



Indeed Certificate Manager

Техническая документация

Версия: 7.1

Дата: 08.05.2026

Содержание

О продукте	6
Компоненты	9
Лицензирование	11
Системные требования	13
Серверные компоненты	14
Клиентские компоненты	19
Сетевое взаимодействие	21
Устройства	24
Порядок установки	29
Настройка окружения	32
Каталог пользователей	33
LDAP	34
ЦР КриптоПро УЦ 2.0	46
Внутренний каталог пользователей	49
Сервисные сертификаты	54
Веб-сервер	66
IIS	67
NGINX	69
Apache HTTP Server	88
Платформа .NET	102
Хранилище данных	104
Удостоверяющие центры	112
Microsoft CA	113
КриптоПро УЦ 2.0	130
КриптоПро DSS 2.0	140
Валидата УЦ	146
Браузеры	156
Установка и настройка серверных компонентов	157
Indeed CM Server	159
Мастер настройки	167
Сервер OpenID Connect	194
Единый журнал событий	212
Indeed CM Agent	232
Установка и настройка клиентских компонентов	245
Indeed CM Client Tools	246

Indeed CM Middleware	252
Indeed CM Agent	264
Руководство администратора	270
Первый запуск	271
Конфигурация	272
Политики	274
Настройки PKI	277
Microsoft CA	280
КриптоПро УЦ 2.0	293
Валидата УЦ	303
КриптоПро DSS 2.0	310
Общие сертификаты	314
Indeed Access Manager	316
Secret Net Studio	320
РутOKEN Логон	322
СМЭВ	323
Поведение	325
Выпуск	331
Аутентификация	336
Агенты	337
Принтер смарт-карт	343
Уведомления	345
Назначения политик	358
Лицензии	360
Типы устройств	361
Организационная структура	371
Роли	373
Теги	387
Шаблоны печати	388
СКЗИ	398
Уведомления	405
Журналы учета	409
Консоль управления	411
Сводная информация	413
Пользователи	416
Карточка пользователя	421
Карточка устройства	425

Выпуск	430
Назначение	438
Сброс PIN-кода	441
Разблокировка	442
Выключение и включение	450
Отзыв	452
Изъятие	454
Замена	456
Обновление	459
Выпуск с печатью	463
Управление СКЗИ	465
Управление документами	471
Устройства	478
Сертификаты	488
Журнал событий	492
Агенты	561
Назначение задач в карточке устройства	568
Автоматические задачи	576
Журнал учета СКЗИ	581
Журнал учета устройств и сертификатов	587
Документы	588
Руководство пользователя	590
Операции с устройствами	593
Выпуск	594
Обновление	609
Выключение и включение	616
Отзыв и очистка	619
Сброс и изменение PIN-кода	622
Просмотр содержимого	623
Изменение ответов на секретные вопросы	624
СКЗИ	625
Документы	628
Клиентский агент	632
Просмотр файлов и ресурсов	635
Выгрузка сертификата DSS	636
API	638
Аутентификация	639

Устройства	645
СКЗИ	653
Дополнительные инструкции	678
Работа с устройствами JaCarta с ГОСТ-областью	679
Indeed CM Card Template Designer	681
Массовый выпуск смарт-карт	695
Перенос данных из сторонних систем	699
Aladdin JMS	700
SafeNet Authentication Manager	704
Решение проблем	713
Сбор логов	714
Контакты	727
История версий	728

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

Совместимость

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

Каталоги пользователей	• LDAP-каталоги Microsoft Active Directory, FreeIPA, ALD Pro • Центр Регистрации КриптоПро УЦ 2.0 • Внутренний каталог пользователей в СУБД Microsoft SQL Server или PostgreSQL
Удостоверяющие центры	• Microsoft CA • КриптоПро УЦ 2.0 (варианты исполнения для ОС Windows и Astra Linux SE) и КриптоПро PKI-Кластер • КриптоПро DSS • Валидата УЦ
Хранилище данных	• Microsoft SQL Server • PostgreSQL • Postgres Pro

Интеграции

• КриптоПро Шлюз УЦ-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.
- **Indeed CM MS CA Proxy** – дополнительный компонент для настройки интеграции с Центрами сертификации Microsoft Enterprise CA, находящимися за пределами домена, в котором развернут Indeed CM.
- **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



ПОДСКАЗКА

Веб-приложения OpenID Connect Server, Indeed CM MS CA Proxy и Indeed Log Server являются обязательными для инсталляций Indeed CM под управлением ОС Linux и дополнительными для инсталляций под управлением ОС Windows.

Вспомогательные утилиты

- *Storage.sql* – скрипт наполнения базы данных Microsoft SQL.
- *Storage-Postgre.sql* – скрипт наполнения базы данных PostgreSQL.
- *Cm.CertEnroll.MsCA.exe* – утилита для выпуска сертификата Агент регистрации для сервисной учетной записи с Microsoft Enterprise CA.
- *Cm.Agent.Cert.Generator* – утилита для создания сертификатов клиентского агента.
- *Cm.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 КристоПро DSS дает право на управление **ключами и сертификатами КристоПро DSS** в инфраструктуре Indeed CM.
Учитывается количество пользователей с сертификатами КристоПро 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 КристоПро 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 2012/2012 R2 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022 • Windows Server 2025 • Debian 9–12 • Astra Linux Special Edition 1.6–1.8 • Ubuntu 18.04 LTS–25.04 LTS • Red Hat Enterprise Linux 8–9 • CentOS Stream 8–9 • РЕД ОС 7.2–8  ПРЕДУПРЕЖДЕНИЕ Убедитесь, что в ОС Windows параметр Язык программ, не поддерживающих Юникод имеет значение Русский (Россия).

Веб-сервер	• Internet Information Services (IIS) 7.0 и выше 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 Hosting Bundle • URL Rewrite (для работы приложения Log Server на ОС Windows)

Компоненты КриптоПро	• КриптоПро CSP 4.0 R4 и выше для выпуска сертификатов в Microsoft Enterprise CA по алгоритмам ГОСТ Р34.10-2001/2012, КриптоПро УЦ 2.0, Валидата УЦ • КриптоПро CSP 5.0 и выше для интеграции с КриптоПро DSS 2.0 • КриптоПро CSP 5.0 R2 и выше для ОС Linux ⚠ ПРИМЕЧАНИЕ Чтобы установить защищенное TLS-соединение между сервером Indeed CM и Центрами Регистрации КриптоПро и Валидата УЦ, вам необходима серверная лицензия КриптоПро CSP. КриптоПро и Валидата УЦ защищены в соответствии с государственными стандартами РФ.

Требования к окружению

Каталог пользователей	• LDAP-каталоги – Active Directory, FreeIPA, ALD Pro • 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 ◦ Windows Server 2019 ◦ Windows Server 2022 ◦ Windows Server 2025 • 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  ПРИМЕЧАНИЕ Microsoft Enterprise CA поддерживает использование КриптоПро CSP в качестве криптопровайдера для выпуска сертификатов.
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, eToken Base Cryptographic Provider и т.д.)
- Microsoft Base Smart Card Cryptographic Service Provider (если CSP не предоставляется производителем устройства)



ПРИМЕЧАНИЕ

Также поддерживается в связке с КриптоПро УЦ 2.0.

ГОСТ Р34.10-2001/2012

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



ПРИМЕЧАНИЕ

Также поддерживается в связке с Microsoft Enterprise CA.

Клиентские компоненты

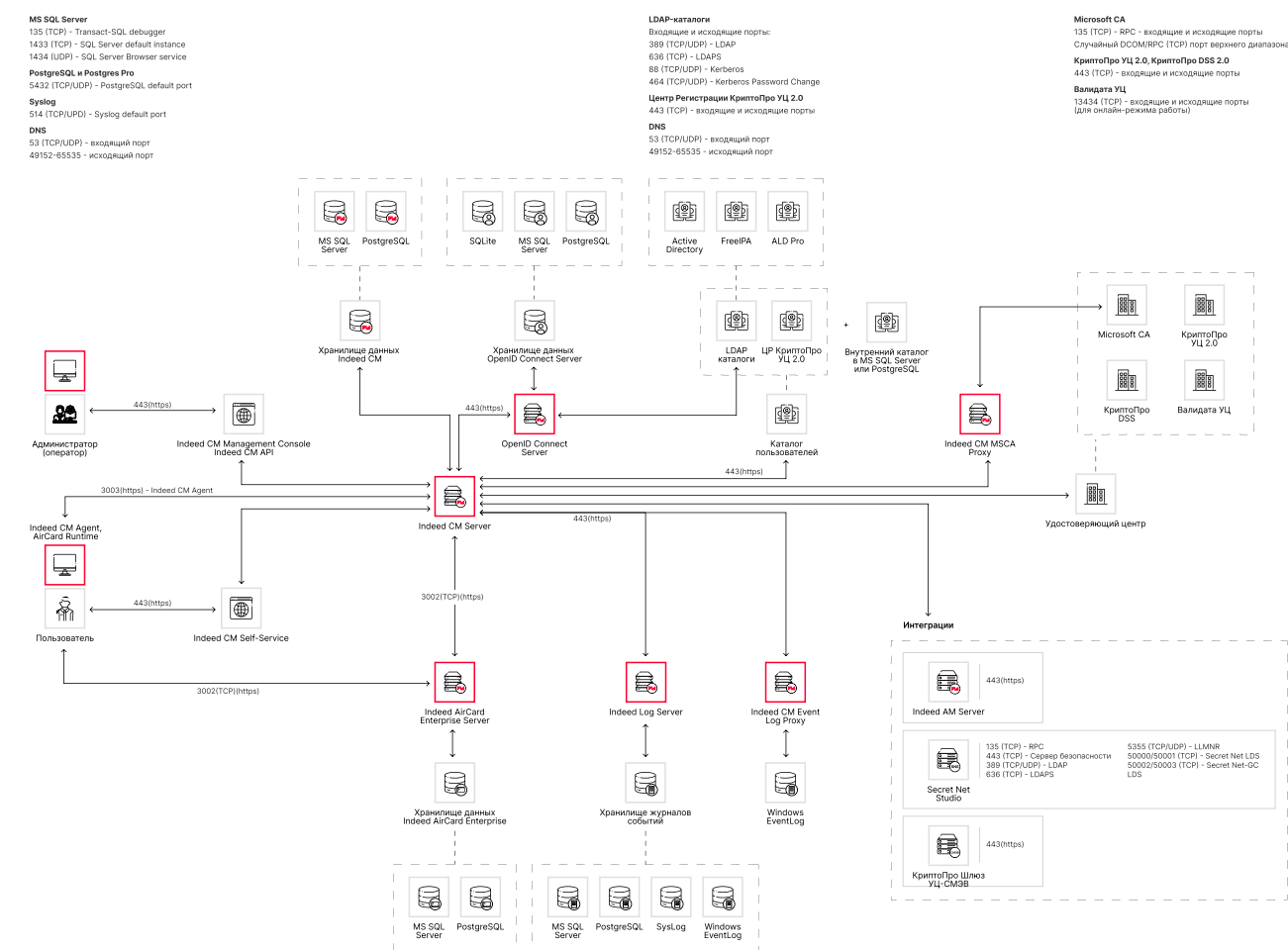
Перед установкой клиентских компонентов убедитесь, что IT-инфраструктура компании соответствует системным требованиям.

Аппаратные требования	Не менее 300 МБ свободного дискового пространства
Операционная система	• Windows Vista SP2 x86/x64 • Windows 7 SP1 x86/x64 • Windows 8/8.1 x86/x64 • Windows 10 x86/x64 • Windows 11 x86/x64 • Windows Server 2008 SP2 x86/x64 (с обновлением KB980368) • Windows Server 2008 R2 SP1 • Windows Server 2012/2012 R2 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022 • Debian 10–11 • Astra Linux Special Edition 1.6–1.8 • Astra Linux Common Edition 2.12 • Ubuntu 18.04 LTS и выше • Red Hat Enterprise Linux 8–9 • CentOS Stream 8–9 • РЕД ОС 7.3–8 • Альт Рабочая станция 9–10

Требования к окружению	• установленные драйверы (PKI-менеджеры) используемых смарт-карт и USB-токенов • Microsoft Edge 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 4.0 R4 и выше для выпуска сертификатов в Microsoft Enterprise CA по алгоритмам ГОСТ Р34.10-2001/2012, КриптоПро УЦ 2.0, Валидата УЦ • КриптоПро CSP 5.0 и выше для интеграции с КриптоПро DSS 2.0

Сетевое взаимодействие

На схеме представлена инфраструктура сетевого взаимодействия между компонентами Indeed CM.



Сервер Indeed CM

Веб-приложения, HTTP, HTTPS	80 (TCP) 443 (TCP) 3001/3002 (TCP) для Indeed AirCard Enterprise 3003 (TCP) для Indeed CM Agent
Почтовые уведомления, SMTP-сервер (исходящие подключения)	25 (TCP) 465 (TCP) 587 (TCP)

LDAP-каталоги	• 53 (TCP/UDP), исходящие подключения – DNS • 389 (TCP/UDP) – LDAP • 636 (TCP) – LDAPS • 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 и Postgres Pro	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  ПРИМЕЧАНИЕ 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.
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
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
Компания Индид	Сетевая смарт-карта AirCard

Производитель	Модель устройства
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 К-"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

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
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
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, где будет установлен сервер Indeed CM.

Windows

Настройка окружения

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 и выпустите **SSL/TLS-сертификат** для настройки защищенного соединения с веб-сайтом, где будет расположен Indeed CM.
3. Установите веб-сервер **Internet Information Services (IIS)**.
4. Установите платформу **.NET**.
5. Создайте **хранилище данных**.
6. Настройте интеграцию с **удостоверяющим центром**.

Установка и настройка Indeed CM

1. Установите и настройте серверные компоненты Indeed CM:
 1. **Сервер Indeed CM**
 2. **Мастер настройки**
2. Установите и настройте клиентские компоненты Indeed CM:
 1. **Indeed CM Client Tools**
 2. **Indeed CM Middleware**
3. Установите расширение Indeed CM Middleware в **браузеры** на рабочих станциях администраторов, операторов и пользователей.

Установка и настройка дополнительных компонентов

Дополнительно можно установить 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

Настройка окружения

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 и выпустите **SSL/TLS-сертификат** для настройки защищенного соединения с веб-сайтом, где будет расположен Indeed CM.
3. Установите веб-сервер **NGINX** или **Apache HTTP Server** и настройте в качестве обратного прокси-сервера.
4. Установите платформу **.NET**.
5. Создайте **хранилище данных**.
6. Настройте интеграцию с **удостоверяющим центром**. Для подключения к центру сертификации Microsoft CA установите компонент **Indeed CM MS CA Proxy**.

Установка и настройка Indeed CM

1. Установите и настройте серверные компоненты Indeed CM:
 1. **Сервер Indeed CM**
 2. **Мастер настройки**
 3. **Сервер OpenID Connect**
 4. **Indeed CM Event Log Proxy** или **Log Server** для записи событий в единый журнал

2. Установите и настройте клиентский компонент **Indeed CM Middleware**.
3. Установите расширение Indeed CM Middleware в **браузеры** на рабочих станциях администраторов, операторов и пользователей.

Установка и настройка дополнительных компонентов

Установите и настройте **Indeed CM Agent** – клиентский агент для управления устройствами на рабочих станциях пользователей. Агент лицензируется отдельно.

Настройка окружения



Каталог пользователей

Настройка каталогов пользователей



Сервисные сертификаты

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



Веб-сервер

Настройка веб-сервера для работы серверных компонентов Indeed CM



Платформа .NET

Установка .NET для работы серверных компонентов Indeed CM



Хранилище данных

Создание хранилища данных в Microsoft SQL, PostgreSQL и Postgres Pro



Удостоверяющие центры

Настройка удостоверяющих центров для интеграции с Indeed CM



Браузеры

Настройка браузеров для доступа к веб-приложениям Indeed CM

Каталог пользователей

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

Поддерживаются следующие службы каталогов:



LDAP

Active Directory, FreeIPA, ALD Pro



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. Поддерживаются следующие службы LDAP-каталогов:

- Active Directory
- FreeIPA
- ALD Pro

Каталог пользователей LDAP может быть составным. В этом случае пользователи будут расположены в разных контейнерах одного домена или в нескольких доменах.

Чтобы настроить каталог пользователей:

Active Directory

1. Подготовьте в Active Directory объект (домен, контейнер, подразделение) с конечными пользователями.
2. Создайте сервисную учетную запись для чтения и записи атрибутов пользователей. Вы можете распределить права между несколькими сервисными учетными записями или создать одну сервисную учетную запись с максимальным набором прав доступа к объектам Active Directory.
3. Откройте свойство **Безопасность** (Security) объекта, где хранятся пользователи Indeed CM.
4. Нажмите **Дополнительно** (Advanced). Нажмите **Добавить** (Add) → **Выбрать субъект** (Select a principal).
5. В текстовом поле **Введите имена выбираемых объектов** (Enter the object name to select) введите имя сервисной учетной записи и нажмите **ОК**.
6. В выпадающем списке **Применяется к** (Applies to) выберите **Дочерние объекты: Пользователь** (Descendant User objects).
7. В списке **Разрешений** (Permissions) выберите:
 - **Список содержимого** (List contents).
 - **Прочитать все свойства** (Read all properties). По умолчанию разрешение на чтение всех свойств пользователя имеется у всех учетных записей домена.
 - **Сброс пароля** (Reset password) для возможности сбросить пароль пользователя.

8. В списке **Свойств** (Properties) отметьте пункты:

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

9. Нажмите **ОК** и **Применить** (Apply).



ПРИМЕЧАНИЕ

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

Предоставление 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:

1. В оснастке **Редактирование ADSI** (ADSI edit) откройте свойство **Безопасность** (Security) объекта, где хранятся пользователи Indeed CM.
2. Для области применения **Этот объект и все дочерние объекты** (This object and all descendant objects):
 1. В списке **Разрешений** (Permissions) отметьте **Список содержимого** (List contents).
 2. В списке **Свойств** (Properties) отметьте пункты:
 - **Чтение: canonicalName** (Read canonicalName)
 - **Чтение: Distinguished Name** (Read Distinguished Name)
 - **Чтение: objectClass** (Read objectClass)
 - **Чтение: objectGuid** (Read objectGuid)
 - **Чтение: showInAdvancedViewOnly** (Read showInAdvancedViewOnly)
3. Для области применения **Дочерние объекты:Пользователь** (Descendant user objects):

1. В списке **Разрешений** (Permissions) отметьте **Список содержимого** (List contents).
2. В списке **Свойств** (Properties) выберите чтение/запись следующих наборов свойств и атрибутов:
 - **Чтение: личные сведения** (Read personal Information)
 - **Чтение: общие сведения** (Read general Information)
 - **Чтение: ограничения учетной записи** (Read account restrictions)
 - **Чтение: открытые сведения** (Read public Information)
 - **Запись: pwdLastSet** (Write pwdLastSet)
 - **Запись: thumbnailPhoto** (Write thumbnailPhoto) или
Запись: jpegPhoto (Write jpegPhoto)
 - **Запись: userAccountControl** (Write userAccountControl)
 - **Запись: userCertificate** (Write userCertificate)

 ПРИМЕЧАНИЕ

Приведены отображаемые имена LDAP (LDAP Display Name).

Предоставление прав доступа к набору свойств значительно улучшает производительность и упрощает управление безопасностью ([подробнее на сайте компании Microsoft](#)).

▼ **Атрибуты, используемые Indeed CM при работе с каталогом пользователей Microsoft AD**

Атрибут (LDAP Display Name)	Common Name	Комментарий
c	Country/Region или Country/Region Abbreviation	Входит в набор свойств «Личные сведения» (Personal Information).
canonicalName	Canonical Name	Входит в набор свойств «Открытые сведения» (Public Information).
cn	Common Name	Входит в набор свойств «Открытые сведения» (Public Information).
company	Company	Входит в набор свойств «Открытые сведения» (Public Information).
department	Department	Входит в набор свойств «Открытые сведения» (Public Information).
distinguishedName	Distinguished Name	Входит в набор свойств «Открытые сведения» (Public Information).
givenName	Given Name	Входит в набор свойств «Открытые сведения» (Public Information).
l	Locality Name	Входит в набор свойств «Личные сведения» (Personal Information).

Атрибут (LDAP Display Name)	Common Name	Комментарий
mail	E-mail Addresses	Входит в набор свойств «Открытые сведения» (Public Information).
manager	Manager	Входит в набор свойств «Открытые сведения» (Public Information).
objectClass	Object Class	Входит в набор свойств «Открытые сведения» (Public Information).
objectGUID	Object GUID	Входит в набор свойств «Открытые сведения» (Public Information).
objectSid	Object Sid	Входит в набор свойств «Общие сведения» (General Information).
otherMailbox	Other Mailbox	Входит в набор свойств «Открытые сведения» (Public Information).
proxyAddresses	Proxy Addresses	Входит в набор свойств «Открытые сведения» (Public Information).
pwdLastSet	Pwd Last Set	Входит в набор свойств «Ограничения учетной записи» (Account Restrictions).

Атрибут (LDAP Display Name)	Common Name	Комментарий
sAMAccountName	SAM Account Name	Входит в набор свойств «Общие сведения» (General Information).
sn	Surname	Входит в набор свойств «Открытые сведения» (Public Information).
st	State or Province Name	Входит в набор свойств «Личные сведения» (Personal Information).
streetAddress	Address (или Street)	Входит в набор свойств «Личные сведения» (Personal Information).
telephoneNumber	Telephone Number	Входит в набор свойств «Личные сведения» (Personal Information).
thumbnailPhoto или jpegPhoto	Picture	Входит в набор свойств «Личные сведения» (Personal Information).
userAccountControl	User Account Control	Входит в набор свойств «Ограничения учетной записи» (Account Restrictions).
userCertificate	User Certificate	Входит в набор свойств «Личные сведения» (Personal Information).

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

FreeIPA

1. Войдите в веб-версию FreeIPA под учетной записью администратора.
2. Создайте сервисную учетную запись для работы с каталогом пользователей. На вкладке **Идентификация (Identity)** → **Пользователи (Users)** нажмите **Добавить (Add)** и 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 КристоПро 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.

▼ **Атрибуты, используемые Indeed CM при работе с каталогом пользователей FreeIPA**

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

ALD Pro

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 КристоПро 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.

▼ **Атрибуты, используемые Indeed CM при работе с каталогом пользователей ALD Pro**

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
krbPasswordExpiration	Атрибут с датой и временем истечения срока действия текущего пароля
userCertificate	Сертификат

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:

▼ **Набор разрешений для сервисной группы пользователей**

Наименование разрешения	Тип объекта	Комментарий
Чтение свойств	Папка, Пользователь	Чтение свойств объекта. Если у субъекта нет права чтения свойств объекта, то объект не виден субъекту. Разрешение необходимо выдать и для корневой папки «Центр Регистрации» с наследованием для чтения списка пользователей.
Запись свойств	Папка	Запись свойств объекта. Необходимо выдать и для корневой папки «Центр Регистрации» с наследованием для публикации списка отозванных сертификатов
Запрос регистрации	Папка	Создание запроса на регистрацию пользователя
Запрос сертификата	Пользователь, шаблон	Создание запроса сертификата для пользователя
Запрос аннулирования	Пользователь	Создание запроса на аннулирование сертификата пользователя
Запрос приостановления	Пользователь	Создание запроса на приостановление сертификата пользователя
Запрос возобновления	Пользователь	Создание запроса на возобновление сертификата пользователя
Одобрение регистрации	Папка	Одобрение запроса на регистрацию пользователя

Наименование разрешения	Тип объекта	Комментарий
Одобрение сертификата	Пользователь, шаблон	Одобрение запроса сертификата для пользователя. Необходимо выдать и для корневой папки «Центр Регистрации» с наследованием.
Одобрение аннулирования	Пользователь	Одобрение запроса на аннулирование сертификата пользователя
Одобрение приостановления	Пользователь	Одобрение запроса на приостановление сертификата пользователя
Одобрение возобновления	Пользователь	Одобрение запроса на возобновление сертификата пользователя
Передача запросов	Пользователь	Передача запросов, подписанных пользователем-получателем услуги, а не подписью пользователя, передающего или одобряющего запрос.
Запрос переименования	Пользователь	Создание запроса на изменение данных пользователя.
Одобрение переименования	Пользователь	Одобрение запроса на изменение данных пользователя.

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 **ОК**.

Сервисная учетная запись

Используйте локальную учетную запись SQL или учетную запись Active Directory 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/postgresql/<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

Сервисные сертификаты

Создайте и выпустите SSL/TLS-сертификаты для настройки защищенного соединения с сервисами Indeed CM:

- Сертификат серверной аутентификации для **веб-сервера** и **сервера OpenID Connect**
- Сертификат клиентской аутентификации для дополнительных сервисов **Indeed CM Event Log Proxy** и **Indeed AirCard Enterprise**

Серверный сертификат

Создайте и выпустите SSL/TLS-сертификат для настройки защищенного соединения с веб-сайтом, где расположен Indeed CM. Используйте тот же сертификат в качестве сертификата подписи для настройки **OpenID Connect**.

Требования

- **Субъект** (Subject) сертификата должен содержать 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 серверной аутентификации должен содержать значение «Проверка подлинности сервера» (Server Authentication).

Создание шаблона

Подготовьте шаблон сертификата. В инструкции описана настройка шаблона сертификата в УЦ Microsoft CA.

1. В оснастке управления УЦ certsrv правой кнопкой мыши нажмите на **Шаблоны сертификатов** (Certificate Templates) и выберите **Управление** (Manage).
2. Скопируйте предустановленный шаблон **Веб-сервер** (Web Server) – правой кнопкой мыши нажмите на название шаблона и выберите **Скопировать шаблон** (Duplicate Template). Откроется окно свойств нового шаблона.
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 расположен 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. Правой кнопкой мыши нажмите 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 TLS-сертификат на имя рабочей станции, где будет установлен веб-сервер.

Сертификат можно выпустить:

- В УЦ
- С помощью самоподписанного сертификата

УЦ

В инструкции описан процесс выпуска сертификата в УЦ Microsoft CA.

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 **ОК**.
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 **ОК**.
9. Нажмите **Заявка** (Enroll).

Сертификат выпущен и установлен в хранилище локального компьютера (**Сертификаты** (Certificates) → **Личное** (Personal) → **Сертификаты** (Certificates)) с назначением «Проверка подлинности сервера» (Server Authentication).

Установка на ОС Linux

Чтобы установить сертификат на рабочие станции под управлением ОС Linux:

1. Выпустите сертификат в УЦ по инструкции выше.

2. Правой кнопкой мыши нажмите на сертификат и выберите **Все задачи** (All Tasks) → **Экспорт** (Export). Откроется мастер экспорта сертификатов.
3. Нажмите **Далее** (Next), выберите **Да, экспортировать закрытый ключ** (Yes, export the private key) и два раза нажмите **Далее** (Next).
4. Установите пароль – включите опцию **Пароль** (Password), введите и подтвердите пароль. Нажмите **Далее** (Next).
5. Выберите папку для экспорта сертификата.
6. Нажмите **Готово** (Finish). В папке сохранится сертификат в формате PFX.
7. Перенесите файл PFX на рабочую станцию под управлением ОС Linux.
8. Разделите файл PFX на файл сертификата и файл закрытого ключа. Вместо PFXFILE подставьте имя импортированного файла.



ПРЕДУПРЕЖДЕНИЕ

При выполнении команд утилита openssl предлагает установить пароль для файла закрытого ключа (KEY). Оставьте файл закрытого ключа 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-----
```

9. 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
```

10. Настройте право доступа 600 к файлу PFX:

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

Самоподписанный сертификат

Самоподписанный корневой сертификат создается с помощью утилиты openssl.

1. Создайте закрытый ключ, а затем корневой сертификат с использованием 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 веб-сервера. Вместо `<FQDN сервера Indeed CM>` подставьте DNS-имя рабочей станции, где будет установлен веб-сервер.

```
nano SSL.conf
```

▼ 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>
```

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

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

Клиентский сертификат

Сервер Indeed CM может выступать в качестве клиента для дополнительных сервисов **Indeed CM Event Log Proxy** и **Indeed AirCard Enterprise**.

В этом случае сервер Indeed CM должен иметь сертификат клиентской аутентификации, чтобы получить доступ к сервисам.

Требования

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

Создание шаблона

Подготовьте шаблон сертификата. В инструкции описана настройка шаблона сертификата в УЦ Microsoft CA.

1. В оснастке управления УЦ certsrv правой кнопкой мыши нажмите на **Шаблоны сертификатов** (Certificate Templates) и выберите **Управление** (Manage).
2. Скопируйте предустановленный шаблон **Проверка подлинности рабочей станции** (Workstation Authentication) – правой кнопкой мыши нажмите на название шаблона и выберите **Скопировать шаблон** (Duplicate Template). Откроется окно свойств нового шаблона.
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 будет расположен 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. Правой кнопкой мыши нажмите 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 TLS-сертификат на имя сервера Indeed CM.

- В УЦ
- С помощью самоподписанного сертификата

УЦ

В инструкции описан процесс выпуска сертификата в УЦ Microsoft CA.

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 **ОК**.

8. Перейдите на вкладку **Закрытый ключ** (Private Key) → **Параметры ключа** (Key Options) и убедитесь, что включена опция **Сделать закрытый ключ экспортируемым** (Make private key exportable). Нажмите **ОК**.

9. Нажмите **Заявка** (Enroll).

Сертификат выпущен и установлен в хранилище локального компьютера (**Сертификаты** (Certificates) → **Личное** (Personal) → **Сертификаты** (Certificates)) с назначением «Проверка подлинности рабочей станции» (Client Authentication).

Установка на ОС Linux

Чтобы перенести и установить сертификат на рабочие станции под управлением ОС Linux, экспортируйте сертификат и разделите его на файл сертификата и файл закрытого ключа:

1. Выпустите сертификат в УЦ по инструкции выше.
2. Правой кнопкой мыши нажмите на сертификат и выберите **Все задачи** (All Tasks) → **Экспорт** (Export). Откроется мастер экспорта сертификатов.
3. Нажмите **Далее** (Next), выберите **Да, экспортировать закрытый ключ** (Yes, export the private key) и два раза нажмите **Далее** (Next).
4. Установите пароль – включите опцию **Пароль** (Password), введите и подтвердите пароль. Нажмите **Далее** (Next).
5. Выберите папку для экспорта сертификата.

6. Нажмите **Готово** (Finish).
7. Перенесите файл PFX на рабочую станцию под управлением ОС Linux.
8. Разделите файл PFX на файл сертификата и файл закрытого ключа. Вместо PFXFILE подставьте имя импортированного файла.

 ПРЕДУПРЕЖДЕНИЕ

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

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

Файл сертификата *client.crt* должен содержать следующее:

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

9. 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 client.key -in client.crt
```

10. Настройте право доступа 600 к файлу PFX:

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

Самоподписанный сертификат

Самоподписанный корневой сертификат создается с помощью утилиты openssl.

1. Создайте закрытый ключ, а затем корневой сертификат с использованием 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 client.conf, который содержит настройки для генерации запроса на сертификат. Вместо `<FQDN сервера Indeed CM>` подставьте DNS-имя рабочей станции, где установлен сервер Indeed CM.

```
nano client.conf
```

▼ Пример файла client.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 = clientAuth
[alt_names]
DNS.1 = <FQDN сервера Indeed CM>
```

3. Создайте утилитой openssl запрос на сертификат и выпустите сертификат с помощью самоподписанного сертификата:

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

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 **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 Internet Information Services (IIS) версии 7.0 или выше со следующими модулями:

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



ПОДСКАЗКА

Для быстрой установки Internet Information Services (IIS) с требуемыми модулями используйте скрипт PowerShell из каталога `\IIS.Setup.Scripts` дистрибутива Indeed CM. Для развертывания сервера Indeed CM установите Microsoft .NET 8.0 после установки и настройки компонентов Internet Information Services (IIS).

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 **ОК**.

NGINX

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

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

Debian-based

Установка веб-сервера

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

Ubuntu:

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

Debian:

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

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

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

3. Для подключения apt-репозитория выполните следующую команду:

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

4. Выполните следующую команду:

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

Документация по установке на прочие ОС доступна [на портале NGINX](#).

Установка TLS-сертификата

Установите TLS-сертификат на веб-сервер. [Как создать TLS-сертификат для веб-сервера](#)

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

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

▼ Таблица рекомендуемых к использованию директив

Контекст	Директива	Значение по умолчанию	Рекомендуемое значение	
http	proxy_buffer_size	4k 8k	16k	Уве. пер. зап.
	proxy_buffers	8 4k 8 8k	4 16k	Уве. пер. зап.
	types_hash_max_size	1024	4096	Уве. храп. кол.
	client_max_body_size	1m	10m	Уве. загр.
server	listen	80	443 ssl	Изм. НТГ. НТГ.
			3003 ssl	Пор. кон. аген.
	ssl_certificate	—	<i>/etc/ssl/private/SSL.crt</i>	Для фай. сер. кор.
	ssl_certificate_key	—	<i>/etc/ssl/private/SSL.key</i>	Для зак.

Контекст	Директива	Значение по умолчанию	Рекомендуемое значение	
	ssl_verify_client	off	optional_no_ca	Доб сер аген
location	proxy_pass	—	*	Оди нап Inde loca сере Точ http http Где кото SEF имя
	include	—	/etc/nginx/conf.d/proxy.conf	Нек каж кон соз дир вме
	proxy_http_version	1.0	1.1	Вер под
	proxy_cache_bypass	—	\$http_upgrade	Оп буд
	proxy_set_header	—	Upgrade \$http_upgrade	Оп пос

Контекст	Директива	Значение по умолчанию	Рекомендуемое значение	
			Connection keep-alive	Для
			Host \$host	Для сер
			X-Real-IP \$remote_addr	По : про пол заде
			X-Forwarded-For \$proxy_add_x_forwarded_for	Под фор про при \$pro
			X-Forwarded-Proto \$scheme	Веб про для
	fastcgi_buffers	8 4k 8k	16 16k	Оп чте под
	fastcgi_buffer_size	4k 8k	32k	Оп час
	proxy_set_header	—	x-ssl-client-cert \$ssl_client_escaped_cert	Дир при кли сер

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

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

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

Рекомендуемое содержимое файла proxy.conf для работы с Indeed CM

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

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

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

```

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

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

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

    server {
        listen                443 ssl;
        server_name           $hostname;

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

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

```



```

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

server {
    listen          3003 ssl;
    server_name     $hostname;

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

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

```

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

```
sudo nginx -s reload
```

RHEL-based

Установка веб-сервера

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

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

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

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

```
[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. Выполните следующую команду:

```
sudo yum install nginx
```

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

Документация по установке на прочие ОС доступна [на портале NGINX](#).

Установка TLS-сертификата

Установите TLS-сертификат на веб-сервер. [Как создать TLS-сертификат для веб-сервера](#)

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 он расположен в каталоге */usr/local/nginx/conf*, */etc/nginx* или */usr/local/etc/nginx*.

▼ Таблица рекомендуемых к использованию директив

Контекст	Директива	Значение по умолчанию	Рекомендуемое значение	
http	proxy_buffer_size	4k 8k	16k	Уве. пер зап
	proxy_buffers	8 4k 8 8k	4 16k	Уве. пер зап
	types_hash_max_size	1024	4096	Уве. хра кол
	client_max_body_size	1m	10m	Уве. заг
server	listen	80	443 ssl	Изм НТ НТ
			3003 ssl	Пор кон аген
	ssl_certificate	—	<i>/etc/ssl/private/SSL.crt</i>	Для фай сер кор
	ssl_certificate_key	—	<i>/etc/ssl/private/SSL.key</i>	Для зак

Контекст	Директива	Значение по умолчанию	Рекомендуемое значение	
	ssl_verify_client	off	optional_no_ca	Доб сер аген
location	proxy_pass	—	*	Оди нап Inde loca сере Точ http http Где кото SEF имя
	include	—	/etc/nginx/conf.d/proxy.conf	Нек каж кон соз дир вме
	proxy_http_version	1.0	1.1	Вер под
	proxy_cache_bypass	—	\$http_upgrade	Оп буд
	proxy_set_header	—	Upgrade \$http_upgrade	Оп пос.

Контекст	Директива	Значение по умолчанию	Рекомендуемое значение	
			Connection keep-alive	Для
			Host \$host	Для сер
			X-Real-IP \$remote_addr	По : про пол заде
			X-Forwarded-For \$proxy_add_x_forwarded_for	Под фор про при \$pro
			X-Forwarded-Proto \$scheme	Веб про для
	fastcgi_buffers	8 4k 8k	16 16k	Оп чте под
	fastcgi_buffer_size	4k 8k	32k	Оп час
	proxy_set_header	—	x-ssl-client-cert \$ssl_client_escaped_cert	Дир при кли сер

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

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

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

Рекомендуемое содержимое файла proxy.conf для работы с Indeed CM

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

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

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


```

user 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;

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

    server {
        listen                443 ssl;
        server_name           $hostname;

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

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

```

```

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

server {
    listen          3003 ssl;
    server_name     $hostname;

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

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

```

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

```
sudo nginx -s reload
```

Apache HTTP Server

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

1. Установите веб-сервер.
2. 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 [портале Apache](#).

Установка TLS-сертификата

Установите TLS-сертификат на веб-сервер. [Как создать TLS-сертификат для веб-сервера](#)

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

1. Для работы системы включите модули:

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

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

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

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



ПРЕДУПРЕЖДЕНИЕ

При установке Apache в ОС Astra Linux в файле *apache2.conf* может потребоваться отключение параметра *AstraMode*, подробнее [на портале Astra Linux](#).

Настройка сайта

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

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

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

2. Заполните файл рекомендуемым содержимым.



ПРЕДУПРЕЖДЕНИЕ

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

▼ Рекомендуемое содержимое файла **SERVER_FQDN.conf**

```

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

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

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

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

    ProxyPreserveHost On

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

```



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

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

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

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

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

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

```
#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 [портале Apache](#).

Установка TLS-сертификата

Установите TLS-сертификат на веб-сервер. [Как создать TLS-сертификат для веб-сервера](#)

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

Настройка сайта

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

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

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

2. Заполните файл рекомендуемым содержимым.



ПРЕДУПРЕЖДЕНИЕ

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

▼ Рекомендуемое содержимое файла **SERVER_FQDN.conf**

```

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

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

    ErrorLog 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.

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-8.0.12-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
```

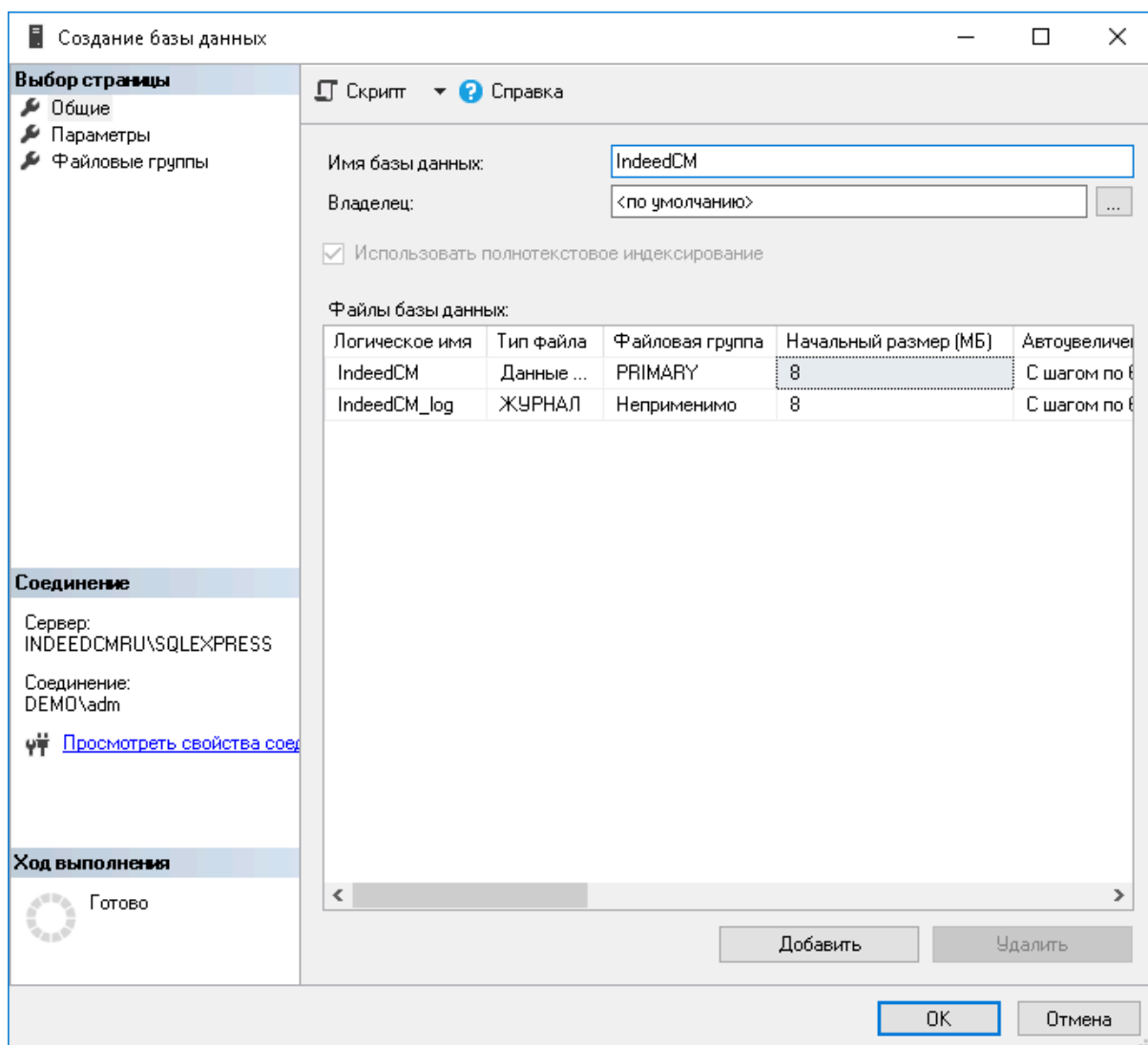
Хранилище данных

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

Microsoft SQL

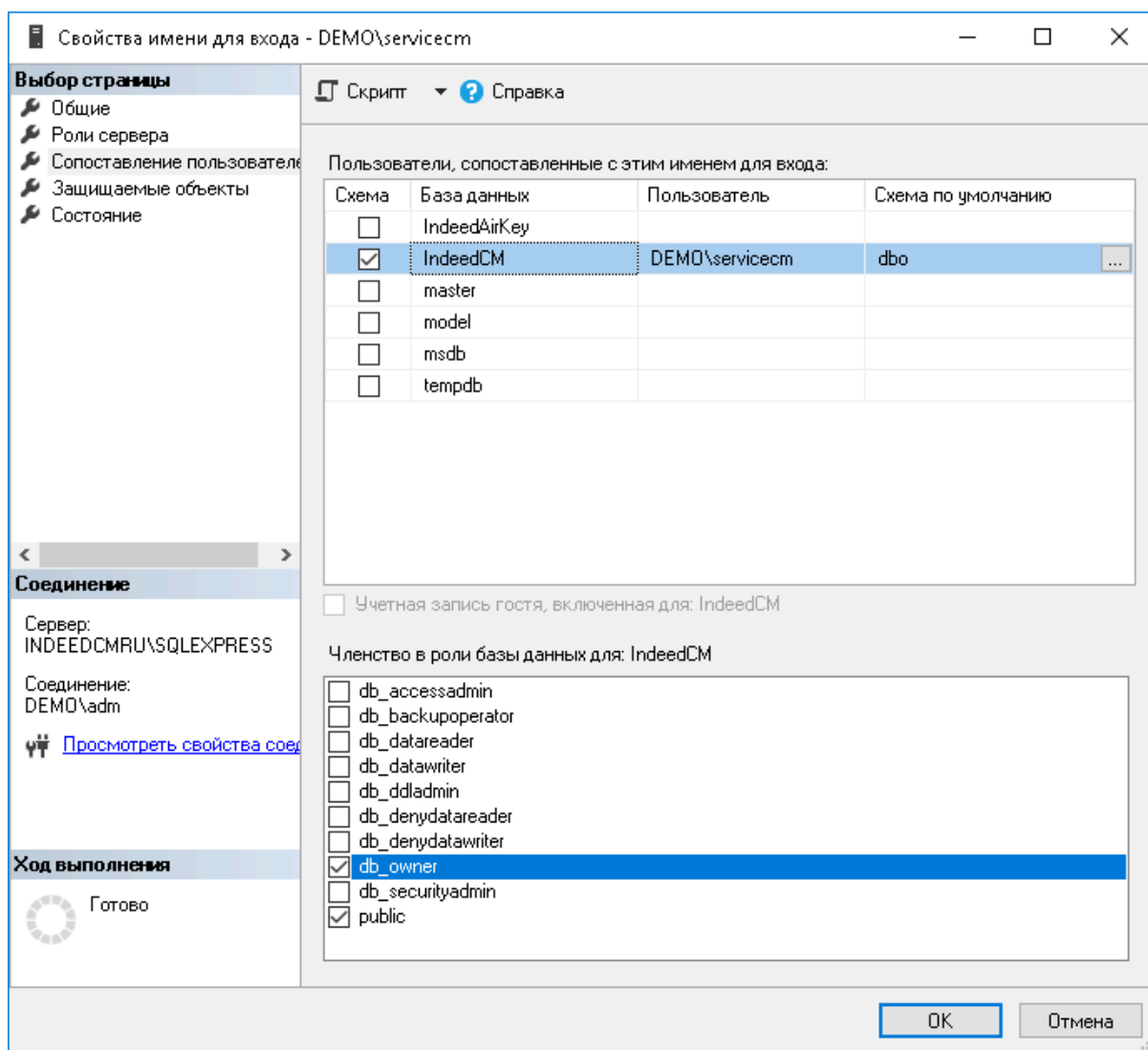
1. Создайте базу данных в среде SQL Server Management Studio с произвольным именем:

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 **ОК**.



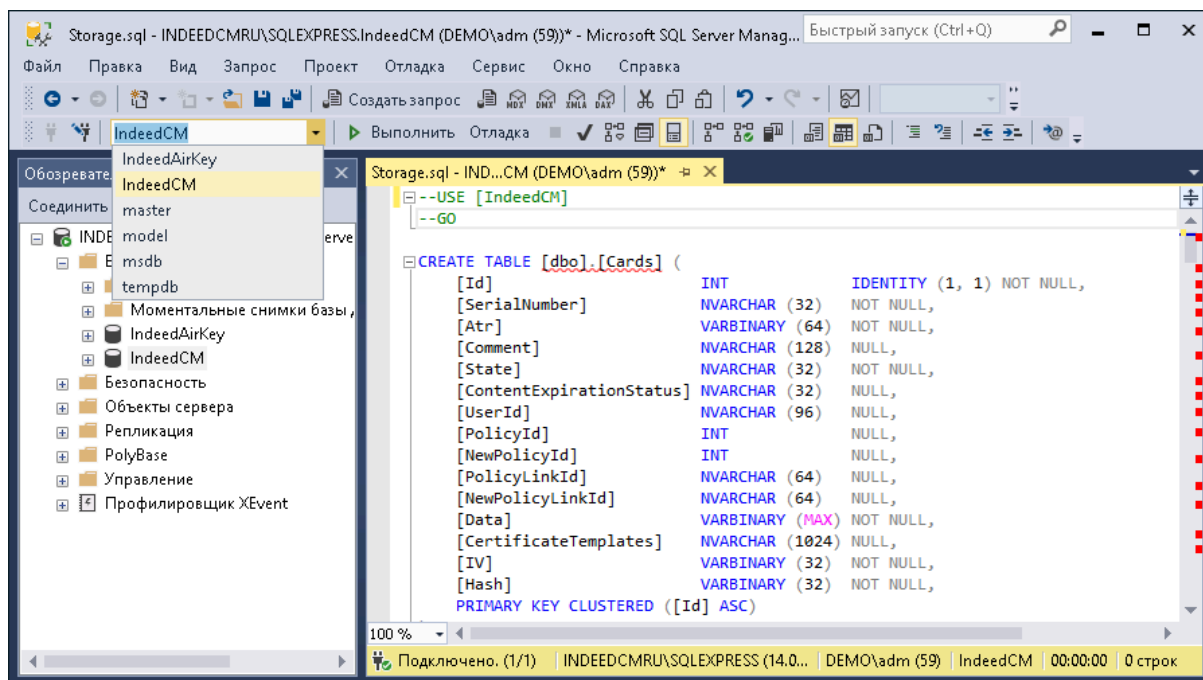
2. Используйте локальную учетную запись SQL или учетную запись Active Directory и наделите ее необходимыми правами для работы с созданной базой данных. Эта учетная запись будет использоваться для выполнения операций чтения и записи в базу данных. Подключение к базе с использованием указанной учетной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

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



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

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

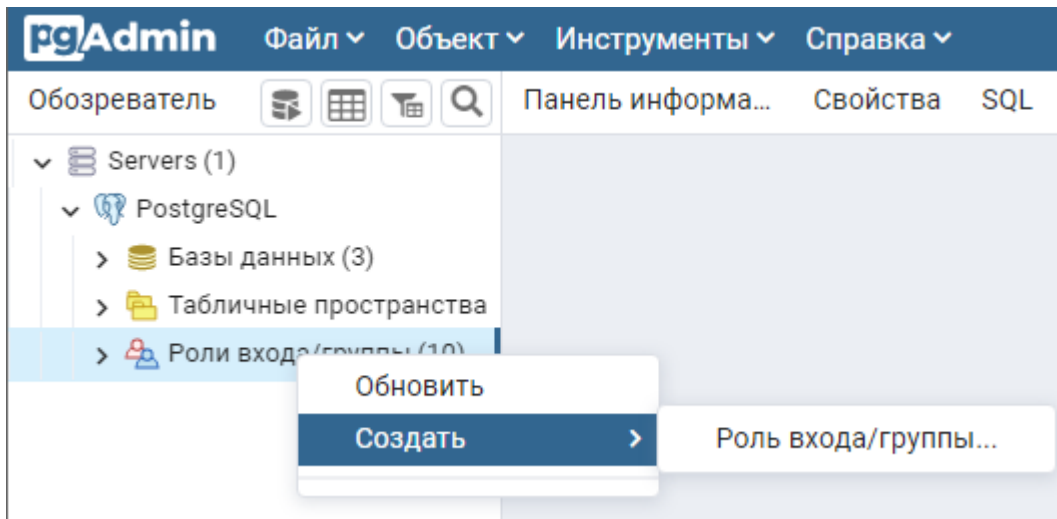


PostgreSQL и Postgres Pro

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

Сервисная учетная запись

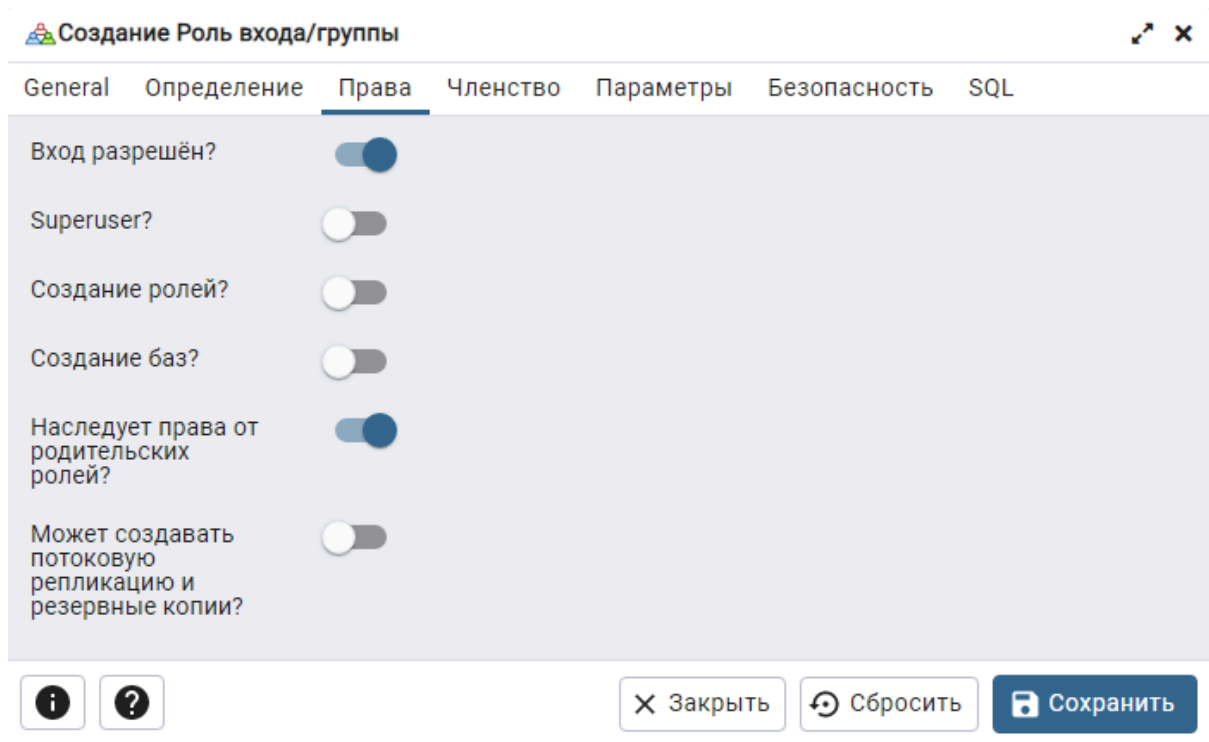
1. Откройте **pgAdmin**, укажите мастер пароль и подключитесь к серверу.
2. В разделе **Обозреватель (Browser)** правой кнопкой мыши нажмите по пункту меню **Роли входа/группы (Login/Group Roles)**.
3. Выберите **Создать → Роль входа/группы (Create → Login/Group Role...)**.



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

5. На вкладке **Определение** (Definition), в поле **Пароль** (Password), укажите пароль пользователя. В поле **Роль активна до** (Account Expires) должно быть указано значение **No Expiry**. При создании сервисной учетной записи требуется отключить срок действия пароля.

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

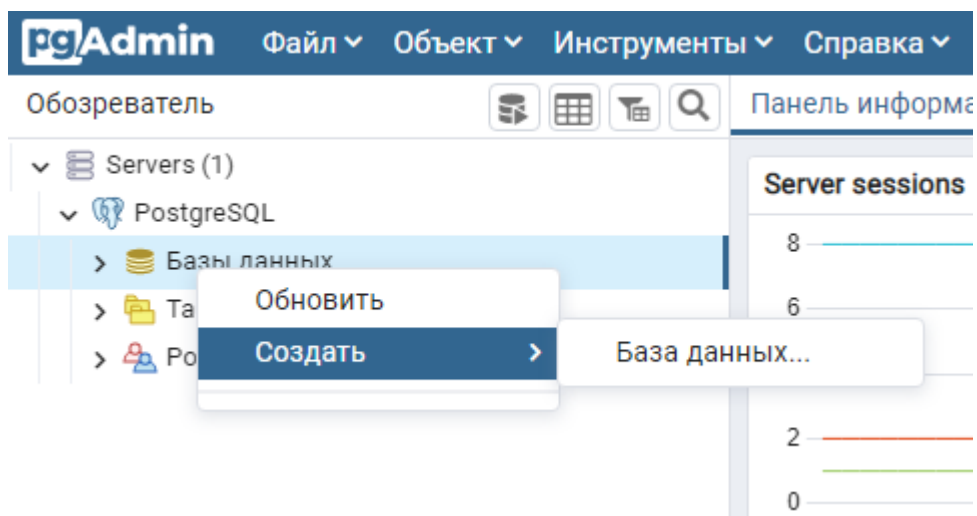


7. Оставьте остальные значения по умолчанию и нажмите **Сохранить** (Save).

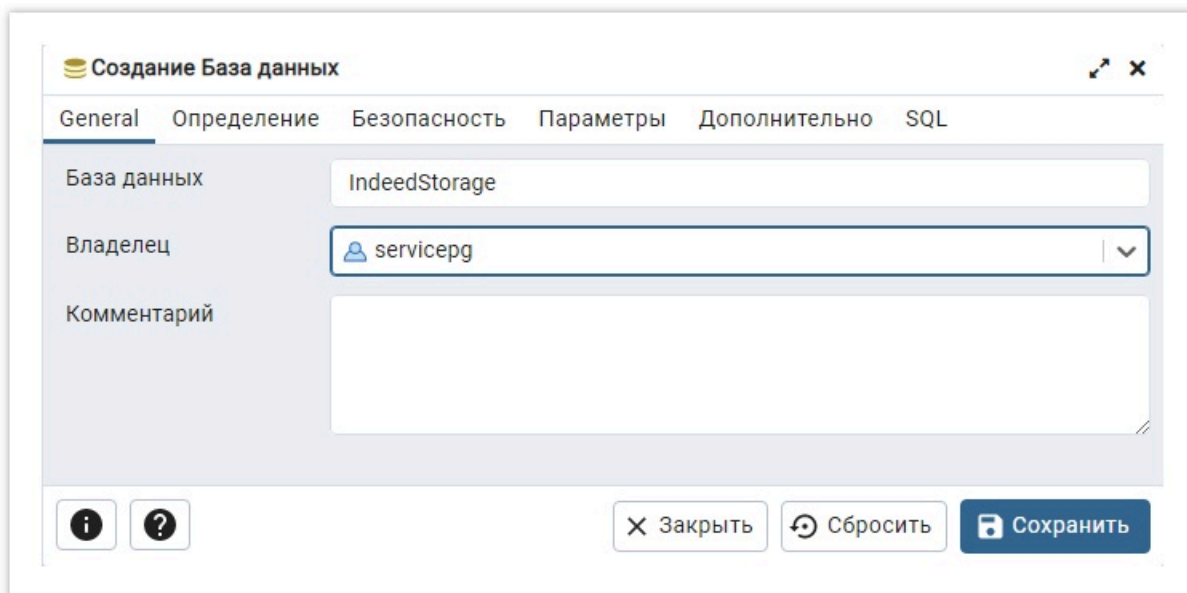
База данных

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

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

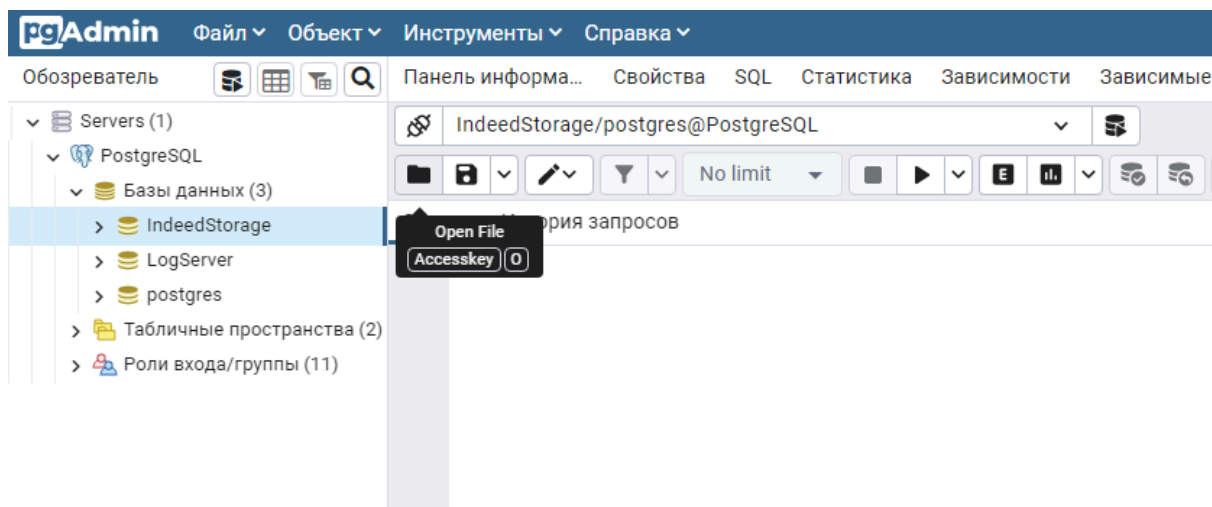


3. На вкладке **Общие** (General) укажите название базы данных в поле **База данных** (Database), например, **IndeedStorage**, выберите пользователя, созданного на первом этапе (**servicepg**) из списка **Владелец** (Owner) и нажмите **Сохранить** (Save).

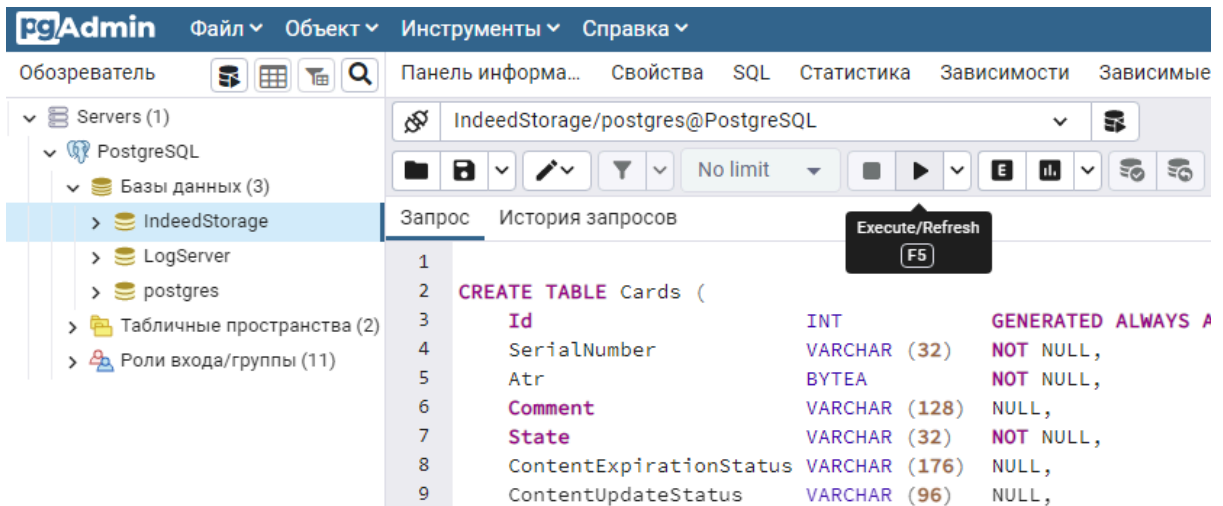


2. Выберите в **Обозревателе** (Browser) созданную базу данных (**IndeedStorage**) и выполните скрипт *Storage-Postgre.sql*:

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

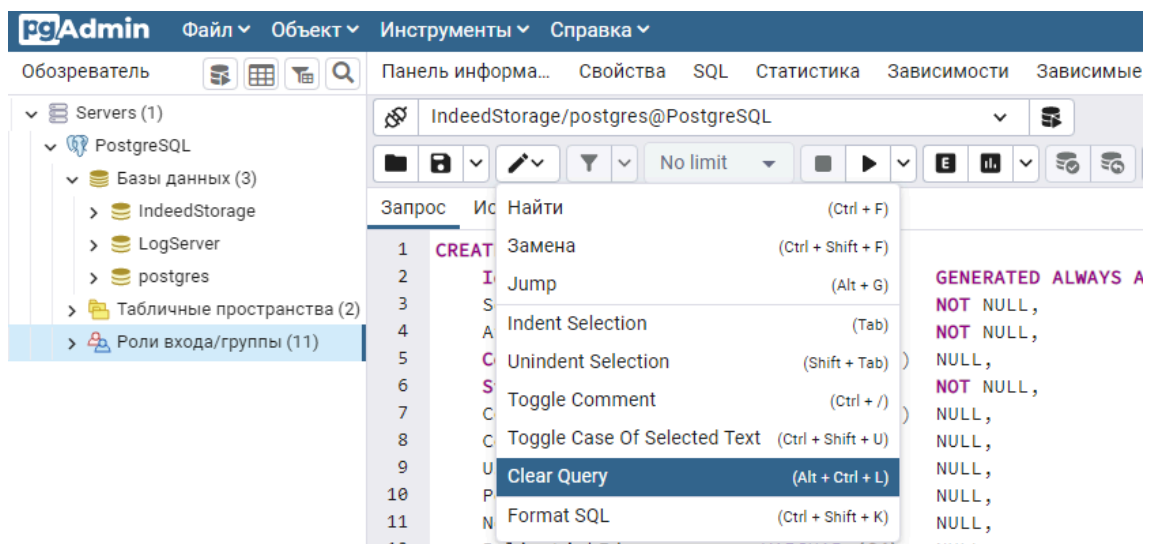


3. В меню запросника нажмите на кнопку **Выполнить** (Execute/Refresh) .



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

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



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

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

Пример запроса

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

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

Удаленное подключение к базе данных

Откройте конфигурационный файл `pg_hba.conf`.

▼ Расположение файла `pg_hba.conf`

PostgreSQL

OC Windows: `C:\Program Files\PostgreSQL\<номер версии>\data`

OC Linux: `/etc/postgresql/<номер версии>/main`

Postgres Pro

OC 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 будет доступно подключение.
- **ADDRESS** – IP-адрес удаленного сервера Indeed Certificate Manager.
- **METHOD** – метод аутентификации пользователя.

Пример строки

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

Удостоверяющие центры



Microsoft CA

Настройка Microsoft 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 Certificate Manager с Microsoft Enterprise CA:

1. **Создайте** сервисную учетную запись для работы с Microsoft CA.
2. **Настройте** шаблоны сертификатов.
3. **Добавьте** подготовленные шаблоны сертификатов в список выдаваемых.
4. **Выпустите** сертификат Агента регистрации (Enrollment Agent) сервисной учетной записи.

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

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

Создание сервисной учетной записи для работы с Microsoft CA

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

1. Создайте учетную запись пользователя в Active Directory.
2. Откройте оснастку **Центр сертификации** (Certification Authority), выберите 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.
5. Нажмите **ОК**, чтобы сохранить настройки.



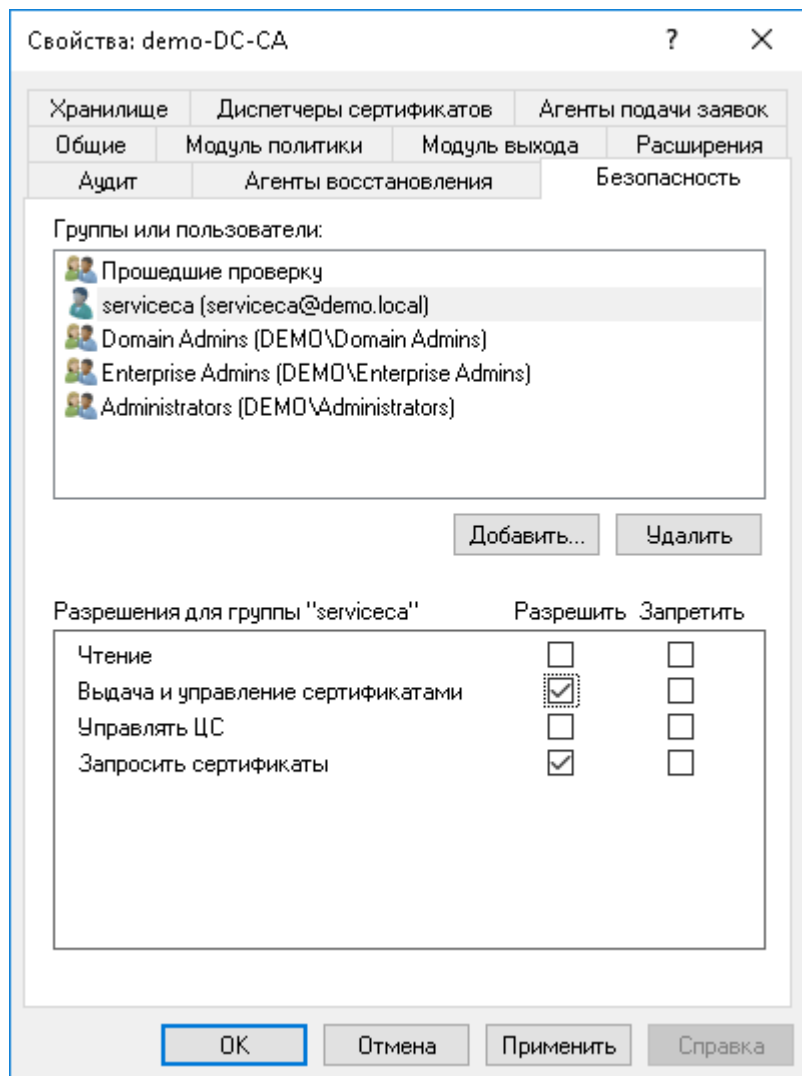
ПОДСКАЗКА

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



ПРЕДУПРЕЖДЕНИЕ

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



Настройка шаблонов сертификатов

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

Агент Регистрации

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

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

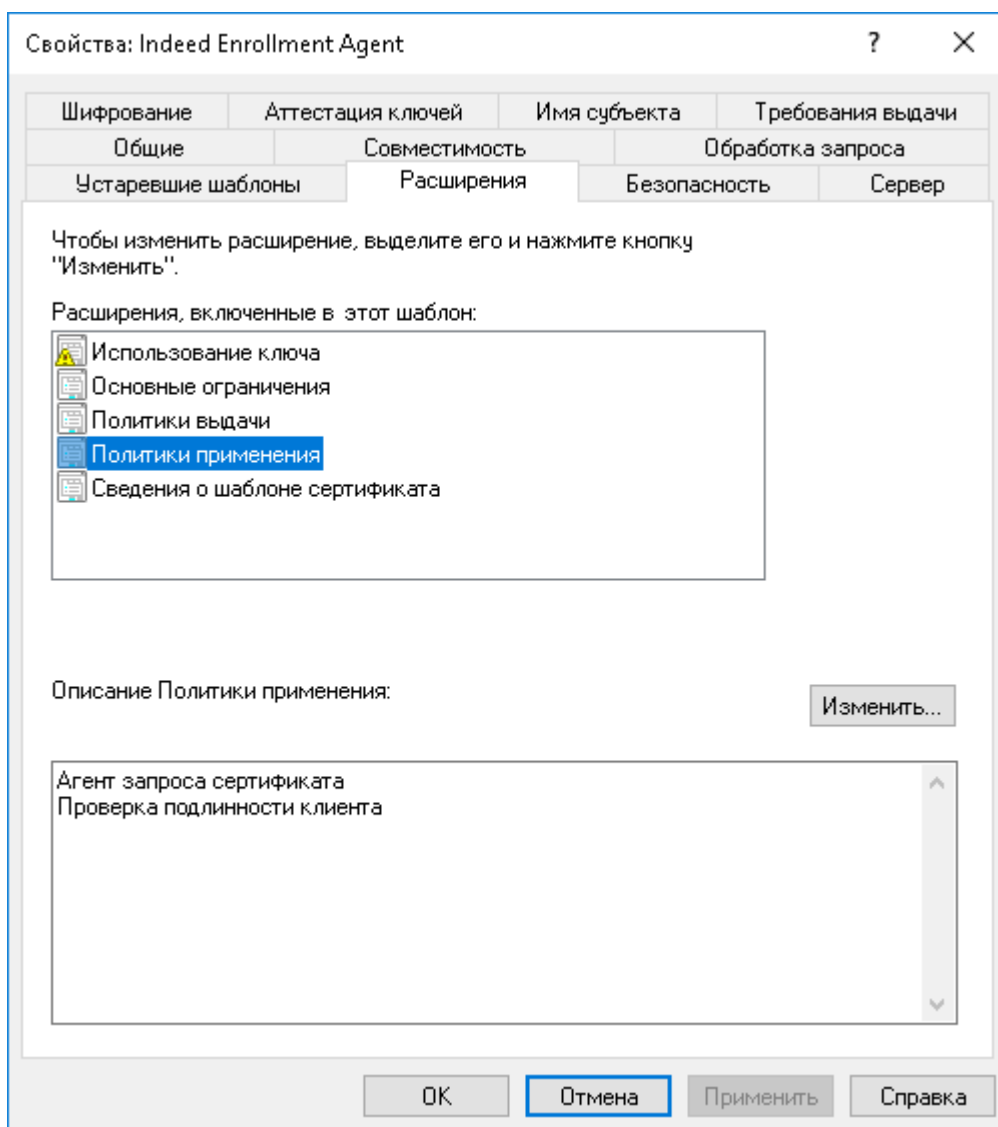
ПРЕДУПРЕЖДЕНИЕ

Сертификат **Агент регистрации** (Enrollment Agent) добавляется в Indeed CM только один раз и выдается только на имя сервисной учетной записи.

Убедитесь, что сертификат **Агент регистрации** не добавлен в политики использования устройств, иначе пользователи будут иметь возможность самостоятельно подписывать сертификаты в УЦ, что создает угрозу безопасности.

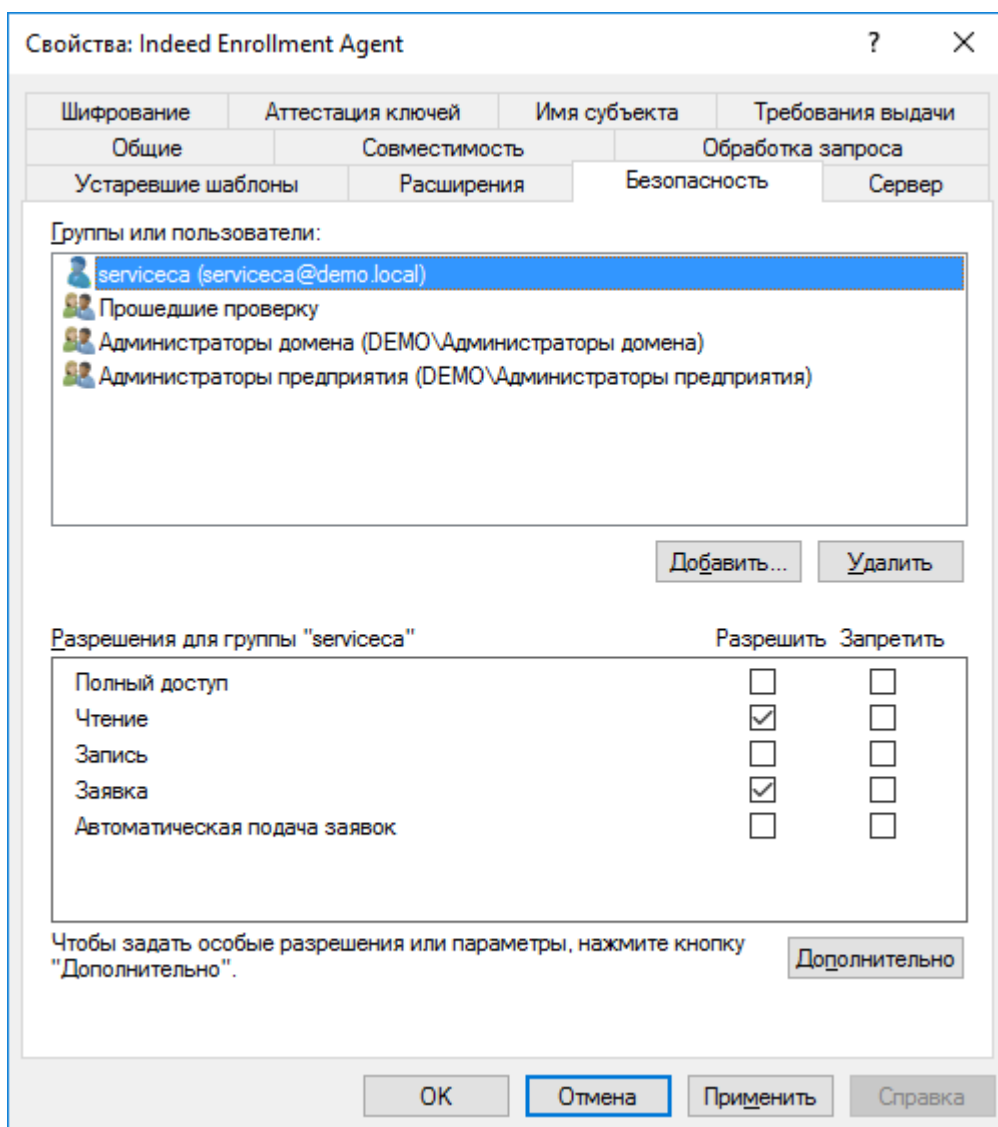
Создайте и настройте шаблон сертификата **Агент регистрации**:

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



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

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



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

Сертификаты пользователей

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

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

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

3. Нажмите правой кнопкой мыши по шаблону **Вход со смарт-картой** (Smartcard Logon) и выберите **Скопировать шаблон** (Duplicate Template).
4. Перейдите на вкладку **Общие** (General) и в поле **Отображаемое имя шаблона** (Template display name) введите **Indeed Smart Card Logon**. Измените **Период действия** (Validity period) и **Период обновления** (Renewal period) в соответствии с потребностями вашей организации.
5. На вкладке **Шифрование** (Cryptography) в поле **Минимальный размер ключа** (Minimum key size) укажите необходимую длину ключа.

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

for reenrollment).

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

Строится на основе данных Active Directory

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

1. Выберите **Полное различающееся имя** (Fully distinguished name) из списка **Формат имени субъекта** (Subject name format).

2. Установите флажок **Имя субъекта-пользователя (UPN)** (User principal name (UPN)).
3. Снимите флажки с опций **Включить имя электронной почты в имя субъекта** (Include e-mail name in subject name) и **Имя электронной почты** (E-mail name), если по данному шаблону будут выпускаться сертификаты для пользователей, у которых не указан адрес электронной почты в Active Directory.

The screenshot shows the 'Свойства: Indeed Smart Card Logon' (Properties: Indeed Smart Card Logon) dialog box. The 'Имя субъекта' (Subject Name) tab is selected. The 'Предоставляется в запросе' (Supply in the request) radio button is selected. Below it, the 'Использовать данные о субъекте из существующих сертификатов для запросов обновления автоматической подачи заявок (*)' (Use subject data from existing certificates for automatic renewal requests) checkbox is unchecked. The 'Строится на основе данных Active Directory' (Built on Active Directory data) radio button is selected. Below it, the text says: 'Выберите этот параметр для повышения согласованности имен субъектов и упрощения администрирования сертификатов.' (Select this parameter to improve subject name consistency and simplify certificate administration). The 'Формат имени субъекта:' (Subject name format:) dropdown menu is set to 'Полное различающееся имя' (Fully qualified name). Below this, the 'Включить имя электронной почты в имя субъекта' (Include e-mail name in subject name) checkbox is unchecked. The 'Включить эту информацию в альтернативное имя субъекта:' (Include this information in the subject's alternative name:) section has four checkboxes: 'Имя электронной почты' (E-mail name) is unchecked, 'DNS-имя' (DNS name) is unchecked, 'Имя субъекта-пользователя (UPN)' (User principal name (UPN)) is checked, and 'Имя субъекта-службы (SPN)' (Service principal name (SPN)) is unchecked. At the bottom, a note states: '* Элемент управления отключен из-за параметров совместимости.' (The control is disabled due to compatibility parameters). The 'Отмена' (Cancel) button is highlighted with a red rectangle.

Предоставляется в запросе

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

- Сертификаты для защиты электронной почты (электронная подпись, шифрование) с назначением «Защита электронной почты» (Secure Email, OID 1.3.6.1.5.5.7.3.4)

- Сертификаты с назначением «Подпись документов» (Document Signing, OID 1.3.6.1.4.1.311.10.3.12)
- ГОСТ-сертификаты для защиты электронной почты и подписи документов

 ПРИМЕЧАНИЕ

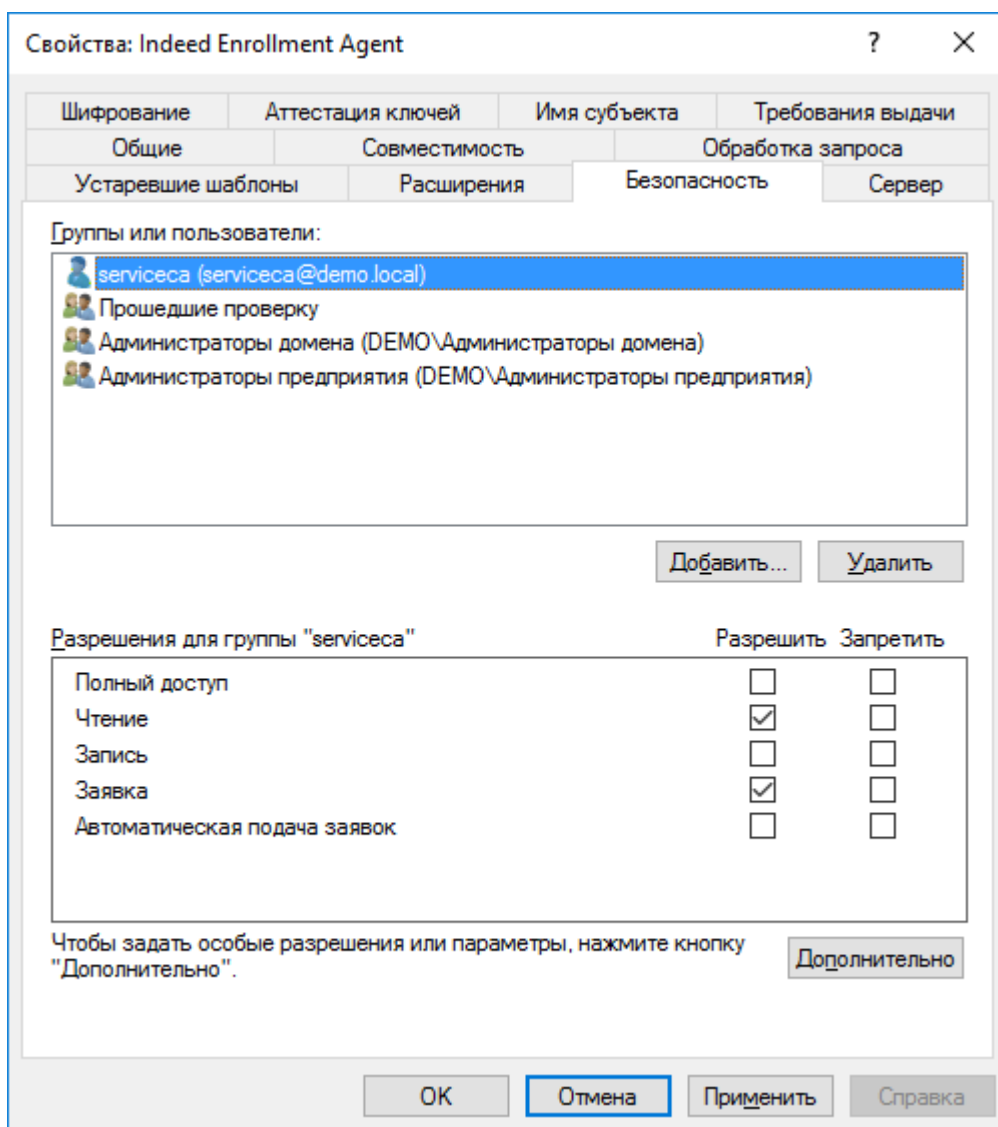
Имя субъекта сертификата будет сформировано из запроса на сертификат. Атрибуты для формирования имени субъекта (Subject) и альтернативного имени субъекта (Subject Alternative Name) можно указать в Консоли управления: **Конфигурация → Политики → Настройки PKI → Microsoft → Шаблоны**.

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

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

 ПРЕДУПРЕЖДЕНИЕ

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



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

Добавление шаблонов сертификатов

1. Откройте консоль управления **Центр сертификации** (Certification Authority) и дважды нажмите на имя ЦС.
2. Нажмите правой кнопкой мыши на контейнере **Шаблоны сертификатов** (Certificate Templates).
3. Выберите команду **Создать** (New), а затем пункт **Выдаваемый шаблон сертификата** (Certificate Template to Issue).
4. Выберите шаблон обязательного сертификата **Indeed Enrollment Agent**, а также все остальные шаблоны сертификатов (например, **Indeed Smart Card Logon**), которые будут выпускаться конечным пользователям системы.
5. Нажмите **ОК**.

Выпуск сертификата Агент регистрации

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

Сертификат можно создать:

- С помощью утилиты Cm.CertEnroll.MsCA
- В диспетчере сертификатов пользователя

Cm.CertEnroll.MsCA

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

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

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

Пример

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

Результат работы утилиты

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

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

```
CA: msca.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.
```

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

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

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

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:

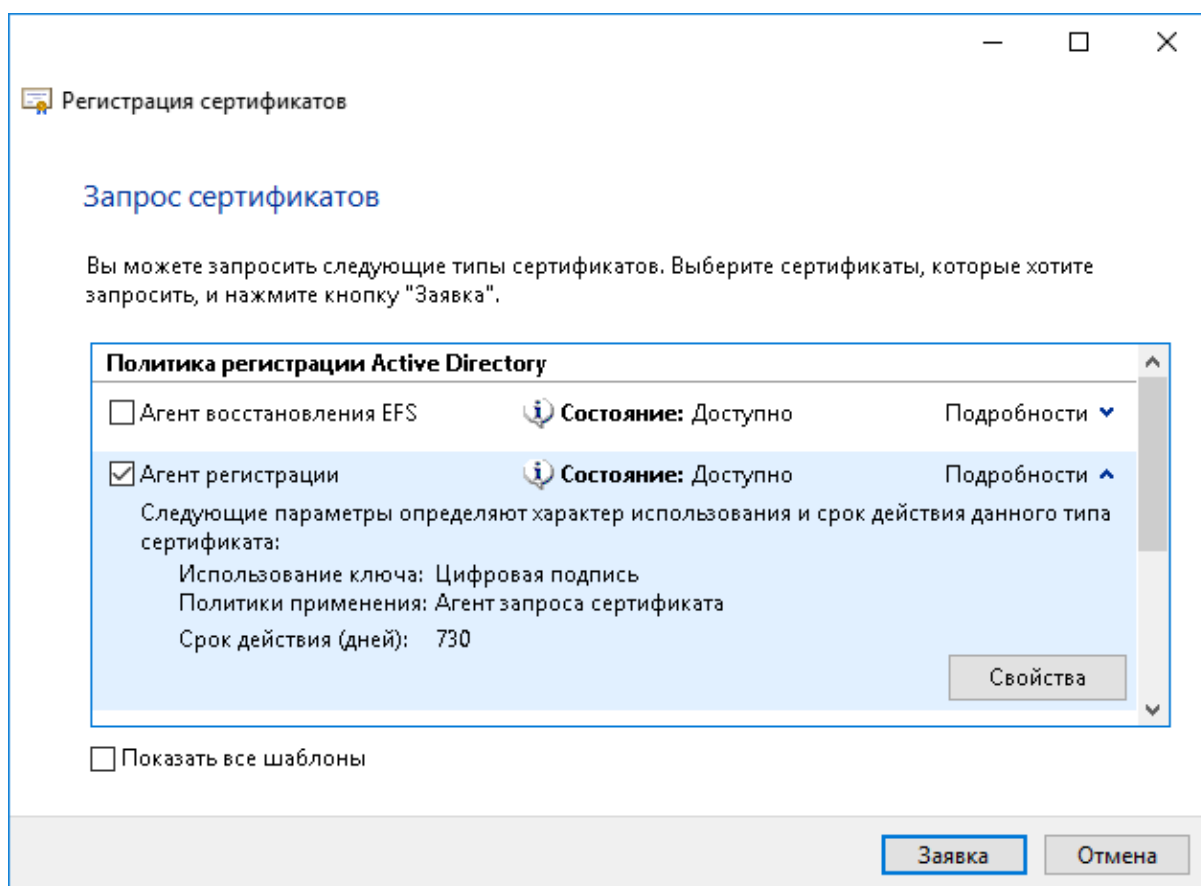
- `CAMachineName` – DNS-имя сервера с ролью ЦС
- `CAName` – имя ЦС

Пример запуска с указанием ЦС

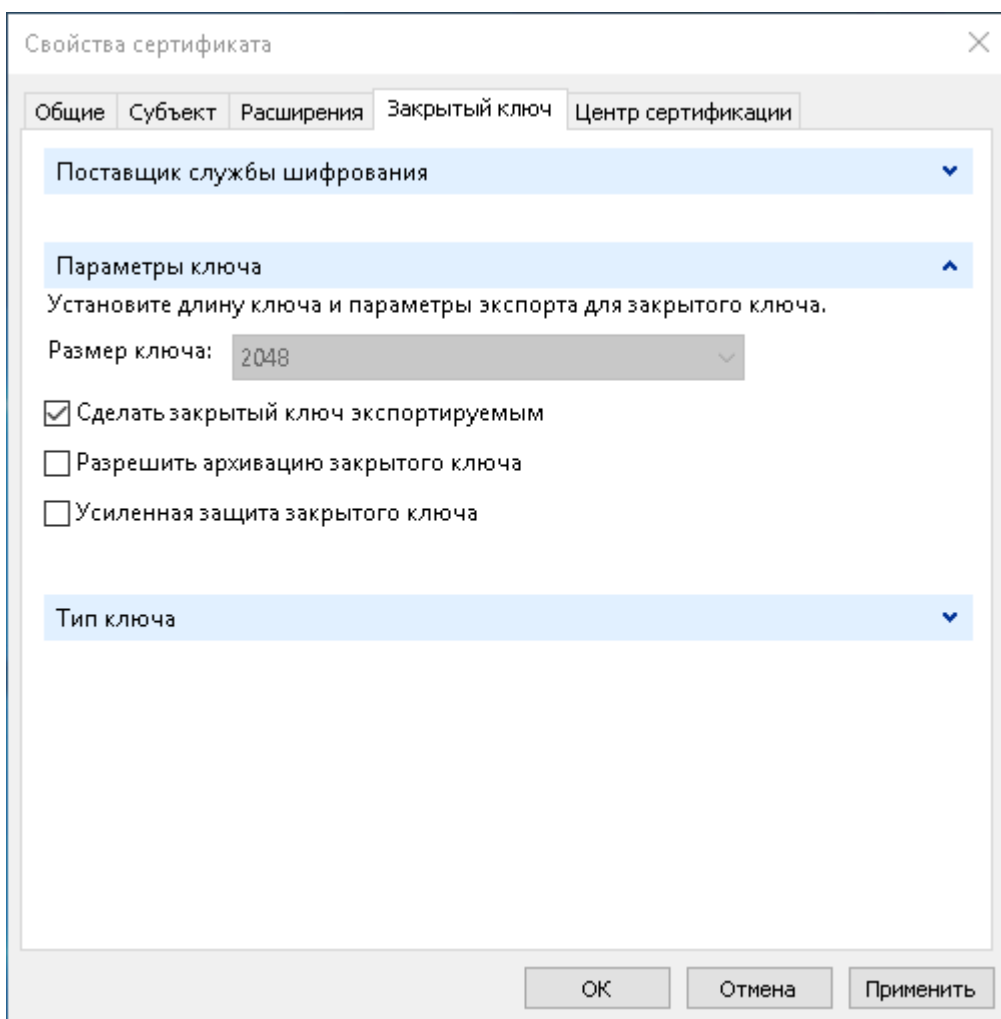
```
Cm.CertEnroll.MsCA.exe /e serviceca p@ssw0rd  
/t="IndeedEnrollmentAgent" /c="msca.domain.loc\Indeed-Demo-CA"
```

Диспетчер сертификатов

1. Выполните вход в систему под сервисной учетной записью и откройте оснастку **Сертификаты** (Certificates) пользователя (certmgr.msc).
2. Запустите мастер выпуска нового сертификата.
3. Выберите тип сертификата **Агент регистрации** (Enrollment Agent), разверните окно подробной информации и перейдите в **Свойства** (Properties).



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



5. Переместите выпущенный сертификат и его закрытый ключ в хранилище сертификатов компьютера, на котором развернут сервер Indeed CM.
6. Выдайте сервисному пользователю права на чтение закрытого ключа сертификата **Агент регистрации** (Enrollment Agent).
 1. Перейдите в оснастку **Сертификаты** (Certificates) компьютера и нажмите правой кнопкой мыши на сертификате.
 2. Выберите **Все задачи** (All tasks) → **Управление закрытыми ключами...** (Manage Private Keys...).
 3. Нажмите **Добавить** (Add), укажите сервисную учетную запись.
 4. Выставьте право **Полный доступ** (Full control).
 5. Нажмите **Применить** (Apply).

Подключение к Microsoft CA через Indeed CM MS CA Proxy

Indeed Certificate Manager может взаимодействовать с ЦС Microsoft, которые находятся за пределами домена сервера Indeed CM, с помощью компонента Indeed CM MS CA Proxy.

Примеры конфигурации:

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

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

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

Установка и настройка

1. **Создайте** во внешнем для системы домене сервисную учетную запись для работы с ЦС Microsoft.
2. **Настройте** для сервисной учетной записи шаблон **Агент регистрации** и **выпустите** для этой учетной записи сертификат по этому шаблону. Сертификат **Агент регистрации** должен располагаться в **Хранилище сертификатов рабочей станции** (Local computer), на которую устанавливается компонент 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 системы 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**.

```
"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**.

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

4. В секции `authSettings` в параметре `allowedCertificateThumbprints` укажите отпечаток сертификата **Агент регистрации**. 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.

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

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).

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.

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

Создание сервисной учетной записи для работы с КриптоПро УЦ

Описанный ниже вариант создания сервисной учетной записи является рекомендуемым, но не единственным. Вы можете создать учетную запись пользователя и выпустить сертификат 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>/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.
7. Завершите регистрацию.
8. В Консоли управления ЦР одобрите запрос на регистрацию нового пользователя.
9. 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:

1. Создайте шаблон сертификата агента подачи заявок для сервисной учетной записи Indeed CM.
2. Получите сертификат.
3. Установите сертификат в хранилище корневых сертификатов компьютера.

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 **ОК**.
9. Нажмите **Применить**.

Получение сертификата

1. На рабочей станции, где установлен сервер Indeed CM, выполните вход в личный кабинет пользователя КристоПро 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 КристоПро 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 развернуто 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 сертификата в личное хранилище компьютера

Выберите инструкцию в зависимости от ОС рабочей станции, где устанавливается сертификат.

Windows

Чтобы установить сертификат в личное хранилище компьютера:

1. Откройте приложение КриптоПро CSP.
2. Перейдите на вкладку **Сервис**.
3. В разделе **Личный сертификат** нажмите **Установить личный сертификат...**
Откроется Мастер установки личного сертификата.
4. Укажите путь к файлу сертификата. Выберите сертификат агента подачи заявок.
Нажмите **Далее**.



ПРЕДУПРЕЖДЕНИЕ

Не устанавливайте пароль на контейнер закрытого ключа сертификата агента подачи заявок при установке сертификата.

5. Включите опцию **Найти контейнер автоматически**. В качестве хранилища контейнера определится **Реестр**.
6. В блоке **Введенное имя задает ключевой контейнер** выберите **Компьютера** и нажмите **Далее**.
7. Завершите установку сертификата.

Выдайте Indeed CM права на чтение закрытого ключа сертификата сервисной учетной записи:

1. Перейдите в оснастку **Сертификаты** (Certificates) компьютера, на котором установлен сервер Indeed CM.
2. Правой кнопкой мыши нажмите на сертификат, 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**, нажмите **Проверить имена** (Check Names) и **ОК**.
6. Выставите права **Полный доступ** (Full Control) и **Чтение** (Read).
7. Нажмите **Применить** (Apply).
8. В хранилище **Локального компьютера** (Local computer), на котором установлен сервер Indeed CM, установите сертификат корневого центра сертификации КристоПро УЦ 2.0 в список **Доверенных Корневых Центров Сертификации** (Trusted Root Certification Authorities).
9. В хранилище **Локального компьютера** (Local Computer), на котором установлен сервер Indeed CM, установите список отозванных сертификатов (CRL) центра сертификации КристоПро УЦ 2.0 в **Промежуточные Центры Сертификации** (Intermediate Certification Authorities).

Linux

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

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
```

3. Выполните вход от имени пользователя `www-data`:

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

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

```
/opt/cprocsp/bin/amd64/certmgr -install -pfx -file <путь к файлу PFX> -pin <пароль от файла PFX>
```

3. Поместите корневой сертификат в локальное хранилище корневых сертификатов пользователя:

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

4. Добавьте корневой сертификат в список доверенных корневых сертификатов:

Debian-based

1. Поместите корневой сертификат в хранилище доверенных корневых сертификатов:

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

2. Обновите хранилище доверенных корневых сертификатов:

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

3. Перезапустите систему:

```
sudo reboot
```

Настройка аутентификации в веб-сервисах Indeed CM по сертификатам

Чтобы настроить аутентификацию в веб-сервисах Indeed Certificate Manager по сертификатам:

1. Получите сертификат аутентификации сервера КристоПро УЦ 2.0.
2. Установите сертификат в личное хранилище компьютера.

Получение сертификата

1. Зарегистрируйте нового пользователя КристоПро УЦ. В качестве имени пользователя укажите FQDN сервера Indeed CM.
2. На рабочей станции, где установлен сервер Indeed CM, войдите в личный кабинет пользователя КристоПро 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**.

Установка сертификата в личное хранилище компьютера

Выберите инструкцию в зависимости от ОС рабочей станции, где устанавливается сертификат.

Windows

Чтобы установить сертификат в личное хранилище компьютера:

1. Откройте приложение КриптоПро CSP.
2. Перейдите на вкладку **Сервис**.
3. В разделе **Личный сертификат** нажмите **Установить личный сертификат...**
Откроется Мастер установки личного сертификата.
4. Укажите путь к файлу сертификата. Выберите сертификат рабочей станции, на которой установлен сервер Indeed CM. Нажмите **Далее**.



ПРЕДУПРЕЖДЕНИЕ

Не устанавливайте пароль на контейнер закрытого ключа при установке сертификата.

5. Включите опцию **Найти контейнер автоматически**. В качестве хранилища контейнера определится **Реестр**.
6. В блоке **Введенное имя задает ключевой контейнер** выберите **Компьютера** и нажмите **Далее**.
7. Завершите установку сертификата.

Выдайте Indeed CM права на чтение закрытого ключа сертификата:

1. Перейдите в оснастку **Сертификаты** (Certificates) компьютера, на котором установлен сервер Indeed CM.
2. Правой кнопкой мыши нажмите на сертификат, 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**, нажмите **Проверить имена** (Check Names) и **ОК**.
6. Выставите права **Полный доступ** (Full Control) и **Чтение** (Read).
7. Нажмите **Применить** (Apply).

Linux

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

1. Проверьте наличие пользователя `www-data`:

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

Пример вывода, если пользователь `www-data` существует, и вход запрещен

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

2. Если пользователь `www-data` существует, и вход запрещен, смените оболочку на `/bin/bash`:

```
sudo usermod -s /bin/bash www-data
```

Если пользователя www-data не существует, выполните:

```
sudo useradd -m -d /var/www -s /bin/bash www-data
```

3. Проверьте результат:

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

Пример вывода, если пользователь www-data существует, и можно выполнить вход

```
www-data:x:33:33:www-data:/var/www:/bin/bash
```

4. Выполните вход от имени пользователя www-data:

```
sudo su www-data
```

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

```
/opt/cprocsp/bin/amd64/certmgr -install -pfx -file <путь к файлу PFX> -pin <пароль от файла PFX>
```

3. Поместите корневой сертификат в локальное хранилище корневых сертификатов пользователя:

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

4. Добавьте корневой сертификат в список доверенных корневых сертификатов:

Debian-based

1. Поместите корневой сертификат в хранилище доверенных корневых сертификатов:

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

2. Обновите хранилище доверенных корневых сертификатов:

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

3. Перезапустите систему:

```
sudo reboot
```

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



ПРИМЕЧАНИЕ

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 по отношению к КриптоПро УЦ 2.0. Создание и обновление пользователей, запрос сертификатов и прочие действия на УЦ в этом случае выполняются от имени **Оператора DSS**. Подробная инструкция по интеграции входит в комплект поставки ПАК "КриптоПро DSS".

Настройка интеграции

Для работы с КриптоПро DSS используется учетная запись Оператор DSS, сертификат которой должен храниться на сервере Indeed CM.

Выберите инструкцию в зависимости от ОС рабочей станции, где устанавливается сертификат Оператора DSS.

Чтобы установить сертификат Оператора DSS:

Windows

1. Добавьте сертификат Оператора DSS в **Локальное хранилище компьютера** (Local Computer) на сервере Indeed CM.
2. Добавьте корневой сертификат КриптоПро УЦ 2.0 и корневой сертификат DSS в **Доверенные корневые центры сертификации** (Trusted Root Certification Authorities) на сервере Indeed CM.
3. Выдайте системе права на чтение закрытого ключа сертификата Оператора DSS:
 1. Перейдите в оснастку **Сертификаты** (Certificates) компьютера, на котором установлен сервер Indeed CM.
 2. Правой кнопкой мыши нажмите на сертификат, 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 **ИИ_ИUSRS**, нажмите **Проверить имена** (Check Names) и **ОК**.
 6. Выставьте права **Полный доступ** (Full Control) и **Чтение** (Read).
 7. Нажмите **Применить** (Apply).
4. Выдайте права на папку с пользователями в КриптоПро УЦ 2.0 для учетной записи Оператор DSS:
 1. Создайте группу безопасности, например, **DSS Operators**, и добавьте в нее учетную запись Оператор DSS.
 2. Откройте свойства папки, где будут располагаться пользователи DSS, перейдите на вкладку **Безопасность** (Security) и добавьте созданную группу **DSS Operators**.
 3. Выдайте группе следующие права:

▼ **Права для сервисной группы пользователей DSS Operators**

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

Наименование разрешения	Тип объекта	Комментарий
Одобрение возобновления	Пользователь	Одобрение запроса на возобновление сертификата пользователя
Передача запросов	Пользователь	Передача запросов, подписанных пользователем-получателем услуги, а не подписью пользователя, передающего или одобряющего запрос.
Запрос переименования	Пользователь	Создание запроса на изменение данных пользователя.
Одобрение переименования	Пользователь	Одобрение запроса на изменение данных пользователя.

Linux

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

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
```

3. Выполните вход от имени пользователя www-data:

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

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

```
/opt/cprosp/bin/amd64/certmgr -install -pfx -file <путь к файлу PFX> -pin <пароль от файла PFX>
```

3. Поместите корневой сертификат DSS в локальное хранилище корневых сертификатов пользователя:

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

4. Добавьте корневой сертификат КриптоПро УЦ 2.0 и корневой сертификат DSS в список доверенных корневых сертификатов:

Debian-based

1. Поместите корневые сертификаты в хранилище доверенных корневых сертификатов:

```
sudo cp <путь к файлу1.crt> <путь к файлу2.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 корневые сертификаты в хранилище доверенных корневых сертификатов:

```
sudo cp <путь к файлу1.crt> <путь к файлу2.crt>  
/etc/pki/ca-trust/source/anchors/
```

2. Обновите хранилище доверенных корневых сертификатов:

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

3. Перезапустите систему:

```
sudo reboot
```

Валидата УЦ

Для настройки работы Indeed Certificate Manager с Валидата УЦ:

1. Настройте режим 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. Настройте шаблоны сертификатов пользователей.

Режим работы

Офлайн

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

- Корневой и промежуточные сертификаты Валидата УЦ
- Актуальный файл Списка Отозванных Сертификатов (СОС)
- 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

Для работы Indeed Certificate Manager с Валидата УЦ в онлайн-режиме:

1. Предоставьте доступ на чтение и запись к каталогу для обмена файлами с Центром Сертификации Валидата.

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 выполнения аутентификации по протоколу TLS, так и для подписания XML-шаблона на получение или отзыв сертификата ключа проверки ЭП пользователя.

Сертификат Оператора ЦР должен содержать значения Оператор Центра Регистрации (OID: 1.3.6.1.4.1.10244.6.1) и Проверка подлинности TLS клиента (OID: 1.3.6.1.5.5.7.3.2).

Сертификат Оператора ЦР можно выпустить с помощью 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 пункт **Центр Регистрации** → **Сформировать запрос на сертификат абонента**.
2. В появившемся окне выберите шаблон, если он был подготовлен ранее, и нажмите **Далее**.
3. Заполните атрибуты сертификата для построения **Имени Владельца сертификата**, установите опцию **Разрешить генерацию ключа шифрования**, если требуется, и нажмите **Далее**.
4. Выберите область применения ключа **Оператор ЦР** и **Проверка подлинности TLS клиента** и нажмите **Далее**.
5. Определите регламент сертификата и нажмите **Далее**.
6. Настройте дополнения для сертификата и нажмите **Далее**.
7. При необходимости настройте атрибуты альтернативного имени владельца сертификата и нажмите **Готово**.

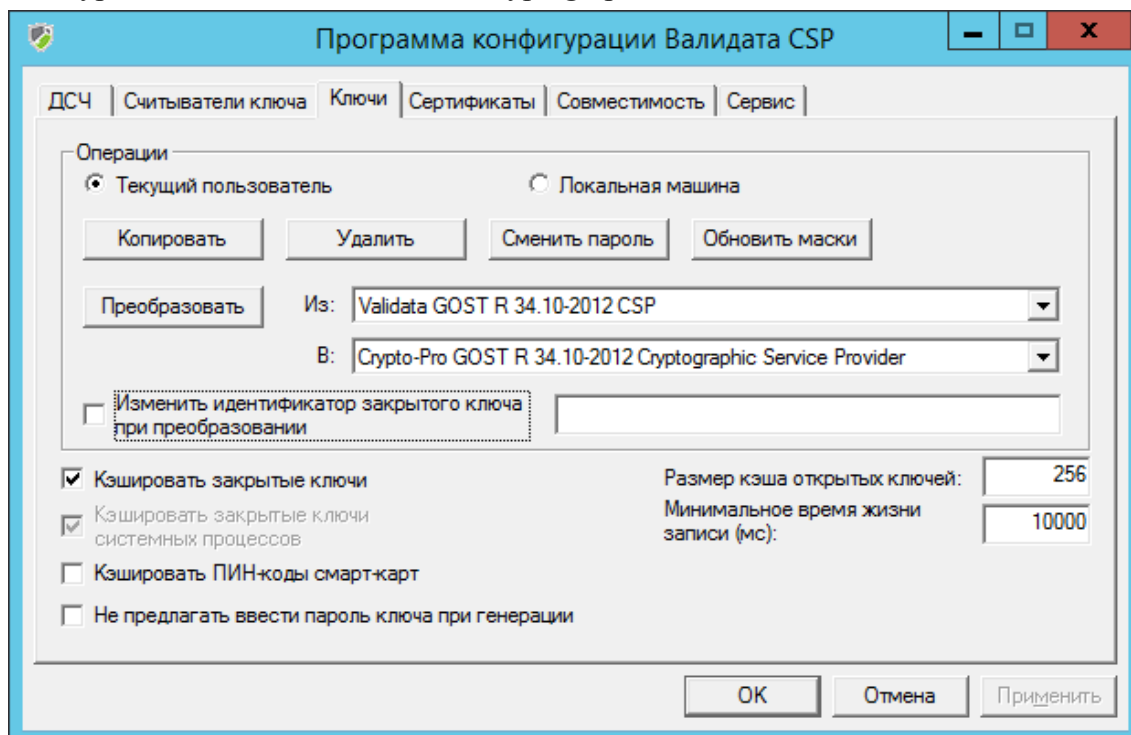
Преобразование закрытого ключа сертификата

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

1. Запустите от имени администратора приложение Validata CSP.

2. Перейдите на вкладку **Ключи**. В поле **Преобразовать** выберите соответствующие поля:

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



3. Следуя подсказкам мастера, преобразуйте закрытый ключ сертификата Оператора ЦР в Crypto-Pro GOST R 34.10-2012 CSP.
4. Установите преобразованный ключ и сертификат Оператора ЦР в контейнер локального хранилища рабочей станции (сервера Indeed CM).
5. Выдайте системе права на чтение закрытого ключа сертификата Оператора, который был установлен на предыдущем шаге:
 1. Перейдите в оснастку **Сертификаты** (Certificates) компьютера, на котором установлен сервер Indeed CM.
 2. Нажмите правой кнопкой мыши на сертификате, выберите **Все задачи** (All tasks) → **Управление закрытыми ключами...** (Manage Private Keys...).
 3. Нажмите **Добавить** (Add), укажите сервер в меню **Размещение** (Location), укажите локальную группу **IIS_IUSRS** в поле **Введите имена выбранных объектов** (Enter the object names to select), нажмите **Проверить имена** (Check Names) и **ОК**.
 4. Выставьте права **Полный доступ** (Full Control) и **Чтение** (Read).
 5. Нажмите **Применить** (Apply).

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

Шаблоны сертификатов пользователей

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

Процесс настройки шаблона сертификата пользователя в Центре Регистрации Валидата УЦ:

1. В основном меню АРМ Оператора или Администратора ЦР выберите пункт **Центр Регистрации → Создать новый шаблон сертификата**.
2. В появившемся окне укажите **Наименование шаблона** и нажмите **Далее**.
3. Заполните атрибуты сертификата для построения **Имени Владельца сертификата**. При необходимости установите опцию **Разрешить генерацию ключа шифрования**, чтобы создать ключ шифрования для сертификата. Если опция не выбрана, то пользователю, для которого создается сертификат, будет запрещено иметь ключ шифрования.

▼ Поддерживаемые атрибуты для построения X.500-имени пользователя

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

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

▼ **Поддерживаемые атрибуты для построения альтернативного имени владельца сертификата**

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

Создание нового шаблона сертификата

Задание альтернативного имени Владельца сертификата

Заполните дополнительные сведения о Владельце сертификата

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

< Назад Готово Отмена

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

▼ **Пример отредактированного шаблона**

```

<?xml version="1.0" encoding="UTF-8" ?>
<pkiUser>
  <templateName>Квалифицированный сертификат</templateName>
  <templateSubject>
    <INN></INN>
    <INNLE></INNLE>
    <OGRNIP></OGRNIP>
    <OGRN></OGRN>
    <SNILS></SNILS>
    <T></T>
    <SN></SN>
    <GN></GN>
    <Email></Email>
    <CN></CN>
    <OU></OU>
    <O></O>
    <street></street>
    <L></L>
    <ST></ST>
    <C></C>
  </templateSubject>
  <subjectAltName>
    <UPN></UPN>
    <emailAddress></emailAddress>
    <description>СЗ № $docNumber от $docDate</description>
  </subjectAltName>
  <ExtKeyUsage>1.3.6.1.5.5.7.3.2</ExtKeyUsage>
  <ExtKeyUsage>1.3.6.1.5.5.7.3.4</ExtKeyUsage>
  <Policy>
    <OID>1.2.643.100.113.1</OID>
    <UserNotice>Класс средства ЭП КС1</UserNotice>
    <Org>Минкомсвязь России</Org>
  </Policy>
  <Policy>
    <OID>1.2.643.100.113.2</OID>
    <UserNotice>Класс средства ЭП КС2</UserNotice>
  </Policy>

```

```
    <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>
```

Браузеры

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*

Установка расширения 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. Нажмите **Добавить** во всплывающем окне.

Установка и настройка серверных КОМПОНЕНТОВ

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

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

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



Indeed CM Server

Установка сервера Indeed CM



Мастер настройки

Настройка файлов конфигурации сервисов Indeed CM в Мастере настройки



Сервер OpenID Connect

Настройка сервера OpenID Connect



Единый журнал событий

Настройка записи событий в общий журнал



Indeed CM Agent

Настройка клиентского агента

Indeed CM Server

Indeed CM состоит из следующих сервисов:

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

ⓘ ПРИМЕЧАНИЕ

Каждый сервис имеет собственные файлы конфигурации и настройки доступа.

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

Windows

1. Запустите файл *IndeedCM.Server-<номер версии>.x64.ru-ru.msi* из каталога *IndeedCM.WindowsServer* дистрибутива системы и установите сервер, следуя указаниям мастера.
2. Выберите способ контроля доступа для всех приложений системы: аутентификация Windows, OpenID Connect или по персональным сертификатам пользователей.

Windows

При выборе аутентификации Windows автоматически устанавливаются следующие параметры контроля доступа:

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

OpenID Connect

При выборе аутентификации OpenID Connect автоматически устанавливаются следующие параметры контроля доступа:

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

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

По сертификатам



ПРЕДУПРЕЖДЕНИЕ

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

При выборе аутентификации по персональным сертификатам пользователей автоматически устанавливаются следующие параметры контроля доступа:

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

(api), Сервис агентов (agentserviceapi).

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



ПРЕДУПРЕЖДЕНИЕ

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

3. Выпустите SSL/TLS-сертификат.

▼ Требования к SSL/TLS-сертификату для IIS

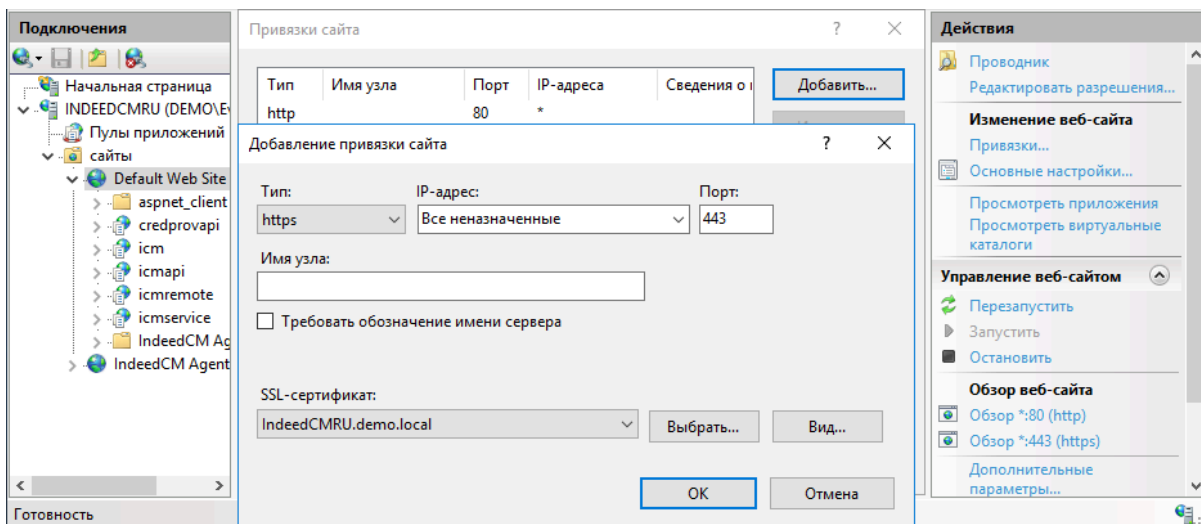
Субъект (Subject) сертификата должен содержать атрибут **Общее имя** (Common name) (FQDN сервера Indeed CM).

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 **ОК**.



Linux

Debian-based

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

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

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

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

RHEL-based

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

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

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

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

3. Настройте управление приложениями.

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

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

❗ **ПРИМЕЧАНИЕ**

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

Пример команды для создания пользователя `www-data`

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

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

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

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

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

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

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



ПРЕДУПРЕЖДЕНИЕ

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

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

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

Debian-based

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

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

RHEL-based

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

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

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

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

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

▼ Как еще получить код аутентификации

Способ 1. Запустите службу `cm-wizard.service`. Код сохранится в файл `wizard_authentication_code.txt` в каталоге `/opt/indeed/cm/wizard/logs`.

Способ 2. Выполните команду `systemctl status`:

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

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

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

Код аутентификации выводится на экран терминала.

Функции системы

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

Журнал событий

Настройте работу журнала событий.

1. Укажите атрибут, по значению которого выполняется поиск пользователей в журнале событий. Значение по умолчанию: CN (Common name).
2. Выберите опцию:
 - **Использовать локальный журнал Windows**, чтобы записывать события с одного или нескольких серверов в единый журнал Windows.
 - **Использовать Log Server**, чтобы записывать события с нескольких серверов Indeed CM в единый журнал Windows, SysLog, базу данных Microsoft SQL или PostgreSQL.

▼ Использовать локальный журнал Windows

События будут записываться в локальный журнал Windows.

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

1. Установите и настройте приложение Indeed CM Event Log Proxy. [Инструкция по установке Indeed CM Event Log Proxy](#)
2. Включите опцию **Включить Event Log Proxy**.
3. Укажите URL подключения к Event Log Proxy. Например,
`https://server.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, вы можете использовать приложение Indeed Log Server, чтобы все серверы записывали события в единый журнал Windows, SysLog, базу данных Microsoft SQL или PostgreSQL.

1. Установите и настройте приложение Indeed Log Server. [Инструкция по установке Indeed Log Server](#)
2. Укажите URL подключения к Indeed Log Server. Например,
`https://server.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 параметры работы с удостоверяющими центрами.

▼ Microsoft CA

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

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

▼ КристоПро УЦ 2.0

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

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

При необходимости укажите информацию о расположении пользователей в Центре Регистрации:

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

▼ КристоПро DSS

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

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

▼ Валидата УЦ

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

AirCard Enterprise

Укажите настройки интеграции с Indeed AirCard Enterprise:

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

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

1. Остановите сервисы агентов `agentregistrationapi` и `agentserviceapi` на сервере Indeed CM.
 2. Удалите все клиентские агенты в разделе **Агенты** Консоли управления или выполните запрос в базу данных Indeed CM, чтобы удалить зарегистрированные агенты и их сессии.
 3. Примените изменения в Мастере настройки и распространите измененный файл конфигурации сервиса `agentregistrationapi` на сервере Indeed CM.
 4. Запустите сервисы агентов `agentregistrationapi` и `agentserviceapi`.
4. Чтобы регистрировать агенты без подтверждения администратора, включите опцию **Автоматическая регистрация Агентов**. После установки и настройки агента на рабочей станции он появится в разделе **Агенты** Консоли управления Indeed CM со статусом *Зарегистрирован*.
5. Загрузите сертификат агента – файл корневого сертификата сервисов агента с закрытым ключом в формате JSON `agent_root_ca.json`.
6. Выберите **Уровень журналирования событий агентом**.
7. Укажите **Периодичность получения данных с сервера** и **Интервал повторного выполнения отмененной пользователем задачи**.
8. Имя заголовка HTTP-запроса сертификата указано по умолчанию. Если Indeed CM используется с балансировщиком нагрузки, включите опцию **Передавать только поле 'Субъект' сертификата агента в заголовках HTTP-запросов**, чтобы снизить трафик.

Каталог пользователей

Настройте подключение к каталогу пользователей Indeed CM. Можно использовать несколько каталогов пользователей. [Как создать каталог пользователей](#)

LDAP

Нажмите **Добавить** и выберите тип каталога пользователей: Active Directory, FreeIPA или ALD Pro.

Active Directory

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

FreeIPA и ALD Pro

1. Укажите данные учетной записи, у которой есть права на доступ к каталогу пользователей: имя в формате Distinguished Name и пароль.
2. Укажите NetBIOS-имя домена.
3. Укажите DNS-имя домена или контроллера домена.
4. Укажите путь к объекту с пользователями в формате Distinguished Name.
Рекомендуем указать корень домена или каталог accounts.
5. Если вы используете протокол LDAPS для доступа к каталогам, включите опцию **Использовать LDAPS**.

6. Нажмите **Сохранить**.

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

В качестве внутреннего каталога пользователей можно использовать 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 можно указать 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**. Для целочисленного атрибута можно указать 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 между атрибутами удостоверяющего центра и атрибутами пользователей в каталоге.

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

Обновляемые атрибуты

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

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

ПРИМЕЧАНИЕ

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

Чтобы отслеживать атрибут:

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

Контроль доступа

Выберите способ контроля доступа к сервисам Indeed CM:

- **Аутентификация Windows**

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

- **Аутентификация OpenID Connect**

Этот способ позволяет аутентифицироваться через **сервер OpenID Connect** и используется для инсталляций Indeed CM на доменной или внедоменной рабочей станции под управлением ОС Windows или Linux.

Перейдите в раздел **OpenID Connect** и укажите параметры подключения к серверу OpenID Connect.

 ПРЕДУПРЕЖДЕНИЕ

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

Администратор ролей

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

Укажите имя администратора ролей в формате 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
 - 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.

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"
```


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
```

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.

! ИНФОРМАЦИЯ

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, где установлен сервер Indeed CM.

Windows

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

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

Сертификат 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. Кликните правой кнопкой мыши на сертификате, 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 **PS_IUSRS**.
6. Нажмите **Проверить имена** (Check Names) и **ОК**.
7. Выставьте права **Полный доступ** (Full Control) и **Чтение** (Read).
8. Нажмите **Применить** (Apply).

Настройка файла appsettings.json

Настройте конфигурацию сервера OIDC:

1. Запустите **Мастер настройки**.
2. Перейдите в раздел **Контроль доступа** → **OpenID Connect**.
3. 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.
4. При необходимости сгенерируйте клиентские секреты.
5. **Примените настройки**.

После завершения работы Мастера в директории `C:\inetpub\wwwroot\cm\oidc` создается конфигурационный файл `appsettings.json`.

Аутентификация

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

▼ Подробнее об аутентификации Windows и Windows Custom

Выберите Windows, если сервер Indeed CM развернут на доменной рабочей станции под управлением ОС Windows.

Выберите WindowsCustom, если сервер Indeed CM развернут вне домена или пользователи домена, где находится каталог пользователей, находятся за пределами домена сервера Indeed CM, и с сервером нет трастовых отношений.

База 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*.

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

SQLite

Изменения не нужны. Секции имеют следующие значения:

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

Microsoft SQL

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

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

Перезагрузите сервер OIDC, чтобы применить изменения в конфигурационном файле.

PostgreSQL

Создайте базу данных в СУБД и настройте в файле подключение к этой базе данных.

Если вы используете файл PGPASS, не включайте директиву `Password` в строку подключения:

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

Перезагрузите сервер OIDC, чтобы применить изменения в конфигурационном файле.

▼ Пример заполненного файла конфигурации

```

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

```

```

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

```

```

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

```

Linux

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

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

Сертификат подписи JWT-токенов

В качестве сертификата подписи используйте сертификат и закрытый ключ, созданные для **веб-сервера**. Сертификат и закрытый ключ необходимо объединить в файл PFX, и поместить файл PFX в поддиректорию домашнего каталога пользователя, от имени которого запускается сервер OIDC.

По умолчанию сервер OIDC запускается от имени пользователя *www-data*. Поддиректория домашнего каталога пользователя *www-data* находится по пути */var/www/.dotnet/corefx/cryptography/x509stores/my/*.



ПОДСКАЗКА

Убедитесь, что пользователь *www-data* существует: выполните `/etc/passwd | grep www-data`.

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

Чтобы сменить пользователя, выполните `/etc/systemd/system/cm-<имя сервиса>.service`. Укажите имя пользователя в директиве `User`.

Чтобы подготовить сертификат подписи:

1. Создайте поддиректорию домашнего каталога пользователя, от имени которого запускается сервер OIDC (*www-data*):

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

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  
~/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
```

Настройка файла appsettings.json

Настройте конфигурацию сервера OIDC:

1. Запустите **Мастер настройки**.
2. Перейдите в раздел **Контроль доступа** → **OpenID Connect**.
3. 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.
4. При необходимости сгенерируйте клиентские секреты.
5. **Примените настройки**.

После завершения работы Мастера в директории `/opt/indeed/cm/oidc` создается конфигурационный файл `appsettings.json`.

База 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 будут храниться в каталоге `/opt/indeed/cm/oidc/data`.

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

SQLite

Внесение изменений не требуется. Секции имеют следующие значения:

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

Microsoft SQL

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

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

Перезагрузите сервер OIDC, чтобы применить изменения в конфигурационном файле.

PostgreSQL

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

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

Перезагрузите сервер OIDC, чтобы применить изменения в конфигурационном файле.

▼ Пример заполненного файла конфигурации

```

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

```

```

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

```

```

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

```

▼ Параметры файла appsettings.json

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

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



КАК УЗНАТЬ DNS-ИМЯ И NETBIOS-ИМЯ ДОМЕНА

Выполните в командной строке:

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

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

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 систему под управлением ОС Windows. Системные требования совпадают с **требованиями для установки серверных компонентов**.

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="DEMO\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.

Log Server можно установить на систему под управлением ОС Windows или Linux. Системные требования совпадают с **требованиями для установки серверных компонентов**.

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 системы и следуйте указаниям Мастера.
3. Из каталога *Log.Server* скопируйте:
 - Файл *cmSchema.config* в каталог *C:\inetpub\wwwroot\ls*.
 - Файлы *EventLogTarget.config*, *MsSqlTarget.config*, *PgSqlTarget.config* и *SysLogTarget.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**).

Поддерживается настройка чтения и записи событий в следующие хранилища:

- Windows Event Log
- MS SQL
- PostgreSQL
- Syslog

Windows Event Log

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

- В секции **Applications** добавьте:

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

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

```
<Targets>
  <Target Id="EventLogTarget" Type="eventlog"/>
</Targets>
```

2. Сохраните изменения и закройте файл конфигурации.

MS 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:

- 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 MS SQL или Active Directory. 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 `C:\inetpub\wwwroot\ls\targetConfigs` и отредактируйте файл `MsSqlTarget.config`. В секции `<Settings>...</Settings>` задайте 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=LogS
Id=servicesql;Password=P@ssw0rd;TrustServerCertificate=True</Con
</Settings>
```

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

- В секции `Application` добавьте:

```

<Application Id="cm" SchemaId="cmSchema">
  <ReadTargetId>MsSqlTarget</ReadTargetId>

  <WriteTargets>
    <TargetId>MsSqlTarget</TargetId>
  </WriteTargets>

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

```

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

```

<Targets>
  <Target Id="MsSqlTarget" Type="mssql"/>
</Targets>

```

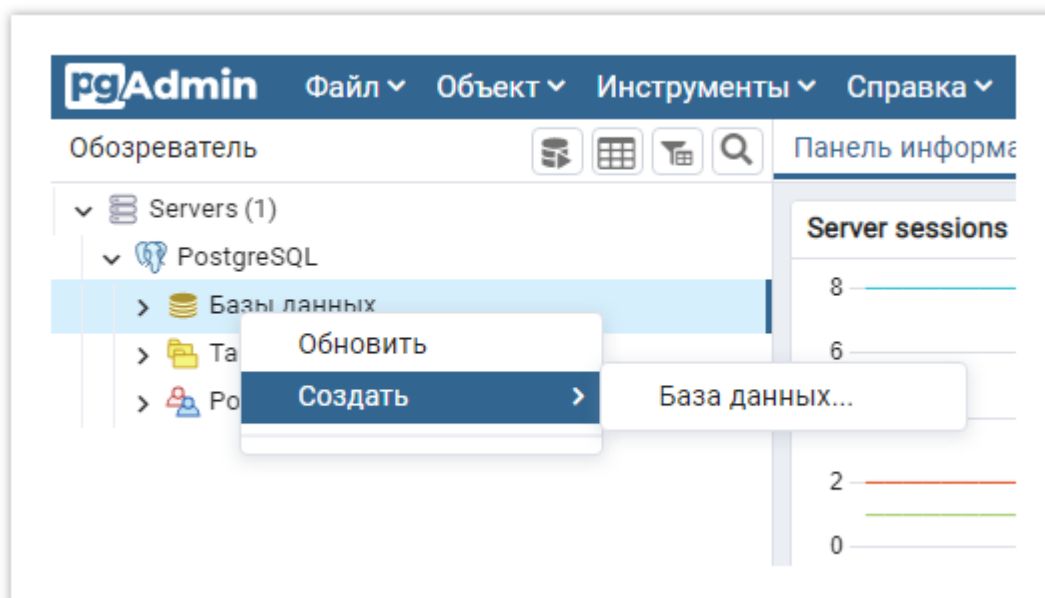
4. Сохраните изменения и закройте файл конфигурации.

PostgreSQL

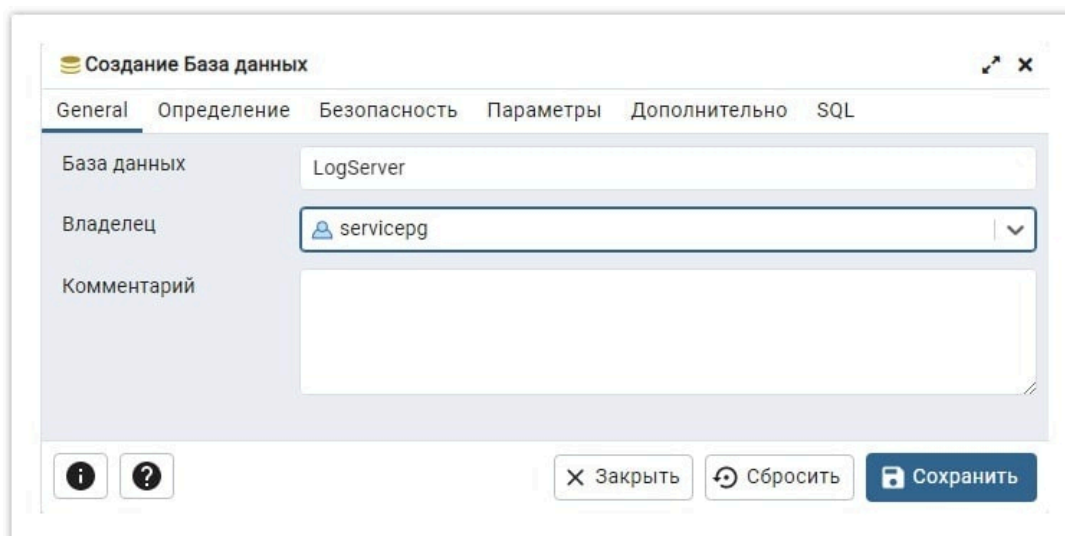
База для хранения данных Log Server создается вручную, а ее наполнение происходит автоматически.

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



2. Предоставьте сервисной учетной записи привилегии на таблицы базы данных:
 1. Выберите созданную базу данных 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. По умолчанию в PostgreSQL разрешены только локальные подключения к базам данных, поэтому для работы между различными серверами требуется настройка удаленного подключения к БД:

1. В каталоге PostgreSQL откройте конфигурационный файл *pg_hba.conf*. Файл находится в каталоге *C:\Program Files\PostgreSQL\<номер версии>\data*.
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
```

4. В каталоге *C:\inetpub\wwwroot\ls\targetConfigs* отредактируйте файл *PgSqlTarget.config*. В секции `<ConnectionString>...</ConnectionString>` задайте параметры:

- **Host** - имя сервера PostgreSQL Server.
- **Port** - порт для подключения к PostgreSQL (5432 — значение по умолчанию).

- `Database` - имя созданной в п.1 базы данных.
- `Username` - сервисная учетная запись для подключения к указанной базе данных.
- `Password` - пароль сервисной учетной записи.

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

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

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

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

  <WriteTargets>
    <TargetId>PgSqlTarget</TargetId>
  </WriteTargets>

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

- В секции `Targets` добавьте новый элемент:

```
<Targets>
  <Target Id="PgSqlTarget" 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 `SysLogTarget.config`. В секции `<ConnectionString>...</ConnectionString>` задайте 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>PgSqlTarget</ReadTargetId>

    <WriteTargets>
      <TargetId>PgSqlTarget</TargetId>
      <TargetId>SysLogTarget</TargetId>
    </WriteTargets>

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

```

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

```

<Targets>
  <Target Id="PgSqlTarget" Type="pgsql"/>
  <Target Id="SysLogTarget" 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).

Установка

Debian-based

1. Установите Log Server из DEB пакета *indeed.logserver-<номер версии>_amd64.deb*.

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

RHEL-based

1. Установите Log Server из RPM-пакета *indeed.logserver-<номер версии>.x86_64.rpm*:

```
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**).

Поддерживается настройка чтения и записи событий в следующие хранилища:

- MS SQL
- PostgreSQL
- Syslog

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 MS SQL или Active Directory. 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 `MsSqlTarget.config`. В секции `<Settings>...</Settings>` задайте 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=LogS
Id=servicesql;Password=P@ssw0rd;TrustServerCertificate=True</Con
</Settings>
```

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

- В секции `Application` добавьте:

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

  <WriteTargets>
    <TargetId>MsSqlTarget</TargetId>
  </WriteTargets>

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

- В секции `Targets` добавьте новый элемент:

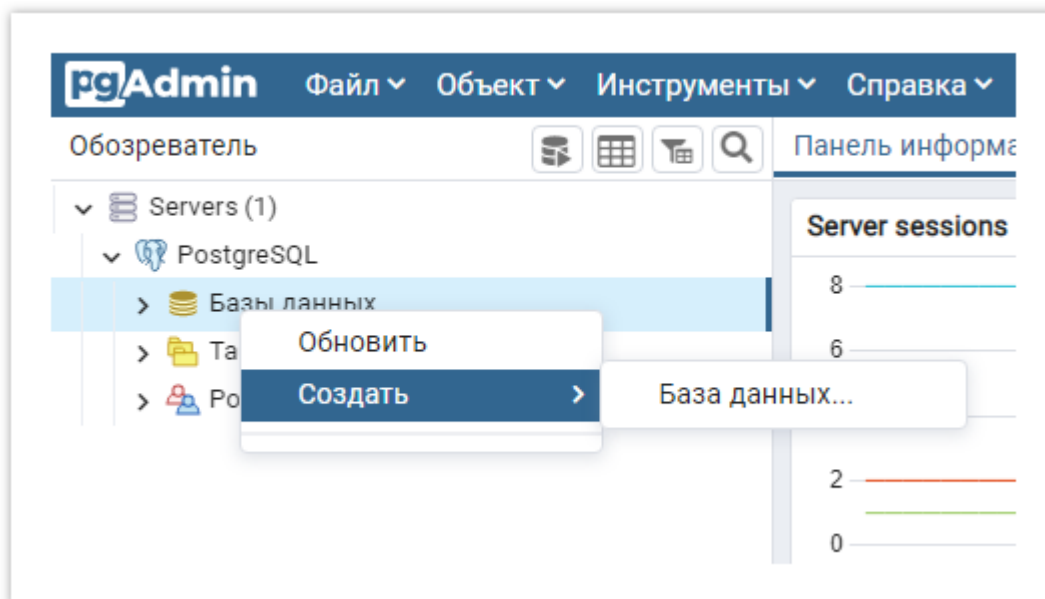
```
<Targets>
  <Target Id="MsSqlTarget" Type="mssql"/>
</Targets>
```

PostgreSQL

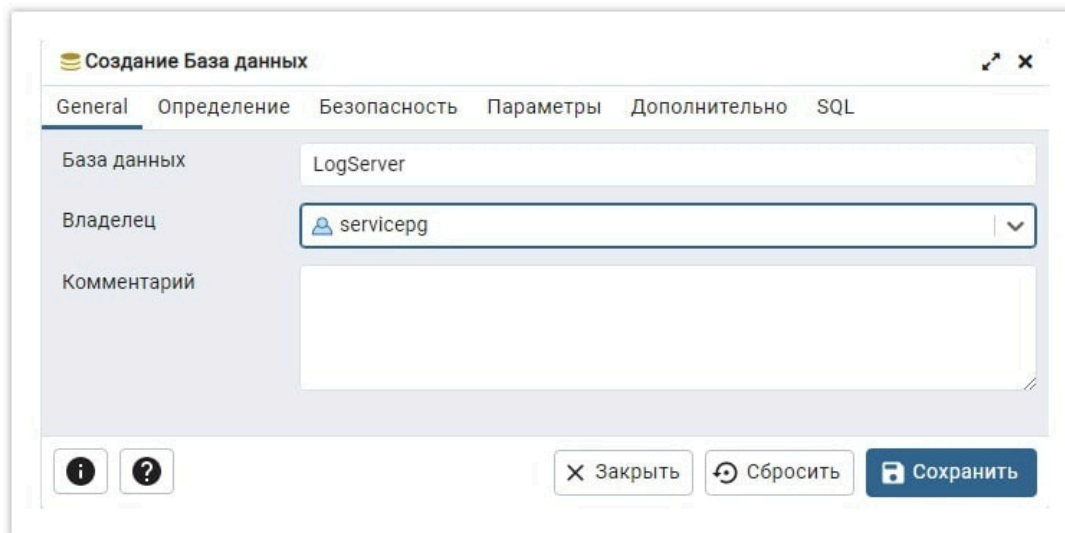
База для хранения данных Log Server создается вручную, а ее наполнение происходит автоматически.

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

1. В каталоге PostgreSQL откройте конфигурационный файл *pg_hba.conf*. Файл находится в каталоге */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
```

4. В каталоге */opt/indeed/ls/targetConfigs* отредактируйте файл *PgSqlTarget.config*. В секции **<ConnectionString>...</ConnectionString>** задайте параметры:

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

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

5. 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>PgSqlTarget</ReadTargetId>

  <WriteTargets>
    <TargetId>PgSqlTarget</TargetId>
  </WriteTargets>

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

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

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


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

1. В каталоге `/opt/indeed/ls/targetConfigs` отредактируйте файл `SysLogTarget.config`. В секции `<ConnectionString>...</ConnectionString>` задайте параметры:

- `HostName` - имя или IP-адрес Syslog сервера.
- `Port` - порт Syslog сервера. Порт по умолчанию — 514.
- `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>PgSqlTarget</ReadTargetId>

    <WriteTargets>
      <TargetId>PgSqlTarget</TargetId>
      <TargetId>SysLogTarget</TargetId>
    </WriteTargets>

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

- В секции `Targets` добавьте новый элемент:

```
<Targets>
  <Target Id="PgSqlTarget" Type="pgsql"/>
  <Target Id="SysLogTarget" 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 Indeed CM. [Инструкция для подключения журнала событий](#)

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 после развертывания Indeed CM.

С помощью агента на рабочих станциях пользователей в автоматическом режиме 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 истечении заданного количества дней
- Блокировка и сброс PIN-кода пользователя
- Обновление содержимого устройства
- Очистка и инициализация устройства при отзыве
- Смена PIN-кода администратора устройства
- Контроль использования устройств и блокировка пользовательской сессии и устройства
- Мониторинг устройств с информацией об устройствах с заблокированным PIN-кодом пользователя и администратора, о попытках ввода неверного PIN-кода и о подключении незарегистрированных устройств.

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

Установка и настройка

Выберите инструкцию в зависимости от ОС, где установлен сервер Indeed CM:

Windows

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

1. **Создайте** сертификаты сервисов агента.
2. **Настройте** защищенное соединение с сайтом сервисов агента.
3. **Настройте** Indeed CM для работы с клиентскими агентами.

4. **Установите и настройте** агенты на рабочих станциях.

Создание сертификатов сервисов агента

Для работы агента требуются следующие сертификаты:

- **CM Agent CA** – корневой сертификат сервисов агента. Используется для выдачи сертификатов рабочим станциям пользователей, на которых будут устанавливаться агенты.
- **CM Agent SSL** – сертификат проверки подлинности, подписан корневым сертификатом. Необходим для установки двустороннего защищенного соединения между сервером и рабочей станцией с установленным агентом. Сертификат выдается на имя рабочей станции, на которой развернут сервер Indeed CM.
- **Сертификат рабочей станции** – выдается автоматически при регистрации агента. Обращаясь к серверу, клиентский компьютер предоставляет свой сертификат, а сервер Indeed CM проверяет его подлинность. После проверки сервер добавляет клиентский компьютер в список доверенных и может передавать на него задачи.

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

▼ Параметры утилиты Cm.Agent.Cert.Generator

Генерация корневого и SSL-сертификата:

`/root` – генерация корневого сертификата сервисов агента.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Чтобы создать сертификаты сервисов агента:

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

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

В каталоге с утилитой появятся файлы:

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



ПРИМЕЧАНИЕ

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

Для инсталляций с несколькими серверами Indeed CM

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

Чтобы создать SSL-сертификат дополнительного сервера или обновить истекший сертификат, перенесите на сервер каталог с утилитой Cm.Agent.Cert.Generator и корневой сертификат сервисов агента с закрытым ключом в формате JSON (*agent_root_ca.json*) и выполните команду:

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

Пример

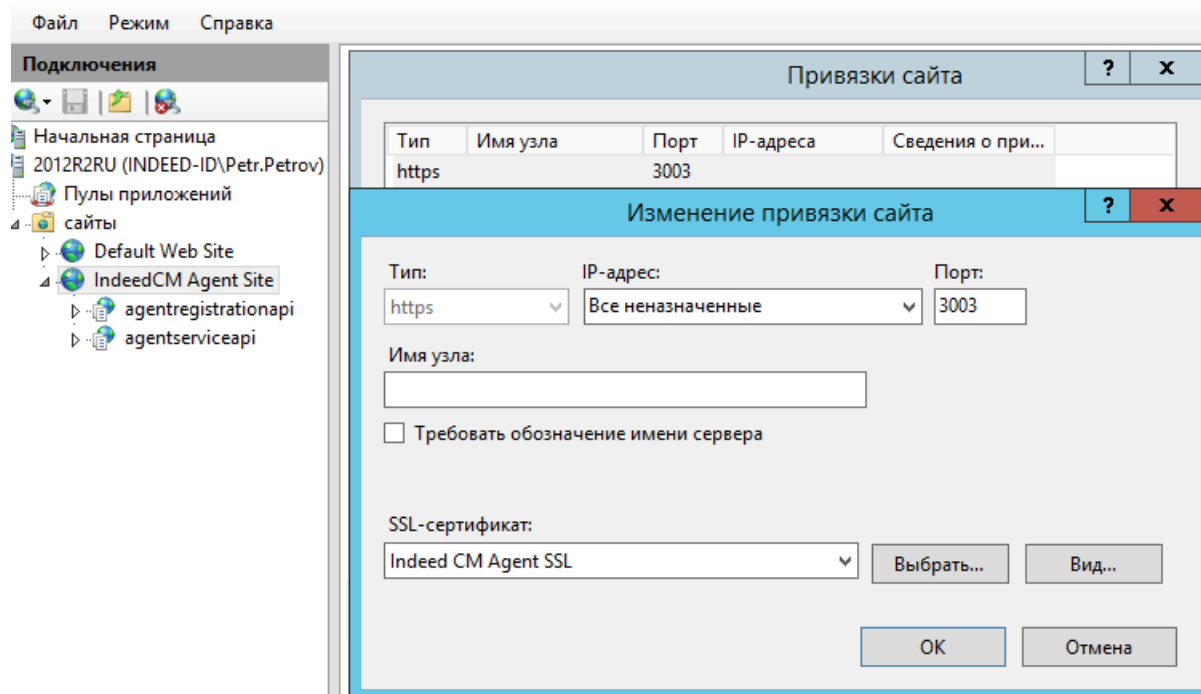
```
Cm.Agent.Cert.Generator.exe /rootKey
```

```
"C:\AgentCertGenerator\agent_root_ca.json" /ssl /sn server.domain.loc  
/installToStore
```

Настройка защищенного соединения с сайтом сервисов агента

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

▼ Пример настройки привязки для сайта IndeedCM Agent Site



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

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

Создание сертификатов сервисов агента

Для работы агента требуются следующие сертификаты:

- **CM Agent CA** – корневой сертификат сервисов агента. Используется для выдачи сертификатов рабочим станциям пользователей, на которых будут устанавливаться агенты.
- **CM Agent SSL** – сертификат проверки подлинности, подписан корневым сертификатом. Необходим для установки двустороннего защищенного соединения между сервером и рабочей станцией с установленным агентом. Сертификат выдается на имя рабочей станции, на которой развернут сервер Indeed CM.
- **Сертификат рабочей станции** – выдается автоматически при регистрации агента. Обращаясь к серверу, клиентский компьютер предоставляет свой сертификат, а сервер Indeed CM проверяет его подлинность. После проверки сервер добавляет клиентский компьютер в список доверенных и может передавать на него задачи.

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

▼ Параметры утилиты Cm.Agent.Cert.Generator

Генерация корневого и SSL-сертификата:

`/root` – генерация корневого сертификата сервисов агента.

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

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

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

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

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

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

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

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

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

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

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

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

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

Чтобы создать сертификаты сервисов агента:

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

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

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

ПРИМЕЧАНИЕ

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

Для инсталляций с несколькими серверами Indeed CM

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

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

```
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 server.domain.loc1
```

Настройка защищенного соединения с сайтом сервисов агента

Выберите инструкцию в зависимости от ОС, где установлен сервер Indeed CM:

Debian-based

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

Конвертируйте формат корневого сертификата агента в CRT.

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

2. Запустите команду обновления хранилища доверенных корневых сертификатов.

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

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

RHEL-based

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

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

2. Запустите команду обновления хранилища доверенных корневых сертификатов.

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

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

▼ 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 для него. Убедитесь, что порт открыт для входящих подключений в брандмауэре.

В качестве SSL/TLS-сертификата допускается использование RSA-сертификата, выпущенного с любого доверенного УЦ на имя сервера Indeed CM.

- **Субъект** (Subject) сертификата должен содержать атрибут **Общее имя** (Common name) (FQDN сервера системы).
- **Дополнительное имя субъекта** (Subject Alternative Name) сертификата должно содержать атрибут **DNS-имя** (DNS Name) (FQDN сервера системы).
Например: *server.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).

Установка и настройка клиентских КОМПОНЕНТОВ

Установите на рабочие станции пользователей следующие клиентские компоненты:



Indeed CM Client Tools

Компонент для разблокировки устройств



Indeed CM Middleware

Компонент для работы с USB-токенами и смарт-картами



Indeed CM Agent

Компонент для удаленного контроля устройств

Indeed CM Client Tools

Indeed CM Client Tools – клиентский компонент Indeed CM, необходимый для разблокировки устройств, которые используются для аутентификации в ОС Windows в режимах онлайн и офлайн, и для разблокировки устройств, которые не используются для входа в ОС.

Установите Indeed CM Client Tools на рабочие станции пользователей. Запустите файл *Cm.Client.Tools-**<номер версии>.ru-ru.msi*** из каталога *CM.Client* дистрибутива системы и выполните установку, следуя указаниям мастера.

Разблокировка устройств реализована в двух режимах: **онлайн и офлайн**.

Онлайн

В онлайн-режиме рабочая станция пользователя, к которой подключено заблокированное устройство, имеет соединение с сервером Indeed CM. Соединение с сервером необходимо для аутентификации пользователя с помощью ответов на секретные вопросы.

Для связи рабочих станций пользователей с сервером Indeed CM при онлайн-разблокировке рекомендуется использовать защищенное соединение https.

Офлайн

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

При исчерпании заданного числа попыток ввода PIN-кода пользователь получает сообщение о блокировке устройства и уникальный 16-символьный код-запрос. Пользователю необходимо связаться с оператором системы (например, по телефону) и подтвердить свою личность.

Настройка онлайн-разблокировки устройств

Настройте разблокировку устройств через групповые политики или реестр Windows (для рабочих станций вне домена Windows).

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

Добавьте административные шаблоны компании Индид:

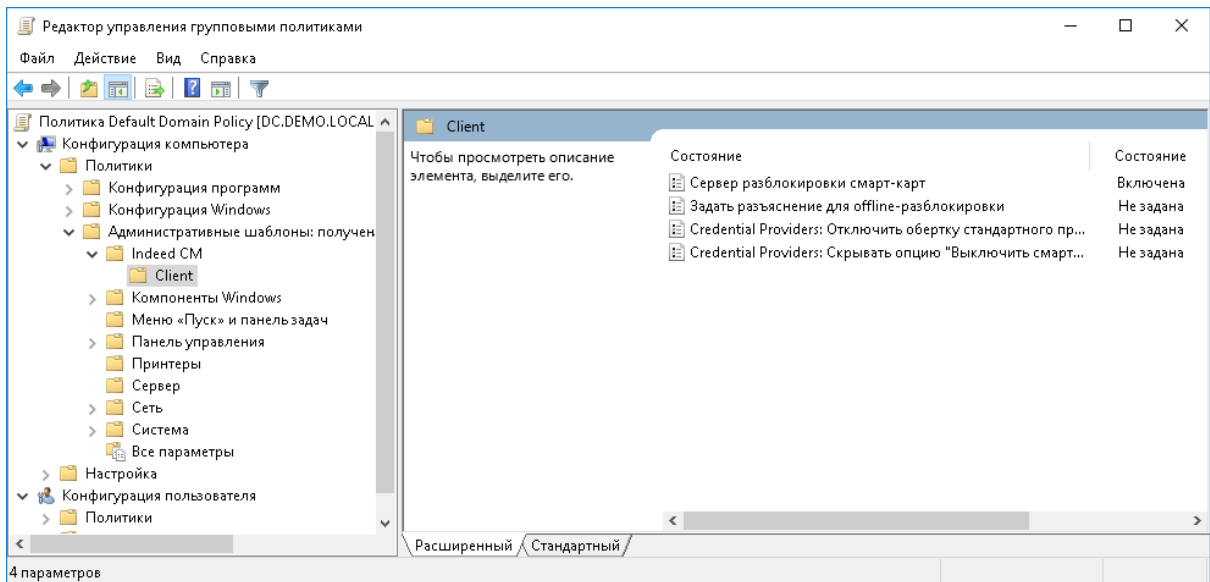
1. Скопируйте содержимое каталога *CM.Client\Misc* в центральное хранилище ADMX-файлов контроллера домена *C:\Windows\SYSVOL\domain\Policies\PolicyDefinitions*.



ПРИМЕЧАНИЕ

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

2. Откройте консоль **Управление групповой политикой** (Group Policy Management).
3. В дереве окна консоли создайте новый объект групповой политики, или выберите существующий.
4. Вызовите контекстное меню и выберите пункт **Изменить** (Edit).
5. В открывшемся **Редакторе управления групповыми политиками** (Group Policy Management Editor) выберите **Конфигурация компьютера** (Computer Configuration) → **Политики** (Policies) → **Административные шаблоны** (Administrative Templates) → **Indeed CM** → **Client**.
6. Включите политику **Сервер разблокировки смарт-карт** (Smart card unlocking server) и укажите ее значения:
 - В параметре **URL сервиса** (Service URL) укажите ссылку на компонент **credprovapi**, размещенный на сервере Indeed CM: `https://<FQDN сервера Indeed CM>/cm/credprovapi`.
 - В параметре **Проверять сертификат сервера** (Verify server certificate) установите значение **Да**, если необходимо проводить проверку подлинности сертификата сервера. Установите **Нет** (значение по умолчанию), если проверку подлинности проводить не требуется.



7. Свяжите этот объект политики с группой, членами которой являются рабочие станции пользователей системы Indeed CM.
8. Нажмите **Применить** (Apply) и обновите политики.

При необходимости настройте дополнительные политики, определяющие работу сервиса разблокировки.

▼ **Дополнительные политики сервиса разблокировки**

Политика	Параметры
Задать разъяснения для офлайн-разблокировки (Set explanations for offline unlocking)	Политика применяется к рабочим станциям пользователей. Если политика выключена или не определена, то при офлайн-разблокировке устройства текст разъяснения в Credential Provider не отображается. Если политика включена, то при офлайн-разблокировке устройства в Credential Provider будет отображаться указанный в политике текст разъяснения. Например, контактный телефон администратора Indeed CM.
Credential Providers: Отключить обертку стандартного провайдера смарт-карт (Credential Providers: Disable smart card standard provider wrapping)	Политика применяется к рабочим станциям пользователей. Если политика выключена или не определена, пользователь имеет возможность выполнить разблокировку смарт-карты в стандартном интерфейсе входа в ОС Windows по смарт-карте. Если политика включена, то отдельная опция для разблокировки смарт-карты будет отображаться на экране входа в ОС. Такая настройка может быть использована в ситуации, когда на рабочей станции установлено стороннее ПО, запрещающее разблокировку карты через стандартный Credential Provider.

Политика	Параметры
Credential Providers: Скрывать опцию "Выключить смарт-карту" (Credential Providers: Hide the "Disable the smart card" option)	Политика применяется к рабочим станциям пользователей. Если политика выключена или не определена, пользователь имеет возможность выполнить выключение смарт-карты в интерфейсе входа в ОС Windows. Если политика включена, то опция для выключения смарт-карты не будет отображаться на экране входа в ОС.

Реестр Windows

Если сервер Indeed CM и рабочие станции пользователей находятся вне домена Windows, пропишите путь к приложению **credprovapi** в реестре каждой клиентской рабочей станции.

Для этого создайте файл реестра REG со следующим содержанием:

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\CM\Client]

"CredProvAPIURL"=""

"AdminDetails"=""

"DisableServerCertificateChecking"=dword:00000000

"DisableSuspendCP"=dword:00000000

"DisableWrapperCP"=dword:00000000

- **CredProvAPIURL**: задайте адрес приложения credprovapi на сервере Indeed CM.
- **AdminDetails**: задайте текст разъяснения для пользователя.
- **DisableServerCertificateChecking**: установите значение 0 (значение по умолчанию), если необходимо проводить проверку подлинности сертификата сервера

Indeed CM. Установите **1** (dword:00000001), если проверку подлинности проводить не требуется.

- **DisableSuspendCP**: установите значение **0** (значение по умолчанию), если в интерфейсе входа в ОС необходимо отображать опцию **Выключение смарт-карты** или значение **1** (dword:00000001), если опцию **Выключение смарт-карты** отображать не требуется.
- **DisableWrapperCP**: установите значение **0** (значение по умолчанию), если необходимо выполнять разблокировку смарт-карты с использованием стандартного Credential Provider. Установите значение **1** (dword:00000001), если необходимо использовать отдельный Credential Provider.

Пример файла REG

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\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

В примере указано имя машины *server.domain.loc*, включена проверка подлинности сертификата сервера, отключено отображение кнопки **Выключить смарт-карту** и включена опция разблокировки смарт-карты в отдельном Credential Provider на экране входа в ОС.

Indeed CM Middleware

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

ⓘ ПРИМЕЧАНИЕ

Для работы Indeed CM Middleware на рабочих станциях пользователей должны быть установлены драйвера и сервисные утилиты устройств и считывателей, которые будут использоваться с Indeed CM. Данное ПО не входит в комплект поставки Indeed CM.

Windows

Установите компоненты Middleware на рабочие станции операторов и пользователей под управлением ОС Windows.

Для разных типов устройств предусмотрены разные файлы Middleware.

Запустите файл *См. <имя типа устройства>.Middleware.<номер версии>.ru-ru.msi* из каталога *СМ.Client* дистрибутива системы и выполните установку, следуя указаниям мастера.

▼ Таблица соответствия производителей, моделей устройств и файлов Middleware

Производитель	Модели устройств	Middleware
Аладдин Р.Д.	JaCarta PKI JaCarta PKI/Flash JaCarta PKI/BIO JaCarta PKI/ГОСТ JaCarta PKI/ ГОСТ/Flash JaCarta-2 PKI/ ГОСТ JaCarta-2 PKI/ ГОСТ/Flash JaCarta-2 SE	<i>IndeedCM.JaCarta.Middleware-<номер версии>.ru-ru.msi</i>

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	<i>IndeedCM.Rutoken.Middleware-<номер версии>.ru-ru.msi</i>
Компания Индид	Сетевая смарт-карта AirCard	<i>IndeedCM.AirCard.Middleware-<номер версии>.ru-ru.msi</i>
ACS	ACOS5-64	<i>IndeedCM.ACOS.Middleware-<номер версии>.ru-ru.msi</i>
Avest	Avest Key 256A	<i>IndeedCM.Avest.Middleware-<номер версии>.ru-ru.msi</i>

Производитель	Модели устройств	Middleware
Bit4id	ID-One Cosmo	<i>IndeedCM.Bit4Id.Middleware-<номер версии>.ru-ru.msi</i>
CRYPTAS	TicTok V2/V3	<i>IndeedCM.TicTok.Middleware-<номер версии>.ru-ru.msi</i>
Cryptovision	ePasslet Suite v3.0, JCOP V3.0	<i>IndeedCM.Cryptovision.Middleware-<номер версии>.ru-ru.msi</i>
Feitian	ePass2003 (A1+, A2) BioPass2003	<i>IndeedCM.ePass.Middleware-<номер версии>.ru-ru.msi</i>
HID	Crescendo C1150 Series Crescendo C1300 Series Crescendo C2300 Series	<i>IndeedCM.HID.Middleware-<номер версии>.ru-ru.msi</i>
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	<i>IndeedCM.ESMART.Middleware-<номер версии>.ru-ru.msi</i>
Kaztoken	Kaztoken, Kaztoken SC	<i>IndeedCM.Kaztoken.Middleware-<номер версии>.ru-ru.msi</i>

Производитель	Модели устройств	Middleware
Microsoft	Реестр Локального компьютера Реестр Пользователя	<i>IndeedCM.Registry.Middleware-<номер версии>.ru-ru.msi</i>
	TPM Virtual Smart Card (Microsoft VSC)	<i>IndeedCM.TPM.Middleware-<номер версии>.ru-ru.msi</i>
	Windows Hello for Business (WHfB)	<i>IndeedCM.WHfB.Middleware-<номер версии>.ru-ru.msi</i>
RSA	RSA SecurID 800	<i>IndeedCM.RSA.Middleware-<номер версии>.ru-ru.msi</i>

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	<i>IndeedCM.eToken.Middleware-<номер версии>.ru-ru.msi</i>

Производитель	Модели устройств	Middleware
	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)	<i>IndeedCM.IDPrime.Middleware-<номер версии>.ru-ru.msi</i>
Yubico	YubiKey 5 Series	<i>IndeedCM.YubiKey.Middleware-<номер версии>.ru-ru.msi</i>

Linux

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

Установите Indeed CM Middleware:

Debian-based

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

RHEL-based

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

▼ Таблица моделей устройств, поддерживаемых Indeed CM на ОС Linux

Производитель	Модели устройств
Аладдин Р.Д.	JaCarta PKI JaCarta PKI/Flash JaCarta PKI/BIO JaCarta PKI/ГОСТ JaCarta PKI/ГОСТ/Flash JaCarta-2 PKI/ГОСТ JaCarta-2 PKI/ГОСТ/Flash JaCarta-2 SE
Компания «Актив»	Рутокен 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
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

Поддержка устройств Registry

Настройте поддержку устройств Registry через групповые политики или реестр Windows (для рабочих станций вне домена Windows).

Групповые политики

Чтобы разрешить пользователям Indeed CM выпускать устройства Registry с записью сертификатов в локальное хранилище компьютера и/или пользователя через **Сервис самообслуживания**, настройте соответствующую групповую политику. Политика должна распространяться на рабочие станции пользователей Indeed CM.

Добавьте административные шаблоны компании Индид:

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



ПРИМЕЧАНИЕ

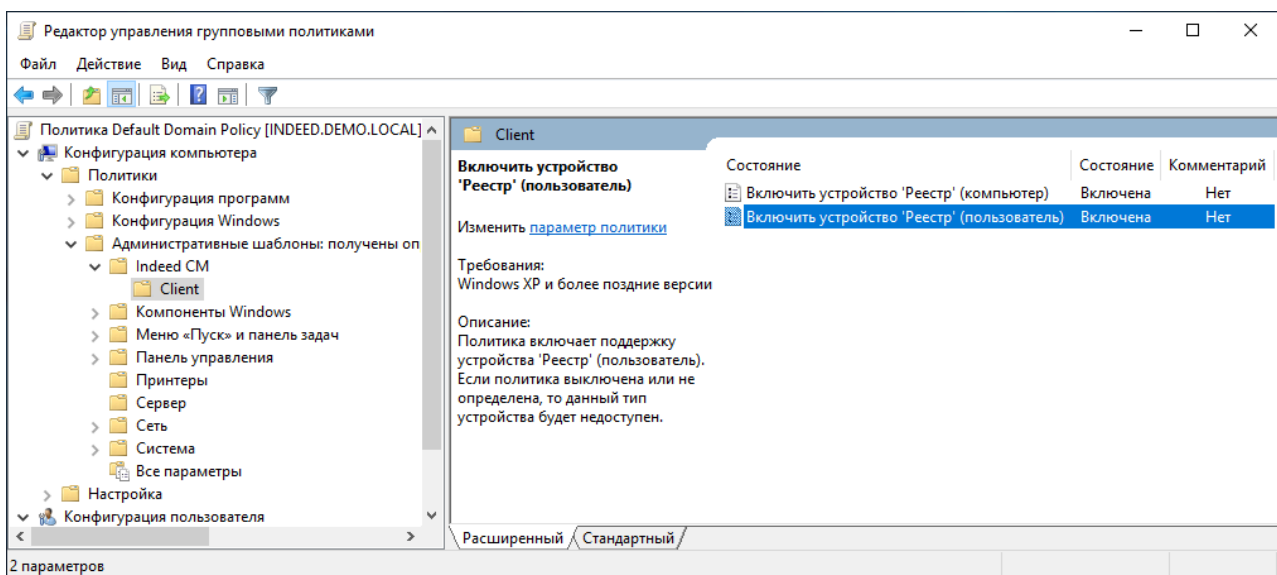
При использовании локального хранилища ADMX-файлов поместите шаблоны в *C:\Windows\PolicyDefinitions*.

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

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

6. Включите политики:

- **Включить устройство 'Реестр' (компьютер)** (Enable 'Registry' card (Machine)), если требуется выпуск сертификатов в локальное хранилище рабочей станции
- **Включить устройство 'Реестр' (пользователь)** (Enable 'Registry' card (User)), если требуется выпуск сертификатов в хранилище пользователя



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

8. Нажмите **Применить** (Apply) и обновите политики.

Реестр Windows

Если сервер Indeed CM и рабочие станции пользователей находятся вне домена Windows, задайте возможность выпуска устройств Registry в реестре каждой клиентской рабочей станции.

Для этого создайте файл реестра REG со следующим содержанием:

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\CM\Client]

"MachineRegistryCardEnabled"=dword:00000000

"UserRegistryCardEnabled"=dword:00000000

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

Пример файла REG

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\CM\Client]

"MachineRegistryCardEnabled"=dword:00000001

"UserRegistryCardEnabled"=dword:00000001

В примере включена возможность выпускать устройства Registry в хранилище компьютера и пользователя.

Indeed CM Agent

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

Установите Indeed CM Agent вместе с Indeed CM Middleware на рабочие станции пользователей Indeed CM. Запустите файл *Cm.Agent-<номер версии>.ru-ru.msi* из каталога *CM.Client* дистрибутива системы и установите Indeed CM Agent, следуя указаниям мастера. После установки агент запустится автоматически.

Задайте настройки для связи с сервером Indeed CM через групповые политики или реестр Windows.

Групповые политики

Для добавления административных шаблонов компании Индид выполните следующие действия:

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



ПРИМЕЧАНИЕ

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

2. Откройте консоль **Управление групповой политикой** (Group Policy Management).
3. В дереве окна консоли создайте новый объект групповой политики или выберите существующий.
4. Вызовите контекстное меню и выберите пункт **Изменить** (Edit).
5. В открывшемся **Редакторе управления групповыми политиками** (Group Policy Management Editor) выберите **Конфигурация компьютера** (Computer Configuration) → **Политики** (Policies) → **Административные шаблоны** (Administrative Templates) → **CM** → **Agent**.
6. Включите политику **Настройка URL сервисов агентов** (Agent's URL Settings) и укажите ее значения:

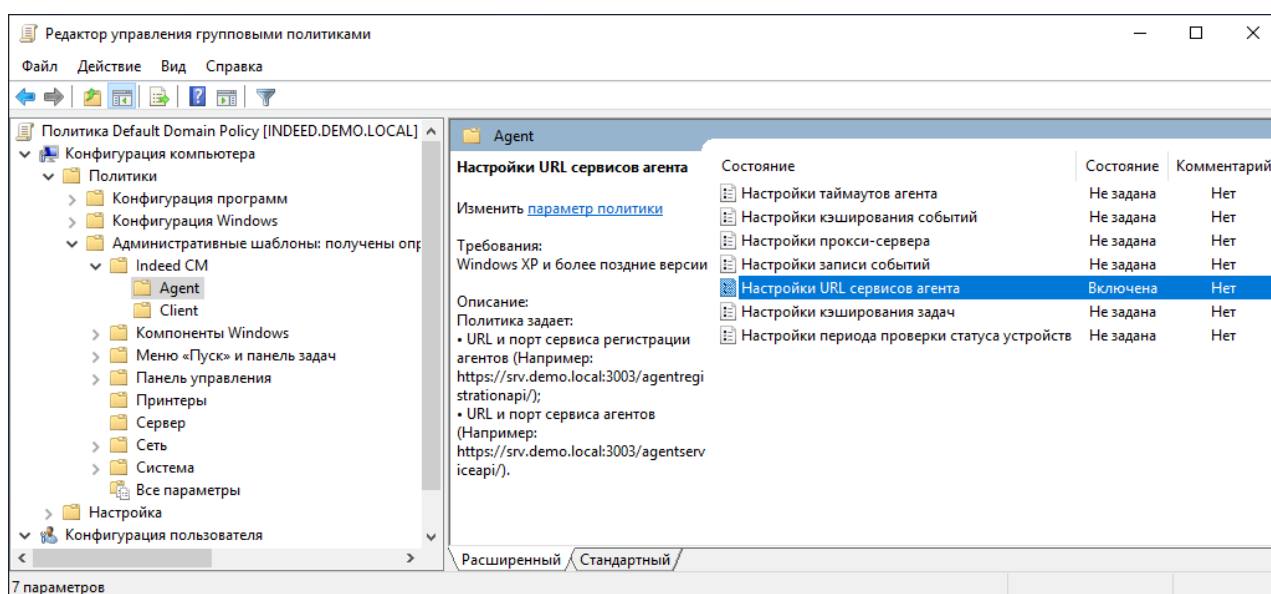
- В параметре **URL сервиса регистрации агентов** (Agents registration service URL) укажите веб-адрес и порт подключения к приложению **agentregistrationapi**, размещенного на сервере Indeed CM.
- В параметре **URL сервиса агентов** (Agents service URL) укажите веб-адрес и порт сервиса **agentserviceapi**.

❗ ПРИМЕРЫ URL

URL сервиса регистрации агентов:

`https://server.domain.loc:3003/agentregistrationapi/`

URL сервиса агентов: `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) и обновите политики. Чтобы обновить политики, перезагрузите рабочую станцию с установленным клиентским агентом. Для принудительного обновления групповых политик без перезагрузки выполните команду `gpupdate/force`.

Вы можете настроить дополнительные политики, определяющие работу Агентов.

▼ **Дополнительные политики Агента**

Политика	Параметры
Настройки таймаутов агентов (Agent's timeouts settings)	- Таймаут запросов к сервисам агента (по умолчанию: 30 сек.) - Периодичность запроса проверки статуса агента (по умолчанию: 300 сек.) - Периодичность запроса на обновление настроек, привязок, задач и сессий (по умолчанию: 30 сек.) - Таймаут запроса отключения агента от сервера (по умолчанию: 3 сек.)
Настройки кэширования событий (Events caching settings)	- Период в минутах, в течение которого агент будет пытаться отправить события из кэша на сервер (по умолчанию: 10 мин.) - Количество событий, передаваемых за один раз из кэша рабочей станции пользователя на сервер (по умолчанию: 500 событий)
Настройки прокси-сервера (Proxy server settings)	Политика определяет использование прокси-сервера при подключении к серверу Indeed CM. Если политика не задана или отключена, прокси-сервер использоваться не будет. В параметре Прокси-сервер задается адрес прокси-сервера.
Настройки записи событий (Event log settings)	Политика задает уровень записи событий в серверный журнал: - все (по умолчанию), - только ошибки, - только ошибки и предупреждения.

Политика	Параметры
Настройки кэширования задач (Tasks caching settings)	- Периодичность обновления кэша задач и отправки статуса выполнения задачи на сервер, если сразу не удалось сообщить статус серверу (по умолчанию: 60 сек) - Таймаут, при котором задачи будут удалены из кэша при очередном обновлении кэша (по умолчанию: 300 сек.) - Таймаут, после которого можно будет повторно выполнить отмененную пользователем задачу (по умолчанию: 60 сек.)
Настройки периода проверки статуса устройств (Smart card status update settings)	Политика задает периодичность проверки статуса устройств (по умолчанию: 30 сек.): - Блокировка PIN-кода пользователя\администратора - Попытки ввода неверного PIN-кода пользователя\администратора

Реестр Windows

Создайте файл реестра REG со следующим содержанием:

```
Windows Registry Editor Version 5.00

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



ПОДСКАЗКА

Для 32-разрядных ОС параметры настраиваются в ветке:
[HKEY_LOCAL_MACHINE\SOFTWARE\CM\Agent]

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

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

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



ВОЗМОЖНЫЕ ЗНАЧЕНИЯ ПАРАМЕТРОВ ИСПОЛЬЗОВАНИЯ ПРОКСИ-СЕРВЕРА

"ProxyEnable"=dword:00000000 – прокси не используется.

"ProxyEnable"=dword:00000001 и "ProxyServer"= "" – используются настройки прокси по умолчанию.

"ProxyEnable"=dword:00000001 и "ProxyServer"="<URL прокси-сервера>" – используется прокси-сервер, указанный в настройке.

Пример файла REG

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\CM\Agent]

"AgentRegistrationServiceUrl"="https://server.domain.loc:3003/agentregi

"AgentServiceUrl"="https://server.domain.loc:3003/agentserviceapi/"

"ProxyEnable"=dword:00000001

"ProxyServer"="https://192.168.10.10:443"

В примере файла REG указано имя сервера Indeed CM *server.domain.loc*, протокол *https*, порт *3003*, прокси-сервер *https://192.168.10.10:443*.



ПРЕДУПРЕЖДЕНИЕ

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

Руководство администратора



Первый запуск

Вход в Консоль управления Indeed CM



Конфигурация

Настройка конфигурации Indeed CM



Консоль управления

Управление функциями Indeed CM

Первый запуск

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

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

Вы можете получить доступ к Консоли управления в соответствии с настройками аутентификации, заданными на этапе развертывания **сервера Indeed CM**.

Перед началом работы с Indeed CM:

1. Запустите Консоль управления от имени учетной записи, которая указана в Мастере настройки Indeed CM в разделе **Контроль доступа** → **Администратор ролей**.
2. Перейдите в раздел **Конфигурация** → **Роли**, добавьте текущего пользователя в роль **Администраторы**. Создайте роли для администраторов и операторов, настройте привилегии.
3. Загрузите файл лицензии в раздел **Лицензии**.
4. Загрузите файлы типов устройств в разделе **Типы устройств**.
5. Настройте политики использования устройств в разделе **Политики**.
6. Назначьте политики на пользователей Indeed CM в разделе **Назначения политик**.

Конфигурация



Политики

Создание и редактирование политик использования устройств



Назначения политик

Для централизованного управления объектами или пользователями



Лицензии

Управление лицензиями



Типы устройств

Настройки типов и моделей устройств, управление PIN-кодами администратора и пользователя



Организационная структура

Объединение объектов каталога пользователей под действие одной политики использования устройств



Роли

Полномочия администраторов и операторов



Теги

Настройка тегов для гибкого учета устройств в организации



Шаблоны печати

Настройка шаблонов документов



СКЗИ

Управление средствами криптографической защиты информации



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.

Политики можно назначить на пользователей в разделе **Конфигурация** → **Назначения политик**.

Создание

1. Откройте Консоль управления Indeed CM и 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.

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

Удаление

Чтобы удалить политику:

1. Выберите политику в списке и нажмите **✕**.
2. Нажмите **Удалить**.

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

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



КриптоПро УЦ 2.0

Параметры работы с КриптоПро УЦ 2.0



Валидата УЦ

Параметры работы с Валидата УЦ



КриптоПро DSS 2.0

Параметры работы с КриптоПро DSS 2.0



Общие сертификаты

Настройка общих сертификатов

Microsoft CA

Добавьте информацию об удостоверяющем центре (УЦ) Microsoft CA и настройте шаблоны сертификатов, которые будут выпускаться в этом УЦ.

Предварительные настройки

Чтобы разрешить доступ к разделу **Microsoft**:

1. Запустите **Мастер настройки**.
2. Перейдите в раздел **Microsoft CA**.
3. Включите опцию **Включить интеграцию с Microsoft CA Enterprise**.

Добавление УЦ

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

Windows

1. Нажмите **Добавить УЦ**.
2. В поле **Адрес** задайте адрес УЦ, если он не определился автоматически.
3. Укажите логин в формате `DOMAIN\Username` и пароль сервисной учетной записи, обладающей сертификатом **Агент регистрации** (Enrollment Agent).
4. Нажмите **Добавить**.



ПРЕДУПРЕЖДЕНИЕ

Наличие пользователя с сертификатом **Агент регистрации** (Enrollment Agent) является обязательным условием для работы Indeed CM с УЦ. От имени этого пользователя будут отправляться запросы в указанный УЦ на выдачу сертификатов пользователям Indeed CM. Учетные данные этого пользователя можно изменить после добавления УЦ в Indeed CM.

Чтобы изменить учетные данные пользователя с сертификатом **Агент регистрации** (Enrollment Agent), выберите нужный УЦ и нажмите  справа от имени пользователя.

Добавление УЦ, расположенного за пределами домена пользователей Indeed CM

1. Нажмите **Добавить УЦ**.
2. В поле **Адрес** укажите URL-адрес приложения **Indeed CM MSCA Proxy**. Если Indeed CM развернут в лесу доменов, использовать Indeed CM MSCA Proxy необязательно. В этом случае в поле **Адрес** укажите имя УЦ.
3. Укажите логин в формате `DOMAIN\Username` и пароль учетной записи пользователя, обладающего сертификатом **Агент регистрации** (Enrollment Agent) на УЦ, расположенном вне домена с каталогом пользователей Indeed CM.
4. Включите опцию **Выпускать сертификаты для пользователей из внешнего сопоставленного каталога**.
5. В поле **Путь (LDAP)** укажите путь к каталогу пользователей Indeed CM внешнего домена.

▼ Пример работы с каталогом пользователей внешнего домена

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

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



ПРЕДУПРЕЖДЕНИЕ

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

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

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



ПОДСКАЗКА

Чтобы настроить разрешение на чтение только необходимого набора свойств, перейдите в список Разрешений (Permissions) указанной учетной записи Active Directory и выберите нужные свойства.

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**

➕ Добавить УЦ

Добавить удостоверяющий центр

Адрес

Укажите учетные данные пользователя для подключения к УЦ

Имя пользователя

Пароль

Сертификат агента регистрации

☒ Выпускать сертификаты для пользователей из внешнего сопоставленного каталога

Путь (LDAP)

Имя пользователя

Пароль

Атрибут сопоставления каталогов

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.

Добавление УЦ, расположенного за пределами домена пользователей Indeed CM

1. Включите опцию **Выпускать сертификаты для пользователей из внешнего сопоставленного каталога**.
2. В поле **Путь (LDAP)** укажите путь к каталогу пользователей Indeed CM внешнего домена.

▼ **Пример работы с каталогом пользователей внешнего домена**

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

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



ПРЕДУПРЕЖДЕНИЕ

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

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

3. В поле **Имя пользователя** укажите учетную запись (в формате DOMAIN\Username), обладающую правами на чтение всех свойств пользователей во внешнем домене.



ПОДСКАЗКА

Чтобы настроить разрешение на чтение только необходимого набора свойств, перейдите в список Разрешений (Permissions) указанной учетной записи Active Directory и выберите нужные свойства.

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.

Настройка шаблонов сертификатов

Перед началом работы с шаблонами сертификатов в Indeed CM убедитесь, что необходимые шаблоны настроены и добавлены в центр сертификации 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

Параметр	Описание
Префикс имени ключа	Если не указать префикс имени ключа, то имя контейнера, содержащего ключевую пару, формируется случайным образом. Если вы указали префикс, то он добавится перед именем контейнера. Значение префикса отображается в Indeed CM (имя контейнера в разделе СКЗИ) и в стороннем ПО для работы с контейнерами закрытого ключа (КриптоПро CSP, клиенты устройств). Устройства могут не поддерживать отображение имени контейнера с префиксом.

Параметр	Описание
Включить в имя субъекта	Укажите 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 Чтобы сформировать имя субъекта (Subject) и альтернативное имя субъекта (Subject Alternative Name) сертификата из списка атрибутов в свойствах шаблона Microsoft CA на вкладке Имя субъекта (Subject Name) укажите Предоставляется в запросе (Supply in the request).

Параметр	Описание
Включить в альтернативное имя субъекта	Укажите атрибуты для формирования альтернативного имени субъекта (Subject Alternative Name) сертификата: ▼ 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.
Создавать резервную копию ключа	При генерации ключевой пары на смарт-карте применится опция ее архивации. Это значит, что ключевая пара сгенерируется на смарт-карте, и ее копия (открытый и закрытый ключи) будут отправлены на сервер Indeed CM и затем в хранилище системы. Архивация ключевой пары возможна только один раз. Если опция выключена, то ключевая пара генерируется сразу на устройстве.
Записывать копию ключа при временной замене устройства	Копии сертификатов и закрытых ключей будут записаны на временное устройство при временной и постоянной замене. Если опция выключена, то копии сертификатов и закрытых ключей не будут записаны на временное устройство при замене.
Использовать ключи повторно	При обновлении сертификатов, записанных на устройство, существующий ключ шифрования используется повторно.

Параметр	Описание
Импортировать сертификат, если существует	Indeed CM будет искать существующие сертификаты на устройстве (для указанного пользователя, УЦ и шаблона) и использовать их, не создавая новых ключей. Сертификат невозможно импортировать, если устройство будет инициализировано перед выпуском.
Не удалять сертификат при обновлении/очистке устройства	При обновлении или очистке устройства истекающий/истекший сертификат не удалится с устройства и отозван на 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 будет запрошен и записан 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. Если опция выключена, сертификаты не отзываются.
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.

Параметр	Описание
Публиковать сертификат в файловое хранилище	Выпущенный сертификат помещается в сетевое 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.
Автоматически одобрять запрос на сертификат	Запрос на сертификат одобряется автоматически. Если опция выключена, то для завершения выпуска необходимо дождаться, когда УЦ одобрит запрос, или отменить выпуск, если запрос отклонен.
Автоматически одобрять подписанный запрос на обновление сертификата	Запрос на обновление сертификата одобряется автоматически. Если опция выключена, то для обновления сертификата необходимо дождаться, когда УЦ одобрит запрос.

Параметр	Описание
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: 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.
Шаблон печати запроса на сертификат	Если параметр не задан, то используется стандартный шаблон печати запроса на сертификат. Если в Indeed CM добавлены Шаблоны печати запроса сертификата, то выберите шаблон из выпадающего меню.

Параметр	Описание
Шаблон печати сертификата	Если параметр не задан, то используется стандартный шаблон печати сертификата. Если в Indeed CM добавлены Шаблоны печати сертификата, то выберите шаблон из выпадающего меню.
Шаблон печати запроса на отзыв сертификата	Если параметр не задан, то используется стандартный шаблон печати запроса на отзыв сертификата. Если в Indeed CM добавлены Шаблоны печати запроса на отзыв сертификата, выберите шаблон из выпадающего меню.
Использовать по умолчанию	Сертификат используется по умолчанию для входа в стороннее ПО.
Необязательный сертификат	При выпуске устройства появится возможность выбрать, какие сертификаты из списка необязательных, записать на устройство. Если опция выключена, то сертификат считается обязательным для записи на устройство.

КриптоПро УЦ 2.0

Добавьте информацию о КриптоПро УЦ 2.0 и настройте шаблоны сертификатов, которые будут выпускаться в этом УЦ.

Предварительные настройки

Чтобы разрешить доступ к разделу **КриптоПро 2.0**:

1. Запустите **Мастер настройки**.
2. Перейдите в раздел **КриптоПро УЦ 2.0**.
3. Включите опцию **Включить интеграцию с КриптоПро УЦ 2.0**.

Добавление УЦ

1. Нажмите **Добавить УЦ**.
2. Введите **URL-адрес веб-службы Центра Регистрации**. В зависимости от используемого варианта исполнения КриптоПро УЦ 2.0 укажите:

- URL-адрес в полном или сокращенном виде для вариантов исполнений 5, 6, 9, 10 для ОС Windows:

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

- URL-адрес для вариантов исполнений для вариантов исполнений 15 и 16 для ОС Windows и Astra Linux SE:

```
https://<host_name>
```

3. Если для соединения с УЦ используется прокси-сервер, укажите имя сервера и порт в поле **URL-адрес прокси-сервера**. Например, `http://proxy.company.com:8080`.

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

4. Выберите тип API в зависимости от используемого варианта исполнения КристоПро УЦ 2.0:
- REST для вариантов исполнений 15, 16 для ОС Windows и Astra Linux SE
 - SOAP для вариантов исполнений 5, 6, 9, 10 для ОС Windows
5. Укажите имя пользователя, обладающего сертификатом **Indeed CM Service User**. **Как создать сервисную учетную запись для работы с КристоПро УЦ 2.0**
6. При необходимости включите опцию **Устанавливать привязку между пользователем УЦ и пользователем каталога**.
7. Нажмите **Добавить**.

▼ Подробнее об установке связи между пользователем УЦ и пользователем каталога

Установите связь между пользователями каталога и пользователями УЦ, если каталог пользователей Indeed CM не является каталогом пользователей УЦ. Такая ситуация может быть в следующих сценариях использования:

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

Если включить опцию **Устанавливать привязку между пользователем УЦ и пользователем каталога**, Indeed CM позволяет определить следующие параметры работы с УЦ

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

Indeed CM может обновить данные ранее созданных пользователей КриптоПро УЦ 2.0 при выпуске или обновлении устройства. Например, поменять адрес электронной почты, если он изменился в профиле пользователя в Active Directory. Включите опцию **Обновлять учетные данные пользователя УЦ**.



ПРИМЕЧАНИЕ

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

Настройка шаблонов 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 УЦ	Загружается из выбранного удостоверяющего центра.
Префикс имени ключа	Если префикс не задан, то имя контейнера, содержащего ключевую пару, будет сформировано случайным образом. Если указан префикс, то он добавится перед именем контейнера. Значение префикса отображается в системе (имя контейнера в разделе СКЗИ) и в стороннем ПО для работы с контейнерами закрытого ключа (КриптоПро CSP, клиенты устройств и пр.). Имя контейнера с префиксом может не поддерживаться устройством.
Выпускать сертификат на указанного пользователя	Если опция включена, то в свойствах шаблона отобразится поле поиска пользователя в каталоге ЦР КриптоПро УЦ, на которого будут выпускаться сертификаты. Опция доступна при включении Разрешить выпуск сертификатов на имя общей учетной записи в разделе КриптоПро УЦ 2.0 Мастера настройки Indeed CM. Изменить значение опции при редактировании шаблона нельзя.

Параметр	Описание
Использовать аппаратную криптографию, если поддерживается	Если опция включена, то при выпуске сертификата ключевая пара будет создаваться с использованием криптографических алгоритмов, поддерживаемых устройством. Если устройство не поддерживает аппаратную криптографию, то будет использоваться КриптоПро CSP, установленный на рабочей станции, к которой подключено устройство. Изменить значение опции при редактировании шаблона нельзя.
Создавать резервную копию ключа	Если опция включена, то при генерации ключевой пары на смарт-карте будет применена опция ее архивации. Это значит, что ключевая пара будет сгенерирована на смарт-карте и ее копия (открытый и закрытый ключи) будут отправлены на сервер Indeed CM и затем в хранилище системы. Архивация ключевой пары возможна только один раз. Если опция выключена, то ключевая пара сразу генерируется на устройстве.
Записывать копию ключа при временной замене устройства	Если опция включена, то копии сертификатов и закрытых ключей будут записаны на временное устройство при замене, как и в случае с постоянной заменой. Если опция выключена, то копии сертификатов и закрытых ключей не будут записаны на временное устройство при замене.

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

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

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

Параметр	Описание
Требовать подписанный документ сертификата перед продолжением выпуска/обновления устройства	Если опция включена, то сертификат будет записан на устройство только после того, как пользователь предоставит на проверку администратору подписанную форму сертификата. После одобрения запроса в УЦ форма сертификата будет доступна пользователю в Сервисе самообслуживания. Пользователь может скачать и подписать форму сертификата и предоставить ее на проверку.
Отслеживаемые атрибуты пользователя	Укажите атрибуты пользователя, при изменении которых необходимо обновление сертификата: - Общее имя; - E-mail; - UPN-имя пользователя. Изменение e-mail приводит к обновлению сертификата в случае, если этот атрибут включен в свойствах шаблона сертификата в Microsoft CA на вкладке Имя субъекта (Subject Name) опции Включить имя электронной почты в имя субъекта (Include e-mail name in subject name) и Имя электронной почты (E-mail name). Дополнительный список отслеживаемых атрибутов пользователей задается в разделе Обновляемые атрибуты Мастера настройки Indeed CM.
Шаблон печати запроса на сертификат	Если параметр не задан, то используется стандартный шаблон печати запроса на сертификат. Если в систему добавлены Шаблоны печати запроса сертификата, то выберите шаблон из выпадающего меню.

Параметр	Описание
Шаблон печати сертификата	Если параметр не задан, то используется стандартный шаблон печати сертификата. Если в систему добавлены Шаблоны печати сертификата, то выберите шаблон из выпадающего меню.
Шаблон печати запроса на отзыв сертификата	Если параметр не задан, то используется стандартный шаблон печати запроса на отзыв сертификата. Если в систему добавлены Шаблоны печати запроса на отзыв сертификата, выберите шаблон из выпадающего меню.
Период обновления (дней)	Период времени, в течение которого сертификат и закрытый ключ можно обновить. Значение по умолчанию – 30 дней.
Необязательный сертификат	Если опция включена, то при выпуске устройства появится возможность выбрать, какие сертификаты из списка необязательных, записать на устройство. Если опция выключена, то сертификат считается обязательным для записи на устройство.

Валидата УЦ

Добавьте информацию о Валидата УЦ и настройте шаблоны сертификатов, которые будут выпускаться в этом УЦ.

Предварительные настройки

Чтобы разрешить доступ к разделу **Валидата**:

1. Запустите **Мастер настройки**.
2. Перейдите в раздел **Валидата УЦ**.
3. Включите опцию **Включить интеграцию с Валидата УЦ**.

Добавление УЦ

Офлайн-режим

1. Нажмите **Добавить УЦ**.
2. Укажите **Каталог для обмена файлами с ЦР/ЦС** – каталог для обмена файлами Indeed CM с Центром Регистрации.



ПРИМЕЧАНИЕ

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

3. В полях **Имя пользователя** и **Пароль** укажите учетные данные пользователя для подключения к выбранному каталогу.
 - Укажите **Подкаталог для запросов** – подкаталог для входящих незащищенных запросов пользователей в формате PKCS#10. Обработка запросов в формате PKCS#10 выполняется в ручном режиме на АРМ Администратора ЦР.
 - Укажите **Подкаталог для сертификатов** – подкаталог сертификатов для выдачи конечным пользователям.

4. Нажмите **Добавить**.

Онлайн-режим

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

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

```
ncacn_ip_tcp:<ip>[<port>]
```

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

⚠ ПРИМЕЧАНИЕ

Поле **Улучшенный ключ** сертификата должно содержать значения **Оператор Центра Регистрации** (OID 1.3.6.1.4.1.10244.6.1) и **Проверка подлинности TLS клиента** (OID 1.3.6.1.5.5.7.3.2).

Клиентский сертификат используется:

- При подключении к сервису ЦР, чтобы выполнить аутентификацию по протоколу TLS.
- Для подписи XML-шаблона на получение или отзыв сертификата ключа проверки ЭП пользователя.

4. Укажите **Каталог для обмена файлами с ЦР/ЦС** – каталог для обмена файлами Indeed CM с Центром Регистрации. В каталоге должны присутствовать цепочка сертификатов Валидата УЦ и актуальный список отозванных сертификатов X.509 (CRL или CAC).
5. В полях **Имя пользователя** и **Пароль** укажите учетные данные пользователя для подключения к выбранному каталогу.
 - В поле **Подкаталог для запросов** укажите подкаталог запросов в формате CMS/PKCS#7 для Центра Сертификации, обработанных Оператором ЦР.

- В поле **Подкаталог для сертификатов** укажите подкаталог сертификатов в формате CMS/PKCS#7, обработанных Центром Сертификации.

6. Нажмите **Добавить**.

Настройка шаблонов сертификатов

Перед началом работы с шаблонами сертификатов в Indeed CM убедитесь, что необходимые шаблоны 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 УЦ	Загружается из выбранного удостоверяющего центра.
Префикс имени ключа	Если префикс не задан, то имя контейнера, содержащего ключевую пару, будет сформировано случайным образом. Если указан префикс, то он добавится перед именем контейнера. Значение префикса отображается в системе (имя контейнера в разделе СКЗИ) и в стороннем ПО для работы с контейнерами закрытого ключа (КриптоПро CSP, клиенты устройств и пр.). Имя контейнера с префиксом может не поддерживаться устройством.

Параметр	Описание
Использовать аппаратную криптографию, если поддерживается	Если опция включена, то при выпуске сертификата ключевая пара будет создаваться с использованием криптографических алгоритмов, поддерживаемых устройством. Если устройство не поддерживает аппаратную криптографию, то будет использоваться КриптоПро CSP, установленный на рабочей станции, к которой подключено устройство. Изменить значение опции при редактировании шаблона нельзя.
Создавать резервную копию ключа	Если опция включена, то при генерации ключевой пары на смарт-карте будет применена опция ее архивации. Это значит, что ключевая пара будет сгенерирована на смарт-карте и ее копия (открытый и закрытый ключи) будут отправлены на сервер Indeed CM и затем в хранилище системы. Архивация ключевой пары возможна только один раз. Если опция выключена, то ключевая пара сразу генерируется на устройстве.
Записывать копию ключа при временной замене устройства	Если опция включена, то копии сертификатов и закрытых ключей будут записаны на временное устройство при замене, как и в случае с постоянной заменой. Если опция выключена, то копии сертификатов и закрытых ключей не будут записаны на временное устройство при замене.
Импортировать сертификат, если существует	Если опция включена, то система будет искать существующие сертификаты на устройстве (для указанного пользователя, УЦ и шаблона) и использовать их, не создавая новых ключей. Импорт сертификата невозможен, если устройство будет инициализировано перед выпуском.

Параметр	Описание
Не удалять сертификат при обновлении/очистке устройства	Если опция включена, то при обновлении или очистке устройства истекающий/истекший сертификат не будет удален с устройства и отозван на УЦ. В процессе обновления будет запрошен новый сертификат с новым закрытым ключом и записан на устройство. Истекающий/истекший сертификат будет удален, если устройство изъято с инициализацией.
Отзывать сертификат при отзыве или выключении устройства	Если опция включена, то сертификаты пользователя будут отозваны при выключении или отзыве устройства. Если опция выключена, то при выключении или отзыве устройства сертификаты не будут отозваны.
Устанавливать сертификат в локальное хранилище	Если опция включена, то при выпуске (обновлении) устройства через Сервис самообслуживания записанные на него сертификаты добавятся в локальное хранилище пользователя на рабочей станции.
Публиковать сертификат в каталоге пользователей	Если опция включена, то выпущенный сертификат опубликуется в профиле пользователя в Active Directory на вкладке Опубликованные сертификаты (Published Certificates). Сертификат удалится из профиля при включении опции Удалять опубликованный сертификат при отзыве устройства. Необходимо наличие прав на Запись: userCertificate (Write userCertificate) для сервисной учетной записи для работы с каталогом пользователей Active Directory.

Параметр	Описание
Публиковать сертификат в ЕСИА	Если опция включена, то выпущенный квалифицированный сертификат будет зарегистрирован в Единой системе идентификации и аутентификации (ЕСИА). Опция доступна при включении Интеграция со СМЭВ в разделе Общие функции Мастера настройки Indeed CM.
Отслеживаемые атрибуты пользователя	Укажите атрибуты пользователя при изменении которых необходимо обновление сертификата: 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 Indeed CM.
Шаблон печати запроса на сертификат	Если параметр не задан, то используется стандартный шаблон печати запроса на сертификат. Если в систему добавлены Шаблоны печати запроса сертификата, то выберите шаблон из выпадающего меню.
Шаблон печати сертификата	Если параметр не задан, то используется стандартный шаблон печати сертификата. Если в систему добавлены Шаблоны печати сертификата, то выберите шаблон из выпадающего меню.

Параметр	Описание
Шаблон печати запроса на отзыв сертификата	Если параметр не задан, то используется стандартный шаблон печати запроса на отзыв сертификата. Если в систему добавлены Шаблоны печати запроса на отзыв сертификата, то выберите шаблон из выпадающего меню.
Период обновления (дней)	Период времени, в течение которого сертификат и закрытый ключ можно обновить. Значение по умолчанию – 30 дней.
Необязательный сертификат	Если опция включена, то при выпуске устройства появится возможность выбора сертификатов для записи из числа отмеченных, как необязательные. Если опция выключена, то сертификат считается обязательным для записи на устройство.

КриптоПро DSS 2.0

Добавьте информацию о КриптоПро DSS и настройте 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 **КриптоПро DSS**.
3. Включите опцию **Включить интеграцию с КриптоПро DSS**.

Добавление УЦ

Чтобы установить подключение к серверу КриптоПро DSS:

1. Перейдите в раздел **КриптоПро DSS → Серверы**.
2. Нажмите **Добавить сервер**.
3. Укажите параметры подключения:
 - **Имя** – произвольное имя сервера.
 - **URL-адрес веб-службы СЭП** – адрес службы электронной подписи DSS.
 - **URL-адрес веб-службы ЦИ** – адрес центра идентификации DSS.
 - **URL-адрес прокси-сервера**. Если для соединения с сервером DSS используется прокси сервер, укажите имя сервера и порт. Например,
`https://proxy.company.com:8080`.
 - **Идентификатор клиента OAuth** – идентификатор клиента (`client_id`) для взаимодействия через API.
 - **Адрес возврата** – укажите адрес возврата (`redirect_uri`), если он отличается от значения по умолчанию.
 - **Клиентский сертификат** – выберите сертификат оператора DSS.
4. С помощью опции **Устанавливать привязку между пользователем DSS и пользователем каталога** определите настройки связи между пользователем DSS и пользователем каталога при выпуске или обновлении устройства:
 - **Устанавливать привязку автоматически**
Связь между пользователем каталога и пользователем DSS устанавливается

автоматически. При необходимости можно **Создавать пользователя DSS**, если он не существует.

- **Обновлять учетные данные пользователя DSS**

При обновлении или выпуске устройства обновляются данные пользователя DSS.

5. Нажмите **Добавить**.

Настройка шаблонов 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 УЦ	Загружается из выбранного удостоверяющего центра.
Импортировать сертификат, если существует	Если опция включена, то система будет искать существующие сертификаты на устройстве (для указанного пользователя, УЦ и шаблона) и использовать их, не создавая новых ключей. Импорт сертификата невозможен, если устройство будет инициализировано перед выпуском.
Отзывать сертификат при отзыве/выключении устройства	Если опция включена, то сертификаты пользователя будут отозваны при выключении или отзыве устройства. Если опция выключена, то при выключении или отзыве устройства сертификаты не будут отозваны.

Параметр	Описание
Публиковать сертификат в каталоге пользователей	Если опция включена, то выпущенный сертификат опубликуется в профиле пользователя в Active Directory на вкладке Опубликованные сертификаты (Published Certificates). Сертификат удалится из профиля при включении опции Удалять опубликованный сертификат при отзыве устройства. Необходимо наличие прав на Запись: userCertificate (Write userCertificate) для сервисной учетной записи для работы с каталогом пользователей Active Directory.
Автоматически одобрять запрос на сертификат	Если опция включена, то запросы на сертификат будут автоматически одобрены. Если опция выключена, то для завершения выпуска потребуется дождаться одобрения запроса на УЦ или отменить выпуск, если запрос будет отклонен.
Требовать подписанный документ сертификата перед продолжением выпуска/обновления устройства	Если опция включена, то сертификат будет записан на устройство только после того, как пользователь предоставит на проверку администратору подписанную форму сертификата. После одобрения запроса в УЦ форма сертификата будет доступна пользователю в Сервисе самообслуживания. Пользователь может скачать и подписать форму сертификата и предоставить ее на проверку.
Период обновления (дней)	Период времени, в течение которого сертификат и закрытый ключ можно обновить. Значение по умолчанию – 30 дней.

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

Общие сертификаты

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 Active Directory, файловое хранилище, базу 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

Indeed CM может отправить уведомление администраторам об истечении срока действия общих сертификатов. Для этого перейдите в настройки политики использования устройств в раздел **Уведомления** и 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.

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.

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.

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**.

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»**.

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 можно интегрировать с Рутокен Логон – программным продуктом компании «Актив». Рутокен Логон позволяет использовать схему двухфакторной аутентификации пользователей в ОС Linux с помощью устройства, на котором содержится сертификат или пароль в зашифрованном виде.

Возможности интеграции

Интеграция позволяет настроить доменную аутентификацию по сертификату. С помощью Indeed CM можно выпустить устройство, которое будет использоваться для входа в ОС Linux. На это устройство можно записать сертификат и объект данных, необходимый для аутентификации через Рутокен Логон.

Предварительные настройки

Чтобы разрешить доступ к разделу **Рутокен Логон**:

1. Запустите **Мастер настройки**.
2. Перейдите в раздел **Общие функции**.
3. Включите опцию **Интеграция с Рутокен Логон**.

Перед настройкой интеграции в Indeed CM убедитесь, что Рутокен Логон настроен на доменный режим работы.

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. В выпадающем списке **Шаблон сертификата** выберите шаблон, на основе которого формируется сертификат. Шаблоны сертификатов задаются в настройках политики использования устройств в разделе **Удостоверяющие центры** → **Шаблоны**.
5. 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.

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 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)

ПРОВЕРКА ДЕЙСТВИТЕЛЬНОСТИ ПАСПОРТА

КриптоПро Шлюз УЦ-СМЭВ позволяет провести расширенную проверку паспорта – отправить дополнительный запрос в МВД, чтобы получить сведения о действительности паспорта. Проверяется ФИО, серия и номер паспорта.

Предварительные настройки

Чтобы разрешить доступ к разделу **СМЭВ**:

1. Запустите **Мастер настройки**.
2. Перейдите в раздел **Общие функции**.
3. Включите опцию **Интеграция со СМЭВ**.

Проверка данных пользователя в СМЭВ доступна при выпуске или обновлении устройства, если согласно политике использования устройств пользователю нужно выпустить или обновить сертификат КриптоПро УЦ 2.0 или Валидата УЦ.

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 и его контейнер закрытого ключа установлены в локальное хранилище сертификатов на сервере Indeed CM.
6. Чтобы проводить расширенную проверку паспорта, включите опцию **Проверять действительность паспорта**.
7. Нажмите **Сохранить**.

Поведение

В разделе **Поведение** политики использования устройств задаются настройки, которые определяют доступные операции для администраторов/операторов в Консоли управления и для пользователей в Сервисе самообслуживания.

Опция	Описание
Разрешить сброс PIN-кода устройства	Разрешить администратору сбросить PIN-кода пользователей устройств.
Разрешить пользователю сброс PIN-кода устройства	Разрешить пользователю сбросить PIN-кода своего устройства.
Разрешить пользователю очистку устройства	Разрешить пользователю очистить содержимое своего устройства при его отзыве оператором с причинами Изъятие устройства и Обновление устройства . После очистки устройство останется назначенным пользователю.
Разрешить пользователю обновление устройства	Разрешить пользователю обновлять сертификаты, хранящиеся на его устройстве, если их срок действия истек или истекает.
Разрешить пользователю выпуск устройства КристоПро DSS	Если опция включена, то пользователи могут самостоятельно выполнять запрос и выпуск устройств DSS. Если опция выключена, то выпустить устройство КристоПро DSS может только администратор или оператор.

Опция	Описание
Разрешить пользователю выпуск AirCard карты	Если опция включена, то пользователи смогут самостоятельно выпускать карты AirCard в Сервисе самообслуживания. Выпуск карт AirCard возможен только при настроенной интеграции с Indeed AirCard Enterprise.
Разрешить пользователю выключение устройства	Разрешить пользователю выключение своего устройства (если оно была включено ранее).
Разрешить пользователю выбор необязательных сертификатов при обновлении устройства	Если опция включена, то при обновлении устройства в Сервисе самообслуживания пользователь может записать на него сертификаты, отмеченные как необязательные, по шаблонам, выбранным из списка. Если опция выключена, то выбор шаблонов необязательных сертификатов не будет доступен пользователю при обновлении устройства. Вы можете задать сообщение, которое отображается в виде предупреждения в окне выбора необязательных сертификатов, когда пользователь выпускает или обновляет устройство. Для этого введите текст в поле Сообщение пользователю при выборе необязательных сертификатов.
Разрешить пользователю выбор необязательных сертификатов при выпуске устройства	Если опция включена, то при выпуске устройства в Сервисе самообслуживания пользователь может записать на него сертификаты, отмеченные как необязательные, по шаблонам, выбранным из списка. Если опция выключена, то выбор шаблонов необязательных сертификатов не будет доступен пользователю при выпуске устройства.

Опция	Описание
Разрешить пользователю включение устройства	Разрешить пользователю включить свое устройство, если оно было выключено ранее.
Разрешить пользователю удаление устройства КристоПро DSS	Если опция включена, то пользователи могут самостоятельно отзывать и удалять устройство DSS. Если опция выключена, то отзывать и удалять устройства DSS могут только администраторы или операторы Indeed CM.
Разрешить пользователю редактирование данных в форме проверки в СМЭВ	Если опция включена, то пользователи могут редактировать данные, полученные из Active Directory, в форме проверки в СМЭВ. Если опция выключена, то редактировать пользовательские данные в форме проверки в СМЭВ могут только администраторы или операторы Indeed CM.
Разрешить пользователю просмотр СКЗИ	Если опция включена, список СКЗИ будет доступен пользователям в Сервисе самообслуживания.
Разрешить пользователю удаление документа	Если опция включена, то пользователи могут удалять свои документы в Сервисе самообслуживания.
Разрешить пользователю отзыв устройства	Разрешить пользователю отзывать свои устройства.
Разрешить пользователю назначение устройства	Разрешить пользователю выпустить устройство, которое не назначили на этого пользователя.

Опция	Описание
Разрешить пользователю изменение ответов на секретные вопросы	Если опция включена, то пользователи могут изменять ответы на секретные вопросы после их установки в Сервисе самообслуживания. Если опция выключена, то пользователям не смогут менять ответы на секретные вопросы. Администраторы и операторы могут сбросить ответы на секретные вопросы, чтобы пользователи могли их установить.
Разрешить пользователю добавление устройства	Разрешить пользователю выпуск устройства, не добавленного в систему. Устройство будет добавлено автоматически в процессе выпуска. Опция работает только если включена опция Добавлять устройство автоматически.
Разрешить офлайн-разблокировку	Опция позволяет разблокировать устройство пользователя с привлечением администратора системы, если отсутствует соединение между рабочей станцией пользователя и сервером Indeed CM. Чтобы разблокировать устройство, пользователь должен знать ответы на секретные вопросы. Проверку ответов на секретные вопросы при разблокировке устройства в случае необходимости можно отключить (опция Проверять ответы на секретные вопросы).
Разрешить отмену обновления устройства	Позволяет администратору или оператору Indeed CM отменить обновление содержимого устройства пользователя.

Опция	Описание
Пользователь должен задать ответы на секретные вопросы при первом входе в сервис самообслуживания	Если опция включена, то при первичном входе в Сервис самообслуживания пользователь должен установить секретные вопросы и ответы на них. Вопросы в дальнейшем будут использоваться для аутентификации пользователя. Если опция выключена, то форма установки секретных вопросов при входе в Сервис самообслуживания не будет отображаться. Пользователь сможет установить секретные вопросы позднее в любой момент.
Добавлять устройство автоматически	Опция позволяет добавлять устройство в систему (если оно не было добавлено ранее) в момент выпуска или назначения устройства пользователю. Если опция выключена, то выпуск или назначение устройства, подключенного к компьютеру, но не добавленного в систему, запрещен.

Опция	Описание
Включить отслеживание сертификатов	Если опция включена, то при выпуске устройства Indeed CM найдет на устройстве сторонние сертификаты и закрытые ключи. Поддерживается отслеживание сертификатов, выпущенных удостоверяющими центрами Microsoft CA, КриптоПро УЦ 2.0, ViPNet УЦ 4, Валидата УЦ. Indeed CM может отправить уведомление об истечении срока действия таких сертификатов. Для этого создайте для администратора и пользователя уведомление о событии Отслеживаемые сертификаты истекают в разделе Уведомления. Отслеживаемые сертификаты можно распечатать в Консоли управления и в Сервисе самообслуживания по стандартному шаблону печати сертификата. - Разрешить пользователю выбор сертификатов для отслеживания Включите опцию, чтобы при выпуске/обновлении устройства пользователи могли выбирать сторонние сертификаты для отслеживания. Если опция выключена, то отслеживаются все сторонние сертификаты, хранящиеся на устройстве. - Добавлять отслеживаемые сертификаты в журналы учета Включите опцию, чтобы данные по отслеживаемым сертификатам попадали в журналы учета. Опция доступна, если Журнал учета устройств и сертификатов настроен в разделе Общие функции Мастера настройки Indeed CM.

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..

Опция	Описание
	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.
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 КристоПро DSS администратору	При создании пользователя КристоПро DSS и выпуске сертификата администратор может посмотреть пароль в карточке пользователя.

Опция	Описание
Отображать установленный пароль пользователя КристоПро DSS пользователю	При создании пользователя КристоПро 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 секретный вопрос не создан, 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

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 включайте 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 агента, 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 содержит 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 КристоПро DSS
- Выключение устройства
- Выключение устройства КристоПро DSS
- Выпуск сертификата (Событие доступно для каждого добавленного шаблона сертификата в политику)
- Выпуск сертификата КристоПро DSS (Событие доступно для каждого добавленного шаблона сертификата DSS в политику)
- Выпуск устройства
- Выпуск устройства КристоПро DSS
- Выпуск устройства КристоПро DSS ожидает решения
- Выпуск устройства ожидает решения
- Добавление 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
- Иазначение СКЗИ
- Назначение устройства
- Нарушение условий привязки устройства к агенту
- Нарушение условий привязки устройства к пользователю

- Обнаружена блокировка PIN-кода администратора на устройстве
- Обнаружена блокировка PIN-кода пользователя на устройстве
- Обновление СКЗИ
- Обновление устройства
- Обновление устройства КристоПро DSS
- Обновление устройства КристоПро DSS ожидает решения
- Обновление устройства ожидает решения
- Общие сертификаты истекают
- Одобрение выпуска устройства
- Одобрение выпуска устройства КристоПро DSS
- Одобрение документа
- Одобрение замены устройства
- Одобрение обновления устройства
- Одобрение обновления устройства КристоПро DSS
- Отзыв устройства
- Отзыв устройства КристоПро DSS
- Отклонение выпуска устройства
- Отклонение выпуска устройства КристоПро DSS
- Отклонение замены устройства
- Отклонение обновления устройства
- Отклонение обновления устройства КристоПро DSS
- Отмена назначения устройства
- Отмена обновления устройства
- Отмена обновления устройства КристоПро DSS
- Отслеживаемые сертификаты истекают
- Очистка устройства
- Политика была обновлена
- Политика пользователя была изменена
- Политика пользователя устройства КристоПро DSS была изменена
- Политика устройства КристоПро DSS была обновлена
- Разблокировка пользователя
- Разблокировка устройства
- Сброс 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 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 КристоПро DSS
- Отзыв устройства
- Отзыв устройства КристоПро DSS
- Отклонение выпуска устройства
- Отклонение выпуска устройства КристоПро DSS
- Отклонение замены устройства
- Отклонение обновления устройства
- Отклонение обновления устройства КристоПро DSS
- Отмена назначения устройства
- Отмена обновления устройства
- Отмена обновления устройства КристоПро DSS
- Отслеживаемые сертификаты истекают
- Очистка устройства
- Политика была обновлена
- Политика пользователя была изменена
- Политика пользователя устройства КристоПро DSS была изменена
- Политика устройства КристоПро DSS была обновлена
- Разблокировка пользователя
- Разблокировка устройства
- Сброс PIN-кода
- Сброс ответов на секретные вопросы
- Сброс пароля пользователя
- Содержимое устройства истекает
- Содержимое устройства КристоПро DSS истекает
- Создание кода подключения AirCard к компьютеру
- Удаление документа
- Удаление AirCard от компьютера
- Удаление устройства КристоПро DSS
- Уничтожение/изъятие СКЗИ
- Установка пароля пользователя КристоПро 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 Active Directory
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 КристоПро DSS
- Одобрение замены устройства
- Одобрение обновления устройства
- Одобрение обновления устройства КристоПро DSS
- Отклонение выпуска устройства
- Отклонение выпуска устройства КристоПро DSS
- Отклонение замены устройства
- Отклонение обновления устройства
- Отклонение обновления устройства КристоПро DSS
- Отслеживаемые сертификаты истекают
- Политика была обновлена
- Политика пользователя была изменена
- Политика пользователя устройства КристоПро DSS была изменена
- Политика устройства КристоПро DSS была обновлена
- Управляемые сертификаты истекают
- Управляемые сертификаты КристоПро DSS истекают

Уведомления можно изменить  или удалить .

Уведомления пользователя

Настройте почтовые уведомления для пользователей Indeed CM. Убедитесь, что в свойствах учетных записей пользователей в Active Directory 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 КристоПро DSS
- Одобрение замены устройства
- Одобрение обновления устройства
- Одобрение обновления устройства КристоПро DSS
- Отклонение выпуска устройства
- Отклонение выпуска устройства КристоПро DSS
- Отклонение замены устройства
- Отклонение обновления устройства
- Отклонение обновления устройства КристоПро DSS
- Отслеживаемые сертификаты истекают
- Политика была обновлена
- Политика пользователя была изменена
- Политика пользователя устройства КристоПро DSS была изменена
- Политика устройства КристоПро DSS была обновлена
- Управляемые сертификаты истекают
- Управляемые сертификаты КристоПро 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

Событие и тип события

Управляемые сертификаты истекают ▼

Предупреждение ▼

Тема

Истекает срок действия управляемых сертификатов

Текст сообщения

Paragraph ▼

B

I

@

:=

½=

≡

≡

🖼️

“”

📅 ▼

⋮

На устройстве {cardType} с серийным номером {cardSerialNumber} истекает срок действия сертификатов: {certificates: {n} {templateName}:{serialNumber}:{validTo}}.

Устройство принадлежит пользователю {userName}.

Обновите сертификаты согласно [инструкции](#).

Сохранить

Сбросить

▼ Пример персонализированного шаблона уведомления для пользователя

Событие и тип события

Установка PIN-кода

Информация

Тема

Установка PIN-кода

Текст сообщения

Paragraph

▼

B

I

@

:=

:=

≡

≡

🖼️

“

📅

▼

⋮

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

Назначения политик

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

Политики распространяются на следующие объекты:

- **Active Directory:** Домен (Domain), Контейнер (Container), Подразделение (Organizational Unit)
- **КриптоПро УЦ 2.0:** часть существующей в Центре Регистрации структуры контейнеров (папок) или на весь ЦР
- **Организационная структура Indeed CM,** в узлы которой могут входить:
 - Домен (Domain), Контейнер (Container), Подразделение (Organization Unit), пользователи или группы безопасности Active Directory
 - Часть существующей в Центре Регистрации структуры контейнеров (папок) или на весь ЦР, пользователи или группы безопасности ЦР



ПРИМЕЧАНИЕ

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

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

Создание назначения

Чтобы назначить политику на объект:

1. Нажмите **Создать назначение политики**.
2. В выпадающем списке **Политика** выберите нужную политику.
3. Задайте следующие параметры:
 - **Контейнер** – область действия политики. Контейнером может быть подразделение Active Directory, папка Центра Регистрации КриптоПро УЦ 2.0 или узел

Организационной структуры Indeed CM.

- **Группы** – дополнительный фильтр для распространения политики. Например, на один контейнер с пользователями организации можно назначить несколько политик, которые будут распространяться на пользователей, входящих в определенные группы Active Directory.
- **Приоритет** – значение, определяющее применение той или иной политики к пользователю. Если пользователь попадает под область действия нескольких политик выпуска устройств одного типа (политики Active Directory, ЦР КристоПро УЦ или Организационной структуры), например, состоит в двух группах, расположенных в одном ОУ, то на пользователя будет действовать политика с большим приоритетом.
- **Роли** – если в разделе **Роли** есть хотя бы одна локальная роль, то ее можно добавить в назначение политики и добавить пользователей этой роли.

4. Нажмите **Создать**

Назначение политики можно изменить  или удалить  .

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.

В разделе **Типы устройств** для каждого типа устройств можно задать следующие настройки :

- Значения PIN-кода администратора и пользователя, установленные на устройстве
- Новое значение PIN-кода администратора, на которое меняется PIN-код, установленный на устройстве, после добавления устройства в Indeed CM
- Настройки инициализации устройства при добавлении
- Настройки моделей устройств

Количество поддерживаемых устройств аутентификации и типов постоянно увеличивается.

Если в вашей организации появились устройства нового типа, или наоборот, устройства одного типа перестали использоваться, внесите изменения в Indeed CM.

Добавление и удаление типов устройств

Чтобы добавить тип устройства:

1. Нажмите **Добавить тип устройства**.
2. Выберите файл типа устройства.
3. Нажмите **Добавить**. Чтобы заменить имеющийся файл типа устройства, включите опцию **Заменить существующий**.



ПОДСКАЗКА

Файлы типов устройств находятся в каталоге `\Misc\CardTypes` дистрибутива Indeed CM Server.

▼ **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	<i>JaCarta.xml</i>

Производитель	Модель устройства	Файл типа устройства
Компания «Актив»	Рутокен Lite 1000 Рутокен Lite 1010	<i>RutokenLite.xml</i>
	Смарт-карта Рутокен Lite 1000	<i>RutokenLiteSC.xml</i>
	Рутокен S	<i>RutokenS.xml</i>
	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	<i>RutokenECP.xml</i>
	Смарт-карты: Рутокен PKI 1800 Рутокен ЭЦП 2.0 2100	<i>RutokenECPSC.xml</i>
	Смарт-карты: Рутокен ЭЦП 3.0 NFC 3100 Рутокен ЭЦП 3.0 3100 Рутокен ЭЦП 3.0 3100 SAM 3100	<i>RutokenECPNFCSC.xml</i>
	Рутокен 2151	<i>Rutoken2151.xml</i>
	Смарт-карта Рутокен 2151	<i>Rutoken2151SC.xml</i>
Компания Индид	AirCard	<i>AirCard.xml</i>
ACS	ACOS5-64	<i>Acos5-64.xml</i>

Производитель	Модель устройства	Файл типа устройства
Avest	Avest Key 256A	<i>AvestKey-256-A.xml</i>
Bit4id	ID-One Cosmo	<i>Bit4Id.xml</i>
CRYPTAS	TicTok V2	<i>TicTok_v2.xml</i>
	TicTok V3	<i>TicTok_v3.xml</i>
Cryptovision	ePasslet Suite v3.0, JCOP V3.0	<i>cv-ePassletSuite3.0-JCOP3.0.xml</i>
Feitian	ePass2003 (A1+, A2) BioPass2003	<i>ePass2003.xml</i>
HID	Crescendo C1150 Series	<i>CrescendoC1150.xml</i>
	Crescendo C1300 Series	<i>CrescendoC1300.xml</i>
	Crescendo C2300 Series	<i>CrescendoC2300.xml</i>
ISBC	ESMART Token USB 64K и ESMART Token CARD 64K	<i>EsmartToken64K.xml</i>
	ESMART Token USB 192K и ESMART Token CARD 192K	<i>EsmartToken192K.xml</i>
	ESMART Token ГОСТ	<i>EsmartTokenGOST.xml</i>
	ESMART Token CARD ГОСТ	<i>EsmartTokenGOST-D.xml</i>
Kaztoken	Kaztoken	<i>Kaztoken.xml</i>
	Kaztoken SC	<i>KaztokenSC.xml</i>

Производитель	Модель устройства	Файл типа устройства
Microsoft	Реестр Локального компьютера Реестр Пользователя	<i>Registry.xml</i>
	TPM Virtual Smart Card (Microsoft VSC)	<i>Tpm.xml</i>
	Windows Hello for Business (WHfB)	<i>Whfb.xml</i>
RSA	RSA SecurID 800	<i>RSASecurID.xml</i>

Производитель	Модель устройства	Файл типа устройства
Thales Group	SafeNet eToken PRO 32k	<i>eTokenPro32K.xml</i>
	SafeNet eToken PRO 64k	<i>eTokenPro4.2B.xml</i>
	SafeNet eToken PRO Java 72K OS755 SafeNet eToken 5105 SafeNet eToken 5110 IDCore30B eToken 1.7.7	<i>eTokenProJava72K.xml</i>
	SafeNet eToken 5300 SafeNet eToken Fusion SafeNet eToken Fusion CC	<i>eToken 5300.xml</i>
	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	<i>IDPrimeMD T=0.xml</i>
	SafeNet eToken 5110 CC (940)	<i>IDPrimeMD T=1.xml</i>
	IDPrime 930 IDPrime 930nc	<i>IDPrimeMD v2 T=0.xml</i>
	IDPrime 3940 FIDO	<i>IDPrimeMD Fido T=1.xml</i>
Yubico	YubiKey 5 Series	<i>YubiKey5.xml</i>

Чтобы удалить тип устройства:

1. Выберите тип устройства в списке и нажмите  .

2. Нажмите **Удалить**.

 ПРИМЕЧАНИЕ

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

Редактирование типов устройств

Чтобы редактировать тип устройства, нажмите  напротив нужного типа.

В файле типа устройства можно увидеть 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.

При редактировании типа устройства доступны следующие возможности:

- Просмотреть и изменить значения PIN-кодов администратора и пользователя, установленных на устройстве
- Указать параметры инициализации и PIN-кодов, которые конфигурируют процесс добавления устройств различных типов

Просмотр и изменение PIN-кодов администратора и пользователя

Чтобы увидеть значения PIN-кодов администратора и пользователя, нажмите . Чтобы изменить значение PIN-кода, введите новое значение и нажмите **Сохранить**.

Настройки добавления устройств

Indeed CM позволяет задать отдельные параметры для **добавления** устройств различных типов:

▼ Инициализировать устройство при добавлении

Если опция включена, то при добавлении устройства произойдет следующее:

- Устройство очищается – удаляются сертификаты, добавленные с помощью Indeed CM
- Имя устройства меняется на Empty
- PIN-код администратора меняется на случайный, известный 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, его минимальная длина и количество попыток ввода до блокировки меняются на значения, указанные в файле типа устройства



ПРИМЕЧАНИЕ

Устройства eToken поддерживают инициализацию с любым состоянием и значением PIN-кода администратора.

▼ 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.

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 добавляемого устройства не найдена или настройки моделей отсутствуют, то устройство настраивается по умолчанию.

Если в вашей организации используются модели устройств, которых нет в списке моделей, поддерживаемых Indeed CM, обратитесь в службу технической поддержки компании Индид.

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 моделей устройств

JaCarta PKI/ГОСТ/Flash

PIN-код администратора

PIN-код пользователя

PIN-код администратора (ГОСТ)

PIN-код пользователя (ГОСТ)

☒ Инициализировать устройство при добавлении

☒ Устанавливать неслучайный PIN-код администратора

☒ Устанавливать неслучайный PIN-код администратора (ГОСТ)

[+ Добавить настройки модели устройства](#)

Сохранить

Отмена

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

Имя

Q

▲

ООО Тестовая компания

Бухгалтерия

Кадры

Юристы

▲

Филиал в Воронеже

Менеджеры

Производство

Филиал в Самаре

+

Добавить

-

Удалить

Политики

☐

Общее имя(CN)

Контейнер

☐

Бухгалтеры головного офиса

indeed-id.local

+

Добавить

-

Удалить

Добавить объекты каталога

☐ Контейнер ☒ Группа ☐ Пользователь

indeed-id.local



Общее имя(CN)



Добавить

Отмена

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	✓	✓
Одобрение данных запроса СМЭВ	✓	✓
Назначение пользователя УЦ	✓	✓
Назначение обучающих курсов	✓	✗
Завершение обучающих курсов	✓	✗
Одобрение завершения обучающих курсов	✓	✗
Отмена обучающих курсов	✓	✗
Конфигурация		
Просмотр политики	✓	✗

Привилегия	Администратор	Оператор
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	✓	✗
Просмотр организационной структуры	✓	✗
Изменение организационной структуры	✓	✗

Привилегия	Администратор	Оператор
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	✓	✗
Изменение типа СКЗИ	✓	✗
Удаление типа СКЗИ	✓	✗

Привилегия	Администратор	Оператор
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	✓	✗
Изменение уведомлений администратора	✓	✗
Удаление уведомлений администратора	✓	✗

Привилегия	Администратор	Оператор
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	✓	✓
Устройства		
Просмотр репозитория устройств	✓	✓

Привилегия	Администратор	Оператор
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	✓	✓
Замена устройства	✓	✓
Сброс PIN-кода	✓	✗

Привилегия	Администратор	Оператор
Изменение PIN-кода	✓	✗
Блокировка устройства	✓	✗
Разблокировка устройства	✓	✓
Печать устройства	✓	✓
Отзыв устройства	✓	✓
Очистка устройства	✓	✓
Отмена назначения устройства	✓	✓
Удаление устройства	✓	✓
Сертификаты		
Просмотр репозитория сертификатов	✓	✓
Устройства AirCard		
Изменение привязки AirCard	✓	✓
Удаление AirCard	✓	✓
Агенты		
Просмотр репозитория агентов	✓	✓
Изменение привязки устройства к агенту	✓	✓

Привилегия	Администратор	Оператор
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		
Просмотр репозитория документов	✓	✓
Добавление документа	✓	✓
Изменение документа	✓	✓
Удаление документа	✓	✓

Привилегия	Администратор	Оператор
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	<i>C:\inetpub\wwwroot\cm\mc\wwwroot\content\reque</i>
	Сертификат	<i>C:\inetpub\wwwroot\cm\mc\wwwroot\content\cert_i</i>
	Запроса на отзыв сертификата	<i>C:\inetpub\wwwroot\cm\mc\wwwroot\content\revoc</i>
Сервис самообслуживания	Запрос на сертификат	<i>C:\inetpub\wwwroot\cm\ss\wwwroot\content\reques</i>
	Сертификат	<i>C:\inetpub\wwwroot\cm\ss\wwwroot\content\cert_r</i>
	Запрос на отзыв сертификата	<i>C:\inetpub\wwwroot\cm\ss\wwwroot\content\revoca</i>

Linux

Компонент	Документ	Путь к файлу шаблона

Консоль управления	Запрос на сертификат	<i>/opt/indeed/cm/mc/wwwroot/content/request_ru.xml</i>
	Сертификат	<i>/opt/indeed/cm/mc/wwwroot/content/cert_ru.xml</i>
	Запрос на отзыв сертификата	<i>/opt/indeed/cm/mc/wwwroot/content/revocationReq</i>
Сервис самообслуживания	Запрос на сертификат	<i>/opt/indeed/cm/ss/wwwroot/content/request_ru.xml</i>
	Сертификат	<i>/opt/indeed/cm/ss/wwwroot/content/cert_ru.xml</i>
	Запрос на отзыв сертификата	<i>/opt/indeed/cm/ss/wwwroot/content/revocationRequ</i>

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
<code>user_name</code>	Общее имя пользователя
<code>user_logonName</code>	Логин пользователя
<code>user_email</code>	Email пользователя
<code>user_organization</code>	Организация
<code>user_jobTitle</code>	Должность

Информация об СКЗИ

Атрибут	Описание атрибута
<code>skzi_timeCreated</code>	Время добавления СКЗИ в Indeed CM
<code>skzi_skziType</code>	Тип СКЗИ
<code>skzi_objectType</code>	Тип объекта СКЗИ
<code>skzi_serialNumber</code>	Серийный номер СКЗИ
<code>skzi_instanceNumber</code>	Номер экземпляра СКЗИ
<code>skzi_creationData_creator</code>	Имя изготовителя СКЗИ
<code>skzi_creationData_timeCreated</code>	Время изготовления СКЗИ
<code>skzi_creationData_docNumber</code>	Номер документа об изготовлении СКЗИ

Атрибут	Описание атрибута
<code>skzi_sendingData_recipient</code>	Имя сотрудника, который подтверждает получение СКЗИ
<code>skzi_sendingData_timeSent</code>	Время передачи СКЗИ
<code>skzi_sendingData_docNumber</code>	Номер сопроводительного письма при передаче СКЗИ
<code>skzi_sendingData_timeConfirmed</code>	Время подтверждения получения СКЗИ
<code>skzi_sendingData_confirmationDocNumber</code>	Номер документа о подтверждении получения СКЗИ
<code>skzi_returnData_timeReturned</code>	Время возврата СКЗИ
<code>skzi_returnData_docNumber</code>	Номер сопроводительного письма при возврате СКЗИ
<code>skzi_returnData_timeConfirmed</code>	Время подтверждения возврата СКЗИ
<code>skzi_returnData_confirmationDocNumber</code>	Номер документа о подтверждении возврата СКЗИ
<code>skzi_issueData_timeIssued</code>	Время выдачи СКЗИ
<code>skzi_issueData_docNumber</code>	Номер сопроводительного письма при выдаче СКЗИ
<code>skzi_installationData_installer</code>	Ф.И.О. сотрудников органа криптографической защиты, пользователей СКЗИ, производивших установку СКЗИ
<code>skzi_installationData_timeInstalled</code>	Время установки СКЗИ

Атрибут	Описание атрибута
<code>skzi_installationData_docNumber</code>	Номер документа об установке СКЗИ
<code>skzi_installationData_hardwareId</code>	Номер аппаратного средства, на котором установлено или к которому подключено СКЗИ
<code>skzi_installationData_location</code>	Место установки СКЗИ
<code>skzi_destructionData_destructor</code>	Ф.И.О. сотрудников органа криптографической защиты, пользователей СКЗИ, производивших уничтожение/изъятие СКЗИ
<code>skzi_destructionData_timeDestroyed</code>	Время уничтожения/изъятия СКЗИ
<code>skzi_destructionData_docNumber</code>	Номер акта или расписки об уничтожении СКЗИ
<code>skzi_comment</code>	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
<code>user_name</code>	Общее имя пользователя
<code>user_logonName</code>	Логин пользователя
<code>user_email</code>	Email пользователя
<code>user_organization</code>	Организация
<code>user_jobTitle</code>	Должность

Информация об обучении по работе с СКЗИ

Атрибут	Описание атрибута
<code>training_courseName</code>	Название обучающего курса.
<code>training_initiator</code>	Имя оператора, заполнившего номер заключения и одоббившего прохождение обучения, в формате Common name.
<code>training_initiator_logonName</code>	Имя оператора, заполнившего номер заключения и одоббившего прохождение обучения, в формате Logon name.
<code>training_certificateNumber</code>	Номер заключения о прохождении обучения.
<code>training_completionDate</code>	Время завершения обучения в сокращенном формате – дата.
<code>training_completionDate_full</code>	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, КристоПро 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 определяют, какие пользователи получают 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

Шаблоны администратора

Событие и тип события

Срок действия лицензии истек

Предупреждение

Тема

Срок действия лицензии истек

Текст сообщения

Paragraph

B

I





















Срок действия лицензии истек.

Лицензии: {licenses:

{n}. Тип лицензии: {licenseType}; количество лицензий: {licenseCount}; срок действия (до): {validTo}}

Сохранить

Сбросить

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**
- **Количество** – общее количество лицензий
- **Используется** – количество лицензий, занятых пользователями
- **Осталось** – количество свободных лицензий



ПОДСКАЗКА

Иконка предупреждения  появляется, если:

- 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 выполнить поиск пользователей, создать и редактировать пользователей, создать и редактировать контейнеры с пользователями, импортировать файл с пользователями.



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 Active Directory.

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.

Поле	Обязательно/ необязательно	Описание
CN	Необязательно	Имя пользователя в формате CommonName. Если значение не указано, имя пользователя формируется из значений <code>LastName</code> и <code>FirstName</code> .
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 СМ 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
;Арте́м;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.

Загрузка фотографии

Фотография отображается в карточке пользователя, если она есть в профиле пользователя в Active Directory.

Чтобы добавить фотографию, нажмите **Загрузить фотографию**.

Параметры загрузки фотографии

- Фотография пользователя может быть записана в атрибуты `thumbnailPhoto` или `jpegPhoto`. Чтобы выбрать атрибут, откройте Мастер настройки Indeed CM и перейдите в раздел **Каталог пользователей** → **Active Directory** → **Расширенные настройки**.
- Сервисная учетная запись для работы с **каталогом пользователей** 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 КристоПро 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 **КристоПро 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 КристоПро 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 КристоПро 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 КристоПро 2.0**.
3. Введите имя пользователя КристоПро 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 КристоПро 2.0** и **Отменить привязку**.

Чтобы создать нового пользователя в каталоге КристоПро УЦ 2.0:

1. Перейдите в карточку пользователя.
2. Нажмите **Пользователь КристоПро 2.0** и перейдите на вкладку **Создать**.

Вы можете отредактировать данные создаваемого пользователя. Перечень полей для редактирования зависит от настроек используемого удостоверяющего центра КристоПро.



ПРИМЕЧАНИЕ

При создании пользователя КристоПро 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.

Действие доступно, если:

- В разделе **Общие функции** Мастера настройки Indeed CM включена опция **Сброс пароля пользователя в Active Directory**.

- В разделе **Каталог пользователей** Мастера настройки Indeed CM в настройках каталога пользователей Active Directory 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) в **Active Directory**.

Нажмите **Сбросить пароль пользователя** в карточке пользователя, задайте новый пароль и время истечения срока действия пароля, после которого значение пароля сменится на случайное. Дополнительно можно включить опцию **Пользователь должен поменять пароль при первом входе**.

ПРИМЕЧАНИЕ

Установленный пароль не будет записан 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

Как разблокировать устройство в режиме онлайн или офлайн



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



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

Управляемые сертификаты

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 сертификаты

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.

Чтобы в карточке устройства отображалась информация о сторонних сертификатах, хранящихся на устройстве, настройте отслеживание сторонних сертификатов. Для этого перейдите в настройки политики использования устройств в раздел **Поведение** и включите опцию **Включить отслеживание сертификатов**.

Indeed CM может отправить уведомление администраторам и пользователям об истечении срока действия отслеживаемых сертификатов. Для этого перейдите в настройки политики использования устройств в раздел **Уведомления** и создайте уведомление о событии *Отслеживаемые сертификаты истекают*.

Общие сертификаты

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**.

Indeed CM может отправить уведомление администраторам об истечении срока действия общих сертификатов. Для этого перейдите в настройки политики использования устройств в раздел

Уведомления и 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 КристоПро 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.

Состояние сертификата	Описание
Одобен	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

Во время процедуры выпуска устройство персонализируется для пользователя. В соответствии с **настройками назначенной политики** устройство инициализируется, генерируются ключевые пары, выпускаются сертификаты и записываются в память устройства.

Процесс получения сертификата включает следующие шаги:

1. Пользователь создает запрос на сертификат по заданному шаблону и генерирует на устройстве пару ключей (открытый и закрытый) с использованием криптопровайдера (CSP).
2. Пользователь формирует запрос на сертификат, в который записывается открытый ключ.
3. Пользователь подписывает запрос закрытым ключом.
4. Оператор удостоверяющего центра (УЦ) подписывает запрос ключом сервисной учетной записи с необходимыми правами, которыми владеет сервер Indeed CM.
5. Запрос отправляется в УЦ.
6. УЦ одобряет или отклоняет запрос. После одобрения в УЦ выпущенный сертификат записывается на носитель с помощью криптопровайдера.

Процедура выпуска

Чтобы выпустить устройство пользователю, выполните следующие действия:

1. Перейдите в раздел **Пользователи** и выполните поиск пользователя.
2. Нажмите на логин и перейдите в карточку пользователя.
3. Нажмите **Выпустить устройство**.
4. Выберите шаблоны, по которым будут сформированы сертификаты для записи на устройство. Обязательные сертификаты запишутся на устройство автоматически.
5. Если в политике использования устройств настроена **Интеграция со СМЭВ** и сертификат выпускается по шаблону для КриптоПро УЦ 2.0 или Валидата УЦ, отобразится **форма проверки СМЭВ**. Проверьте данные пользователя.
6. Подключите устройство к компьютеру и задайте следующие настройки:

▼ Инициализировать устройство

Опция **Инициализировать устройство** позволяет отключить и включить инициализацию для конкретного устройства.

При выпуске устройства с инициализацией все данные на устройстве будут удалены.

Параметры инициализации настраиваются в разделе **Выпуск** политики использования устройств.

▼ Имя устройства

Имя устройства выставится автоматически, если в разделе **Выпуск** политики использования устройств задана опция **Генерировать имя устройства автоматически**.

▼ Комментарий к устройству

Указание комментария обязательно, если в разделе **Выпуск** политики использования устройств задана опция **Требовать указания комментария к устройству**.

Если в [параметрах шаблона сертификата КриптоПро УЦ 2.0](#) включена опция **Использовать комментарий устройства в качестве комментария пользователя к запросу на сертификат**, то текст комментария будет добавлен в запрос.

▼ Теги

Добавьте теги, если их создал администратор в разделе **Конфигурация** → **Теги**.

Добавление тегов обязательно, если в разделе **Выпуск** политики использования устройств задана опция **Требовать указания тегов к устройству**.

▼ Номер и дата документа

Выставите данные о документе, на основании которого будет изготовлено СКЗИ с информацией об устройстве.

Поле **Номер и дата документа** отображается, если:

- Устройство поддерживает аппаратную криптографию.
- Устройство не добавлено в Indeed CM, и в разделе **Поведение** политики использования устройств задана опция **Добавлять устройство автоматически**.

7. Раздел **Дополнительно** отображается, если устройство не было ранее добавлено в Indeed CM. Введите нужный PIN-код в зависимости от настроек инициализации:

Выпуск с инициализацией

Устройство будет инициализировано, если задать опцию **Инициализировать устройство** (шаг 6) и **настроить параметры инициализации при выпуске**. Все данные на устройстве будут удалены.

1. Введите **PIN-код администратора**. Поле отображается, если устройство не добавлено в Indeed CM и в разделе **Поведение** политики использования устройств задана опция **Добавлять устройство автоматически**.



ПРИМЕЧАНИЕ

Если поле **PIN-код администратора** оставить пустым, то установится значение, указанное в разделе **Типы устройств**.

Поддерживается ввод PIN-кодов для нескольких областей. Например, для PKI и ГОСТ на устройствах JaCarta.

2. Если вы выпускаете устройство eToken со встроенной защитой от форматирования, то укажите ключ инициализации.
3. Нажмите **Выпустить**.

1. Введите **PIN-код пользователя**.
2. Введите **PIN-код администратора**. Поле отображается, если устройство не добавлено в Indeed CM и в разделе **Поведение** политики использования устройств задана опция **Добавлять устройство автоматически**.

 ПРИМЕЧАНИЕ

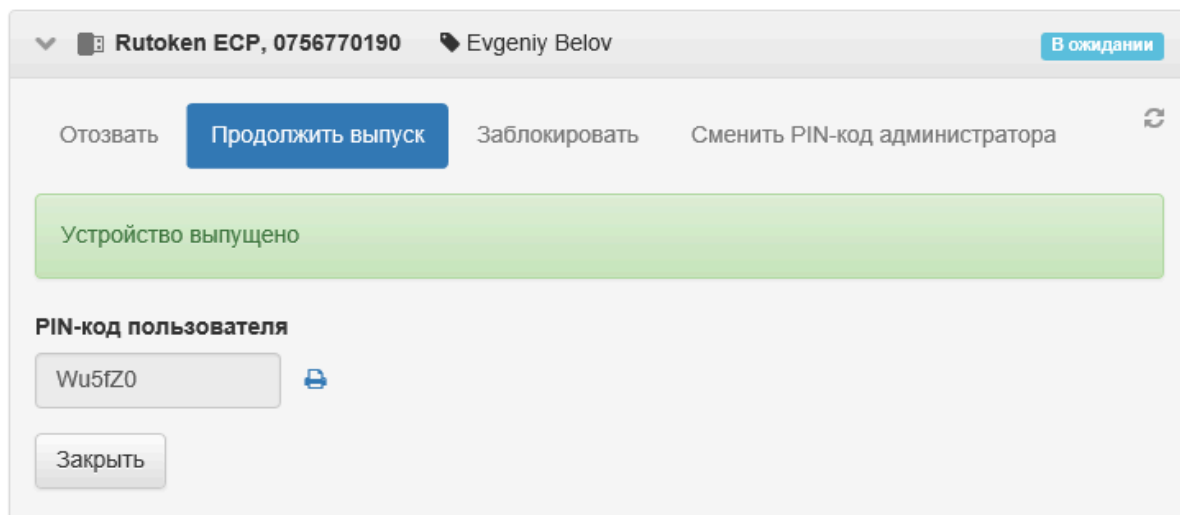
Если поля **PIN-код администратора** и **PIN-код пользователя** оставить пустыми, то установятся значения, указанные в разделе **Типы устройств**. Поддерживается ввод PIN-кодов для нескольких областей. Например, для PKI и ГОСТ на устройствах JaCarta.

3. Нажмите **Выпустить**.
 4. Если устройство содержит сторонние сертификаты, Indeed CM может их обнаружить и внести информацию о таких сертификатах в систему – отследить. Окно выбора сертификатов для отслеживания отображается, если в разделе **Поведение** политики использования устройств задана опция **Включить отслеживание сертификатов**. Выберите сертификаты для отслеживания, если они есть на устройстве, и нажмите **ОК**.
8. Если в разделе **Выпуск** политики использования устройств задана опция **Установить случайный PIN-код пользователя**, то после выпуска устройства отобразится PIN-код пользователя.

▼ Как передать PIN-код пользователю

Если в разделе **Уведомления** настроена рассылка уведомлений по электронной почте, PIN-код можно отправить на электронную почту пользователя и его руководителя.

PIN-код можно распечатать и отправить в конверте. Нажмите . PIN-код будет сохранен в файле *PinEnvelope.pdf*.



The screenshot shows the 'Rutoken ECP, 0756770190' window for user 'Evgeniy Belov'. The status is 'В ожидании' (Waiting). The main area has buttons: 'Отозвать', 'Продолжить выпуск' (highlighted in blue), 'Заблокировать', and 'Сменить PIN-код администратора'. A green bar indicates 'Устройство выпущено'. Below, the 'PIN-код пользователя' is displayed as 'Wu5fZ0' with a print icon. A 'Заккрыть' button is at the bottom.

⚠ ПРИМЕЧАНИЕ

Параметры печати содержатся в шаблоне

C:\inetpub\wwwroot\cm\mc\wwwroot\content\pinenvelope.xml.

По умолчанию на печать выводится информация о пользователе (имя и email) и устройстве (тип, серийный номер и PIN-код пользователя). Для изменения шаблона печати отредактируйте файл *pinenvelope.xml*.

9. По завершении выпуска устройства нажмите **Заккрыть**.

После выпуска устройства в разделе **Назначенные устройства** карточки пользователя отобразятся сведения об устройстве.

Контроль выпуска

Выпуск устройства можно приостановить, если регламент вашей организации предусматривает проверку запроса на сертификат в УЦ.

Чтобы настроить проверку запроса на сертификат в УЦ:

1. Откройте раздел **Конфигурация** и перейдите в настройки политики.
2. Откройте раздел **Удостоверяющие центры** → **Шаблоны** используемых УЦ.
3. Отключите опцию **Автоматически одобрять запрос на сертификат**.

В окне выпуска устройства появится сообщение *Выпуск устройства ожидает решения*.

Устройство переходит в состояние *В ожидании*. Это означает, что запрос на выпуск устройства перешел в стадию рассмотрения.

Если запрос на сертификат одобрен в УЦ, то сертификат получает статус *Одобен* и записывается на устройство. Нажмите **Продолжить выпуск устройства** в карточке устройства.

Если запрос отклонен в УЦ, **отзовите и очистите устройство**, после чего **начните выпуск устройства заново**.

Если в политике **настроена** автоматическая рассылка уведомлений по электронной почте, то вам придет уведомление о статусе одобрения. Если автоматическая рассылка уведомлений не настроена, дождитесь появления кнопки **Продолжить обновление устройства** в карточке устройства.



ПРЕДУПРЕЖДЕНИЕ

Если на устройство одновременно записываются несколько сертификатов, устройство можно выпустить, когда оба запроса на сертификат одобрены в УЦ.

Если один из сертификатов был одобрен автоматически и имеет статус *Действительный*, он будет записан на устройство вместе со вторым сертификатом.

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. Для этого настройте интеграцию со СМЭВ в **политике использования устройств**.

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 в двух случаях:

- Если проверка занимает больше 15 минут
- Если проверка завершилась с ошибкой



ПРИМЕЧАНИЕ

Опция доступна для администраторов и операторов Indeed CM с привилегией **Одобрение данных запроса СМЭВ**. Привилегия назначается в разделе **Конфигурация → Роли**.

Публикация выпущенных сертификатов

Сертификаты, выпущенные и записанные на устройство, можно опубликовать в различные хранилища.

Чтобы настроить публикацию сертификатов в хранилища, в разделе **Конфигурация** откройте настройки политики использования устройств, перейдите в раздел **Шаблоны** и нажмите  напротив нужного шаблона сертификата. Включите следующие опции:

- **Устанавливать сертификат в локальное хранилище**, чтобы опубликовать сертификат в локальное хранилище сертификатов пользователя на рабочей станции.
- **Публиковать сертификат в каталоге пользователей**, чтобы опубликовать сертификат в каталог пользователей в Active Directory.
- **Публиковать сертификат в ЕСИА**, чтобы опубликовать сертификат в Единой системе идентификации и аутентификации (ЕСИА).
- **Публиковать сертификат в файловое хранилище**, чтобы опубликовать сертификат в файловое хранилище.
- **Публиковать сертификат в ЦФТ**, чтобы опубликовать сертификат в базе приложений ЦФТ.

Назначение

При назначении устройство закрепляется за пользователем, чтобы пользователь мог выпустить это устройство самостоятельно в Сервисе самообслуживания.

Условия назначения устройств

Одно устройство может одновременно принадлежать только одному пользователю. У одного пользователя может быть несколько устройств.

Пользователи могут назначать себе устройства самостоятельно в Сервисе самообслуживания. Чтобы это настроить, перейдите в настройки политики использования устройств, действующей на пользователя, и откройте раздел **Поведение**. Включите опцию **Разрешить пользователю назначение устройства**.

Как назначить устройство пользователю

Чтобы назначить устройство, перейдите в карточку пользователя и нажмите **Назначить устройство**. Откроется окно назначения устройства. В зависимости от того, есть ли у вас доступ к устройству, выберите опцию:

- Устройство доступно
- Устройство недоступно

Устройство доступно

Назначить зарегистрированное устройство

Если устройство было ранее **добавлено** в Indeed CM, подключите его к рабочей станции и выберите в выпадающем списке **Устройство**. Нажмите **Назначить**.

Назначить незарегистрированное устройство

Если устройство не было ранее добавлено в Indeed CM, то его можно добавить автоматически при назначении. Чтобы настроить возможность добавить устройство при назначении, перейдите в настройки политики использования устройств, действующей на пользователя, откройте раздел **Поведение** и включите опцию **Добавлять устройство автоматически**.

Чтобы добавить и назначить устройство, подключите его к рабочей станции и выберите 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**.

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

PIN-код устройства пользователя можно сбросить. В этом случае PIN-код, заданный пользователем, изменяется на значение, указанное в разделе **Типы устройств**.

ⓘ ПРИМЕЧАНИЕ

Если в разделе **Выпуск** политики использования устройств включена опция **Инициализировать устройство**, то PIN-код пользователя изменится на значение, указанное в параметрах инициализации типа устройства.

Чтобы сбросить PIN-кода пользователя:

1. Перейдите в раздел **Пользователи** и выполните поиск пользователя.
2. Нажмите на логин и перейдите в карточку пользователя.
3. Выберите нужное устройство и раскройте карточку устройства.
4. Нажмите **Сбросить PIN-код**.
5. Подключите устройство и нажмите **Сбросить**. Если устройство недоступно, выберите опцию **Сбросить PIN-код пользователя на агенте**, чтобы создать задачу для агента, установленного на рабочей станции пользователя.

Когда администратор сбросит PIN-код, пользователь сможет задать новый PIN-код самостоятельно в **Сервисе самообслуживания**.

Разблокировка

Устройство блокируется, если пользователь ввел неверный PIN-код устройства больше определенного количества раз.

Максимальное количество попыток ввода PIN-кода пользователем задает администратор в разделе **Выпуск** → **Инициализация устройства** политики использования устройств.

Существует два режима разблокировки устройства пользователя: онлайн и офлайн.

Онлайн

Онлайн-разблокировка осуществляется пользователем в окне входа ОС Windows.

Пользователь отвечает на секретные вопросы, задает и подтверждает новый PIN-код, после чего устройство разблокируется.

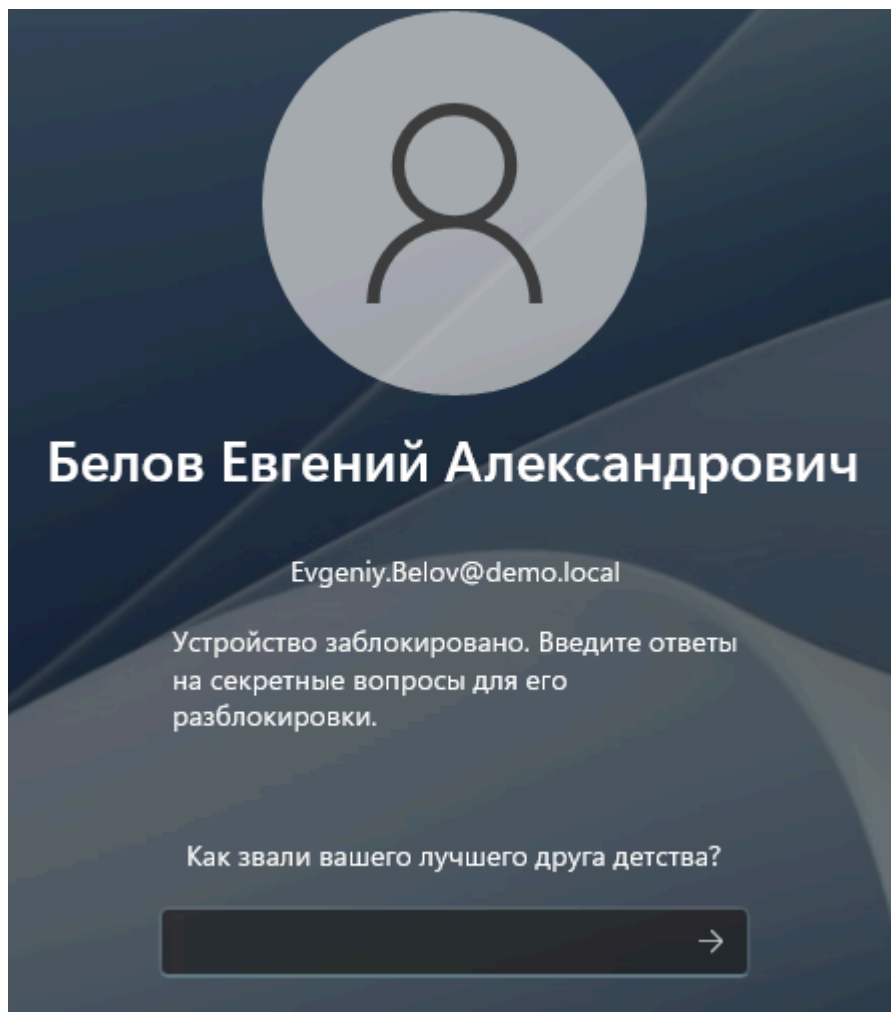
Обязательные условия для онлайн-разблокировки:

- Рабочая станция пользователя, к которой подключено заблокированное устройство, связана с сервером Indeed CM.
- Пользователь задал ответы на секретные вопросы в Сервисе самообслуживания.

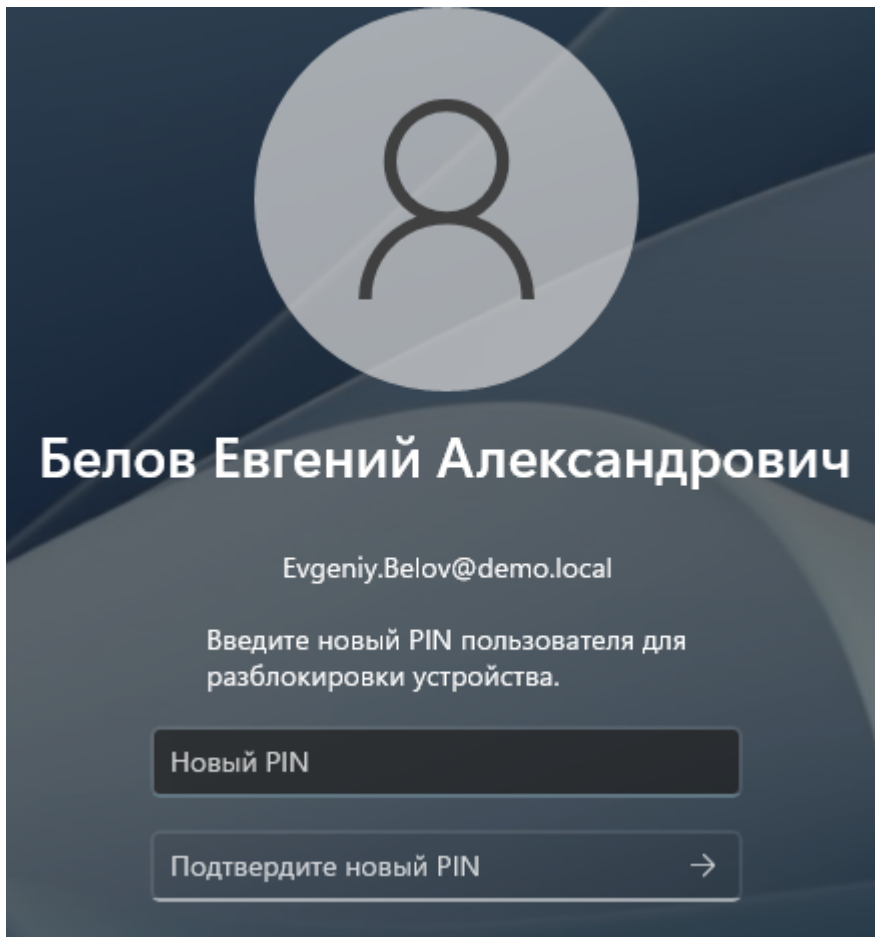
Если секретные вопросы пользователя не установлены, онлайн-разблокировка устройства будет недоступна. Разблокировать устройство можно в офлайн-режиме.

Пример онлайн-разблокировки устройства в окне входа ОС Windows 11

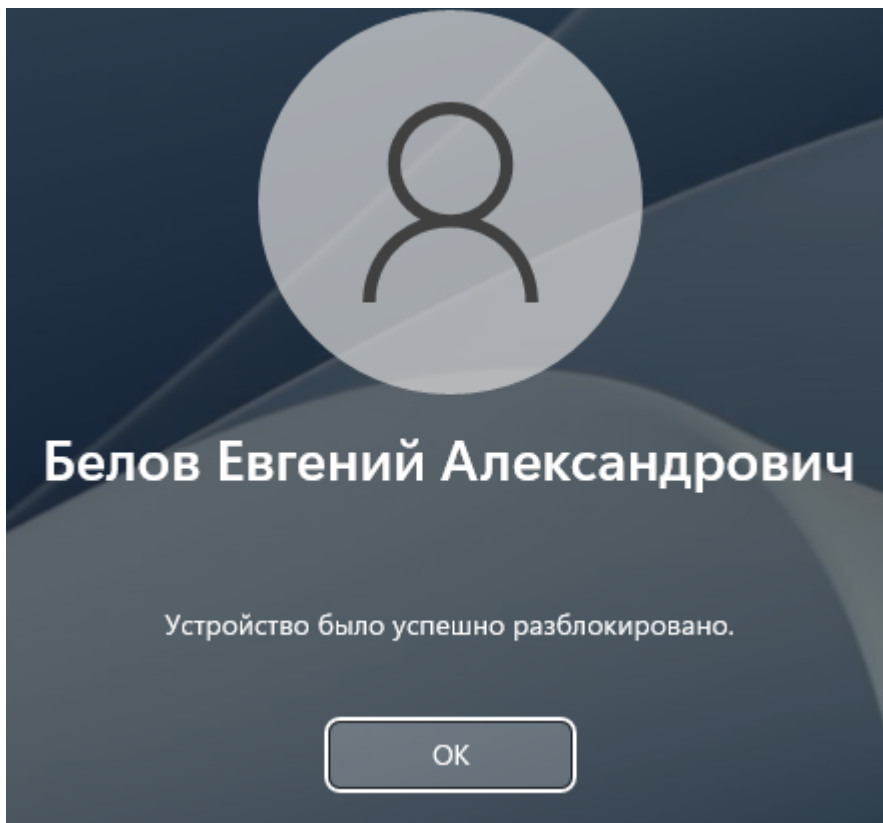
1. Введите ответы на секретные вопросы и нажмите .



2. Введите **Новый PIN** и его **Подтверждение**.



3. В случае успешной разблокировки устройства появится сообщение.



Механизм разблокировки устройства в ОС Windows других версий выглядит похожим образом.

Офлайн

Разблокировать устройство офлайн можно в окне входа Windows или в Windows сессии.

Окно входа



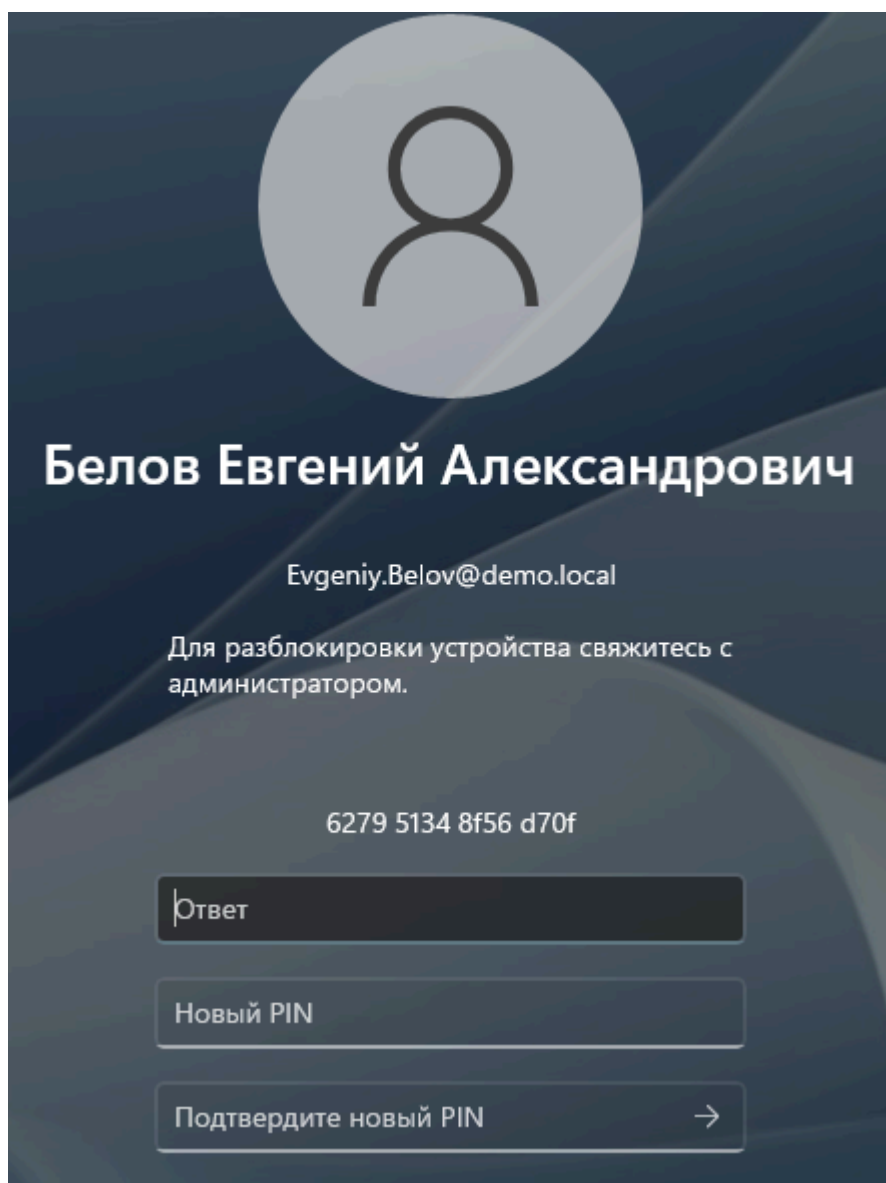
ПРЕДУПРЕЖДЕНИЕ

Разблокировка устройства на экране входа в Windows не поддерживается при удаленном подключении через Remote Desktop.

Офлайн-разблокировка осуществляется оператором Indeed CM по принципу аутентификации вида запрос-ответ (challenge-response authentication mechanism).

При исчерпании заданного числа попыток ввода PIN-кода пользователь получает сообщение, что его устройство заблокировано. Вместе с сообщением пользователь получает уникальный код-запрос из 16 символов. Пользователю необходимо связаться с оператором системы (например, по телефону), подтвердить свою личность, ответив на секретные вопросы, и сообщить полученный код.

Пример экрана офлайн-разблокировки устройства в окне входа ОС Windows 11



The image shows a user card for Evgeniy Belov. At the top is a circular placeholder for a profile picture. Below it is the name "Белов Евгений Александрович" in a large, bold font. Under the name is the email address "Evgeniy.Belov@demo.local". A message in Russian states: "Для разблокировки устройства свяжитесь с администратором." (To unlock the device, contact the administrator.). Below this is a unique identifier "6279 5134 8f56 d70f". At the bottom are three input fields: the first is labeled "Ответ" (Answer) and contains a cursor; the second is labeled "Новый PIN" (New PIN); the third is labeled "Подтвердите новый PIN" (Confirm new PIN) and has a right-pointing arrow button.

Белов Евгений Александрович

Evgeniy.Belov@demo.local

Для разблокировки устройства свяжитесь с администратором.

6279 5134 8f56 d70f

Ответ

Новый PIN

Подтвердите новый PIN →

Оператор системы открывает карточку пользователя и в перечне действий над устройством выбирает пункт **Разблокировать**. Прежде чем выполнить генерацию ответного кода для разблокировки устройства, администратор системы задает секретный вопрос (или несколько вопросов, в зависимости от настроек политики использования устройств) и вводит полученный от пользователя ответ в соответствующую форму.



ПРИМЕЧАНИЕ

Опцию **Разрешить офлайн-разблокировку** можно отключить в разделе **Поведение** политики использования устройств. В этом случае кнопка **Разблокировать** в карточке устройства будет недоступна.

Необходимость проверки ответов на секретные вопросы при офлайн-разблокировке определяется опцией **Проверять ответы на секретные вопросы** в разделе **Поведение** политики использования устройств.

Назначенные устройства

▼ Rutoken ECP, 0756770190

Выпущено

Сбросить PIN-код

Разблокировать

Выключить

Отозвать

Заменить

Обновить

↺

Пожалуйста, ответьте на секретные вопросы

Как называется наша компания?

ОК

Отмена

Если ответы на все вопросы даны верно, то оператор вводит код, полученный от пользователя, и система генерирует ответный код, который оператор сообщает пользователю.

Назначенные устройства

▼ Rutoken ECP, 0756770190

Выпущено

Сбросить PIN-код

Разблокировать

Выключить

Отозвать

Заменить

Обновить

↺

Пожалуйста, введите запрос и нажмите 'Получить ответ'

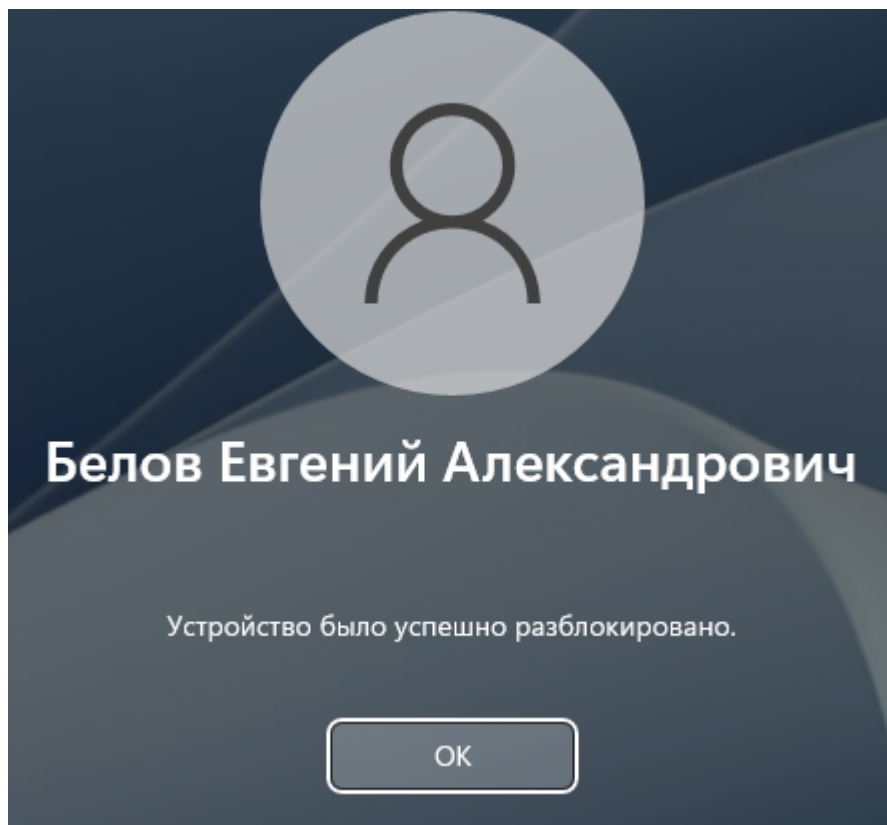
Запрос

Ответ

Получить ответ

Закрыть

Пользователь вводит код, полученный от оператора, и задает новый PIN-код устройства. В случае успешной разблокировки отображается соответствующее сообщение.



Механизм разблокировки устройства в ОС Windows других версий выглядит похожим образом.

Сессия

Если устройство не используется для входа на рабочую станцию и было заблокировано, то для его разблокировки применяется утилита Indeed CM - Unblock (*Пуск – Все программы – Indeed*).

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.

Выключение и включение

Устройство пользователя можно выключить на определенный промежуток времени и затем снова включено. Например, на период отпуска сотрудника.

Оператор может выключить и включить устройство без подключения устройства 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. Выберите нужное устройство и раскройте карточку устройства.
4. Нажмите **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. Выберите нужное устройство и раскройте карточку устройства.
4. Нажмите **Включить**.

ОТЗЫВ

Оператор или пользователь могут отозвать устройство, если оно повреждено, утеряно, изъято, или нуждается в обновлении.



ПРЕДУПРЕЖДЕНИЕ

Если в параметрах шаблонов сертификатов используемого УЦ включена опция **Отзывать сертификат при отзыве/выключении устройства**, то все сертификаты на устройстве отзываются без возможности восстановления.

Чтобы отозвать устройство:

1. Перейдите в раздел **Пользователи** и выполните поиск пользователя.
2. Нажмите на логин и перейдите в карточку пользователя.
3. Выберите нужное устройство и раскройте карточку устройства.
4. Нажмите **Отозвать**.
5. Укажите **Причину отзыва**:
 - *Устройство неисправно* – устройство технически неисправно или уничтожено.
 - *Устройство утеряно* – устройство утеряно.
 - *Обновление устройства* – обновление устройства (например, замена старого устройства на новое).
 - *Изъятие устройства* – удаление устройства из системы в связи с увольнением сотрудника (значение по умолчанию).
 - *Компрометация устройства* – подозрение на компрометацию ключа, при этом устройство не утеряно и исправно.



ПРИМЕЧАНИЕ

Если устройство отзывается по причинам **Устройство утеряно** или **Компрометация устройства**, то все сертификаты на устройстве отзываются.

6. Нажмите **Отозвать**, если устройство доступно. Если устройство недоступно, создайте задачу на агенте – выберите опцию **Очистить устройство на агенте**.

Причина отзыва устройства отображается в карточке пользователя. При попытке использования отозванного устройства для аутентификации пользователь получит сообщение, что его сертификаты отозваны.

Изъятие

Вы можете **заменить** или изъять устройство, которое было отозвано. После изъятия устройство 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. Выберите нужное устройство и раскройте информацию о нем.
4. Нажмите **Изъять**.
5. В зависимости от того, есть ли у вас доступ к устройству, выберите:
 - **Устройство недоступно (потеряно или повреждено)**
 - **Устройство доступно**
6. Если устройство недоступно, нажмите **Изъять**.
Если устройство доступно, подключите его к рабочей станции и при необходимости выберите:

▼ Очистить устройство

После изъятия с устройства удалятся все сертификаты, записанные через Indeed CM. Сертификаты, запросы, ключи, записанные вне Indeed CM, не удаляются.

Введите **PIN-код пользователя**, который установится на устройстве после изъятия. Если не задать PIN-код пользователя, то после изъятия устанавливается PIN-код, указанный в файле [типа устройства](#).

ⓘ ПРИМЕЧАНИЕ

Обязательно задайте PIN-код пользователя при изъятии с очисткой, если PIN-код, указанный в файле типа устройства, не соответствует требованиям к PIN-коду, установленным для данного типа устройства в политике использования устройств в разделе **Выпуск → Инициализация**.

▼ Инициализировать устройство

После изъятия с устройства удаляются все данные.

Для инициализации используются параметры, заданные для опции

Инициализировать устройство при добавлении в разделе **Конфигурация → Типы устройств**.

7. Если при выпуске устройства было создано СКЗИ, то автоматически выставятся **Номер и дата документа**, на основании которого происходит уничтожение/изъятие СКЗИ. В поле **Пользователь, производивший уничтожение/изъятие** через запятую указывается ФИО сотрудников органа криптографической защиты, пользователей СКЗИ, производивших уничтожение/изъятие СКЗИ.
8. Нажмите **Изъять**.

Замена

Indeed CM позволяет выполнить временную или постоянную замену устройств пользователей. Содержимое одного устройства полностью переносится на другое устройство.

Временная замена

Новое устройство выдается на определенный срок. Например, сотрудник забыл свою смарт-карту дома. Для работы в офисе оператор выпускает ему новое устройство с ограниченным сроком действия.

В этом случае действие сертификатов на забытой карте сотрудника приостанавливается. Действительные сертификаты и ключи будут записаны на новое устройство.

В карточке пользователя отображаются два устройства:

- Основное устройство Rutoken S выключено. Действие всех сертификатов на устройстве приостановлено.
- Устройство-дубликат Rutoken ECP выпущено с ограниченным сроком действия.



Белов Евгений Александрович

Логин	DEMO\Evgeniy.Belov
Путь	demo.local/Indeed CM RU/Белов Евгений Александрович
Политика	Базовая политика
E-mail	evgeniy.belov@demo.com
Телефон	+7 (905) 288-58-23

[Загрузить фотографию](#) [Пользователь КристоПро 2.0](#) [Сбросить ответы на секретные вопросы](#)
[Сбросить пароль пользователя](#)

Назначенные устройства

>	Rutoken ECP, 0756770190	Евгений Белов	01.04.2017 0:00	Выпущено
>	Rutoken S, 0755398982	Евгений Белов		Выключено

[+ Выпустить устройство](#) [+ Назначить устройство](#)

Постоянная замена

Заменяемое устройство отзывается, вместо него выпускается новое. На новое устройство записываются все данные заменяемого устройства (ключевые пары, сертификаты).

Сертификаты на заменяемом устройстве отзываются без возможности восстановления.



ПРЕДУПРЕЖДЕНИЕ

При замене устройства PIN-код устройства не переносится на новое устройство. На устройство-дубликат PIN-код установится в соответствии с настройками политики использования устройств:

- Установленный производителем по умолчанию
- Заданный администратором в параметрах инициализации устройства
- Случайный

Пользователь может изменить PIN-код устройства в Сервисе самообслуживания, если администратор настроил разрешение в разделе **Поведение** 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. Выберите нужное устройство и раскройте карточку устройства.
4. Нажмите **Заменить**.
5. Укажите тип замены:
 - **Временная**. Укажите срок окончания действия временного устройства.
 - **Постоянная**. Укажите причину.
6. Задайте имя устройства. Имя подставится автоматически, если администратор настроил разрешение в разделе **Поведение** политики использования устройств.
7. Подключите новое устройство к компьютеру.
8. Укажите PIN-код администратора в разделе **Дополнительно**, если новое устройство не добавлено в Indeed CM. Нажмите **Заменить** или **Отмена**.



ПРЕДУПРЕЖДЕНИЕ

Если в политике использования устройств настроена инициализация устройства при замене, то новое устройство будет инициализировано. Все данные, хранящиеся на устройстве будут удалены.

Если Indeed CM интегрирован с **Indeed AirCard Enterprise**, то аппаратное устройство можно заменить на сетевую смарт-карту AirCard. Для замены устройства на AirCard нажмите **Заменить на AirCard** в карточке устройства.

▼  **Rutoken ECP, 1079203323**  Белов Выпущено

Сбросить PIN-код Разблокировать Выключить Отозвать Заменить

Заменить на AirCard

Обновить Заблокировать Сменить PIN-код администратора

☐ Временная
☒ Постоянная

Причина отзыва

Устройство утеря ▼

Имя устройства

Белов

Заменить Отмена

Обновление

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.

Процедура обновления

Для обновления устройства выполните следующие действия:

1. Перейдите в раздел **Пользователи** и выполните поиск пользователя.
2. Нажмите на логин и перейдите в карточку пользователя.
3. Выберите нужное устройство и нажмите **Обновить**.



ПОДСКАЗКА

Если у вас нет доступа к устройству пользователя, задайте опцию **Обновить устройство на агенте**. Клиентский агент, установленный на рабочей станции пользователя, выполнит задачу по обновлению.

[Как создать задачу по обновлению на агенте Indeed CM](#)

4. Подключите устройство к компьютеру.
5. Выберите шаблоны, по которым будут сформированы сертификаты для записи на устройство. Обязательные сертификаты запишутся на устройство автоматически.
6. Если в политике использования устройств настроена **Интеграция со СМЭВ** и сертификат выпускается по шаблону для КриптоПро УЦ 2.0 или Валидата УЦ, отобразится **форма проверки СМЭВ**.
Проверьте данные пользователя.
7. Введите **PIN-код пользователя**.
8. Если на устройство были добавлены сторонние сертификаты, Indeed CM может их обнаружить и внести информацию о таких сертификатах в систему – отследить.
Окно выбора сертификатов для отслеживания отображается, если в разделе **Поведение** политики использования устройств задана опция **Включить отслеживание сертификатов**.
Выберите сертификаты для отслеживания, если они есть на устройстве, и нажмите **Ок**.
9. Нажмите **Обновить**.
10. По завершении обновления устройства нажмите **Заккрыть**.

Контроль обновления

Обновление устройства можно приостановить, если регламент вашей организации предусматривает проверку запроса на обновление сертификата в УЦ.

Чтобы настроить проверку запроса на обновление сертификата в УЦ:

1. Откройте раздел **Конфигурация** и перейдите в настройки политики.
2. Откройте раздел **Удостоверяющие центры** → **Шаблоны** используемых УЦ.

3. Отключите опцию **Автоматически одобрять подписанный запрос на обновление сертификата**.

В окне обновления устройства появится сообщение *Обновление устройства ожидает решения*. Устройству присваивается статус **В ожидании**. Это означает, что запрос на обновление перешел в стадию рассмотрения.

Если запрос на обновление сертификата одобрен в УЦ, то сертификат получает статус **Одобен** и записывается на устройство. Нажмите **Продолжить обновление устройства** в карточке устройства.

Если запрос отклонен в УЦ:

- **Отзовите и очистите устройство**, после чего **выпустите устройство заново**.
- **Отмените обновление устройства** и **обновите устройство заново**.

Если в политике **настроена** автоматическая рассылка уведомлений по электронной почте, то вам придет уведомление о статусе одобрения – *Одобрение обновления устройства* или *Отклонение обновления устройства*. Если автоматическая рассылка уведомлений не настроена, дождитесь появления кнопки **Продолжить обновление устройства** в карточке устройства.



ПРЕДУПРЕЖДЕНИЕ

Настройки УЦ могут ограничивать автоматическое обновление сертификатов – обновлять только действующие сертификаты. В этом случае опция **Автоматически одобрять подписанный запрос на обновление сертификата** в Indeed CM не регулирует автоматическое обновление сертификатов.

Отмена обновления

Вы можете отменить обновление устройства на агенте, если в разделе **Поведение** политики использования устройств включена опция **Разрешить отмену обновления устройства**.

Чтобы отменить обновление устройства:

1. Нажмите **Отменить обновление** в карточке устройства.
2. Введите **PIN-код пользователя**.
3. Подключите устройство и нажмите **Отменить обновление**.



ПОДСКАЗКА

Если у вас нет доступа к устройству, задайте опцию **Отменить обновление на агенте**. Клиентский агент, установленный на рабочей станции пользователя, отменит задачу по обновлению.

Выпуск 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, включите опцию **Разрешить пользователю просмотр СКЗИ** в разделе **Поведение** политики использования устройств.

Добавление

СКЗИ можно назначить автоматически при его добавлении в карточке пользователя Indeed CM.

Чтобы создать новое СКЗИ и закрепить его за пользователем, нажмите **Добавить СКЗИ**, 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	<i>В процессе</i>
Завершение обучения	- Пользователь проходит обучение и завершает его самостоятельно - Администратор завершает обучение пользователя	<i>Ожидание одобрения</i>
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.	<i>Завершено</i>

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 имели возможность отменить обучение самостоятельно, перейдите в настройки политики в раздел **Поведение** и включите опцию **Разрешить пользователю отмену обучения СКЗИ**.

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 СМ ЭДО позволяет пользователям, администраторам и операторам обмениваться документами для получения сертификата ключа проверки электронной подписи (далее – сертификат подписи) и нормативными документами СКЗИ.

Администраторы могут управлять документами пользователя в его карточке и в репозитории документов в разделе **Документы**.

Пользователи могут добавлять, подписывать электронной подписью, скачивать, редактировать и удалять документы в Сервисе самообслуживания в разделе **Ваши документы**.



ПРИМЕЧАНИЕ

Чтобы разрешить пользователю удалять документы в Сервисе самообслуживания, включите опцию **Разрешить пользователю удаление документа** в разделе **Поведение** политики использования устройств.

Предварительные настройки

Чтобы настроить управление документами:

1. Откройте **Мастер настройки**, перейдите в раздел **Общие функции** и включите опцию **Внутренний документооборот**.
2. Откройте Консоль управления, перейдите в раздел **Конфигурация** → **Роли** и предоставьте членам роли привилегии для управления документами.

▼ Список привилегий

- Просмотр репозитория документов
- Добавление документа
- Изменение документа
- Удаление документа
- Одобрение документа

Чтобы управлять нормативными документами СКЗИ, убедитесь, что в Мастере настройки Indeed CM в разделе **Функции системы** → **Журнал учета СКЗИ** включена опция **Вести журнал учета СКЗИ**.

[Подробнее об настройке учета СКЗИ](#)

Требования для подписи документов

Документ можно подписать его электронной подписью, если:

- Есть устройство, которое содержит сертификат подписи.
- Сертификат подписи имеет любой статус, кроме *Отозван*, *Истек*, *Ключ истек* и *Ошибка*.
- Поле Улучшенный ключ сертификата содержит значения «Защита электронной почты» (Secure Email, OID 1.3.6.1.5.5.7.3.4) и «Подписание кода» (codeSigning, OID 1.3.6.1.5.5.7.3.3) согласно требованиям к электронной подписи ([RFC 5280](#)).

[Как пользователи загружают и подписывают документы в Indeed CM](#)

Проверка документов

Администраторы могут проверять документы пользователей, чтобы избежать ошибок в работе со следующими документами:

- Документы для получения сертификата подписи
- Нормативные документы СКЗИ

Пользователи [загружают и подписывают документы](#) в Сервисе самообслуживания. Документы становятся доступны в карточке пользователя, где администраторы проверяют документы – одобряют или отклоняют их.

Если в политике использования устройств настроена [автоматическая рассылка уведомлений](#) по электронной почте, администраторы получают уведомление, когда пользователи загружают документы. К уведомлению прикреплен документ в формате PDF.

Документы для получения сертификата подписи

Вы можете дополнительно приостановить выпуск и обновление устройства пользователя. В этом случае документы проверяет не только удостоверяющий центр (УЦ), но и администратор или оператор Indeed CM.

Пользователь может продолжить выпуск или обновление устройства только после того, как предоставит на проверку администратору пакет необходимых документов – запрос на сертификат, форму сертификата или оба документа.

Устройство переходит в состояние *В ожидании*. Это означает, что запрос пользователя на выпуск или обновление устройства перешел в стадию рассмотрения.

▼ Предварительные настройки шаблонов сертификатов

Запрос на сертификат

Вы можете проверить запрос на сертификат перед отправкой в УЦ, чтобы убедиться, что пользователь сформировал корректный запрос.

Чтобы настроить дополнительную проверку запроса на сертификат:

1. Откройте раздел **Конфигурация** и перейдите в настройки политики.
2. Откройте раздел **Удостоверяющие центры** → **Шаблоны** используемых УЦ.
3. Отключите опцию:
 - **Автоматически одобрять запрос на сертификат**, если пользователь выпускает устройство в первый раз.
 - **Автоматически одобрять подписанный запрос на обновление сертификата**, если пользователь обновляет устройство.

Сертификат

После одобрения запроса в УЦ форма сертификата будет доступна пользователю в Сервисе самообслуживания. Пользователь может скачать и подписать форму сертификата и предоставить ее на проверку администратору/оператору.

Таким образом вы можете убедиться, что пользователь ознакомился с содержимым сертификата до записи сертификата на устройство.

Чтобы настроить дополнительную проверку формы сертификата:

1. Откройте раздел **Конфигурация** и перейдите в настройки политики.
2. Откройте раздел **Удостоверяющие центры** → **Шаблоны** используемых УЦ.
3. Включите опцию **Требовать подписанный документ сертификата перед продолжением выпуска/обновления устройства**.

Запрос на сертификат и сертификат

Чтобы настроить дополнительную проверку запроса на сертификат и формы сертификата:

1. Откройте раздел **Конфигурация** и перейдите в настройки политики.
2. Откройте раздел **Удостоверяющие центры** → **Шаблоны** используемых УЦ.

3. Отключите опцию:

- **Автоматически одобрять запрос на сертификат**, если пользователь выпускает устройство в первый раз.
- **Автоматически одобрять подписанный запрос на обновление сертификата**, если пользователь обновляет устройство.

4. Включите опцию **Требовать подписанный документ сертификата перед продолжением выпуска/обновления устройства**.

Процесс проверки

Чтобы проверить документ:

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 документа необходимо установить связь между загруженным документом, шаблоном сертификата и устройством:

1. В раскрывающемся списке **Сертификат** выберите шаблон, по которому выпускается сертификат.
2. В раскрывающемся списке **Устройство** выберите устройство, на которое записывается сертификат.
3. Нажмите **Одобрить**.

Если пользователь сформировал документ по шаблону на вкладке **Содержимое устройства**, то связь между документом, шаблоном сертификата и устройством устанавливается автоматически. В этом случае вам не нужно одобрять документ.



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.

Нормативные документы СКЗИ

При работе с нормативными документами СКЗИ, вы можете:

- Проверить нормативные документы СКЗИ, которые пользователи добавляют в Сервисе самообслуживания.
- Подписать нормативные документы СКЗИ самостоятельно в карточке пользователя или в разделе **СКЗИ** Консоли управления.

Проверка нормативных документов пользователей

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 документа выберите экземпляр СКЗИ, к которому относится документ.
6. Нажмите **Одобрить**.

Если пользователь сформировал документ по шаблону в разделе **Ваши СКЗИ**, то связь между документом и экземпляром СКЗИ устанавливается автоматически. В этом случае вам не нужно одобрять документ.

Подпись нормативных документов

Вы можете подписать нормативные документы СКЗИ в карточке пользователя или в разделе **СКЗИ**. Убедитесь, что выполнены все **требования для подписи документов**.

Чтобы подписать документ:

1. Найдите экземпляр СКЗИ, для которого формируется документ:
 - Перейдите в карточку пользователя в раздел **Назначенные СКЗИ**.
 - Перейдите в раздел **СКЗИ** и выполните поиск СКЗИ.
2. Нажмите  напротив экземпляра СКЗИ, для которого формируется документ.
3. 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**.

4. Нажмите **Распечатать документ**. Откроется файл документа.



ПРЕДУПРЕЖДЕНИЕ

Если экземпляр СКЗИ, для которого формируется документ, не назначен на пользователя, то документ нельзя подписать.

5. Нажмите **Подписать документ**. Если вам необходимо скачать и распечатать документ без подписи, нажмите **Сохранить документ**.
6. Подключите устройство с сертификатом подписи к рабочей станции и выберите его в выпадающем списке **Устройство**.
7. В окне подписи в выпадающем списке **Сертификат** выберите подходящий сертификат подписи.
8. Введите PIN-код пользователя.
9. Нажмите **Подписать**.

Подписанные документы автоматически появляются в списке **Документы** в карточке пользователя. В описании указан серийный номер устройства и название шаблона, по которому документ сформирован и подписан.

Получение оригинала документа

Если пользователь предоставил оригинал документа, вы можете зафиксировать получение оригинала в Indeed CM:

- При добавлении нового документа. Нажмите **Добавить документ**, выберите тип документа, загрузите файл, укажите описание и включите опцию **Оригинал получен**.
- При редактировании добавленного документа. Нажмите  напротив нужного документа и включите опцию **Оригинал получен**.

Устройства

В разделе **Устройства** можно выполнить следующие операции:

- Поиск
- Добавление
- Выпуск
- Удаление
- Инициализация пустых устройств
- Изменение тегов
- Пакетное добавление

Поиск

Если устройство физически доступно, 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

Устройство можно найти по фильтрам – серийный номер, тип, комментарий, состояние, статус содержимого, имя пользователя, политика, теги.

Чтобы увидеть список всех устройств, введите символ  в поле **Серийный номер** и нажмите . Чтобы найти устройство по части серийного номера, введите символ  и часть серийного номера.



ПРИМЕЧАНИЕ

Чтобы отфильтровать устройств по статусу содержимого, убедитесь, что в Мастере настройки указано расписание запуска службы Card Monitor.

Результаты поиска устройств можно сохранить в файл. Нажмите  и выберите формат PDF или CSV.

Чтобы просмотреть содержимое устройства, нажмите  .

Чтобы просмотреть PIN-код администратора, нажмите  . Администраторы имеют доступ к PIN-кодам всех устройств, добавленных в Indeed CM. Администраторы отдельных политик имеют доступ к PIN-кодам устройств, назначенных/выпущенных пользователям, на которых действуют эти политики.

Добавление

1. Подключите устройство к компьютеру 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. 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**.
4. Нажмите **Добавить** и **Заккрыть**.

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 **Типы устройств**, при добавлении устройства PIN-код администратора автоматически меняется на случайное или неслучайное значение.

Если после добавления устройства значение PIN-кода администратора поменялось на случайное, то вы можете разблокировать PIN-код пользователя и инициализировать отдельные виды устройств только с помощью Indeed CM.

Выпуск

Выпуск устройств и виртуальных карт AirCard в разделе **Устройства** аналогичен выпуску из **карточки пользователя**.

Удаление

Удалить устройство из Indeed CM можно как при наличии устройства, так и без него.



ПРЕДУПРЕЖДЕНИЕ

Если после добавления устройства значение PIN-кода администратора поменялось на случайное, то при удалении недоступного устройства PIN-код администратора останется случайным и неизвестным.

Для удаления устройства найдите его и нажмите . В зависимости от того, есть ли у вас доступ к устройству, выберите опцию:

- Устройство доступно
- Устройство недоступно (потеряно или повреждено)

Если устройство поддерживает аппаратную криптографию и в Indeed CM ведется учет СКЗИ, то отобразится поле **Номер и дата документа**, в соответствии с которым уничтожается СКЗИ по данному устройству.

При удалении доступного устройства его можно инициализировать. Чтобы инициализировать устройство, включите опцию **Инициализировать устройство**. Все данные, которые хранятся на устройстве, удаляются.

Если устройство доступно, подключите устройство к компьютеру и нажмите **Удалить**. Если устройство недоступно, нажмите **Удалить**.

Вы можете изъять устройство у пользователя, если оно было выпущено ранее и затем отозвано, без удаления из Indeed CM. Действие применимо как для доступного, так и для недоступного устройства.

Инициализация пустых устройств

Indeed CM позволяет инициализировать устройства, которые были добавлены в Indeed CM и находятся в состоянии *Пустое*, т.е. не закреплены за пользователем. Устройство можно инициализировать в Консоли управления и с помощью клиентского агента.



ПРИМЕЧАНИЕ

Операция **Инициализировать** доступна, если задана соответствующая привилегия в разделе **Роли**.

1. Выберите устройство и нажмите  для просмотра его содержимого.

2. Подключите устройство к рабочей станции и нажмите **Инициализировать**. Если устройство недоступно, создайте задачу на клиентском агенте – выберите опцию **Инициализировать устройство на агенте**.

- Если PIN-код администратора на устройстве совпадает с сохраненным в хранилище Indeed CM, нажмите **Инициализировать**. После инициализации PIN-код администратора на устройстве и в базе не меняется. PIN-код пользователя сбрасывается на значение, указанное в разделе **Типы устройств**.
- Если PIN-код администратора на устройстве не совпадает с сохраненным в хранилище Indeed CM, то укажите его в разделе **Дополнительно**. Задайте **Новый PIN-код пользователя**, если требуется установить его в процессе выполнения инициализации, и нажмите **Инициализировать**. После инициализации PIN-код администратора в хранилище Indeed CM меняется на указанное значение.

ПРИМЕЧАНИЕ

Устройства Rutoken и eToken можно инициализировать с PIN-кодом администратора в состоянии: известный, неизвестный, заблокированный.

Если PIN-код администратора не указан, то после инициализации на устройство записывается PIN-код, сохраненный в базе Indeed CM. Если PIN-код администратора указан, то после инициализации он записывается на устройство и в базу Indeed CM.

Изменение тегов

Изменение тегов доступно для нескольких устройств сразу. Теги создает администратор в разделе **Конфигурация** → **Теги**.

Чтобы добавить или удалить теги, перейдите в раздел **Устройства** на вкладку **Расширенный**, выберите устройства и нажмите **Изменить теги**. Укажите **Теги для добавления** или **Теги для удаления** и нажмите **Изменить**.

Пакетное добавление

Чтобы добавить несколько устройств одновременно:

1. Нажмите **Импортировать устройства**.
2. Загрузите подготовленный **Файл устройств**.

3. Нажмите **Импортировать**.

Поддерживается импорт устройств из файла в формате TXT (UTF-8) и CSV. Файл должен содержать строки с набором полей следующего формата:

```
Serial Number;Card Type;Model;Form Factor;Admin PIN;Gost Admin  
PIN;Comment;Tags;SKZI Document Number;Time Created
```

Где:

- **Serial Number** – серийный номер устройства. Обязательный параметр.
- **Card Type** – тип устройства. Обязательный параметр. Укажите имя типа устройства в том виде, в котором он указан в разделе **Типы устройств**.
- **Model** – модель устройства доступна только для устройств Рутокен, JaCarta, eToken PRO Java 72K и IDPrime MD, если в разделе **Типы устройств** для данных карт заданы отдельные настройки для различных моделей.
- **Form Factor** – форм-фактор устройства. Поддерживаются: SmartCard (по умолчанию), UsbToken, MicroSD. Если форм-фактор не указан, то устройство будет добавлено как смарт-карта.
- **Admin PIN** – значение PIN-кода администратора, которое будет присвоено всем перечисленным в файле импорта устройствам.
- **Gost Admin PIN** – значение PIN-кода администратора ГОСТ областей для устройств JaCarta/JaCarta-2, которое будет присвоено всем устройствам, перечисленным в файле импорта.
- **Comment** – комментарий к устройствам.
- **Tags** – теги к устройствам. Указываемые теги необходимо предварительно создать в разделе **Теги**. Если требуется добавить несколько тегов для импортируемых устройств, то в файле импорта укажите их через запятую: Tag1,Tag2.
- **SKZI Document Number** – если импортируемые устройства поддерживают аппаратную криптографию и в системе ведется учет СКЗИ, то укажите **Номер документа** (приказа, распоряжения), в соответствии с которым произведена постановка на учет СКЗИ (Тип: Ключевой носитель). Информация об имеющихся в системе средствах криптографической защиты информации находится в разделе **СКЗИ**.
- **Time Created** – время создания документа. Указывается в формате ууууMMddHHmmss (UTC). Если значение не указано, то в качестве времени создания документа автоматически подставляется время импорта СКЗИ.

ⓘ **ПРИМЕЧАНИЕ**

Если вместо поля **Serial Number** (Серийный номер) устройства прописано значение **default**, то значения оставшихся полей в строке используются как значения по умолчанию для соответствующих полей последующих строк, т.е. для последующих строк необходимо указать только серийный номер и поле, которое отличается от указанного в строке **default**.

▼ Пример файла устройств

```
default;Rutoken S;;UsbToken;87654321;;Московский офис;VPN,IT;;
0755398982
0756309531
default;Rutoken
ECP;;UsbToken;87654321;;Бухгалтерия;VPN;BH-169;20220412134200
0894130607
0894130536
default;Rutoken ECP SC;;;87654321;;;BH-170;20220329111500
0862287268
0862287403
default;Rutoken 2151;;UsbToken;87654321;;;BH-171;
0963474291
default;ESMART Token 64K;;UsbToken;12345678;;;
609BC06881C7
B0B340508942
E0D8806291CB;;;SmartCard;;;
D050806291CB;;;SmartCard;;;
default;eToken PRO Java 72K;eToken PRO Java 72K
0S755;SmartCard;1234567890;;;
01cec45d
default;JaCarta;JC210;UsbToken;00000000;;;
0B53002004417597
0B53001122617597
default;JaCarta;JC300;SmartCard;00000000;;;
0153001910367618
default;JaCarta;JC267-
1236J.J01Q01;UsbToken;00000000;1234567890;;;BH-172;
6082057494937678
4C54001522634C50
0B53001917347618;;JC305;SmartCard;;;BH-173;20220412145500
```

В файл добавлены:

- USB-токены Rutoken S с серийными номерами: 0755398982, 0756309531, с указанным комментарием: Московский офис и тегами: VPN, IT
- USB-токены Rutoken ECP с серийными номерами: 0894130607, 0894130536, с указанным комментарием: Бухгалтерия, тегом: VPN и номером документа СКЗИ: ВН-169 от 04.12.2022 в 16:42:00 по московскому времени (GMT+3)
- Смарт-карты Rutoken ECP с серийными номерами: 0862287268, 0862287403, с указанным номером документа СКЗИ: ВН-170 от 29.03.2022 в 14:15:00 по московскому времени (GMT+3)
- USB-токен Rutoken 2151 с серийным номером: 0963474291, с указанным номером документа СКЗИ: ВН-171 от текущего числа и времени
- USB-токены ESMART Token 64K с серийными номерами: 609BC06881C7, B0B340508942
- Смарт-карты ESMART Token 64K с серийными номерами: E0D8806291CB, D050806291CB
- Смарт-карта eToken PRO Java 72K модели eToken PRO Java 72K OS755 с серийным номером: 01cec45d
- USB-токены JaCarta PKI/Flash (без ГОСТ области) модели JC210 с серийными номерами: 0B53002004417597, 0B53001122617597
- Смарт-карта JaCarta PKI (без ГОСТ области) модели JC300 с серийным номером: 0153001910367618
- USB-токены JaCarta-2 SE/PKI/ГОСТ модели JC267-1236J.J01Q01 с серийными номерами: 6082057494937678, 4C54001522634C50 и с указанным номером документа СКЗИ: ВН-172 от текущего числа и времени
- Смарт-карта JaCarta PKI/ГОСТ модели JC305 с серийным номером: 0B53001917347618 и с указанным номером документа СКЗИ: ВН-173 от 12.04.2022 в 17:55:00 по московскому времени (GMT+3)

Изменение иконок устройства

В Indeed CM существует набор изображений, который отображает форм-фактор устройства: USB-токен или смарт-карта.

Серийный номер	Тип	Состояние	
 003bc82b	eToken PRO Java 72K (JC1.0b)	Пустое	
 0641367757	Rutoken S	Пустое	

Для изменения иконок:

1. Подготовьте изображение в формате PNG с максимальным размером **20x20 px**.
2. Для формирования имени файла воспользуйтесь следующим шаблоном **<Название типа устройства>_<Название модели>**, где:
 - **Название типа устройства** – имя, указанное в конфигурационном JSON-файле устройства. Название типа находится в секции **<name>...</name>**
 - **Название модели** – если в конфигурационном файле JSON есть данные о нескольких устройствах, то необходимо указать точное название модели. Название модели находится в секции **<models>...</models>>**

ПРИМЕЧАНИЕ

В названии файла запрещены символы: /, \, :, *, ?, ", <, >, |. Если они встречаются в названии типа устройства или модели, то их необходимо удалить. Все пробелы необходимо заменить символом подчеркивания "_".

Пример:

- Rutoken_S.png – изменение иконки для устройств **Rutoken S**
- eToken_PRO_Java_72K_eToken_PRO_Java_72K_OS755.png – изменение иконки для устройств типа **eToken PRO Java 72K**, модели **eToken PRO Java 72K OS755**.

3. Скопируйте изображение в папки:
 - *C:\inetpub\wwwroot\mc\Content\images*
 - *C:\inetpub\wwwroot\mcremote\Content\images*
 - *C:\inetpub\wwwroot\mcservice\Content\images*
4. Проверьте изображение. Откройте Консоль управления и перейдите в раздел **Устройства**.

Сертификаты

В разделе **Сертификаты** можно найти все сертификаты, которые содержатся на устройствах, добавленных в Indeed CM.

Предварительные настройки

Чтобы разрешить доступ к репозиторию сертификатов:

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.
Одобен	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. Для этого 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:
10	Информация	Замена устройства	Устройство успешно заменено. Пользователь: Устройство: Новое Устройство: Сертификаты: Общие сертификаты: Дата истечения: Инициатор:

Код	Тип	Событие	Описание
1010	Ошибка	Замена устройства	Произошла ошибка при замене устройства. Пользователь: Устройство: Новое устройство: Инициатор: Сообщение об ошибке:
11	Информация	Очистка устройства	Устройство успешно очищено. Пользователь: Устройство: Состояние устройства: Инициатор:
1011	Ошибка	Очистка устройства	Произошла ошибка при очистке устройства. Пользователь: Устройство: Инициатор: Сообщение об ошибке:
12	Информация	Сброс PIN-кода	PIN-код устройства успешно сброшен. Пользователь: Устройство: Инициатор:
1012	Ошибка	Сброс PIN-кода	Произошла ошибка при сбросе PIN-кода устройства. Пользователь: Устройство: Инициатор: Сообщение об ошибке:

Код	Тип	Событие	Описание
13	Информация	Разблокировка устройства	Код разблокировки успешно сгенерирован. Пользователь: Устройство: Инициатор:
1013	Ошибка	Разблокировка устройства	Произошла ошибка при генерации кода разблокировки. Пользователь: Устройство: Инициатор: Сообщение об ошибке:
14	Информация	Изменение PIN-кода	PIN-код устройства успешно изменен. Пользователь: Устройство: Инициатор:
1014	Ошибка	Изменение PIN-кода	Произошла ошибка при изменении PIN-кода устройства. Пользователь: Устройство: Инициатор: Сообщение об ошибке:
15	Информация	Выпуск устройства ожидает решения	Выпуск устройства ожидает решения. Пользователь: Политика: Устройство: Сертификаты: Общие сертификаты: Отслеживаемые сертификаты: Инициатор:

Код	Тип	Событие	Описание
16	Информация	Обновление устройства ожидает решения	Выпуск устройства ожидает решения. Пользователь: Устройство: Новые сертификаты: Обновленные сертификаты: Удаленные сертификаты: Новые общие сертификаты: Удаленные общие сертификаты: Отслеживаемые сертификаты: Новая политика: Инициатор:
17	Информация	Замена устройства ожидает решения	Замена устройства ожидает решения. Пользователь: Устройство: Новое устройство: Сертификаты: Общие сертификаты: Дата истечения: Инициатор:
18	Информация	Отмена обновления устройства	Обновление устройства успешно отменено. Пользователь: Устройство: Инициатор:
1018	Ошибка	Отмена обновления устройства	Произошла ошибка при отмене обновления устройства. Пользователь: Устройство: Инициатор: Сообщение об ошибке:

Код	Тип	Событие	Описание
19	Информация	Предварительное обновление устройства	Предварительное обновление устройства успешно выполнено. Пользователь: Устройство: Отозванные сертификаты: Инициатор:
1019	Ошибка	Предварительное обновление устройства	Произошла ошибка при предварительном обновлении устройства. Пользователь: Устройство: Инициатор: Сообщение об ошибке:
20	Информация	Импортирование устройства	Устройство успешно импортировано. Пользователь: Устройство: Состояние: Сертификаты: Инициатор:
1020	Ошибка	Импортирование устройства	Устройство успешно импортировано. Пользователь: Устройство: Состояние: Сертификаты: Инициатор:
21	Информация	Изменение комментария	Комментарий устройства успешно изменен. Устройство: Комментарий: Инициатор:

Код	Тип	Событие	Описание
1021	Ошибка	Изменение комментария	Произошла ошибка при изменении комментария устройства. Устройство: Инициатор: Сообщение об ошибке:
22	Информация	Просмотр PIN-кода администратора	PIN-код администратора устройства просмотрен. Устройство: Инициатор:
23	Информация	Смена PIN-кода администратора	PIN-код администратора устройства успешно изменен Пользователь: Устройство: Инициатор:
1023	Ошибка	Смена PIN-кода администратора	Произошла ошибка при изменении PIN-кода устройства. Пользователь: Устройство: Инициатор: Сообщение об ошибке:
24	Информация	Изменение тега	Теги устройства успешно изменены. Устройство: Новые теги: Удаленные теги: Инициатор:

Код	Тип	Событие	Описание
1024	Ошибка	Изменение тега	Произошла ошибка при изменении тегов устройства. Устройство: Новые теги: Удаленные теги: Инициатор: Сообщение об ошибке:
25	Информация	Инициализация устройства	Устройство успешно инициализировано. Устройство: Инициатор:
1025	Ошибка	Инициализация устройства	Произошла ошибка при инициализации устройства. Устройство: Инициатор: Сообщение об ошибке:
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:

Код	Тип	Событие	Описание
1101	Ошибка	Изменение ответов на секретные вопросы	Произошла ошибка при изменении ответов на секретные вопросы. Пользователь: Инициатор: Сообщение об ошибке:
102	Информация	Аутентификация	Пользователь успешно аутентифицирован. Пользователь: Инициатор:
1102	Ошибка	Аутентификация	Произошла ошибка при аутентификации пользователя. Пользователь: Инициатор: Сообщение об ошибке:
2103	Предупреждение	Блокировка пользователя	Пользователь заблокирован. Пользователь: Инициатор:
104	Информация	Разблокировка пользователя	Пользователь успешно разблокирован. Пользователь: Инициатор:
1104	Ошибка	Разблокировка пользователя	Произошла ошибка при разблокировке пользователя. Пользователь: Инициатор: Сообщение об ошибке:

Код	Тип	Событие	Описание
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:
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:

Код	Тип	Событие	Описание
1112	Ошибка	Результат проверки в СМЭВ	Проверка данных пользователя в СМЭВ завершилась ошибкой. Пользователь: Инициатор: Сообщение об ошибке:
113	Информация	Публикация сертификата в ЕСИА	Данные сертификата опубликованы в СМЭВ для регистрации в ЕСИА. Пользователь: Сертификат: Инициатор:
1113	Ошибка	Публикация сертификата в ЕСИА	Произошла ошибка при публикации сертификата в СМЭВ для регистрации в ЕСИА. Пользователь: Сертификат: Инициатор: Сообщение об ошибке:
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:

Код	Тип	Событие	Описание
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:
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:

Код	Тип	Событие	Описание
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:
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:

Код	Тип	Событие	Описание
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:
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:

Код	Тип	Событие	Описание
201	Информация	Создание политики	Политика успешно создана. Имя политики: Контейнер: Группа: Приоритет: Скопирована с: Инициатор:
1201	Ошибка	Создание политики	Произошла ошибка при создании политики. Имя политики: Контейнер: Группа: Приоритет: Инициатор: Сообщение об ошибке:
202	Информация	Удаление политики	Политика успешно удалена. Имя политики: Инициатор:
1202	Ошибка	Удаление политики	Произошла ошибка при удалении политики. Имя политики: Инициатор: Сообщение об ошибке:
203	Информация	Изменение политики	Политика успешно изменена. Имя политики: Инициатор:

Код	Тип	Событие	Описание
1203	Ошибка	Изменение политики	Произошла ошибка при изменении политики. Имя политики: Инициатор: Сообщение об ошибке:
204	Информация	Добавление лицензии	Лицензия успешно добавлена. Тип: Действительна с: Действительна по: Количество: Инициатор:
1204	Ошибка	Добавление лицензии	Произошла ошибка при добавлении лицензии. Инициатор: Сообщение об ошибке:
205	Информация	Удаление лицензии	Лицензия успешно удалена. Тип: Действительна с: Действительна по: Количество: Инициатор:
1205	Ошибка	Удаление лицензии	Произошла ошибка при удалении лицензии. Инициатор: Сообщение об ошибке:
206	Информация	Добавление типа устройства	Тип устройства успешно добавлен. Имя: Инициатор:

Код	Тип	Событие	Описание
1206	Ошибка	Добавление типа устройства	Произошла ошибка при добавлении типа устройства. Имя: Инициатор: Сообщение об ошибке:
207	Информация	Удаление типа устройства	Тип устройства успешно удален. Имя: Инициатор:
1207	Ошибка	Удаление типа устройства	Произошла ошибка при удалении типа устройства. Имя: Инициатор: Сообщение об ошибке:
208	Информация	Изменение типа устройства	Тип устройства успешно изменен. Имя: Инициатор:
1208	Ошибка	Изменение типа устройства	Произошла ошибка при изменении типа устройства. Имя: Инициатор: Сообщение об ошибке:
209	Информация	Добавление узла организационной структуры	Узел организационной структуры успешно добавлен. Путь: Инициатор:

Код	Тип	Событие	Описание
1209	Ошибка	Добавление узла организационной структуры	Произошла ошибка при добавлении узла организационной структуры. Путь: Инициатор: Сообщение об ошибке:
210	Информация	Удаление узла организационной структуры	Узел организационной структуры успешно удален. Путь: Инициатор:
1210	Ошибка	Удаление узла организационной структуры	Произошла ошибка при удалении узла организационной структуры. Путь: Инициатор: Сообщение об ошибке:
211	Информация	Переименование узла организационной структуры	Узел организационной структуры успешно переименован. Старый путь: Новый путь: Инициатор:
1211	Ошибка	Переименование узла организационной структуры	Произошла ошибка при переименовании узла организационной структуры. Старый путь: Новый путь: Инициатор: Сообщение об ошибке:

Код	Тип	Событие	Описание
212	Информация	Перемещение узла организационной структуры	Узел организационной структуры успешно перемещен. Старый путь: Новый путь: Инициатор:
1212	Ошибка	Перемещение узла организационной структуры	Произошла ошибка при перемещении узла организационной структуры. Старый путь: Новый путь: Инициатор: Сообщение об ошибке:
213	Информация	Добавление связанных объектов каталога	Связанные объекты каталога успешно добавлены. Путь: Пользователи: Группы: Контейнеры: Инициатор:
1213	Ошибка	Добавление связанных объектов каталога	Произошла ошибка при добавлении связанных объектов каталога. Путь: Пользователи: Группы: Контейнеры: Инициатор: Сообщение об ошибке:

Код	Тип	Событие	Описание
214	Информация	Удаление связанных объектов каталога	Связанные объекты каталога успешно удалены. Путь: Пользователи: Группы: Контейнеры: Инициатор:
1214	Ошибка	Удаление связанных объектов каталога	Произошла ошибка при удалении связанных объектов каталога. Путь: Пользователи: Группы: Контейнеры: Инициатор: Сообщение об ошибке:
215	Информация	Создание роли	Роль успешно создана. Имя: Тип: Пользователи: Группы: Привилегии: Разрешить: Запретить: Инициатор:

Код	Тип	Событие	Описание
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:

Код	Тип	Событие	Описание
1237	Ошибка	Создание группы получателей	Произошла ошибка при создании группы получателей. Имя: Инициатор: Сообщение об ошибке:
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:

Код	Тип	Событие	Описание
1240	Ошибка	Создание уведомления администратора	Произошла ошибка при создании уведомления администратора. Событие: Тип события: Инициатор: Сообщение об ошибке:
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:

Код	Тип	Событие	Описание
243	Информация	Обновление шаблона администратора	Шаблон администратора успешно обновлен. Событие: Тип события: Инициатор:
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:

Код	Тип	Событие	Описание
1331	Ошибка	Добавление документа	Произошла ошибка при добавлении документа. Пользователь: Тип: Имя файла: Описание: Подпись: Оригинал: Инициатор: Сообщение об ошибке:
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:

Код	Тип	Событие	Описание
1333	Ошибка	Удаление документа	Произошла ошибка при удалении документа. Пользователь: Тип: Имя файла: Описание: Инициатор: Сообщение об ошибке:
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:

Код	Тип	Событие	Описание
605	Информация	Удаление агента	Агент успешно удален Имя агента: Инициатор:
1605	Ошибка	Удаление агента	Произошла ошибка при удалении агента. Имя агента: Инициатор: Сообщение об ошибке:
606	Информация	Регистрация агента	Агент успешно зарегистрирован. Имя агента: Инициатор:
1606	Ошибка	Регистрация агента	Произошла ошибка при регистрации агента. Имя агента: Инициатор: Сообщение об ошибке:
607	Информация	Отклонение агента	Агент успешно отклонен. Имя агента: Инициатор:
1607	Ошибка	Отклонение агента	Произошла ошибка при отклонении агента. Имя агента: Инициатор: Сообщение об ошибке:

Код	Тип	Событие	Описание
608	Информация	Добавление задачи	Задача успешно добавлена. Устройство: Тип задачи: Комментарий: Инициатор:
1608	Ошибка	Добавление задачи	Произошла ошибка при добавлении задачи. Устройство: Тип задачи: Комментарий: Инициатор: Сообщение об ошибке:
609	Информация	Удаление задачи	Задача успешно удалена. Устройство: Тип задачи: Комментарий: Инициатор:
1609	Ошибка	Удаление задачи	Произошла ошибка при удалении задачи. Устройство: Тип задачи: Комментарий: Инициатор: Сообщение об ошибке:
610	Информация	Обновление имени агента	Имя агента успешно обновлено. Текущее имя агента: Новое имя агента: Инициатор:

Код	Тип	Событие	Описание
1610	Ошибка	Обновление имени агента	Произошла ошибка при обновлении имени агента. Текущее имя агента: Новое имя агента: Инициатор: Сообщение об ошибке:
611	Информация	Обновление комментария агента	Комментарий агента успешно обновлен. Имя агента: Текущий комментарий агента: Новый комментарий агента: Инициатор:
1611	Ошибка	Обновление комментария агента	Произошла ошибка при обновлении комментария агента. Имя агента: Текущий комментарий агента: Новый комментарий агента: Инициатор: Сообщение об ошибке:

Код	Тип	Событие	Описание
612	Информация	Выполнение задачи	Задача была успешно выполнена. Информация о сессии: Идентификатор сессии: Пользователь: Sid: Тип сессии: Имя агента: Устройство: Тип задачи: Комментарий: Создана пользователем: Инициатор:
1612	Ошибка	Выполнение задачи	Не удалось выполнить задачу. Информация о сессии: Идентификатор сессии: Пользователь: Sid: Тип сессии: Имя агента: Устройство: Тип задачи: Комментарий: Создана пользователем: Описание ошибки при выполнении задачи Инициатор: Сообщение об ошибке:

Код	Тип	Событие	Описание
613	Информация	Отмена задачи пользователем	Задача была отменена пользователем. Информация о сессии: Идентификатор сессии: Пользователь: Sid: Тип сессии: Имя агента: Устройство: Тип задачи: Комментарий: Создана пользователем: Инициатор:
1613	Ошибка	Отмена задачи пользователем	Пользователю не удалось отменить задачу. Информация о сессии: Идентификатор сессии: Пользователь: Sid: Тип сессии: Имя агента: Устройство: Тип задачи: Комментарий: Создана пользователем: Инициатор: Сообщение об ошибке:
614	Информация	Обновление задачи	Задача успешно обновлена. Устройство: Тип задачи: Старый комментарий: Новый комментарий: Инициатор:

Код	Тип	Событие	Описание
1614	Ошибка	Обновление задачи	Произошла ошибка при обновлении задачи. Устройство: Тип задачи: Старый комментарий: Новый комментарий: Инициатор: Сообщение об ошибке:
2615	Предупреждение	Подключение незарегистрированного устройства	Подключение незарегистрированного устройства. Информация о сессии: Идентификатор сессии: Пользователь: Sid: Тип сессии: Информация об устройстве: Серийный номер: Метка: Тип: Модель: Atr: Идентификатор агента: Имя агента: Инициатор:
2616	Предупреждение	Отсутствие связи с агентом	Длительное отсутствие связи с агентом. Идентификатор агента: Имя агента: Инициатор:

Код	Тип	Событие	Описание
700	Информация	Инициализация сессий	Инициализация сессий. Количество сессий: Информация о сессиях: Идентификатор агента: Имя агента: Инициатор:
701	Информация	Пользователь вошел в систему	Пользователь вошел в систему. Идентификатор сессии: Пользователь: Sid: Тип сессии: Идентификатор агента: Имя агента: Инициатор:
702	Информация	Пользователь вышел из системы	Пользователь вышел из системы. Идентификатор сессии: Пользователь: Sid: Тип сессии: Идентификатор агента: Имя агента: Инициатор:
703	Информация	Компьютер заблокирован	Компьютер заблокирован. Идентификатор сессии: Пользователь: Sid: Тип сессии: Идентификатор агента: Имя агента: Инициатор:

Код	Тип	Событие	Описание
704	Информация	Компьютер разблокирован	Компьютер разблокирован. Идентификатор сессии: Пользователь: Sid: Тип сессии: Идентификатор агента: Имя агента: Инициатор:
705	Информация	Пользователь подключился к сеансу	Пользователь подключился к сеансу. Идентификатор сессии: Пользователь: Sid: Тип сессии: Идентификатор агента: Имя агента: Инициатор:
706	Информация	Пользователь отключился от сеанса	Пользователь отключился от сеанса. Идентификатор сессии: Пользователь: Sid: Тип сессии: Идентификатор агента: Имя агента: Инициатор:

Код	Тип	Событие	Описание
707	Информация	Пользователь подключился к терминальному сеансу	Пользователь подключился к терминальному сеансу. Идентификатор сессии: Пользователь: Sid: Тип сессии: Идентификатор агента: Имя агента: Инициатор:
708	Информация	Пользователь отключился от терминального сеанса	Пользователь отключился от терминального сеанса. Идентификатор сессии: Пользователь: Sid: Тип сессии: Идентификатор агента: Имя агента: Инициатор:
709	Информация	Подключение устройства	Подключение устройства. Идентификатор сессии: Пользователь: Sid: Тип сессии: Информация об устройстве: Серийный номер: Метка: Тип: Модель: Atr: Идентификатор агента: Имя агента: Инициатор:

Код	Тип	Событие	Описание
710	Информация	Отключение устройства	Отключение устройства. Идентификатор сессии: Пользователь: Sid: Тип сессии: Информация об устройстве: Серийный номер: Метка: Тип: Модель: Atr: Идентификатор агента: Имя агента: Инициатор:
2711	Предупреждение	Нарушение привязки устройства к пользователю	Нарушение привязки устройства к пользователю. Информация о сессии: Идентификатор сессии: Пользователь: Sid: Тип сессии: Настройки привязки: Серийный номер: Atr: Ожидаемый Sid пользователя: Действие: Идентификатор агента: Имя агента: Инициатор:

Код	Тип	Событие	Описание
2712	Предупреждение	Нарушение привязки устройства к агенту	Нарушение привязки устройства к агенту. Информация о сессии: Идентификатор сессии: Пользователь: Sid: Тип сессии: Настройки привязки: Серийный номер: Atr: Ожидаемый идентификатор агента: Действие: Идентификатор агента: Имя агента: Инициатор:
2714	Предупреждение	Блокировка пользовательской сессии	Устройство не удовлетворяет условиям привязки. Блокировка пользовательской сессии. Информация о сессии: Идентификатор сессии: Пользователь: Sid: Тип сессии: Серийный номер: Atr: Идентификатор агента: Имя агента: Инициатор:

Код	Тип	Событие	Описание
2715	Предупреждение	Блокировка устройства	Устройство не удовлетворяет условиям привязки. Блокировка устройства. Информация о сессии: Идентификатор сессии: Пользователь: Sid: Тип сессии: Серийный номер: Atr: Идентификатор агента: Имя агента: Инициатор:
2716	Предупреждение	Блокировка пользовательской сессии и устройства	Устройство не удовлетворяет условиям привязки. Блокировка пользовательской сессии и устройства. Информация о сессии: Идентификатор сессии: Пользователь: Sid: Тип сессии: Серийный номер: Atr: Идентификатор агента: Имя агента: Инициатор:

Код	Тип	Событие	Описание
1720	Ошибка	Обнаружена блокировка PIN-кода администратора на устройстве	Обнаружена блокировка PIN-кода администратора на устройстве. Информация об устройстве: Серийный номер: Метка: Тип: Модель: Atr: Апплет: Информация о сессии: Идентификатор сессии: Пользователь: Sid: Тип сессии: Идентификатор агента: Имя агента: Инициатор:

Код	Тип	Событие	Описание
2721	Предупреждение	Обнаружена блокировка PIN-кода пользователя на устройстве	Обнаружена блокировка PIN-кода пользователя на устройстве. Информация об устройстве: Серийный номер: Метка: Тип: Модель: Atr: Апплет: Информация о сессии: Идентификатор сессии: Пользователь: Sid: Тип сессии: Идентификатор агента: Имя агента: Инициатор:

Код	Тип	Событие	Описание
1722	Ошибка	Ввод неверного PIN-кода администратора на устройстве	Ввод неверного PIN-кода администратора на устройстве. Информация об устройстве: Серийный номер: Метка: Тип: Модель: Atr: Апплет: Информация о сессии: Идентификатор сессии: Пользователь: Sid: Тип сессии: Идентификатор агента: Имя агента: Инициатор:

Код	Тип	Событие	Описание
2723	Предупреждение	Ввод неверного PIN-кода пользователя на устройстве	Ввод неверного PIN-кода пользователя на устройстве. Информация об устройстве: Серийный номер: Метка: Тип: Модель: Atr: Апплет: Информация о сессии: Идентификатор сессии: Пользователь: Sid: Тип сессии: Идентификатор агента: Имя агента: Инициатор:

▼ События журнала учета

Код	Тип	Событие	Описание
230	Информация	Создание справочника журнала учета	Справочник успешно создан. Имя: Инициатор:
1230	Ошибка	Создание справочника журнала учета	Произошла ошибка при создании справочника. Имя: Инициатор: Сообщение об ошибке:
231	Информация	Удаление справочника журнала учета	Справочник успешно удален. Имя: Инициатор:
1231	Ошибка	Удаление справочника журнала учета	Произошла ошибка при удалении справочника. Имя: Инициатор: Сообщение об ошибке:
232	Информация	Изменение справочника журнала учета	Справочник успешно изменен. Имя: Инициатор:
1232	Ошибка	Изменение справочника журнала учета	Произошла ошибка при изменении справочника. Имя: Инициатор: Сообщение об ошибке:

Код	Тип	Событие	Описание
233	Информация	Создание шаблона журнала учета	Шаблон журнала успешно создан. Имя: Тип объектов: Инициатор:
1233	Ошибка	Создание шаблона журнала учета	Произошла ошибка при создании шаблона журнала. Имя: Тип объектов: Инициатор: Сообщение об ошибке:
234	Информация	Удаление шаблона журнала учета	Шаблон журнала успешно удален. Имя: Инициатор:
1234	Ошибка	Удаление шаблона журнала учета	Произошла ошибка при удалении шаблона журнала. Имя: Инициатор: Сообщение об ошибке:
235	Информация	Изменение шаблона журнала учета	Шаблон журнала успешно изменен. Имя: Инициатор:
1235	Ошибка	Изменение шаблона журнала учета	Произошла ошибка при изменении шаблона журнала. Имя: Инициатор: Сообщение об ошибке:

Код	Тип	Событие	Описание
351	Информация	Изменение записи в журнале учета	Запись успешно добавлена. Журнал учета: Поля: Инициатор:
1351	Ошибка	Изменение записи в журнале учета	Произошла ошибка при добавлении записи. Журнал учета: Поля: Инициатор: Сообщение об ошибке:
352	Информация	Изменение записи в журнале учета	Запись успешно изменена. Журнал учета: Поля: Новые поля: Инициатор:
1352	Ошибка	Изменение записи в журнале учета	Произошла ошибка при изменении записи. Журнал учета: Поля: Новые поля: Инициатор: Сообщение об ошибке:
353	Информация	Изменение записи в журнале учета	Запись успешно удалена. Журнал учета: Поля: Инициатор:

Код	Тип	Событие	Описание
1353	Ошибка	Изменение записи в журнале учета	Произошла ошибка при удалении записи. Журнал учета: Поля: Инициатор: Сообщение об ошибке:

▼ События СКЗИ

Код	Тип	Событие	Описание
301	Информация	Добавление СКЗИ	СКЗИ успешно добавлено. Пользователь: Наименование: Серийный номер: Номер экземпляра: Инициатор:
1301	Ошибка	Добавление СКЗИ	Произошла ошибка при добавлении СКЗИ. Пользователь: Наименование: Серийный номер: Номер экземпляра: Инициатор: Сообщение об ошибке:
302	Информация	Обновление СКЗИ	СКЗИ успешно обновлено. Пользователь: Наименование: Серийный номер: Номер экземпляра: Инициатор:
1302	Ошибка	Обновление СКЗИ	Произошла ошибка при обновлении СКЗИ. Пользователь: Наименование: Серийный номер: Номер экземпляра: Инициатор: Сообщение об ошибке:

Код	Тип	Событие	Описание
303	Информация	Уничтожение/изъятие СКЗИ	СКЗИ успешно уничтожено/изъято. Пользователь: Наименование: Серийный номер: Номер экземпляра: Инициатор:
1303	Ошибка	Уничтожение/изъятие СКЗИ	Произошла ошибка при уничтожении/изъятии СКЗИ. Пользователь: Наименование: Серийный номер: Номер экземпляра: Инициатор: Сообщение об ошибке:
304	Информация	Назначение СКЗИ	СКЗИ успешно назначено. Пользователь: Наименование: Серийный номер: Номер экземпляра: Инициатор:
1304	Ошибка	Назначение СКЗИ	Произошла ошибка при назначении СКЗИ. Пользователь: Наименование: Серийный номер: Номер экземпляра: Инициатор: Сообщение об ошибке:

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:

Код	Тип	Событие	Описание
1505	Ошибка	Обновление устройства КриптоПро DSS	Произошла ошибка при обновлении устройства КриптоПро DSS. Пользователь: Инициатор: Сообщение об ошибке:
506	Информация	Удаление устройства КриптоПро DSS	Устройство КриптоПро DSS успешно удалено. Пользователь: Инициатор:
1506	Ошибка	Удаление устройства КриптоПро DSS	Произошла ошибка при удалении устройства КриптоПро DSS. Пользователь: Инициатор: Сообщение об ошибке:
507	Информация	Выпуск устройства КриптоПро DSS ожидает решения	Выпуск устройства КриптоПро DSS ожидает решения. Пользователь: Политика: Сертификаты: Инициатор:
508	Информация	Обновление устройства КриптоПро DSS ожидает решения	Обновление устройства КриптоПро DSS ожидает решения. Пользователь: Новые сертификаты: Обновленные сертификаты: Удаленные сертификаты: Новая политика: Инициатор:

Код	Тип	Событие	Описание
509	Информация	Отмена обновления устройства КристоПро DSS	Обновление устройства КристоПро DSS успешно отменено. Пользователь: Инициатор:
1509	Ошибка	Отмена обновления устройства КристоПро DSS	Произошла ошибка при отмене обновления устройства КристоПро DSS. Пользователь: Инициатор: Сообщение об ошибке:

▼ 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. Возможные значения: *Не задано*, *Ожидает регистрации*, *Зарегистрирован*, *Отклонен*.
- **Имя компьютера** – DNS имя компьютера.
- **Операционная система** – версия операционной системы, на которой установлен агент.
- **IP-адрес** – IP-адрес компьютера (IPv4 или IPv6), на котором установлен агент.
- **Комментарий** – комментарий, заданный администратором 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, 7.1.0.178.

- *Неизвестная*, чтобы найти агенты устаревших версий или неактивные агенты, у которых нет связи с сервером.

Поддерживаемые шаблоны поиска

- Полное совпадение – `Win7x86.domain.loc`
- Частичное совпадение – `*86.domain.loc` или `*domain*`
- Все результаты – `*`

Нажмите на имя агента в результатах поиска, чтобы перейти в профиль агента. Нажмите **Зарегистрировать** для подтверждения запроса на регистрацию или **Отклонить**, чтобы отклонить запрос.

Профиль агента

В профиле содержится информация об агенте, сессиях пользователей, привязанных устройствах и последних событиях, связанных с агентом.

- **Имя агента** – обязательный параметр. По умолчанию в качестве значения используется DNS-имя компьютера, на котором установлен агент. Чтобы редактировать имя агента, нажмите **Изменить имя**.
- **Комментарий** – необязательный параметр. По умолчанию отсутствует. Чтобы установить или редактировать комментарий, нажмите **Изменить комментарий**.
- **Сессии** – сессии пользователей, выполнивших вход на рабочую станцию (необязательно по смарт-карте) или сессии сервисных служб (отображаются, когда рабочая станция включена). Есть два типа сессий пользователя:
 - Консольная – пользователь выполнил вход на рабочую станцию напрямую.
 - Терминальная – пользователь подключился к рабочей станции удаленно (например, по RDP).
- **Привязанные устройства** – список устройств, которые администратор Indeed CM закрепил за агентом.
- **Последние события** – последние пять событий, связанных с работой агента.

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 требуется.

Закрепление устройства за рабочей станцией (агентом) позволит контролировать использование устройств в организации. Например, агент сможет выполнять определенные действия при подключении незакрепленных за ним устройств. [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 разделе **Привязанные устройства** профиля агента. Для отвязки устройства нажмите **✕** и затем **Отвязать**.

Контроль использования устройств

Настройки использования привязанных устройств задаются 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 КристоПро УЦ 2.0.

При обнаружении агентом одного из событий возможны следующие действия:

- Запись события в журнал системы
- Блокировка пользовательской сессии, запись события
- Блокировка устройства, запись события

- Блокировка пользовательской сессии и устройства, запись события.

Если выбрано действие **Блокировка пользовательской сессии** или **Блокировка пользовательской сессии и устройства**, то укажите **Таймаут до блокировки пользовательской сессии**, максимальное значение 5 секунд.

Чтобы агент отслеживал привязку сессии пользователя к подключенному устройству, включите опцию **Включить проверку привязки устройства к пользователю**.

Если агенты и устройства будут использоваться на рабочих станциях, не входящих в домен вашей организации, то включите опцию **Проверять условия привязки устройства к пользователю на компьютерах, не включенных в домен**.

Задайте сообщение, которое будет отображаться пользователю при нарушении привязки, и действие, которое должен выполнить агент в этом случае.

В сообщениях пользователю допустимо использовать следующие атрибуты:

- {sn} – вывод серийного номера устройства
- {atr} – вывод значения ATR (Answer to reset) устройства
- {model} – вывод модели устройства
- {label} – вывод метки устройства



ПРИМЕР СООБЩЕНИЯ

Подключенное устройство {model}: {sn} не соответствует сессии пользователя.

Мониторинг подключенных устройств

Клиентский агент проверяет все устройства, подключенные к рабочей станции пользователя, и фиксирует в системный **Журнал** следующие события:

- Наличие устройств с заблокированным PIN-кодом пользователя и администратора (в том числе для ГОСТ-областей, если поддерживается устройством)
- Попытки ввода неверных PIN-кодов пользователя и администратора (в том числе для ГОСТ-областей, если поддерживается устройством)
- Подключение незарегистрированных устройств

При длительном отсутствии связи агента с сервером Indeed CM служба Card Monitor фиксирует это событие в системный журнал. Период отсутствия связи агента с сервером задается в разделе

Служба Card Monitor Мастера настройки Indeed CM.

Администратор 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

Чтобы назначить задачу:

1. Найдите нужное устройство в разделе **Устройства** или в карточке пользователя.
2. Раскройте карточку устройства и в верхнем меню выберите задачу.

Задача добавляется в раздел **Назначенные задачи** и отображается до тех пор, пока не выполнится или не отменится. В свойствах задачи отображаются **Тип, Комментарий, Дата создания, Статус**.

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.

Список задач

Агент Indeed CM выполняет следующие задачи:

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. При необходимости введите **Комментарий**, 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.

Смена PIN-кода администратора

1. В карточке устройства нажмите **Сменить PIN-код администратора**.
2. Задайте и подтвердите **Новый PIN-код администратора**.
3. При необходимости введите **Комментарий**, 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. Укажите **Причину отзыва**.
3. Включите опцию **Очистить устройство на агенте**.
4. Если при выпуске устройства было создано/назначено СКЗИ, укажите **Номер и дату документа**, на основании которого происходит уничтожение/изъятие СКЗИ.
5. При необходимости выберите опцию:
 - **Очистить устройство**, чтобы удалить все сертификаты, записанные на устройство с помощью Indeed CM. Сертификаты и ключи, хранившиеся на устройстве до ввода в Indeed CM, не удаляются.

- **Инициализировать устройство**, чтобы удалить все содержимое, политику паролей (если она была на устройстве) и изменить имя устройства.

6. Укажите **Новый PIN-код пользователя**, который установится на устройстве после его изъятия. Если не задать PIN-код пользователя, то после изъятия устройства установится PIN-код, указанный в разделе **Типы устройств**.

ИНФОРМАЦИЯ

PIN-код необходимо установить в том случае, если PIN-код пользователя, указанный в файле типа устройства, не соответствует требованиям, установленным для данного типа устройства при инициализации в момент выпуска.

7. При необходимости введите **Комментарий**, который отобразится в Журнале событий Indeed CM.
8. 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.
9. Нажмите **Отозвать**.

Обновление содержимого устройства

Чтобы создать задачу обновления устройства:

1. В карточке устройства нажмите **Обновить**.
2. Включите опцию **Обновить устройство на агенте**.
3. При необходимости введите **Комментарий**, 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, перейдите в раздел **Поведение** политики использования устройств и включите опции **Включить отслеживание сертификатов** и **Разрешить пользователю выбор сертификатов для отслеживания**.

Когда пользователь подключит устройство к рабочей станции, начнется процедура 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 контроле обновления устройств

Отмена обновления

Вы можете отменить обновление устройства на агенте, если в разделе **Поведение** политики использования устройств включена опция **Разрешить отмену обновления 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**.

Блокировка устройства

При блокировке устройства блокируется PIN-код пользователя. Чтобы заблокировать PIN-код пользователя:

1. В карточке устройства нажмите **Заблокировать**.
2. При необходимости введите **Комментарий**, который отобразится в Журнале событий Indeed CM.

3. Нажмите **Заблокировать**.

ИНФОРМАЦИЯ

Если на устройстве несколько областей (например, РКІ 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 Indeed CM, 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 Indeed CM, укажите его в разделе **Дополнительно**. При необходимости установите **Новый PIN-код пользователя** и нажмите **Инициализировать**. PIN-код администратора в хранилище Indeed CM изменится на указанное значение.

ИНФОРМАЦИЯ

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 Indeed CM.
- Если PIN-код администратора указан, то после инициализации он установится на устройстве и в хранилище Indeed CM.

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

Операции выполняются удаленно на рабочих станциях пользователей, где установлены агенты Indeed CM.

Настройки, которые определяют доступные операции для агентов Indeed CM, задаются в разделе **Конфигурация** в политике использования устройств в разделе **Агенты** → **Поведение**.

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 следующие опции:

- **Добавлять устройство**
- **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 назначится на пользователя, в активной сессии которого оно добавляется.

Чтобы настроить автоматическое назначение устройств при добавлении, включите следующие опции:

- **Добавлять устройство**
- **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. **Настройки выпуска устройства** определяет политика, действующая на пользователя, в активной сессии которого подключается устройство.

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*. **Настройки выпуска устройства** определяет политика, действующая на пользователя.

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 содержат 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 СМ 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 ууууММддННммсс (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

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** отображается список документов, загруженных в Indeed CM.

Предварительные настройки

Чтобы разрешить доступ к репозиторию документов:

1. Откройте **Мастер настройки**, перейдите в раздел **Общие функции** и включите опцию **Внутренний документооборот**.
2. Откройте Консоль 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. Для этого нажмите  и выберите формат XLSX.

Действия с документами

Документы можно скачать , удалить  и редактировать .

Если пользователь предоставил оригинал документа, вы можете зафиксировать получение оригинала в Indeed СМ. Для этого нажмите  напротив нужного документа и включите опцию **Оригинал получен**.

ПРИМЕЧАНИЕ

Функция внутреннего электронного документооборота Indeed СМ 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.

Руководство пользователя

Пользователи Indeed CM могут управлять своими устройствами самостоятельно в Сервисе самообслуживания и в Сервисе удаленного самообслуживания.

Сервис самообслуживания

Сервис самообслуживания (Self-Service) — это веб-приложение, где пользователи Indeed Certificate Manager могут управлять своими устройствами самостоятельно. Доступен по адресу: *https://<FQDN сервера Indeed CM>/cm/ss*.

Настройки входа в приложение определяет администратор в разделе **Конфигурация** → **Политики** → **Аутентификация**.

В Сервисе самообслуживания пользователю доступна следующая информация:

- **О себе** – имя, логин, электронная почта, телефон и фото. Информация о пользователе (имя, имя для входа в домен, электронная почта, телефон и фото) добавляется в Indeed CM автоматически из профиля пользователя в Active Directory. Изменения в профиле пользователя в Active Directory отображаются в Сервисе самообслуживания.
- **Устройства** – список устройств, закрепленных за пользователем, и их содержимое.
- **СКЗИ** – список назначенных СКЗИ.
- **Документы** – список документов пользователя.

ПРИМЕЧАНИЕ

Список действий пользователя с устройствами определяет администратор в разделе **Конфигурация** → **Политики** → **Поведение** Консоли управления Indeed CM.

Операции, доступные пользователю в Сервисе самообслуживания:



Операции с устройствами

Доступные действия со смарт-картами и USB-токенами



Изменение ответов на секретные вопросы

Как изменить ответы на секретные вопросы



СКЗИ

Как просмотреть и распечатать нормативные документы СКЗИ



Документы

Внутренний электронный документооборот



Клиентский агент

Удаленное управление устройствами пользователей



Просмотр файлов и ресурсов

Как просмотреть файлы и ресурсы в Indeed CM



Выгрузка сертификата DSS

Как установить сертификат DSS на рабочую станцию пользователя

Сервис удаленного самообслуживания

Сервис удаленного самообслуживания позволяет выполнять операции с устройствами без подключения к компьютеру, за исключением разблокировки устройства при помощи утилиты Indeed CM - Unblock.

Вход

Сервис удаленного самообслуживания доступен по адресу: *https://<FQDN сервера Indeed CM>/cm/rss*.

Чтобы войти в Сервис удаленного самообслуживания, введите **Имя пользователя**(логин) и символы с изображения. Чтобы получить доступ к карточке пользователя, пройдите аутентификацию по секретным вопросам.

Операции **выключения, включения и отзыва устройств** производятся так же, как и в Сервисе самообслуживания.

Разблокировка устройства

Чтобы разблокировать устройство:

1. Запустите утилиту Indeed CM Unblock (*Пуск – Все программы – Indeed*). Расположение по умолчанию: */IndeedCM/IndeedCM.Unblock.exe*.
2. Выберите устройство в выпадающем списке **Доступные устройства**.
3. Скопируйте код разблокировки из поля **Запрос**.
4. Перейдите в Сервис удаленного самообслуживания, выберите нужное устройство и нажмите **Разблокировать устройство**.
5. Введите код разблокировки и нажмите **Получить ответ**.
6. Введите полученный код ответа в поле **Ответ** утилиты разблокировки.
7. Введите новый PIN-код, подтвердите его и нажмите **Разблокировать**.

Операции 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 и распечатать содержимое устройства

Выпуск

Вы можете получить уже готовое к работе устройство или выпустить устройство самостоятельно, если администратор или оператор Indeed CM выдал вам пустое устройство.

Если вы получили готовое к работе устройство, то при входе в Сервис самообслуживания отобразится вся информация об этом устройстве.

Дополнительные опции:

- **Установить секретные вопросы и ответы на них.** Опция доступна при первом входе в Сервис самообслуживания перед выпуском устройства. Количество секретных вопросов и необходимость установки ответов задает администратор Indeed CM в разделах **Поведение** и **Аутентификация** политики использования устройств.
- **Выпустить устройство самостоятельно.** Опция доступна, если выпущенных устройств нет, и администратор разрешил вам выпускать устройства.

Процедура выпуска

1. Нажмите **Выпустить устройство**.
2. Если администратор задал опцию **Разрешить пользователю выбор необязательных сертификатов при выпуске устройства** в разделе **Поведение** политики использования устройств, отобразится окно выбора шаблонов сертификатов.
Выберите шаблоны, по которым будут сформированы сертификаты для записи на устройство.
3. Если администратор настроил интеграцию в разделе **СМЭВ** политики использования устройств и сертификат выпускается по шаблону для КриптоПро УЦ 2.0 или Валидата УЦ, отобразится форма проверки СМЭВ.
Вы можете проверить данные на соответствие и изменить их, если администратор задал опцию **Разрешить пользователю редактирование данных в форме проверки в СМЭВ** в разделе **Поведение**.
4. Если устройство поддерживает аппаратную криптографию, не добавлено в Indeed CM, и администратор включил опцию **Разрешить пользователю добавление устройства** в разделе **Поведение**, то в окне выпуска устройства отобразится поле **Номер и дата документа**.

Выставите данные о документе, на основании которого будет изготовлено СКЗИ с информацией об устройстве.

5. Если администратор задал опцию **Инициализировать устройство** в разделе **Выпуск** и настроил параметры инициализации в разделе **Инициализация устройства** политики использования устройств, устройство будет инициализировано.

Выпуск с инициализацией



ПРЕДУПРЕЖДЕНИЕ

При выпуске устройства с инициализацией все данные на устройстве будут удалены.

1. Введите **PIN-код администратора**. Поле отображается, если устройство не добавлено в Indeed CM и администратор включил опцию **Разрешить пользователю добавление устройства** в разделе **Поведение**.



ПРИМЕЧАНИЕ

Если поле **PIN-код администратора** оставить пустым, то установится значение, указанное администратором в разделе **Типы устройств**.
Поддерживается ввод PIN-кодов для нескольких областей. Например, для РКІ и ГОСТ на устройствах JaCarta.

2. Нажмите **Выпустить**.

Выпуск без инициализации

1. Введите **PIN-код пользователя**.
2. Введите **PIN-код администратора**. Поле отображается, если устройство не добавлено в Indeed CM и администратор включил опцию **Разрешить пользователю добавление устройства** в разделе **Поведение**.

 ПРИМЕЧАНИЕ

Если поля **PIN-код администратора** и **PIN-код пользователя** оставить пустыми, то установятся значения, указанные администратором в разделе **Типы устройств**.

Поддерживается ввод PIN-кодов для нескольких областей. Например, для PKI и ГОСТ на устройствах JaCarta.

3. Нажмите **Выпустить**.

4. Если устройство содержит сторонние сертификаты, Indeed CM может их обнаружить и внести информацию о таких сертификатах в систему – отследить. Вы можете выбрать сертификаты для отслеживания, если администратор задал опции **Включить отслеживание сертификатов** и **Разрешить пользователю выбор сертификатов для отслеживания** в разделе **Поведение** политики использования устройств.

6. Если администратор задал опцию **Установить случайный PIN-код пользователя** в разделе **Выпуск** политики использования устройств, то после выпуска устройства вы увидите свой PIN-код.

Если администратор настроил рассылку уведомлений по электронной почте в разделе **Уведомления**, PIN-код можно отправить на вашу электронную почту или почту руководителя.

7. По завершении выпуска устройства нажмите **Заккрыть**.

В Сервисе самообслуживания появится раздел **Ваши устройства**, где отображаются сведения о выпущенном устройстве – тип, серийный номер, имя, статус.

Если вы не установили ответы на секретные вопросы, перейдите к их настройке.

Одобрение выпуска

Выпуск устройства может быть приостановлен, если регламент вашей организации предусматривает проверку документов для получения цифровых сертификатов – одобрение.

В окне выпуска устройства появится сообщение *Выпуск устройства ожидает решения*. Устройству присваивается статус **В ожидании**. Это означает, что ваш запрос на выпуск

устройства перешел в стадию рассмотрения.

Отправьте документы для получения сертификата:

- С помощью Indeed CM, если настроена функция внутреннего электронного документооборота Indeed CM ЭДО.
- Вне Indeed CM любым другим способом, принятым в вашей организации. Например, по электронной почте.

Обмен документами в Indeed CM

Если в Indeed CM настроена функция внутреннего электронного документооборота Indeed CM ЭДО, вы можете отправить документы администратору в Сервисе самообслуживания.



ПОДСКАЗКА

Настройки одобрения задает администратор в разделе **Шаблоны** политики использования устройств.

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 **Одобен** 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 **Одобен** 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

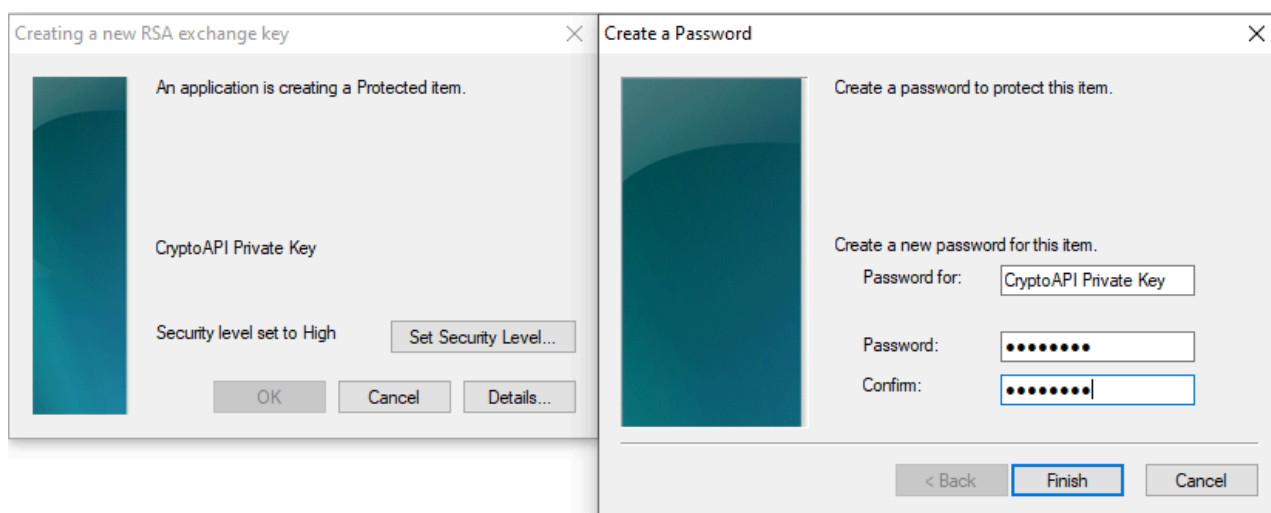
- Поддерживается выпуск только RSA сертификатов
- Не поддерживается работа с PIN-кодами
- Не поддерживается инициализация устройства

Чтобы выпустить устройство Registry, выполните следующие действия:

1. Нажмите **Выпустить устройство**.
2. Задайте имя устройства.
3. В поле **Устройство** выберите:
 - **Registry - Machine: Registry**, чтобы выпустить сертификат в хранилище сертификатов локального компьютера.
 - **Registry - User: Registry**, чтобы выпустить сертификат в хранилище сертификатов текущего пользователя.
4. Нажмите **Выпустить**. Indeed CM отправит запрос на сертификат в УЦ.
5. Создайте пароль для контейнера закрытого ключа в окне создания приватного RSA-ключа.

Это необходимо, если в настройках шаблона сертификата в Microsoft CA администратор задал опцию **При регистрации выводить запрос и требовать от пользователя ответ, если используется закрытый ключ** (Prompt the user during enrollment and require user input when the private key is used) на вкладке **Обработка запроса** (Request Handling).

1. Нажмите **Выбор уровня безопасности..** (Set security Level..) и задайте пароль, удовлетворяющий требованиям безопасности вашей организации.
2. Нажмите **Finish** и **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 *Trm.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, выполните следующие действия:

1. Нажмите **Выпустить устройство**.
2. Задайте имя устройства.
3. Выберите **Создать виртуальное устройство TPM** или выберите уже созданное устройство.
4. Нажмите **Выпустить**.

Indeed CM создаст виртуальную карту. Виртуальную карту TPM можно использовать как аппаратное устройство на вашей рабочей станции. Например, для аутентификации в домене.

Windows Hello for Business

▼ Инструкция для администратора 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, выполните следующие действия:

1. Нажмите **Выпустить устройство**.
2. Задайте имя устройства.
3. Выберите **Настроить WHfB**.
4. Нажмите **Выпустить**.
5. Настройте PIN-код в окне настройки PIN-кода для Windows Hello:

1. Нажмите **Задать PIN-код (Set up PIN)**.

2. Введите учетные данные для основной и пользовательской проверки подлинности (с помощью Indeed CM MFA адаптера) и нажмите **Submit**.
3. Создайте PIN-код и нажмите **ОК**.

После создания PIN-кода Indeed CM продолжит выпуск устройства.

Windows Hello for Business может использоваться как аппаратное устройство на вашей рабочей станции пользователя. Например, для аутентификации в домене.

AirCard

▼ Инструкция для администратора по настройке выпуска устройств AirCard

1. Задайте опцию **Разрешить пользователю выпуск AirCard устройств** в разделе **Поведение** политики использования устройств.
2. **Добавьте** тип устройства *AirCard.xml* в конфигурацию системы.
3. **Установите** компоненты 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, выполните следующие действия:

1. Нажмите **Выпустить устройство**.
2. Задайте имя устройства.
3. Выберите **Создать новое устройство AirCard** или выберите уже созданное устройство.
4. Нажмите **Выпустить**.

После выпуска устройство AirCard автоматически привяжется к вашей рабочей станции. Список разрешенных компьютеров для подключения выпущенного устройства отображается в карточке устройства AirCard.

Подключение AirCard к рабочей станции

AirCard можно подключить двумя способами:

- Автоматически в Indeed CM
- Вручную в панели управления Indeed AirCard Enterprise

Indeed CM

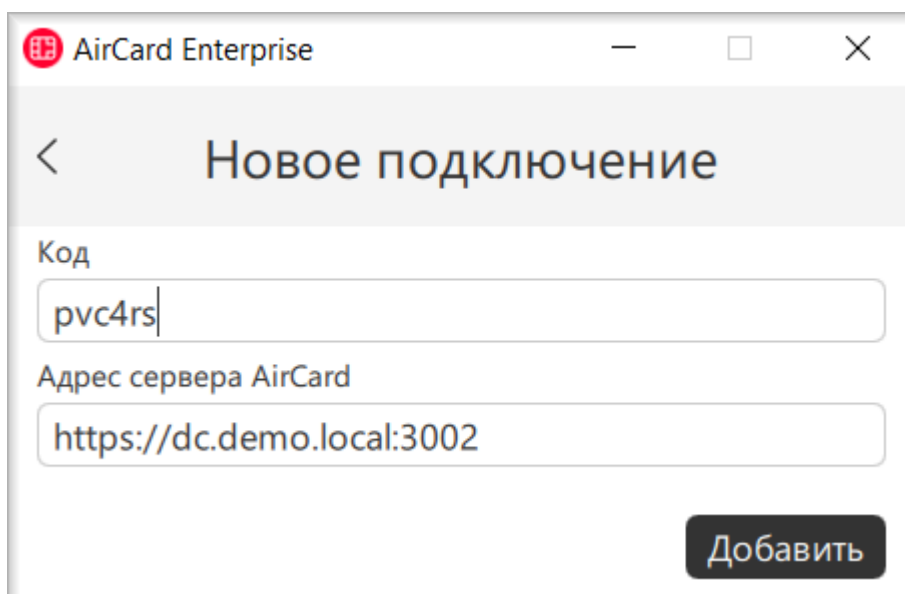
После выпуска устройство AirCard автоматически подключится к разрешенным компьютерам, если они находятся в корпоративной сети предприятия.

Indeed AirCard Enterprise

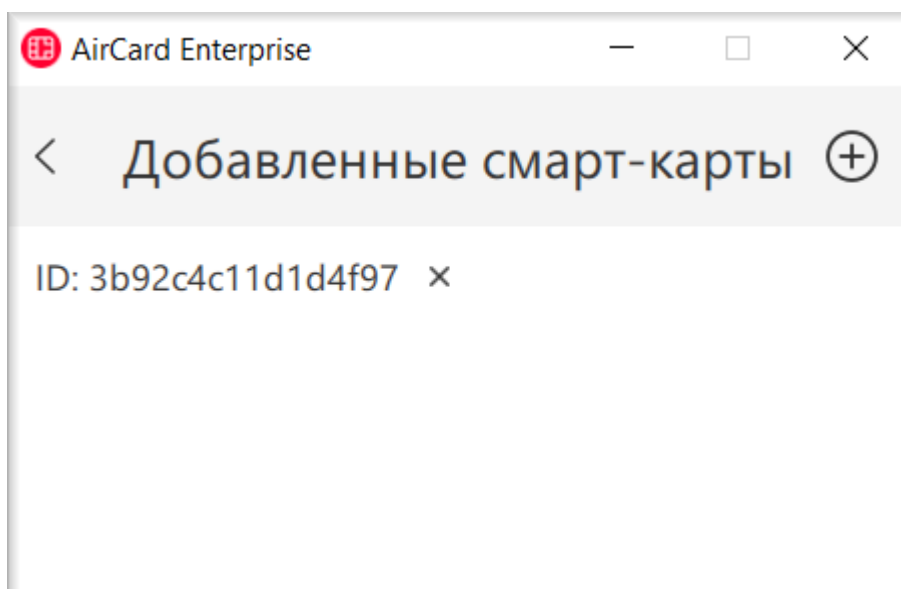
Применяется, если устройство нельзя подключить автоматически (например, если компьютер находится за пределами корпоративной сети предприятия). В этом случае устройство может выпустить только администратор Indeed CM.

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

Вы можете обновить устройство, если администратор задал опцию **Разрешить пользователю обновление устройства** в разделе **Поведение** политики использования устройств.

Чтобы обновить устройство:

1. Подключите устройство к компьютеру.
2. Нажмите **Обновить содержимое устройства**.
3. Если администратор задал опцию **Разрешить пользователю выбор необязательных сертификатов при обновлении устройства** в разделе **Поведение** политики использования устройств, отобразится окно выбора шаблонов сертификатов.
Выберите шаблоны, по которым будут сформированы сертификаты для записи на устройство.
4. Если администратор настроил интеграцию в разделе **СМЭВ** политики использования устройств и сертификат выпускается по шаблону для КриптоПро УЦ 2.0 или Валидата УЦ, отобразится форма проверки СМЭВ.
Вы можете проверить данные на соответствие и изменить их, если администратор задал опцию **Разрешить пользователю редактирование данных в форме проверки в СМЭВ** в разделе **Поведение**.
5. Введите **PIN-код пользователя**.
6. Если на устройство были добавлены сторонние сертификаты, Indeed CM может их обнаружить и внести информацию о таких сертификатах в систему – отследить.
Вы можете выбрать сертификаты для отслеживания, если администратор задал опции **Включить отслеживание сертификатов** и **Разрешить пользователю выбор сертификатов для отслеживания** в разделе **Поведение** политики использования устройств.
7. Нажмите **Обновить**.

Контроль 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**.



ПОДСКАЗКА

Настройки одобрения задает администратор Indeed CM в разделе **Шаблоны** политики использования устройств.

В зависимости от настроек, заданных администратором Indeed CM, вам необходимо подписать и загрузить в Indeed CM следующие документы:

▼ Запрос на сертификат

Предоставьте подписанную форму запроса на сертификат для одобрения в удостоверяющем центре (УЦ). Администратор Indeed CM может предварительно проверить запрос на сертификат перед отправкой запроса в УЦ.

Выполните следующие действия:

1. Загрузите подписанный запрос на сертификат в Indeed CM:
 1. Распечатайте запрос на сертификат. Перейдите на вкладку **Содержимое** в карточке устройства и нажмите  напротив сертификата.
 2. Подпишите запрос на сертификат и добавьте в Indeed CM. **Как подписать и загрузить документ в Indeed CM**
2. Дождитесь одобрения запроса на сертификат в УЦ. На вкладке **Содержимое** в карточке устройства можно проверить статус сертификата – **В ожидании**.
3. Если запрос на сертификат одобрен в УЦ, то сертификат получает статус **Одобен** 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 **Одобен** 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 **Одобен**.

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 **Одобен** 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 СМ 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

Устройство пользователя можно выключить на определенный промежуток времени (например, на период отпуска) и затем снова включить.

В зависимости от настроек политики использования устройств вам доступны следующие действия:

- Выключить и включить устройство
- Только выключить устройство
- Только включить устройство



ПРИМЕЧАНИЕ

Чтобы выключить и включить устройство, его не нужно подключать к рабочей станции.

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*.



ПРЕДУПРЕЖДЕНИЕ

При выключении устройства все или только некоторые из записанных на него сертификатов могут быть отозваны. Настройки отзыва сертификатов при выключении устройства задает администратор Indeed CM.

Выключение устройств без выполнения входа в систему

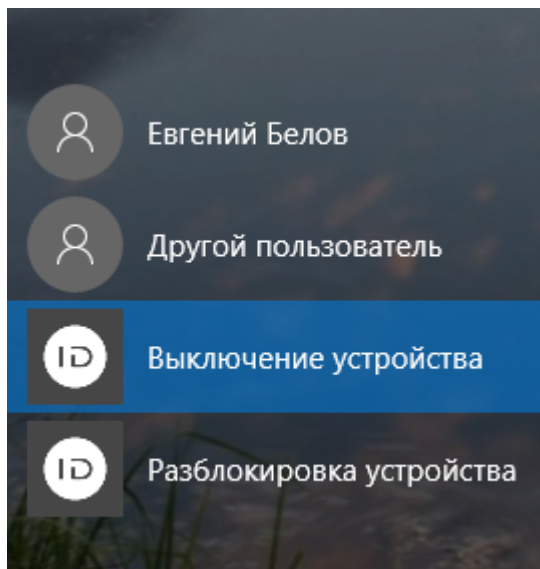
В экстренном случае пользователь может самостоятельно выключить устройство без входа в операционную систему, если администратор настроил **разрешение**.

Выключение устройства доступно только в том случае, если у рабочей станции, с которой осуществляется операция, есть связь с сервером Indeed CM, и у пользователя настроены секретные вопросы.

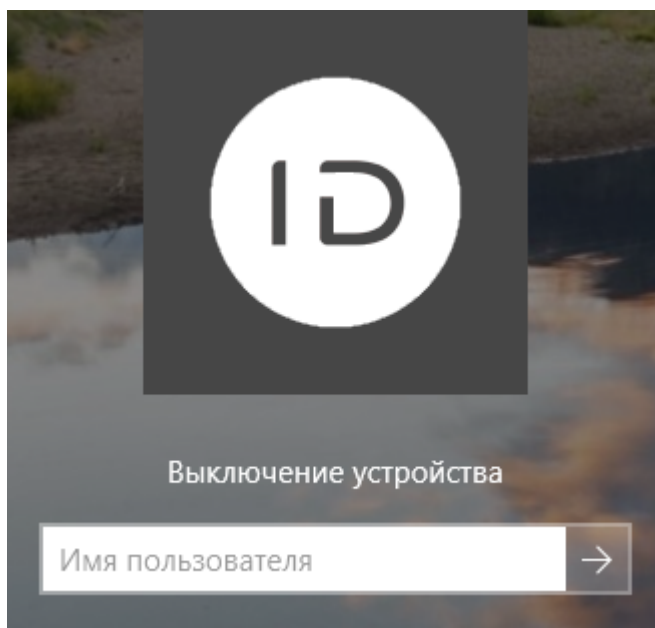
Пример выключения устройства в ОС Windows 10

Чтобы выключить устройство:

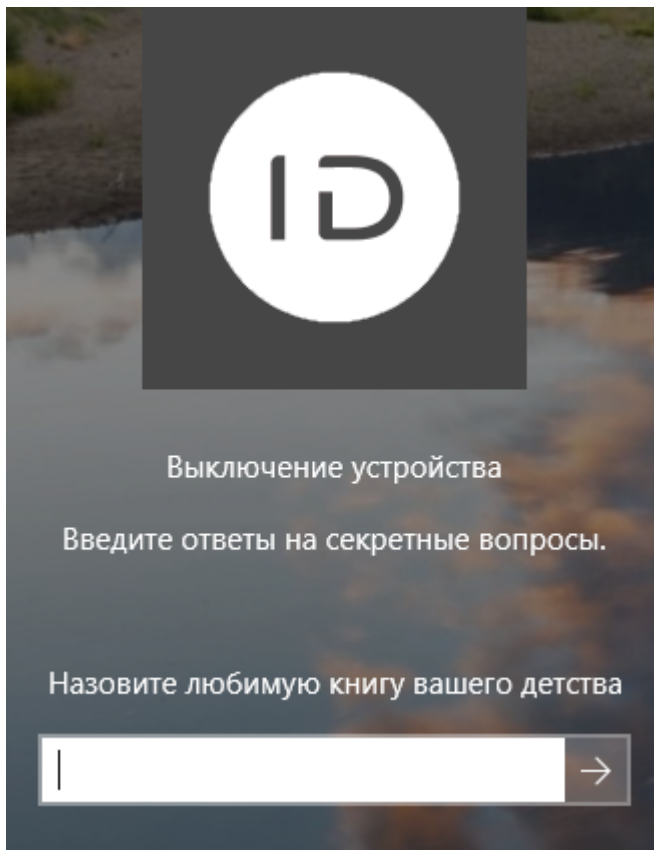
1. На экране выбора пользователей для входа в ОС выберите **Выключение устройства**.



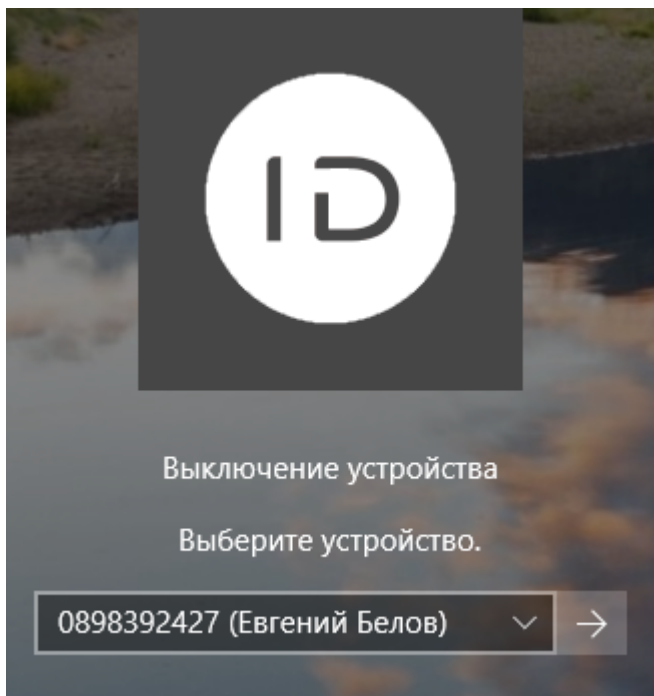
2. В окне входа в ОС укажите ваше имя пользователя (логин), устройство (смарт-карту) которое необходимо выключить.



3. Введите ответы на секретные вопросы.



4. Выберите устройство из списка и нажмите .



Отзыв и очистка

Устройство пользователя можно отозвать в случае его повреждения, утери или компрометации.

ПРЕДУПРЕЖДЕНИЕ

При отзыве устройства все или только некоторые из записанных на него сертификатов могут быть отозваны без возможности восстановления. Настройку **Отзывать сертификат при отзыве или выключении устройства** задает администратор Indeed CM в параметрах шаблонов сертификатов используемых УЦ.

Отзыв

Чтобы отозвать устройство:

1. В карточке устройства нажмите **Прекратить использование устройства**.
2. Укажите причину отзыва:
 - Устройство неисправно
 - Устройство утеряно
 - Компрометация устройства
3. Нажмите **Отозвать**.

Состояние устройства изменится с *Выпущено* на *Отозвано*.

Очистка

Вы можете очистить только устройство в состоянии *Отозвано*. Чтобы очистить устройство, подключите его к своей рабочей станции и нажмите **Очистить устройство**.

ПРИМЕЧАНИЕ

Чтобы очистить и удалить устройство TPM, Registry, Windows Hello for Business, нажмите **Удалить устройство**.

Ваши устройства

▼ Rutoken S, 0755398982

Евгений Белов

Отозвано

Очистить устройство 

Номер документа

[Дополнительно](#) 

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

Новый PIN-код пользователя

Пожалуйста, вставьте устройство и нажмите 'Очистить'

Очистить

Отмена



ПРЕДУПРЕЖДЕНИЕ

При очистке устройства все данные, записанные на него с помощью Indeed CM, удаляются.

Номер документа СКЗИ

Если на очищаемом устройстве содержатся средства криптографической защиты информации (СКЗИ), подлежащие учету в соответствии с законодательством РФ, то в процессе очистки имеющиеся СКЗИ будут уничтожены. Укажите **Номер документа**, в соответствии с которым выполняется уничтожение СКЗИ.

PIN-код пользователя

При очистке устройства можно изменить PIN-код пользователя. Indeed CM может изменить его на значение по умолчанию или на значение, соответствующее политике безопасности вашей компании (требования к длине и сложности пароля).

Укажите **Новый PIN-код пользователя**, который должен быть установлен на устройстве после его очистки или оставьте это поле пустым для установки PIN-кода по умолчанию. Нажмите

Очистить.

После очистки устройство останется закрепленным за вами в Indeed CM, и его можно выпустить повторно. [Подробнее о выпуске устройства](#)

Сброс и изменение PIN-кода

Если пользователь забыл PIN-код своего устройства и заблокировал его, он может сбросить PIN-код и задать новый, чтобы разблокировать устройство.



ПРИМЕЧАНИЕ

Возможность сброса PIN-кода настраивает администратор Indeed CM в политике использования устройств в разделе Поведение.

Чтобы сбросить PIN-код устройства:

1. В карточке устройства нажмите **Сбросить PIN-код устройства**.
2. Подключите устройство к компьютеру.
3. Задайте новый PIN-код и подтвердите его.
4. Нажмите **Сбросить**.
5. Нажмите **Заккрыть**.

Чтобы изменить PIN-код устройства:

1. В карточке устройства нажмите **Изменить PIN-код устройства**.
2. Подключите устройство к компьютеру.
3. Введите текущий PIN-код, задайте новый PIN-код и подтвердите его.
4. Нажмите **Изменить**.
5. Нажмите **Заккрыть**.

Просмотр содержимого

Если администратор разрешил пользователям просмотр содержимого устройства в Сервисе самообслуживания, то в карточке выпущенного устройства доступна вкладка **Содержимое** с информацией о сертификатах.

⚠ ПРИМЕЧАНИЕ

Просмотр содержимого устройства доступен, если в Мастере настройки в разделе **Общие функции** включена опция **Просмотр содержимого устройства**.

Пользователи могут распечатать  сведения о сертификате и запросе на сертификат.

Ваши устройства

▼  Rutoken ECP, 0894130607

👤 Evgeniy Belov

Выпущено

Действия

Содержимое

↻

Сертификаты

Шаблон	УЦ	Действителен до	Состояние
Вход по смарт-карте	demo-DC-CA	21.01.2021 12:11	Действительный 

Отслеживаемые сертификаты

Субъект	Издатель	Действителен до	Состояние
Operator	Тестовый головной УЦ	22.04.2021 15:00	Действительный 

Сертификат

Запрос на сертификат

Изменение ответов на секретные вопросы

Чтобы изменить ответы на заданные секретные вопросы:

1. Под информацией о пользователе нажмите **Изменить ответы на секретные вопросы**.
2. Выберите вопрос и введите ответ на вопрос.
3. Нажмите **ОК**.



ПРИМЕЧАНИЕ

Возможность изменения ответов на секретные вопросы настраивает администратор Indeed СМ в разделе Поведение политики использования устройств.



Белов Евгений Александрович

Логин	DEMO\Evgeniy.Belov
E-mail	evgeniy.belov@demo.com
Телефон	+7 (905) 288-58-23

[? Изменить ответы на секретные вопросы](#) [Пользователь КристоПро 2.0](#)

Секретные вопросы

Секретные вопросы необходимы для подтверждения операций с вашими устройствами

Секретный вопрос

Ваш любимый цвет? ▼

Ответ

ОК

Отмена

СКЗИ

В разделе **Ваши СКЗИ** в Сервисе самообслуживания вы можете управлять средствами криптографической защиты информации (СКЗИ) – распечатать и подписать нормативные документы СКЗИ и получить доступ к работе с СКЗИ после прохождения обучающих курсов.

ⓘ ПРИМЕЧАНИЕ

Доступ к разделу **Ваши СКЗИ** настраивает администратор. [Инструкция](#)

Печать документов

Чтобы распечатать документ СКЗИ:

1. Нажмите  напротив нужного экземпляра СКЗИ.
2. Выберите вид нормативного документа или шаблон печати.

Выпадающий список **Вид нормативного документа** отображается, если администратор **настроил** шаблон печати для данного объекта СКЗИ в текущем состоянии.

Если администратор не настроил шаблон печати, отображается выпадающий список **Шаблон печати**, где можно выбрать любой из шаблонов, **загруженных** для данного объекта СКЗИ.

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](#)

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](#)

Документы

Функция внутреннего электронного документооборота Indeed CM ЭДО позволяет пользователям, администраторам и операторам обмениваться документами для получения сертификата ключа проверки электронной подписи (далее – сертификат подписи) и нормативными документами СКЗИ.

▼ 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

Вы можете управлять документами в разделе **Ваши документы**. Документы можно добавить, подписать, скачать, редактировать или удалить.

Документы для получения сертификата подписи доступны в карточке устройства в разделе **Содержимое**. Нормативные документы СКЗИ доступны в разделе **Ваши СКЗИ**.

Настройки доступа к работе с документами

Пользователи могут:

- Управлять документами, если администратор включил опцию **Внутренний документооборот** в Мастере настройки Indeed CM в разделе **Общие функции**
- Управлять нормативными документами СКЗИ, если администратор включил опцию **Вести журнал учета СКЗИ** в Мастере настройки Indeed CM в разделе **Функции системы** → **Журнал учета СКЗИ** и опцию **Разрешить пользователю просмотр СКЗИ** в настройках политики использования устройств в разделе **Поведение**
- Удалять документы, если администратор включил опцию **Разрешить пользователю удаление документа** в настройках политики использования устройств в разделе **Поведение**.

Подпись документов

При работе с подписью документов вам доступны следующие действия:

- Добавить документы, подписанные на бумаге
- Добавить документы и подписать электронной подписью (ЭЦП)
- Подписать документы, сформированные по готовым шаблонам

Добавление документов, подписанных на бумаге

Чтобы добавить документ, подписанный на бумаге:

1. В разделе **Ваши документы** нажмите **Добавить документ**.
2. Выберите тип документа.
3. Загрузите файл.
4. Заполните поле **Описание** (необязательно).
5. Нажмите **Добавить**.

Добавление документов и подпись ЭЦП

При добавлении документа вы можете подписать его электронной подписью.



ТРЕБОВАНИЯ ДЛЯ ПОДПИСИ ДОКУМЕНТОВ В INDEED CM

- У вас есть устройство, которое содержит сертификат подписи.
- Сертификат подписи имеет любой статус, кроме *Отозван*, *Истек* и *Ключ истек*.

Чтобы добавить и подписать документ:

1. В разделе **Ваши документы** нажмите **Добавить документ**.
2. Выберите тип документа и загрузите файл.
3. Заполните поле **Описание** (необязательно).
4. Включите опцию **Подписать документ**.
5. Подключите устройство с сертификатом подписи к рабочей станции и выберите его в выпадающем списке **Устройство**.
6. В выпадающем списке **Сертификат** выберите подходящий сертификат.
7. Введите PIN-код пользователя.
8. Нажмите **Добавить**.

Подпись документов, сформированных по готовым шаблонам

Вы можете 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**.

Подпись документов 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**. Если вам необходимо 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.
6. Введите PIN-код пользователя.
7. Нажмите **Подписать**.

Подпись нормативных документов СКЗИ

1. В разделе **Ваши СКЗИ** нажмите  напротив экземпляра СКЗИ, для которого формируется документ.
2. Выберите вид нормативного документа или шаблон печати.
Выпадающий список **Вид нормативного документа** отображается, если администратор **настроил** шаблон печати для данного объекта СКЗИ в текущем состоянии.
Если администратор не настроил шаблон печати, отображается выпадающий список **Шаблон печати**, где можно выбрать любой из шаблонов, **загруженных** для данного объекта СКЗИ.
3. Нажмите **Распечатать документ**. Откроется файл документа.
4. Нажмите **Подписать документ**. Если вам необходимо скачать и распечатать 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.
7. Введите PIN-код пользователя.
8. Нажмите **Подписать**.

Клиентский агент

На рабочую станцию пользователя можно установить клиентский агент Indeed CM Agent, который позволит администраторам назначать задачи на устройства пользователя и выполнять их в полностью автоматическом или полуавтоматическом режиме.

[Подробнее о работе Indeed CM Agent](#)

Агент запускается автоматически.

Задачи, которые требуют действия пользователя:

- Смена PIN-кода устройства
- Сброс и разблокировка PIN-кода
- Обновление содержимого устройства

Смена PIN-кода

Администратор Indeed CM может установить **срок действия PIN-кода** вашего устройства.

Если срок действия истек, то при подключении устройства к рабочей станции вы увидите окно смены PIN-кода. Задайте новый PIN-код.

УСТРОЙСТВА РУТОКЕН ЭЦП 3.0 И ЕТОКЕН 72К

Если администратор настроил требование сменить PIN-код устройств Рутокен ЭЦП 3.0, IDPrime и eToken 72K, вам понадобится задать новый PIN-код при первом подключении таких устройств к рабочей станции.

Сброс и разблокировка PIN-кода

Если вы забыли PIN-код устройства или заблокировали его, сообщите администратору. Администратор создаст задачу по сбросу PIN-кода для вашего устройства. Подключите устройство к компьютеру и дождитесь, когда появится форма сброса PIN-кода.



ПРЕДУПРЕЖДЕНИЕ

Для сброса PIN-кода у вас должны быть заданы ответы на секретные вопросы. Если вы не помните ответы, измените их в [Сервисе самообслуживания](#).

Чтобы сбросить PIN-код:

1. Подключите устройство к компьютеру. Появится форма сброса PIN-кода.
2. Введите ответ на один или несколько секретных вопросов.
3. Задайте новый PIN-код и подтвердите его.
4. Нажмите **Сбросить**.

Появится сообщение *PIN-код пользователя на устройстве успешно сброшен*.

Обновление содержимого устройства

Обновление устройства может потребоваться, если срок действия одного или нескольких сертификатов на устройстве подходит к концу, или вам необходимо записать на устройство новый сертификат.

Администратор Indeed CM создаст задачу по обновлению содержимого вашего устройства.

Чтобы обновить устройство:

1. Подключите устройство к компьютеру. Появится форма обновления.
2. Введите PIN-код и нажмите **Обновить**.
3. Если в процессе обновления отобразилось окно выбора сертификатов для отслеживания, выберите сертификаты и нажмите **ОК**.



ПРИМЕЧАНИЕ

Если на устройство были добавлены сторонние сертификаты, Indeed CM может их обнаружить и внести информацию о таких сертификатах в систему – отследить.

Вы можете выбрать сертификаты для отслеживания, если администратор задал опции **Включить отслеживание сертификатов** и **Разрешить пользователю выбор сертификатов для отслеживания** в разделе [Поведение](#) политики использования устройств.

Обновление может длиться несколько минут. После успешного завершения обновления отобразится сообщение *Устройство успешно обновлено*. В случае ошибки обновления ее текст появится в информационном сообщении.

Обновление устройства может быть приостановлено, если регламент вашей организации предусматривает проверку документов для обновления цифровых сертификатов. В окне обновления устройства появится сообщение *Обновление устройства ожидает решения*. Устройству присваивается статус **В ожидании**.

[Подробнее о контроле обновления устройств](#)

Просмотр файлов и ресурсов

При настройке Indeed CM администратор может добавить файлы и ссылки, которые будут доступны пользователям в Сервисе самообслуживания по ссылке *https://<FQDN сервера Indeed CM>/cm/ss/Downloads*.



ПОДСКАЗКА

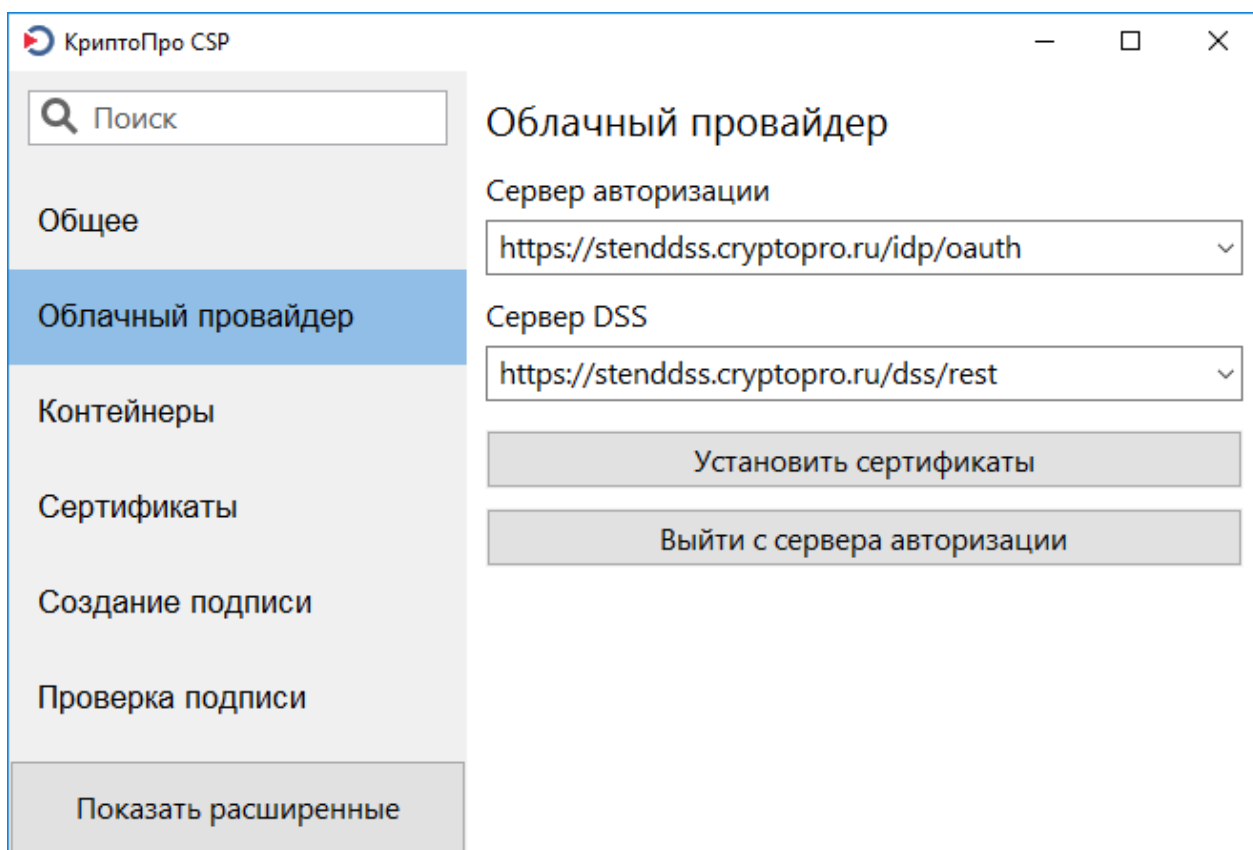
Администраторы могут загружать файлы и ресурсы, если в разделе **Общие функции** Мастера настройки Indeed CM включена опция **Загрузка файлов и ресурсов**.

Ресурсы доступны на странице **Загрузки**.

Выгрузка сертификата DSS

Чтобы выгрузить сертификат из облачного хранилища:

1. Запустите компонент **Инструменты КriptoПро**.
2. Перейдите в раздел **Облачный провайдер**.
3. Укажите URL-адрес для сервера авторизации и сервера DSS.



4. Нажмите **Установить сертификат**.
5. Введите логин и пароль от личного кабинета пользователя DSS.
6. Нажмите **Войти**.

 CryptoPro Web Authentication✕



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

Аутентификация в сервисе API



Устройства

Управление устройствами через API



СКЗИ

Управление СКЗИ через API

Аутентификация

Для работы с API вы можете использовать любые инструменты. Далее описана настройка работы с API в Swagger, Postman, Windows Powershell, Linux Bash.

Выберите инструкцию в зависимости от типа аутентификации, настроенного на этапе конфигурирования Indeed CM в **Мастере настройки**.

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. Откройте конфигурационный файл `C:\inetpub\wwwroot\cm\api` и убедитесь, что в параметре `authentication` установлено значение `Windows`.

Swagger

Чтобы работать с API через Swagger, внесите изменения в конфигурационный файл для приложения API:

1. Откройте файл `appsettings.json`. Файл находится в каталоге `C:\inetpub\wwwroot\cm\api`.
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

Postman доступен в виде приложения или в веб-интерфейсе. Ниже описана работа с API через приложение 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 и пароль.
4. В выпадающем списке запросов выберите тип запроса и укажите URL.
5. 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. Откройте конфигурационный файл приложения Indeed CM API *appsettings.json*. Файл находится в каталоге *C:\inetpub\wwwroot\cm\api*.
7. Убедитесь, что в параметре `authentication` установлено значение `OAuth2Introspection`.

Чтобы проверить настройки аутентификации в API на Linux-сервере Indeed CM:

1. Откройте конфигурационный файл приложения Indeed CM API *appsettings.json*. Файл находится в каталоге */opt/indeed/cm/api*.
2. Убедитесь, что в параметре `authentication` установлено значение `OAuth2Introspection`.

Swagger

Чтобы работать с API через Swagger, внесите изменения в конфигурационный файл для приложения API:

1. Откройте файл *appsettings.json*. Файл находится в каталоге *C:\inetpub\wwwroot\cm\api* в ОС Windows и */opt/indeed/cm/api* в ОС Linux.
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 строке **Scopes** нажмите **Select all**.
4. Нажмите **Authorize**.

Postman

Postman доступен в виде приложения или в веб-интерфейсе. Ниже описана работа с API через приложение Postman.

Чтобы настроить аутентификацию в Postman:

1. В левой части верхней панели управления Postman нажмите **+**. Откроется поле, в котором можно вводить запросы.
2. Перейдите на вкладку **Auth**.
3. В выпадающем списке выберите **OAuth 2.0**.
4. В поле **Add auth data to** оставьте значение по умолчанию **Request Headers**.
5. В разделе **Current Token** в поле **Header Prefix** оставьте значение по умолчанию **Bearer**.
6. В разделе **Configure New Token** укажите данные для получения токена доступа:
 - **Token Name** – укажите имя токена.
 - **Grant Type** – выберите значение **Password Credentials**.
 - **Access Token URL** – укажите ссылку для получения токена доступа:
`https://<FQDN сервера Indeed CM>/oidc/connect/token`.

- **Client ID** – укажите идентификатор сервиса API `WebApiClient`.
- **Username** – укажите имя пользователя в формате `Domain\Username`.
- **Password** – укажите пароль.
- **Client Authentication** – выберите **Send as Basic Auth header**.

7. Нажмите **Get New Access Token**. Откроется окно с токеном.

8. 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. В терминале или в файле Powershell-скрипта подготовьте следующие переменные.

```
$body = @{grant_type='password'; username='Domain\Username';  
password='P@ssw0rd'; scope='openid  
webapi';client_id='WebApiClient' }  
$url="https://<FQDN сервера Indeed CM>/oidc/connect/token"
```

2. Извлеките токен доступа (access_token) из ответа.

```
$resp = Invoke-RestMethod -Method Post -Uri $url -Body $body -  
UseDefaultCredentials  
$token = $resp.access_token
```

3. Добавьте полученный токен в заголовок запроса.

```
$headers = @{Authorization="Bearer $token"}
```

4. Выполните запрос.

```
Invoke-RestMethod -Method Get -Uri $url -Headers $headers -
UseDefaultCredentials
```

Linux Bash

Чтобы работать с API через Linux Bash, используйте Bash-скрипты.

Получите токен доступа и выполните запрос:

1. В терминале или в файле Bash-скрипта подготовьте следующие переменные.

```
username="DOMAIN\username"
password="P@ssw0rd"
base_url="https://<FQDN сервера Indeed CM>"
body="grant_type=password&username=$username&password=$password&scope=openid"
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"
token_url="$base_url/cm/oidc/connect/token"
# Get token
resp=$(curl -s -X POST $token_url -H "Content-Type: application/x-www-form-urlencoded" -d "$body")
# Parse token
token=$(echo $resp | grep -o '"access_token": "[^"]*"' | cut -d'"' -f4)
# Combine header
headers="Authorization: Bearer $token"
# Test enable card (POST)
curl -X POST "https://cm-test.local/cm/api/Cards/123/Enable" -H "$headers" -d "$body"
# Test Get enabled card (GET)
curl -X GET "https://cm-test.local/cm/api/Cards?state=Issued&offset=0"
```


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
<code>userName</code>	Имя пользователя в формате DOMAIN\LogonName или User Principal Name (UPN)
<code>policyName</code>	Название политики, действующей на устройство
<code>serialNumber</code>	Серийный номер устройства
<code>cardTypeName</code>	Название типа устройства
<code>cardModelName</code>	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
<code>comment</code>	Комментарий
<code>tags</code>	Теги
<code>state</code>	Состояние устройства: <code>Clean</code> – пустое <code>Assigned</code> – назначено <code>Pending</code> – в ожидании <code>Issued</code> – выпущено <code>Disabled</code> – выключено <code>Revoked</code> – отозвано

Параметр	Описание
<code>contentExpirationStatus</code>	Информация об истечении срока действия сертификатов на устройстве: <code>None</code> – нет истекающих или истекших сертификатов <code>ManagedCertificatesExpiring</code> – управляемые сертификаты истекают <code>ManagedCertificatesExpired</code> – управляемые сертификаты истекли <code>CommonCertificatesExpiring</code> – общие сертификаты истекают <code>CommonCertificatesExpired</code> – общие сертификаты истекли <code>TracedCertificatesExpiring</code> – отслеживаемые сертификаты истекают <code>TracedCertificatesExpired</code> – отслеживаемые сертификаты истекли
<code>timeIssued</code>	Время выпуска устройства в формате ISO 8601. Например: 2024-12-03T11:22:20.1824104Z, 2024-12-03
<code>timeUpdated</code>	Время обновления устройства в формате ISO 8601
<code>timeRevoked</code>	Время отзыва устройства в формате ISO 8601
<code>offset</code>	Сдвиг на указанное количество устройств
<code>count</code>	Количество устройств, информация о которых передается в ответе

▼ Возвращаемые значения

Параметр	Описание
<code>id</code>	Идентификатор устройства
<code>serialNumber</code>	Серийный номер устройства
<code>cardTypeName</code>	Название типа устройства
<code>cardModelName</code>	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
<code>atr</code>	Answer To Reset устройства
<code>label</code>	Метка устройства
<code>comment</code>	Комментарий
<code>tags</code>	Теги
<code>state</code>	Состояние устройства
<code>formFactor</code>	Форм-фактор устройства
<code>pacNumber</code>	HID-метка устройства
<code>expirationDate</code>	Срок действия устройства
<code>timeIssued</code>	Время выпуска устройства
<code>timeDisabled</code>	Время выключения устройства
<code>timeUpdated</code>	Время обновления устройства

Параметр	Описание
<code>timeRevoked</code>	Время отзыва устройства
<code>userId</code>	Идентификатор пользователя, на которого назначено устройство
<code>userName</code>	Имя пользователя устройства в формате DOMAIN\LogonName или User Principal Name (UPN)
<code>policyId</code>	Идентификатор политики, действующей на устройство
<code>policyName</code>	Название политики, действующей на устройство
<code>certificates</code>	<code>type</code> – тип сертификата <code>serialNumber</code> – серийный номер сертификата <code>thumbprint</code> – отпечаток сертификата <code>subject</code> – общее имя (CN) субъекта сертификата <code>issuer</code> – общее имя (CN) издателя сертификата <code>validFrom</code> – дата начала срока действия сертификата в формате ISO 8601 <code>validTo</code> – 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
<code>id</code>	Обязательно	Идентификатор устройства
<code>reason</code>	Необязательно	Причина отзыва устройства: 0 – <code>--</code> – причина отзыва не указана 1 – <code>CardBroken</code> – устройство неисправно 2 – <code>CardLost</code> – устройство утеряно 3 – <code>CardUpgrade</code> – обновление устройства 4 – <code>CardExpired</code> – истечение срока действия устройства 4 – <code>CardWithdraw</code> – изъятие устройства 5 – <code>UserRemoved</code> – пользователь удален 6 – <code>CardCompromised</code> – 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
<code>id</code>	Обязательно	Идентификатор устройства
<code>destructor</code>	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
<code>objectType</code>	Необязательно	Тип объекта: <code>Distributive</code> – дистрибутив <code>License</code> – лицензия <code>Documentation</code> – документация <code>KeyDocument</code> – ключевой документ <code>Card</code> – ключевой носитель <code>Custom</code> – пользовательский
<code>skziTypeId</code>	Необязательно	Идентификатор типа СКЗИ
<code>serialNumber</code>	Необязательно	Серийный номер СКЗИ
<code>instanceNumber</code>	Необязательно	Номер экземпляра
<code>state</code>	Необязательно	Состояние: <code>Created</code> – изготовлено <code>Assigned</code> – назначено <code>Sent</code> – передано <code>Returned</code> – возвращено <code>Issued</code> – выдано <code>Installed</code> – установлено <code>Destructed/Withdrawn</code> – уничтожено/изъято
<code>userName</code>	Необязательно	Имя пользователя в формате Common Name
<code>startDate</code>	Необязательно	Поиск СКЗИ с указанной даты
<code>endDate</code>	Необязательно	Поиск СКЗИ до указанной даты

Параметр	Обязательно/ необязательно	Описание
<code>offset</code>	Необязательно	Сдвиг на указанное количество записей СКЗИ
<code>count</code>	Необязательно	Количество СКЗИ для вывода в ответе

▼ Возвращаемые значения

Параметр	Описание
<code>id</code>	Идентификатор СКЗИ
<code>timeCreated</code>	Время изготовления СКЗИ
<code>userId</code>	Идентификатор пользователя
<code>userName</code>	Имя пользователя в формате Common Name
<code>logonName</code>	Имя учетной записи пользователя в формате DOMAIN\LogonName
<code>objectType</code>	Тип объекта: <code>Distributive</code> – дистрибутив <code>License</code> – лицензия <code>Documentation</code> – документация <code>KeyDocument</code> – ключевой документ <code>Card</code> – ключевой носитель <code>Custom</code> – пользовательский
<code>skziTypeId</code>	Идентификатор типа СКЗИ
<code>serialNumber</code>	Серийный номер СКЗИ
<code>instanceNumber</code>	Номер экземпляра
<code>creationData</code>	Объект с информацией об изготовлении СКЗИ: <code>creator</code> – имя изготовителя <code>timeCreated</code> – время изготовления <code>docNumber</code> – 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

Параметр	Описание
<code>destructionData</code>	Объект с информацией об уничтожении/изъятии СКЗИ: <code>destructor</code> – ФИО сотрудников органа криптографической защиты, пользователей СКЗИ, производивших уничтожение/изъятие СКЗИ <code>timeDestroyed</code> – время уничтожения/изъятия <code>docNumber</code> – номер акта или расписки об уничтожении
<code>comment</code>	Примечание
<code>customFields</code>	Объект с информацией о дополнительных полях в журнале учета СКЗИ <code>id</code> – идентификатор атрибута, который подставляется в шаблоны печати нормативных документов <code>value</code> – имя поля, которое отображается в журнале СКЗИ Дополнительные поля задаются в Мастере настройки Indeed СМ в разделе Журнал учета СКЗИ
<code>state</code>	Состояние СКЗИ: <code>Created</code> – изготовлено <code>Assigned</code> – назначено <code>Sent</code> – передано <code>Returned</code> – возвращено <code>Issued</code> – выдано <code>Installed</code> – установлено <code>Destructed/Withdrawn</code> – 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 ууууMMddHHmmss (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
<code>skziTypeName</code>	Необязательно	Название типа СКЗИ.
<code>family</code>	Необязательно	Семейство СКЗИ: <code>Hardware</code> – аппаратный <code>Software</code> – программный <code>HardwareSoftware</code> – аппаратно-программный
<code>includeArchived</code>	Необязательно	<code>true</code> – включить в возвращаемые значения информацию об СКЗИ архивных типов <code>false</code> – не включать в возвращаемые значения информацию об СКЗИ архивных типов Значение по умолчанию – <code>false</code>

▼ Возвращаемые значения

Параметр	Описание
<code>id</code>	Идентификатор СКЗИ.
<code>skziTypeName</code>	Название типа СКЗИ.
<code>family</code>	Семейство СКЗИ: <code>Hardware</code> – аппаратный <code>Software</code> – программный <code>HardwareSoftware</code> – аппаратно-программный
<code>conformityCertificate</code>	Информация о сертификате соответствия на СКЗИ: <code>number</code> – номер <code>issueDate</code> – дата выдачи <code>notAfter</code> – дата окончания срока действия
<code>supportCertificate</code>	Информация о сертификате технической поддержки: <code>number</code> – номер <code>issueDate</code> – дата выдачи <code>notAfter</code> – дата окончания срока действия
<code>cardTypeName</code>	Название типа устройства. Параметр отображается только для СКЗИ аппаратных типов
<code>cardTypeModel</code>	Название модели устройства. Параметр отображается только для устройств Рутокен и JaCarta, если в разделе Типы СКЗИ настроены типы СКЗИ для различных моделей
<code>isDefault</code>	<code>true</code> – тип СКЗИ, используемый по умолчанию (для программных СКЗИ) <code>false</code> – тип СКЗИ, не используемый по умолчанию

Параметр	Описание
<code>isArchived</code>	<code>true</code> – архивный тип СКЗИ <code>false</code> – 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
<code>id</code>	Идентификатор СКЗИ
<code>timeCreated</code>	Время изготовления СКЗИ
<code>userId</code>	Идентификатор пользователя
<code>userName</code>	Имя пользователя в формате Common Name
<code>logonName</code>	Имя учетной записи пользователя
<code>objectType</code>	Тип объекта: <code>Distributive</code> – дистрибутив <code>License</code> – лицензия <code>Documentation</code> – документация <code>KeyDocument</code> – ключевой документ <code>Card</code> – ключевой носитель <code>Custom</code> – пользовательский
<code>skziTypeId</code>	Идентификатор типа СКЗИ
<code>serialNumber</code>	Серийный номер СКЗИ
<code>instanceNumber</code>	Номер экземпляра
<code>creationData</code>	Объект с информацией об изготовлении СКЗИ: <code>creator</code> – имя изготовителя <code>timeCreated</code> – время изготовления <code>docNumber</code> – номер документа об изготовлении

Параметр	Описание
<code>sendingData</code>	Объект с информацией о передаче СКЗИ: <code>docNumber</code> – номер сопроводительного письма <code>recipient</code> – ФИО сотрудника, который подтверждает получение СКЗИ <code>timeSent</code> – время передачи <code>timeConfirmed</code> – время подтверждения получения <code>confirmationDocNumber</code> – номер документа о подтверждении получения
<code>returnData</code>	Объект с информацией о возврате СКЗИ: <code>docNumber</code> – номер сопроводительного письма <code>timeReturned</code> – время возврата <code>timeConfirmed</code> – время подтверждения получения СКЗИ <code>confirmationDocNumber</code> – номер документа о подтверждении получения
<code>issueData</code>	Объект с информацией о выдаче СКЗИ: <code>docNumber</code> – номер сопроводительного письма <code>timeIssued</code> – время выдачи
<code>installationData</code>	Объект с информацией об установке СКЗИ: <code>docNumber</code> – номер документа об установке <code>installer</code> – ФИО сотрудников органа криптографической защиты, пользователей СКЗИ, производивших установку СКЗИ <code>timeInstalled</code> – время установки <code>hardwareId</code> – номер аппаратного средства, на котором установлено или к которому подключено СКЗИ <code>location</code> – место установки

Параметр	Описание
<code>destructionData</code>	Объект с информацией об уничтожении/изъятии СКЗИ: <code>destructor</code> – ФИО сотрудников органа криптографической защиты, пользователей СКЗИ, производивших уничтожение/изъятие СКЗИ <code>timeDestroyed</code> – время уничтожения/изъятия <code>docNumber</code> – номер акта или расписки об уничтожении
<code>comment</code>	Примечание
<code>customFields</code>	Объект с информацией о дополнительных полях в журнале учета СКЗИ: <code>id</code> – идентификатор атрибута, который подставляется в шаблоны печати нормативных документов <code>value</code> – имя поля, которое отображается в журнале СКЗИ Дополнительные поля задаются в Мастере настройки Indeed СМ в разделе Журнал учета СКЗИ
<code>state</code>	Состояние СКЗИ: <code>Created</code> – изготовлено <code>Assigned</code> – назначено <code>Sent</code> – передано <code>Returned</code> – возвращено <code>Issued</code> – выдано <code>Installed</code> – установлено <code>Destructed/Withdrawn</code> – 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
<code>id</code>	Идентификатор СКЗИ
<code>userName</code>	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
<code>id</code>		Идентификатор СКЗИ

Объект	Параметр	Описание
sendingData информация о передаче СКЗИ	recipient	ФИО сотрудника, который подтверждает получение СКЗИ
	timeSent	Время отправления документа. Указывается в формате ууууММддННммсс (UTC). Если значение не указано, то подставляется текущее время
	timeConfirmed	Время подтверждения получения. Указывается в формате ууууММддННммсс (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

Объект	Параметр	Описание
	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 ууууММддННммсс (UTC). Если значение не указано, то подставляется текущее время
	timeConfirmed	Время подтверждения получения СКЗИ. Указывается в формате ууууММддННммсс (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

Объект	Параметр	Описание
	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 ууууММддННммсс (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 ууууММддННммсс (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
<code>id</code>	Обязательно	Идентификатор СКЗИ
<code>reuse</code>	Необязательно	Укажите значение: <code>true</code> , чтобы изъять СКЗИ у пользователя и использовать повторно – например, для другого пользователя <code>false</code> , чтобы уничтожить СКЗИ Значение по умолчанию – <code>false</code>
<code>destructor</code>	Необязательно	ФИО сотрудников органа криптографической защиты, пользователей СКЗИ, производивших уничтожение/изъятие СКЗИ. Имена указываются в формате Common Name через запятую
<code>timeDestroyed</code>	Необязательно	Время уничтожения/изъятия. Указывается в формате ууууMMddHHmmss (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



Работа с устройствами JaCarta с ГОСТ-областью

Особенности использования



Indeed CM Card Template Designer

Утилита для создания шаблонов печати



Массовый выпуск смарт-карт

Режим массового выпуска

Работа с устройствами JaCarta с ГОСТ-областью

При использовании устройств **JaCarta с PKI/ГОСТ-областями** и **JaCarta-2 с PKI/ГОСТ1/ГОСТ2-областями** следует учитывать следующее:

JaCarta PKI/ГОСТ

- PIN-код администратора области ГОСТ по умолчанию меняется на случайный после добавления устройства в Indeed Certificate Manager. При удалении устройства из Indeed CM с подключением устройства к рабочей станции случайный PIN-код администратора области ГОСТ меняется на значение, указанное в разделе **Конфигурация** → **Типы устройств**.
- PIN-код пользователя для области ГОСТ можно установить и изменить только при инициализации устройства после выпуска устройства.
- При изъятии у пользователя устройства с подключением к рабочей станции нужно ввести PIN-код пользователя для области ГОСТ. Если PIN-код пользователя для области ГОСТ неизвестен, то такое устройство изымается у пользователя без подключения к рабочей станции. Чтобы выпустить такое устройство повторно, устройство нужно инициализировать, и будет задан новый PIN-код пользователя для области ГОСТ, известный пользователю и/или оператору.
- При разблокировке области ГОСТ PIN-код пользователя не меняется. На счетчике попыток ввода PIN-кода до блокировки устройства устанавливается 10 попыток.

Для PIN-кода пользователя области ГОСТ в политиках Indeed CM не поддерживаются следующие опции:

- Парольная политика в разделе **Выпуск** → **Инициализация устройства**.
- Опция **Пользователь должен поменять PIN-код при первом входе** в разделе **Выпуск**.

Для PIN-кода пользователя области ГОСТ в политиках Indeed CM поддерживаются следующие опции:

- Опция **Установить случайный PIN-код пользователя** в разделе **Выпуск**. При этом случайный PIN-код будет одинаковым для областей PKI и ГОСТ.
- Опция **Блокировать устройство** в разделе **Выпуск**.
- Установка PIN-кода в параметрах инициализации устройства.

- Управление PIN-кодами пользователей областей ГОСТ1 и ГОСТ2 в Indeed CM происходит синхронно, т.е. смена PIN-кода ГОСТ1 повлечет за собой смену и PIN-кода ГОСТ2 и наоборот. Аналогично и для прочих операций (сброс, разблокировка).
- PIN-коды пользователя для обоих ГОСТ-областей можно установить или изменить только при инициализации устройства (при выпуске смарт-карты с включенной опцией **Инициализировать устройство**), при этом содержимое устройства для ГОСТ2-области не будет очищено. Новое значение PIN-кода необходимо указать в параметрах инициализации для устройств JaCarta-2.
- Для добавления устройства в Indeed CM PIN-код администратора ГОСТ1 должен совпадать с PUK-кодом области ГОСТ2. Таким образом, изменить PIN-код администратора ГОСТ1 при выпуске устройства нельзя, т.е. все устройства JaCarta-2 после добавления в Indeed CM будут иметь PIN-код администратора, заданный производителем (**1234567890**).

Чтобы сменить PIN-код администратора ГОСТ1:

- Измените PUK-код через АРМ-администратора JaCarta (предоставляется разработчиком устройств JaCarta)
- Измените PIN-код администратора ГОСТ1 через АРМ или Единый клиент.

Для работы в Indeed CM с новым PIN-кодом администратора ГОСТ1 необходимо:

- Прописать новые значения в типе устройства JaCarta.
- **Выпустить устройство** с включенными опциями **Добавлять устройства автоматически** и **Инициализировать устройство** через Indeed CM.
- Для PKI-области инициализация проходит с очисткой содержимого и изменением PIN-кодов администратора и пользователя согласно заданным политикам инициализации в Indeed CM.

Indeed CM Card Template Designer

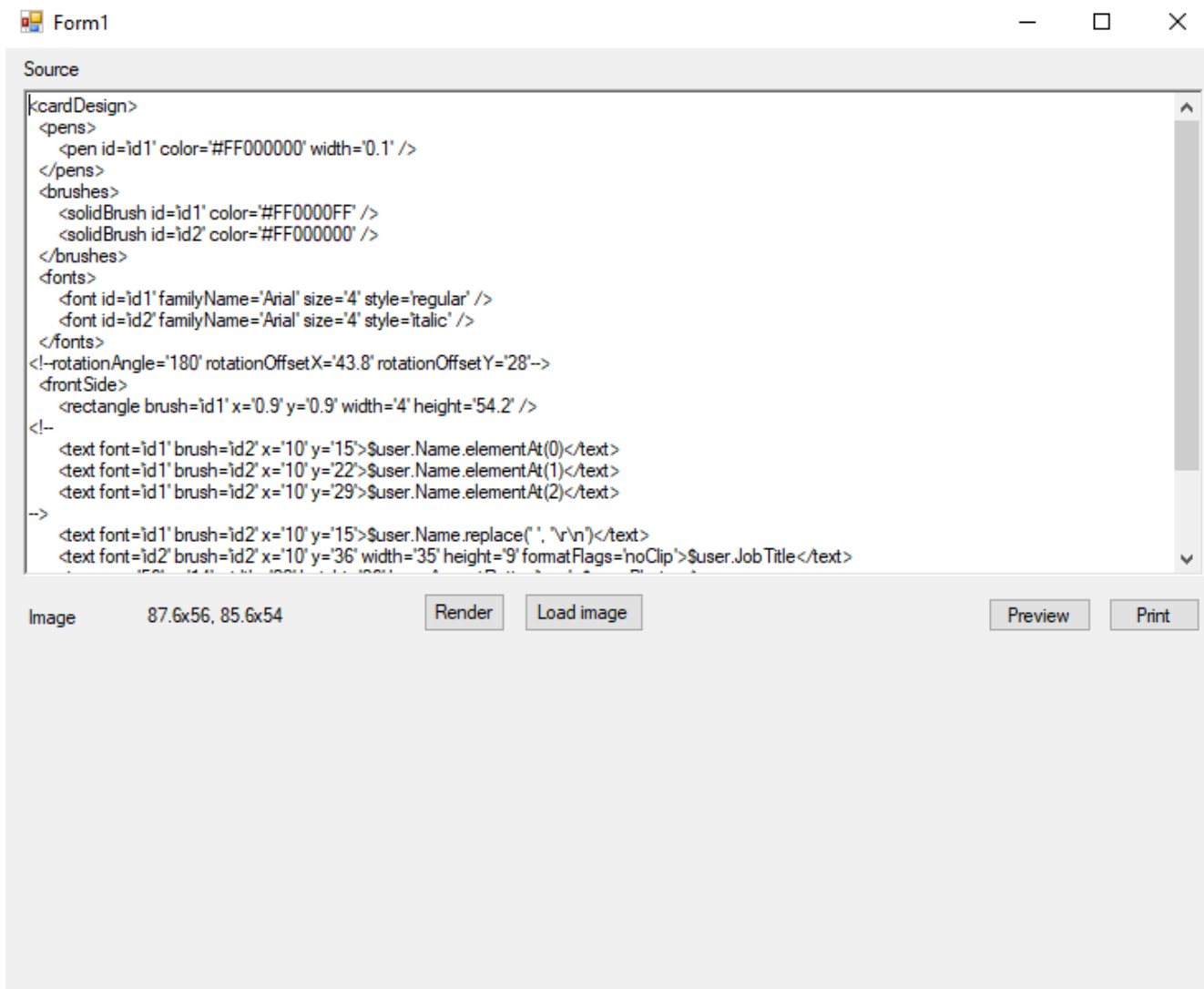
Утилита Indeed CM Card Template Designer позволяет создавать шаблоны печати на смарт-картах, которые используются с принтером **EDIsure XID 8100\8300**.

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

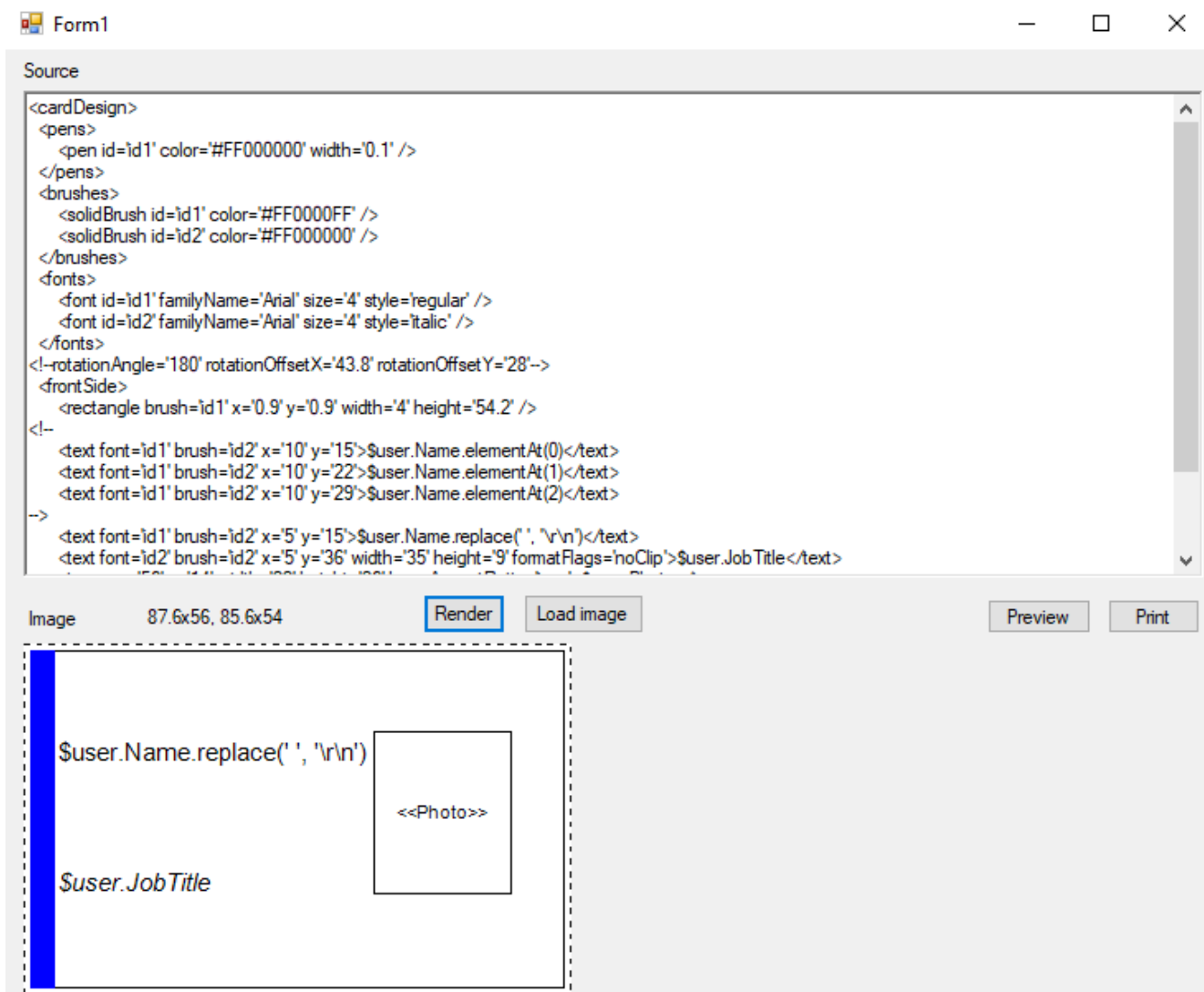
Утилиту Card Template Designer предоставляет по запросу **служба технической поддержки компании Индид**.

Запустите приложение *cardTemplateDesigner.exe* из дистрибутива. 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 `<font>` с параметрами `font id`, `familyName`, `size`, `style`

❗ ПРИМЕР

```
<font>
<font id='id1' familyName='Arial' size='3' style='regular' />
<font id='id2' familyName='Arial' size='4' style='italic' />
</font>
```

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`
 - `width` (опциональный)
 - `height` (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
 - width (опциональный)

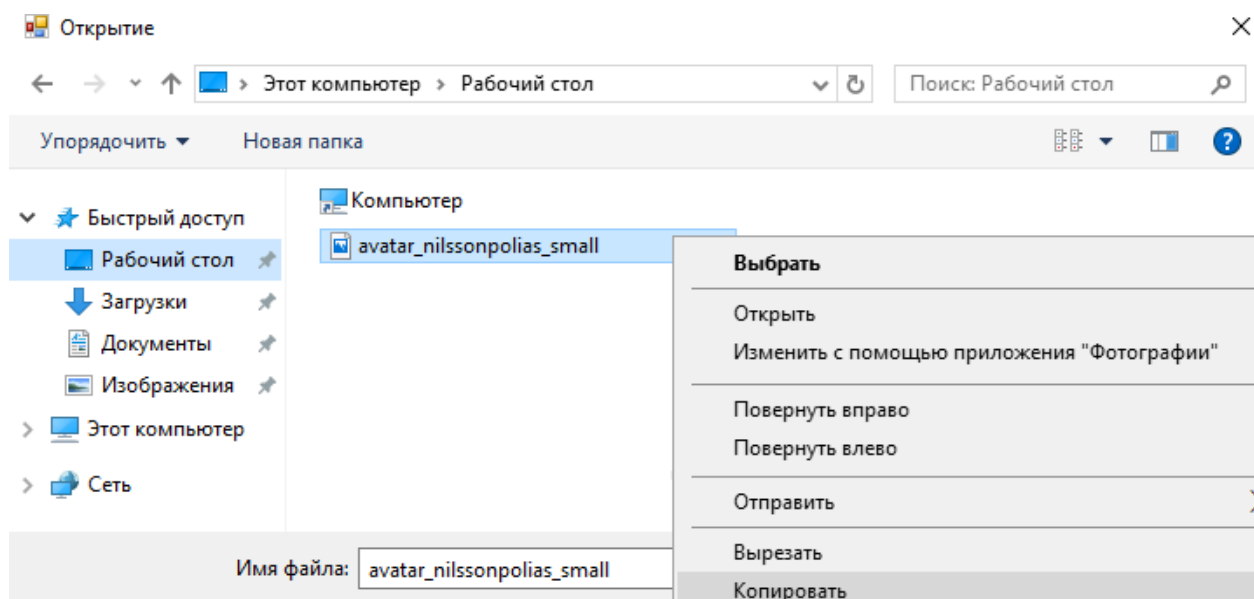
- height (опциональный)
- keepAspectRatio (true или false)
- data (опциональный)

❗ ПРИМЕР

```
<image x='56' y='14' width='22' height='26'
keepAspectRatio='true'>$user.Photo</image>
```

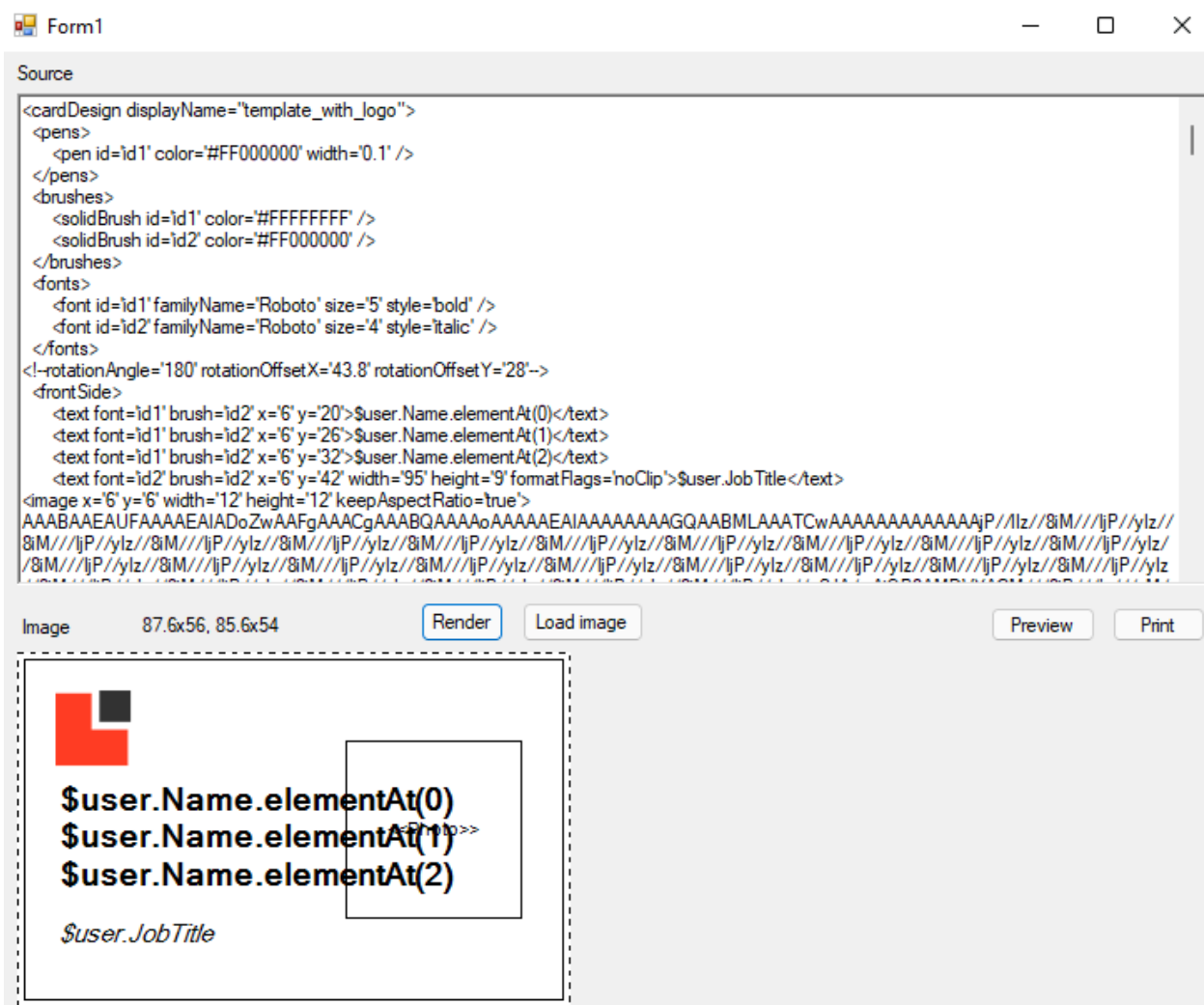
Описанная строка определяет положение, размер и следование пропорциям изображения, подставляемого из атрибута Active Directory (переменная `$user.Photo`). Помимо переменной можно подставить и изображение в кодировке base64 (например, для добавления в шаблон логотипа компании) и затем визуализировать его выполнив следующие действия:

1. Нажмите **Load image** и перейдите в окно выбора изображения в формате JPEG. Размер изображения подбирается исходя из желаемого дизайна шаблона и размеров смарт-карты.
2. 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.

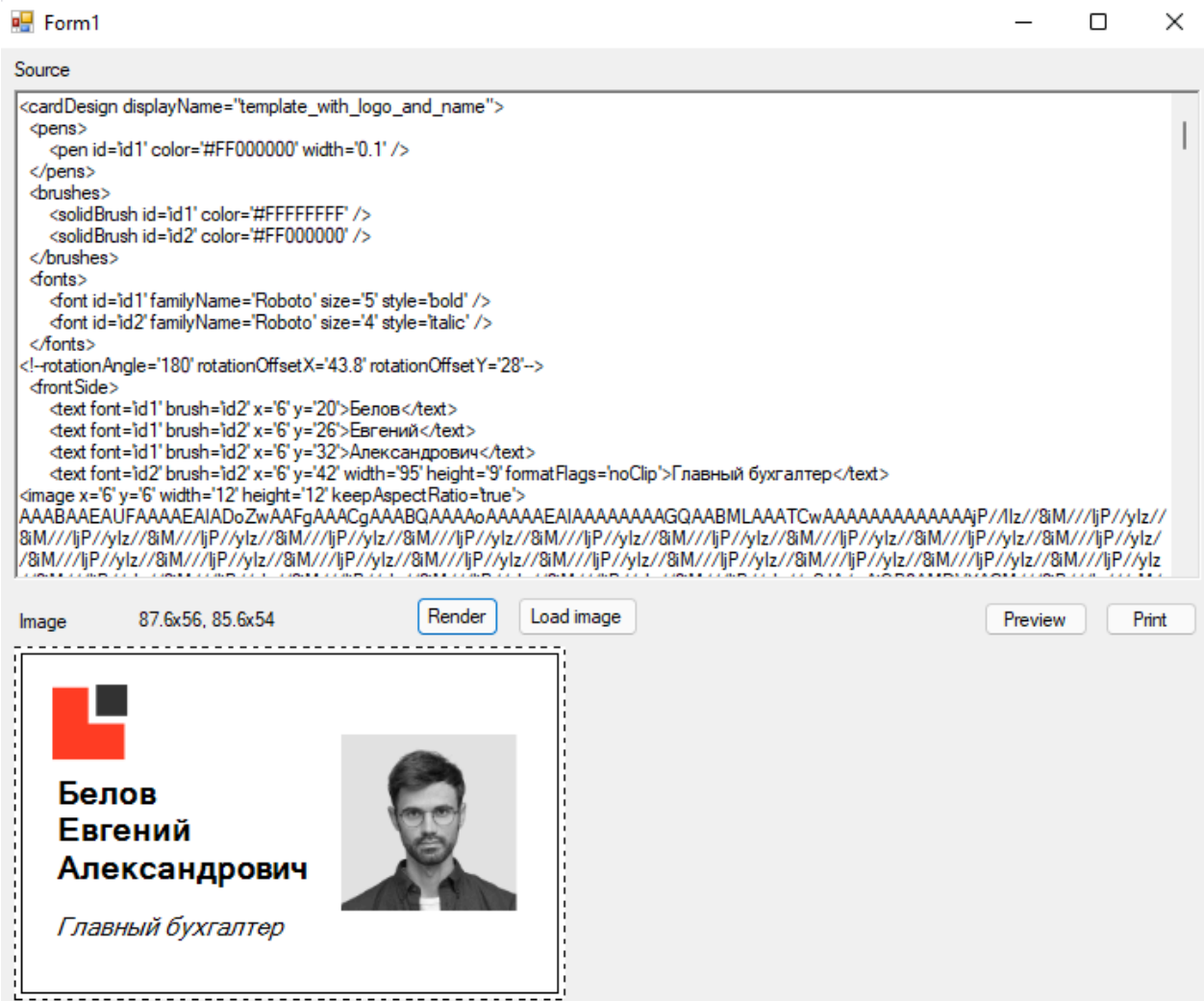


Ниже на рисунке приведен пример шаблона со статическим логотипом компании и подстановкой данных пользователя из Active Directory:

- 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`.

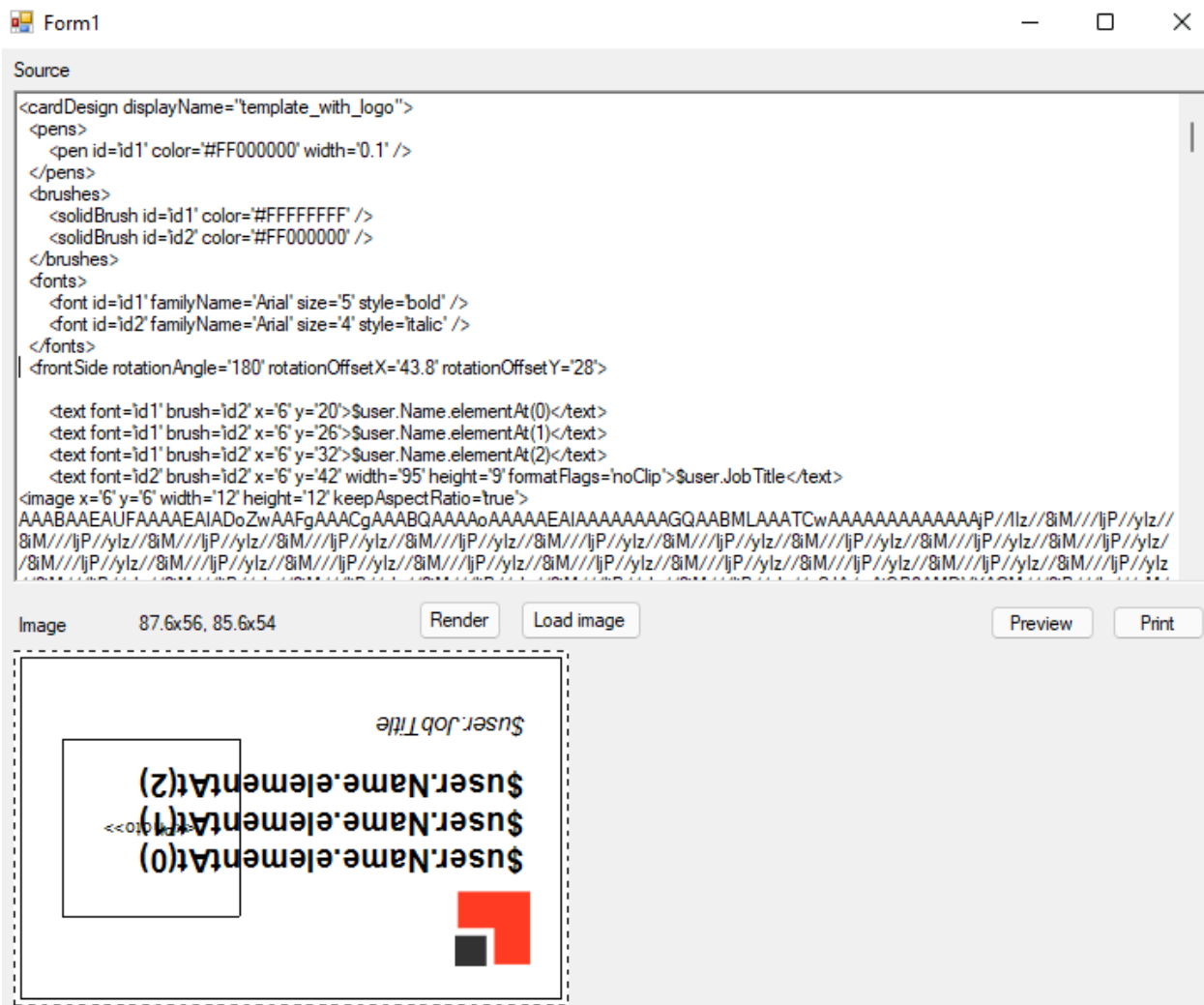
❗ ПРИМЕР:

```
<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		#FFFFFFE0		#B0E0E6	
#F5F5DC		#696969		#00FF00		#800080	
#FFE4C4		#1E90FF		#32CD32		#FF0000	
#000000		#B22222		#FAF0E6		#BC8F8F	
#FFEBCD		#FFFAF0		#FF00FF		#4169E1	
#0000FF		#228B22		#800000		#8B4513	
#8A2BE2		#FF00FF		#66CDAA		#FA8072	
#A52A2A		#DCDCDC		#0000CD		#F4A460	
#DEB887		#F8F8FF		#BA55D3		#2E8B57	
#5F9EA0		#FFD700		#9370DB		#FFF5EE	
#7FFF00		#DAA520		#3CB371		#A0522D	
#D2691E		#808080		#7B68EE		#C0C0C0	
#FF7F50		#008000		#00FA9A		#87CEEB	
#6495ED		#ADFF2F		#48D1CC		#6A5ACD	
#FFF8DC		#F0FFF0		#C71585		#708090	
#DC143C		#FF69B4		#191970		#FFFAFA	
#00FFFF		#CD5C5C		#F5FFFA		#00FF7F	
#00008B		#4B0082		#FFE4E1		#4682B4	
#008B8B		#FFFFFF0		#FFE4B5		#D2B48C	
#B8860B		#F0E68C		#FFDEAD		#008080	
#A9A9A9		#E6E6FA		#000080		#D8BFD8	
#006400		#FFF0F5		#FDF5E6		#FF6347	
#BDB76B		#7CFC00		#808000		#40E0D0	
#8B008B		#FFFACD		#6B8E23		#EE82EE	
#556B2F		#ADD8E6		#FFA500		#F5DEB3	
#FF8C00		#F08080		#FF4500		#FFFFFF	
#9932CC		#E0FFFF		#DA70D6		#F5F5F5	
#8B0000		#FAFAD2		#EEE8AA		#FFFF00	
#E9967A		#90EE90		#98FB98		#9ACD32	
#8FBC8F		#D3D3D3		#AFEEEE		#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 .



Массовый выпуск смарт-карт

При использовании Indeed Certificate Manager с принтером смарт-карт (опция **Включить поддержку принтера смарт-карт** в политике использования устройств) существует возможность массового выпуска карт пользователям.

В этом случае оператор определяет группу пользователей, которым необходимо выпустить карты, помещает нужное количество карт в лоток принтера и запускает процесс массового выпуска.

Режим массового выпуска имеет следующие особенности и ограничения:

- Отсутствует возможность выбора необязательных сертификатов. Будут выпущены только обязательные. Необязательные сертификаты можно выпустить для каждого пользователя отдельно через карточку пользователя или Сервис самообслуживания.
- Отсутствует возможность указания имя карты. Имя будет пустым или сформированным по правилам, обозначенным в политике использования устройств.
- Отсутствует возможность создать автоматически документ учета СКЗИ. В случае необходимости, такой документ следует указать вручную в карточке пользователя.
- При возникновении любой ошибки массовый выпуск останавливается. Для дальнейшей работы следует устранить ошибку или исключить проблемного пользователя из списка и запустить массовый выпуск заново.
- При нажатии кнопки **Отмена** во время массового выпуска загруженная в принтер карта будет выпущена, выпуск следующей карты не будет начат.
- Массовый выпуск может осуществляться как с печатью данных на карте так и без.



ПРЕДУПРЕЖДЕНИЕ

Для печати на устройствах на рабочей станции должны быть установлены следующие компоненты:

- Драйвера принтера EDISecure XID8300
- Настроенное соединение с принтером в утилите EDI Secure Connect
- Компонент поддержки принтера *IndeedCM.EdiSecure.Middleware*
- Подключенный через интерфейс USB принтера XID8300

Драйвера принтера EDISecure XID8300 и утилита EDI Secure Connect поставляются производителем вместе с принтером. *IndeedCM.EdiSecure.Middleware* поставляется в составе дистрибутива Indeed CM.

Для массового выпуска устройств выполните следующие действия:

1. Перейдите на страницу сервиса <https://<FQDN сервера Indeed CM>/cm/mc/bulkissue>
2. Выполните поиск пользователей (например, по месту расположения). Результат поиска отобразится в таблице слева.
3. Отметьте среди найденных пользователей всех, кому необходимо выпустить смарт-карты и нажмите  .
4. Нажмите **Выпустить**. Имя будет подставлено автоматически.
5. Нажмите **Выпустить**.

Массовый выпуск

Корневой контейнер

Общее имя(CN)

Контейнер

Имя

Фамилия

Отображать заблокированные учетные записи

	Общее имя(CN)	Имя и фамилия	Контейнер
☒	Алексей Дмитриев	Алексей Дмитриев	cmad.indeed/MSK Office (Обособленное подразделение)
☒	Евгений Белов	Евгений Белов	cmad.indeed/MSK Office (Обособленное подразделение)
☐	Кирилл Руссов	Кирилл Руссов	cmad.indeed/MSK Office (Обособленное подразделение)

	Общее имя(CN)	Имя и фамилия	Контейнер
☐	Алексей Дмитриев	Алексей Дмитриев	cmad.indeed/MSK Office (Обособленное подразделение)
☐	Евгений Белов	Евгений Белов	cmad.indeed/MSK Office (Обособленное подразделение)

Принтер

XID 8300 (DS)

Выпустить

Отмена

Прогресс выпуска карты для каждого пользователя отображается в нижней части экрана. Выпуск карты можно приостановить или отменить.

Пользователь: Евгений Белов

Загрузка карты

Пауза

Отмена

Если при массовом выпуске возникла ошибка, пользователь, на котором произошла ошибка, выделяется красным, а в нижней части экрана отображается текст ошибки.

Массовый выпуск

Корневой контейнер

Общее имя(CN)

Контейнер

Имя

Фамилия

Отображать заблокированные учетные записи

cmad.indeed

Общее имя(CN)

msk

Имя

Фамилия

🔍

☐	Общее имя(CN)	Имя и фамилия	Контейнер
☒	Алексей Дмитриев	Алексей Дмитриев	cmad.indeed/MSK Office (Обособленное подразделение)
☒	Евгений Белов	Евгений Белов	cmad.indeed/MSK Office (Обособленное подразделение)
☐	Кирилл Руссов	Кирилл Руссов	cmad.indeed/MSK Office (Обособленное подразделение)

☐	Общее имя(CN)	Имя и фамилия	Контейнер
☐	Алексей Дмитриев	Алексей Дмитриев	cmad.indeed/MSK Office (Обособленное подразделение)
☐	Евгений Белов	Евгений Белов	cmad.indeed/MSK Office (Обособленное подразделение)

➕ Выпустить

Пользователь: Евгений Белов

Смарт-карта не отвечает на сигнал сброса состояния.

Повторить

Пропустить

Отмена

После устранения ошибки выпуск можно повторить. Для игнорирования ошибки и продолжения массового выпуска карт нажмите **Пропустить**. Для отмены массового выпуска для всех пользователей нажмите **Отмена**.

Перенос данных из сторонних систем



Aladdin JMS

Миграция данных из Aladdin JaCarta Management System в Indeed CM



SafeNet Authentication Manager

Миграция данных из SafeNet Authentication Manager в Indeed CM

Aladdin JMS

Миграция данных не затрагивает базу данных JMS — состояние и содержимое устройств остаются неизменными. После переноса в Indeed CM для всех перенесенных устройств и сертификатов доступны все возможные операции: выпуск, обновление содержимого, отзыв и другие.

Утилита миграции переносит в Indeed CM следующие данные устройств:

- Модель
- Форм-фактор
- Состояние
- Метка
- PIN-код администратора
- Ключевая информация для JMS-коннектора MS PKI (9C66741E-E5B1-40E3-B047-9A2D598CA913):
 - Выпущенные на УЦ
 - Отслеживаемые (выпущены на стороннем УЦ)
- Связь с пользователем



ПРЕДУПРЕЖДЕНИЕ

Для JaCarta PKI/ГОСТ информация о приложении ГОСТ-апплете не импортируется. В Indeed CM возможны операции только с PKI-областью устройства.

В Indeed CM не переносятся следующие данные:

- Метки АМДЗ Аккорд
- Сертификаты Валидата УЦ
- Сертификаты КриптоПро УЦ

Если такие данные есть на устройстве, то они не отображаются в Indeed CM после переноса, но остаются на устройстве.

Предварительные настройки

Миграция данных возможна при соблюдении условий:

- У сервера JMS, на котором выполняется запуск утилиты миграции, есть сетевой доступ к серверу с базой данных Indeed CM.
- Каталог пользователей Indeed CM совпадает с каталогом пользователей JMS. Путь к каталогу пользователей задается в разделе **Каталог пользователей** Мастера настройки Indeed CM.
- В разделе **Конфигурация** → **Типы устройств** Indeed CM добавлены все типы устройств JaCarta, которые используются в JMS.
- В Indeed CM есть свободные лицензии: в разделе **Конфигурация** → **Лицензии** есть действующая лицензия на достаточное количество пользователей.
- На всех пользователей, устройства которых будут переноситься из JMS, должны быть **назначены политики использования устройств в Indeed CM**.
- В политиках Indeed CM настроены те же УЦ и те же шаблоны сертификатов, что и в JMS.

Создание политики использования устройств

Indeed Certificate Manager использует механизм политик выпуска устройств пользователям. Каждая политика содержит в себе параметры работы с устройством: перечень УЦ и шаблонов сертификатов, требования к установке PIN-кодов, перечень действий с устройством доступных пользователю и другие.

Каждая политика имеет область действия. Для каталога пользователей Indeed CM в Active Directory областью действия может быть:

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

Для всех пользователей в пределах области действия политики будут выпускаться устройства с параметрами, определенными в этой политике. Политика может распространяться как на весь объект целиком (домен, контейнер или подразделение), так и на отдельные группы пользователей внутри него. Если пользователь попадает под действие нескольких политик выпуска устройств (например, состоит в двух группах в одном подразделении), применяется политика с наивысшим приоритетом.

Перед миграцией данных из JMS заранее создайте одну или несколько **политик использования устройств в Indeed CM**. Настройте в политике те же самые УЦ и шаблоны, которые использовались для выпуска сертификатов в JMS.

В результате миграции данных из JMS все пользователи, обладающие токенами и сертификатами, попадут под действие ранее созданных политик Indeed CM.

Процесс миграции

1. Настройте файл конфигурации утилиты миграции.
2. Запустите утилиту миграции.

Настройка файла конфигурации утилиты миграции

Для работы утилиты заполните файл конфигурации *IndeedCM.Migrate.JMS.exe.config*, находящийся в каталоге с утилитой.

1. Заполните параметры в секции `<migrateJMSSettings>`:
 - `operatorTokenPin` — PIN-код администратора устройства, на котором записан сертификат оператора JMS. Необходим для монтирования криптохранилища JMS.
 - `notIssuedTokenAdminPin` — если ключевой носитель в JMS находится в состоянии *Зарегистрирован* и ни разу не выпускался, то в этом параметре задается PIN-код администратора, который установится на устройстве после его переноса в Indeed CM.
 - `issuedTokenAdminPin` — если ключевой носитель в JMS находится в любом другом состоянии и выпускался без инициализации, то в параметре задается PIN-код администратора, который установится на устройстве после его переноса в Indeed CM.
2. В секции `<sqlPersistenceSettings>` заполните параметры подключения к базе данных Indeed CM. Всю секцию можно перенести из файла конфигурации *Web.config* веб-приложения mc (Консоль управления).
3. В секции `<adUserCatalogSettings>` заполните параметры подключения к каталогу пользователей. Всю секцию можно перенести из файла конфигурации *Web.config* веб-приложения mc (Консоль управления).



ПРЕДУПРЕЖДЕНИЕ

Секции `sqlPersistenceSettings` и `adUserCatalogSettings` должны быть в расшифрованном виде. Для расшифровки секций используйте файл `decryptConfigsSQL_AKEAgent.bat` из дистрибутива сервера Indeed CM, каталог `..\Misc\EncryptConfigs`. Запустите файл на сервере Indeed CM в командной строке, запущенной от имени администратора, и дождитесь завершения расшифровки. Для шифрования используйте файл `encryptConfigsSQL_AKEAgent.bat`.

Работа с утилитой миграции

Запустите утилиту `IndeedCM.Migrate.JMS.exe` на сервере JMS в командной строке, запущенной от имени администратора.

Для работы с резервной копией базы данных JMS необходимо прописать в реестре сервера JMS путь к копии рабочей базы данных.

По умолчанию строка подключения к базе хранится в значении параметра `ConnectionString` в разделе `[HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\Enterprise Application Platform Server\JaCarta Management System\default\DatabaseManager]`.

SafeNet Authentication Manager

Предварительные настройки

Для миграции данных из SafeNet Authentication Manager в Indeed CM убедитесь, что выполнены следующие предварительные условия:

Со стороны SAM:

- Версия SafeNet Authentication Manager 8.0, 8.2 Rev E и 9.0 SP2/SP3
- Хранилище данных SAM в Active Directory
- Редакция удостоверяющего центра Microsoft, сертификаты которого будут перенесены
- Известны все типы устройств (USB-токенов, смарт-карт) и значения их ATR (Answer To Reset), которые используются в SAM и будут использоваться в Indeed CM

Со стороны Indeed Certificate Manager:

- Версия Indeed CM Server 4.1.3 и выше
- Хранилище данных в Active Directory или Microsoft SQL

Процесс миграции

1. Настройте Indeed CM для работы с данными из SAM.
2. Создайте политики использования устройств.
3. Настройте утилиту миграции `IndeedCM.Migrate.SAM`:
 1. Заполните файл конфигурации `IndeedCM.Migrate.SAM.exe.config`.
 2. Заполните файл конфигурации `unity.config`.
 3. Запустите процесс миграции.

Настройка Indeed CM для работы с данными из SAM

Прежде чем приступить к выгрузке данных из SAM, подготовьте Indeed CM к приему данных. Убедитесь, что выполнены следующие условия:

1. Каталог пользователей Indeed CM совпадает с каталогом пользователей SAM. Путь к каталогу задается в Мастере настройки в разделе **Каталог пользователей**.

2. В разделе **Конфигурация** → **Лицензии** есть действующая лицензия на достаточное количество пользователей.
3. В разделе **Конфигурация** → **Типы устройств** добавлены все типы устройств eToken, которые используются в SAM.
4. Для всех пользователей, устройства которых будут переноситься из SAM, созданы и назначены политики использования устройств в Indeed CM.

Создание политики использования устройств

Indeed Certificate Manager использует механизм политик выпуска устройств пользователям. Каждая политика содержит в себе параметры работы с устройством: перечень УЦ и шаблонов сертификатов, требования к установке PIN-кодов, перечень действий с устройством доступных пользователю и другие.

Каждая политика имеет область действия. Для каталога пользователей Indeed CM в Active Directory областью действия может быть:

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

Для всех пользователей в пределах области действия политики будут выпускаться устройства с параметрами, определенными в этой политике. Политика может распространяться как на весь объект целиком (домен, контейнер или подразделение), так и на отдельные группы пользователей внутри него. Если пользователь попадает под действие нескольких политик выпуска устройств (например, состоит в двух группах в одном подразделении), применяется политика с наивысшим приоритетом.

Перед миграцией данных из SAM заранее создайте одну или несколько **политик использования устройств в Indeed CM**. Настройте в политике те же самые УЦ и шаблоны, которые использовались для выпуска сертификатов в SAM.

В результате миграции данных из SAM все пользователи, обладающие токенами и сертификатами, попадут под действие ранее созданных политик Indeed CM.

Утилита миграции

Данные из SAM переносятся с помощью утилиты *IndeedCM.Migrate.SAM.exe*, расположенной в дистрибутиве сервера Indeed Certificate Manager (каталог *Misc\SAMMigration*). Для работы

утилиты заполните файлы конфигурации *IndeedCM.Migrate.SAM.exe.config* и *IndeedCM.Migrate.SAM.unity.config*.

IndeedCM.Migrate.SAM.exe.config

Откройте файл *SAMMigration\IndeedCM.Migrate.SAM.exe.config* от имени администратора в текстовом редакторе и заполните следующие секции:

- **samSettings** – параметры подключения к хранилищу данных SAM.
- **MsCAConnectorId** – идентификатор коннектора к Microsoft CA. Значение параметра можно найти в файле XML коннектора в каталоге SAM.
Путь по умолчанию:
C:\ProgramFiles\SafeNet\Authentication\SAM\x64\Bin\MsCAConnectorDescriptor.xml.
Значение по умолчанию: {1A30B883-CD69-4cbb-8D61-E72E9697D8B1}.
- **connectionString** - путь к файлу XML (в названии файла имя домена, в котором развернут SAM) с информацией для подключения к SAM серверу.
Путь по умолчанию *C:\ProgramData\SafeNet\Authentication\SAM*.
- **migrateSAMSettings** – параметры переноса данных.
- **ignoreCMCertificateTemplateNotFound** – параметр импорта устройств.
Процесс импорта карт не останавливается. Может иметь два значения:
 - **true** – из SAM импортируется устройство вместе с сертификатами, для которых в политике Indeed CM создан шаблон.
 - **false** – из SAM не импортируется устройство, если в политике Indeed CM нет хотя бы одного шаблона для сертификата, выпущенного в SAM. Значение по умолчанию.
- **notIssuedTokenAdminPin** – если ключевой носитель в SAM находится в состоянии *Зарегистрирован* и ни разу не выпускался, то в этом параметре задается PIN-код администратора, который будет установлен на устройстве после его переноса в Indeed CM.
- **issuedTokenAdminPin** – если ключевой носитель в SAM находится любом другом состоянии и выпускался без инициализации, то в параметре задается PIN-код администратора, который будет установлен на устройстве после его переноса в Indeed CM.
- **tokenTypes** – секция, в которой должны быть перечислены все устройства, которые необходимо перенести из SAM в Indeed CM. Необходимо указать модель устройства

(токена, смарт-карты), product name, цвет устройства и значение ATR (Answer To Reset).

 ПРЕДУПРЕЖДЕНИЕ

Значение ATR для каждого устройства можно получить у производителя или при помощи стороннего ПО, обратившись в службу технической поддержки компании Индид.

Если при работе утилиты *IndeedCM.Migrate.SAM.exe* с хранилищем SAM встречается устройство с моделью и product name, которые не указаны в секции **tokenTypes**, то такие устройства не переносятся в хранилище Indeed CM, а утилита выводит соответствующую ошибку.

- **adPersistenceSettings** – параметры подключения к хранилищу данных Indeed CM в Active Directory. Содержимое секции должно полностью совпадать с содержимым одноименной секции файла конфигурации Консоли управления Indeed CM (*mc\Web.config*).
- **sqlPersistenceSettings** – параметры подключения к хранилищу данных Indeed CM в Microsoft SQL. По умолчанию секция закомментирована символами `<!--`. Содержимое секции должно полностью совпадать с содержимым одноименной секции файла конфигурации Консоли управления Indeed CM (*mc\Web.config*).
- **adUserCatalogSettings** – параметры подключения к каталогу пользователей Indeed CM в Active Directory. Содержимое секции должно полностью совпадать с содержимым одноименной секции файла конфигурации Консоли управления Indeed CM (*mc\Web.config*).

Сохраните изменения.

▼ Пример файла IndeedCM.Migrate.SAM.exe.config

```
<samSettings MsCAConnectorId="{1A30B883-CD69-4cbb-8D61-E72E9697D8B1}"
connectionString="C:\ProgramData\SafeNet\Authentication\SAM\demo.local
/>
<migrateSAMSettings ignoreCMCertificateTemplateNotFoundError="true"
notIssuedTokenAdminPin="adminpass"
issuedTokenAdminPin="adminpass2">
<tokenTypes>
<tokenType model="Token 12.0.0.0 12.0.12"
productName="SafeNet eToken 5110"
color="8"
atr="3bd5180081313a7d8073c8211030" />
<tokenType model="Token JC"
productName="eToken PRO Java 72K OS755"
color="4"
atr="3bd518008131fe7d8073c82110f4" />
</migrateSAMSettings>
<adPersistenceSettings path="LDAP://CN=Indeed CM,CN=Indeed Identity,
DC=demo,DC=local" userName="DEMO\cmadmin" password="Password1"
cryptoAlgName="AES"
cryptoKey="11d2f5051684451860ad177ebc39b55cacaf2a0a843b05ddf273b955c93
/>
<adUserCatalogSettings>
<rootContainers>
<container path="LDAP://OU=SAM_USERS,DC=demo,DC=local"
userName="DEMO\cmadmin"
password="Password1" />
</rootContainers>
</adUserCatalogSettings>
```

IndeedCM.Migrate.SAM.unity.config

Откройте файл *SAMMigration\unity.config* от имени администратора в текстовом редакторе и заполните секцию **container**:

- Все строки до `<register type="ISAMDbContext". . . />` должны совпадать с теми, что указаны в файле конфигурации Консоли управления Indeed CM (*mc\unity.config*).



ПРЕДУПРЕЖДЕНИЕ

Добавлять секции, которых по умолчанию нет в *unity.config* утилиты миграции (но есть в *mc\unity.config*) не нужно.

- `<register type="IMigrateReporter"`
`mapTo="IndeedCM.Migrate.SAM.Reporter.CSVMigrateReporter,`
`IndeedCM.Migrate.SAM/>"` – определяет режим вывода отчета по работе утилиты миграции. Если секция не закомментирована символами `<! - - . . . - ->`, то отчет будет записываться в файл CSV, созданный в папке расположения утилиты с именем *IndeedCM.Migrate.SAM.Report_dd-MM-yyyy_HH-mm-ss.csv*. По умолчанию отчет не создается.
- `<register type="IMigrateReporter"`
`mapTo="IndeedCM.Migrate.SAM.Reporter.NullMigrateReporter,`
`IndeedCM.Migrate.SAM"/>` – отключает создание отчета о работе утилиты миграции данных. По умолчанию секция закомментирована символами `*<! - - . . . - ->`.



ПРЕДУПРЕЖДЕНИЕ

Использование двух активных секций с параметрами *IndeedCM.Migrate.SAM.Reporter.CSVMigrateReporter*, *IndeedCM.Migrate.SAM* и *IndeedCM.Migrate.SAM.Reporter.NullMigrateReporter*, *IndeedCM.Migrate.SAM* не допускается. Одна из них обязательно должна быть закомментирована или удалена.

Сохраните изменения.

▼ Пример заполненной секции файла unity.config

```
<container>
  <register type="ICardRepository"
mapTo="IndeedCM.Persistence.AD.CardRepository,
IndeedCM.Persistence.AD" />
  <register type="IUserDataRepository"
mapTo="IndeedCM.Persistence.AD.UserDataRepository,
IndeedCM.Persistence.AD" />
  <register type="IPolicyRepository"
mapTo="IndeedCM.Persistence.AD.PolicyRepository,
IndeedCM.Persistence.AD" />
  <register type="ICardTypeRepository"
mapTo="IndeedCM.Persistence.AD.CardTypeRepository,
IndeedCM.Persistence.AD" />
  <register type="ILicenseRepository"
mapTo="IndeedCM.Persistence.AD.LicenseRepository,
IndeedCM.Persistence.AD" />
  <register type="ISkziRepository"
mapTo="IndeedCM.Persistence.AD.SkziRepository,
IndeedCM.Persistence.AD" />
  <register type="IUserCatalog"
mapTo="IndeedCM.UserCatalog.AD.UserCatalog, IndeedCM.UserCatalog.AD"
/>
  <register type="ISAMDbContext"
mapTo="IndeedCM.Migrate.SAM_8_0.Core.SAMDbContext,
IndeedCM.Migrate.SAM_8_0" />
  <register type="ISAMHelpers"
mapTo="IndeedCM.Migrate.SAM_8_0.Utils.SAMHelpers,
IndeedCM.Migrate.SAM_8_0" />
  <register type="IMigrateReporter"
mapTo="IndeedCM.Migrate.SAM.Reporter.CSVMigrateReporter,
IndeedCM.Migrate.SAM" />
</container>
```

Работа с утилитой IndeedCM.Migrate.SAM

Чтобы запустить процесс миграции данных:

1. Войдите на сервер SAM под сервисной учетной записью SAM (Service Account).
2. Запустите утилиту в тестовом режиме в командной строке Windows от имени администратора.

```
IndeedCM.Migrate.SAM.exe /test
```

Тестовый запуск утилиты требуется для генерации отчета об устройствах и сертификатах, которые будут перенесены в ходе миграции, а также для вывода информации по ошибкам. В этом режиме работы утилиты данные не переносятся с репозитория, и не заносятся события в журнал.

3. Если в тестовом режиме не было критических ошибок, продолжите миграцию. Запустите утилиту *IndeedCM.Migrate.SAM.exe* в командной строке Windows от имени администратора.

В ходе работы утилита отображает выполняемые действия с устройствами и выводит сведения об ошибках.

Если в файле конфигурации *IndeedCM.Migrate.SAM.exe.config* включена опция ведения отчета, то в каталоге с утилитой миграции автоматически создается файл отчета

IndeedCM.Migrate.SAM.Report_dd-MM-yyyy_HH-mm-ss.csv.

▼ Пример содержимого файла отчета в Microsoft Excel

	A	B	C	D	E
1	SAMTokenId	TokenSerialNumber	Status	StatusDescription	ExStackTrace
2	{9FB7F1AE-A694-4119-A198-21E761E3DA98}	0036d261	Success	Token has been successfully imported	
3	{5A3B0D47-D97F-4104-A8FE-D718054F2582}	003bc82b	Success	Token has been successfully imported	
4	{48389550-E500-4EB5-9144-1AD2ED9A8CE4}	005edc38	Success	Token has been successfully imported	
5	{22F758F7-3778-4031-A8A9-CB62E0DEB1AE}	01cec45d	Success	Token has been successfully imported	
6	{E60BF1F6-A2B7-4A16-B4BF-8BFD2D834DF6}	024084ab	Success	Token has been successfully imported	
7	{CED8DAED-3863-4457-8FD8-FFB847AB8BE}	2533c7052520	Success	Token has been successfully imported	
8	{89BFCC4A-B3F6-46A9-B786-63D28356C0DF}	2656440a0e2e	Success	Token has been successfully imported	
9	{813A950E-9E05-4225-848B-6F3B25AFB815}	6de79301b42fdfe1	Failed	Failed to import token	System.Exception: ATR for token is not set. (Token model - 'ST02', product name - 'SafeNet eToken Virtual').

Запись событий миграции в журнал

События успешности или ошибки переноса данных можно записать в журнал на сервере Indeed CM. Для записи событий используется компонент Indeed CM EventLog Proxy.

Чтобы настроить запись событий утилиты миграции данных в журнал событий сервера Indeed CM:

1. Откройте файл *SAMMigration\IndeedCM.Migrate.SAM.exe.config* от имени администратора в текстовом редакторе и добавьте элемент `proxyServer` в секцию `eventLogAuditSettings` со следующими атрибутами:

- `url` – путь к сервису eventlogproxy, развернутому на сервере Indeed CM.
- `userName` – имя пользователя, под которым осуществлять подключение к сервису (должно совпадать с именем в секции `authorization` файла *web.config* приложения Indeed CM EventLog Proxy).
- `password` - пароль учетной записи, используемой для подключения к сервису.

Пример заполненной секции

```
<proxyServer url="https://server.demo.local/eventlogproxy"
userName="DEMO\Administrator" password="P@ssw0rd" />
```

2. Сохраните изменения.
3. Установите компонент IndeedCM.EventLog.Proxy на сервер Indeed CM. [Как установить Indeed CM EventLog Proxy.](#)
4. Откройте файл *C:\inetpub\wwwroot\eventlogproxy\Web.config* от имени администратора в текстовом редакторе и укажите в секции `authorization` учетные данные для доступа к сервису eventlogproxy.

Пример заполненной секции

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

5. Сохраните изменения.

Решение проблем



Сбор логов

Как собрать логи компонентов Indeed CM



Контакты

Техническая поддержка и отдел по работе с клиентами

Сбор логов

Серверные компоненты

1. Перейдите в каталог сервиса, логи которого необходимо получить.

▼ Расположение сервисов

Windows

Имя сервиса	Расположение
Служба Монитора устройств (Card Monitor)	<i>%ProgramFiles%\Indeed CM\CardMonitor</i>
Сервис регистрации агентов – веб-приложение agentregistrationapi	<i>%SystemDrive%\inetpub\wwwroot\cm\agent\agentregistrationapi</i>
Сервис агентов – веб-приложение agentserviceapi	<i>%SystemDrive%\inetpub\wwwroot\cm\agent\agentserviceapi</i>
Сервис API – веб-приложение api	<i>%SystemDrive%\inetpub\wwwroot\cm\api</i>
Сервис онлайн-разблокировки и выключения устройств – веб-приложение credprovapi	<i>%SystemDrive%\inetpub\wwwroot\cm\credprovapi</i>
Консоль управления (Management Console) – веб-приложение mc	<i>%SystemDrive%\inetpub\wwwroot\cm\mc</i>

Имя сервиса	Расположение
OpenID Connect Server – веб-приложение oide	<i>%SystemDrive%\inetpub\wwwroot\cm\oidc</i>
MS CA Proxy – веб-приложение mscaproxy	<i>%SystemDrive%\inetpub\wwwroot\cm\mscaproxy</i>
Сервис удаленного обслуживания (Remote Self-Service) – веб-приложение rss	<i>%SystemDrive%\inetpub\wwwroot\cm\rss</i>
Сервис самообслуживания (Self-Service) – веб-приложение ss	<i>%SystemDrive%\inetpub\wwwroot\cm\ss</i>
Мастер настройки Indeed CM (Indeed CM Setup Wizard) – веб-приложение wizard	<i>%SystemDrive%\inetpub\wwwroot\cm\wizard</i>
Сервер Indeed AirCard Enterprise	<i>%SystemDrive%\inetpub\wwwroot\Indeed.AirCard.EntServer</i>

Linux

Имя сервиса	Расположение
Служба Card Monitor	<i>/opt/indeed/cm/cardmonitor</i>

Имя сервиса	Расположение
Сервис регистрации агентов – веб-приложение agentregistrationapi	<i>/opt/indeed/cm/agentregistrationapi</i>
Сервис агентов – веб-приложение agentserviceapi	<i>/opt/indeed/cm/agentserviceapi</i>
Сервис API – веб-приложение api	<i>/opt/indeed/cm/api</i>
Сервис онлайн-разблокировки и выключения устройств – веб-приложение credprovapi	<i>/opt/indeed/cm/credprovapi</i>
Консоль управления (Management Console) – веб-приложение mc	<i>/opt/indeed/cm/mc</i>
OpenID Connect Server – веб-приложение oidc	<i>/opt/indeed/cm/oidc</i>
Сервис удаленного обслуживания (Remote Self-Service) – веб-приложение rss	<i>/opt/indeed/cm/rss</i>
Сервис самообслуживания (Self-Service) – веб-приложение ss	<i>/opt/indeed/cm/ss</i>
Мастер настройки Indeed CM (Indeed CM Setup Wizard) – веб-приложение wizard	<i>/opt/indeed/cm/wizard</i>

- Откройте файл *nlog.config* в текстовом редакторе, например, в Блокноте, запущенном от имени администратора, и измените значение параметра `minlevel` с **Off** на **Trace**:

```
<logger name="*" minlevel="Trace" writeTo="file" />
```

- Сохраните изменения в файле.
- Перейдите в каталог **logs**, расположенный в каталоге сервиса, и удалите существующие логи.

5. Воспроизведите проблему.
6. Вернитесь в каталог **logs**, расположенный в каталоге сервиса, и убедитесь, что в нем появились подкаталоги с файлами отладочной информации.
7. Пришлите каталог **logs** со всем его содержимым специалистам **технической поддержки компании Индид** с описанием проблемы.
8. Для отключения логирования измените значение параметра `minlevel` с **Trace** на **Off** и сохраните изменения в файле.

Клиентские компоненты

Windows

Утилита CM GetLog предназначена для локального и удаленного сбора программных логов следующих компонентов:

- Indeed CM Middleware
- Indeed CM Client Tools
- Indeed CM Agent



ПРЕДУПРЕЖДЕНИЕ

Для работы утилиты CM GetLog необходимы права локального администратора. На операционных системах Windows Vista и выше утилита запускается от имени администратора (Run As Administrator).

Запустите приложение *Cm.GetLog.zip* из каталога *GetLog* дистрибутива Indeed CM.

Выполните следующие действия:

1. Подключитесь к компьютеру. Для этого введите *localhost* в поле **Computer** для подключения к локальному компьютеру или имя/IP-адрес удаленного компьютера для подключения к удаленному компьютеру. Нажмите **Connect**.



ПРЕДУПРЕЖДЕНИЕ

Для установки подключения к удаленному компьютеру под управлением Windows Vista и выше убедитесь, что на удаленном компьютере запущена и не заблокирована служба **Инструментарий управления Windows (WMI)** (Windows Management Instrumentation).

2. Нажмите **Enable Log**, чтобы включить логирование.
3. Воспроизведите проблему.
4. Нажмите **Disable Log**, чтобы отключить логирование.
5. Нажмите **Get Log...**, чтобы получить логи.
6. Укажите каталог для сохранения zip-архива и нажмите **Сохранить**.
7. Нажмите **Disconnect**, чтобы отключиться от компьютера.
8. Отправьте логи специалистам **технической поддержки компании Индид**. Подробно опишите действия пользователя и укажите точное время воспроизведения проблемы.



ПРИМЕЧАНИЕ

По умолчанию логи пишутся в каталог *C:\Windows\System32\LogFiles\cm*. Для доступа к лог-файлам удаленного компьютера по умолчанию используется сетевой каталог *ADMIN\$\System32\LogFiles\cm*. Каталог для записи логов задается опцией **Use alternative location** в разделе **Advanced Settings**.

▼ Дополнительные настройки

В окне **Advanced Settings** доступны следующие настройки:

Настройка	Описание
Max. log size (bytes)	Максимальный размер в байтах всех файлов в каталоге. Значение по умолчанию – 1Гб. При достижении максимального размера содержимое каталога будет автоматически удалено, за исключением файлов логов, время изменения которых не превышает значение поля Max. log file age.
Max. log file age (s)	"Возраст" файла лога в секундах. Если размер логов в каталоге превысил значение Max. log size, то из каталога будут удалены все файлы, дата изменения которых старше значения Max.log file age. Например: максимальный размер всех логов в каталоге <i>LogFiles\cm</i> 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: <i>\WINDOWS\System32\LogFiles\cm</i>, - сетевой путь: <i>ADMIN\$\System32\LogFiles\cm</i>

▼ Ошибки сбора логов и способы их устранения

- при подключении к удаленному компьютеру:

Ошибка	Причина	Решение
<code>0x800706BA</code> 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)).
<code>0x000004B3</code> 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 <i>HKEY_LOCAL_MACHINE\SOFTWARE\Cm</i> 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 <i>ADMIN\$\System32\LogFiles</i>).	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, установленного на ОС Linux, записываются в каталог *tmp/cm/logs*.

Управление логированием

1. Откройте файл */etc/cm/logging.cfg* с правами администратора.
2. Измените значение параметра *enabled*:
 - Значение *1* включает логирование.
 - Значение *0* отключает логирование.
3. Сохраните файл.

Сбор логов

1. Очистите существующие логи Indeed CM Middleware в каталоге */tmp/cm/logs*.
2. Воспроизведите проблему.
3. Отправьте новые логи специалистам **технической поддержки компании Индид**. Подробно опишите действия пользователя и укажите точное время воспроизведения проблемы.

Инсталляторы

Все инсталляторы Indeed Certificate Manager для ОС Windows представляют собой msi-пакеты. Отладочные логи для msi-пакетов можно получить стандартными средствами Windows Installer, запустив установку через командную строку с определенными параметрами.

Формат команды для запуска msi-пакета с записью логов:

```
msiexec /i <путь к файлу инсталлятора> /lv <путь к файлу с логами>
```

После завершения работы инсталлятора отправьте файл с логами специалистам **технической поддержки компании Индид** с описанием проблемы.

Примеры запуска

```
msiexec /i IndeedCM.Client.Tools-<номер версии>.x64.ru-ru.msi /lv  
log.txt
```

Данная команда запускает установочный пакет Indeed CM Client Tools из текущей папки. Логи инсталлятора пишутся в файл log.txt, который расположен в этой же папке.

```
msiexec /i D:\CM.Client\IndeedCM.Client.Tools-<номер версии>.x64.ru-  
ru.msi /lv C:\install_log.txt
```

Данная команда запускает установочный пакет Indeed CM Client Tools из папки D:\CM.Client. Логи инсталлятора пишутся в файл install_log.txt, который расположен в корне диска C.

Если вам необходимо собрать логи инсталлятора при установке компонента через групповые политики, и у вас нет возможности задать параметры командной строки, включите логи Windows Installer с помощью ключа в реестре.

- Чтобы включить логирование, в ветке реестра *HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer* создайте ключ **Reg_SZ: Logging** с значением *voicewarmupx*.
- Чтобы выключить логирование, задайте пустое значение ключа **Logging**.

Включить и выключить отладочные логи инсталляторов Indeed CM можно с помощью файлов REG, которые входят в состав дистрибутива и находятся в папке *\GetLog\Regfiles* (файлы *MSI logs On.reg* и *MSI logs Off.reg*).

- Чтобы включить запись отладочных логов инсталляторов на рабочей станции, запустите файл *MSI logs On.reg*.

- Чтобы выключить запись отладочных логов инсталляторов на рабочей станции, запустите файл *MSI logs Off.reg*.

Файл с логами сохраняется в папку *Temp*. Имя нового файла журнала выбирается произвольно, но начинается с букв *Msi* и заканчивается расширением LOG. Чтобы определить местоположение папки *Temp*, введите в командную строку следующую команду:

```
cd %temp%
```

Контакты

Служба поддержки

Если у вас возникли вопросы, связанные с документацией, или вы столкнулись с проблемами в планировании инфраструктуры Indeed Certificate Manager, трудностями при установке, настройке, или ошибками при эксплуатации, то вы можете обратиться в службу технической поддержки:

- email — support@indeed-id.com
- Телефон — 8-800-333-09-06 (звонок бесплатный)
- Портал поддержки <https://support.indeed-company.ru>

Отдел по работе с клиентами

Если у вас возникли вопросы, по условиям приобретения или сотрудничества, то вы можете обратиться к руководителю по работе с ключевыми заказчиками:

- Контактное лицо — Бегунова Екатерина
- email — sales@indeed-company.ru
- Телефон — +7 (495) 640-06-09

История версий

В этом разделе содержится краткое описание изменений и улучшений Indeed Certificate Manager по версиям.

7.2

- Реализована интеграция с удостоверяющими центрами Aladdin Enterprise CA и SafeTech CA для выпуска сертификатов с поддержкой алгоритмов шифрования RSA и ГОСТ.
- Реализована поддержка LDAP-каталогов пользователей Samba AD DC и РЕД АДМ.
- Добавлена поддержка Windows Server 2025 для серверных компонентов Indeed CM.
- Добавлена поддержка Альт 8 СП релиз 10 (c10f2) для серверных и клиентских компонентов Indeed CM.
- Оптимизировано определение параметров работы Indeed CM в Мастере настройки.
- Оптимизировано администрирование Indeed CM в Консоли управления.
- Расширена функциональность сервиса внутреннего электронного документооборота:
 - Реализована поддержка CAdES – стандарта, по которому формируется усовершенствованная электронная подпись с временным штампом.
 - В настройки политики добавлена возможность установить тип подписи, который разрешено использовать при подписи документов в Сервисе самообслуживания (CMS, CAdES-BES, CAdES-T, CAdES-X Long Type 1, CAdES-A).
- Исправлена ошибка при импорте корневых сертификатов Microsoft CA на устройство.
- Исправлена ошибка установки виртуальной смарт-карты AirCard на все разрешенные компьютеры.
- Исправлена ошибка прав доступа к ключу шифрования при работе Log Server в ОС Linux.

7.1

Интеграции

- Добавлена поддержка LDAP-каталогов FreeIPA и ALD Pro.
- Добавлена совместимость Indeed CM с новыми версиями удостоверяющего центра ПАК «КриптоПро УЦ» 2.0 (варианты исполнения 15, 16) и КриптоПро PKI-Кластером, которые доступны на ОС Astra Linux и Windows.

- Реализована интеграция Indeed CM с РутOKEN 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.