Каталог в Active Directory

Создание сервисной учетной записи для работы с каталогом пользователей Active Directory и хранилищем данных системы

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) поставьте разрешение напротив:
   - **Список содержимого** (List contents).
   - **Прочитать все свойства** (Read all properties).

     > По умолчанию разрешение на чтение всех свойств пользователя имеется у всех учетных записей домена.

   - **Сброс пароля** (Reset password) - Требуется для возможности **Сброса пароля пользователя** через интерфейс системы.
6. В списке **Свойств** (Properties) отметьте пункты:
   - **Запись: pwdLastSet** (Write pwdLastSet) - Также требуется для возможности сброса пароля пользователя.
   - **Запись: thumbnailPhoto** (Write thumbnailPhoto) или **Запись: jpegPhoto** (Write jpegPhoto) - Требуется для возможности Загрузки фотографии пользователю в Active Directory через интерфейс системы.
   - **Запись: userAccountControl** (Write userAccountControl) - Необходима для работы опции **Требовать логон по смарт-карте**.
   - **Запись: userCertificate** (Write userCertificate) - Требуется для возможности **Публиковать сертификат КриптоПро 2.0** в профиль пользователя Active Directory.
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.

Если в домене чтение всех свойств пользователя запрещено политиками безопасности, то выдайте сервисной учетной записи права на чтение только необходимых атрибутов пользователей, описанных ниже в таблице и атрибутов объекта (домена, контейнера или подразделения), в котором располагаются пользователи Indeed CM.

1. В оснастке **Редактирование ADSI** (ADSI edit) откройте свойство **Безопасность** (Securit y) объекта (домена, контейнера или подразделения), в котором содержатся пользователи системы Indeed CM.
2. Для области применения **Этот объект и все дочерние объекты** (This object and all descendant objects).
   - В списке **Разрешений** (Permissions) отметьте **Список содержимого** (List contents).
   - В списке **Свойств** (Properties) отметьте пункты:
     - **Чтение: canonicalName** (Read canonicalName)
     - **Чтение: Distinguished Name** (Read Distinguished Name)
     - **Чтение: objectClass** (Read objectClass)
     - **Чтение: objectGuid** (Read objectGuid)
     - **Чтение: showInAdvancedViewOnly** (Read showInAdvancedViewOnly)
3. Для области применения **Дочерние объекты: Пользователь** (Descendant user objects).
   - В списке **Разрешений** (Permissions) отметьте **Список содержимого** (List contents).
   - В списке **Свойств** (Properties) выберите чтение/запись следующих наборов свойств и атрибутов, соответствующих таблице:
     - **Чтение: личные сведения** (Read personal Information)
     - **Чтение: общие сведения** (Read general Information)
     - **Чтение: ограничения учетной записи** (Read account restrictions)
     - **Чтение: открытые сведения** (Read public Information)
     - **Запись: pwdLastSet** (Write pwdLastSet)
     - **Запись: thumbnailPhoto** (Write thumbnailPhoto) или **Запись: jpegPhoto** (Wri te jpegPhoto)
     - **Запись: userAccountControl** (Write userAccountControl)
     - **Запись: userCertificate** (Write userCertificate)

> 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).

Атрибуты, используемые Indeed CM при работе с каталогом пользователей.

Атрибут (LDAP Display Name)	Common Name	Комментарий

c	Country/Region или Country /Region Abbreviation	Входит в набор свойств «Личные сведения» (Personal Information).
canonicalName	Canonical Name	Входит в набор свойств «Открытые сведения» (Public Information).
cn	Common Name	Входит в набор свойств «Открытые сведения» (Public Information).
company	Company	Входит в набор свойств «Открытые сведения» (Public Information).
department	Department	Входит в набор свойств «Открытые сведения» (Public Information).
distinguishedName	Distinguished Name	Входит в набор свойств «Открытые сведения» (Public Information).
givenName	Given Name	Входит в набор свойств «Открытые сведения» (Public Information).
l	Locality Name	Входит в набор свойств «Личные сведения» (Personal Information).
mail	E-mail Addresses	Входит в набор свойств «Открытые сведения» (Public Information).
manager	Manager	Входит в набор свойств «Открытые сведения» (Public Information).
objectClass	Object Class	Входит в набор свойств «Открытые сведения» (Public Information).
objectGUID	Object GUID	Входит в набор свойств «Открытые сведения» (Public Information).
objectSid	Object Sid	Входит в набор свойств «Общие сведения» (General Information).
otherMailbox	Other Mailbox	Входит в набор свойств «Открытые сведения» (Public Information).
proxyAddresses	Proxy Addresses	Входит в набор свойств «Открытые сведения» (Public Information).
pwdLastSet	Pwd Last Set	Входит в набор свойств «Ограничения учетной записи» (Account Restrictions).
sAMAccountName	SAM Account Name	Входит в набор свойств «Общие сведения» (General Information).
sn	Surname	Входит в набор свойств «Открытые сведения» (Public Information).
st	State or Province Name	Входит в набор свойств «Личные сведения» (Personal Information).
streetAddress	Address (или Street)	Входит в набор свойств «Личные сведения» (Personal Information).

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