

Настройка параметров системы

На этапе развертывания системы необходимо указать нужные значения в файлах конфигурации для каждого сервиса. Файлы конфигурации всех сервисов системы

располагаются в корневом каталоге веб-приложений IIS (путь по умолчанию %SystemDrive%\inetpub\wwwroot\cm) для ОС Windows или в каталоге /opt/indeed/cm для ОС Linux.

- [Настройка параметров системы](#)
 - [Применение файлов конфигурации на сервере системы](#)
- Файлы конфигурации службы Card Monitor для ОС Windows расположены в %ProgramFiles%\Indeed CM\CardMonitor.

Настройка файлов конфигурации осуществляется при помощи Мастера настройки Indeed CM, который является независимым компонентом и устанавливается отдельно.

✔ **Системные требования для установки компонента совпадают с требованиями для установки серверных компонентов системы.**

Установка и запуск Мастера настройки Indeed CM

Установка мастера на ОС Windows

Запустите файл **IndeedCM.Wizard-*<номер версии>.x64.ru-ru.msi*** из каталога IndeedCM. Server дистрибутива системы и выполните установку, следуя указаниям мастера. Мастер настройки устанавливается в каталог *C:\inetpub\wwwroot\cm\wizard*.

Установка и запуск мастера на ОС Linux

Выполните установку веб-приложения из DEB или RPM пакета (**cm.wizard-*<номер версии>_amd64.deb*** или **cm.wizard-*<номер версии>.x86_64.rpm***) в зависимости от используемого Linux дистрибутива.

RHEL и производные дистрибутивы:

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

Debian и производные дистрибутивы:

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

Запустите bash-скрипт **start-cm-wizard.sh** расположенный в каталоге с дистрибутивом сервера системы.

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



В целях безопасности рекомендуется отключать веб-приложение Мастер настройки Indeed CM после проведения конфигурации системы.

ОС Windows:

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

ОС Linux:

1. Откройте эмулятор терминала.
2. Выполните команду:

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

Аутентификация в Мастере настройки Indeed CM

Аутентификация в приложении **Мастер Настройки Indeed CM** осуществляется по временным кодам аутентификации. Код аутентификации формируется в момент запуска пула приложения IIS IndeedCM Wizard на ОС Windows или в момент старта службы *cm-wizard.service* на ОС Linux и сохраняется в файл **wizard_authentication_code.txt** в подкаталоге *logs*.



Файл **wizard_authentication_code.txt** расположен:

- в каталоге *C:\inetpub\wwwroot\cm\wizard\logs* для ОС Windows
- в каталоге */opt/indeed/cm/wizard/logs* для ОС Linux.

1. Откройте файл **wizard_authentication_code.txt** и скопируйте Код аутентификации.

wizard_authentication_code.txt

2023-09-20 09:40:06.1557|AuthenticationCode: "YoQZdL2mJC4pYmKJmC7YT8mXDv3FPj2v"

-  Код аутентификации для Мастера настроек Indeed CM, развернутого на сервере под управлением ОС Linux, также можно получить командой `systemctl status`

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

или получить из журнала приложения systemd юнита `cm-wizard.service`, выполнив команду:

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

В результате, код аутентификации будет выведен на экран терминала:

```
Sep 20 09:40:06 indeedcm cm-wizard[416403]: AuthenticationCode:
"YoQZdL2mJC4pYmKJmC7YT8mXDv3FPj2v"
```

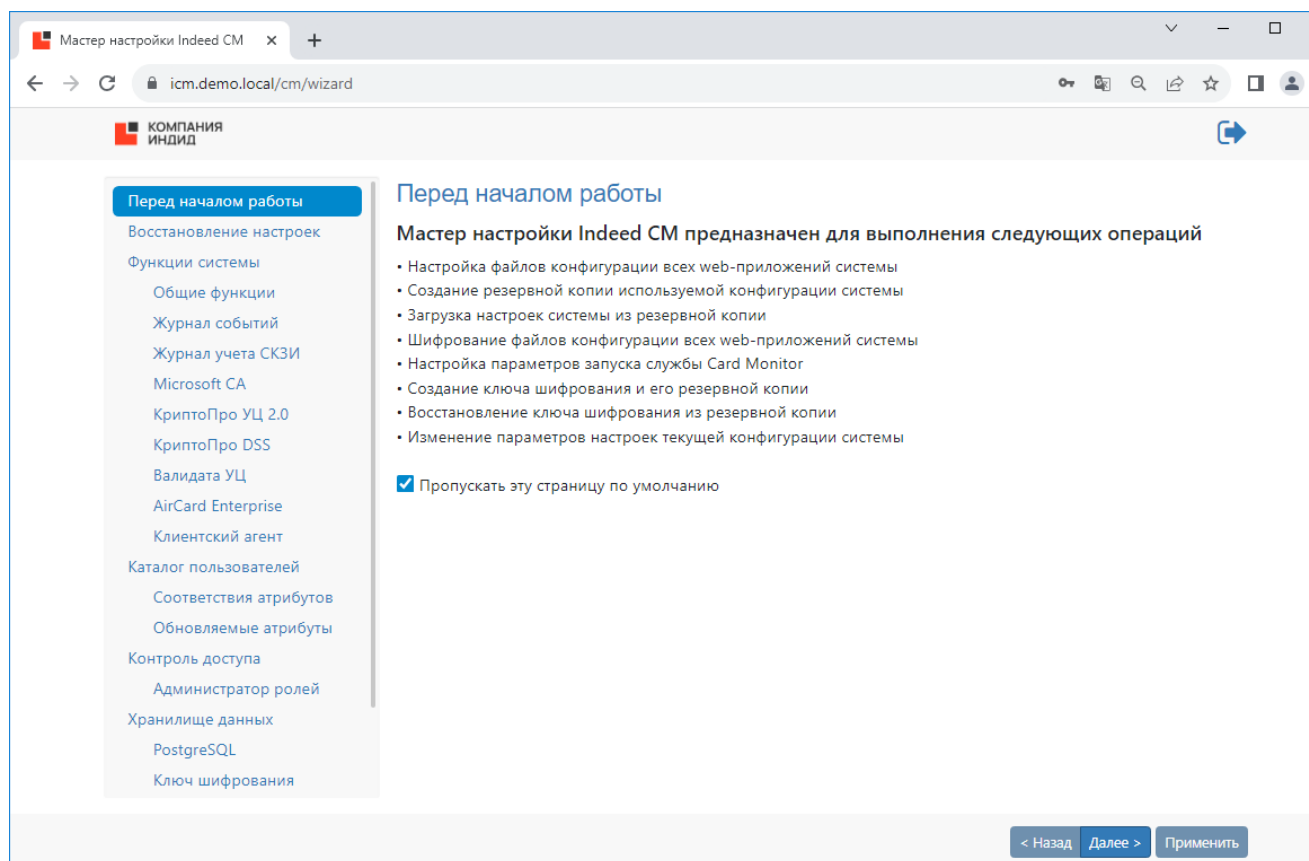
2. С помощью интернет браузера перейдите по адресу **<https://<FQDN сервера Indeed CM>/cm/wizard>**. Введите код в поле Код аутентификации и нажмите Войти:

Введите код аутентификации



Войти

Настройка параметров системы



В таблице приведены разделы мастера настройки Indeed CM и их описание.

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

Функции системы: • Общие функции • Журнал событий • Журнал учета СКЗИ • Microsoft CA • КриптоПро УЦ 2.0 • КриптоПро DSS • Валидата УЦ • AirCard Enterprise • Клиентский агент	Общие функции: настройка внутренних параметров веб-приложений Indeed CM. Консоль управления (Management Console) • Журнал учета устройств и сертификатов • Организационная структура • Интеграция с Indeed Access Manager • Интеграция с Secret Net Studio (доступна только для инсталляций под управлением ОС Windows) • Интеграция со СМЭВ • Внутренний документооборот • Сброс пароля пользователя в Active Directory • Просмотр SO PIN устройства • Публикация сертификатов в файловое хранилище  Публикация сертификатов не поддерживается для примонтированных сетевых дисков. Задайте путь к файловому хранилищу в формате: \\Имя рабочей станции\Имя сетевого каталога Сервис самообслуживания (Self-Service) • Просмотр содержимого устройства • Работа с TPM Virtual Smart Card • Работа с Windows Hello for Business • Загрузка файлов и ресурсов Журнал событий: • Переопределять атрибут имени пользователя для поиска в Журнале событий. Значение по умолчанию: CN (common name) • Настройка подключения к единому журналу событий для нескольких серверов Indeed CM Журнал учета СКЗИ: настройка параметров ведения журнала учета СКЗИ. Удостоверяющие центры: настройка параметров работы с центрами сертификации MS CA, КриптоПро УЦ 2.0 и Валидата УЦ. КриптоПро DSS: настройка интеграции с ПАК КриптоПро DSS. AirCard Enterprise: настройка интеграции с сервером виртуальных смарт-карт Indeed AirCard Enterprise. Клиентский агент: настройка параметров работы клиентского агента Indeed CM.
---	--

Каталог пользователей: • Active Directory • КриптоПро УЦ 2.0 • Active Directory + КриптоПро УЦ 2.0	Определение каталога пользователей системы. Параметры подключения отображаются в зависимости от выбранного каталога.
• Соответствия атрибутов	Определение атрибутов, с которыми необходимо создать нового пользователя в Центре Регистрации КриптоПро УЦ 2.0 с использованием Indeed CM в момент выпуска устройства. Например: создать нового пользователя в ЦР КриптоПро с теми же значениями атрибутов, как и для существующего пользователя Active Directory.
• Обновляемые атрибуты	Определение списка атрибутов пользователя при изменении которых требуется обновление сертификата на устройстве.  Отслеживание изменений в атрибутах пользователей Active Directory доступно только для атрибутов из полей Субъект (Subject) и Дополнительное имя субъекта (Subject Alternative Name) сертификата.
Контроль доступа: • Администратор ролей	Определение параметров доступа к сервисам системы. Доступ к веб-приложениям Indeed CM предоставляется либо с использованием Аутентификации Windows (в случае, если сервер системы развернут на доменной рабочей станции под управлением ОС Windows), либо с использованием OpenID Connect сервера. Определение учетной записи для первоначальной настройки привилегий пользователей в разделе Роли Консоли управления Indeed Certificate Manager.  Указанная учетная запись должна иметь User Principal Name (UPN) и входить в выбранный каталог пользователей системы.
Хранилище данных: • Microsoft SQL или PostgreSQL • Ключ шифрования	Определение хранилища данных системы, алгоритма шифрования данных. Создание резервной копии ключа шифрования и восстановление ключа из копии. Параметры подключения к хранилищу определяются в зависимости от выбранного типа.
Служба Card Monitor	Служба Card Monitor предназначена для выполнения операций по контролю за обращением устройств (USB-токенов и смарт-карт) и выполняет:

- Отзыв и изъятие (опционально) устройств пользователей, чьи учетные записи были удалены из каталога пользователей системы
- Отзыв временных устройств с истекшим сроком действия
- Выключение (опционально) устройств пользователей, чьи учетные записи Active Directory были отключены
- Удаление учетных записей (опционально) из каталога пользователей системы, чьи учетные записи Active Directory были отключены
- Установку и сброс статуса содержимого устройства (истекает/истекло)
- Обновление содержимого устройств

 Card Monitor создает. Если обновление устройства проводилось через клиентский агент без автоматического одобрения сертификатов оператором УЦ. Администратор может обновить содержимое устройства без его перевыпуска или создать задачу на клиентском агенте, установленном на рабочей станции пользователя. Обновление содержимого устройства по умолчанию также доступно и пользователю в приложении **Сервис самообслуживания (Self Service)**.

- Регистрации события Длительное отсутствие связи с агентом в системный журнал
- Удаление агентов, которые были неактивны в течение настраиваемого периода времени
- Рассылку почтовых уведомлений администраторам и пользователям системы:
 - Истечение срока действия сертификатов пользователей, хранящихся на устройстве
 - Одобрение/отклонение выпуска устройства
 - Одобрение/отклонение обновления сертификатов на устройстве
 - Одобрение/отклонение замены устройства
 - Изменение политики, действующей на пользователя

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

Для работы Card Monitor в разделе **Роли** потребуются создать сервисную роль, включить в нее учетную запись, от имени которой будет работать Card Monitor и определить для роли привилегии:

	• Выключение устройства • Обновление устройства • Отмена обновления устройства • Отзыв устройства • Очистка устройства • Отмена назначения устройства • Удаление устройства • Выключение устройства КристоПро DSS • Обновление устройства КристоПро DSS • Отмена обновления устройства КристоПро DSS • Отзыв устройства КристоПро DSS • Удаление устройства КристоПро DSS • Удаление AirCard • Удаление агента • Удаление задачи • Удаление записи из журнала учета  Если настроена интеграция с КристоПро DSS и AirCard Enterprise, то задайте привилегии для работы с данными устройствами.
Подтверждение	Сводная информация по настройкам всех разделов Мастера. После нажатия кнопки Применить указанные значения для всех параметров будут записаны в файлы конфигурации всех приложений и сохранены в каталоги <code>C:\inetpub\wwwroot\cm\wizard\configs</code> для ОС Windows и <code>/opt/indeed/cm/wizard/configs/</code> для ОС Linux для дальнейшего их применения на сервере системы.
Результаты	Результат работы Мастера по записи указанных значений в файлы конфигурации сервисов системы. Файлы конфигурации можно выгрузить в архив (опция Сохранить файлы конфигурации) для переноса и применения настроек на сервере системы. При первой установке системы настройте необходимые параметры и сохраните их копию (опция Сохранить резервную копию параметров конфигурации в разделе Результаты). Резервная копия настроек включает в себя все параметры, определенные при установке системы для всех сервисов, а также алгоритм и ключ шифрования базы данных. При развертывании новых серверов системы используйте файл резервной копии, указав его в разделе Восстановление настроек Мастера настройки.  Файл резервной копии содержит данные сервисных учетных записей для работы с каталогом пользователей, и хранилищем данных, алгоритм и ключ шифрования базы данных системы. Храните файл резервной копии в защищенном месте.

Применение файлов конфигурации на сервере системы

Примените файлы конфигурации, созданные Мастером настройки на сервере (серверах) системы.

ОС Windows:

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

```
.\deploy_configuration.ps1
```

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

ОС Linux:

1. Откройте эмулятор терминала.
2. Перейдите в директорию */opt/indeed/cm/wizard/configs*.
3. Запустите скрипт *deploy_configuration.sh*, выполнив команду:

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

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



Рекомендуется указывать локальную учетную запись, от имени которой запускаются остальные веб-приложения системы.