

Подключение к центру сертификации Microsoft через IndeedCM MSCA Proxy


Indeed Certificate Manager может взаимодействовать с центрами сертификации Microsoft, расположенными за пределами домена, в котором находится сервер Indeed CM.

Например, в конфигурации, когда у одной организации есть несколько независимых доменов с самостоятельными центрами сертификации в каждом, а Indeed CM развернут только в одном из этих доменов. При этом учетные записи пользователей в этих доменах одинаковы.


Использование компонента **IndeedCM.MSCA.Proxy** позволит запрашивать и записывать на устройства при помощи Indeed CM сертификаты со всех УЦ, находящихся за пределами того домена, в котором развернут Indeed CM. В такой схеме в политику использования устройств Indeed CM добавляется адрес MSCA Proxy, который развернут во внешнем домене с каталогом пользователей и центром сертификации. При выпуске устройства Indeed CM обращается к MSCA Proxy, а тот, используя сертификат Агента Регистрации (располагается в хранилище рабочей станции с установленным компонентом IndeedCM.MSCA.Proxy) передает запрос на целевой центр сертификации.

Для установки и настройки приложения MSCA Proxy выполните следующие действия:

1. Создайте во внешнем домене сервисную учетную запись для работы с центром сертификации Microsoft (см. [Создание сервисной учетной записи для работы с Microsoft CA](#)).
2. Настройте для сервисной учетной записи из п.1 шаблон Агент регистрации (см. [Настройка шаблонов сертификатов](#)) и выпустите для этой учетной записи сертификат по этому шаблону (см. [Выпуск сертификата Агент регистрации \(Enrollment Agent\)](#)).

 Сертификат **Агент регистрации** должен располагаться в **хранилище сертификатов рабочей станции (Local computer)**, на которой установлен компонент IndeedCM.MSCA.Proxy.

3. Установите компонент **IndeedCM.MSCA.Proxy.msi** из дистрибутива (распологающемся в каталоге IndeedCM.Server) на рабочей станции в домене с внешним УЦ.

 Системные требования для установки компонента совпадают с требованиями для установки сервера Indeed CM.

4. Перейдите в каталог **C:\inetpub\wwwroot\mscaproxy** и откройте в редакторе Блокнот, запущенном от имени администратора, файл **Web.config**.

5. Укажите в секции **caProxySettings**:

- Имя центра сертификации в параметре **ca**.
- Данные учетной записи (логин и пароль), обладающей сертификатом **Агент регистрации** в параметрах **userName** и **password** соответственно.
- **Отпечаток** (Thumbprint) сертификата **Агент регистрации** в параметре **enrollmentAgentCertificateThumbprint**.

Пример заполненной секции:

```
<caProxySettings ca="servercm.external.com\EXTERNAL-CA" userName="EXTERNAL\service" password="p@ssw0rd" enrollmentAgentCertificateThumbprint="dbd1859d27395860843643ebe17e2ee3fc463aba"/>
```

6. В секции **authorization** в параметре **allow users** также укажите сервисную учетную запись для работы с центром сертификации.

Пример заполненной секции:

```
<authorization>
  <deny users="?" />
  <allow users="EXTERNAL\service" />
  <deny users="*" />
</authorization>
```

7. **Сохраните** изменения в файле.