Indeed AirCard Enterprise

Техническая документация

Версия: 2.0

Дата: 08.05.2026

Содержание

О продукте

Indeed AirCard Enterprise (AirCard) полностью эмулирует поведение физического устройства (смарт-карты) и позволяет выполнять весь набор операций, доступный аппаратным ключевым носителям:

- Электронная подпись документов
- Шифрование и расшифровка данных
- Двухфакторная аутентификация пользователей
- Выполнение операций по стандарту Microsoft CryptoAPI

Характеристики виртуальных сетевых смарт-карт AirCard

Параметр	Значение
PIN-код администратора (по умолчанию)	87654321
PIN-код пользователя (по умолчанию)	12345678
Длина PIN-кода	от 1 до 31
Допустимые к использованию в PIN-коде символы	Символы латинского алфавита Символы верхнего и нижнего регистра Специальные символы Числа
История PIN-кода	от 0 до 16
Количество попыток ввода PIN-кода до блокировки	от 1 до 10
Максимальная длина ключа	до 4096 бит включительно
Максимальное количество последовательно повторяющихся символов	от 0 до 16

Параметр	Значение
Максимальное количество сертификатов на карте	100
Поддерживаемые криптопровайдеры	Microsoft Base Smart Card Cryptographic Service Provider (CSP)
Требования к вхождению определенных символов	Не важно Запрещено Обязательно

Компоненты Indeed AirCard Enterprise

Indeed AirCard Enterprise работает на базе серверных компонентов Indeed Certificate Manager. Для хранения данных и настроек используется СУБД Microsoft SQL, PostgreSQL или Postgres Pro.

Операции с виртуальными смарт-картами выполняются в Indeed Certificate Manager.

Клиентские компоненты

- **Indeed AirCard Runtime** – драйвер виртуального устройства с панелью управления.
- **Indeed CM AirCard Middleware** – компонент, который предоставляет системе Indeed CM единый интерфейс для управления виртуальными смарт-картами AirCard.

Системные требования

Серверные компоненты

Требования для работы серверных компонентов

Клиентские компоненты

Требования для работы клиентских компонентов

Сетевое взаимодействие

Взаимодействие компонентов AirCard

Серверные компоненты

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

Аппаратные требования

- Не менее 4 ГБ оперативной памяти
- Не менее 30 ГБ свободного дискового пространства

Программные требования

Операционная система	Windows Server 2012–2025
Веб-сервер	Internet Information Services (IIS) 7.0 и выше со следующими модулями: • Статическое содержимое (Static Content) • Перенаправление HTTP (HTTP Redirection) • ASP.NET – Расширяемость .NET (.NET Extensibility) • Расширения ISAPI (ISAPI Extensions) • Фильтры ISAPI (ISAPI Filters) • Обычная проверка подлинности (Basic Authentication) • Windows-проверка подлинности (Windows Authentication) • Консоль управления службами IIS (IIS Management Console)
Дополнительные компоненты Microsoft	Microsoft .NET 8.0

ДЛЯ УСТАНОВКИ IIS

Запустите скрипт PowerShell из дистрибутива Indeed CM (*\IIS.Setup.Scripts*), чтобы автоматически установить все необходимые компоненты сервера IIS.

При развертывании сервера Indeed AirCard Enterprise сначала установите и настройте сервер IIS, а затем Microsoft .NET 8.0.

Требования к окружению

Хранилище данных	Microsoft SQL Server 2012 SP2 и выше PostgreSQL 13 и выше Postgres Pro Standard, Postgres Pro Enterprise 13 и выше
Дополнительные настройки	DNS-зона обратного просмотра

ПРИМЕЧАНИЕ

DNS-зона обратного просмотра позволяет автоматически подключать сетевые смарт-карты Indeed AirCard к рабочим станциям сети организации. Если карты подключаются вручную, эта настройка не нужна.

Клиентские компоненты

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

Аппаратные требования	Не менее 200 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 2012–2022
Браузер	Microsoft Edge 88 и выше Google Chrome или Chromium 88 и выше Яндекс.Браузер 22.1.1 и выше Mozilla Firefox 109 и выше

Сетевое взаимодействие

В разделе перечислены системные требования для сетевого взаимодействия между компонентами Indeed AirCard Enterprise.

Сервер Indeed Aircard Enterprise

Веб-приложения, HTTP, HTTPS Входящие и исходящие подключения	3001 (TCP) 3002 (TCP)
Microsoft SQL Server Входящие и исходящие подключения	135 (TCP) – Transact-SQL debugger/RPC 1433 (TCP) – SQL Server default instance 1434 (UDP) – SQL Server Browser service
PostgreSQL	5432 (TCP/UDP) - PostgreSQL default port

Клиентские рабочие станции

DNS Исходящие подключения	53 (TCP/UDP)
Веб-приложения, HTTP, HTTPS Входящие и исходящие подключения	3001 (TCP) 3002 (TCP)

Установка и настройка

Хранилище данных

Microsoft SQL, PostgreSQL, Postgres Pro

Сервер Indeed AirCard Enterprise

Установка сервера, создание сертификата подписи, настройка интеграции с Indeed CM

Клиентские компоненты

Indeed CM AirCard Middleware и Indeed AirCard Runtime

Настройка работы в Indeed CM

Добавление лицензии и типа устройства, настройка привилегий

Хранилище данных

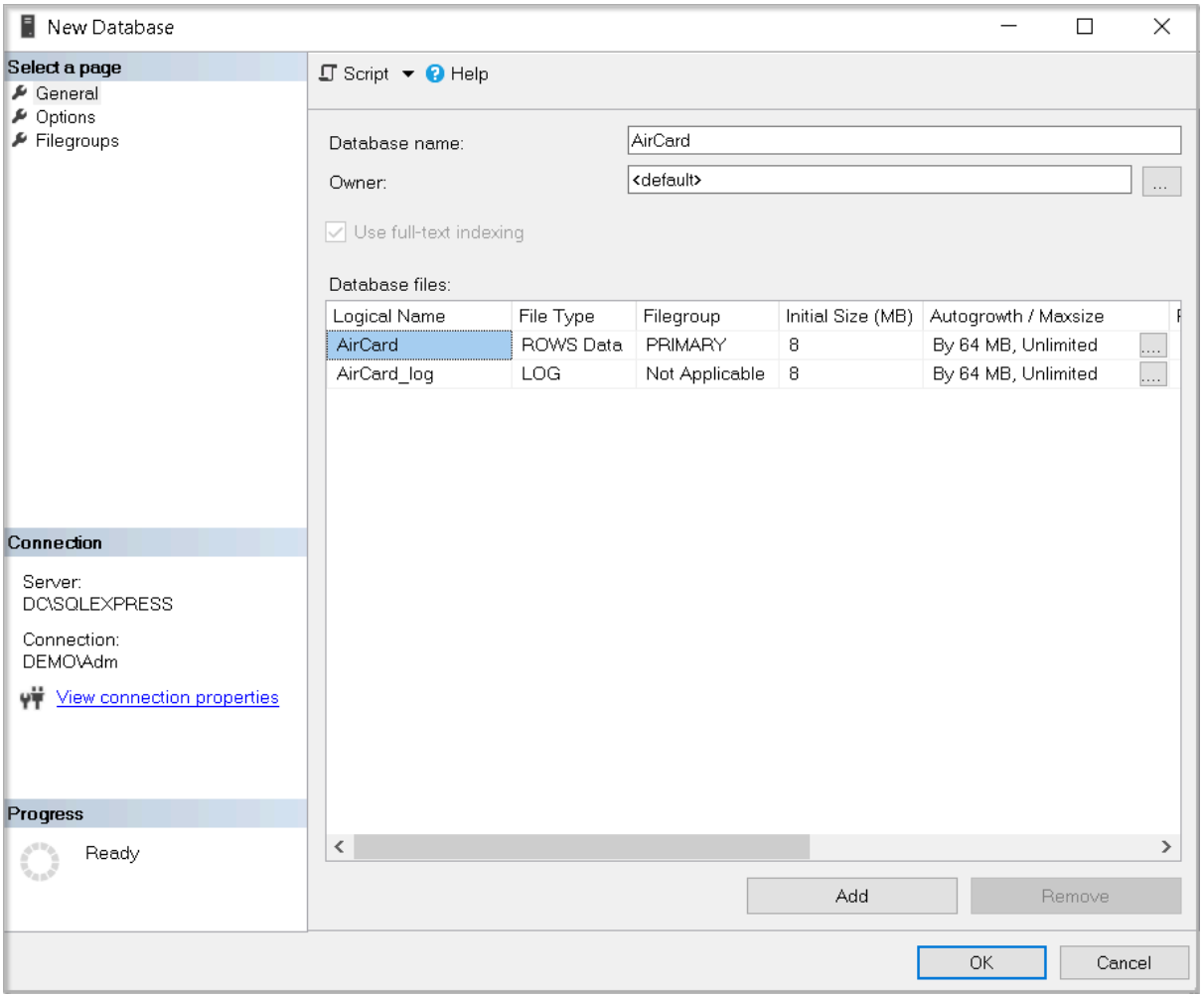
Данные Indeed AirCard Enterprise можно хранить в Microsoft SQL, PostgreSQL и Postgres Pro.

База данных создается вручную, а для ее наполнения используются скрипты из дистрибутива Indeed AirCard Enterprise.

Microsoft SQL

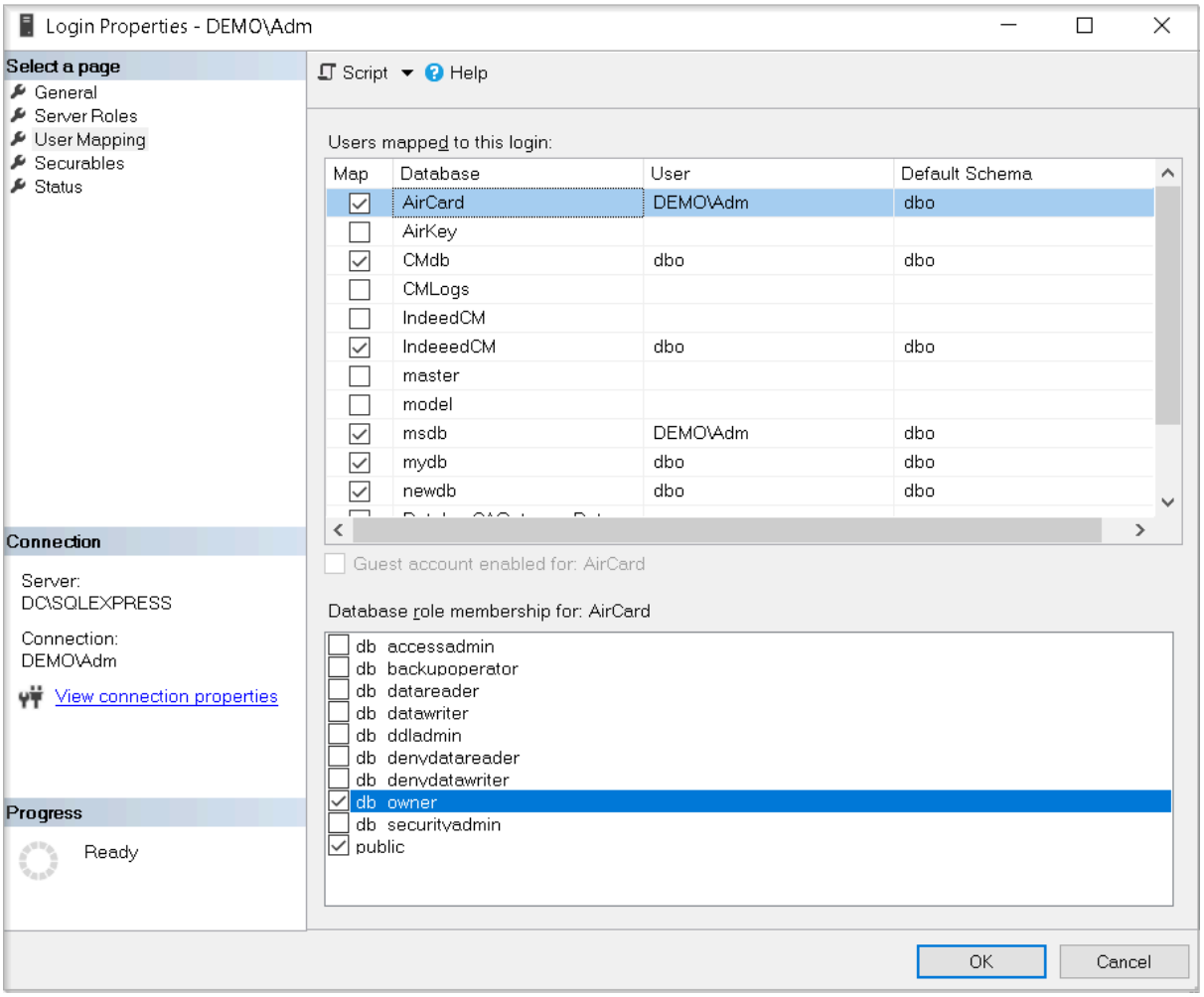
1. Создайте базу данных в среде SQL Management Studio с произвольным именем:

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



2. Определите **Имя для входа** (Logins) для созданной базы. 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 конфигурационном файле *appsettings.json*.

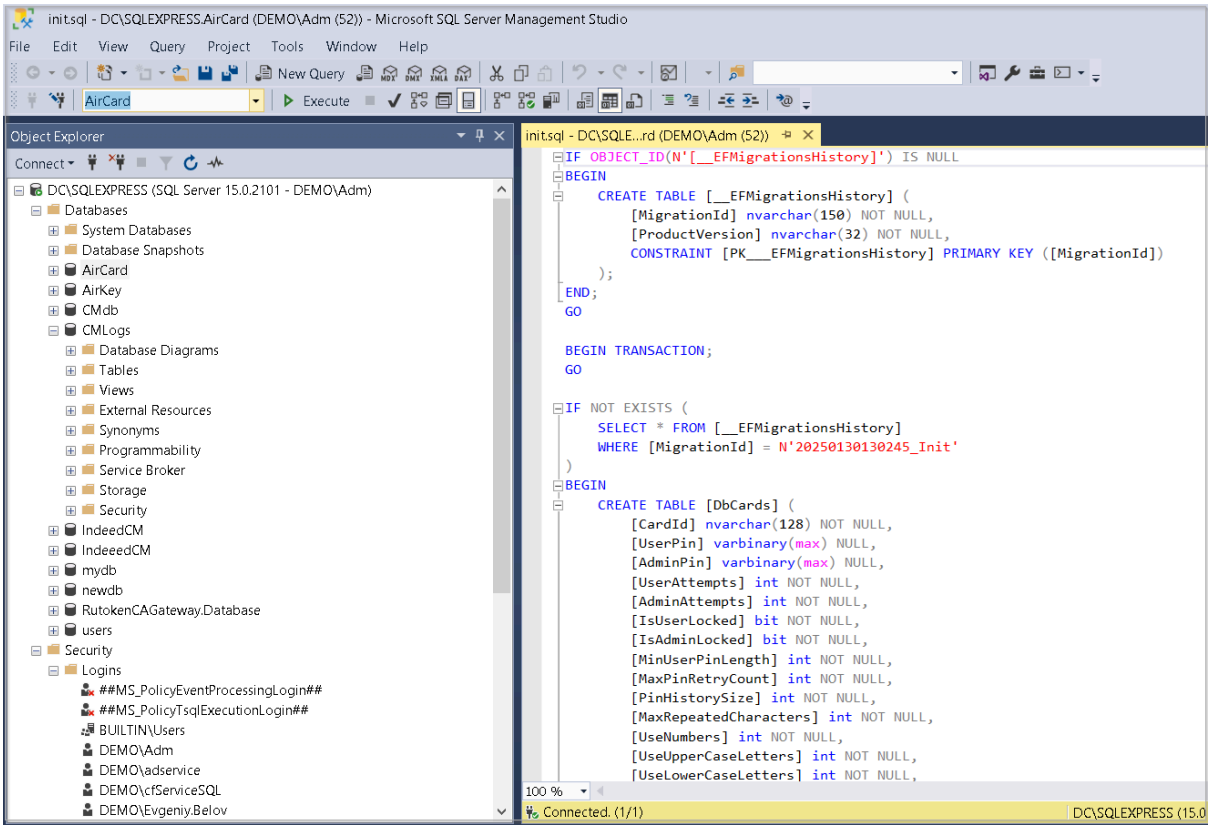
    1. Нажмите **Безопасность** (Security) → **Имя для входа** (Logins), из списка выберите учетную запись.
    2. Перейдите на вкладку **Сопоставление пользователей** (User Mapping).
    3. Выдайте права на работу с базой для выбранного имени входа.
       Укажите разрешения **db_owner** и **public** и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



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

    1. Выберите меню **Файл** (File) → **Открыть** (Open)→**Файл...** (File...), укажите путь к файлу *init.sql* (*\IndeedACES\Misc*) и нажмите **Открыть** (Open).

2. Выберите созданную базу данных в выпадающем меню.
3. Нажмите **Выполнить** (Execute).

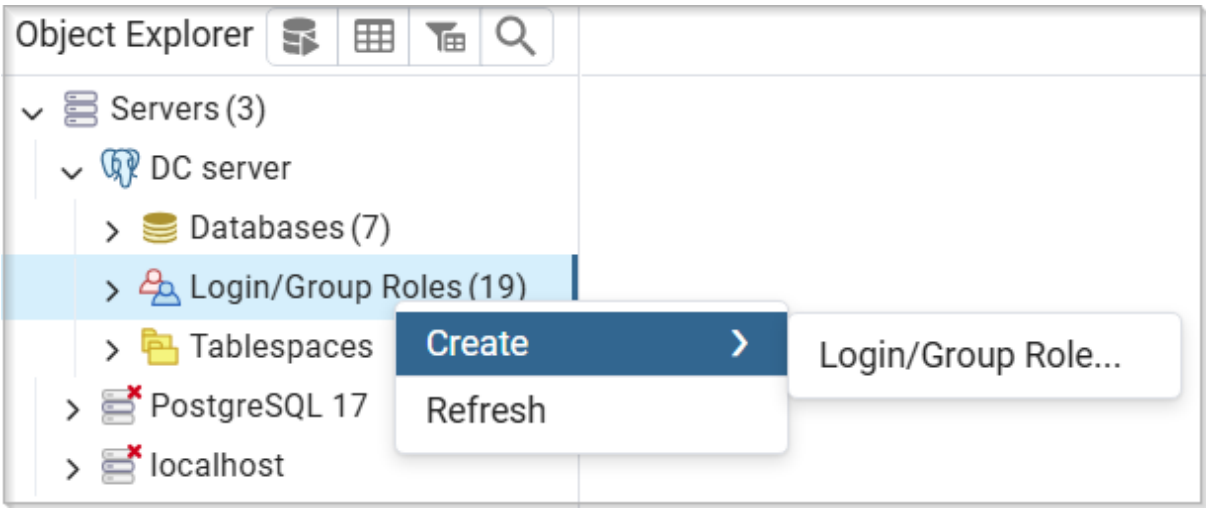


PostgreSQL и Postgres Pro

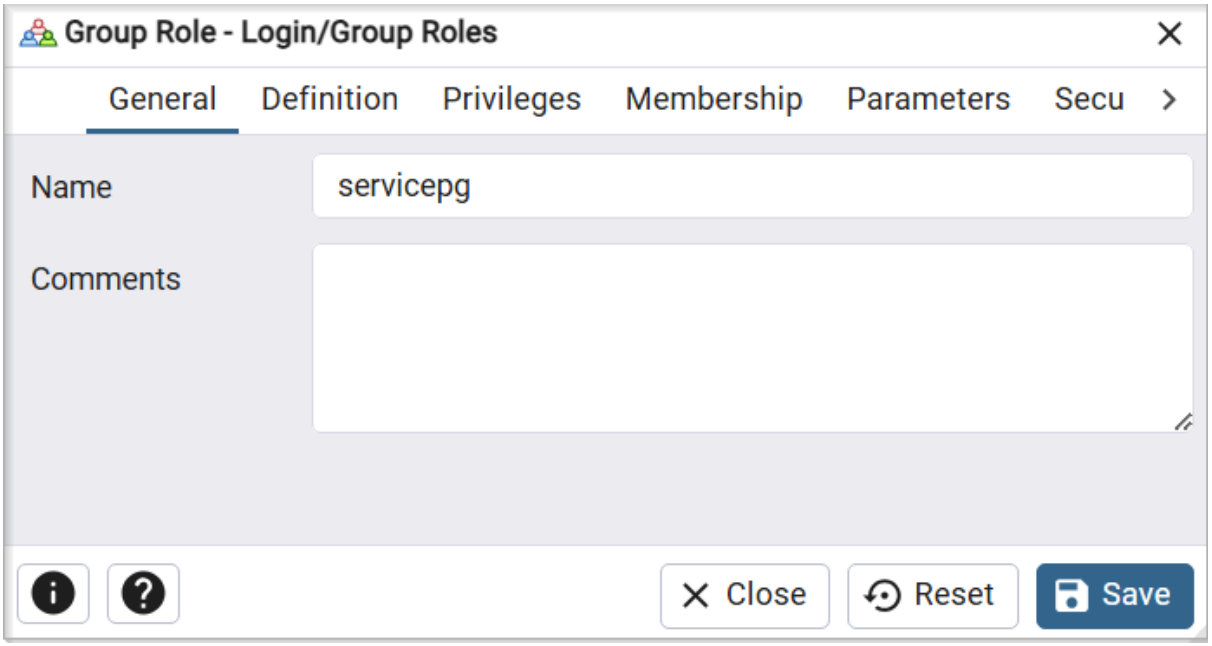
Создайте сервисную учетную запись и базу данных. Настройте удаленное подключение к базе данных.

Сервисная учетная запись

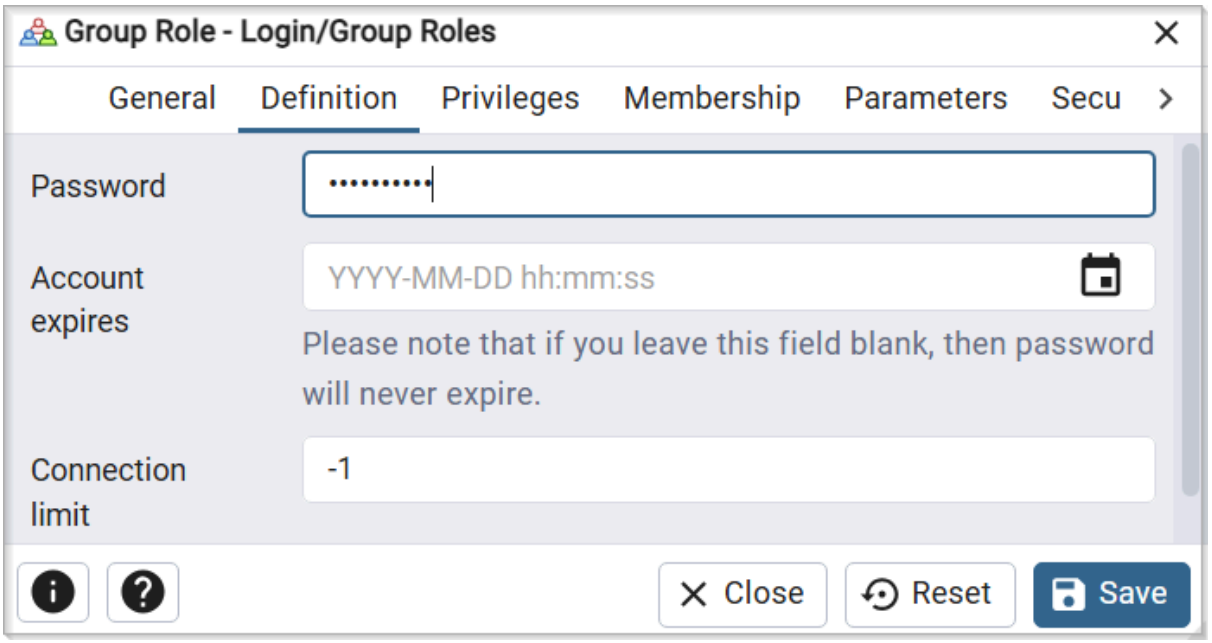
1. Откройте pgAdmin, укажите мастер пароль и подключитесь к серверу.
2. В разделе **Обозреватель** (Object Explorer) правой кнопкой мыши нажмите **Роли входа/группы** (Login/Group Roles).
3. Выберите **Создать → Роль входа/группы** (Create→Login/Group Role…).



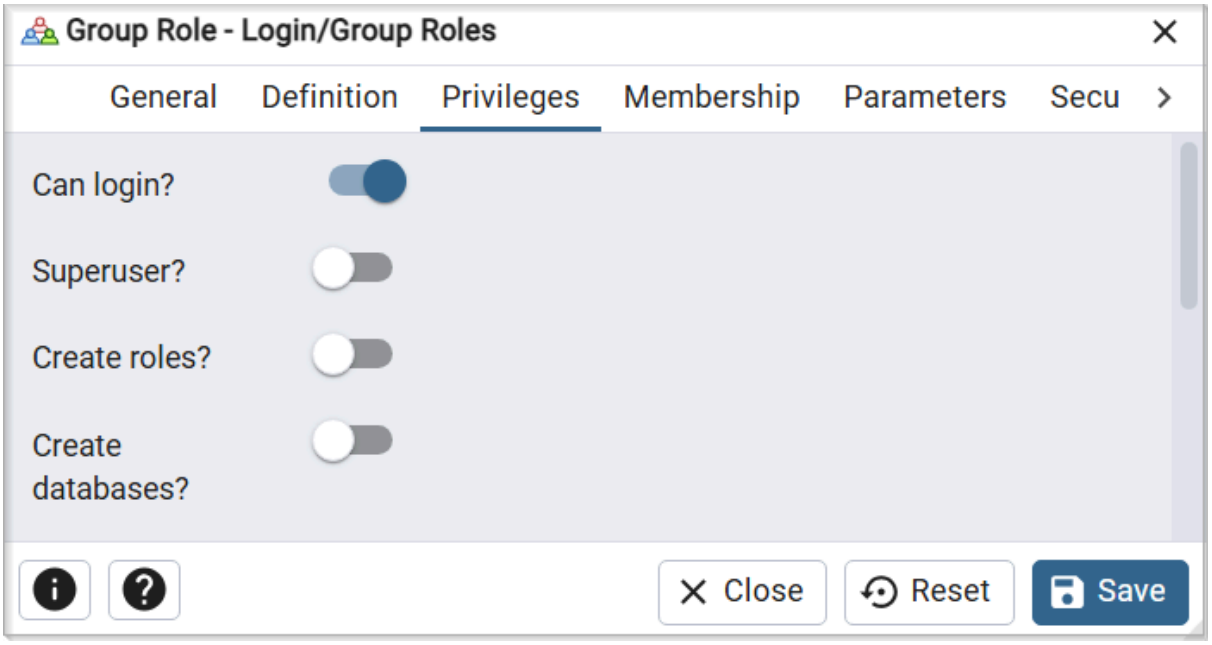
4. На вкладке **Общие** (General), в поле **Имя** (Name), укажите произвольное имя пользователя.



5. На вкладке **Определение** (Definition), в поле **Пароль** (Password), укажите пароль пользователя. Оставьте пустым поле **Роль активна до** (Account Expires), чтобы отключить срок действия пароля.



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

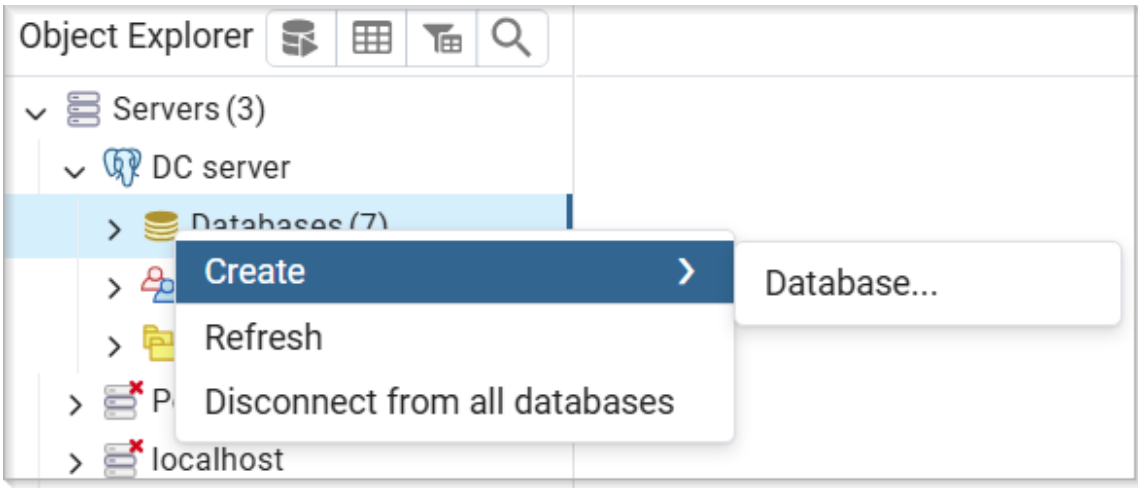


7. Оставьте остальные значения по умолчанию и нажмите **Сохранить** (Save).

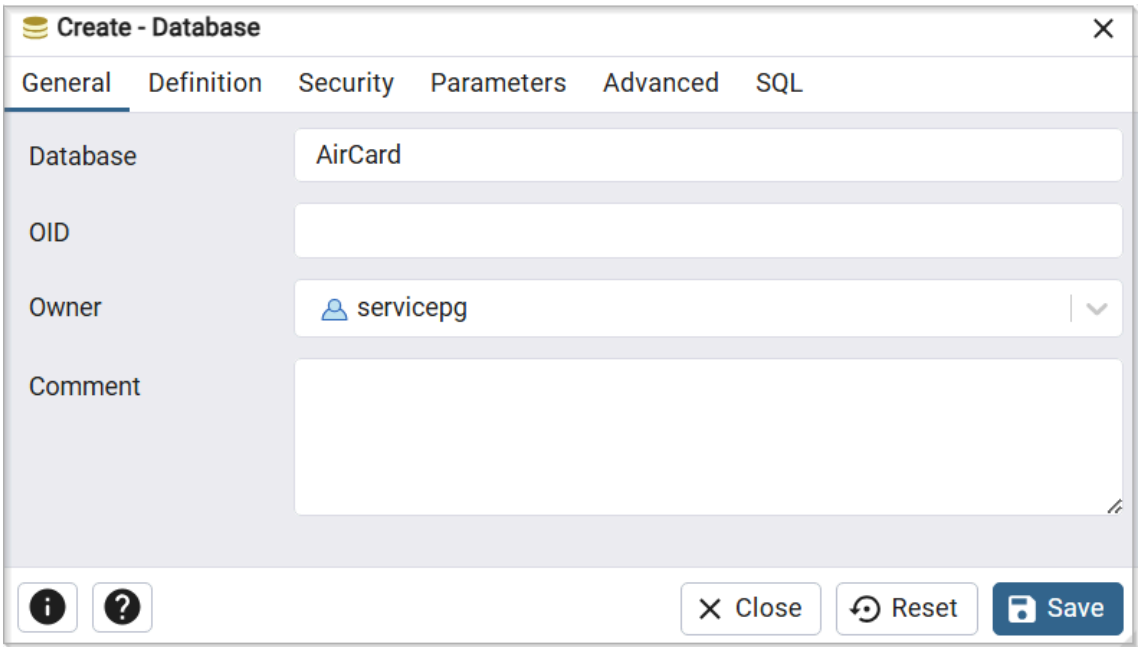
База данных

1. Создайте базу данных:

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



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



2. Выберите в **Обозревателе** (Object Explorer) созданную базу данных и выполните скрипт *init-postgre.sql*:

    1. Выберите меню **Инструменты** (Tools) → **Запросник** (Query Tool).

    2. В меню запросника нажмите , чтобы открыть файл скрипта, и укажите путь к файлу *init-postgre.sql* (*\IndeedACES\Misc*). Нажмите **Выбрать** (Select).

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

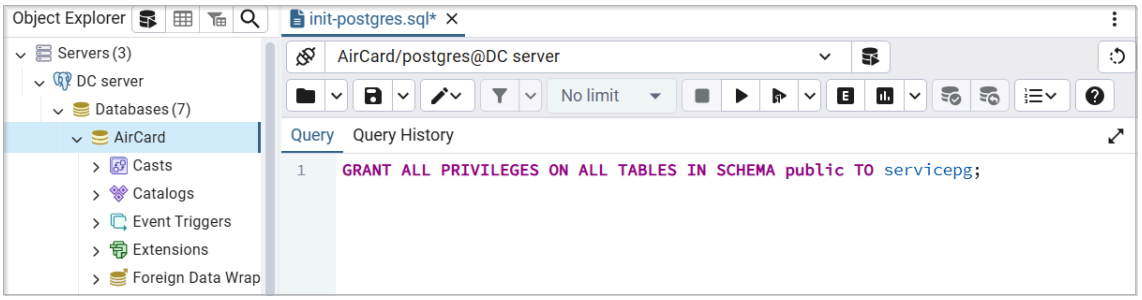
3. Предоставьте сервисной учетной записи привилегии на таблицы базы данных:

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

    2. Введите текст запроса и укажите имя сервисной учетной записи:

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

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



Удаленное подключение к базе данных

Откройте конфигурационный файл *pg_hba.conf*.

Расположение файла pg_hba.conf

PostgreSQL

ОС Windows: `C:\Program Files\PostgreSQL\<номер версии>\data`
ОС Linux: `/etc/postgresql/<номер версии>/main`

Postgres Pro

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

Добавьте строку следующего формата:

```
CONNECTIONTYPE DATABASE USER ADDRESS METHOD
```

Где:

- `CONNECTIONTYPE` – тип подключения. Укажите `host`, чтобы использовать подключение по TCP/IP.
- `DATABASE` – имя базы данных, для которой предоставляется доступ.
- `USER` – имя пользователя, для которого будет доступно подключение.
- `ADDRESS` – IP-адрес удаленного сервера Indeed AirCard Enterprise.
- `METHOD` – метод аутентификации пользователя.

Пример строки

```
host AirCard servicepg 192.200.1.0/24 md5
```

Сервер Indeed AirCard Enterprise

Системные требования

Чтобы установить и настроить сервер Indeed AirCard Enterprise:

1. Установите сервер Indeed AirCard Enterprise и настройте защищенное соединение в IIS.
2. Создайте сертификат подписи.
3. Настройте параметры работы Indeed AirCard Enterprise в конфигурационном файле.
4. Настройте интеграцию в Indeed Certificate Manager.

Установить сервер

Запустите файл *Indeed.AirCard.Enterprise.Server-<номер версии>.msi* из дистрибутива Indeed AirCard Enterprise и следуйте инструкциям мастера.

После установки сервера автоматически задаются следующие параметры контроля доступа для сайта Indeed.AirCard.EntServer:

- **Проверка подлинности** (Authentication): включена **Анонимная проверка подлинности** (Anonymous Authentication), остальные способы отключены.
- **Параметры SSL** (SSL Settings): **Требовать SSL** (Require SSL) и **Принимать** (Accept) сертификаты клиента.

Настроить защищенное соединение в IIS

Настройте защищенное соединение в Диспетчере служб IIS (Internet Information Services Manager). Установите привязку для доступа к серверу AirCard по HTTPS:

1. Перейдите в Диспетчер служб IIS (IIS Manager).
2. Выберите сайт Indeed AirCard EntServer и перейдите в раздел **Привязки** (Bindings).
3. Нажмите **Добавить** (Add).
4. Выберите **Тип** (Type) **https**.
5. Укажите **Порт** (Port), например **3002**. Убедитесь, что порт открыт для входящих подключений в брандмауэре.
6. Если сервер AirCard Enterprise установлен на Windows Server 2019 и выше, включите опцию **Отключить HTTP/2** (Disable HTTP/2).

7. Укажите **SSL-сертификат** (SSL certificate). Убедитесь, что поле **Улучшенный ключ** сертификата содержит значение «Проверка подлинности сервера» (Server Authentication) и выдан на имя рабочей станции, которое указывается в адресе подключения.
8. Нажмите **OK**.

Создать сертификат подписи

Сертификат подписи необходим для выдачи сертификатов пользовательским рабочим станциям, к которым подключаются устройства AirCard.

Подробнее о сертификате подписи

Клиентский сертификат выдается автоматически при первом подключении устройства AirCard к компьютеру.

При обращении к серверу клиентский компьютер предоставляет свой сертификат, а сервер Indeed AirCard Enterprise проверяет подлинность клиентского сертификата и разрешает подключение виртуальной карты.

Чтобы создать сертификат подписи:

1. Откройте командную строку с правами администратора на сервере Indeed AirCard Enterprise и запустите утилиту AirCard.VTServer.CertificateGenerator.exe. После завершения работы утилиты в оснастке **Сертификаты** (Certificates) локального компьютера появится сертификат AirCard Enterprise Server CA.
2. Выдайте серверу AirCard права на чтение закрытого ключа сертификата сервера:
    1. Перейдите в оснастку **Сертификаты** (Certificates) локального компьютера.
    2. Нажмите правой кнопкой мыши на сертификат AirCard Enterprise Server CA и выберите **Все задачи** (All tasks) → **Управление закрытыми ключами** (Manage Private Keys).
    3. Нажмите **Добавить** (Add) и укажите локальную группу *IIS_IUSRS*.
    4. Выставьте право на **Чтение** (Read).
    5. Нажмите **Применить** (Apply).
    6. Добавьте сертификат AirCard Enterprise Server CA в список **Доверенных Корневых Центров Сертификации** (Trusted Root Certification Authorities) на сервере AirCard и на рабочих станциях, к которым будут подключаться устройства AirCard.

Настроить параметры работы AirCard

1. Откройте файл конфигурации *appsettings.json*. Файл находится по пути *C:\inetpub\wwwroot\aircard\server*.
2. Заполните параметры и сохраните изменения.

Параметр	Значение
`adminFilter`	Необязательный параметр. Данные клиентского сертификата сервера Indeed CM для аутентификации на сервере Indeed Aircard Enterprise: • **Назначение** (OID) сертификата в разделе **Улучшенны** (Enhanced Key Usage) Например, `EKUs:1.3.6.1.5.5.7.3.2`. • **Отпечаток** (Thumbprint) сертификата Например, `Thumbprint:05eac3725eaa791f18ef45118ff3fa2` Если в инфраструктуре развернуто несколько серверов Inde укажите OID или Thumbprint сертификата для каждого серв `;`.
`isCardsAllowedForAllUsers`	• `true` – в активной сессии пользователя отобразятся в карты AirCard, которые подключены к рабочей станци • `false` – в активной сессии пользователя отобразятся подключенные смарт-карты AirCard текущего пользов устройства других пользователей не будут видны
`serverCertThumbprint`	**Отпечаток** (Thumbprint) сертификата подписи
`storage`	Хранилище данных: `SqlServer` или `PostgreSql`
`connectionString`	Строка подключения к хранилищу данных
`cryptoAlgName`	Алгоритм шифрования
`cryptoKey`	Ключ шифрования

Пример заполненного файла конфигурации с хранилищем в Microsoft SQL

```
{
  "certificateAccessControlSettings": {
    "adminFilter": "EKUs:1.3.6.1.5.5.7.3.1"
  },
  "airCardSettings": {
    "isCardsAllowedForAllUsers": true,
    "serverCertThumbprint":
"138c1215787e4cb3460b7af46be77291bd4c7c1a"
  },
  "storage": "SqlServer",
  "sqlPersistenceSettings": {
    "connectionString": "Data Source=DC;Initial Catalog=AirCard;User
ID=Admin;Password=P@ssword;TrustServerCertificate=True",
    "cryptoAlgName": "AES",
    "cryptoKey":
"9542a73b8208b601b50fc7ef53ab8065254394048e1ca155fac1e954fe965a71"
  },
  "eventLogAuditSettings": {
    "providerGuid": "{79A2642D-FDC4-4B29-88E6-972D2B7CECF7}"
  },
  "logging": {
    "logLevel": {
      "default": "Information",
      "microsoft": "Warning",
      "microsoft.Hosting.Lifetime": "Information"
    }
  },
  "allowedHosts": "*"
}
```

Пример заполненного файла конфигурации с хранилищем в PostgreSQL

```
{
  "certificateAccessControlSettings": {
    "adminFilter": "EKUs:1.3.6.1.5.5.7.3.1"
  },
  "airCardSettings": {
    "isCardsAllowedForAllUsers": true,
    "serverCertThumbprint":
"138c1215787e4cb3460b7af46be77291bd4c7c1a"
  },
  "storage": "PostgreSql",
  "sqlPersistenceSettings": {
    "connectionString":
"Host=DC;Database=AirCard;Username=Adm;Password=P@ssword",
    "cryptoAlgName": "AES",
    "cryptoKey":
"9542a73b8208b601b50fc7ef53ab8065254394048e1ca155fac1e954fe965a71"
  },
  "eventLogAuditSettings": {
    "providerGuid": "{79A2642D-FDC4-4B29-88E6-972D2B7CECF7}"
  },
  "logging": {
    "logLevel": {
      "default": "Information",
      "microsoft": "Warning",
      "microsoft.Hosting.Lifetime": "Information"
    }
  },
  "allowedHosts": "*"
}
```

Настроить интеграцию с Indeed CM

Чтобы выпускать устройства AirCard для пользователей через Indeed Certificate Manager, настройте интеграцию и определите параметры работы с сервером Indeed AirCard Enterprise.

1. На сервере Indeed CM запустите Мастер настройки и перейдите в раздел **AirCard Enterprise**.
   Как запустить Мастер настройки Indeed CM
2. Включите опцию **Включить интеграцию с Indeed AirCard Enterprise**.
3. В поле **URL подключения к серверу AirCard Enterprise** укажите ссылку и порт для подключения к серверу. Убедитесь, что порт открыт в брандмауэре для входящих подключений на сервере AirCard.
4. В поле **Отпечаток сертификата** укажите Отпечаток (Thumbprint) сертификата, выданного рабочей станции, на которой установлен сервер Indeed CM.
   Убедитесь, что поле **Улучшенный ключ** сертификата содержит значение «Проверка подлинности клиента» (Client Authentication). У группы *IIS_IUSRS* должны быть права на **Чтение** (Read) закрытого ключа указанного сертификата.
   Как создать клиентский сертификат для сервера Indeed CM
5. В поле **Время существования незарегистрированных смарт-карт AirCard Enterprise в секундах** укажите время, по истечению которого служба Card Monitor удалит незарегистрированные устройства AirCard. Значение по умолчанию – 120 секунд.
6. Перейдите в раздел **Подтверждение** и нажмите **Применить** для сохранения настроек. Рекомендуется сохранить файл резервной копии Indeed Certificate Manager вместе с параметрами подключения к Indeed AirCard Enterprise.

Клиентские компоненты

Системные требования

Indeed CM AirCard Middleware

Чтобы установить Indeed CM AirCard Middleware, запустите файл *IndeedCM.AirCard.Middleware-<номер версии>.msi* из дистрибутива Indeed CM (каталог *IndeedCM.Client*) и следуйте инструкциям мастера.

Indeed AirCard Runtime

Чтобы установить Indeed AirCard Runtime, запустите файл *Indeed.AirCard.Runtime-<номер версии>.msi* из дистрибутива Indeed AirCard Enterprise и следуйте инструкциям мастера.

Indeed AirCard Runtime можно установить через групповые политики Windows:

1. Поместите в хранилище **Компьютера** (Local Computer) каждой рабочей станции сертификат подписи msi-пакета *Indeed_LLC.cer*. Сертификат находится по пути *Indeed.AirCard.Runtime\Misc\Certificates*.
2. Поместите сертификат в раздел **Доверенные издатели** (Trusted Publishers).

Настроить параметры Indeed AirCard Runtime

Параметры работы считывателя устройств AirCard можно изменить через:

- Групповые политики Active Directory – для рабочих станций, входящих в домен организации
- Реестр Windows – для рабочих станций вне домена Windows

Групповые политики Active Directory

Перед настройкой групповой политики добавьте шаблоны политик Indeed AirCard Enterprise в список административных шаблонов Active Directory. Файлы шаблонов политик входят в состав дистрибутива Indeed AirCard Runtime и находятся в каталоге *\Misc\PolicyDefinitions*.

AirCard Enterprise Server

Политика **AirCard Enterprise Server** применяется к рабочим станциям пользователей и определяет настройки подключения к серверу Indeed AirCard Enterprise.

Параметр	Описание
Не задан (Not Configured) **Отключен** (Disabled)	Ссылка для подключения не указана. Работа с устройствами AirCard на рабочей станции пользователя невозможна. Значение по умолчанию – **Не задан**.
Включен (Enabled)	В параметре **URL сервера** укажите ссылку и порт для подключения к серверу. Убедитесь, что указанный порт открыт в брандмауэре для входящих подключений на сервере Indeed AirCard Enterprise.

Виртуальный считыватель AirCard

Политика **Виртуальный считыватель AirCard** применяется к рабочим станциям пользователей и определяет количество считывателей устройств AirCard на рабочей станции.

Параметр	Описание
Не задан (Not Configured) **Отключен** (Disabled)	Количество считывателей для подключения устройств AirCard равно 1. Значение по умолчанию – **Не задан**.
Включен (Enabled)	В параметре **Количество считывателей** укажите количество считывателей, к которым могут подключаться устройства AirCard. Значение по умолчанию – 3. Максимальное количество – 10.

Реестр Windows

1. Создайте файл реестра REG со следующим содержанием:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\AirCard]
"AirCardEnterpriseServerUrl"=""
"ReaderInstanceCount"=dword:00000000
```

2. В параметре `AirCardEnterpriseServerUrl` укажите ссылку и порт подключения к серверу AirCard.

3. В параметре `ReaderInstanceCount` укажите количество считывателей, к которым могут подключиться устройства AirCard. Значение по умолчанию – 3. Максимальное количество – 10.

Пример содержимого файла реестра

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\AirCard]
"AirCardEnterpriseServerUrl"="https://aircard.demo.local:3002"
"ReaderInstanceCount"=dword:00000003
```

Настройка работы в Indeed CM

Прежде чем начать работу с устройствами AirCard, выполните следующие действия:

1. Запустите Консоль управления Indeed Certificate Manager и перейдите на вкладку **Конфигурация**.
2. Добавьте лицензию Indeed AirCard Enterprise.
3. Добавьте тип устройства.
4. Настройте привилегии для работы с устройствами AirCard.

Добавить лицензию

1. В Консоли управления Indeed CM перейдите в раздел **Конфигурация → Лицензии**.
2. Нажмите **Добавить лицензию**, загрузите файл лицензии и нажмите **Добавить**.

Добавить тип устройства AirCard

1. В Консоли управления Indeed CM перейдите в раздел **Конфигурация → Типы устройств**.
2. Нажмите **Добавить тип устройства**.
3. Выберите файл типа устройства *AirCard.xml*. Файл находится в дистрибутиве сервера Indeed CM по пути *\Misc\CardTypes*.
   Чтобы заменить установленный файл типа устройства, включите опцию **Заменить существующий**.
4. Нажмите **Добавить**.

Файл типа устройства по умолчанию содержит предустановленные значения PIN-кодов администратора и пользователя. Эти значения можно изменить после добавления файла устройства в Indeed CM.

Редактировать файл типа устройства

При редактировании типа устройства доступны следующие опции:

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.

Устанавливать неслучайный PIN-код администратора

Если опция включена, при добавлении устройства устанавливается указанный PIN-код, если выключена – устанавливается случайный PIN-код, известный только Indeed CM.

Удалить тип устройства

Чтобы удалить тип устройства, выберите его в списке и нажмите ✖. Удалить тип устройства можно только в том случае, если в Indeed CM нет ни одного устройства этого типа.

Настроить привилегии для работы с устройствами AirCard

1. В Консоли управления Indeed CM перейдите в раздел **Конфигурация → Роли**.
2. Выдайте членам ролей следующие привилегии:
    - Изменение привязки AirCard
    - Удаление AirCard

Операции с устройствами

Операции с устройствами AirCard выполняются по аналогии с аппаратными устройствами в Indeed Certificate Manager.

> ⚠ **ЗАМЕНА AIRCARD**
>
> Устройство AirCard можно заменить только на аппаратное устройство (USB-токен или смарт-карту). Замена AirCard на другую виртуальную смарт-карту невозможна.

Выпуск

Выпустить устройство AirCard и назначить пользователю

Подключение к рабочей станции

Добавить рабочую станцию пользователя в список разрешенных компьютеров

Отзыв и изъятие

Удалить устройство AirCard

Выпуск

При выпуске устройство AirCard автоматически добавится в Indeed Certificate Manager и назначится пользователю. AirCard можно выпустить в карточке пользователя или в разделе **Устройства**.

Чтобы выпустить AirCard в карточке пользователя:

1. В Консоли управления Indeed CM перейдите в раздел **Пользователи** и выполните поиск пользователя.
2. Нажмите на логин пользователя в результатах поиска и перейдите в карточку.
3. Нажмите **Выпустить AirCard**.

Чтобы выпустить AirCard в разделе **Устройства**:

1. В Консоли управления Indeed CM перейдите в раздел **Устройства**.
2. Нажмите **Выпустить AirCard**.
3. Выберите пользователя и нажмите **Выбрать.**
4. Задайте **Имя устройства** или оставьте значение по умолчанию.
5. Нажмите **Выпустить**.

> **ПРИМЕЧАНИЕ**
>
> Если в политике использования устройств Indeed CM включена интеграция с Indeed AM, то выпущенное устройство AirCard можно использовать для аутентификации в домене и SSO-приложениях, для цифровой подписи или для доступа к ресурсам, требующих персональных сертификатов.

Подключение к рабочей станции

Чтобы подключить устройство AirCard к рабочей станции, укажите разрешенные компьютеры для каждого устройства.

Чтобы добавить компьютер:

1. В Консоли управления Indeed CM откройте карточку устройства AirCard.
2. В строке **Разрешенные компьютеры** нажмите **Добавить**.

Добавить компьютер можно двумя способами: по DNS-имени или с помощью уникального кода.

DNS-имя

Подключитесь к рабочей станции пользователя по DNS-имени, если она находится в сети предприятия, где установлен сервер Indeed AirCard Enterprise.

Чтобы добавить компьютер, укажите DNS-имя рабочей станции и нажмите **Добавить**.

Уникальный код

Подключитесь к рабочей станции пользователя по уникальному коду, если она находится за пределами сети предприятия, а сервер Indeed AirCard Enterprise доступен через Интернет.

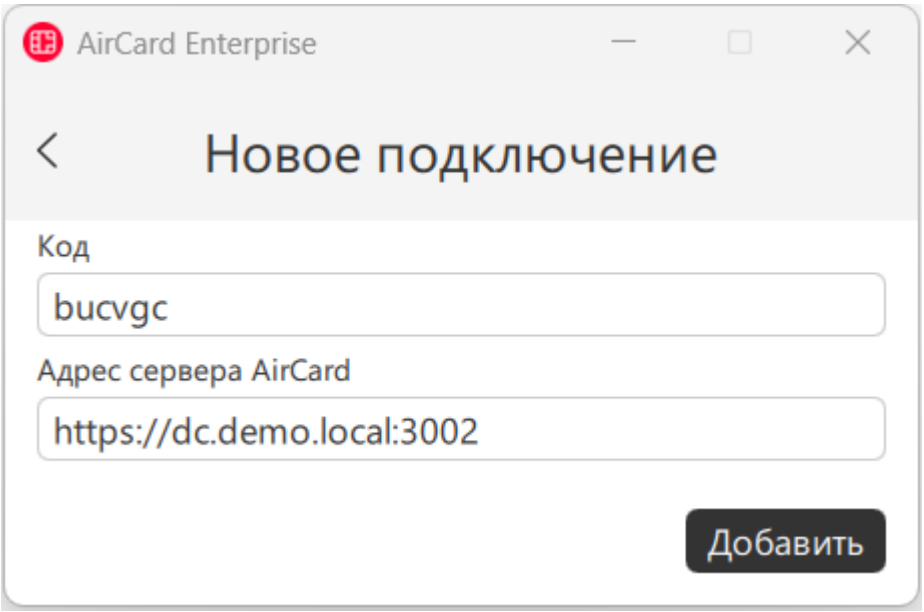
Чтобы добавить компьютер:

1. Укажите имя компьютера, которое будет отображаться в карточке устройства, и нажмите **Добавить**.
2. Сервер Indeed CM сгенерирует уникальный код. Сообщите код пользователю, чтобы продолжить подключение устройства. Код действителен в течение часа, его можно использовать только один раз.
3. Нажмите **Закрыть**.

Чтобы добавить и подключить AirCard к рабочей станции, пользователю необходимо:

1. Открыть Панель управления Indeed AirCard Enterprise, нажать и .

2. Ввести код, полученный от администратора, и нажать **Добавить**. Адрес сервера Indeed AirCard Enterprise подставляется автоматически.



Отзыв и изъятие

При отзыве устройство AirCard изымается у пользователя и очищается.

Чтобы отозвать устройство, в карточке устройства AirCard нажмите **Отозвать и изъять**.

> **ПРИМЕЧАНИЕ**
>
> Если в настройках шаблонов сертификатов выбранного УЦ включена опция **Отзывать сертификат при отзыве/выключении устройства**, то сертификат, выпущенный по этому шаблону, отзывается без возможности восстановления.
> Подробнее в документации Indeed CM

Выпущенное устройство AirCard можно также удалить из Indeed CM в разделе **Устройства**.