ в разделе Шаблоны печати.

3. Нажмите **Распечатать документ**.

Подпись документов

Нормативные документы СКЗИ можно подписать, если в Indeed CM настроена функция внутреннего электронного документооборота, и у вас есть подходящий сертификат подписи.

Как подписать нормативный документ СКЗИ

Обучающие курсы по работе с СКЗИ

С помощью Indeed CM вы можете предоставить пользователям доступ к работе с СКЗИ. Пользователи проходят обучающие курсы, ожидают проверки администратора и получают документ, подтверждающий специальную подготовку и допуск к самостоятельной работе с СКЗИ – заключение органа криптографической защиты.

Чтобы создать обучающие курсы, перейдите в раздел **Конфигурация** → **СКЗИ** → Обучающие курсы. Чтобы управлять обучением пользователя по работе с СКЗИ, в карточке пользователя перейдите в раздел **СКЗИ** на вкладку **Обучающие курсы**.

Пользователи проходят обучающие курсы в Сервисе самообслуживания в разделе **Ваши СКЗИ** на вкладке **Обучающие курсы**.

Процесс обучения

Администраторам доступны следующие действия по управлению обучением пользователя:

- Назначить обучение
- Завершить обучение
- Отменить обучение
- Одобрить завершение обучения

Этапы обучения	Описание	Состояние обучения
Начало обучения	• Пользователь начинает обучение самостоятельно • Администратор назначает обучение на пользователя	*В процессе*
Завершение обучения	• Пользователь проходит обучение и завершает его самостоятельно • Администратор завершает обучение пользователя	*Ожидание одобрения*
Подтверждение завершения обучения	Чтобы подтвердить завершение обучения, администратор нажимает **Одобрить завершение обучения** и формирует документ о прохождении обучения. Пользователь получает допуск к работе с СКЗИ.	*Завершено*

Документ о прохождении обучения формируется по шаблону, настроенному в разделе **Конфигурация** → Шаблоны печати. Номер документа выставляется автоматически по шаблону нумерации, настроенному в разделе **Конфигурация** → **СКЗИ** → Нормативные документы.

Отмена обучения

Вы можете отменить обучение, например, если пользователь не сдал тест на знание правил работы с СКЗИ. Отмена доступна для обучений в состоянии *В процессе* и *Ожидание одобрения*.

Вы можете разрешить пользователям отменить обучение самостоятельно. Чтобы пользователи могли отменить обучение самостоятельно:

1. Перейдите в настройки политики в раздел **Поведение** → **Разрешения пользователя** → **Действия с СКЗИ**.
2. Включите опцию **Отменять обучение**.

Настройка уведомлений

Настройте уведомления, чтобы сообщать администраторам и пользователям о событиях, связанных с обучением.

Уведомления администратора

Администраторы могут получать уведомления о следующих событиях:

- Начало обучения СКЗИ
- Отмена обучения СКЗИ
- Завершение обучения СКЗИ

Чтобы настроить уведомления для администраторов, перейдите в настройки политики в раздел **Уведомления администратора**.

Уведомления пользователя

Пользователи могут получать уведомления о следующих событиях:

- Начало обучения СКЗИ
- Отмена обучения СКЗИ
- Одобрение завершения обучения СКЗИ

Чтобы настроить уведомления для пользователей, перейдите в настройки политики в раздел **Уведомления пользователя**.

Управление документами

Функция внутреннего электронного документооборота Indeed CM ЭДО позволяет пользователям, администраторам и операторам обмениваться документами в рамках выпуска сертификатов и работы с СКЗИ. Через Indeed CM ЭДО проходят два типа документов:

- Документы для получения сертификата
- Нормативные документы СКЗИ

Управление документами доступно в карточке пользователя и в разделе **Документы**.

Предварительные настройки

Чтобы управлять документами, убедитесь, что выполнены следующие настройки.

Общие

- В Мастере настройки в разделе **Общие функции** включена опция **Внутренний документооборот**.
- В разделе **Конфигурация** → **Роли** членам роли предоставлены привилегии:
  - Просмотр репозитория документов
  - Добавление документа
  - Изменение документа
  - Удаление документа
  - Одобрение документа

Для работы с нормативными документами СКЗИ

- В Мастере настройки в разделе **Функции системы** → **Журнал учета СКЗИ** включена опция **Вести журнал учета СКЗИ**.
  Подробнее о настройке работы с СКЗИ

- В разделе **Конфигурация** → **Роли** членам роли предоставлены привилегии:

  - Просмотр шаблона нормативных документов
  - Изменение шаблона нормативных документов

Подпись документов

В Консоли управления администратор может добавлять документы для получения сертификата и нормативные документы СКЗИ и подписывать их электронной подписью.

Требования к сертификату подписи

- Есть устройство, которое содержит сертификат подписи.
- Сертификат 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).

> **ОСОБЕННОСТИ ПОДПИСИ С ПОМОЩЬЮ УСТРОЙСТВ РУТОКЕН БИО**
>
> Если вы подписываете документ с помощью устройства Рутокен ЭЦП 3.0 3250 БИО (Рутокен БИО) и сертификат подписи защищен биометрией, в процессе подписания откроется окно биометрической аутентификации. Подключите к рабочей станции сканер отпечатков пальцев и пройдите биометрическую аутентификацию, чтобы подтвердить подпись.
>
> Подробнее о работе с устройствами Рутокен БИО

Чтобы подписать документ:

1. В карточке пользователя в разделе **Документы** нажмите **Добавить документ**.
2. Выберите тип документа и загрузите файл.
3. (Опционально) Заполните поле **Описание**.
4. Нажмите **Подписать документ**.
5. Подключите устройство с сертификатом подписи и выберите его в списке **Устройство**.
6. В списке **Сертификат** выберите подходящий сертификат.
7. В списке **Тип подписи** выберите тип электронной подписи. Подробнее о типах подписи
8. Введите PIN-код пользователя.
9. Нажмите **Добавить**.

Подпись нормативных документов СКЗИ при печати

1. Найдите экземпляр СКЗИ:

- В карточке пользователя — раздел **Назначенные СКЗИ**.
- В разделе **СКЗИ** — поиск по списку.

2. Нажмите  напротив экземпляра.
3. Выберите шаблон печати документа. В зависимости от настроек печати нормативных документов СКЗИ отображается один из списков:
   - **Вид нормативного документа** — список шаблонов печати, привязанных к объекту СКЗИ в разделе Конфигурация → СКЗИ → Нормативные документы.
   - **Шаблон печати** — список всех шаблонов печати, загруженных в разделе Конфигурация → Шаблоны печати.
4. Нажмите **Распечатать документ**. Откроется файл документа.
5. Нажмите **Подписать документ**.
6. Подключите устройство и выберите его в списке **Устройство**.
7. В списке **Сертификат** выберите сертификат подписи.
8. В списке **Тип подписи** выберите тип электронной подписи. Подробнее о типах подписи
9. Введите PIN-код пользователя.
10. Нажмите **Подписать**.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Если экземпляр СКЗИ, для которого сформирован документ, не назначен на пользователя, документ нельзя подписать.

Подписанные документы появляются в списке **Документы** в карточке пользователя. Чтобы скачать файл подписи, нажмите  .

Проверка документов пользователей

Вы можете проверять документы, загруженные пользователями — одобрять их или отклонять.

Если в политике настроена автоматическая рассылка уведомлений по электронной почте, вы получите уведомление, когда пользователь загрузит документ. К уведомлению прикреплен PDF документа.

Настройка проверки документов

По умолчанию запрос на сертификат проверяется в удостоверяющем центре (УЦ). Вы можете настроить дополнительную проверку документов сертификата при выпуске и обновлении устройств. Документы проверяет администратор или оператор Indeed CM.

Чтобы настроить проверку документов:

1. В разделе **Конфигурация** перейдите в настройки политики использования устройств.
2. В разделе **Настройки PKI** выберите нужный УЦ и перейдите в раздел **Шаблоны**.
3. Нажмите ✎ напротив нужного шаблона сертификата.
4. Настройте опции проверки документов сертификата в зависимости от планируемого сценария работы.

Опция	Действие
Автоматически одобрять запрос на сертификат	Выключите, чтобы администратор проверял запрос на выпуск сертификата перед отправкой в УЦ.
Автоматически одобрять подписанный запрос на обновление сертификата	Выключите, чтобы администратор проверял запрос на обновление сертификата перед отправкой в УЦ.
Требовать подписанный документ сертификата перед продолжением выпуска/ обновления устройства	Включите, чтобы пользователь мог записать сертификат на устройство только после того, как предоставит подписанную форму сертификата. После одобрения запроса в УЦ форма сертификата доступна пользователю в Сервисе самообслуживания.

После настройки выпуск или обновление устройства приостанавливается до решения администратора. Устройство переходит в состояние *В ожидании*.

Проверка документов сертификата

1. Перейдите в раздел **Пользователи** 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. Нажмите ?.

5. Установите связь между документом, шаблоном сертификата и устройством:
    1. В списке **Сертификат** выберите шаблон, по которому выпускается сертификат.
    2. В списке **Устройство** выберите устройство, на которое записывается сертификат.
6. Нажмите **Одобрить**.

Если пользователь сформировал документ по шаблону на вкладке **Содержимое устройства**, связь устанавливается автоматически — одобрять не нужно.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> Если на устройство одновременно записываются несколько сертификатов, устройство можно выпустить только когда оба запроса одобрены в УЦ. Если один сертификат одобрен автоматически и имеет статус *Действителен*, он будет записан на устройство вместе со вторым сертификатом.

Проверка нормативных документов СКЗИ

1. Перейдите в раздел **Пользователи** 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. Нажмите .
5. В окне одобрения выберите экземпляр СКЗИ, к которому относится документ.
6. Нажмите **Одобрить**.

Если пользователь сформировал документ по шаблону, связь устанавливается автоматически — одобрять не нужно.

Отметка о получении оригинала

Вы можете отметить, что пользователь предоставил оригинал документа.

При добавлении нового документа:

1. Нажмите **Добавить документ**.
2. Выберите тип документа и загрузите файл.
3. Введите описание.

4. Включите опцию **Оригинал получен**.

При редактировании добавленного документа:

1. Нажмите  напротив документа.
2. Включите опцию **Оригинал получен**.

Типы электронной подписи

В Indeed CM поддерживаются следующие типы электронной подписи:

- CMS
- CAdES-BES
- CAdES-T
- CAdES-X Long Type 1
- CAdES-A

Выбор типа зависит от сертификата подписи:

- **CMS** — для сертификатов, выпущенных в любом поддерживаемом УЦ и записанных на любые поддерживаемые устройства.
- **CAdES** — только для сертификатов КриптоПро УЦ 2.0, записанных на устройство с поддержкой ГОСТ-криптографии (Рутокен, JaCarta, ESMART).

Настройка окружения для CAdES

Чтобы использовать подпись CAdES, настройте окружение на клиентских рабочих станциях:

- КриптоПро CSP с компонентами КриптоПро TSP Client и КриптоПро OCSP Client
- КриптоПро ЭЦП Browser plug-in
- Indeed CM Middleware для нужной модели устройства

> **ПРИМЕЧАНИЕ**
>
> Убедитесь, что на рабочих станциях настроены политики КриптоПро TSP Client и КриптоПро OCSP Client. Подробнее о настройке политик на сайте КриптоПро

Настройка разрешенного типа подписи в политике

При подписи документов в Консоли управления вы можете выбрать тип подписи. При подписи в Сервисе самообслуживания выбор недоступен — разрешенный тип подписи настраивается в политике.

Чтобы определить, какой тип подписи разрешено использовать пользователям в Сервисе самообслуживания:

1. В разделе **Конфигурация** перейдите в настройки политики использования устройств.
2. Перейдите в раздел **Поведение** → **Разрешения пользователя** → **Действия с документами**.
3. Выберите значение в списке **Использовать тип подписи**.
4. Нажмите **Сохранить**.

Если выбран один из типов CAdES, пользователи могут подписывать документы только сертификатом КриптоПро УЦ 2.0, записанным на устройство с поддержкой ГОСТ-криптографии.

Устройства

В разделе **Устройства** Консоли управления вы можете управлять устройствами пользователей Indeed CM.

> **ПРИМЕЧАНИЕ**
> Действия с устройством конкретного пользователя доступны в карточке устройства.

Поиск

Если устройство подключено к рабочей станции, его можно найти на вкладке **Подключенное устройство**. Если устройство недоступно, воспользуйтесь расширенным поиском на вкладке **Расширенный**.

Поиск по подключенным устройствам

Подключите устройство к рабочей станции и нажмите  . Чтобы просмотреть тип устройства, наведите указатель мыши на изображение устройства.

Расширенный поиск

На вкладке **Расширенный** можно найти устройство по одному или нескольким фильтрам:

- Серийный номер
- Тип
- Комментарий
- Состояние
- Статус содержимого
- Имя пользователя
- Политика
- Теги

В поле **Серийный номер** поддерживается подстановочный символ `*`. Чтобы найти устройство по части серийного номера, введите `*` и часть номера. Чтобы вывести список всех устройств, введите `*`.

Установите фильтры и нажмите  .

> **ПРИМЕЧАНИЕ**
> Фильтр по статусу содержимого доступен, если в Мастере настройки настроено расписание запуска службы Card Monitor.

В результатах поиска доступны следующие действия:

 — сохранить результаты поиска в файл формата PDF или CSV

 — просмотреть содержимое устройства

 — просмотреть PIN-код администратора

Администраторы имеют доступ к PIN-кодам всех устройств, добавленных в Indeed CM. Администраторы отдельных политик имеют доступ к PIN-кодам устройств, назначенных или выпущенных пользователям, на которых действуют эти политики.

Добавление

1. Подключите устройство к рабочей станции и нажмите **Добавить устройство**.
2. Если устройство поддерживает аппаратную криптографию и в Indeed CM ведется учет средств криптографической защиты информации (СКЗИ), то отобразится поле **Номер и дата документа**, в соответствии с которым изготовится СКЗИ.
3. PIN-код администратора подставляется автоматически из настроек, заданных в разделе **Конфигурация** → Типы устройств. Если фактический PIN-код на устройстве отличается, введите его вручную в разделе **Дополнительно**.
4. Нажмите **Добавить**, затем нажмите **Закрыть**.

Устройства можно добавлять автоматически, подключая их последовательно к одному и тому же считывателю.

⚠ **ПРЕДУПРЕЖДЕНИЕ**

Если PIN-код администратора неверный, он может заблокироваться.

Подробнее о блокировке PIN-кода администратора

У каждого устройства есть счетчик неудачных попыток ввода PIN-кода администратора. Например, на устройствах Рутокен по умолчанию установлено 10 попыток ввода PIN-кода администратора. Если на устройстве, которое добавляется в Indeed CM, осталась одна попытка, и введен неверный PIN-код, то PIN-код администратора заблокируется.

На некоторых устройствах разблокировать PIN-код администратора невозможно. В случае блокировки PIN-кода администратора необходимо инициализировать устройство, но при этом все данные, хранящиеся на нем, будут удалены.

Смена PIN-кода администратора

В зависимости от настроек, заданных в разделе **Конфигурация** → Типы устройств, при добавлении устройства PIN-код администратора автоматически меняется на случайное или неслучайное значение.

При автоматической замене PIN-кода администратора на случайное значение новый PIN-код сохраняется только в базе данных Indeed CM. Без доступа к Indeed CM разблокировка PIN-кода пользователя и инициализация устройства будут недоступны.

Выпуск

Выпуск устройства выполняется так же, как в карточке пользователя. Подробнее о выпуске устройства

Удаление

Устройство можно удалить из Indeed CM независимо от того, доступно оно физически или нет.

Чтобы удалить устройство:

1. Выполните поиск устройства и нажмите ✖ .
2. Выберите одну из опций:
    - **Устройство доступно** — подключите устройство к рабочей станции. При необходимости включите опцию **Инициализировать устройство**, чтобы очистить все данные на устройстве.
    - **Устройство недоступно** — выберите, если устройство утеряно или повреждено.
3. Если устройство поддерживает аппаратную криптографию и в Indeed CM ведется учет СКЗИ, в поле **Номер и дата документа** автоматически сформируются данные документа об уничтожении СКЗИ.
4. Нажмите **Удалить**.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> При удалении недоступного устройства со случайным PIN-кодом администратора PIN-код не сбрасывается на исходное значение. Вы не сможете управлять таким устройством вне Indeed CM.

Отозванное устройство можно изъять у пользователя без удаления из Indeed CM. Изъять можно как доступное, так и недоступное устройство.

Инициализация пустых устройств

Инициализация доступна для устройств в состоянии *Пустое*, то есть не закрепленных за пользователем. Инициализацию можно выполнить в Консоли управления или через клиентский агент.

> ⓘ **ПРИМЕЧАНИЕ**
>
> Опция **Инициализировать** доступна, если члены роли обладают привилегией **Инициализация устройства**. Привилегия назначается в разделе **Конфигурация** → **Роли**.

Чтобы инициализировать устройство:

1. Выполните поиск устройства и нажмите ✎, чтобы просмотреть его содержимое.
2. Подключите устройство к рабочей станции и нажмите **Инициализировать**. Если устройство недоступно, создайте задачу на клиентском агенте — выберите опцию

Инициализировать устройство на агенте.

3. Если PIN-код администратора на устройстве отличается от сохраненного в Indeed CM, введите актуальный PIN-код в разделе **Дополнительно**. При необходимости задайте **Новый PIN-код пользователя**.
4. Нажмите **Инициализировать**.

После инициализации PIN-код пользователя сбрасывается на значение, указанное в разделе **Конфигурация** → Типы устройств.

Если на шаге 3 вы указали PIN-код администратора, то после инициализации устройства PIN-код обновится в базе данных Indeed CM.

> **ПРИМЕЧАНИЕ**
>
> Устройства Rutoken и eToken можно инициализировать при любом состоянии PIN-кода администратора: известном, неизвестном или заблокированном.
>
> - Если PIN-код администратора не указан, после инициализации на устройство записывается PIN-код из базы данных Indeed CM.
> - Если PIN-код указан, после инициализации он записывается на устройство и в базу данных Indeed CM.

Изменение тегов

Вы можете изменить теги для нескольких устройств одновременно. Теги создает администратор в разделе **Конфигурация** → Теги.

Чтобы добавить или удалить теги:

1. В разделе **Устройства** перейдите на вкладку **Расширенный** и выполните поиск устройств.
2. Нажмите **Изменить теги**.
3. Укажите **Теги для добавления** или **Теги для удаления** и нажмите **Изменить**.

Пакетный импорт

Вы можете добавить в Indeed CM несколько устройств одновременно с помощью файла пакетного импорта.

1. Перейдите в раздел **Устройства** Консоли управления.
2. Нажмите **Импортировать устройства**.
3. Загрузите подготовленный файл со списком устройств.
4. Нажмите **Импортировать**.

Формат файла импорта

Поддерживаются файлы формата TXT (UTF-8) и CSV. Для каждого устройства добавьте строку с необходимым набором полей. Укажите поля через точку с запятой в следующем порядке:

```
Serial Number;Card Type;Model;Form Factor;Admin PIN;Gost Admin PIN;Comment;Tags;SKZI Document Number;Time Created
```

Поле	Описание	Обязательное поле
`Serial Number`	Серийный номер устройства	✓
`Card Type`	Тип устройства. Укажите имя в том виде, в котором оно задано в разделе **Конфигурация** → Типы устройств.	✓
`Model`	Модель устройства. Доступно для устройств Рутокен, JaCarta, eToken PRO Java 72K и IDPrime MD, если в разделе **Конфигурация** → **Типы устройств** заданы отдельные настройки для моделей.	—
`Form Factor`	Форм-фактор: `SmartCard` (по умолчанию), `UsbToken`, `MicroSD`.	—
`Admin PIN`	PIN-код администратора	—
`Gost Admin PIN`	PIN-код администратора для приложения ГОСТ на устройствах JaCarta	—
`Comment`	Комментарий	—
`Tags`	Теги через запятую. Теги необходимо предварительно создать в разделе **Конфигурация** → Теги.	—

Поле	Описание	Обязательное поле
`SKZI Document Number`	Номер документа о постановке на учет СКЗИ (тип объекта: ключевой носитель). Заполняется, если устройство поддерживает аппаратную криптографию и в Indeed CM ведется учет СКЗИ. Если не указан, выставляется автоматически после добавления устройства. Подробнее об учете СКЗИ	—
`Time Created`	Время создания документа о постановке на учет СКЗИ в формате `yyyyMMddHHmmss` (UTC). Если не указано, выставляется автоматически после добавления устройства.	—

Значения по умолчанию

Чтобы не дублировать одинаковые значения в каждой строке, используйте строку `default`. Укажите `default` вместо серийного номера — остальные поля этой строки станут значениями по умолчанию для всех последующих строк. В последующих строках достаточно указать только серийный номер устройства и поля, которые отличаются от значений `default`.

Пример файла импорта

```
default;Rutoken S;;UsbToken;87654321;;Московский офис;VPN,IT;;
0755398982
0756309531
default;Rutoken ECP;;UsbToken;87654321;;Бухгалтерия;VPN;ВН-169;20220412134200
0894130607
0894130536
default;Rutoken ECP SC;;;87654321;;;;ВН-170;20220329111500
0862287268
0862287403
default;Rutoken 2151;;UsbToken;87654321;;;;ВН-171;
0963474291
default;ESMART Token 64K;;UsbToken;12345678;;;;;
609BC06881C7
B0B340508942
E0D8806291CB;;;SmartCard;;;;;
D050806291CB;;;SmartCard;;;;;
default;eToken PRO Java 72K;eToken PRO Java 72K OS755;SmartCard;1234567890;;;;
01cec45d
default;JaCarta;JC210;UsbToken;00000000;;;;
0B53002004417597
0B53001122617597
default;JaCarta;JC300;SmartCard;00000000;;;;
0153001910367618
default;JaCarta;JC267-1236J.J01Q01;UsbToken;00000000;1234567890;;;ВН-172;
6082057494937678
4C54001522634C50
0B53001917347618;;JC305;SmartCard;;;;;ВН-173;20220412145500
```

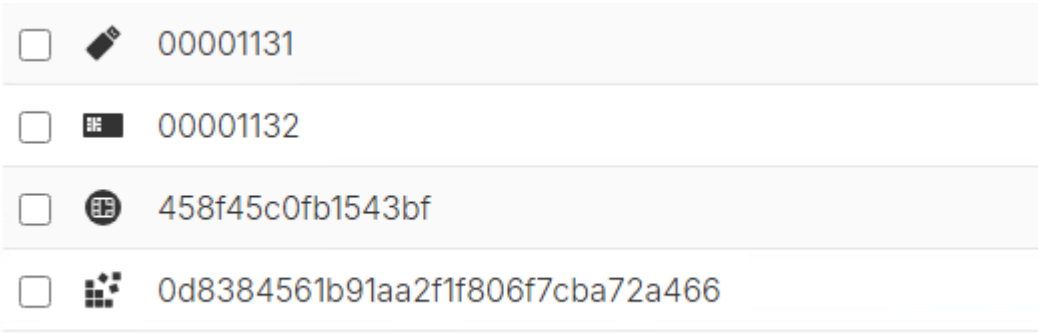
В примере импортируются:

- USB-токены **Rutoken S** (0755398982, 0756309531) — комментарий: Московский офис, теги: VPN, IT.
- USB-токены **Rutoken ECP** (0894130607, 0894130536) — комментарий: Бухгалтерия, тег: VPN, документ СКЗИ: ВН-169 от 12.04.2022 13:42 UTC.
- Смарт-карты **Rutoken ECP SC** (0862287268, 0862287403) — документ СКЗИ: ВН-170 от 29.03.2022 11:15 UTC.
- USB-токен **Rutoken 2151** (0963474291) — документ СКЗИ: ВН-171, дата — время импорта.
- USB-токены **ESMART Token 64K** (609BC06881C7, B0B340508942).
- Смарт-карты **ESMART Token 64K** (E0D8806291CB, D050806291CB).
- Смарт-карта **eToken PRO Java 72K** модели eToken PRO Java 72K OS755 (01cec45d).
- USB-токены **JaCarta** модели JC210 (0B53002004417597, 0B53001122617597).

- Смарт-карта **JaCarta** модели JC300 (0153001910367618).
- USB-токены **JaCarta** модели JC267-1236J.J01Q01 (6082057494937678, 4C54001522634C50) — документ СКЗИ: ВН-172, дата — время импорта.
- Смарт-карта **JaCarta** модели JC305 (0B53001917347618) — документ СКЗИ: ВН-173 от 12.04.2022 14:55 UTC.

Замена иконок устройств

В Консоли управления каждое устройство отображается с иконкой, соответствующей его форм-фактору.



Вы можете заменить стандартные иконки на собственные. Чтобы заменить иконку:

1. Подготовьте изображение в формате PNG размером не более 20x20 px.
2. Сформируйте имя файла в формате `<Название типа устройства>_<Название модели>.png`:
    - `Название типа устройства` — значение из секции `<name>...</name>` в конфигурационном JSON-файле устройства.
    - `Название модели` — значение из секции `<models>...</models>` в конфигурационном JSON-файле устройства. Укажите модель, если в конфигурационном файле описано несколько моделей для одного типа устройства.

Правила формирования имени файла

- Не используйте запрещенные символы (`/`, `\`, `:`, `*`, `?`, `"`, `<`, `>`, `|`).
- Пробелы замените символом подчеркивания `_`.

  Примеры:

- `Rutoken_S.png` — имя файла с иконкой для устройств Rutoken S.
- `eToken_PRO_Java_72K_eToken_PRO_Java_72K_OS755.png` — имя файла с иконкой для устройств типа eToken PRO Java 72K, модели eToken PRO Java 72K OS755.

3. Скопируйте файл в следующие каталоги:

Windows	Linux
C:\inetpub\wwwroot\cm\mc\wwwroot\css\images	*/opt/indeed/cm/mc/wwwroot/css/images*
C:\inetpub\wwwroot\cm\ss\wwwroot\css\images	*/opt/indeed/cm/ss/wwwroot/css/images*
C:\inetpub\wwwroot\cm\rss\wwwroot\css\images	*/opt/indeed/cm/rss/wwwroot/css/images*

4. Откройте Консоль управления, перейдите в раздел **Устройства** и убедитесь, что иконка отображается корректно.

Сертификаты

В разделе **Сертификаты** можно найти все сертификаты, которые содержатся на устройствах, добавленных в Indeed CM.

Предварительные настройки

Чтобы разрешить доступ к разделу **Сертификаты**:

1. Перейдите в раздел **Конфигурация** → **Роли**.
2. Назначьте привилегию *Просмотр репозитория сертификатов* членам роли администратора или оператора.

Поиск сертификатов

Чтобы найти сертификат, установите следующие фильтры:

Объект	Фильтр
Сертификат	• Тип сертификата – управляемый, отслеживаемый, общий • Серийный номер • Отпечаток • Субъект • Издатель • Шаблон – список шаблонов сертификатов интегрированных УЦ и действующая политика • Улучшенный ключ – введите цифровое значение OID. Например, 1.3.6.1.5.5.7.3.4. • Действителен с – диапазон даты начала действия сертификата • Действителен до – диапазон даты окончания действия сертификата
Пользователь	Общее имя пользователя
Устройство	• Тип устройства • Серийный номер

Например, чтобы получить список сертификатов, срок действия которых заканчивается в текущем месяце, в фильтре **Действителен до** выберите диапазон дат.

В результатах поиска дополнительно отображается состояние сертификата – *Действительный, Отозван, Истекает, Ключ истекает, Истек, Ключ истек, Ошибка*.

Подробнее о состояниях сертификата

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 не пригоден для использования. Срок действия сертификата можно продлить на период, равный сроку его действия, заданный в шаблоне сертификата на УЦ. Подробнее об обновлении сертификатов
Ключ истек	Срок действия закрытого ключа сертификата КриптоПро УЦ истек. Срок действия сертификата можно продлить на период, равный сроку его действия, заданный в шаблоне сертификата на УЦ. Подробнее об обновлении сертификатов

Состояние сертификата	Описание
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.
Отклонен	Администратор отклонил запрос на сертификат.
В ожидании	Запрос на сертификат ожидает рассмотрения оператора УЦ или форма сертификата ожидает рассмотрения администратора Indeed CM.

Экспорт результатов поиска

Результаты поиска можно выгрузить в файл XLSX. Нажмите → XLSX.

Действия с сертификатами

Файлы сертификатов можно скачать или отправить по электронной почте .

Для скачивания и отправки по электронной почте доступны формы запроса на сертификат, сертификат и запрос на отзыв сертификата.

Журнал событий

Записи об операциях, совершенных во всех приложениях Indeed CM, фиксируются в разделе **Журнал**.

По умолчанию в инсталляциях под управлением ОС Windows события хранятся в Журнале Событий (Event Viewer) на сервере Indeed CM в каталоге *Indeed CM/Operational*.

Чтобы увидеть список событий, установите фильтры 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

Чтобы выбрать атрибут, по значению которого выполняется поиск пользователя в журнале событий:

1. Запустите Мастер настройки Indeed CM и перейдите в раздел **Журнал событий**.
2. Выберите атрибут:

- Общее имя – значение по умолчанию
- sAMAccountName
- UserPrincipalName
- Пользовательский

Экспорт

Чтобы сформировать отчет 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:

Код	Тип	Событие	Описание
10	Информация	Замена устройства	Устройство успешно заменено. Пользователь: Устройство: Новое Устройство: Сертификаты: Общие сертификаты: Дата истечения: Инициатор:
1010	Ошибка	Замена устройства	Произошла ошибка при замене устройства. Пользователь: Устройство: Новое устройство: Инициатор: Сообщение об ошибке:
11	Информация	Очистка устройства	Устройство успешно очищено. Пользователь: Устройство: Состояние устройства: Инициатор:
1011	Ошибка	Очистка устройства	Произошла ошибка при очистке устройства. Пользователь: Устройство: Инициатор: Сообщение об ошибке:
12	Информация	Сброс PIN-кода	PIN-код устройства успешно сброшен. Пользователь: Устройство: Инициатор:

Код	Тип	Событие	Описание
1012	Ошибка	Сброс PIN-кода	Произошла ошибка при сбросе PIN-кода устройства. Пользователь: Устройство: Инициатор: Сообщение об ошибке:
13	Информация	Разблокировка устройства	Код разблокировки успешно сгенерирован. Пользователь: Устройство: Инициатор:
1013	Ошибка	Разблокировка устройства	Произошла ошибка при генерации кода разблокировки. Пользователь: Устройство: Инициатор: Сообщение об ошибке:
14	Информация	Изменение PIN-кода	PIN-код устройства успешно изменен. Пользователь: Устройство: Инициатор:
1014	Ошибка	Изменение PIN-кода	Произошла ошибка при изменении PIN-кода устройства. Пользователь: Устройство: Инициатор: Сообщение об ошибке:

Код	Тип	Событие	Описание
15	Информация	Выпуск устройства ожидает решения	Выпуск устройства ожидает решения. Пользователь: Политика: Устройство: Сертификаты: Общие сертификаты: Отслеживаемые сертификаты: Инициатор:
16	Информация	Обновление устройства ожидает решения	Выпуск устройства ожидает решения. Пользователь: Устройство: Новые сертификаты: Обновленные сертификаты: Удаленные сертификаты: Новые общие сертификаты: Удаленные общие сертификаты: Отслеживаемые сертификаты: Новая политика: Инициатор:
17	Информация	Замена устройства ожидает решения	Замена устройства ожидает решения. Пользователь: Устройство: Новое устройство: Сертификаты: Общие сертификаты: Дата истечения: Инициатор:

Код	Тип	Событие	Описание
18	Информация	Отмена обновления устройства	Обновление устройства успешно отменено. Пользователь: Устройство: Инициатор:
1018	Ошибка	Отмена обновления устройства	Произошла ошибка при отмене обновления устройства. Пользователь: Устройство: Инициатор: Сообщение об ошибке:
19	Информация	Предварительное обновление устройства	Предварительное обновление устройства успешно выполнено. Пользователь: Устройство: Отозванные сертификаты: Инициатор:
1019	Ошибка	Предварительное обновление устройства	Произошла ошибка при предварительном обновлении устройства. Пользователь: Устройство: Инициатор: Сообщение об ошибке:
20	Информация	Импортирование устройства	Устройство успешно импортировано. Пользователь: Устройство: Состояние: Сертификаты: Инициатор:

Код	Тип	Событие	Описание
1020	Ошибка	Импортирование устройства	Устройство успешно импортировано. Пользователь: Устройство: Состояние: Сертификаты: Инициатор:
21	Информация	Изменение комментария об устройстве	Комментарий устройства успешно изменен. Устройство: Комментарий: Инициатор:
1021	Ошибка	Изменение комментария об устройстве	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:

Код	Тип	Событие	Описание
1023	Ошибка	Смена PIN-кода администратора	Произошла ошибка при изменении PIN-кода устройства. Пользователь: Устройство: Инициатор: Сообщение об ошибке:
24	Информация	Изменение тега	Теги устройства успешно изменены. Устройство: Новые теги: Удаленные теги: Инициатор:
1024	Ошибка	Изменение тега	Произошла ошибка при изменении тегов устройства. Устройство: Новые теги: Удаленные теги: Инициатор: Сообщение об ошибке:
25	Информация	Инициализация устройства	Устройство успешно инициализировано. Устройство: Инициатор:
1025	Ошибка	Инициализация устройства	Произошла ошибка при инициализации устройства. Устройство: Инициатор: Сообщение об ошибке:

Код	Тип	Событие	Описание
26	Информация	Задание PIN-кода администратора	PIN-код администратора устройства успешно задан. Устройство: Инициатор: {initiator}
1026	Ошибка	Задание PIN-кода администратора	Произошла ошибка при задании PIN-кода администратора устройства. Устройство: Инициатор: Сообщение об ошибке:
101	Информация	Изменение ответов на секретные вопросы	Ответы на секретные вопросы успешно изменены. Пользователь: Инициатор:
1101	Ошибка	Изменение ответов на секретные вопросы	Произошла ошибка при изменении ответов на секретные вопросы. Пользователь: Инициатор: Сообщение об ошибке:
102	Информация	Аутентификация	Пользователь успешно аутентифицирован. Пользователь: Инициатор:
1102	Ошибка	Аутентификация	Произошла ошибка при аутентификации пользователя. Пользователь: Инициатор: Сообщение об ошибке:

Код	Тип	Событие	Описание
2103	Предупреждение	Блокировка пользователя	Пользователь заблокирован. Пользователь: Инициатор:
104	Информация	Разблокировка пользователя	Пользователь успешно разблокирован. Пользователь: Инициатор:
1104	Ошибка	Разблокировка пользователя	Произошла ошибка при разблокировке пользователя. Пользователь: Инициатор: Сообщение об ошибке:
105	Информация	Сброс ответов на секретные вопросы	Ответы на секретные вопросы успешно сброшены. Пользователь: Инициатор:
1105	Ошибка	Сброс ответов на секретные вопросы	Произошла ошибка при сбросе ответов на секретные вопросы. Пользователь: Инициатор: Сообщение об ошибке:
106	Информация	Сброс пароля	Пароль пользователя успешно сброшен. Пользователь: Время истечения: Инициатор:
1106	Ошибка	Сброс пароля	Произошла ошибка при сбросе пароля пользователя. Пользователь: Инициатор: Сообщение об ошибке:

Код	Тип	Событие	Описание
107	Информация	Изменение комментария о пользователе	Комментарий о пользователе успешно изменен. Пользователь: Инициатор: Комментарий:
1107	Ошибка	Изменение комментария о пользователе	Произошла ошибка при изменении комментария о пользователе. Пользователь: Инициатор: Комментарий: 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:
114	Информация	Результат проверки в СМЭВ	Данные пользователя не прошли проверку в СМЭВ, но были подтверждены оператором. Пользователь: Инициатор:
121	Информация	Начало обучения СКЗИ	Обучение по работе с СКЗИ начато. Пользователь: Обучающий курс: Инициатор:
1121	Ошибка	Ошибка начала обучения СКЗИ	Произошла ошибка при начале обучения СКЗИ. Пользователь: Обучающий курс: Инициатор: Сообщение об ошибке:
122	Информация	Завершение обучения СКЗИ	Обучение по работе с СКЗИ завершено. Пользователь: Обучающий курс: Инициатор:

Код	Тип	Событие	Описание
1122	Ошибка	Ошибка завершения обучения СКЗИ	Произошла ошибка при завершении обучения СКЗИ. Пользователь: Обучающий курс: Инициатор: Сообщение об ошибке:
123	Информация	Одобрение завершения обучения СКЗИ	Завершение обучения по работе с СКЗИ одобрено. Пользователю предоставлен допуск к работе с СКЗИ. Пользователь: Обучающий курс: Инициатор:
1123	Ошибка	Ошибка одобрения обучения СКЗИ	Произошла ошибка при одобрении обучения СКЗИ. Пользователь: Обучающий курс: Инициатор: Сообщение об ошибке:
124	Информация	Отмена обучения СКЗИ	Обучение по работе с СКЗИ отменено. Пользователь: Обучающий курс: Инициатор:
1124	Ошибка	Ошибка отмены обучения СКЗИ	Произошла ошибка при отмене обучения СКЗИ. Пользователь: Обучающий курс: Инициатор: Сообщение об ошибке:

Код	Тип	Событие	Описание
131	Информация	Создание пользователя	Пользователь успешно создан. Путь: Инициатор:
1131	Ошибка	Ошибка создания пользователя	Произошла ошибка при создании пользователя. Путь: Инициатор: Сообщение об ошибке:
132	Информация	Изменение пользователя	Пользователь успешно изменен. Путь: Изменения: Инициатор:
1132	Ошибка	Ошибка изменения пользователя	Произошла ошибка при изменении пользователя. Путь: Изменения: Инициатор: Сообщение об ошибке:
133	Информация	Удаление пользователя	Пользователь успешно удален. Путь: Инициатор:
1133	Ошибка	Ошибка удаления пользователя	Произошла ошибка при удалении пользователя. Путь: Инициатор: Сообщение об ошибке:
141	Информация	Создание контейнера	Контейнер успешно создан. Путь: Инициатор:

Код	Тип	Событие	Описание
1141	Ошибка	Ошибка создания контейнера	Произошла ошибка при создании контейнера. Путь: Инициатор: Сообщение об ошибке:
142	Информация	Изменение контейнера	Контейнер успешно изменен. Путь: Изменения: Инициатор:
1142	Ошибка	Ошибка изменения контейнера	Произошла ошибка при изменении контейнера. Путь: Изменения: 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:

Код	Тип	Событие	Описание
202	Информация	Удаление политики	Политика успешно удалена. Имя политики: Инициатор:
1202	Ошибка	Удаление политики	Произошла ошибка при удалении политики. Имя политики: Инициатор: Сообщение об ошибке:
203	Информация	Изменение политики	Политика успешно изменена. Имя политики: Инициатор:
1203	Ошибка	Изменение политики	Произошла ошибка при изменении политики. Имя политики: Инициатор: Сообщение об ошибке:
204	Информация	Добавление лицензии	Лицензия успешно добавлена. Тип: Действительна с: Действительна по: Количество: Инициатор:
1204	Ошибка	Добавление лицензии	Произошла ошибка при добавлении лицензии. Инициатор: Сообщение об ошибке:

Код	Тип	Событие	Описание
205	Информация	Удаление лицензии	Лицензия успешно удалена. Тип: Действительна с: Действительна по: Количество: Инициатор:
1205	Ошибка	Удаление лицензии	Произошла ошибка при удалении лицензии. Инициатор: Сообщение об ошибке:
206	Информация	Добавление типа устройства	Тип устройства успешно добавлен. Имя: Инициатор:
1206	Ошибка	Добавление типа устройства	Произошла ошибка при добавлении типа устройства. Имя: Инициатор: Сообщение об ошибке:
207	Информация	Удаление типа устройства	Тип устройства успешно удален. Имя: Инициатор:
1207	Ошибка	Удаление типа устройства	Произошла ошибка при удалении типа устройства. Имя: Инициатор: Сообщение об ошибке:

Код	Тип	Событие	Описание
208	Информация	Изменение типа устройства	Тип устройства успешно изменен. Имя: Инициатор:
1208	Ошибка	Изменение типа устройства	Произошла ошибка при изменении типа устройства. Имя: Инициатор: Сообщение об ошибке:
209	Информация	Добавление узла организационной структуры	Узел организационной структуры успешно добавлен. Путь: Инициатор:
1209	Ошибка	Добавление узла организационной структуры	Произошла ошибка при добавлении узла организационной структуры. Путь: Инициатор: Сообщение об ошибке:
210	Информация	Удаление узла организационной структуры	Узел организационной структуры успешно удален. Путь: Инициатор:
1210	Ошибка	Удаление узла организационной структуры	Произошла ошибка при удалении узла организационной структуры. Путь: Инициатор: Сообщение об ошибке:

Код	Тип	Событие	Описание
211	Информация	Переименование узла организационной структуры	Узел организационной структуры успешно переименован. Старый путь: Новый путь: Инициатор:
1211	Ошибка	Переименование узла организационной структуры	Произошла ошибка при переименовании узла организационной структуры. Старый путь: Новый путь: Инициатор: Сообщение об ошибке:
212	Информация	Перемещение узла организационной структуры	Узел организационной структуры успешно перемещен. Старый путь: Новый путь: Инициатор:
1212	Ошибка	Перемещение узла организационной структуры	Произошла ошибка при перемещении узла организационной структуры. Старый путь: Новый путь: Инициатор: Сообщение об ошибке:
213	Информация	Добавление связанных объектов каталога	Связанные объекты каталога успешно добавлены. Путь: Пользователи: Группы: Контейнеры: Инициатор:

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:
236	Информация	Обновление настроек почтового сервера	Настройки почтового сервера успешно обновлены. Инициатор:
1236	Ошибка	Обновление настроек почтового сервера	Произошла ошибка при изменении настроек почтового сервера. Инициатор: Сообщение об ошибке:
237	Информация	Создание группы получателей	Группа получателей успешно создана. Имя: Инициатор:
1237	Ошибка	Создание группы получателей	Произошла ошибка при создании группы получателей. Имя: Инициатор: Сообщение об ошибке:

Код	Тип	Событие	Описание
238	Информация	Обновление группы получателей	Группа получателей успешно обновлена. Имя: Инициатор:
1238	Ошибка	Обновление группы получателей	Произошла ошибка при обновлении группы получателей. Имя: Инициатор: Сообщение об ошибке:
239	Информация	Удаление группы получателей	Группа получателей успешно удалена. Имя: Инициатор:
1239	Ошибка	Удаление группы получателей	Произошла ошибка при удалении группы получателей. Имя: Инициатор: Сообщение об ошибке:
240	Информация	Создание уведомления администратора	Уведомление администратора успешно создано. Событие: Тип события: Инициатор:
1240	Ошибка	Создание уведомления администратора	Произошла ошибка при создании уведомления администратора. Событие: Тип события: Инициатор: Сообщение об ошибке:

Код	Тип	Событие	Описание
241	Информация	Обновление уведомления администратора	Уведомление администратора успешно обновлено. Событие: Тип события: Инициатор:
1241	Ошибка	Обновление уведомления администратора	Произошла ошибка при обновлении уведомления администратора. Событие: Тип события: Инициатор: Сообщение об ошибке:
242	Информация	Удаление уведомления администратора	Уведомление администратора успешно удалено. Событие: Тип события: Инициатор:
1242	Ошибка	Удаление уведомления администратора	Произошла ошибка при удалении уведомления администратора. Событие: Тип события: Инициатор: Сообщение об ошибке:
243	Информация	Обновление шаблона администратора	Шаблон администратора успешно обновлен. Событие: Тип события: Инициатор:

Код	Тип	Событие	Описание
1243	Ошибка	Обновление шаблона администратора	Произошла ошибка при обновлении шаблона администратора. Событие: Тип события: Инициатор: Сообщение об ошибке:
1801	Ошибка	Отправка уведомления	Произошла ошибка при отправке уведомления. Сообщение об ошибке:
331	Информация	Добавление документа	Документ успешно добавлен. Пользователь: Тип: Имя файла: Описание: Подпись: Оригинал: Инициатор:
1331	Ошибка	Добавление документа	Произошла ошибка при добавлении документа. Пользователь: Тип: Имя файла: Описание: Подпись: Оригинал: Инициатор: Сообщение об ошибке:

Код	Тип	Событие	Описание
332	Информация	Изменение документа	Документ успешно изменен. Пользователь: Тип: Имя файла: Описание: Оригинал: Инициатор:
1332	Ошибка	Изменение документа	Произошла ошибка при изменении документа. Пользователь: Тип: Имя файла: Описание: Оригинал: Инициатор: Сообщение об ошибке:
333	Информация	Удаление документа	Документ успешно удален. Пользователь: Тип: Имя файла: Описание: Инициатор:
1333	Ошибка	Удаление документа	Произошла ошибка при удалении документа. Пользователь: Тип: Имя файла: Описание: Инициатор: Сообщение об ошибке:

Код	Тип	Событие	Описание
334	Информация	Одобрение документа	Документ успешно одобрен. Пользователь: Тип: Имя файла: Описание: Инициатор:
1334	Ошибка	Одобрение документа	Произошла ошибка при одобрении документа. Пользователь: Тип: Имя файла: Описание: Инициатор: 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:
605	Информация	Удаление агента	Агент успешно удален Имя агента: Инициатор:

Код	Тип	Событие	Описание
1605	Ошибка	Удаление агента	Произошла ошибка при удалении агента. Имя агента: Инициатор: Сообщение об ошибке:
606	Информация	Регистрация агента	Агент успешно зарегистрирован. Имя агента: Инициатор:
1606	Ошибка	Регистрация агента	Произошла ошибка при регистрации агента. Имя агента: Инициатор: Сообщение об ошибке:
607	Информация	Отклонение агента	Агент успешно отклонен. Имя агента: Инициатор:
1607	Ошибка	Отклонение агента	Произошла ошибка при отклонении агента. Имя агента: Инициатор: Сообщение об ошибке:
608	Информация	Добавление задачи	Задача успешно добавлена. Устройство: Тип задачи: Комментарий: Инициатор:

Код	Тип	Событие	Описание
1608	Ошибка	Добавление задачи	Произошла ошибка при добавлении задачи. Устройство: Тип задачи: Комментарий: Инициатор: Сообщение об ошибке:
609	Информация	Удаление задачи	Задача успешно удалена. Устройство: Тип задачи: Комментарий: Инициатор:
1609	Ошибка	Удаление задачи	Произошла ошибка при удалении задачи. Устройство: Тип задачи: Комментарий: Инициатор: Сообщение об ошибке:
610	Информация	Обновление имени агента	Имя агента успешно обновлено. Текущее имя агента: Новое имя агента: Инициатор:
1610	Ошибка	Обновление имени агента	Произошла ошибка при обновлении имени агента. Текущее имя агента: Новое имя агента: Инициатор: Сообщение об ошибке:

Код	Тип	Событие	Описание
611	Информация	Обновление комментария агента	Комментарий агента успешно обновлен. Имя агента: Текущий комментарий агента: Новый комментарий агента: Инициатор:
1611	Ошибка	Обновление комментария агента	Произошла ошибка при обновлении комментария агента. Имя агента: Текущий комментарий агента: Новый комментарий агента: Инициатор: Сообщение об ошибке:
612	Информация	Выполнение задачи	Задача была успешно выполнена. Информация о сессии: Идентификатор сессии: Пользователь: Sid: Тип сессии: Имя агента: Устройство: Тип задачи: Комментарий: Создана пользователем: Инициатор:

Код	Тип	Событие	Описание
1612	Ошибка	Выполнение задачи	Не удалось выполнить задачу. Информация о сессии: Идентификатор сессии: Пользователь: Sid: Тип сессии: Имя агента: Устройство: Тип задачи: Комментарий: Создана пользователем: Описание ошибки при выполнении задачи Инициатор: Сообщение об ошибке:
613	Информация	Отмена задачи пользователем	Задача была отменена пользователем. Информация о сессии: Идентификатор сессии: Пользователь: Sid: Тип сессии: Имя агента: Устройство: Тип задачи: Комментарий: Создана пользователем: Инициатор:

Код	Тип	Событие	Описание
1613	Ошибка	Отмена задачи пользователем	Пользователю не удалось отменить задачу. Информация о сессии: Идентификатор сессии: Пользователь: Sid: Тип сессии: Имя агента: Устройство: Тип задачи: Комментарий: Создана пользователем: Инициатор: Сообщение об ошибке:
614	Информация	Обновление задачи	Задача успешно обновлена. Устройство: Тип задачи: Старый комментарий: Новый комментарий: Инициатор:
1614	Ошибка	Обновление задачи	Произошла ошибка при обновлении задачи. Устройство: Тип задачи: Старый комментарий: Новый комментарий: Инициатор: Сообщение об ошибке:

Код	Тип	Событие	Описание
2615	Предупреждение	Подключение незарегистрированного устройства	Подключение незарегистрированного устройства. Информация о сессии: Идентификатор сессии: Пользователь: Sid: Тип сессии: Информация об устройстве: Серийный номер: Метка: Тип: Модель: Atr: Идентификатор агента: Имя агента: Инициатор:
2616	Предупреждение	Отсутствие связи с агентом	Длительное отсутствие связи с агентом. Идентификатор агента: Имя агента: Инициатор:
700	Информация	Инициализация сессий	Инициализация сессий. Количество сессий: Информация о сессиях: Идентификатор агента: Имя агента: Инициатор:

Код	Тип	Событие	Описание
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:
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:

Код	Тип	Событие	Описание
311	Информация	Добавление типа СКЗИ	Тип СКЗИ успешно добавлен. Наименование: Семейство: Сертификат соответствия: Номер: Дата выпуска: Срок действия: Сертификат поддержки: Номер: Дата выпуска: Срок действия: Инициатор:
1311	Ошибка	Добавление типа СКЗИ	Произошла ошибка при добавлении типа СКЗИ. Наименование: Семейство: Сертификат соответствия: Номер: Дата выпуска: Срок действия: Сертификат поддержки: Номер: Дата выпуска: Срок действия: Инициатор: Сообщение об ошибке:
312	Информация	Удаление типа СКЗИ	Тип СКЗИ успешно удален. Наименование: Инициатор:

Код	Тип	Событие	Описание
1312	Ошибка	Удаление типа СКЗИ	Произошла ошибка при удалении типа СКЗИ. Наименование: Инициатор: Сообщение об ошибке:
313	Информация	Изменение типа СКЗИ	Тип СКЗИ успешно изменен. Наименование: Новое наименование: Сертификат соответствия: Номер: Дата выпуска: Срок действия: Сертификат поддержки: Номер: Дата выпуска: Срок действия: Архивный: Инициатор:
1313	Ошибка	Изменение типа СКЗИ	Произошла ошибка при изменении типа СКЗИ. Наименование: Новое наименование: Сертификат соответствия: Номер: Дата выпуска: Срок действия: Сертификат поддержки: Номер: Дата выпуска: Срок действия: Архивный: Инициатор: Сообщение об ошибке:

Код	Тип	Событие	Описание
248	Информация	Создание обучающего курса	Обучающий курс успешно создан. Имя: Инициатор:
1248	Ошибка	Создание обучающего курса	Произошла ошибка при создании обучающего курса. Имя: Инициатор: Сообщение об ошибке:
249	Информация	Изменение обучающего курса	Обучающий курс успешно изменен. Имя: Инициатор:
1249	Ошибка	Изменение обучающего курса	Произошла ошибка при изменении обучающего курса. Имя: Инициатор: Сообщение об ошибке:
250	Информация	Удаление обучающего курса	Обучающий курс успешно удален. Имя: Инициатор:
1250	Ошибка	Удаление обучающего курса	Произошла ошибка при удалении обучающего курса. Имя: 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:
1505	Ошибка	Обновление устройства КриптоПро DSS	Произошла ошибка при обновлении устройства КриптоПро DSS. Пользователь: Инициатор: Сообщение об ошибке:

Код	Тип	Событие	Описание
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:
509	Информация	Отмена обновления устройства КриптоПро DSS	Обновление устройства КриптоПро DSS успешно отменено. Пользователь: Инициатор:

Код	Тип	Событие	Описание
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:

Агенты

В разделе **Агенты** можно найти все агенты, зарегистрированные в Indeed CM.

Предварительные настройки

Чтобы разрешить доступ к репозиторию агентов:

1. Откройте Мастер настройки, перейдите в раздел Клиентский агент и включите опцию **Разрешить использование клиентских агентов**.
2. Откройте Консоль управления, перейдите в раздел **Конфигурация** → **Роли** и назначьте привилегию *Просмотр репозитория агентов* членам роли администратора или оператора.

> **ПРИМЕЧАНИЕ**
>
> Если в Мастере настройки отключена **Автоматическая регистрация агентов**, то после установки и настройки агента на рабочей станции он появится в разделе со статусом *Ожидает регистрации*.

Поиск

Для поиска агента укажите один или несколько параметров.

Имя	По умолчанию в качестве имени агента задается имя компьютера, на котором установлен агент. Имя можно изменить в профиле агента.

Статус	Текущее состояние агента. Значения: • *Не задано* – статус агента не выбран. • *Ожидает регистрации* – агент установлен на рабочей станции и отправил запрос на подключение к серверу Indeed CM. Агент неактивен и не выполняет задачи от сервера. • *Зарегистрирован* – администратор принял запрос на регистрацию агента. Агент готов к выполнению задач. • *Отклонен* – администратор отклонил запрос на регистрацию агента. Агент неактивен и не выполняет задачи от сервера. • *Отозван* – сертификат агента приостановлен или отозван в УЦ. Агент неактивен и не выполняет задачи от сервера.
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 в профиле агента
Версия клиента	Версия клиентского компонента Indeed CM Agent, установленного на рабочей станции. В выпадающем списке выберите: • *Не задано*, чтобы найти агенты всех версий • Номер версии, например, 7.3.0 • *Неизвестная*, чтобы найти агенты устаревших версий или неактивные агенты, у которых нет связи с сервером

Поддерживаются следующие шаблоны поиска:

- Полное совпадение – `Win7x86.domain.loc`
- Частичное совпадение – `*86.domain.loc` или `*domain*`
- Все результаты – `*`

Чтобы перейти в профиль агента, нажмите на имя агента в результатах поиска.

Чтобы подтвердить запрос на регистрацию агента, нажмите **Зарегистрировать**. Чтобы отклонить запрос на регистрацию агента, нажмите **Отклонить**.

Профиль агента

В профиле содержится информация об агенте, сессиях пользователей, привязанных устройствах и последних событиях, связанных с агентом.

Параметр	Описание
Имя агента	Обязательный параметр. По умолчанию в качестве имени агента используется DNS-имя компьютера, на котором установлен агент. Чтобы редактировать имя агента, нажмите **Изменить имя**.
Комментарий	Необязательный параметр. По умолчанию отсутствует. Чтобы установить или редактировать комментарий, нажмите **Изменить комментарий**.
Сессии	Сессии пользователей, которые выполнили вход на рабочую станцию (необязательно по смарт-карте) или сессии сервисных служб (отображаются, когда рабочая станция включена). Есть два типа сессий пользователя: 1. консольная – пользователь выполнил вход на рабочую станцию напрямую. 2. 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.

Назначение устройства

Агент 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 нужно.

Закрепление устройства за рабочей станцией (агентом) позволяет контролировать использование устройств в организации. Например, агент может реагировать, если пользователь подключил к рабочей станции устройство, которое не закреплено за агентом.
Подробнее о контроле использования устройств

Чтобы закрепить устройство за агентом:

1. В профиле агента перейдите в раздел **Привязанные устройства** и нажмите **Привязать устройство**.
2. 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 профиле агента в разделе **Привязанные устройства**. Чтобы отменить привязку устройства, нажмите ✖ и **Отвязать**.

Контроль использования устройств

Параметры использования привязанных устройств настраиваются в политике в разделе Контроль.

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.

> ⓘ **ПРИМЕЧАНИЕ**
> 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 вы выбрали 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**.

Введите сообщение, которое отображается пользователю при нарушении привязки, и действие, которое должен выполнить агент.

В сообщениях можно 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 системном Журнале 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 регистрирует это событие в системном журнале. Период отсутствия связи агента с сервером указывается в Мастере настройки в разделе **Служба Card Monitor**.

Администратор может получать почтовые уведомления о следующих событиях:

- 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*.

Уведомления администратора настраиваются глобально или локально для политики.

Список производителей устройств с поддержкой регистрации событий

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 заносятся в журналы сервера и клиента. События агентов фиксируют сервис регистрации агентов, сервис агентов и монитор устройств.

Для просмотра событий агентов в разделе **Журнал** Консоли управления отфильтруйте содержимое журнала по одному из сервисов или по событиям.

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 отправятся на сервер, когда связь восстановится.

Назначение задач в карточке устройства

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.

Задачи выполняются следующим образом:

1. Когда устройство подключается к рабочей станции, агент запрашивает у сервера Indeed CM назначенные 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.

> **ПРИМЕЧАНИЕ**
>
> 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 выполнит задачи, требующие действия от пользователя, в сессии любого пользователя.

Назначение задач

1. Найдите нужное устройство в разделе **Устройства** или в карточке пользователя.
2. В карточке устройства выберите задачу.

Задача добавляется в раздел **Назначенные задачи** и отображается до тех пор, пока не выполнится или не отменится.

Если задача ожидает выполнения или выполняется слишком долго, ее можно отменить. Нажмите ✖ и подтвердите действие.

Статусы задачи

Ожидает выполнения – задача ожидает выполнения (когда включится рабочая станция с агентом, когда к рабочей станции подключится устройство или когда завершится предыдущая задача).

Выполняется – агент приступил к выполнению задачи.

Выполняется – задача выполняется слишком долго (более 10 минут).

Выполнена – задача успешно выполнена.

Ошибка – при выполнении задачи возникла ошибка.

Сброс PIN-кода пользователя

Вы можете сбросить забытый или заблокированный PIN-код пользователя. Чтобы сбросить PIN-код, пользователь должен ввести ответы на секретные вопросы. Убедитесь, что вопросы и ответы на них установлены в Сервисе самообслуживания.

Чтобы разблокировать устройство с помощью агента:

1. В карточке устройства нажмите **Сбросить PIN-код**.
2. Включите опцию **Сбросить PIN-код пользователя на агенте**.
3. (Опционально) В поле **Комментарий** введите текст, который отобразится в Журнале событий Indeed CM.
4. Нажмите **Сбросить**.

При выполнении задачи агент запустит на рабочей станции пользователя утилиту разблокировки. PIN-код 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, что пользователь отменил задачу. Повторный запрос ответов на секретные вопросы появится в сессии пользователя через 60 секунд.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Чтобы разблокировать устройства с несколькими логическими областями (например, JaCarta PKI/ГОСТ), создайте две задачи для поочередного сброса PIN-кода каждой области.

Разблокировка биометрии

Биометрическая аутентификация на устройстве Рутокен БИО блокируется, если пользователь не прошел проверку отпечатка пальца пять раз подряд. Вы можете разблокировать биометрию, чтобы сбросить счетчик попыток аутентификации. Если устройство недоступно, разблокируйте биометрию с помощью агента, установленного на рабочей станции пользователя.

> **ПРИМЕЧАНИЕ**
>
> Действие **Разблокировать биометрию** доступно в карточке устройства членам роли с привилегией **Разблокировка биометрии**. Чтобы настроить привилегии, перейдите в раздел **Конфигурация** → **Роли**.

Чтобы разблокировать биометрию на агенте:

1. В карточке устройства нажмите **Разблокировать биометрию**.
2. Включите опцию **Разблокировать биометрию на агенте**.
3. (Опционально) В поле **Комментарий** введите текст, который отобразится в Журнале событий Indeed CM.
4. Нажмите **Разблокировать**.

Биометрия разблокируется автоматически, как только пользователь подключит устройство к рабочей станции с агентом.

Сообщение пользователю

Вы можете настроить сообщение, которое увидит пользователь, когда подключит устройство к рабочей станции с агентом после разблокировки биометрии. Чтобы настроить сообщение:

1. В разделе **Конфигурация** перейдите в настройки политики.
2. Перейдите в раздел **Агенты** → **Сообщения пользователю**.
3. Введите текст сообщения в поле **Разблокировка биометрической аутентификации на устройстве**.
4. Нажмите **Сохранить**.

Смена PIN-кода администратора

1. В карточке устройства нажмите **Сменить PIN-код администратора**.
2. В поле **Новый PIN-код администратора** введите и подтвердите новый PIN-код.
3. (Опционально) В поле **Комментарий** введите текст, который отобразится в Журнале событий Indeed CM.
4. Нажмите **Сменить**.

PIN-код администратора изменится автоматически при подключении устройства к рабочей станции с установленным агентом. 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.

Отзыв с очисткой и инициализацией устройства

1. В карточке устройства нажмите **Отозвать**.
2. Выберите причину отзыва:
   - **Устройство неисправно** — техническая неисправность или физическое повреждение.
   - **Устройство утеряно** — устройство утеряно или украдено. Все сертификаты на устройстве отзываются.
   - **Обновление устройства** — замена устройства на новое.
   - **Изъятие устройства** — удаление устройства из Indeed CM, например, при увольнении сотрудника.
   - **Компрометация устройства** — подозрение на компрометацию ключа. Все сертификаты на устройстве отзываются.
3. Включите опцию **Очистить устройство на агенте** и выберите действие, которое произойдет при отзыве устройства:
   - **Очистить** — с устройства удаляется только управляемое содержимое: данные, записанные через Indeed CM (сертификаты и ключи, аутентификаторы Indeed AM,

идентификаторы SNS, сложный пароль Рутокен Логон). Данные, записанные на устройство вне Indeed CM, сохраняются.

- **Инициализировать** — с устройства удаляются все данные.

4. В поле **Новый PIN-код пользователя** укажите PIN-код, который установится на устройстве после отзыва.

   Если оставить поле пустым, установится PIN-код из настроек типа устройства (**Конфигурация** → **Типы устройств**). Обязательно укажите PIN-код, если значение из настроек типа устройства не соответствует требованиям инициализации в политике (**Выпуск** → **Инициализация**).

5. (Опционально) В поле **Комментарий** введите текст, который отобразится в Журнале событий Indeed CM.

6. Чтобы отвязать устройство от пользователя, нажмите **Дополнительно** и включите опцию **Отменить назначение устройства на пользователя**. Если опция выключена, то после очистки или инициализации устройство останется закрепленным за пользователем, и его можно использовать повторно.

7. Нажмите **Отозвать**.

> **ОСОБЕННОСТИ ОТЗЫВА УСТРОЙСТВ РУТОКЕН БИО С ОЧИСТКОЙ НА АГЕНТЕ**
>
> Для устройства Рутокен ЭЦП 3.0 3250 БИО (Рутокен БИО), содержащего сертификат, защищенный биометрией, при отзыве с очисткой на агенте доступна только инициализация. При инициализации с устройства удаляются все данные, включая биометрию пользователя.
>
> Подробнее о работе с устройствами Рутокен БИО

Обновление содержимого устройства

Чтобы создать задачу обновления устройства:

1. В карточке устройства нажмите **Обновить**.
2. Включите опцию **Обновить устройство на агенте**.
3. (Опционально) В поле **Комментарий** введите текст, который отобразится в Журнале событий Indeed CM.

4. Нажмите **Обновить**.

Настройка отслеживания сторонних сертификатов при обновлении устройства

Если устройство содержит сторонние сертификаты, Indeed CM может их обнаружить и внести информацию о таких сертификатах в систему – отследить. В процессе обновления устройства пользователь может выбрать, какие сертификаты нужно отследить.

Чтобы настроить отслеживание сторонних сертификатов:

1. Перейдите в настройки политики использования устройств в раздел **Поведение** → **Общие разрешения**.
2. Включите опции **Искать сертификаты при выпуске/обновлении устройства для отслеживания срока действия** и **Разрешить пользователю выбирать отслеживаемые сертификаты**.

Когда пользователь подключит устройство к рабочей станции, начнется процесс обновления.

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*. Устройство переходит в состояние *В ожидании*.

Подробнее о проверке документов при обновлении устройств

Отмена обновления

Вы можете отменить обновление устройства на агенте, если в настройках политики использования устройств в разделе **Поведение** → **Разрешения администратора** включена опция **Отменять обновление устройства**.

Чтобы отменить обновление устройства:

1. В карточке устройства нажмите **Отменить обновление**.
2. Введите **PIN-код пользователя**.
3. Включите опцию **Отменить обновление на агенте**.
4. Нажмите **Отменить обновление**.

ОСОБЕННОСТИ ОТМЕНЫ ОБНОВЛЕНИЯ УСТРОЙСТВ РУТОКЕН БИО

Отмена обновления на агенте недоступна для устройства Рутокен ЭЦП 3.0 3250 БИО (Рутокен БИО), которое содержит сертификат, защищенный биометрией.

Подробнее о работе с устройствами Рутокен БИО

Блокировка устройства

При блокировке устройства блокируется PIN-код пользователя. Чтобы заблокировать PIN-код пользователя:

1. В карточке устройства нажмите **Заблокировать**.
2. (Опционально) В поле **Комментарий** введите текст, который отобразится в Журнале событий Indeed CM.
3. Нажмите **Заблокировать**.

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.

Инициализация устройства на агенте

Агент может инициализировать добавленное устройство, которое находится в состоянии *Пустое*. Чтобы инициализировать устройство:

1. В карточке устройства нажмите **Инициализировать**.
2. Включите опцию **Инициализировать устройство на агенте**:
   - Если PIN-код администратора на устройстве совпадает с сохраненным в хранилище системы, нажмите **Инициализировать**. PIN-код администратора на устройстве и в базе не изменится, PIN-код пользователя сбросится на значение, указанное в файле типа устройства.

- Если PIN-код администратора на устройстве не совпадает с сохраненным в хранилище системы, укажите его в разделе **Дополнительно**. При необходимости установите **Новый PIN-код пользователя** и нажмите **Инициализировать**. PIN-код администратора в хранилище системы изменится на указанное значение.

> **ПРИМЕЧАНИЕ**
>
> Устройства Рутокен и eToken можно инициализировать с PIN-кодом администратора в состоянии: известный, неизвестный, заблокированный.
>
> - Если PIN-код администратора не указан, то после инициализации на устройстве установится PIN-код, сохраненный в хранилище системы.
> - Если PIN-код администратора указан, то после инициализации он установится на устройстве и в хранилище системы.

Массовые задачи

Массовые задачи – задачи, которые можно назначить на несколько устройств одновременно. Массовые задачи назначаются на выбранные устройства и выполняются, когда пользователь подключает устройство к рабочей станции, на которой установлен агент.

Список задач

- **Блокировка устройства**
  PIN-код пользователя заблокируется. Задачу можно назначить на устройства в состоянии *Выпущено* или *В ожидании*.
- **Смена PIN-кода**
  Пользователь получит уведомление о необходимости сменить PIN-код. Задачу можно назначить на устройства в состоянии *Выпущено* или *В ожидании*.
- **Смена PIN-кода администратора**
  PIN-код администратора автоматически изменится. Задачу можно назначить на устройства в любом состоянии.
- **Обновление устройства**
  Содержимое устройства обновится. Задачу можно назначить на устройства в состоянии *Выпущено*.
- **Очистка устройства**
  Устройство очистится или инициализируется. Дополнительно можно отменить

назначение (изъять) устройство у пользователя. Задачу можно назначить на устройства в состоянии *Отозвано*.

Создание задач

Чтобы создать массовую задачу:

1. Перейдите в раздел **Устройства** Консоли управления.
2. Найдите нужные устройства и нажмите **Создать задачи**.
3. Выберите задачу, укажите параметры и нажмите **Создать**.

Задачи появятся в карточках выбранных устройств. В разделе **Журнал** фиксируются события о результатах выполнения задач на каждом агенте.

Рассылка сообщений пользователю

Агент 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 отображаются у пользователя. Чтобы их включить, введите текст сообщений.

Автоматические задачи

Клиентский агент Indeed CM может автоматически выполнить следующие операции:

- Добавить и назначить устройство
- Выпустить пустое или назначенное устройство
- Продолжить выпуск и обновление устройства в состоянии *В ожидании*
- Запросить смену PIN-кода пользователя по истечении заданного времени

Настройки, которые определяют доступные операции для агентов, задаются в разделе **Конфигурация** в политике использования устройств в разделе **Агенты** → **Поведение**. Операции выполняются удаленно на рабочих станциях пользователей, где установлены агенты.

Пустые и назначенные устройства выпускаются согласно настройкам, заданным в политике использования устройств в разделе **Выпуск**. Применяются настройки политики, действующей на пользователя, в сессии которого подключается устройство.

Добавление устройства

Если к рабочей станции подключается устройство, не зарегистрированное в Indeed CM, агент может добавить его автоматически. Устройство привязывается к агенту рабочей станции, на которой оно добавлено.

Чтобы настроить автоматическое добавление устройств, включите опции **Добавлять устройство** и **Добавлять устройство без PIN-кода администратора, если предоставленный PIN-код недействителен**.

При добавлении устройства агент проходит аутентификацию, чтобы получить доступ к устройству. Агент автоматически подставляет значение PIN-кода администратора, которое указано в политике для данного типа устройства в разделе **Агенты** → **Поведение** → **PIN-коды администратора**.

> **ПРИМЕЧАНИЕ**
>
> Если PIN-код администратора не задан в политике, агент подставляет значение, указанное при редактировании типа устройства в разделе **Конфигурация** → **Типы устройств**.

Агент может добавить устройство и поменять PIN-код администратора или добавить устройство без PIN-кода администратора.

Добавить устройство и поменять PIN-код

Если PIN-код верный, агент добавляет устройство и устанавливает новый PIN-код. PIN-код меняется на случайный или на указанный в опции **Устанавливать неслучайный PIN-код администратора** в разделе **Конфигурация** → **Типы устройств**.

Если PIN-код неверный, он может заблокироваться. Чтобы не допустить блокировку PIN-кода, убедитесь, что включена опция **Добавлять устройство без PIN-кода администратора, если предоставленный PIN-код недействителен**. В этом случае агент добавляет устройство в Indeed CM без PIN-кода.

Подробнее о блокировке PIN-кода администратора

У каждого устройства есть счетчик неудачных попыток ввода PIN-кода администратора. Например, на устройствах Рутокен по умолчанию установлено 10 попыток ввода PIN-кода администратора. Если на устройстве, которое добавляется в Indeed CM, осталась одна попытка, и введен неверный PIN-код, то PIN-код блокируется.

На некоторых устройствах разблокировать PIN-код администратора невозможно. В случае блокировки PIN-кода администратора необходимо инициализировать устройство, но при этом все данные, которые хранятся на устройстве, удаляются.

Добавить устройство без PIN-кода

Если PIN-код неверный, устройство можно добавить в Indeed CM без PIN-кода. Чтобы добавить устройство без PIN-кода, убедитесь, что включена опция **Добавлять устройство без PIN-кода администратора, если предоставленный PIN-код недействителен**.

Если устройство добавилось в Indeed CM без PIN-кода, вы можете установить PIN-код с помощью следующих настроек:

- Вручную в карточке устройства, если в разделе **Конфигурация** → **Роли** администратору назначена привилегия **Задание PIN-кода администратора**
- Автоматически при выпуске устройства с инициализацией
- Назначить агенту, установленному на рабочей станции пользователя, задачу **Сменить PIN-код администратора**

Если PIN-код верный, агент добавляет устройство и устанавливает новый PIN-код. PIN-код меняется на случайный или на указанный в опции **Устанавливать неслучайный PIN-код администратора** в разделе **Конфигурация** → **Типы устройств**.

Назначение устройства на пользователя

Агент может автоматически назначить устройство на пользователя при добавлении. Устройство назначается на пользователя, в активной сессии которого оно добавляется.

Чтобы настроить автоматическое назначение устройств при добавлении, включите опции **Добавлять устройство** и **Назначать устройство**.

Назначенные устройства можно выпустить автоматически с помощью опции **Выпускать назначенное устройство**.

Выпуск пустого устройства

Агент может автоматически выпустить устройства в состоянии *Пустое* – не назначенное на пользователя.

Сценарий использования

Вам необходимо массово выпустить большое количество новых устройств, которые вы выдали пользователям. Устройства еще не назначены на пользователей и находятся в состоянии *Пустое*. Чтобы пользователям не пришлось выпускать устройства самостоятельно в Сервисе самообслуживания, вы можете настроить автоматический выпуск с помощью агентов, установленных на рабочих станциях пользователей.

Настройка

Чтобы настроить автоматический выпуск пустых устройств, включите опцию **Выпускать пустое устройство**.

После того как все устройства выпустятся, отключите опцию **Выпускать пустое устройство**. Это необходимо, чтобы устройство не выпускалось повторно в процессе своего жизненного цикла, например, после изъятия.

> **ПОДСКАЗКА**
>
> Рекомендуем выпускать только назначенные устройства.

Выпуск назначенного устройства

Агент может автоматически выпускать устройства в состоянии *Назначено*.

Чтобы настроить автоматический выпуск назначенных устройств, включите опцию **Выпускать назначенное устройство**.

При выпуске назначенного устройства агент проверяет привязку сессии пользователя к устройству. Если к рабочей станции одного пользователя подключить устройство, назначенное на другого пользователя, то агент не выпускает устройство.

Продолжение выпуска и обновления устройства

Агент может автоматически продолжить выпуск и обновление устройств, которые находятся в состоянии *В ожидании*. Чтобы настроить автоматическое продолжение выпуска или обновления устройства, включите следующие опции:

- **Продолжать выпуск устройства**
- **Продолжать обновление устройства**

Устройство переходит в состояние *В ожидании*, если выпуск или обновление устройства приостановлено для проверки документов. Агент продолжает выпуск или обновление, если администратор одобрил документы пользователя.

Подробнее о контроле выпуска и обновления устройств

Смена PIN-кода пользователя

Вы можете настроить срок действия PIN-кода пользователя на устройстве. Задача создается только для устройств в состоянии *Выпущено*.

Чтобы настроить срок действия PIN-кода пользователя:

1. Включите опцию **Запрашивать смену PIN-кода пользователя по истечении (дней)**.
2. Укажите, сколько дней действует PIN-код пользователя.

По истечении этого времени служба Card Monitor создает задачу **Смена PIN-кода пользователя** на агенте, к которому привязано устройство. Когда пользователь подключает устройство к рабочей станции, агент открывает окно смены PIN-кода.

Смена PIN-кода пользователя при первом входе

> **ПРИМЕЧАНИЕ**
>
> Устройства Рутокен ЭЦП 3.0, IDPrime и eToken поддерживают аппаратное требование смены PIN-кода пользователя при первом подключении устройства к рабочей станции.

Чтобы настроить требование о смене PIN-кода для устройств Рутокен ЭЦП 3.0, IDPrime и eToken, включите опцию **Пользователь должен поменять PIN-код при первом входе** в политике использования устройств в разделе Выпуск.

> **ПОДСКАЗКА**
>
> Требование о смене PIN-кода можно настроить вне Indeed CM. Например, в PKI-клиенте.

Когда пользователь подключает устройство к рабочей станции в первый раз, агент открывает окно смены PIN-кода.

Журнал учета СКЗИ

Журнал учета СКЗИ содержит данные об СКЗИ, пользователях и системах, в которых они используются.

Предварительные настройки

Чтобы разрешить доступ к журналу учета СКЗИ:

1. Откройте Мастер настройки, перейдите в раздел **Журнал учета СКЗИ** и включите опцию **Вести журнал учета СКЗИ**.
2. Откройте Консоль управления, перейдите в раздел **Конфигурация** → **Роли** и назначьте привилегию *Просмотр репозитория СКЗИ* членам роли администратора или оператора.
3. Задайте настройки использования СКЗИ в разделе **Конфигурация** → СКЗИ.

Поиск

Для поиска СКЗИ установите параметры выборки:

- **Тип объекта** – дистрибутив, лицензия, документация, ключевой документ, ключевой носитель, пользовательский
- **Тип СКЗИ**
- **Пользователь**
- **Серийный номер**
- **Номер экземпляра**
- **Состояние** – не задано, изготовлено, назначено, передано, возвращено, выдано, установлено, уничтожено/изъято
- **Дата** – за все время или за период

Экспорт результатов поиска

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 (если в условиях поиска выбран конкретный пользователь)
- Пользовательская форма

Добавление

СКЗИ можно создать вручную или автоматически.

Автоматически

СКЗИ создается 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)

Вручную

Чтобы создать СКЗИ вручную, нажмите **Добавить СКЗИ** и задайте значения параметров СКЗИ:

- **Тип объекта** – дистрибутив, лицензия, документация, ключевой документ, ключевой носитель, пользовательский
- **Тип СКЗИ**
- **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

Чтобы закрепить созданное СКЗИ за пользователем:

1. Выберите СКЗИ (одно или несколько) и нажмите **Назначить СКЗИ**.

2. Выполните поиск пользователя 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. Укажите **Номер и дату документа**, на основании которого выполняется уничтожение/изъятие.
4. Выберите опцию **Использовать повторно**, если СКЗИ будет использоваться повторно, например, для передачи другому сотруднику.

5. Нажмите **Уничтожить/Изъять**.

Пакетный импорт

Вы можете зарегистрировать в Indeed CM несколько СКЗИ с помощью файла пакетного импорта.

Создание файла

Поддерживается файл в формате TXT (UTF-8) или CSV.

В файл пакетного импорта для каждого СКЗИ добавьте строку с необходимым набором полей. Поля указываются через точку с запятой в следующем порядке:

```
SerialNumber;InstanceNumber;ObjectType;SkziType;DocNumber;TimeCreated
```

Поле	Описание
`SerialNumber`	Серийный номер СКЗИ
`InstanceNumber`	(Необязательное поле) Номер экземпляра
`ObjectType`	Тип объекта СКЗИ: Distributive, License, Documentation, KeyDocument, Card, Custom.
`SkziType`	Тип СКЗИ из справочника типов СКЗИ
`DocNumber`	Номер документа, на основании которого создается СКЗИ
`TimeCreated`	(Необязательное поле) Время создания СКЗИ. Указывается в формате yyyyMMddHHmmss (UTC). Если значение не указано, то в качестве времени создания СКЗИ автоматически подставляется время импорта

ПРИМЕЧАНИЕ

Если в строке в поле `Serial Number` прописано значение default, то значения всех полей этой строки используются как значения по умолчанию для соответствующих полей последующих строк. В последующих строках укажите только серийный номер СКЗИ, номер экземпляра и значение поля, которое отличается от указанного в строке default.

Если поле пустое, вместо него укажите `;`.

Пример содержимого файла импорта

```
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

Импорт в Indeed CM

1. Перейдите в раздел **СКЗИ** Консоли управления.
2. Нажмите **Импортировать СКЗИ**.
3. Загрузите подготовленный файл СКЗИ.

4. Нажмите **Импортировать**.

Журнал учета устройств и сертификатов

Журналы учета содержат данные об устройствах и сертификатах, их владельцах и системах, в которых используются эти устройства и сертификаты.

Записи в журналы учета заносятся автоматически при выпуске, замене и изъятии устройств в Консоли управления, в Сервисе самообслуживания и при работе клиентского агента. В журналы учета сертификатов дополнительно заносятся записи при обновлении устройств.

Предварительные настройки

Чтобы разрешить доступ к журналам учета:

1. Откройте Мастер настройки, перейдите в раздел **Общие функции** и включите опцию **Журнал учета устройств и сертификатов**.
2. Откройте Консоль управления, перейдите в раздел **Конфигурация** → **Роли** и назначьте привилегию *Просмотр журнала учета* членам роли администратора или оператора.
3. Настройте поля журналов учета в разделе **Конфигурация** → Шаблоны журналов.

Добавление и просмотр записей

Записи в журналы учета заносятся автоматически при выпуске, замене и изъятии устройств в Консоли управления, в Сервисе самообслуживания и при работе клиентского агента. В журналы учета сертификатов дополнительно заносятся записи при обновлении устройств.

Администратор или оператор могут выбрать созданный журнал и запросить необходимую информацию с помощью фильтров, настроенных для конкретного журнала.

Чтобы добавить запись вручную, нажмите **Добавить запись**, заполните **Обязательные поля** и нажмите **Добавить**.

Экспорт

Чтобы выгрузить журнал учета в файл, нажмите  и выберите формат XLSX или CSV.

Документы

В разделе **Документы** можно найти все документы, загруженные в Indeed CM.

> **ПРИМЕЧАНИЕ**
>
> Функция внутреннего электронного документооборота Indeed CM ЭДО позволяет пользователям и администраторам обмениваться документами для получения сертификата ключа проверки электронной подписи и нормативными документами СКЗИ.
>
> Администраторы могут управлять документами в Консоли управления, а пользователи – в Сервисе самообслуживания.

Предварительные настройки

Чтобы разрешить доступ к разделу **Документы**:

1. В Мастере настройки перейдите в раздел **Общие функции** и включите опцию **Внутренний документооборот**.
2. В Консоли управления перейдите в раздел **Конфигурация** → **Роли** и назначьте привилегию *Просмотр репозитория документов* членам роли администратора или оператора.

Поиск документов

Чтобы найти документы, установите фильтры:

- **Тип**
- **Имя файла**
- **Описание**
- **Пользователь**
- **Подпись** – присутствует или отсутствует
- **Оригинал документа** – предоставлен или отсутствует
- **Дата** – за период или за все время

Например, если установить фильтры **Тип** → **Сертификат** и **Оригинал документа** → **Отсутствует**, можно найти всех пользователей, которые не загрузили оригиналы сертификатов в Indeed CM.

Экспорт результатов поиска

Результаты поиска можно выгрузить в файл XLSX. Нажмите  и выберите формат XLSX.

Действия с документами

Документы можно скачать  , редактировать  или удалить  .

Если пользователь предоставил оригинал документа, вы можете зафиксировать получение оригинала в Indeed CM. Нажмите  напротив нужного документа и включите опцию **Оригинал получен**.

Руководство пользователя

Пользователи Indeed CM управляют своими устройствами, сертификатами и документами в веб-приложениях:

- Сервис самообслуживания (Self-Service) — для операций с устройством, подключенным к рабочей станции.
- Сервис удаленного самообслуживания (Remote Self-Service) — для операций без подключения устройства.

Список разрешенных действий определяет администратор в Консоли управления в разделе **Конфигурация** → **Политики** → Поведение.

Сервис самообслуживания

Веб-приложение Self-Service

Сервис удаленного самообслуживания

Веб-приложение Remote Self-Service для операций без подключения устройства

Действия с устройствами

Доступные действия со смарт-картами и USB-токенами

Изменение ответов на секретные вопросы

Восстановление доступа

СКЗИ

Управление СКЗИ

Документы

Управление документами сертификата и нормативными документами СКЗИ

Клиентский агент

Задачи клиентского агента Indeed CM Agent

Просмотр файлов и ресурсов

Доступ к файлам и ресурсам

Выгрузка сертификата КриптоПро DSS

Установка сертификата из облачного хранилища КриптоПро DSS на рабочую станцию

Сервис самообслуживания

Сервис самообслуживания (Self-Service) — веб-приложение Indeed CM, в котором пользователи управляют своими устройствами, сертификатами, документами И скзи.

Сервис самообслуживания доступен по ссылке: `https://<FQDN сервера Indeed CM>/cm/ss`.

> **ПРИМЕЧАНИЕ**
>
> Настройки входа в Сервис самообслуживания определяет администратор в разделе **Конфигурация** → **Политики** → Аутентификация.

Профиль пользователя

В Сервисе самообслуживания доступна следующая информация:

- **О себе** — имя, логин, электронная почта, телефон и фото. Данные добавляются в Indeed CM автоматически из каталога пользователей.
- **Ваши устройства** — список устройств, закрепленных за пользователем, и их содержимое.
- **Ваши СКЗИ** — список назначенных СКЗИ.
- **Ваши документы** — список документов.

Действия

Список разрешенных действий определяет администратор в Консоли управления в разделе **Конфигурация** → **Политики** → Поведение.

Основные действия в Сервисе самообслуживания:

- Работа с устройствами: выпуск, обновление, отзыв и очистка, сброс и изменение PIN-кода, просмотр содержимого
- Работа с документами и СКЗИ
- Изменение ответов на секретные вопросы

Сервис удаленного самообслуживания

Сервис удаленного самообслуживания (Remote Self-Service) — веб-приложение Indeed CM, в котором вы можете управлять устройствами без подключения к рабочей станции (за исключением разблокировки устройства).

Сервис удаленного самообслуживания доступен по ссылке: `https://<FQDN сервера Indeed CM>/cm/rss`.

Вход

Чтобы войти в Сервис удаленного самообслуживания:

1. Перейдите по ссылке `https://<FQDN сервера Indeed CM>/cm/rss`.
2. Введите имя пользователя (логин) и символы с изображения.
3. Пройдите аутентификацию по секретным вопросам, чтобы получить доступ к профилю пользователя.

> **ПРИМЕЧАНИЕ**
>
> Если вы не помните ответы на секретные вопросы, измените их в Сервисе самообслуживания.

Действия

Действия выключения и включения, отзыва и очистки устройств выполняются так же, как в Сервисе самообслуживания.

Разблокировка устройства

В Сервисе удаленного самообслуживания вы можете разблокировать устройство, у которого превышено число попыток ввода PIN-кода. Для разблокировки используется утилита Indeed CM Unblock, установленная на вашей рабочей станции.

Чтобы разблокировать устройство:

1. Запустите утилиту Indeed CM Unblock. Расположение по умолчанию: `Пуск` → `Все программы` → `Indeed` (файл *IndeedCM.Unblock.exe*).
2. В выпадающем списке **Доступные устройства** выберите устройство.
3. Скопируйте код разблокировки из поля **Запрос**.
4. Перейдите в Сервис удаленного самообслуживания: `https://<FQDN сервера Indeed CM>/cm/rss`.
5. Выберите устройство и нажмите **Разблокировать устройство**.
6. Введите код разблокировки и нажмите **Получить ответ**.
7. Введите полученный код ответа в поле **Ответ** утилиты разблокировки.
8. Введите новый PIN-код, подтвердите его и нажмите **Разблокировать**.

Действия с устройствами

Выпуск

Как выпустить смарт-карту или USB-токен

Обновление

Как обновить содержимое устройства

Выключение и включение

Как включить и выключить устройство

Отзыв и очистка

Как отозвать и очистить устройство

Сброс и изменение PIN-кода

Как задать новый PIN-код

Просмотр содержимого

Как просмотреть сертификаты на устройстве, скачать или подписать документы

Выпуск

Вы можете получить уже готовое к работе устройство или выпустить устройство самостоятельно, если администратор или оператор выдал вам пустое устройство.

Если вы получили готовое к работе устройство, то при входе в Сервис самообслуживания отобразится вся информация об этом устройстве.

Процесс выпуска

Действия, доступные во время выпуска устройства, зависят от предварительных настроек, заданных администратором в политике использования устройств. Инструкция описывает процесс выпуска устройства с максимальным набором доступных действий.

1. Подключите устройство к рабочей станции.
2. Нажмите **Выпустить устройство**.
3. Выберите шаблоны, по которым будут сформированы сертификаты для записи на устройство.

   Условие доступности

   Администратор включил опцию **Выбирать необязательные сертификаты при выпуске** в политике использования устройств в разделе **Поведение** → **Разрешения пользователя** → **Действия при выпуске устройства**.

4. В форме проверки в СМЭВ внесите недостающие данные или проверьте данные на соответствие и редактируйте при необходимости.

Условие доступности

Форма проверки в СМЭВ отображается, если администратор настроил интеграцию со СМЭВ в разделе СМЭВ, и сертификат выпускается по шаблону для КриптоПро УЦ 2.0 или Валидата УЦ.

Пользователь может редактировать данные, если администратор включил опцию **Редактировать данные в форме проверки СМЭВ** в разделе **Поведение** → **Разрешения пользователя** → **Общие разрешения**.

5. Укажите номер и дату нормативного документа, на основании которого вы выпускаете СКЗИ.

Условие доступности

Пользователь может выпустить СКЗИ, если:

- Устройство поддерживает аппаратную криптографию
- Устройство еще не добавлено в Indeed CM
- Администратор включил опцию **Разрешить пользователю добавлять устройства при выпуске** в разделе **Поведение** → **Общие разрешения**

6. В зависимости от настроек, заданных администратором, устройство выпускается с инициализацией или без инициализации.

Выпуск без инициализации

1. Введите **PIN-код пользователя**.
2. Введите **PIN-код администратора**.

Условие доступности

Поле **PIN-код администратора** отображается, если устройство не добавлено в Indeed CM и администратор включил опцию **Разрешить пользователю добавлять устройства при выпуске** в разделе **Поведение** → **Общие разрешения**.

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, выберите сертификаты, чтобы внести информацию о них в Indeed CM и отслеживать их срок действия.

Условие доступности

Пользователь может выбрать сертификаты для отслеживания, если администратор включил опции **Искать сертификаты при выпуске/обновлении устройства для отслеживания срока действия** и **Разрешить пользователю выбирать отслеживаемые сертификаты** в разделе **Поведение → Общие разрешения**.

Выпуск с инициализацией

Предварительные настройки инициализации

Администратор включил опцию **Инициализировать устройство** в разделе Выпуск и настроил параметры инициализации в разделе Инициализация устройства.

ПРЕДУПРЕЖДЕНИЕ

При выпуске устройства с инициализацией все данные на устройстве будут удалены.

1. Введите **PIN-код администратора**. Если поле оставить пустым, то установится значение, указанное администратором в разделе Типы устройств.

Условие доступности

Поле **PIN-код администратора** отображается, если устройство не добавлено в Indeed CM и администратор включил опцию **Разрешить пользователю добавлять устройства при выпуске** в разделе **Поведение** → **Общие разрешения**.

2. Нажмите **Выпустить**.

7. Если в процессе выпуска устройства был установлен случайный PIN-код, то он отобразится на экране. При необходимости сохраните свой PIN-код и отправьте его по электронной почте себе или своему руководителю.

Условие доступности

Случайный PIN-код устанавливается, если администратор задал опцию **Установить случайный PIN-код пользователя** в разделе Выпуск.

PIN-код можно отправить по электронной почте, если администратор настроил рассылку уведомлений по электронной почте в разделе Уведомления.

8. Нажмите **Закрыть**.

В Сервисе самообслуживания появится раздел **Ваши устройства**, где отображаются сведения о выпущенном устройстве – тип, серийный номер, имя, состояние.

ОСОБЕННОСТИ ВЫПУСКА УСТРОЙСТВ РУТОКЕН БИО

Если вы выпускаете устройство Рутокен ЭЦП 3.0 3250 БИО (Рутокен БИО), на которое записывается сертификат с биометрической защитой, в процессе выпуска откроется окно биометрической аутентификации. Подключите сканер отпечатков пальцев к рабочей станции и пройдите биометрическую аутентификацию, чтобы подтвердить выпуск.

Если на устройстве не зарегистрирована биометрия, обратитесь к администратору.

Подробнее о работе с устройствами Рутокен БИО

Проверка документов для выпуска устройства

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*. Устройство переходит в состояние *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, вы можете отправить документы администратору в Сервисе самообслуживания.

> **ПРИМЕЧАНИЕ**
>
> Настройки проверки документов задает администратор. Инструкция для администратора

В зависимости от настроек, заданных администратором, 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 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**
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 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 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**
2. Дождитесь одобрения документа от администратора.
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 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.

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**
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 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 согласно регламенту получения сертификата проверки электронной подписи, принятому в вашей организации.

Выполните следующие действия:

1. Предоставьте администратору 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 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 по настройке выпуска устройств Registry

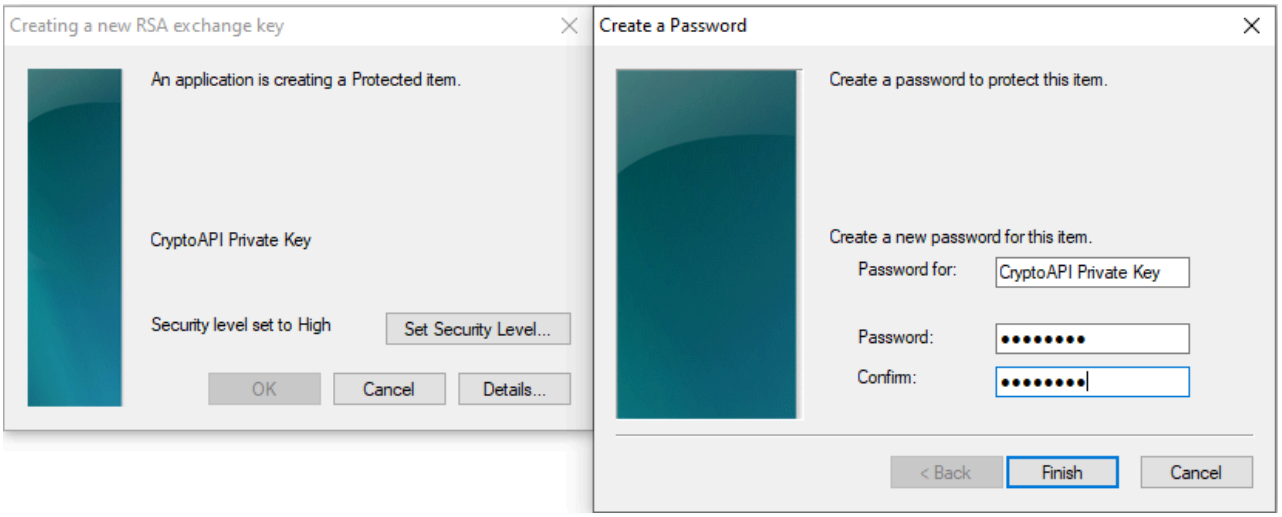
1. Настройте поддержку устройств Registry.
2. Добавьте тип устройства *Registry.xml* в конфигурацию Indeed CM.
3. Установите компонент Cm.Registry.Middleware на рабочую станцию пользователя.

> **ОСОБЕННОСТИ ВЫПУСКА УСТРОЙСТВ REGISTRY**
>
> - Поддерживается выпуск только RSA сертификатов
> - Не поддерживается работа с PIN-кодами
> - Не поддерживается инициализация устройства

Чтобы выпустить устройство Registry:

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 **OK**.



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 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 Cm.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:

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 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 Cm.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:

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 по настройке выпуска устройств AirCard

1. Перейдите в настройки политики использования устройств в раздел **Поведение** → **Разрешения пользователя** → **Общие разрешения** и включите опцию **Выпускать AirCard**.
2. Добавьте тип устройства *AirCard.xml* в конфигурацию системы.
3. Установите компоненты Cm.AirCard.Middleware и Cm.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:

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.

Подключение AirCard к рабочей станции

AirCard можно подключить двумя способами:

- Автоматически в Indeed CM
- Вручную в панели управления Indeed AirCard Enterprise

Indeed CM

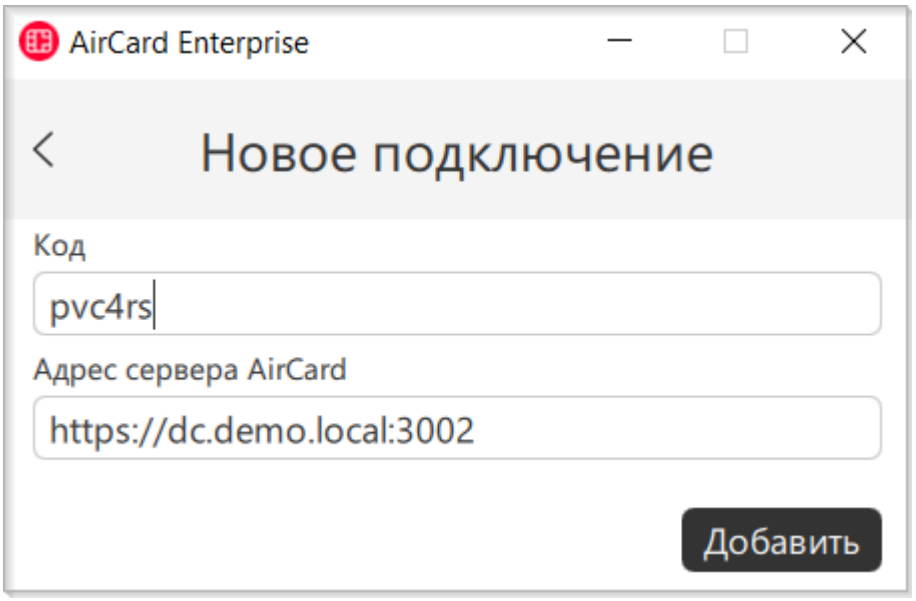
После выпуска устройство AirCard автоматически подключится к разрешенным компьютерам, если они находятся в корпоративной сети предприятия.

Indeed AirCard Enterprise

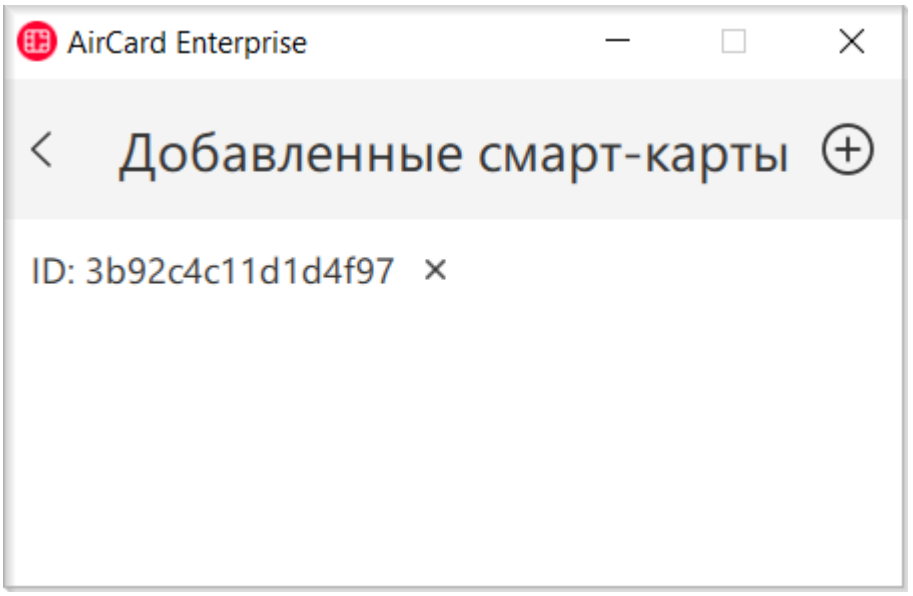
Применяется, если устройство нельзя подключить автоматически (например, если компьютер находится за пределами корпоративной сети предприятия). В этом случае устройство может выпустить только администратор Indeed CM.

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. Код действителен в течение часа, его можно использовать только один раз. Адрес сервера Indeed AirCard Enterprise подставляется автоматически.
4. Нажмите **Добавить**.



После добавления устройство AirCard отобразится в панели управления.



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.

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 .

Обновление

Если срок действия одного или нескольких сертификатов на вашем устройстве подходит к концу, или вам потребовался новый сертификат, то устройство необходимо обновить.

> **ПРИМЕЧАНИЕ**
>
> Возможность обновлять устройства настраивает администратор. Инструкция для администратора

Процесс обновления

Действия, доступные во время обновления устройства, зависят от предварительных настроек, заданных администратором в политике использования устройств. Инструкция описывает процесс обновления устройства с максимальным набором доступных действий.

1. Подключите устройство к рабочей станции.
2. В карточке устройства выберите действие **Обновить содержимое устройства**.
3. Выберите шаблоны, по которым будут сформированы сертификаты для записи на устройство.

   Условие доступности

   Администратор включил опцию **Выбирать необязательные сертификаты при обновлении** в политике использования устройств в разделе **Поведение** → **Разрешения пользователя** → **Действия с выпущенным устройством**.
4. В форме проверки в СМЭВ внесите недостающие данные или проверьте данные на соответствие и редактируйте при необходимости.

Условие доступности

Форма проверки в СМЭВ отображается, если администратор настроил интеграцию со СМЭВ в разделе СМЭВ, и сертификат выпускается по шаблону для КриптоПро УЦ 2.0 или Валидата УЦ.

Пользователь может редактировать данные, если администратор включил опцию **Редактировать данные в форме проверки СМЭВ** в разделе **Поведение** → **Разрешения пользователя** → **Общие разрешения**.

5. Введите **PIN-код пользователя**.

6. Если устройство содержит сторонние сертификаты, выберите сертификаты, чтобы внести информацию о них в Indeed CM и отслеживать их срок действия.

Условие доступности

Пользователь может выбрать сертификаты для отслеживания, если администратор включил опции **Искать сертификаты при выпуске/обновлении устройства для отслеживания срока действия** и **Разрешить пользователю выбирать отслеживаемые сертификаты** в разделе **Поведение** → **Общие разрешения**.

7. Нажмите **Обновить**.

ОСОБЕННОСТИ ОБНОВЛЕНИЯ УСТРОЙСТВ РУТОКЕН БИО

Если вы обновляете устройство Рутокен ЭЦП 3.0 3250 БИО (Рутокен БИО) и в процессе обновления записывается или удаляется сертификат, защищенный биометрией, откроется окно биометрической аутентификации. Подключите сканер отпечатков пальцев к рабочей станции и пройдите биометрическую аутентификацию, чтобы подтвердить обновление. Аутентификация может потребоваться несколько раз — например, при создании нового защищенного сертификата и удалении старого.

Подтверждение не требуется, если в параметрах шаблона сертификата включена опция **Не удалять сертификат при обновлении/очистке устройства**.

Подробнее о работе с устройствами Рутокен БИО

Проверка документов для обновления устройства

Обновление устройства приостанавливается, 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**.

> **ПРИМЕЧАНИЕ**
>
> Настройки проверки документов задает администратор. Инструкция для администратора

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

Вы можете выключить устройство, например, на время отпуска, и затем снова включить. Чтобы выключить или включить устройство, его не нужно подключать к рабочей станции.

> **ПРИМЕЧАНИЕ**
>
> Возможность включать и выключать устройства настраивает администратор. Инструкция для администратора
>
> Если в параметрах шаблонов сертификатов используемого УЦ администратор включил опцию **Отзывать сертификат при отзыве/выключении устройства**, то все сертификаты на устройстве отзываются без возможности восстановления.

Чтобы выключить устройство, в карточке устройства нажмите **Временно выключить устройство** → **Выключить**. Состояние устройства изменится с *Выпущено* на *Выключено*.

Чтобы включить устройство, в карточке устройства нажмите **Включить устройство** → **Включить**. Состояние устройства изменится с *Выключено* на *Выпущено*.

Выключение устройств без входа в ОС

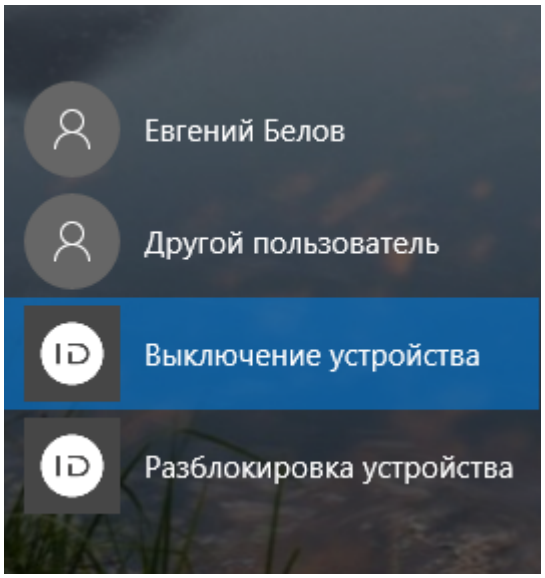
В экстренном случае вы можете самостоятельно выключить устройство без входа в операционную систему, если администратор настроил разрешение.

Выключение устройства доступно только в том случае, если у рабочей станции есть связь с сервером Indeed CM, и у вас настроены секретные вопросы и ответы.

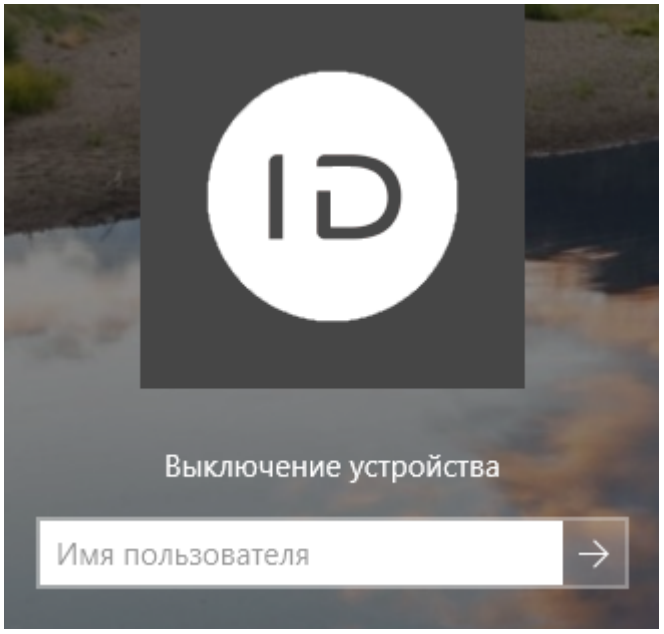
Пример выключения устройства в ОС Windows 10

Чтобы выключить устройство:

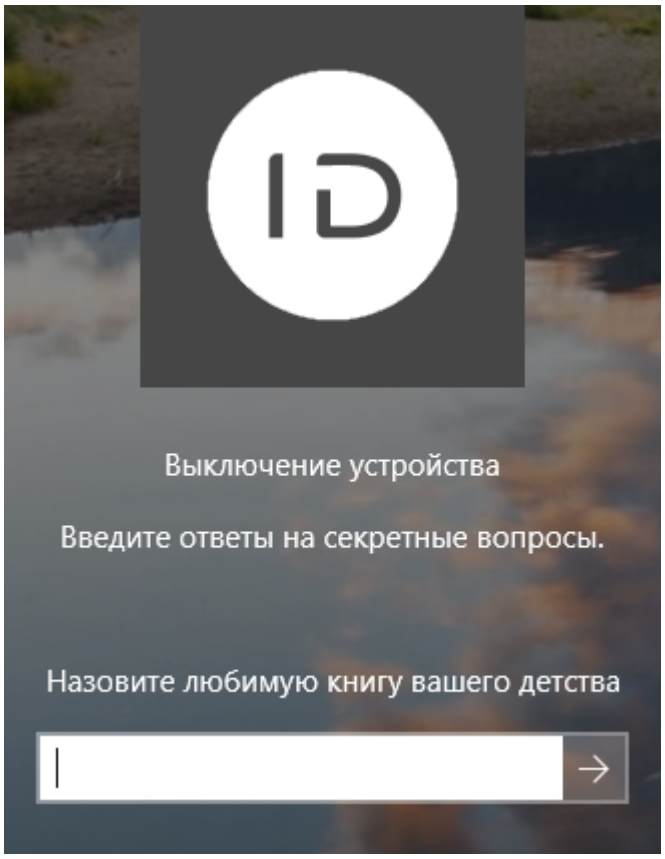
1. На экране выбора пользователей для входа в ОС выберите **Выключение устройства**.



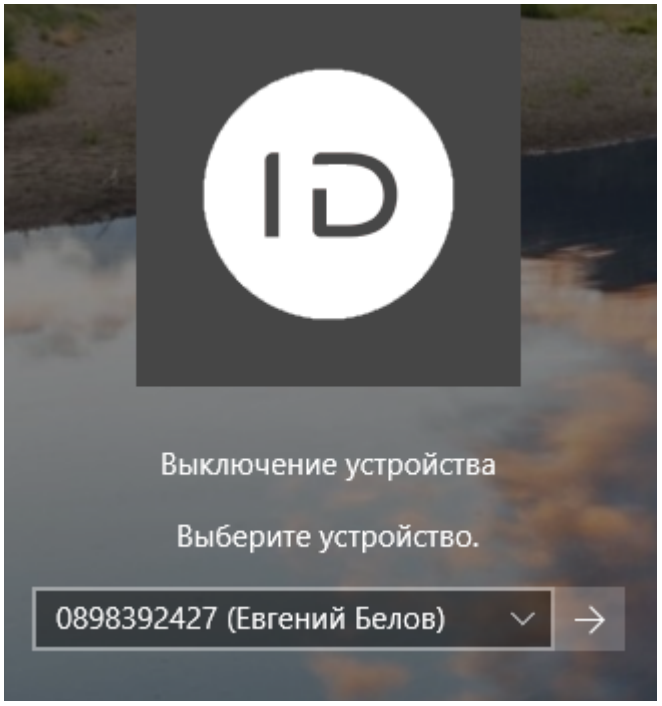
2. В окне входа в ОС укажите имя пользователя (логин), устройство (смарт-карту), которое необходимо выключить.



3. Введите ответы на секретные вопросы.



4. Выберите устройство из списка и нажмите  .



Отзыв и очистка

Отзовите устройство, если оно повреждено, утеряно или скомпрометировано. После отзыва устройство можно очистить или инициализировать. Устройство останется закрепленным за вами, и его можно выпустить повторно.

> **ПРИМЕЧАНИЕ**
>
> Возможность отзывать и очищать устройства настраивает администратор. Инструкция для администратора
>
> Если в параметрах шаблонов сертификатов используемого УЦ включена опция **Отзывать сертификат при отзыве/выключении устройства**, все сертификаты на устройстве отзываются без возможности восстановления.

Отзыв

1. В карточке устройства выберите действие **Сообщить о том, что устройство неисправно, утеряно или скомпрометировано**.
2. Выберите причину отзыва:
   - Устройство неисправно
   - Устройство утеряно
   - Компрометация устройства
3. Нажмите **Отозвать**.

Состояние устройства изменится с *Выпущено* на *Отозвано*.

Очистка и инициализация

1. Подключите устройство к рабочей станции.
2. В карточке устройства выберите действие **Очистить устройство**.
3. Выберите действие, которое произойдет с устройством:
   - **Очистить** — с устройства удаляется только управляемое содержимое: данные, записанные через Indeed CM (сертификаты и ключи, аутентификаторы Indeed AM,

идентификаторы SNS, сложный пароль Рутокен Логон). Данные, записанные на устройство вне Indeed CM, сохраняются.

- **Инициализировать** — с устройства удаляются все данные.

4. Если в Indeed CM ведется учет СКЗИ, укажите номер и дату нормативного документа, на основании которого выполняется уничтожение СКЗИ.
5. В поле **Новый PIN-код пользователя** введите PIN-код, который установится на устройстве. Если оставить поле пустым, установится PIN-код по умолчанию.
6. Нажмите **Очистить**.

> **ОСОБЕННОСТИ ОЧИСТКИ И ИНИЦИАЛИЗАЦИИ УСТРОЙСТВ РУТОКЕН БИО**
>
> Для устройства Рутокен ЭЦП 3.0 3250 БИО (Рутокен БИО), которое содержит сертификат, защищенный биометрией:
>
> - При выборе действия **Очистить** откроется окно биометрической аутентификации. Подключите сканер отпечатков пальцев к рабочей станции и пройдите биометрическую аутентификацию, чтобы подтвердить удаление сертификата. После очистки биометрические данные остаются на устройстве.
> - При выборе действия **Инициализировать** биометрическое подтверждение не требуется. С устройства удаляются все данные, включая биометрию.
>
> Подробнее о работе с устройствами Рутокен БИО

Сброс и изменение PIN-кода

Если вы забыли PIN-код устройства и заблокировали его, PIN-код можно сбросить. Если PIN-код известен, его можно изменить без сброса.

> **ПРИМЕЧАНИЕ**
>
> Возможность сбросить и изменить PIN-код настраивает администратор. Инструкция для администратора

Сброс PIN-кода

1. В карточке устройства выберите действие **Сбросить PIN-код устройства**.
2. Подключите устройство к рабочей станции.
3. Введите новый PIN-код и подтвердите его.
4. Нажмите **Сбросить**.

Изменение PIN-кода

1. В карточке устройства выберите действие **Изменить PIN-код устройства**.
2. Подключите устройство к рабочей станции.
3. Введите текущий PIN-код, задайте новый PIN-код и подтвердите его.
4. Нажмите **Изменить**.

Просмотр содержимого

В карточке устройства на вкладке **Содержимое** отображаются сертификаты, которые хранятся на устройстве, и информация о них: шаблон, удостоверяющий центр, срок действия, состояние.

> **ПРИМЕЧАНИЕ**
>
> Доступ к содержимому устройства настраивает администратор. Инструкция для администратора

Документы сертификата

На вкладке **Содержимое** вы можете скачать или подписать документы сертификата — форму сертификата, запрос на сертификат или запрос на отзыв.

1. В разделе **Ваши устройства** выберите устройство и перейдите на вкладку **Содержимое**.
2. Нажмите  напротив нужного сертификата.
3. Выберите шаблон документа: сертификат, запрос на сертификат или запрос на отзыв сертификата. Откроется файл документа.
4. Выберите действие:
   - **Сохранить документ**, чтобы скачать файл.
   - **Подписать документ**, чтобы подписать документ электронной подписью. Подробнее о подписи документов

Изменение ответов на секретные вопросы

Секретные вопросы используются для аутентификации в следующих случаях:

- Разблокировка устройства
- Выключение устройства без входа в ОС
- Доступ в Сервис удаленного самообслуживания
- Выполнение задачи по сбросу PIN-кода пользователя на клиентском агенте

> **ПРИМЕЧАНИЕ**
>
> В политике использования устройств администратор настраивает:
>
> - Список секретных вопросов — в разделе **Аутентификация**
> - Возможность изменить ответы — в разделе **Поведение**

Чтобы изменить ответы на секретные вопросы:

1. Выберите действие **Изменить ответы на секретные вопросы**.
2. Выберите вопрос и введите ответ на вопрос.
3. Нажмите **ОК**.

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

OK Отмена

СКЗИ

В разделе **Ваши СКЗИ** в Сервисе самообслуживания вы можете управлять средствами криптографической защиты информации (СКЗИ) – печатать и подписывать нормативные документы СКЗИ, проходить обучающие курсы для доступа к работе с СКЗИ.

> **ПРИМЕЧАНИЕ**
>
> Доступ к разделу **Ваши СКЗИ** настраивает администратор. Инструкция для администратора

Печать документов

Чтобы распечатать документ СКЗИ:

1. Нажмите  напротив нужного экземпляра СКЗИ.
2. Выберите шаблон печати документа. В зависимости от настроек, заданных администратором, отображается один из списков:
   - **Вид нормативного документа** — список шаблонов печати, привязанных к объекту СКЗИ в разделе **Конфигурация** → **СКЗИ** → Нормативные документы.
   - **Шаблон печати** — список всех шаблонов печати, загруженных в разделе **Конфигурация** → Шаблоны печати.
3. Нажмите **Распечатать документ**.

Подпись документов

Вы можете подписывать нормативные документы СКЗИ, если администратор настроил функцию внутреннего электронного документооборота Indeed CM ЭДО и у вас есть подходящий сертификат подписи.

Как подписать нормативный документ СКЗИ

Обучающие курсы по работе с СКЗИ

С помощью Indeed CM вы можете проходить обучающие курсы по работе с СКЗИ. После прохождения курсов вы получаете документ, подтверждающий специальную подготовку и

допуск к самостоятельной работе с СКЗИ.

Администраторы могут управлять обучением пользователя по работе с СКЗИ в его карточке в разделе **Назначенные СКЗИ** → Обучающие курсы.

Доступ к обучающему курсу определяется политикой, действующей на пользователя. Администратор выбирает политики при создании курса.

Прохождение обучения

1. Откройте раздел **Ваши СКЗИ** → **Обучающие курсы**.
2. Выберите обучающий курс и нажмите **Начать обучение**. Администратор может назначить вам обучение в Консоли управления. Состояние обучения меняется с *Не пройдено* на *В процессе*.
3. Пройдите обучение и нажмите **Завершить обучение**. Администратор может завершить ваше обучение в Консоли управления. Состояние обучения меняется с *В процессе* на *Ожидание одобрения*.
4. Пройдите тест на знание правил по работе с СКЗИ согласно регламенту, принятому в вашей организации. После проверки знаний администратор одобряет завершение обучения. Состояние обучения меняется с *Ожидание одобрения* на *Завершено*.

Печать документа о прохождении обучения

Чтобы распечатать документ о прохождении обучения:

1. Нажмите  напротив пройденного обучающего курса.
2. Выберите шаблон, по которому формируется документ.
3. Нажмите **Распечатать документ**.

Отмена обучения

Вы можете отменить назначенное обучение. Отмена доступна для обучений в состоянии *В процессе* и *Ожидание одобрения*. Администратор может отменить обучение, например, если вы не прошли тест на знание правил по работе с СКЗИ.

> **ПРИМЕЧАНИЕ**
>
> Возможность отменить обучение настраивает администратор. Инструкция для администратора

Уведомления

Вы можете получать уведомления о следующих событиях, связанных с обучением:

- Начало обучения СКЗИ
- Отмена обучения СКЗИ
- Одобрение завершения обучения СКЗИ

> **ПРИМЕЧАНИЕ**
>
> Возможность получать уведомления настраивает администратор. Инструкция для администратора

Документы

Вы можете управлять документами в разделе **Ваши документы** вы можете управлять документами для получения сертификата подписи и нормативными документами СКЗИ. Документы можно добавить, подписать, скачать, редактировать или удалить.

Предварительные настройки для администратора

Чтобы раздел **Ваши документы** отображался в Сервисе самообслуживания:

1. Откройте Мастер настройки.
2. Перейдите в раздел **Общие функции**.
3. Включите опцию **Внутренний документооборот**.

Чтобы пользователи могли управлять нормативными документами СКЗИ:

1. Откройте Мастер настройки.
2. Перейдите в раздел **Функции системы** → **Журнал учета СКЗИ**.
3. Включите опцию **Вести журнал учета СКЗИ**.
4. Откройте Консоль управления.
5. Перейдите в настройки политики в раздел **Поведение** → **Разрешения пользователя** → **Действия с СКЗИ**.
6. Включите опцию **Просматривать**.

Чтобы пользователи могли удалять документы:

1. Откройте Консоль управления.
2. Перейдите в настройки политики в раздел **Поведение** → **Разрешения пользователя** → **Действия с документами**.
3. Включите опцию **Удалять**.

Чтобы установить тип электронной подписи, который разрешено использовать для подписания документов:

1. Откройте раздел **Конфигурация** и перейдите в настройки политики использования устройств.
2. Перейдите в раздел **Поведение** → **Разрешения пользователя** → **Действия с документами**.
3. Выберите значение в выпадающем списке **Использовать тип подписи**.
4. Нажмите **Сохранить**.

Типы документов

Документы для получения сертификата подписи

- 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
- Пользовательский документ – другие виды документов, например, подписанный регламент удостоверяющего центра

Нормативные документы СКЗИ

Если в вашей организации ведется учет средств криптографической защиты информации (СКЗИ), поддерживается обмен документами для следующих объектов СКЗИ:

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

Требования для подписи документов

- Наличие устройства с сертификатом 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).

ОСОБЕННОСТИ ПОДПИСИ ДОКУМЕНТОВ С ПОМОЩЬЮ УСТРОЙСТВ РУТОКЕН БИО

Если вы подписываете документ с помощью устройства Рутокен ЭЦП 3.0 3250 БИО (Рутокен БИО) и сертификат подписи защищен биометрией, в процессе подписания откроется окно биометрической аутентификации. Подключите сканер отпечатков пальцев к рабочей станции и пройдите биометрическую аутентификацию, чтобы подтвердить подпись документа.

Подробнее о работе с устройствами Рутокен БИО

Тип подписи и выбор сертификата

Список сертификатов, доступных для подписи документов, зависит от типа подписи, настроенного администратором в политике использования устройств.
Инструкция для администратора

- **CMS** — для подписи подходят сертификаты из любого поддерживаемого УЦ, записанные на любые поддерживаемые устройства.
- **CAdES** — для подписи подходит только сертификат КриптоПро УЦ 2.0, записанный на устройство с поддержкой ГОСТ-криптографии (Рутокен, JaCarta, ESMART).

Добавление документов

Документ, подписанный на бумаге

Чтобы добавить документ, подписанный на бумаге:

1. В разделе **Ваши документы** нажмите **Добавить документ**.
2. Выберите тип документа и загрузите файл.
3. (Опционально) Заполните поле **Описание**.
4. Нажмите **Добавить**.

Документ с электронной подписью

При добавлении документа вы можете подписать его электронной подписью.

Чтобы добавить и подписать документ:

1. В разделе **Ваши документы** нажмите **Добавить документ**.
2. Выберите тип документа и загрузите файл.
3. (Опционально) Заполните поле **Описание**.
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 подписи.

   Если сертификат не отображается
7. Введите PIN-код пользователя.
8. Нажмите **Добавить**.

Подпись документов по шаблонам

Пользователи могут подписать документы, которые уже доступны в Indeed CM. Документы формируются по шаблонам, которые настраивает администратор в разделе **Конфигурация** → Шаблоны печати.

Подписанные документы автоматически появляются в списке **Ваши документы**.

Документы для получения сертификата подписи

1. В разделе **Ваши устройства** выберите устройство, на котором содержится нужный сертификат, и перейдите на вкладку **Содержимое**.
2. Нажмите  напротив нужного сертификата и выберите шаблон документа: сертификат, запрос на сертификат или запрос на отзыв сертификата. Откроется файл документа.
3. Нажмите **Подписать документ**. Чтобы скачать и распечатать документ без подписи, нажмите **Сохранить документ**.
4. Подключите устройство с сертификатом подписи к рабочей станции и выберите его в выпадающем списке **Устройство**.

5. В выпадающем списке **Сертификат** выберите подходящий сертификат подписи.

   Если сертификат не отображается

6. Введите PIN-код пользователя.

7. Нажмите **Подписать**.

Нормативные документы СКЗИ

1. В разделе **Ваши СКЗИ** нажмите  напротив экземпляра СКЗИ, для которого формируется документ.

2. Выберите шаблон печати документа. В зависимости от настроек печати нормативных документов СКЗИ отображается один из списков:

   - **Вид нормативного документа** — список шаблонов печати, привязанных к объекту СКЗИ в разделе **Конфигурация** → **СКЗИ** → Нормативные документы.
   - **Шаблон печати** — список всех шаблонов печати, загруженных в разделе **Конфигурация** → Шаблоны печати.

3. Нажмите **Распечатать документ**. Откроется файл документа.

4. Нажмите **Подписать документ**. Чтобы скачать документ без подписи, нажмите **Сохранить 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 подписи.

   Если сертификат не отображается

7. Введите PIN-код пользователя.

8. Нажмите **Подписать**.

Клиентский агент

Клиентский агент Indeed CM Agent работает в фоновом режиме на вашей рабочей станции. Когда администратор назначает задачу на ваше устройство, агент открывает окно с запросом и предлагает выполнить необходимые действия.

Задачи, которые требуют действия:

- Изменение PIN-кода
- Сброс и разблокировка PIN-кода
- Обновление содержимого устройства

Изменение PIN-кода

Администратор может установить срок действия PIN-кода вашего устройства. Если срок действия PIN-кода истек, при подключении устройства к рабочей станции откроется окно смены PIN-кода. Задайте новый PIN-код.

> **РУТОКЕН ЭЦП 3.0, IDPRIME И ETOKEN 72K**
>
> Устройства Рутокен ЭЦП 3.0, IDPrime и eToken поддерживают аппаратное требование смены PIN-кода при первом подключении устройства к рабочей станции.

Сброс PIN-кода

Если вы забыли PIN-код или заблокировали устройство, обратитесь к администратору, чтобы он создал задачу по сбросу PIN-кода.

> **ПРЕДУПРЕЖДЕНИЕ**
>
> Для возможности сбросить PIN-код у вас должны быть заданы ответы на секретные вопросы. Если вы не помните ответы, измените их.

Чтобы сбросить PIN-код:

1. Подключите устройство к рабочей станции. Откроется окно сброса PIN-кода.
2. Введите ответ на один или несколько секретных вопросов.

3. Введите новый PIN-код и подтвердите его.
4. Нажмите **Сбросить**.

Появится сообщение *PIN-код пользователя на устройстве успешно сброшен*.

Обновление устройства

Когда администратор назначит задачу по обновлению устройства, при подключении устройства к рабочей станции откроется окно обновления.

Чтобы обновить устройство:

1. Подключите устройство к рабочей станции. Откроется окно обновления.
2. Введите PIN-код и нажмите **Обновить**.
3. Выберите сторонние сертификаты, чтобы внести информацию о них в Indeed CM и отслеживать их срок действия.

   Условие доступности

   Выбор сертификатов для отслеживания доступен, если в настройках политики в разделе **Поведение** → **Общие разрешения** администратор включил опции **Искать сертификаты при выпуске/обновлении устройства для отслеживания срока действия** и **Разрешить пользователю выбирать отслеживаемые сертификаты**.
4. Нажмите **ОК**.

Обновление может длиться несколько минут. По завершении появится сообщение *Устройство успешно обновлено*.

Если регламент вашей организации предусматривает проверку документов для обновления сертификатов, обновление может быть приостановлено. В окне появится сообщение *Обновление устройства ожидает решения*, устройству присвоится статус *В ожидании*.
Подробнее о проверке документов

Разблокировка биометрии

Биометрическая аутентификация на устройстве Рутокен БИО блокируется, если вы не прошли проверку отпечатка пальца пять раз подряд. Обратитесь к администратору, чтобы он создал задачу по разблокировке биометрии для вашего устройства.

Биометрия разблокируется автоматически, как только вы подключите устройство к рабочей станции с агентом.

Подробнее о работе с устройствами Рутокен БИО

Просмотр файлов и ресурсов

При настройке Indeed CM администратор может добавить файлы и ресурсы, которые будут доступны в Сервисе самообслуживания на странице **Загрузки**: `https://<FQDN сервера Indeed CM>/cm/ss/Downloads`.

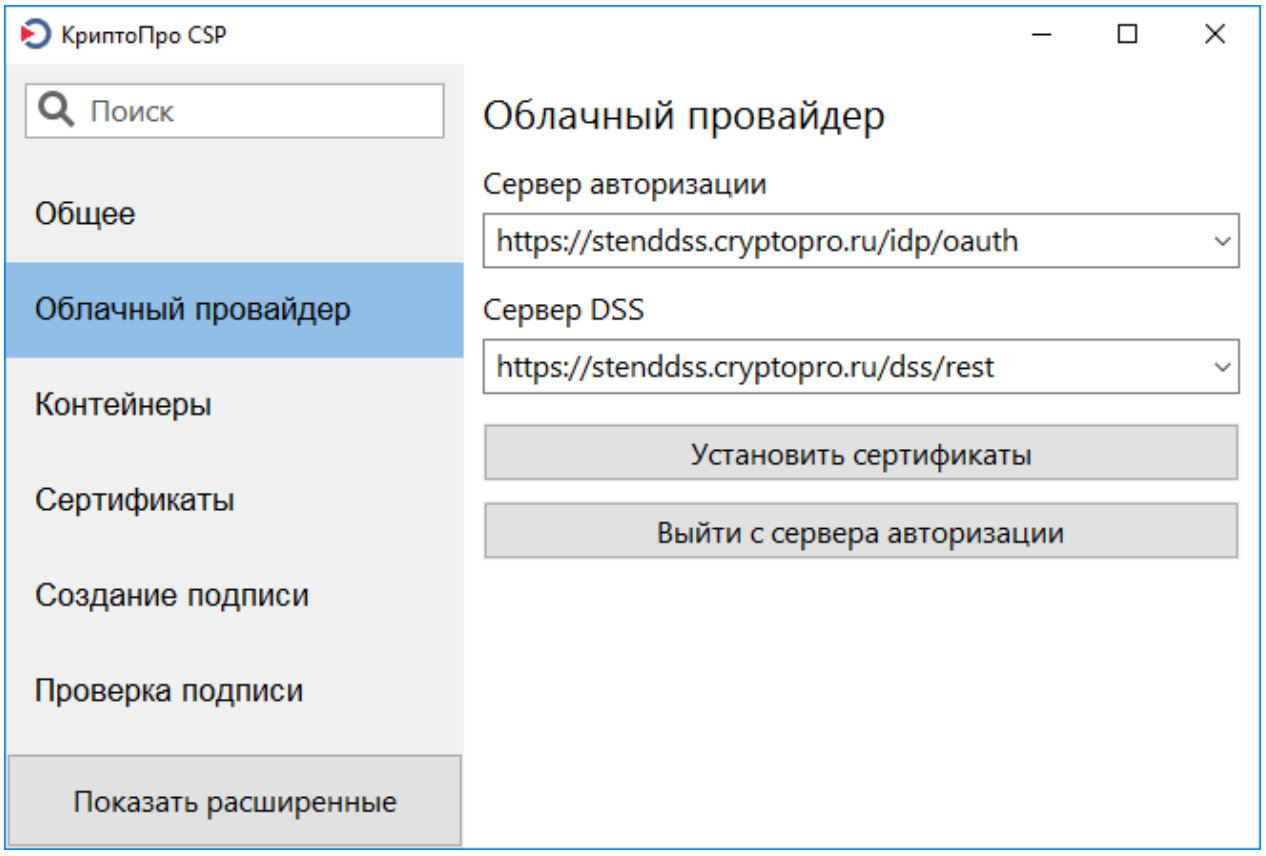
> **ПОДСКАЗКА**
>
> Администраторы могут загружать файлы и ресурсы, если в Мастере настройки в разделе **Общие функции** включена опция **Загрузка файлов и ресурсов**.

Выгрузка сертификата КриптоПро DSS

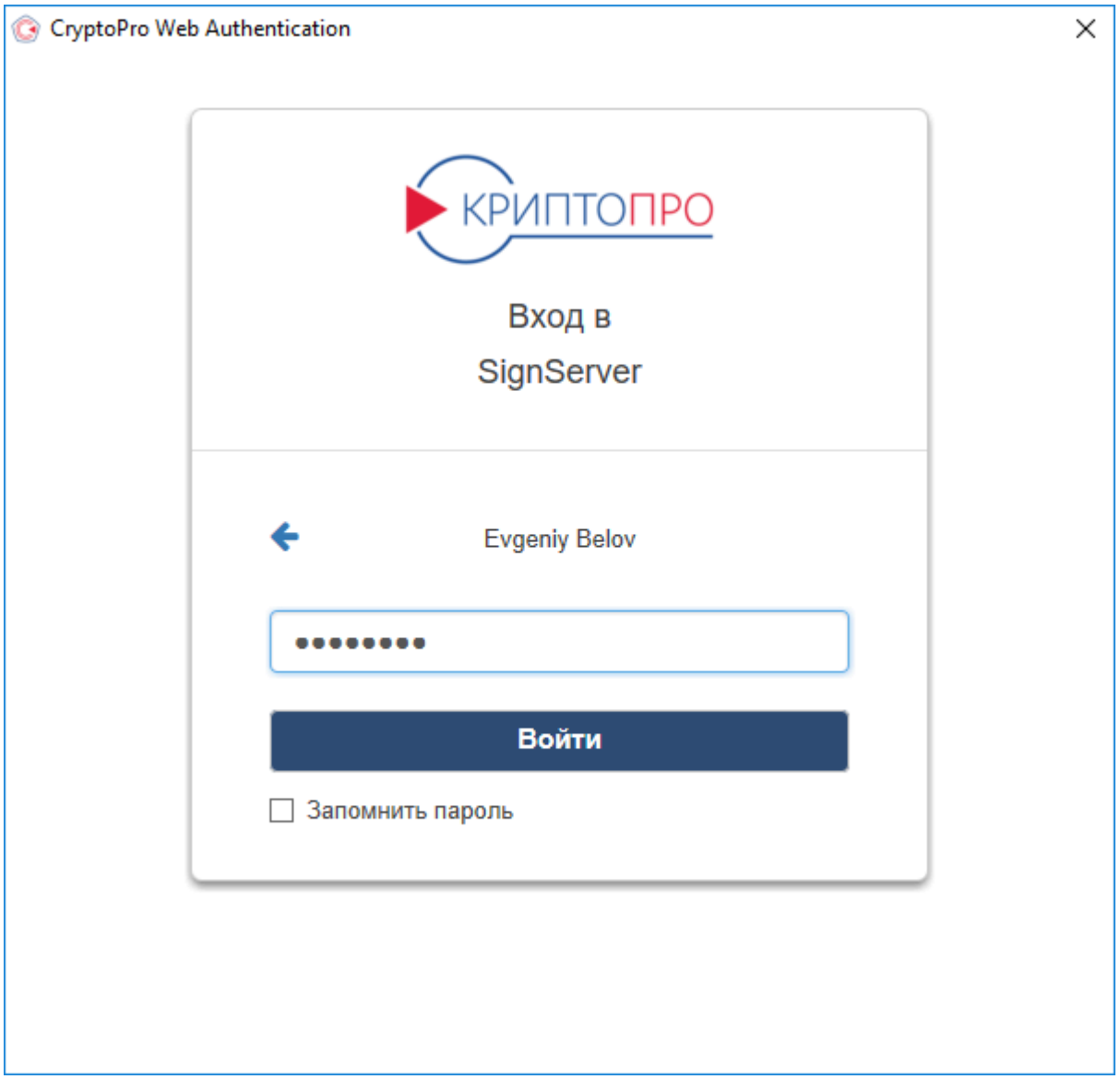
Если ваш сертификат хранится в облачном сервисе КриптоПро DSS, вы можете выгрузить его на свою рабочую станцию с помощью компонента Инструменты КриптоПро.

Чтобы выгрузить сертификат из облачного сервиса КриптоПро DSS:

1. Запустите компонент Инструменты КриптоПро и перейдите в раздел **Облачный провайдер**.
2. Укажите URL-адрес сервера авторизации и сервера DSS.



3. Нажмите **Установить сертификаты**.
4. Введите логин и пароль от личного кабинета пользователя DSS.
5. Нажмите **Войти**.


CryptoPro Web Authentication
КРИПТОПРО
Вход в
SignServer
Evgeniy Belov
Войти
Запомнить пароль

API

Набор API-функций позволяет управлять устройствами и средствами криптографической защиты информации (СКЗИ) с помощью клиентских приложений.

API-функции доступны через веб-приложение API. Приложение входит в состав сервера Indeed CM и доступно по адресу: `https://<FQDN сервера Indeed CM>/cm/api`.

Аутентификация

Настройка аутентификации для работы с API в Swagger, Postman, PowerShell и Bash

Устройства

Управление устройствами через API

СКЗИ

Управление СКЗИ через API

Аутентификация

Для работы с Indeed CM API вы можете использовать любые инструменты. Далее описана настройка работы с API в Swagger, Postman, Windows PowerShell и Linux Bash. Настройка инструмента зависит от типа аутентификации, заданного в Мастере настройки:

- **Windows** — по учетной записи Windows. Доступна только на Windows-сервере Indeed CM.
- **OpenID Connect** — по протоколу OAuth 2.0 с получением токена доступа. Доступна на Windows- и Linux-серверах Indeed CM.

Windows

Проверка настроек аутентификации

1. Запустите Диспетчер служб IIS (Internet Information Services (IIS) Manager).
2. В левом меню выберите сайт **Default Web Site** и раскройте список приложений **cm**.
3. Выберите приложение **api**.
4. В панели управления приложением выберите свойство **Проверка подлинности** (Authentication) и убедитесь, что выбрана **Проверка подлинности Windows** (Windows Authentication).
5. Закройте Диспетчер служб IIS.
6. Перейдите в каталог *C:\inetpub\wwwroot\cm\api* и откройте конфигурационный файл приложения Indeed CM API *appsettings.json*.
7. Убедитесь, что в параметре `authentication` установлено значение `Windows`.

Swagger

Чтобы работать с API через Swagger, внесите изменения в конфигурационный файл приложения Indeed CM API:

1. Перейдите в каталог *C:\inetpub\wwwroot\cm\api* и откройте файл *appsettings.json*.
2. В секции `webApiSettings` в параметре `enableSwagger` установите значение `true` и сохраните изменения.
3. Примените настройки на сервере Indeed CM.

Интерфейс Swagger будет доступен по ссылке `https://<FQDN сервера Indeed CM>/cm/api/swagger`.

При аутентификации в Swagger автоматически используются учетные данные Windows.

Postman

Чтобы настроить аутентификацию в Postman:

1. В левой части верхней панели управления Postman нажмите **+**. Откроется поле для ввода запросов.
2. Перейдите на вкладку **Auth** и в выпадающем списке выберите **NTLM Authentication**.
3. Введите имя пользователя в формате `DOMAIN\Username` и пароль.

Чтобы выполнить запрос:

1. В строке запроса выберите тип.
2. Укажите URL запроса.
3. Нажмите **Send**.

OpenID Connect

Проверка настроек аутентификации

Чтобы проверить настройки аутентификации в API на Windows-сервере Indeed CM:

1. Запустите Диспетчер служб IIS (Internet Information Services (IIS) Manager).
2. В левом меню выберите сайт **Default Web Site** и раскройте список приложений **cm**.
3. Выберите приложение **api**.
4. В панели управления приложением выберите свойство **Проверка подлинности** (Authentication) и убедитесь, что выбрана **Анонимная проверка подлинности** (Anonymous Authentication).
5. Закройте Диспетчер служб IIS.
6. Перейдите в каталог *C:\inetpub\wwwroot\cm\api* и откройте конфигурационный файл приложения Indeed CM API *appsettings.json*.
7. Убедитесь, что в параметре `authentication` установлено значение `OAuth2Introspection`.

Чтобы проверить настройки аутентификации в API на Linux-сервере Indeed CM:

1. Перейдите в каталог */opt/indeed/cm/api* и откройте конфигурационный файл приложения Indeed CM API *appsettings.json*.

2. Убедитесь, что в параметре `authentication` установлено значение `OAuth2Introspection`.

Swagger

Чтобы работать с API через Swagger, внесите изменения в конфигурационный файл приложения Indeed CM API:

1. Перейдите в каталог *C:\inetpub\wwwroot\cm\api* в ОС Windows или */opt/indeed/cm/api* в ОС Linux и откройте файл *appsettings.json*.
2. В секции `webApiSettings` в параметре `enableSwagger` установите значение `true`.
3. Сохраните изменения.
4. Примените настройки на сервере Indeed CM.

Чтобы аутентифицироваться в Swagger:

1. Откройте браузер и перейдите по ссылке `https://<FQDN сервера Indeed CM>/cm/api/swagger`.
2. В правой части окна нажмите **Authorize**.
3. В поле **Scopes** нажмите **Select all**.
4. Нажмите **Authorize**.

Postman

Чтобы настроить аутентификацию в Postman:

1. В левой части верхней панели управления Postman нажмите **+**. Откроется поле для ввода запросов.
2. Перейдите на вкладку **Auth** и в выпадающем списке выберите **OAuth 2.0**.
3. В поле **Add auth data to** оставьте значение по умолчанию **Request Headers**.
4. В разделе **Current Token** в поле **Header Prefix** оставьте значение по умолчанию **Bearer**.
5. В разделе **Configure New Token** заполните поля:
   - **Token Name** – произвольное имя токена.
   - **Grant Type** – **Password Credentials**.
   - **Access Token URL** – `https://<FQDN сервера Indeed CM>/cm/oidc/connect/token`.
   - **Client ID** – `WebApiClient`.
   - **Username** – имя пользователя в формате `DOMAIN\Username`.

- **Password** – пароль пользователя.
- **Client Authentication** – **Send as Basic Auth header**.

6. Нажмите **Get New Access Token**. Откроется окно с токеном.
7. Нажмите **Use Token**.

Чтобы выполнить запрос:

1. В строке запроса выберите тип.
2. Укажите URL запроса.
3. Нажмите **Send**.

Windows PowerShell

Чтобы работать с API через PowerShell, используйте PowerShell-скрипты.

Получите токен доступа и выполните запрос:

1. Определите переменные в терминале или в файле PowerShell-скрипта.

```
$body = @{
    grant_type = 'password'
    username = 'DOMAIN\Username'
    password = 'P@ssw0rd'
    scope = 'openid webapi'
    client_id = 'WebApiClient'
}
$base_url = "https://<FQDN сервера Indeed CM>"
$token_url = "$base_url/cm/oidc/connect/token"
```

2. Извлеките токен доступа (access_token) из ответа.

```
$resp = Invoke-RestMethod -Method Post -Uri $token_url -Body $body
$token = $resp.access_token
```

3. Добавьте полученный токен в заголовок запроса.

```
$headers = @{Authorization = "Bearer $token"}
```

4. Выполните запрос.

Пример GET-запроса

```
Invoke-RestMethod -Method Get -Uri "$base_url/cm/api/Cards?
state=Issued&offset=0&count=0" -Headers $headers
```

Пример POST-запроса

```
Invoke-RestMethod -Method Post -Uri "$base_url/cm/api/Cards/123/Enable" -Headers
$headers
```

Linux Bash

Чтобы работать с API через Linux Bash, используйте Bash-скрипты.

Получите токен доступа и выполните запрос:

1. Определите переменные в терминале или в файле Bash-скрипта.

```
username="DOMAIN\\username"
password="P@ssw0rd"
base_url="https://<FQDN сервера Indeed CM>"
body="grant_type=password&username=$username&password=$password&scope=openid%20webapi&cli
token_url="$base_url/cm/oidc/connect/token"
```

2. Извлеките токен доступа (access_token) из ответа.

```
resp=$(curl -s -X POST $token_url -H "Content-Type: application/x-www-form-urlencoded"
--data $body)
token=$(echo $resp | grep -o '"access_token": "[^"]*' | cut -d'"' -f4)
```

3. Добавьте полученный токен в заголовок запроса.

```
headers="Authorization: Bearer $token"
```

4. Выполните запрос.

Пример GET-запроса

```
curl -X GET "$base_url/cm/api/Cards?state=Issued&offset=0&count=0" -H "$headers" -d ''
```

Пример POST-запроса

```
curl -X POST "$base_url/cm/api/Cards/123/Enable" -H "$headers" -d ''
```

Пример Bash-скрипта

```
#!/bin/sh
#User input
username="DEMO\\admin"
password="P@ssw0rd"
base_url="https://cm-test.local"
body="grant_type=password&username=$username&password=$password&scope=openid%20webap
token_url="$base_url/cm/oidc/connect/token"
# Get token
resp=$(curl -s -X POST $token_url -H "Content-Type: application/x-www-form-urlencode
# Parse token
token=$(echo $resp | grep -o '"access_token": "[^"]*' | cut -d'"' -f4)
# Combine header
headers="Authorization: Bearer $token"
# Test enable card (POST)
curl -X POST "https://cm-test.local/cm/api/Cards/123/Enable" -H "accept: */*" -d ''
# Test Get enabled card (GET)
curl -X GET "https://cm-test.local/cm/api/Cards?state=Issued&offset=0&count=0" -H "a
```

Устройства

При работе с устройствами через API вам доступны следующие операции:

- Получить список устройств по заданным фильтрам
- Найти устройство по идентификатору
- Отозвать устройство
- Изъять отозванное устройство
- Временно отключить устройство
- Включить устройство
- Отозвать неактуальный сертификат пользователя

`GET /Cards`

Возвращает список устройств по заданным фильтрам.

Параметры запроса

Параметр	Описание
`userName`	Имя пользователя в формате DOMAIN\LogonName или User Principal Name (UPN)
`policyName`	Название политики, действующей на устройство
`serialNumber`	Серийный номер устройства
`cardTypeName`	Название типа устройства
`cardModelName`	Название модели устройства. Значение выводится только для устройств Рутокен, JaCarta, eToken PRO Java 72K и IDPrime MD, если в разделе **Типы устройств** для данных устройств заданы отдельные настройки для различных моделей
`comment`	Комментарий
`tags`	Теги
`state`	Состояние устройства: `Clean` – пустое `Assigned` – назначено `Pending` – в ожидании `Issued` – выпущено `Disabled` – выключено `Revoked` – отозвано

Параметр	Описание
`contentExpirationStatus`	Информация об истечении срока действия сертификатов на устройстве: `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
`timeIssued`	Время выпуска устройства в формате ISO 8601. Например: 2024-12-03T11:22:20.1824104Z, 2024-12-03
`timeUpdated`	Время обновления устройства в формате ISO 8601
`timeRevoked`	Время отзыва устройства в формате ISO 8601
`offset`	Сдвиг на указанное количество устройств
`count`	Количество устройств, информация о которых передается в ответе

Возвращаемые значения

Параметр	Описание
`id`	Идентификатор устройства
`serialNumber`	Серийный номер устройства
`cardTypeName`	Название типа устройства
`cardModelName`	Название модели устройства. Указывается только для устройств Рутокен, JaCarta, eToken PRO Java 72K и IDPrime MD, если в разделе **Типы устройств** для данных устройств заданы отдельные настройки для различных моделей
`atr`	Answer To Reset устройства
`label`	Метка устройства
`comment`	Комментарий
`tags`	Теги
`state`	Состояние устройства
`formFactor`	Форм-фактор устройства
`pacNumber`	HID-метка устройства
`expirationDate`	Срок действия устройства
`timeIssued`	Время выпуска устройства
`timeDisabled`	Время выключения устройства
`timeUpdated`	Время обновления устройства
`timeRevoked`	Время отзыва устройства

Параметр	Описание
`userId`	Идентификатор пользователя, на которого назначено устройство
`userName`	Имя пользователя устройства в формате DOMAIN\LogonName или User Principal Name (UPN)
`policyId`	Идентификатор политики, действующей на устройство
`policyName`	Название политики, действующей на устройство
`certificates`	`type` – тип сертификата `serialNumber` – серийный номер сертификата `thumbprint` – отпечаток сертификата `subject` – общее имя (CN) субъекта сертификата `issuer` – общее имя (CN) издателя сертификата `validFrom`- дата начала срока действия сертификата в формате ISO 8601 `validTo` – дата окончания срока действия сертификата в формате ISO 8601

ПРИМЕР ЗАПРОСА

`http://localhost/cm/api/Cards` – вывод всех устройств

`http://localhost/cm/api/Cards?offset=0&count=50` – вывод 50 устройств без сдвига

`GET /Cards/{id}`

Возвращает информацию об устройстве по его идентификатору.

Параметры запроса: `id` – идентификатор устройства.

ПРИМЕР ЗАПРОСА

`http://localhost/cm/api/Cards/1`

`POST /Cards/{id}/Revoke`

Позволяет отозвать устройство.

Параметры запроса

Параметр	Обязательно/ необязательно	Описание
`id`	Обязательно	Идентификатор устройства
`reason`	Необязательно	Причина отзыва устройства: 0 – `--` – причина отзыва не указана 1 – CardBroken – устройство неисправно 2 – CardLost – устройство утеряно 3 – CardUpgrade – обновление устройства 4 – CardExpired – истечение срока действия устройства 4 – CardWithdraw – изъятие устройства 5 – UserRemoved – пользователь удален 6 – CardCompromised – компрометация устройства

ПРИМЕР ЗАПРОСА

`http://localhost/cm/api/cards/1/revoke`

`POST /Cards/{id}/Withdraw`

Позволяет изъять отозванное устройство. При изъятии устройство не очищается.

Чтобы изъять устройство, оно должно находиться в состоянии *Отозвано* (Revoked).

Параметры запроса

Параметр	Обязательно/ необязательно	Описание
`id`	Обязательно	Идентификатор устройства
`destructor`	Необязательно	Если в Indeed CM ведется учет СКЗИ, и устройство является СКЗИ, при изъятии можно указать ФИО сотрудников органа криптографической защиты, пользователей СКЗИ, производивших уничтожение/изъятие СКЗИ. Имена указываются в формате Common Name через запятую

ПРИМЕР ЗАПРОСА

`http://localhost/cm/api/cards/1/withdraw`

`POST /Cards/{id}/Disable`

Позволяет временно отключить устройство.

Параметры запроса: `id` – идентификатор устройства.

ПРИМЕР ЗАПРОСА

`http://localhost/cm/api/cards/1/disable`

`POST /Cards/{id}/Enable`

Позволяет включить устройство.

Параметры запроса: `id` – идентификатор устройства.

ПРИМЕР ЗАПРОСА

`http://localhost/cm/api/cards/1/enable`

`POST /Cards/{id}/Preupdate`

Позволяет отозвать неактуальный сертификат пользователя.

Параметры запроса: `id` – идентификатор устройства.

ПРИМЕР ЗАПРОСА

`http://localhost/cm/api/cards/1/preupdate`

ПРЕДУПРЕЖДЕНИЕ

Метод Preupdate можно использовать при изменении политики использования устройств. Если выпущенный сертификат не поддерживается в новой политике и в шаблоне сертификата в старой политике включена опция **Отзывать сертификат при отзыве/выключении устройства**, то сертификат отзывается.

Метод Preupdate нельзя выполнить для выключенного, назначенного, отозванного и ожидающего выпуск или обновление устройства.

СКЗИ

Для управления СКЗИ через API убедитесь, что в Мастере настройки в разделе **Журнал учета СКЗИ** включена опция **Вести журнал учета СКЗИ**.

При работе с СКЗИ через API вам доступны следующие операции:

- Получить список СКЗИ по заданным фильтрам
- Выполнить поиск СКЗИ по идентификатору
- Выполнить поиск СКЗИ по типу
- Добавить СКЗИ в Indeed CM
- Назначить СКЗИ на пользователя
- Изменить состояние СКЗИ
- Уничтожить/изъять СКЗИ

`GET /Skzi`

Возвращает список объектов `skzi record`.

Параметры запроса

Параметр	Обязательно/ необязательно	Описание
`objectType`	Необязательно	Тип объекта: `Distributive` – дистрибутив `License` – лицензия `Documentation` – документация `KeyDocument` – ключевой документ `Card` – ключевой носитель `Custom` – пользовательский
`skziTypeId`	Необязательно	Идентификатор типа СКЗИ
`serialNumber`	Необязательно	Серийный номер СКЗИ
`instanceNumber`	Необязательно	Номер экземпляра
`state`	Необязательно	Состояние: `Created` – изготовлено `Assigned` – назначено `Sent` – передано `Returned` – возвращено `Issued` – выдано `Installed` – установлено `Destructed/Withdrawn` – уничтожено/ изъято
`userName`	Необязательно	Имя пользователя в формате Common Name
`startDate`	Необязательно	Поиск СКЗИ с указанной даты
`endDate`	Необязательно	Поиск СКЗИ до указанной даты
`offset`	Необязательно	Сдвиг на указанное количество записей СКЗИ

Параметр	Обязательно/ необязательно	Описание
`count`	Необязательно	Количество СКЗИ для вывода в ответе

Возвращаемые значения

Параметр	Описание
`id`	Идентификатор СКЗИ
`timeCreated`	Время изготовления СКЗИ
`userId`	Идентификатор пользователя
`userName`	Имя пользователя в формате Common Name
`logonName`	Имя учетной записи пользователя в формате DOMAIN\LogonName
`objectType`	Тип объекта: `Distributive` – дистрибутив `License` – лицензия `Documentation` – документация `KeyDocument` – ключевой документ `Card` – ключевой носитель `Custom` – пользовательский
`skziTypeId`	Идентификатор типа СКЗИ
`serialNumber`	Серийный номер СКЗИ
`instanceNumber`	Номер экземпляра
`creationData`	Объект с информацией об изготовлении СКЗИ: `creator` – имя изготовителя `timeCreated` – время изготовления `docNumber` – номер документа об изготовлении

Параметр	Описание
`sendingData`	Объект с информацией о передаче СКЗИ: `docNumber` – номер сопроводительного письма `recipient` – ФИО сотрудника, который подтверждает получение СКЗИ `timeSent` – время передачи `timeConfirmed` – время подтверждения получения `confirmationDocNumber` – номер документа о подтверждении получения
`returnData`	Объект с информацией о возврате СКЗИ: `docNumber` – номер сопроводительного письма `timeReturned` – время возврата `timeConfirmed` – время подтверждения получения СКЗИ `confirmationDocNumber` – номер документа о подтверждении получения
`issueData`	Объект с информацией о выдаче СКЗИ: `docNumber` – номер сопроводительного письма `timeIssued` – время выдачи
`installationData`	Объект с информацией об установке СКЗИ: `docNumber` – номер документа об установке `installer` – ФИО сотрудников органа криптографической защиты, пользователей СКЗИ, производивших установку СКЗИ `timeInstalled` – время установки `hardwareId` – номер аппаратного средства, на котором установлено или к которому подключено СКЗИ `location` – место установки
`destructionData`	Объект с информацией об уничтожении/изъятии СКЗИ: `destructor` – ФИО сотрудников органа криптографической защиты, пользователей СКЗИ, производивших уничтожение/изъятие СКЗИ `timeDestructed` – время уничтожения/изъятия `docNumber` – номер акта или расписки об уничтожении
`comment`	Примечание

Параметр	Описание
`customFields`	Объект с информацией о дополнительных полях в журнале учета СКЗИ `id` – идентификатор атрибута, который подставляется в шаблоны печати нормативных документов `value` – имя поля, которое отображается в журнале СКЗИ Дополнительные поля задаются в Мастере настройки Indeed CM в разделе **Журнал учета СКЗИ**
`state`	Состояние СКЗИ: `Created` – изготовлено `Assigned` – назначено `Sent` – передано `Returned` – возвращено `Issued` – выдано `Installed` – установлено `Destructed/Withdrawn` – уничтожено/изъято

ПРИМЕР ЗАПРОСА

`http://localhost/cm/api/Object?type=Distributive&state=Installed&offset=0&count=5` – вывод 5 записей СКЗИ типа объекта Дистрибутив в состоянии `Installed` (установлено).

`POST /Skzi`

Позволяет добавить СКЗИ в Indeed CM.

Параметры запроса

Параметр	Обязательно/ необязательно	Описание
`objectType`	Обязательно	Тип объекта: `Distributive` – дистрибутив `License` – лицензия `Documentation` – документация `KeyDocument` – ключевой документ `Card` – ключевой носитель `Custom` – пользовательский
`skziTypeId`	Обязательно	Идентификатор типа СКЗИ
`serialNumber`	Обязательно	Серийный номер СКЗИ
`instanceNumber`	Необязательно	Номер экземпляра
`docNumber`	Необязательно	Номер документа, на основании которого добавляется СКЗИ. Если номер документа не указан, то номер генерируется по шаблону, настроенному для конкретного типа СКЗИ в разделе **Конфигурация** → **СКЗИ** → **Нормативные документы**
`creationDate`	Необязательно	Время создания документа. Указывается в формате yyyyMMddHHmmss (UTC). Если значение не указано, то подставляется текущее время

ПРИМЕР ТЕЛА ЗАПРОСА


```
{
  "objectType": "Distributive",
  "skziType": "3",
  "serialNumber": "0578393357",
  "instanceNumber": "4",
  "docNumber": "35",
  "creationDate": "2024-11-12T15:24:41.979Z"
}
```


`GET /Skzi/Types`

Возвращает список значений `skziType` – список типов СКЗИ.

Параметры запроса

Параметр	Обязательно/ необязательно	Описание
`skziTypeName`	Необязательно	Название типа СКЗИ.
`family`	Необязательно	Семейство СКЗИ: `Hardware` – аппаратный `Software` – программный `HardwareSoftware` – аппаратно-программный
`includeArchived`	Необязательно	`true` – включить в возвращаемые значения информацию об СКЗИ архивных типов `false` – не включать в возвращаемые значения информацию об СКЗИ архивных типов Значение по умолчанию – `false`

Возвращаемые значения

Параметр	Описание
`id`	Идентификатор СКЗИ.
`skziTypeName`	Название типа СКЗИ.
`family`	Семейство СКЗИ: `Hardware` – аппаратный `Software` – программный `HardwareSoftware` – аппаратно-программный
`conformityCertificate`	Информация о сертификате соответствия на СКЗИ: `number` – номер `issueDate` – дата выдачи `notAfter` – дата окончания срока действия
`supportCertificate`	Информация о сертификате технической поддержки: `number` – номер `issueDate` – дата выдачи `notAfter` – дата окончания срока действия
`cardTypeName`	Название типа устройства. Параметр отображается только для СКЗИ аппаратных типов
`cardTypeModel`	Название модели устройства. Параметр отображается только для устройств Рутокен и JaCarta, если в разделе **Типы СКЗИ** настроены типы СКЗИ для различных моделей
`isDefault`	`true` – тип СКЗИ, используемый по умолчанию (для программных СКЗИ) `false` – тип СКЗИ, не используемый по умолчанию
`isArchived`	`true` – архивный тип СКЗИ `false` – действующий тип СКЗИ

ПРИМЕР ЗАПРОСА

`http://localhost/cm/api/Skzi/Types?skziTypeName=JaCarta%20PKI&family=Hardware&includeArchived=false` – вывод списка действующих СКЗИ аппаратного типа JaCarta PKI.

`GET /Skzi/{id}`

Возвращает объект `skzi record` по его идентификатору.

Параметры запроса: `id` – идентификатор СКЗИ.

Возвращаемые значения

Параметр	Описание
`id`	Идентификатор СКЗИ
`timeCreated`	Время изготовления СКЗИ
`userId`	Идентификатор пользователя
`userName`	Имя пользователя в формате Common Name
`logonName`	Имя учетной записи пользователя
`objectType`	Тип объекта: `Distributive` – дистрибутив `License` – лицензия `Documentation` – документация `KeyDocument` – ключевой документ `Card` – ключевой носитель `Custom` – пользовательский
`skziTypeId`	Идентификатор типа СКЗИ
`serialNumber`	Серийный номер СКЗИ
`instanceNumber`	Номер экземпляра
`creationData`	Объект с информацией об изготовлении СКЗИ: `creator` – имя изготовителя `timeCreated` – время изготовления `docNumber` – номер документа об изготовлении

Параметр	Описание
`sendingData`	Объект с информацией о передаче СКЗИ: `docNumber` – номер сопроводительного письма `recipient` – ФИО сотрудника, который подтверждает получение СКЗИ `timeSent` – время передачи `timeConfirmed` – время подтверждения получения `confirmationDocNumber` – номер документа о подтверждении получения
`returnData`	Объект с информацией о возврате СКЗИ: `docNumber` – номер сопроводительного письма `timeReturned` – время возврата `timeConfirmed` – время подтверждения получения СКЗИ `confirmationDocNumber` – номер документа о подтверждении получения
`issueData`	Объект с информацией о выдаче СКЗИ: `docNumber` – номер сопроводительного письма `timeIssued` – время выдачи
`installationData`	Объект с информацией об установке СКЗИ: `docNumber` – номер документа об установке `installer` – ФИО сотрудников органа криптографической защиты, пользователей СКЗИ, производивших установку СКЗИ `timeInstalled` – время установки `hardwareId` – номер аппаратного средства, на котором установлено или к которому подключено СКЗИ `location` – место установки
`destructionData`	Объект с информацией об уничтожении/изъятии СКЗИ: `destructor` – ФИО сотрудников органа криптографической защиты, пользователей СКЗИ, производивших уничтожение/изъятие СКЗИ `timeDestructed` – время уничтожения/изъятия `docNumber` – номер акта или расписки об уничтожении
`comment`	Примечание

Параметр	Описание
`customFields`	Объект с информацией о дополнительных полях в журнале учета СКЗИ: `id` – идентификатор атрибута, который подставляется в шаблоны печати нормативных документов `value` – имя поля, которое отображается в журнале СКЗИ Дополнительные поля задаются в Мастере настройки Indeed CM в разделе **Журнал учета СКЗИ**
`state`	Состояние СКЗИ: `Created` – изготовлено `Assigned` – назначено `Sent` – передано `Returned` – возвращено `Issued` – выдано `Installed` – установлено `Destructed/Withdrawn` – уничтожено/изъято

ПРИМЕР ЗАПРОСА

`http://localhost/cm/api/Skzi/1` – вывод записи СКЗИ с идентификатором 1.

`PUT /Skzi/{id}/Assign`

Позволяет назначить СКЗИ на пользователя.

Параметры запроса

Параметр	Описание
`id`	Идентификатор СКЗИ
`userName`	Имя пользователя в формате Common Name или имя учетной записи пользователя в формате DOMAIN\LogonName или User Principal Name (UPN)

ПРИМЕР ЗАПРОСА

`http://localhost/cm/api/Skzi/8/assign?userName=evgeniy.belov%40demo.com` – назначить СКЗИ с идентификатором 8 на пользователя evgeniy.belov@demo.com.

`PUT /Skzi/{id}`

Позволяет перевести СКЗИ из текущего состояния в следующие состояния по жизненному циклу. Перед изменением состояния СКЗИ рекомендуем назначить СКЗИ на пользователя.

СКЗИ может находиться в следующих состояниях: `Created` (изготовлено), `Assigned` (назначено), `Sent` (передано), `Returned` (возвращено), `Issued` (выдано), `Installed` (установлено), `Destructed/Withdrawn` (уничтожено/изъято).

Возможности изменения состояний СКЗИ:

- `Created` или `Assigned` можно перевести в `Sent`, `Returned`, `Issued`, `Installed`
- `Sent` можно перевести в `Returned`, `Issued`, `Installed`
- `Returned` можно перевести в `Issued`, `Installed`
- `Issued` можно перевести в `Installed`

СКЗИ в состоянии `Destructed/Withdrawn` нельзя перевести в другое состояние – оно завершает свой жизненный цикл. СКЗИ в состоянии `Installed` можно только уничтожить/изъять.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Состояние `Sent` должно передаваться во всех запросах на изменение состояния СКЗИ. Например, нельзя перевести СКЗИ из состояния `Created` в `Installed`, если в теле запроса нет параметра `sendingData`.

Параметры тела запроса

Объект	Параметр	Описание
`id`		Идентификатор СКЗИ
`sendingData` информация о передаче СКЗИ	`recipient`	ФИО сотрудника, который подтверждает получение СКЗИ
	`timeSent`	Время отправления документа. Указывается в формате yyyyMMddHHmmss (UTC). Если значение не указано, то подставляется текущее время
	`timeConfirmed`	Время подтверждения получения. Указывается в формате yyyyMMddHHmmss (UTC). Если значение не указано, то подставляется текущее время
	`confirm`	Укажите значение: `true`, чтобы сформировать документ, подтверждающий получение СКЗИ `false`, чтобы документ, подтверждающий получение СКЗИ, не формировался
	`confirmationDocNumber`	Номер документа о подтверждении получения СКЗИ. Если номер документа не указан, то номер генерируется по шаблону, настроенному для конкретного типа СКЗИ в разделе **Конфигурация → СКЗИ → Нормативные документы**

Объект	Параметр	Описание
`returnData` – информация о возврате СКЗИ	`timeReturned`	Время возврата СКЗИ. Указывается в формате yyyyMMddHHmmss (UTC). Если значение не указано, то подставляется текущее время
	`timeConfirmed`	Время подтверждения получения СКЗИ. Указывается в формате yyyyMMddHHmmss (UTC). Если значение не указано, то подставляется текущее время
	`confirm`	Укажите значение: `true`, чтобы сформировать документ о подтверждении получения СКЗИ `false`, чтобы не формировать документ о подтверждении получения СКЗИ
	`confirmationDocNumber`	Номер документа о подтверждении получения СКЗИ. Если номер документа не указан, то номер генерируется по шаблону, настроенному для конкретного типа СКЗИ в разделе **Конфигурация → СКЗИ → Нормативные документы**
`issueData` – информация о выдаче СКЗИ	`timeIssued`	Время выдачи СКЗИ. Указывается в формате yyyyMMddHHmmss (UTC). Если значение не указано, то подставляется текущее время

Объект	Параметр	Описание
`installationData` — информация об установке СКЗИ	`installer`	ФИО сотрудников органа криптографической защиты, пользователей СКЗИ, производивших установку СКЗИ. Имена указываются в формате Common Name через запятую
	`timeInstalled`	Время установки СКЗИ. Указывается в формате yyyyMMddHHmmss (UTC). Если значение не указано, то подставляется текущее время
	`hardwareId`	Номер аппаратного средства, на котором установлено или к которому подключено СКЗИ
	`location`	Место установки СКЗИ
`comment`		Примечание
`customFields`	`id`	Идентификатор атрибута, который подставляется в шаблоны печати нормативных документов
	`value`	Отображаемое имя поля в журнале СКЗИ

Пример тела запроса для перевода СКЗИ из Created в Installed

```
{
  "sendingData": {
    "recipient": "evgeniy.belov@demo.com",
    "timeSent": "2024-11-11T14:24:16.641Z",
    "timeConfirmed": "2024-11-11T14:24:16.641Z",
    "confirm": true,
    "confirmationDocNumber": "3"
},
  "installationData": {
    "installer": "Никифорова Ольга Петровна",
    "timeInstalled": "2024-11-11T14:24:16.641Z",
    "hardwareId": "PF3N9LFM",
    "location": "г. Москва, ул. Примерная, д. 9, каб. 368"
  },
}
```

В примере тела запроса для перевода СКЗИ из состояния `Created` в `Installed` пропущены состояния `Returned` и `Issued`. Чтобы внести информацию об СКЗИ в состояниях `Returned` и `Issued`, пропишите значения параметров `returnData` и `issueData` в теле запроса:

```
  "sendingData": {
    "recipient": "evgeniy.belov@demo.com",
    "timeSent": "2024-11-11T14:24:16.641Z",
    "timeConfirmed": "2024-11-11T14:24:16.641Z",
    "confirm": true,
    "confirmationDocNumber": "4"
  },
  "returnData": {
    "timeReturned": "2024-12-04T16:11:05.247Z",
    "timeConfirmed": "2024-12-04T16:11:05.247Z",
    "confirm": true,
    "confirmationDocNumber": "5"
  },
  "issueData": {
    "timeIssued": "2024-12-04T16:11:05.247Z"
  },
  "installationData": {
    "installer": "Никифорова Ольга Петровна",
    "timeInstalled": "2024-11-11T14:24:16.641Z",
    "hardwareId": "PF3N9LFM",
    "location": "г. Москва, ул. Примерная, д. 9, каб. 368"
  }
```

`DELETE /Skzi/{id}`

Позволяет уничтожить/изъять СКЗИ.

Параметры запроса

Параметр	Обязательно/ необязательно	Значение
`id`	Обязательно	Идентификатор СКЗИ
`reuse`	Необязательно	Укажите значение: `true`, чтобы изъять СКЗИ у пользователя и использовать повторно – например, для другого пользователя `false`, чтобы уничтожить СКЗИ Значение по умолчанию – `false`
`destructor`	Необязательно	ФИО сотрудников органа криптографической защиты, пользователей СКЗИ, производивших уничтожение/изъятие СКЗИ. Имена указываются в формате Common Name через запятую
`timeDestructed`	Необязательно	Время уничтожения/изъятия. Указывается в формате yyyyMMddHHmmss (UTC). Если значение не указано, то подставляется текущее время

ПРИМЕР ЗАПРОСА

`http://localhost/cm/api/Skzi/5?reuse=false&destructor=evgeniy.belov%40demo.com` – уничтожить СКЗИ с идентификатором 5. Пользователь, производивший уничтожение – evgeniy.belov@demo.com.

Дополнительные инструкции

Рутокен БИО

Биометрическая защита сертификатов

JaCarta ГОСТ

Особенности использования

Indeed CM Card Template Designer

Утилита для создания шаблонов печати

Массовый выпуск смарт-карт

Режим массового выпуска

Рутокен БИО

Indeed CM позволяет управлять устройствами Рутокен ЭЦП 3.0 3250 БИО (Рутокен БИО) — ключевыми носителями с поддержкой биометрической защиты сертификатов. Чтобы сертификатом нельзя было воспользоваться в случае компрометации PIN-кода, контейнер закрытого ключа можно дополнительно защитить биометрией пользователя. Для доступа к закрытому ключу пользователь вводит PIN-код и проходит аутентификацию по отпечатку пальца.

Биометрическая аутентификация подтверждает выполнение операций с сертификатом — выпуск, обновление и удаление сертификата, а также подпись документов.

Предварительные настройки

Биометрическая защита в шаблоне сертификата

Биометрическая защита настраивается в шаблонах сертификатов используемого УЦ с помощью опции **Защищать ключ биометрией, если поддерживается**.

> **ПРИМЕЧАНИЕ**
>
> Биометрическая защита поддерживается для всех сертификатов, кроме ГОСТ-сертификатов с контейнером закрытого ключа, сгенерированным через КриптоПро CSP.

Наличие биометрии на устройстве

Чтобы записать на устройство сертификат с биометрической защитой, необходимо предварительно зарегистрировать на устройстве биометрические данные пользователя одним из способов:

- При выпуске устройства Рутокен БИО в Консоли управления
- Через стороннее ПО производителя устройства («Рутокен БИО. Программа администрирования»)

Привилегии

Действия с биометрией доступны членам роли со следующими привилегиями:

- *Регистрация биометрии* — регистрация отпечатков при выпуске устройства
- *Обновление биометрии* — замена зарегистрированных отпечатков
- *Разблокировка биометрии* — сброс блокировки биометрической аутентификации

Привилегии настраиваются в разделе **Конфигурация** → **Роли**.

Биометрическая аутентификация

Биометрическая аутентификация — дополнительный фактор доступа к защищенному биометрией контейнеру закрытого ключа. После ввода PIN-кода пользователь прикладывает палец к сканеру отпечатков, и Indeed CM сверяет отпечаток с зарегистрированной на устройстве биометрией.

Биометрическая аутентификация блокируется, если пользователь не прошел проверку отпечатка пальца пять раз подряд. Операции с защищенным сертификатом становятся доступны снова после разблокировки биометрии.

Особенности операций с устройствами Рутокен БИО

Операция	Особенности
Выпуск устройства	Пользователь проходит биометрическую аутентификацию, чтобы получить доступ к контейнеру закрытого ключа и подтвердить выпуск сертификата, защищенного биометрией. Если биометрия еще не зарегистрирована, перед аутентификацией открывается окно регистрации биометрии.
Обновление устройства	Пользователь проходит биометрическую аутентификацию, чтобы подтвердить выпуск или удаление сертификата, защищенного биометрией. Окно аутентификации может открываться несколько раз — например, при создании нового защищенного контейнера и удалении старого. Биометрическая аутентификация не требуется, если сертификат не удаляется при обновлении устройства (в параметрах шаблона сертификата включена опция **Не удалять сертификат при обновлении/очистке устройства**). Опция **Обновить устройство на агенте** недоступна.

Операция	Особенности
Отмена обновления	Пользователь проходит биометрическую аутентификацию, чтобы подтвердить удаление контейнера закрытого ключа сертификата, созданного при обновлении. Опция **Отменить обновление на агенте** недоступна.
Отзыв устройства	При отзыве с очисткой устройства, подключенного к рабочей станции, пользователь проходит биометрическую аутентификацию, чтобы подтвердить удаление сертификата. Биометрические данные остаются на устройстве. При отзыве с инициализацией подтверждение не требуется — с устройства удаляются все данные, включая биометрию. При отзыве с помощью агента доступна только инициализация: с устройства удаляются все данные, включая биометрию. Опция **Очистить устройство на агенте** недоступна.
Изъятие устройства	При изъятии с очисткой пользователь проходит биометрическую аутентификацию, чтобы подтвердить удаление сертификата, защищенного биометрией. Подтверждение не нужно, если в параметрах шаблона сертификата включена опция **Не удалять сертификат при обновлении/очистке устройства**. При очистке биометрические данные пользователя сохраняются, при инициализации — удаляются вместе со всеми данными.
Подпись документа	Пользователь проходит биометрическую аутентификацию, чтобы подтвердить подпись документа сертификатом, защищенным биометрией.

Операции с биометрией

Регистрация

Регистрация биометрии выполняется в Консоли управления во время выпуска устройства Рутокен БИО при личном присутствии пользователя. Действие доступно членам роли с привилегией *Регистрация биометрии*.

Регистрация биометрии доступна, если выполнены следующие условия:

- На устройстве еще нет биометрических данных пользователя.
- В шаблоне сертификата включена опция **Защищать ключ биометрией, если поддерживается**.

Чтобы зарегистрировать биометрию:

1. Начните процесс выпуска устройства.
   Подробнее о процессе выпуска устройств
2. Подключите к рабочей станции устройство Рутокен БИО и сканер отпечатков пальцев.
3. Нажмите **Выпустить**. Откроется окно регистрации биометрии.
4. Пользователь регистрирует от одного до трех отпечатков пальцев, последовательно прикладывая пальцы к сканеру.
5. После регистрации биометрии пользователь должен подтвердить выпуск устройства — снова приложить палец к сканеру.
6. Когда выпуск устройства завершится, нажмите **Закрыть**.

Обновление

Зарегистрированные на устройстве отпечатки можно обновить в Консоли управления при личном присутствии пользователя. Действие доступно членам роли с привилегией *Обновление биометрии*.

Чтобы обновить биометрию:

1. В карточке устройства выберите действие **Обновить биометрию**.
2. Подключите к рабочей станции устройство Рутокен БИО и сканер отпечатков пальцев.
3. Нажмите **Обновить**. Откроется окно биометрической аутентификации.
4. Пользователь прикладывает палец к сканеру, чтобы подтвердить обновление биометрии.
5. В окне обновления биометрии пользователь регистрирует от одного до трех отпечатков пальцев, последовательно прикладывая пальцы к сканеру.
6. Нажмите **Продолжить**.
7. Когда обновление биометрии завершится, нажмите **Закрыть**.

Разблокировка

Биометрическая аутентификация блокируется, если пользователь не прошел проверку отпечатка пальца пять раз подряд. Вы можете разблокировать биометрию, счетчик попыток аутентификации при этом сбрасывается. Действие доступно членам роли с привилегией *Разблокировка биометрии*.

Чтобы разблокировать биометрию:

1. В карточке устройства выберите действие **Разблокировать биометрию**.
2. Подключите устройство к рабочей станции и нажмите **Разблокировать**.
   Если устройство недоступно, создайте задачу для агента, установленного на рабочей станции пользователя:
   1. Включите опцию **Разблокировать биометрию на агенте**.
   2. (Опционально) Заполните поле **Комментарий**.
   3. Нажмите **Разблокировать**.

      Биометрия разблокируется автоматически, как только пользователь подключит устройство к рабочей станции с агентом.

Сообщение пользователю

Вы можете настроить сообщение, которое увидит пользователь, когда подключит устройство Рутокен БИО к рабочей станции с агентом после разблокировки биометрии. Чтобы настроить сообщение:

1. В разделе **Конфигурация** перейдите в настройки политики.
2. Перейдите в раздел **Агенты** → **Сообщения пользователю**.
3. В поле **Разблокировка биометрической аутентификации на устройстве** введите текст сообщения.
4. Нажмите **Сохранить**.

События и уведомления

Все операции с устройствами Рутокен БИО фиксируются в журнале событий.

Для администраторов и пользователей вы можете дополнительно настроить уведомления о регистрации, обновлении и разблокировке биометрии. Уведомления настраиваются в политике в разделе **Уведомления**.

JaCarta ГОСТ

В разделе описаны особенности работы с моделями устройств JaCarta, на которых установлено приложение ГОСТ (апплет). К таким устройствам относятся:

- JaCarta PKI/ГОСТ
- JaCarta PKI/ГОСТ/Flash
- JaCarta-2 PKI/ГОСТ
- JaCarta-2 SE
- JaCarta-3 PKI/ГОСТ
- JaCarta-3 SE

Приложение ГОСТ используется для хранения ключей и сертификатов, соответствующих российским криптографическим стандартам. При управлении такими устройствами через Indeed Certificate Manager необходимо учитывать особенности настройки PIN-кодов, инициализации и операций с устройствами.

Особенности

- После добавления устройства в Indeed Certificate Manager PIN-код администратора для приложения ГОСТ, установленный по умолчанию, меняется на случайный. Когда устройство удаляется из Indeed CM с подключением к рабочей станции, случайный PIN-код администратора меняется на значение, указанное в разделе **Конфигурация** → Типы устройств.
- PIN-код пользователя для приложения ГОСТ можно установить и изменить только при инициализации устройства, после того как устройство было выпущено.
- При изъятии устройства с подключением к рабочей станции нужно ввести PIN-код пользователя для приложения ГОСТ. Если PIN-код пользователя неизвестен, то устройство изымается без подключения к рабочей станции. Чтобы выпустить это устройство повторно, его нужно инициализировать. При инициализации устанавливается новый PIN-код пользователя для приложения ГОСТ, известный пользователю и/или оператору.
- При разблокировке приложения ГОСТ PIN-код пользователя не меняется. Устанавливается 10 попыток ввода PIN-кода до блокировки устройства.

Настройки PIN-кода пользователя в политиках

При работе с PIN-кодом пользователя для приложения ГОСТ в политиках Indeed CM (раздел Выпуск) учитывайте следующие особенности:

Доступно:

- Опция **Установить случайный PIN-код пользователя** (устанавливается одинаковый случайный PIN-код для приложений PKI и ГОСТ)
- Опция **Блокировать устройство**
- Установка PIN-кода в параметрах инициализации устройства

Недоступно:

- Опция **Пользователь должен поменять PIN-код при первом входе**
- Настройки парольной политики в параметрах инициализации устройства

Настройки PIN-кодов в типе устройства

В разделе **Конфигурация** → Типы устройств вы можете просмотреть PIN-коды администратора и пользователя, установленные по умолчанию, и настроить новые PIN-коды в соответствии с политиками безопасности, принятыми в вашей организации.

Значения PIN-кодов по умолчанию различаются в зависимости от версии приложения ГОСТ.

Версия приложения ГОСТ	PIN-код пользователя	PIN-код администратора	PUK-код
2.5.3 – 2.5.9 (Криптотокен 2 ЭП)	1234567890	—	0987654321
2.5.13 и выше (ВПО JaCarta-3)	1234567890	0987654321	—

⚠ **ПРЕДУПРЕЖДЕНИЕ**

Обратите внимание, что на моделях устройств JaCarta с версией приложения ГОСТ 2.5.3 – 2.5.9 (Криптотокен 2 ЭП) могут быть установлены PIN-коды «наоборот»:

- PIN-код пользователя: 0987654321
- PIN-код администратора: 1234567890

Версию приложения ГОСТ можно узнать в ПК «Единый клиент JaCarta».

Indeed CM Card Template Designer

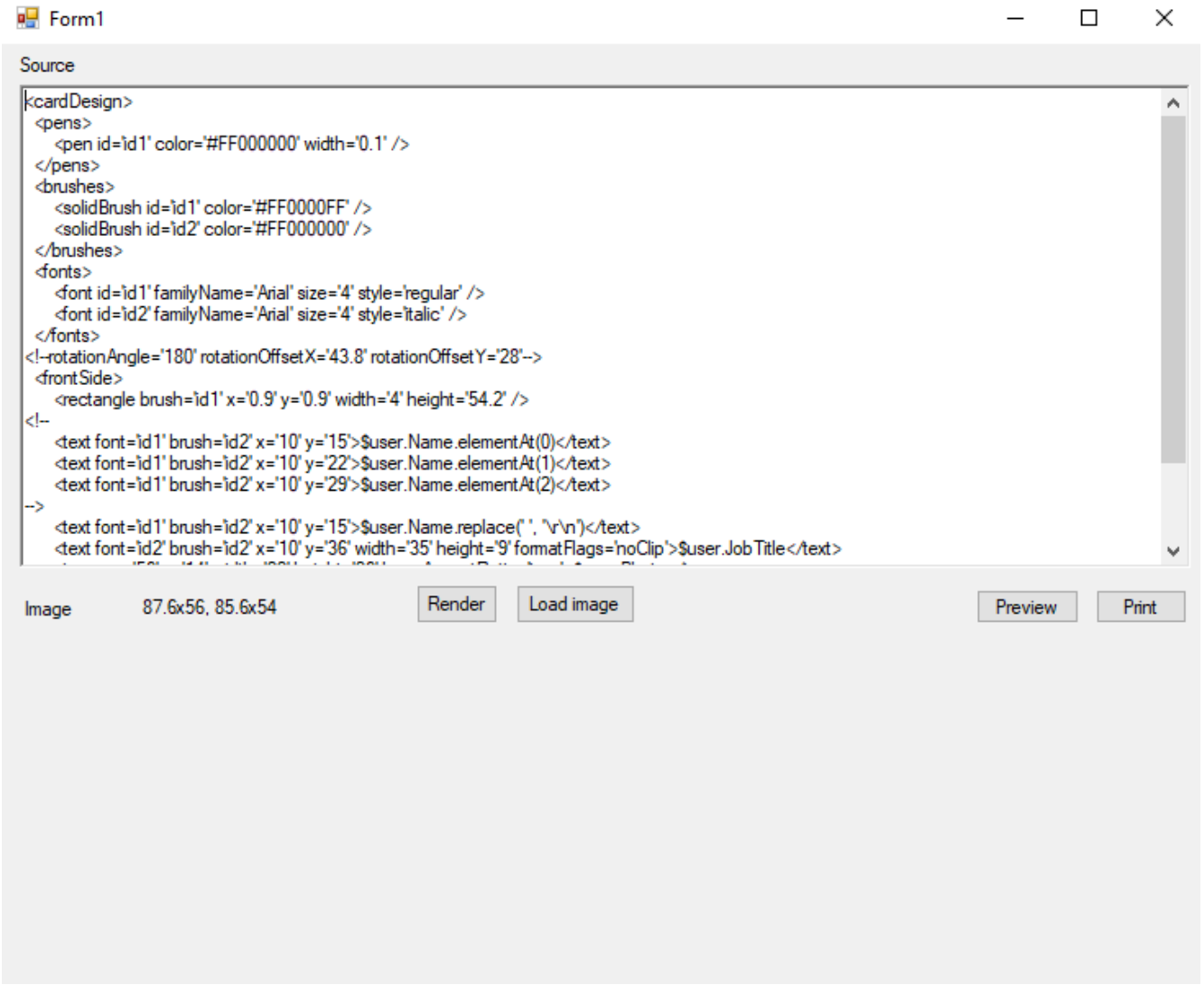
Утилита Indeed CM Card Template Designer позволяет создавать шаблоны печати на смарт-картах, которые используются с принтером **EDIsecure XID 8100\8300**.

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

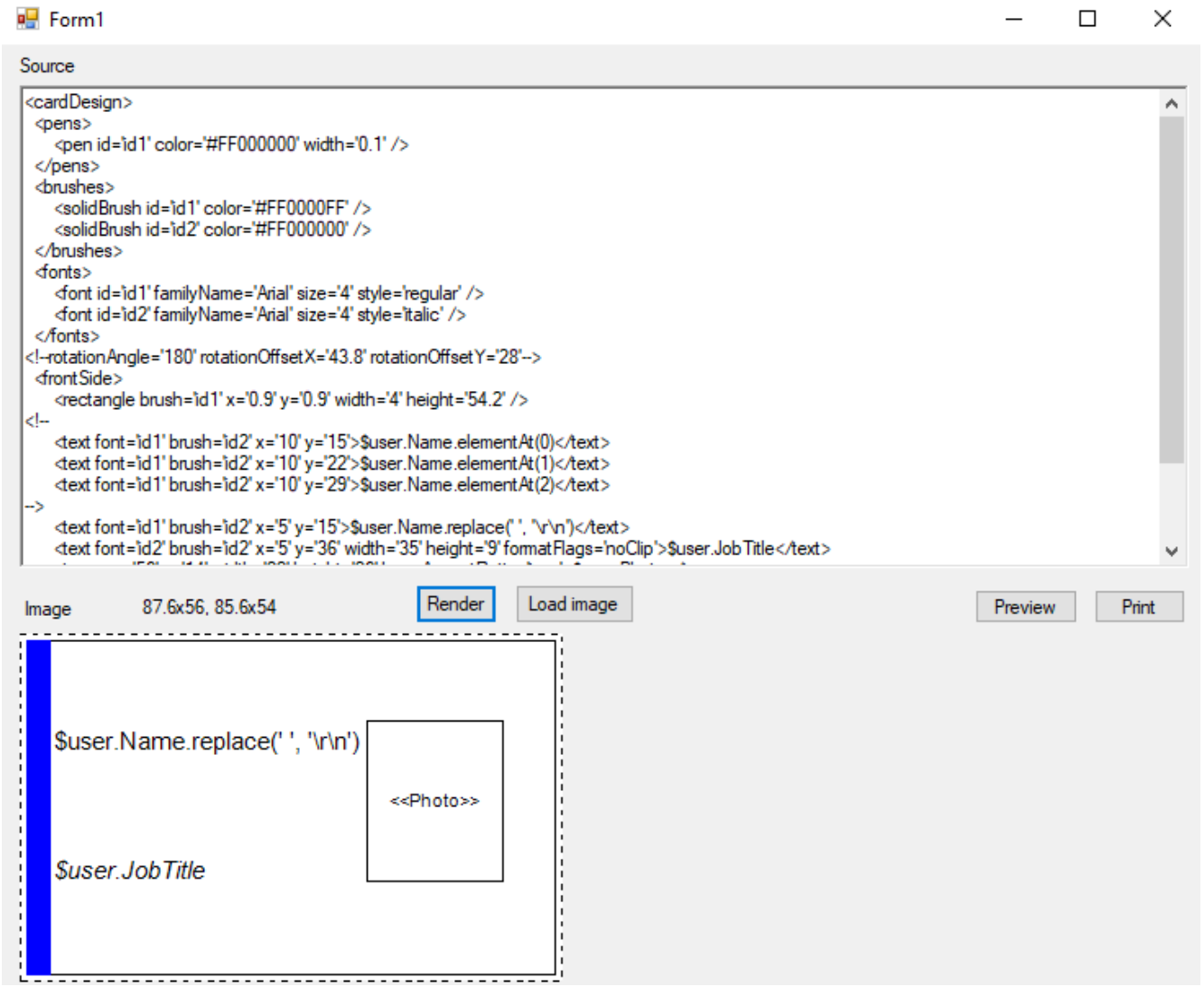
Утилиту Card Template Designer предоставляет по запросу служба технической поддержки компании Индид.

Запустите приложение *cardTemplateDesigner.exe* из дистрибутива Indeed CM. 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)

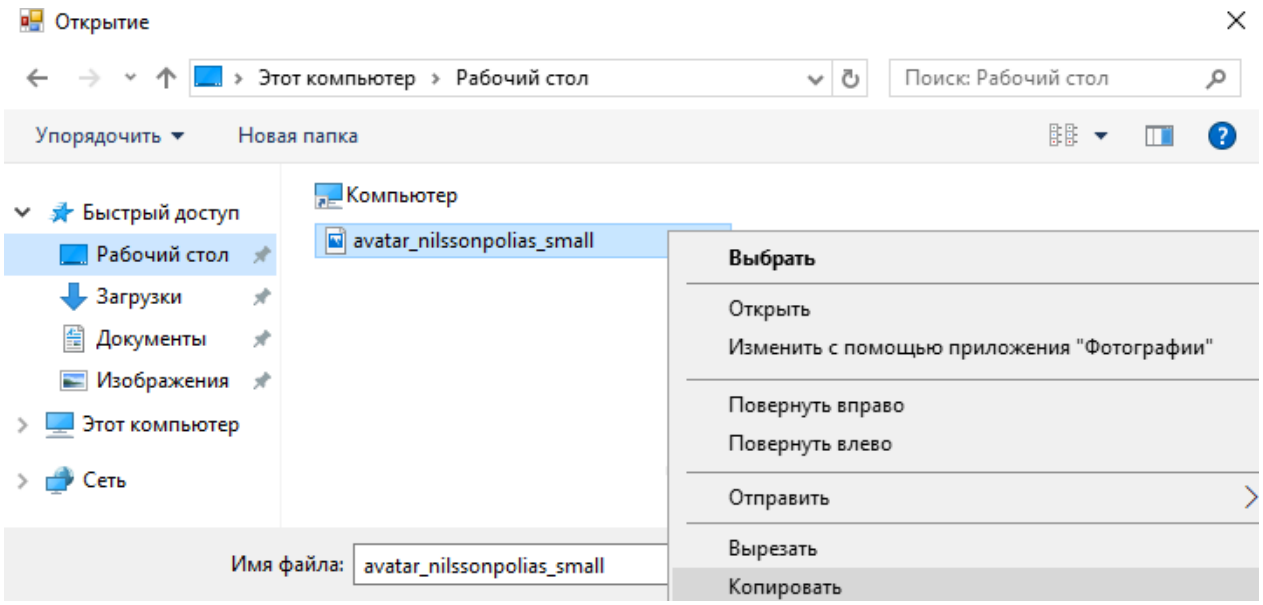
- **Изображение**. Задается в секции `<image>` с параметрами:
  - x
  - y
  - widht (опциональный)
  - heigth (опциональный)
  - keepAspectRatio (true или false)
  - data (опциональный)

ПРИМЕР

<image x='56' y='14' width='22' height='26'
keepAspectRatio='true'>$user.Photo</image>

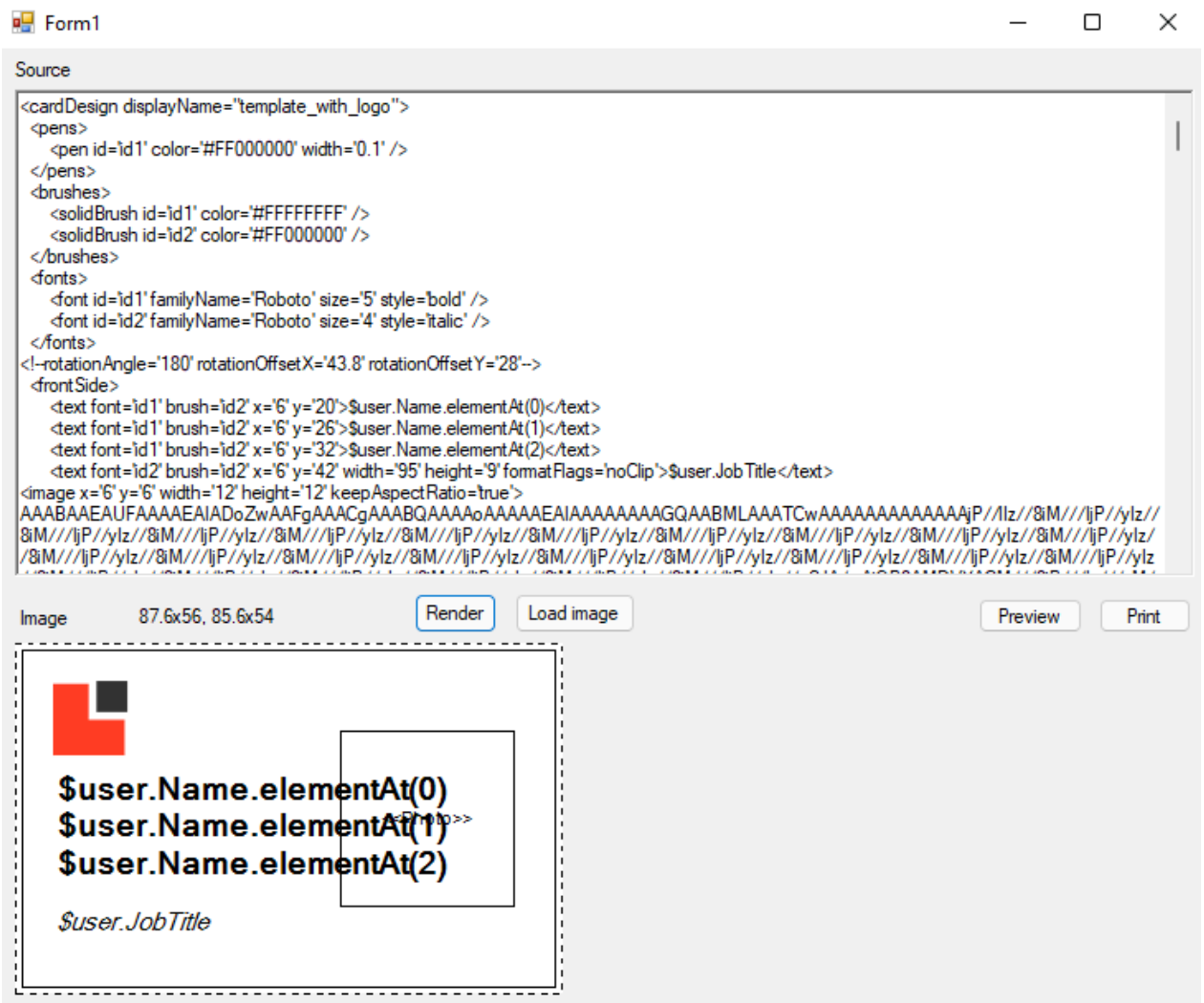
Описанная строка определяет положение, размер и следование пропорциям изображения, подставляемого из атрибута Active Directory (переменная `$user.Photo`). Помимо переменной можно подставить и изображение в кодировке base64 (например, для добавления в шаблон логотипа компании) и затем визуализировать 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.

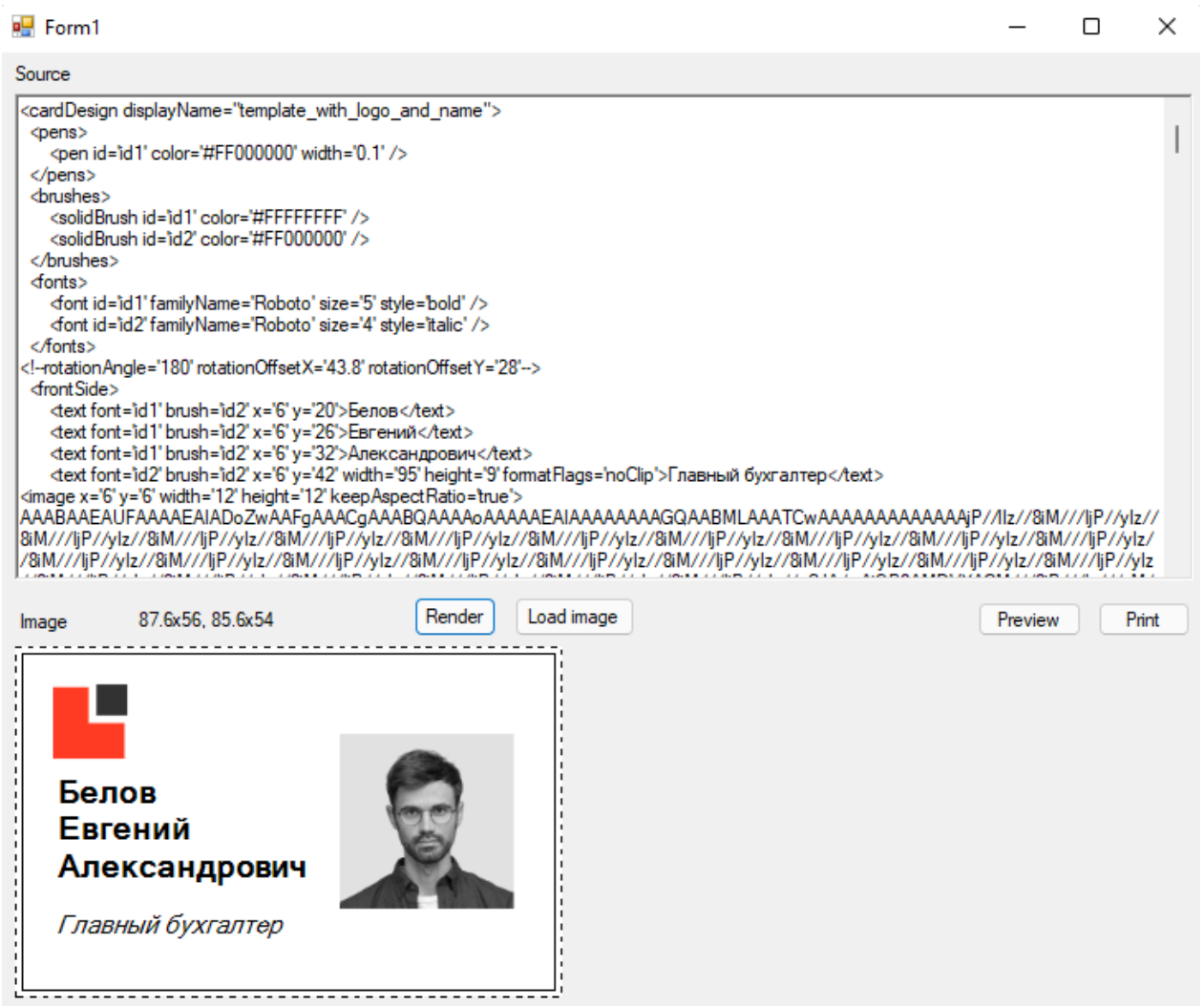


Ниже на рисунке приведен пример шаблона со статическим логотипом компании и подстановкой данных пользователя из Active Directory:

- 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`.

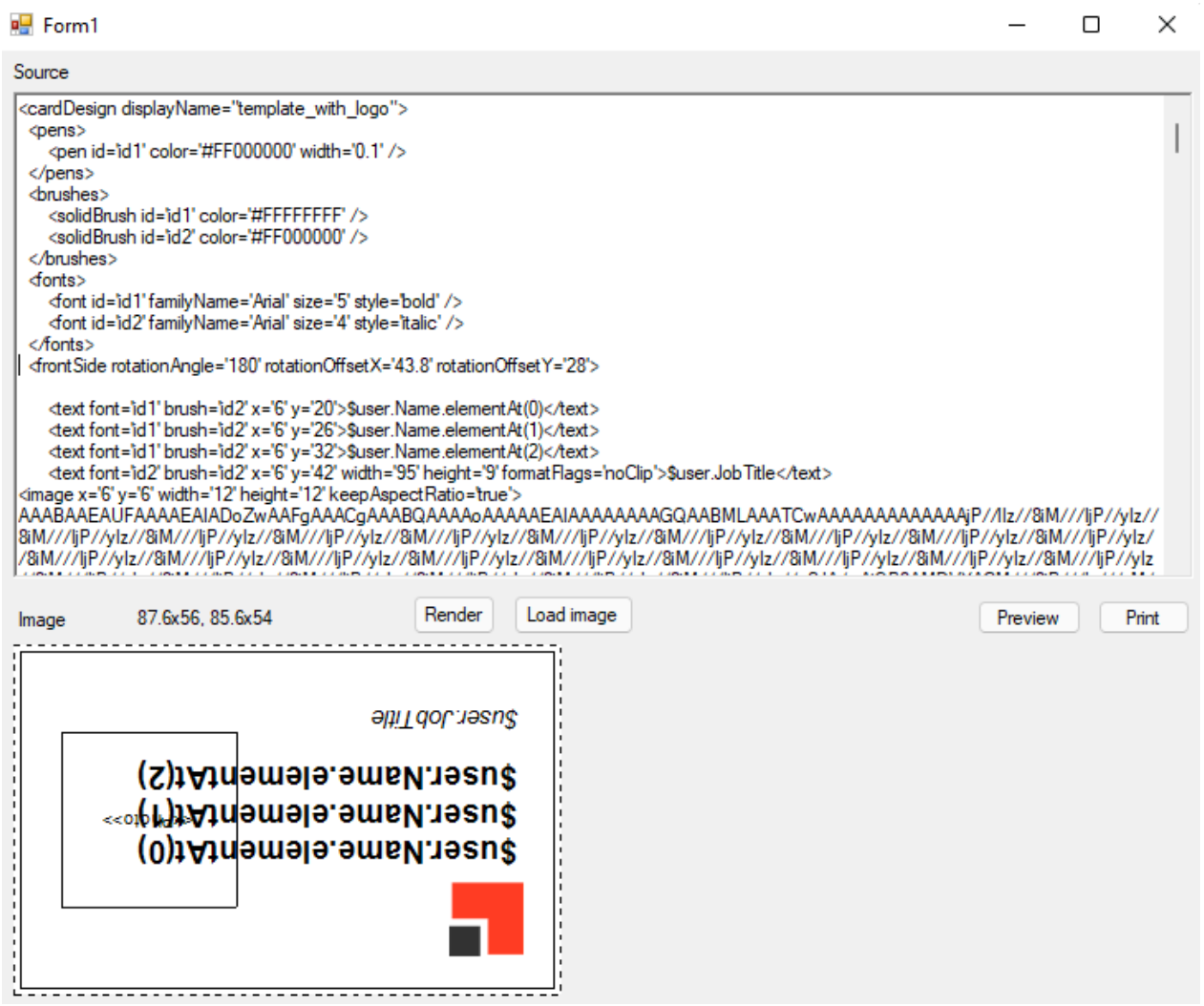
ПРИМЕР:

<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% 

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.

Возможности и ограничения

- Нельзя выбирать необязательные сертификаты. Выпускаются только обязательные сертификаты. Необязательные сертификаты можно выпустить для каждого пользователя отдельно через карточку пользователя или в Сервисе самообслуживания.
- Нельзя указать имя карты. Имя не заполняется или формируется по правилам, настроенным в политике использования устройств.
- Нельзя автоматически создать документ учета СКЗИ. Документ можно добавить вручную в карточке пользователя.
- При возникновении любой ошибки массовый выпуск останавливается. Для дальнейшей работы устраните ошибку или исключите проблемного пользователя из списка и запустите массовый выпуск заново.
- Если нажать **Отмена** во время массового выпуска, выпустится карта, загруженная в принтер карта. Следующая карта не выпустится.
- При массовом выпуске можно напечатать данные на карте.

Печать на смарт-картах

Для печати на смарт-картах на рабочей станции должны быть установлены следующие компоненты:

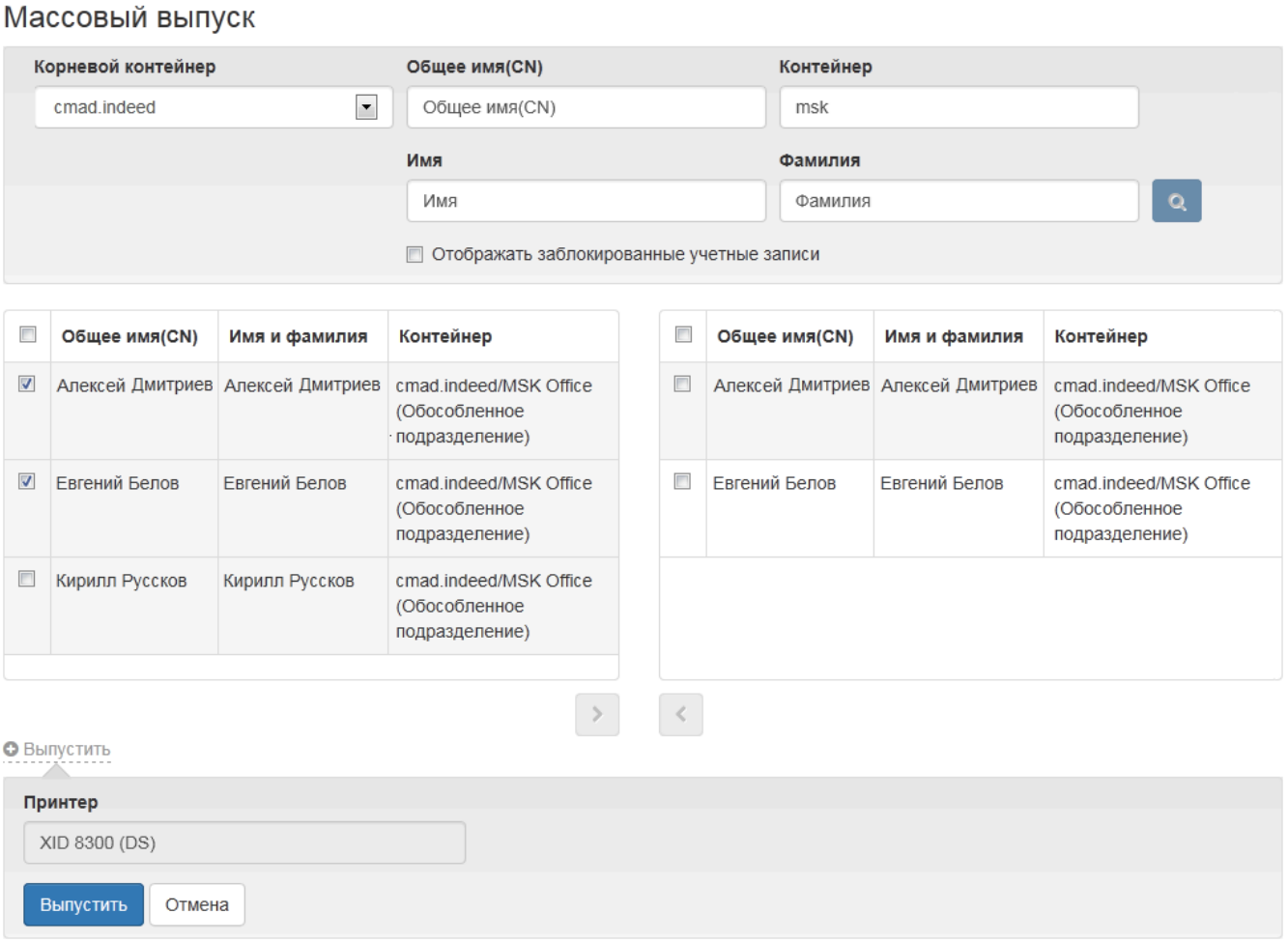
- Драйверы принтера EDISecure XID8300
- Настроенное соединение с принтером в утилите EDI Secure Connect
- Компонент поддержки принтера **IndeedCM.EdiSecure.Middleware**
- Подключенный через интерфейс USB принтера XID8300

Драйверы принтера EDISecure XID8300 и утилита EDI Secure Connect поставляются производителем вместе с принтером. IndeedCM.EdiSecure.Middleware поставляется в составе дистрибутива Indeed CM.

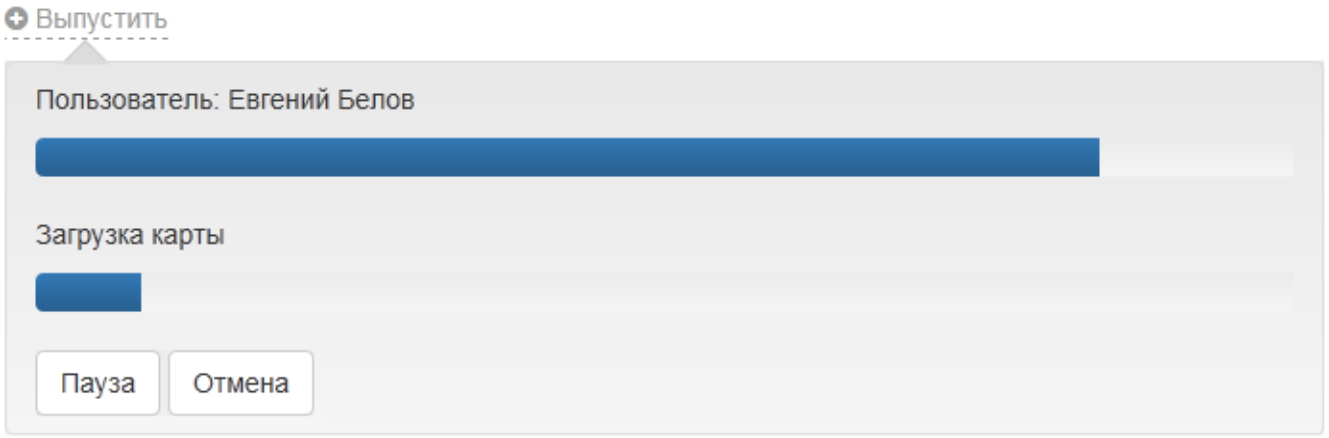
Процесс

Чтобы массово выпустить устройства:

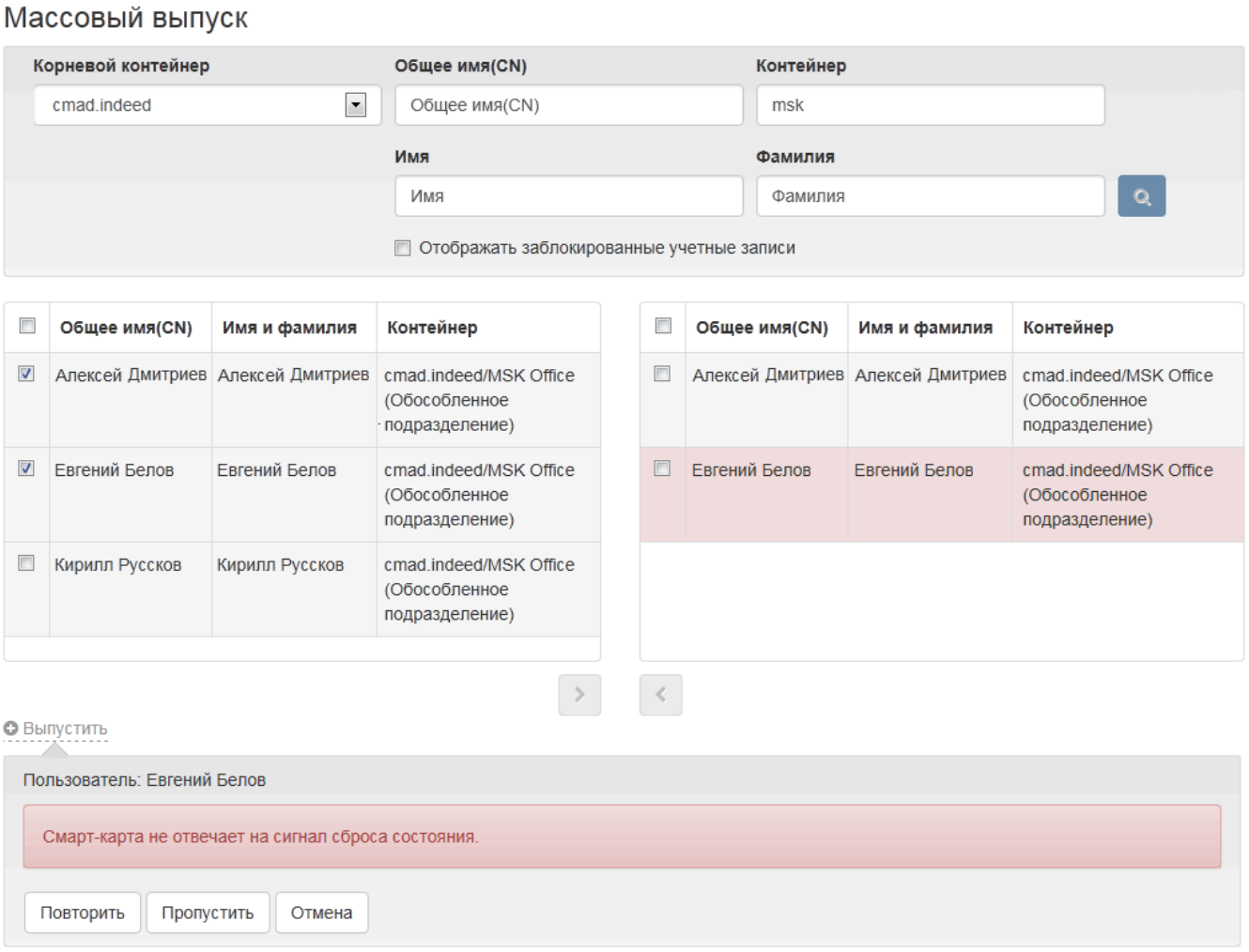
1. Перейдите на страницу сервиса *https://<FQDN сервера Indeed CM>/cm/mc/bulkissue*.
2. Выполните поиск пользователей (например, по месту расположения). Результат поиска отобразится в таблице слева.
3. Выберите пользователей и нажмите  .
4. Нажмите **Выпустить**. Имя устройства подставится автоматически.
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. Чтобы игнорировать ошибку и продолжить массовый выпуск устройств, нажмите **Пропустить**. Чтобы отменить массовый выпуск, нажмите **Отмена**.

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

Вы можете перенести данные об устройствах JaCarta из Aladdin JMS в Indeed CM с помощью утилиты миграции *IndeedCM.Migrate.JMS.exe*. Миграция данных не изменяет базу JMS. Для перенесенных устройств и сертификатов в Indeed CM доступен полный набор действий (выпуск, отзыв, обновление содержимого и другие).

В Indeed CM переносятся следующие данные об устройствах:

- Модель
- Форм-фактор
- Состояние
- Метка
- PIN-код администратора
- Ключевая информация для JMS-коннектора MS PKI (9C66741E-E5B1-40E3-B047-9A2D598CA913) — сертификаты, выпущенные в УЦ, и отслеживаемые сертификаты (выпущенные в стороннем УЦ)
- Привязка к пользователю

В Indeed CM не переносятся:

- Метки АМДЗ Аккорд
- Сертификаты Валидата УЦ
- Сертификаты КриптоПро УЦ

Предварительные требования

Миграция данных возможна при выполнении следующих условий:

- С сервера JMS, на котором выполняется запуск утилиты миграции, есть сетевой доступ к серверу с базой данных Indeed CM.
- Каталог пользователей Indeed CM совпадает с каталогом пользователей JMS.
- В Консоли управления Indeed CM в разделе **Конфигурация** → **Типы устройств** добавлены все типы устройств JaCarta, которые используются в JMS.
- В Консоли управления Indeed CM в разделе **Конфигурация** → **Лицензии** есть действующая лицензия на достаточное количество пользователей.

- Пользователям, устройства которых переносятся из JMS, назначены политики использования устройств.
- В политиках Indeed CM настроены те же УЦ и те же шаблоны сертификатов, что и в JMS.

Создание политики использования устройств

Перед миграцией данных из JMS создайте одну или несколько политик использования устройств в Indeed CM. Настройте в политике те же УЦ и шаблоны, которые использовались для выпуска сертификатов в JMS.

В результате миграции данных из JMS все пользователи с устройствами и сертификатами попадут под действие политик Indeed CM.

Процесс миграции

1. Настройте конфигурационный файл утилиты миграции *IndeedCM.Migrate.JMS.exe*.
2. Запустите утилиту миграции.

Настройка файла IndeedCM.Migrate.JMS.exe.config

Для работы утилиты настройте 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 содержится 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 *appsettings.json* веб-приложения mc (Консоль управления).
3. В секции `<adUserCatalogSettings>` заполните параметры подключения к каталогу пользователей. Всю секцию можно перенести из файла конфигурации *appsettings.json* веб-приложения mc (Консоль управления).

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Секции `sqlPersistenceSettings` и `adUserCatalogSettings` должны быть в расшифрованном виде.
>
> Чтобы расшифровать секции:
>
> 1. В дистрибутиве сервера Indeed CM перейдите в каталог *..\Misc\EncryptConfigs*.
> 2. Запустите файл *decryptConfigsSQL_AKEAgent.bat* в командной строке от имени администратора. Дождитесь завершения расшифровки.
>
> Чтобы зашифровать секции, используйте файл *encryptConfigsSQL_AKEAgent.bat*.

Работа с утилитой IndeedCM.Migrate.JMS.exe

Запустите утилиту *IndeedCM.Migrate.JMS.exe* на сервере JMS в командной строке от имени администратора.

Чтобы работать с резервной копией базы данных JMS, укажите путь к копии в реестре сервера JMS.

По умолчанию строка подключения к базе данных хранится в значении параметра `ConnectionString` в разделе `[HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\Enterprise Application Platform Server\JaCarta Management System\default\DatabaseManager]`.

SafeNet Authentication Manager

Вы можете перенести данные об устройствах eToken из SafeNet Authentication Manager (SAM) в Indeed CM с помощью утилиты миграции *IndeedCM.Migrate.SAM*. Для перенесенных устройств и сертификатов в Indeed CM доступен полный набор действий (выпуск, отзыв, обновление содержимого и другие).

Предварительные требования

Миграция данных возможна при выполнении следующих условий:

SAM

- Установлена версия SafeNet Authentication Manager 8.0, 8.2 Rev E и 9.0 SP2/SP3
- Настроено хранилище данных SAM в Active Directory
- Настроен удостоверяющий центр Microsoft CA
- Известны все типы устройств и значения их ATR (Answer To Reset), которые используются в SAM и будут использоваться в Indeed CM

Indeed Certificate Manager

- Установлена версия Indeed CM Server 4.1.3 и выше.
- Настроено хранилище данных в Active Directory или Microsoft SQL.
- Каталог пользователей Indeed CM совпадает с каталогом пользователей SAM.
- В Консоли управления Indeed CM в разделе **Конфигурация** → **Типы устройств** добавлены все типы устройств eToken, которые используются в SAM.
- В Консоли управления Indeed CM в разделе **Конфигурация** → **Лицензии** есть действующая лицензия на достаточное количество пользователей.
- Пользователям, устройства которых переносятся из SAM, назначены политики использования устройств.

Создание политики использования устройств

Перед миграцией данных из SAM создайте одну или несколько политик использования устройств в Indeed CM. Настройте в политике те же УЦ и шаблоны, которые использовались

для выпуска сертификатов в SAM.

В результате миграции данных из SAM все пользователи с устройствами и сертификатами попадут под действие политик Indeed CM.

Процесс миграции

Для миграции данных из SAM используйте утилиту *IndeedCM.Migrate.SAM.exe*. Утилита находится в дистрибутиве сервера Indeed CM в каталоге *Misc\SAMMigration*.

Заполните файлы конфигурации *IndeedCM.Migrate.SAM.exe.config* и *IndeedCM.Migrate.SAM.unity.config* и запуститу утилиту.

Настройка файла IndeedCM.Migrate.SAM.exe.config

Откройте файл *SAMMigration\IndeedCM.Migrate.SAM.exe.config* от имени администратора в текстовом редакторе, заполните следующие параметры и сохраните изменения.

Параметр	Описание
`samSettings`	Параметры подключения к хранилищу данных SAM
`MsCAConnectorId`	Идентификатор коннектора к Microsoft CA. Значение нахо коннектора в каталоге SAM. Путь по умолчанию: *C:\ProgramFiles\SafeNet\Authentication\SAM\x64\Bin\MsCA* Значение по умолчанию: `{1A30B883-CD69-4cbb-8D61-E72E9`
`connectionString`	Путь к файлу XML с информацией для подключения к сер файла указано имя домена, в котором развернут SAM. Путь по умолчанию: *C:\ProgramData\SafeNet\Authenticatio*
`migrateSAMSettings`	Параметры переноса данных
`ignoreCMCertificateTemplateNotFoundError`	Управляет импортом устройств, для которых нет шаблона CM. Процесс импорта не останавливается. `true` — устройство импортируется вместе с сертификата шаблон. `false` — устройство не импортируется, если хотя бы для нет шаблона. Значение по умолчанию.

Параметр	Описание
`notIssuedTokenAdminPin`	PIN-код администратора, который установится на устрой Применяется к носителям в состоянии *Зарегистрирован* выпускались.
`issuedTokenAdminPin`	PIN-код администратора, который установится на устрой Применяется к носителям в остальных состояниях, выпу инициализации.
`tokenTypes`	Секция с перечнем устройств для миграции. Для каждого модель, product name, цвет и ATR (Answer To Reset). Значение ATR для каждого устройства можно получить у технической поддержки Индид. В Indeed CM не переносятся устройства, модель и produc перечислены в `tokenTypes`.
`adPersistenceSettings`	Параметры подключения к хранилищу данных Indeed CM Содержимое совпадает с одноименной секцией *mc\appse*
`sqlPersistenceSettings`	Параметры подключения к хранилищу данных Indeed CM Содержимое совпадает с одноименной секцией *mc\appse* умолчанию секция закомментирована.
`adUserCatalogSettings`	Параметры подключения к каталогу пользователей Indee Содержимое совпадает с одноименной секцией *mc\appse*

Пример файла *IndeedCM.Migrate.SAM.exe.config*

```
<samSettings MsCAConnectorId="{1A30B883-CD69-4cbb-8D61-E72E9697D8B1}"
connectionString="C:\ProgramData\SafeNet\Authentication\SAM\demo.local.xml" />
<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="11d2f5051684451860ad177ebc39b55cacaf2a0a843b05ddf273b955c93ae015" />
<adUserCatalogSettings>
<rootContainers>
<container path="LDAP://OU=SAM_USERS,DC=demo,DC=local" userName="DEMO\cmadmin"
password="Password1" />
</rootContainers>
</adUserCatalogSettings>
```

Настройка файла IndeedCM.Migrate.SAM.unity.config

Откройте файл *SAMMigration\unity.config* от имени администратора и заполните секцию `container`:

- Строки до `<register type="ISAMDbContext" ... />` скопируйте из файла *mc\unity.config* Консоли управления Indeed CM. Дополнительные секции добавлять не нужно.
- Настройте вывод отчета миграции — раскомментируйте одну из секций, вторую оставьте закомментированной:
  - `IndeedCM.Migrate.SAM.Reporter.CSVMigrateReporter` — отчет сохраняется в CSV-файл *IndeedCM.Migrate.SAM.Report_dd-MM-yyyy_HH-mm-ss.csv* рядом с утилитой.
  - `IndeedCM.Migrate.SAM.Reporter.NullMigrateReporter` — отчет не создается.

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 от имени сервисной учетной записи SAM (Service Account).
2. В командной строке Windows от имени администратора запустите утилиту в тестовом режиме:

   ```
   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 об ошибках. В этом режиме работы утилиты данные не переносятся, события в журнал не заносятся.
3. Если в тестовом режиме не было критических ошибок, продолжите миграцию. Запустите утилиту *IndeedCM.Migrate.SAM.exe* в командной строке Windows от имени администратора.

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

Утилита миграции позволяет отправлять события в общий журнал Indeed CM через компонент Indeed CM EventLog Proxy. В журнал попадают результаты миграции — успех или ошибка переноса каждого устройства.

Чтобы включить отправку событий:

1. Установите Indeed CM EventLog Proxy на сервер Indeed CM.
2. Откройте файл *C:\inetpub\wwwroot\eventlogproxy\Web.config* от имени администратора и в секции `authorization` укажите учетные данные для доступа к сервису.

   Пример

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

3. На сервере SAM откройте файл *SAMMigration\IndeedCM.Migrate.SAM.exe.config* от имени администратора и добавьте элемент `proxyServer` в секцию `eventLogAuditSettings`:

   - `url` — путь к сервису eventlogproxy на сервере Indeed CM.
   - `userName` — имя пользователя из секции `authorization` файла *Web.config* Event Log Proxy.

- `password` — пароль учетной записи.

Пример

```
<proxyServer url="https://server.demo.local/eventlogproxy"
    userName="DEMO\Administrator" password="P@ssw0rd" />
```

4. Сохраните изменения.

Решение проблем

Сбор логов

Как собрать логи компонентов Indeed CM

Техническая поддержка

Как создать обращение в техническую поддержку

Сбор логов

При обращении в техническую поддержку Индид приложите к описанию проблемы отладочные логи компонента, в котором возникла ошибка. Далее описано, как собрать логи серверных и клиентских компонентов Indeed CM, а также логи инсталляторов.

Серверные компоненты

Чтобы собрать логи:

1. Перейдите в каталог нужного сервиса.

Расположение сервисов

Windows

Сервис	Каталог
Служба Card Monitor	`%ProgramFiles%\Indeed CM\CardMonitor`
Сервис регистрации агентов — `agentregistrationapi`	`%SystemDrive%\inetpub\wwwroot\cm\agent\agentregistrationapi`
Сервис агентов — `agentserviceapi`	`%SystemDrive%\inetpub\wwwroot\cm\agent\agentserviceapi`
Сервис API — `api`	`%SystemDrive%\inetpub\wwwroot\cm\api`
Сервис онлайн-разблокировки и выключения устройств — `credprovapi`	`%SystemDrive%\inetpub\wwwroot\cm\credprovapi`
Консоль управления — `mc`	`%SystemDrive%\inetpub\wwwroot\cm\mc`
MS CA Proxy — `mscaproxy`	`%SystemDrive%\inetpub\wwwroot\cm\mscaproxy`
OpenID Connect Server — `oidc`	`%SystemDrive%\inetpub\wwwroot\cm\oidc`
Сервис удаленного обслуживания — `rss`	`%SystemDrive%\inetpub\wwwroot\cm\rss`

Сервис	Каталог
Сервис самообслуживания — `ss`	`%SystemDrive%\inetpub\wwwroot\cm\ss`
Мастер настройки Indeed CM — `wizard`	`%SystemDrive%\inetpub\wwwroot\cm\wizard`
Сервер Indeed AirCard Enterprise	`%SystemDrive%\inetpub\wwwroot\Indeed.AirCard.EntServer`

Linux

Сервис	Каталог
Служба Card Monitor	`/opt/indeed/cm/cardmonitor`
Сервис регистрации агентов — `agentregistrationapi`	`/opt/indeed/cm/agentregistrationapi`
Сервис агентов — `agentserviceapi`	`/opt/indeed/cm/agentserviceapi`
Сервис API — `api`	`/opt/indeed/cm/api`
Сервис онлайн-разблокировки и выключения устройств — `credprovapi`	`/opt/indeed/cm/credprovapi`
Консоль управления — `mc`	`/opt/indeed/cm/mc`
OpenID Connect Server — `oidc`	`/opt/indeed/cm/oidc`
Сервис удаленного обслуживания — `rss`	`/opt/indeed/cm/rss`
Сервис самообслуживания — `ss`	`/opt/indeed/cm/ss`

Сервис	Каталог
Мастер настройки Indeed CM — `wizard`	`/opt/indeed/cm/wizard`

2. Откройте файл *nlog.config* от имени администратора и измените значение параметра `minlevel` с `Off` на `Trace`:

```
<logger name="*" minlevel="Trace" writeTo="file" />
```

3. Сохраните файл.
4. Очистите содержимое подкаталога *logs* внутри каталога сервиса.
5. Воспроизведите проблему.
6. Убедитесь, что в каталоге *logs* появились подкаталоги с файлами логов.
7. Отправьте весь каталог *logs* в техническую поддержку вместе с описанием проблемы.
8. Чтобы отключить логирование, измените значение параметра `minlevel` на `Off` и сохраните файл.

Клиентские компоненты

Windows

Используйте утилиту CM GetLog для локального и удаленного сбора программных логов компонентов Indeed CM Middleware, Indeed CM Client Tools и Indeed CM Agent.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> Для работы утилиты CM GetLog необходимы права локального администратора.

Чтобы собрать логи:

1. В дистрибутиве Indeed CM перейдите в каталог *GetLog* и запустите приложение *Cm.GetLog.exe* от имени администратора.
2. Подключитесь к компьютеру:

1. В поле **Computer** введите *localhost* для подключения к локальному компьютеру или имя/IP-адрес удаленного компьютера для подключения к удаленному компьютеру.
2. 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).

3. Нажмите **Enable Log**, чтобы включить логирование.
4. Воспроизведите проблему.
5. Нажмите **Disable Log**, чтобы отключить логирование.
6. Нажмите **Get Log...**, чтобы получить логи.
7. Укажите каталог для сохранения zip-архива и нажмите **Сохранить**.
8. Нажмите **Disconnect**, чтобы отключиться от компьютера.
9. Отправьте логи в техническую поддержку Индид. Подробно опишите действия пользователя и укажите точное время воспроизведения проблемы.

По умолчанию логи сохраняются в каталоге *C:\Windows\System32\LogFiles\cm*. Для доступа к логам удаленного компьютера по умолчанию используется сетевой каталог *ADMIN$\System32\LogFiles\cm*. Чтобы изменить каталог для записи логов, в меню настроек утилиты нажмите **Advanced Settings**, включите опцию **Use alternative location** и выберите каталог.

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\cm* 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\cm*, - сетевой путь: *ADMIN$\System32\LogFiles\cm*

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** (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 запущена утилита CM 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\Cm* 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.

Ошибка	Причина	Решение
`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 в ОС Linux записываются в каталог */tmp/cm/logs*.

Чтобы собрать логи:

1. Откройте файл */etc/cm/logging.cfg* с правами администратора и задайте параметру `enabled` значение `1`.
2. Сохраните файл.
3. Очистите содержимое каталога */tmp/cm/logs*.
4. Воспроизведите проблему.
5. Задайте параметру `enabled` значение `0`, чтобы выключить логирование.
6. Отправьте логи в техническую поддержку Индид. Подробно опишите действия пользователя и укажите точное время воспроизведения проблемы.

Инсталляторы

Для сбора логов инсталляторов Indeed CM в ОС Windows включите логирование Windows Installer через параметры командной строки или через реестр Windows.

Командная строка

Запустите нужный msi-пакет Indeed CM с параметром `/lv`:

```
msiexec /i <путь к файлу инсталлятора> /lv <путь к файлу с логами>
```

Пример запуска

```
msiexec /i D:\CM.Client\IndeedCM.Client.Tools-<номер версии>.x64.ru-ru.msi /lv
C:\install_log.txt
```

После завершения работы инсталлятора отправьте файл с логами в техническую поддержку Индид вместе с описанием проблемы.

Реестр Windows

Если инсталлятор запускается через групповые политики и параметры командной строки задать нельзя, включите логирование Windows Installer через реестр Windows.

Чтобы собрать логи:

1. Включите логирование одним из способов:
   - С помощью REG-файла — в дистрибутиве Indeed CM перейдите в каталог *\GetLog\Regfiles* и запустите файл *MSI logs On.reg*.
   - Вручную — в ветке *HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer* создайте параметр `Logging` типа `REG_SZ` со значением `voicewarmupx`.
2. Запустите нужный msi-пакет Indeed CM. Файл с логами сохраняется в папку *%Temp%*. Имя файла начинается с *Msi* и заканчивается расширением *.log*.
3. Чтобы открыть папку *%Temp%*, выполните команду:

   ```
   explorer %temp%
   ```
4. Отправьте файл лога в техническую поддержку Индид вместе с описанием проблемы.
5. Выключите логирование:
   - С помощью REG-файла — в дистрибутиве Indeed CM перейдите в каталог *\GetLog\Regfiles* и запустите файл *MSI logs Off.reg*.
   - Вручную — в ветке *HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer* удалите параметр `Logging` или задайте ему пустое значение.

Техническая поддержка

Если вы не нашли ответ на ваш вопрос в документации или базе знаний, обратитесь в службу технической поддержки. Чтобы оперативно решить проблему, предоставьте как можно больше информации, включая файлы, скриншоты, логи.

Создать заявку

1. Откройте портал технической поддержки.
2. Введите электронный адрес и пароль, нажмите **Вход**.
3. Нажмите **Отправить заявку**.
4. Выберите департамент и нажмите **Далее**.
5. Заполните форму заявки и нажмите **Отправить**.

Зарегистрироваться

Если у вас нет учетной записи на портале технической поддержки, зарегистрируйтесь. Вы можете зарегистрироваться самостоятельно или отправить заявку на регистрацию.

Самостоятельная регистрация

1. На странице входа нажмите **Зарегистрироваться**.
2. Заполните форму и нажмите **Зарегистрироваться**.
3. Перейдите по ссылке в письме, чтобы активировать аккаунт.

Заявка на регистрацию

1. На странице входа нажмите **Отправить заявку**.
2. Заполните форму и укажите, что это заявка на создание учетной записи.
3. Перейдите по ссылке в письме, чтобы активировать аккаунт.

Телефоны

Телефоны службы технической поддержки:

- 8 800 333 09 06
- +7 495 640 06 09
- +7 812 640 06 09

История версий

В этом разделе содержится краткое описание изменений и улучшений Indeed Certificate Manager по версиям.

7.3

- Реализована интеграция с удостоверяющим центром Dogtag CA.
- Добавлена поддержка LDAP-каталогов пользователей OpenLDAP и Альт Домен.
- Реализована защита закрытого ключа сертификата биометрическими данными пользователя для устройства Рутокен ЭЦП 3.0 3250 БИО: поддерживаются регистрация и обновление биометрии, биометрическая аутентификация при выпуске, обновлении и очистке устройства, а также при подписи документов.
- Добавлена поддержка устройств JaCarta-3 PKI/ГОСТ и JaCarta-3 SE.
- Добавлен режим аутентификации по сложному паролю при работе с Рутокен Логон.
- В карточку пользователя в Консоли управления добавлена возможность оставить служебные заметки о пользователе.
- Реализован автоматический выпуск сертификатов агента в удостоверяющем центре SafeTech CA.
- Добавлен статус агента *Отозван* при приостановке или отзыве сертификата агента в УЦ.
- Расширен список поддерживаемых ОС: Windows Server 2025 (клиентские компоненты), Debian 13 и Альт 11 (серверные и клиентские компоненты).

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.
- 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).

- Реализована возможность работы с устройствами в ОС Astra Linux SE в режиме замкнутой программной среды (ЗПС). Для поддержки режима ЗПС исполняемые файлы компонента Indeed CM Middleware подписаны встроенной подписью.
- Оптимизировано определение параметров работы Indeed CM в Мастере настройки.
- Оптимизировано администрирование Indeed CM в Консоли управления.
- 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.