# Каталог в Active Directory

## Создание сервисной учетной записи для работы с хранилищем данных

Для полноценной работы системы Indeed Certificate Manager необходимо наличие определенных прав доступа к объектам Active Directory. В соответствии с принятой в вашей компании политикой безопасности, вы можете распределить привилегии между несколькими сервисными учетными записями, либо создать сервисную учетную запись с максимальным набором прав на управление системой.

Создайте сервисную учетную запись (например, **servicecm**), от имени которой будут выполняться операции сохранения и чтения данных в хранилище Active Directory.

Настройка каталога пользователей в Active Directory

Выдайте созданной сервисной учетной записи (**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. Нажмите **Дополнительно** (Advanced). Нажмите кнопку **Добавить** (Add). Щелкните **Выбрать субъект** (Select a principal).
3. В текстовом поле **Введите имена выбираемых объектов** (Enter the object name to select) введите имя сервисной учетной записи (**servicecm**) и нажмите **ОК**.
4. В поле со списком **Применяется к** (Applies to) выберите **Дочерние объекты: Пользователь** (Descendant User objects).
5. В списке **Разрешений** (Permissions) отметьте **Сброс пароля** (Reset password).
6. В списке **Свойств** (Properties) поставьте разрешение напротив **Прочитать все свойства** (Read all properties).
7. 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)

8. 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**<br>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). |