Каталог в Active Directory

Выдайте сервисной учетной записи (например, **servicecm**) необходимые права для работы с объектом (доменом, контейнером, подразделением), в котором будут располагаться пользователи Indeed Certificate Manager. Эта учетная запись будет использоваться для чтения и записи атрибутов пользователей.

Для этого выполните следующее:

1. Откройте свойство **Безопасность** (Security) объекта (домена, контейнера или подразделения), в котором содержатся пользователи системы Indeed CM.
2. Выберите сервисную учетную запись (servicecm) и нажмите **Изменить** (Edit).
3. Выберите область применения **Дочерние объекты: Пользователь** (Descendant User objects).
4. Поставьте разрешение напротив **Прочитать все свойства** (Read all properties) в списке **Свойств** (Properties).
5. Также в списке **Свойств** (Properties) отметьте пункты:

   - **Запись: pwdLastSet** (Write: pwdLastSet)
   - **Запись: thumbnailPhoto** (Write: thumbnailPhoto) или **Запись: jpegPhoto** (Write: jpegPhoto)
   - **Запись: userAccountControl** (Write: userAccountControl)
   - **Запись: userCertificate** (Write: userCertificate)

6. В списке **Разрешений** (Permissions) отметьте **Сброс пароля** (Reset password).
7. Нажмите **ОК** и затем **Применить** (Apply).

> Установите одинаковый набор прав сервисной учетной записи для каждого объекта (домена, контейнера или подразделения) в котором располагаются пользователи Indeed CM.

По умолчанию разрешение на чтение всех свойств пользователя есть у всех учетных записей домена. Если в домене чтение всех свойств пользователя запрещено политиками безопасности, то выдайте сервисной учетной записи права на чтение только необходимых атрибутов по Таблице 3.
При настройке разрешений на чтение свойств пользователей, отличных от значений по умолчанию, необходимо выдать разрешения сервисной учетной записи (**servicecm**) и на чтение значений атрибутов объекта (домена, контейнера или подразделения), в котором содержатся пользователи Indeed CM. Это атрибуты **cn**, **objectGUID**, **name** и **showInAdvancedViewOnly**.

Приведены отображаемые имена **LDAP** (LDAP Display Name).

Предоставление прав доступа к набору свойств значительно улучшает производительность и упрощает управление безопасностью (см. **Наборы свойств Active Directory**).

Таблица 3 – Атрибуты, используемые Indeed CM при работе с каталогом пользователей.

Атрибут (LDAP Display Name)	Common Name	Комментарий
c	Country/Region Abbreviation или Country/Region Name	Входит в набор свойств «Личные данные» (Personal Information).
cn	Common Name	Входит в набор свойств «Публичная информация» (Public Information).
company	Company	Входит в набор свойств «Публичная информация» (Public Information).
department	Department	Входит в набор свойств «Публичная информация» (Public Information).
objectGUID	ObjectGUID	Входит в набор свойств «Публичная информация» (Public Information).
givenName	Given Name	Входит в набор свойств «Публичная информация» (Public Information).
l	Locality Name	Входит в набор свойств «Личные данные» (Personal Information).
mail	E-mail Addresses	Входит в набор свойств «Публичная информация» (Public Information).
manager	Manager	Входит в набор свойств «Публичная информация» (Public Information).
sAMAccountName	SAM Account Name	Входит в набор свойств «Общие сведения» (General Information).
sn	Surname	Входит в набор свойств «Публичная информация» (Public Information).
st	State or Province Name	Входит в набор свойств «Личные данные» (Personal Information).
streetAddress	Address (или Street)	Входит в набор свойств «Личные данные» (Personal Information).

telephoneNumber	Telephone Number	Входит в набор свойств «Личные данные» (Personal Information).
thumbnailPhoto или **jpegPhoto**	Picture	Входит в набор свойств «Личные данные» (Personal Information).
userAccountControl	User Account Control	Входит в набор свойств «Ограничения учетной записи пользователя» (User Account Restrictions).
userPrincipalName	User Principal Name	Входит в набор свойств «Публичная информация» (Public Information).