

Создание сертификатов Агента

Для работы Агентов требуются сертификаты:

- **Indeed CM Agent CA** – корневой сертификат Агента Indeed CM. Используется для выдачи сертификатов рабочим станциям пользователей, на которых будут устанавливаться Агенты.
- **Indeed CM Agent SSL** – сертификат проверки подлинности, подписан корневым сертификатом. Необходим для установления двухстороннего 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, сервер Indeed CM проверяет подлинность сертификата после чего начинает доверять Агенту, установленному на рабочей станции пользователя, и готов передавать на него задачи.

Сертификаты Агента создаются при помощи утилиты **IndeedCM.Agent.Cert.Generator.exe**, входящей в состав дистрибутива Indeed CM (располагается в `IndeedCM.Server\Misc\AgentCertGenerator`).

1. Запустите в командной строке, запущенной от имени администратора, на сервере Indeed CM утилиту с параметрами: **IndeedCM.Agent.Cert.Generator.exe /root /csn /installToStore**. Дождитесь завершения работы утилиты.




Параметр **/csn** запускает процедуру выпуска сертификатов на DNS-имя рабочей станции, на которой запускается утилита. Для создания сертификатов для рабочей станции с другим именем запустите утилиту с параметром **/sn <DNS-имя рабочей станции>**.

Параметр **/installToStore** публикует выпущенные утилитой сертификаты в хранилища сертификатов сервера:


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

2. В каталоге с утилитой появятся файл **Indeed CM Agent CA.key**, содержащий отпечаток сертификата Indeed CM Agent CA и значение ключа сертификата.
3. Поместите сертификат **Indeed CM Agent CA** в **Доверенные корневые центры сертификации** (Trusted Root Certification Authorities) на всех рабочих станциях пользователей.

 Для распространения сертификата на рабочие станции пользователей удобно использовать механизм групповых политик Active Directory.

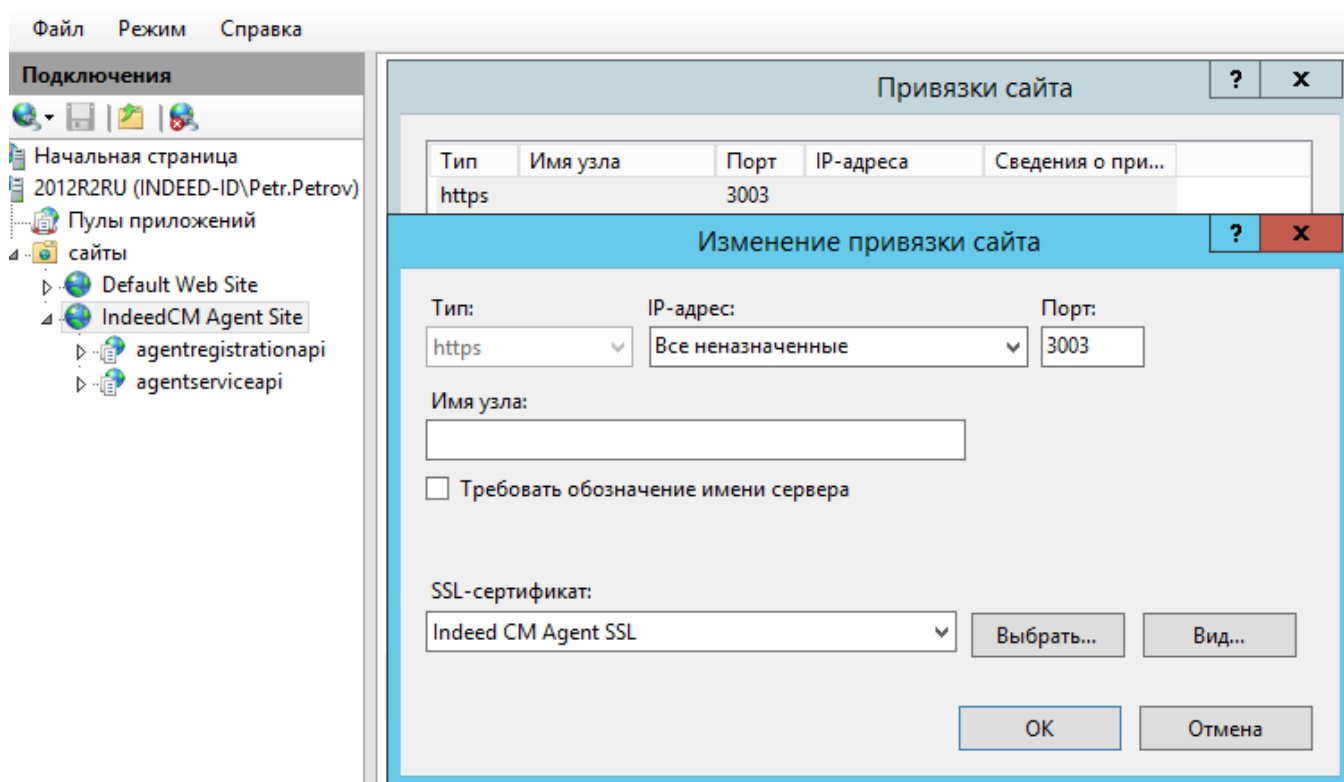
4. Настройте защищенное соединение с сайтом Агентов. Для этого:

- Перейдите в **Диспетчер служб IIS** (Internet Information Services (IIS) Manager).
- Выберите сайт **IndeedCM Agent Site** и перейдите в раздел **Привязки...** (Bindings...).
- Выберите привязку по порту **3003**.
- Нажмите **Изменить...** (Edit...).

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

- Укажите в качестве **SSL-сертификата** сертификат **Indeed CM Agent SSL** и нажмите **ОК**.

5. Пример настройки привязки для сайта IndeedCM Agent Site.



6. Если в вашем окружении используется несколько серверов Indeed CM с Агентами, то для каждого сервера потребуется свой SSL-сертификат Агента (корневой сертификат на всех серверах один и тот же). Для создания SSL-сертификата дополнительного сервера перенесите на него каталог с утилитой **IndeedCM.Agent.Cert.Generator.exe** и файл ключа корневого сертификата **Indeed CM Agent CA.key**, затем выполните команду:

```
IndeedCM.Agent.Cert.Generator.exe /ssl /csn /rootKey <путь к каталогу с ключом корневого сертификата> /installToStore
```

Пример:

```
IndeedCM.Agent.Cert.Generator.exe /ssl /csn /rootKey "C:\AgentCertGenerator\Indeed CM Agent CA.key" /installToStore
```