# Indeed-Id
# FIM Connector

Руководство по установке и настройке



8 (800) 333-09-06
телефон бесплатной горячей линии

ООО Индид
ИНН/КПП 7801540219/780601001, ОГРН 1117847053103

8 (800) 333-09-06 или support@indeed-id.com
служба поддержки пользователей

http://indeed-id.ru/
web-сайт компании

Версия 1.0.2

## Олгавление

# Введение

Приветствуем вас и благодарим за приобретение программных продуктов компании Indeed. Данное руководство описывает способ настройки интеграции систем Indeed-Id Enterprise Authentication/Indeed Enterprise Single Sign-On с системой Microsoft Forefront Identity Manager (FIM) 2010 R2.

# Условные обозначения

В Руководстве используются следующие условные обозначения:

**Важная информация**. Разделы, содержащие важную информацию, необходимую для успешной работы.

**Дополнительная информация**. Разделы, содержащие дополнительную информацию.

# О продукте Indeed-Id FIM Connector

Indeed-Id Enterprise SSO является программным продуктом, решающим задачи single sign-on систем:

- унификация процедуры доступа для конечных пользователей
- централизация управления доступом в руках it-служб
- автоматизация процедуры ввода паролей в конечные приложения
- избавление пользователей от необходимости помнить пароли

Внедрение системы single sign-on является важным, но далеко не единственным шагом на пути построения системы эффективного управления доступом. Важную роль в этом процессе играет интеграция системы single sign-on с системой управления учетными данными (Identity Management или сокращенно IDM).

Коннектор к IDM системе позволяет в автоматическом режиме синхронизировать учетные данные пользователей в БД сервера Indeed Enterprise Server. Учетные данные создаются при помощи IDM-коннекторов и тут же сохраняются в системе Indeed Enterprise SSO, избавляя сотрудника от запоминания и ручного ввода паролей.

В данном документе изложены возможности интеграции продукта Indeed Enterprise SSO с системой Microsoft Forefront Identity Manager 2010 (FIM), а также описываются основные преимущества, получаемые за счет совместного использования указанных решений.

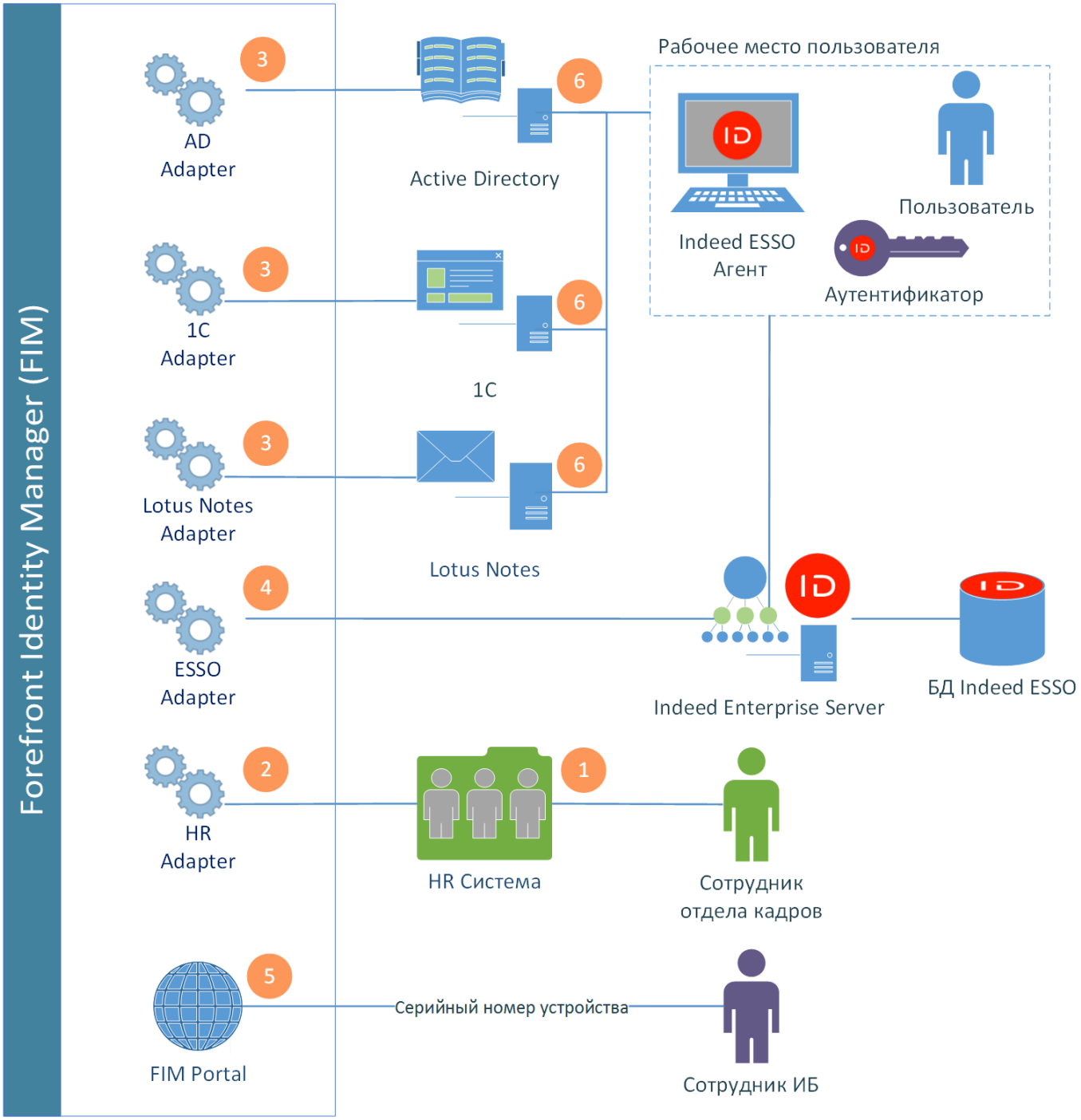
# Цели интеграции Indeed-Id Enterprise SSO с FIM 2010

1. Повышение уровня информационной безопасности компании за счет полной автоматизации жизненного цикла паролей пользователей (пароли создаются, изменяются и вводятся полностью в автоматическом режиме, без участия пользователей и администраторов)
2. Минимизация шагов в предоставлении и получении доступа сотрудниками. После занесения нового пользователя в исходную систему (например, HR-систему) и выполнения синхронизации (в автоматическом режиме), пользователь получает беспарольный доступ во все необходимые ему системы.

3. В случае использования аппаратных средств аутентификации, вынесении операции добавления аутентификатора в БД Indeed-Id ESSO на сторону портала FIM (в результате чего, участие пользователя, как правило, не требуется).

## Схема интеграции Indeed Enterprise SSO с FIM 2010

Рассмотрим схему работы на примере бизнес-операции принятия нового сотрудника на работу и использования для аутентификации при доступе к рабочему столу USB-ключа. Весь процесс можно условно разделить на 6 крупных шагов.



1. Сотрудник отдела кадров регистрирует запись о новом сотруднике в системе учета персонала (HR система).

2. После этого, данные о новом сотруднике попадают в базу данных FIM через адаптер к HR системе.

3. На основе этого события FIM выполняет операцию синхронизации, создавая для пользователя учетные записи во всех приложениях, согласно должности (бизнес-роли) сотрудника. Для данной операции используются специальные адаптеры.

4. Indeed-Id Microsoft Forefront 2010 Connector на заключительном шаге синхронизации создает профиль доступа сотрудника в БД Indeed-Id Enterprise SSO, копируя в него учетные данные пользователя.

5. Дополнительно к учетным данным пользователя, в базе Indeed-Id ESSO, может быть зарегистрирован аппаратный аутентификатор пользователя. Таким аутентификатором, например, может являться USB-ключ (eToken, ruToken и т.п.). Серийный номер ключа сотрудник информационной безопасности заносит через интерфейс специальной формы на портале FIM. Серийный номер ключа регистрируется в БД Indeed-Id ESSO в качестве аутентификатора сотрудника.

*Примечание*: Шаг 5 может быть пропущен, если аутентификация с использованием ключа не требуется (например, сохраняется стандартная схема ввода логин-пароля учетной записи Active Directory).

6. На данном шаге сотрудник имеет все необходимое для работы. Для доступа к рабочему столу он указывает имя своей доменной учетной записи, подключает USB-ключ и вводит PIN-код ключа. После выполнения успешной аутентификации, Indeed-Id Enterprise SSO Агент обеспечивает для сотрудника прозрачный доступ во все необходимые приложения, подставляя учетные данные пользователя в формы входа в приложения.

Таким образом, Indeed-Id FIM Connector реализует следующие функции:

1. Создание учетной записи Indeed-ID
2. Создание и заполнение профиля ESSO учетной записи Indeed-Id
3. Добавления аутентификатора (eToken PASS) для учетной записи Indeed-Id
4. Удаление учетной записи Indeed-Id и ее ESSO профиля

# Компоненты Indeed-Id FIM Connector

В состав модуля **Indeed-Id FIM Connector** входят следующие компоненты:

- IndeedID.server.helper.dll и IndeedID.server.helper.host.exe – компоненты, обеспечивающие связь коннектора с Indeed-Id Enterprise Server. Устанавливаются на рабочую станцию с компонентом FIM Sync Service.
- IndeedID.SSO.MA.dll, Interop.IndeedIDServerHelperLib.dll, Interop.IndeedIDServerHelperHostLib.dll – компоненты, обеспечивающие возможность создания учетных записей Enterprise SSO в Microsoft Forefront Identity Manager. Установка всех компонентов выполняется на рабочую станцию с компонентом FIM Sync Service.
- Indeed-Id Extended Security Provider – компонент, позволяющий участникам группы безопасности Indeed-Id Enrolment Admins обучать и удалять аутентификаторы любых пользователей, не выполняя вход в систему. Установка Indeed-Id Extended Security Provider выполняется на Indeed-Id Server.

# Установка компонентов Indeed-Id FIM Connector

## Предварительные условия для установки

Для корректной установки Indeed-Id FIM Connector должны быть выполнены следующие требования:

- Установлены и запущены все экземпляры Indeed-Id Enterprise Server
- На каждом сервере Indeed установлен набор требуемых провайдеров аутентификации Indeed-Id
- Установлены и настроены компоненты ESSO:
    - Indeed-Id ESSO Management Console на рабочих местах администраторов (с настройкой целевых приложений)
    - Indeed-Id ESSO Agent на рабочих станциях пользователей

## Порядок установки

Установка компонент Indeed-Id FIM Connector выполняется в следующем порядке:

1. Установка Indeed-Id Extended Security Provider на каждый Indeed-Id Server и создание группы безопасности Indeed-Id Enrolment Admins.
2. Установка и настройка компонентов Indeed-Id FIM Connector на сервер FIM Sync Service.
3. Создание сервисной учетной записи, от имени которой будет работать сервис IndeedID.server.helper.host.exe и назначение ей прав Indeed-ID Enrolment Admins и Indeed-ID User Admins
4. Создание и настройка Агента управления (Management Agent)

### Установка Indeed-Id Extended Security Provider

Для получения подробной информации обратитесь к Руководству по установке Indeed-Id Extended Security Provider.

### Установка и настройка компонентов Indeed FIM Connector

Для установки **IndeedID.server.helper.dll** выполните следующие действия:

1. Скопируйте компонент IndeedID.server.helper.dll из каталога дистрибутива на рабочую станцию, где установлен FIM Sync Service.
2. Выполните регистрацию компонента при помощи утилиты Windows regsvr32.exe. Откройте командную строку Windows и выполните команду:
   ***C:\|Windows\|SysWOW64\|regsvr32 IndeedID.server.helper.dll*** – для 64-битных ОС
   ***C:\|Windows\|System32\|regsvr32 IndeedID.server.helper.dll*** – для 32-битных ОС

Для установки **IndeedID.server.helper.host.exe** выполните следующие действия:

1. Скопируйте компонент IndeedID.server.helper.host.exe из каталога дистрибутива на рабочую станцию, где установлен FIM Sync Service.
2. Выполните регистрацию компонента. Откройте командную строку Windows и выполните команду вида <путь к компоненту IndeedID.server.helper.host.exe> -regserver. **Пример: C:\Users\Administrator\Desktop>IndeedID.server.helper.host.exe -regserver**

Настройте права запуска и доступа к компоненту IndeedID.server.helper.host.exe. Для этого выполните следующие действия:

1. Откройте оснастку **Службы компонентов** (Component Services) на рабочей станции с зарегистрированным компонентом IndeedID.server.helper.host.exe.
2. Найдите в дереве зарегистрированный компонент: **Службы компонентов** (Component Services) -> **Компьютеры** (Computers) -> **Мой компьютер** (My Computer) -> **Настройка DCOM** (DCOM Config) -> **Indeed-Id Server Helper Host**.
3. Откройте вкладку **Безопасность** (Security) в свойствах компонента.
4. В разделе **Разрешения на запуск и активацию** (Launch and Activation Permissions) добавьте учетную запись пользователя, от имени которой работает FIM Sync Service и определите для неё разрешения на **Локальный запуск** (Local Launch) и **Локальную активацию** (Local Activation).
5. В разделе **Разрешения на доступ** (Access Permissions) добавьте учетную запись пользователя, от имени которой работает FIM Sync Service и определите для неё разрешение на **Локальный доступ** (Local Access).
6. Скопируйте компоненты **IndeedID.SSO.MA.dll**, **Interop.IndeedIDServerHelperLib.dll** и **Interop.IndeedIDServerHelperHostLib.dll** из каталога дистрибутива в каталог %ProgramFiles%\Microsoft Forefront Identity Manager\2010\Synchronization Service\Extensions.

### Создание сервисной учетной записи

Создайте сервисную учетную запись, от имени которой будет работать компонент IndeedID.server.helper.host.exe. Для этого выполните следующие действия:

1. Создайте доменного пользователя с произвольным именем (например, indeedFIMservice).
2. Добавьте созданного пользователя в группы: Indeed-ID User Admins и Indeed-ID Enrolment Admins.
3. Запустить оснастку **Службы компонентов** (Component Services) на рабочей станции с

зарегистрированным компонентом IndeedID.server.helper.host.exe.

4. Найдите в дереве зарегистрированный компонент: **Службы компонентов** (Component Services) -> **Компьютеры** (Computers) -> **Мой компьютер** (My Computer) -> **Настройка DCOM** (DCOM Config) -> **Indeed-Id Server Helper Host**.
5. Откройте вкладку **Удостоверение** (Identity) в свойствах компонента, выберите **Указанный пользователь** (This User) и укажите учетную запись пользователя, созданную в п. 1.

### Создание и настройка Агента управления (Management Agent)

Указания по настройке Агента управления:

1. Запустите Synchronization Service Manager и перейдите в раздел Management Agents.
2. В меню Actions выберите пункт Create.
3. В окне создания Management Agent в разделе Create Management Agent выполните следующее (Рисунок 1):
    a. В списке Management agent for выберите **Extensible Connectivity**;
    b. Задайте имя Management Agent и описание;
    c. В списке Architecture выберите **Process**;
    d. Нажмите Next.

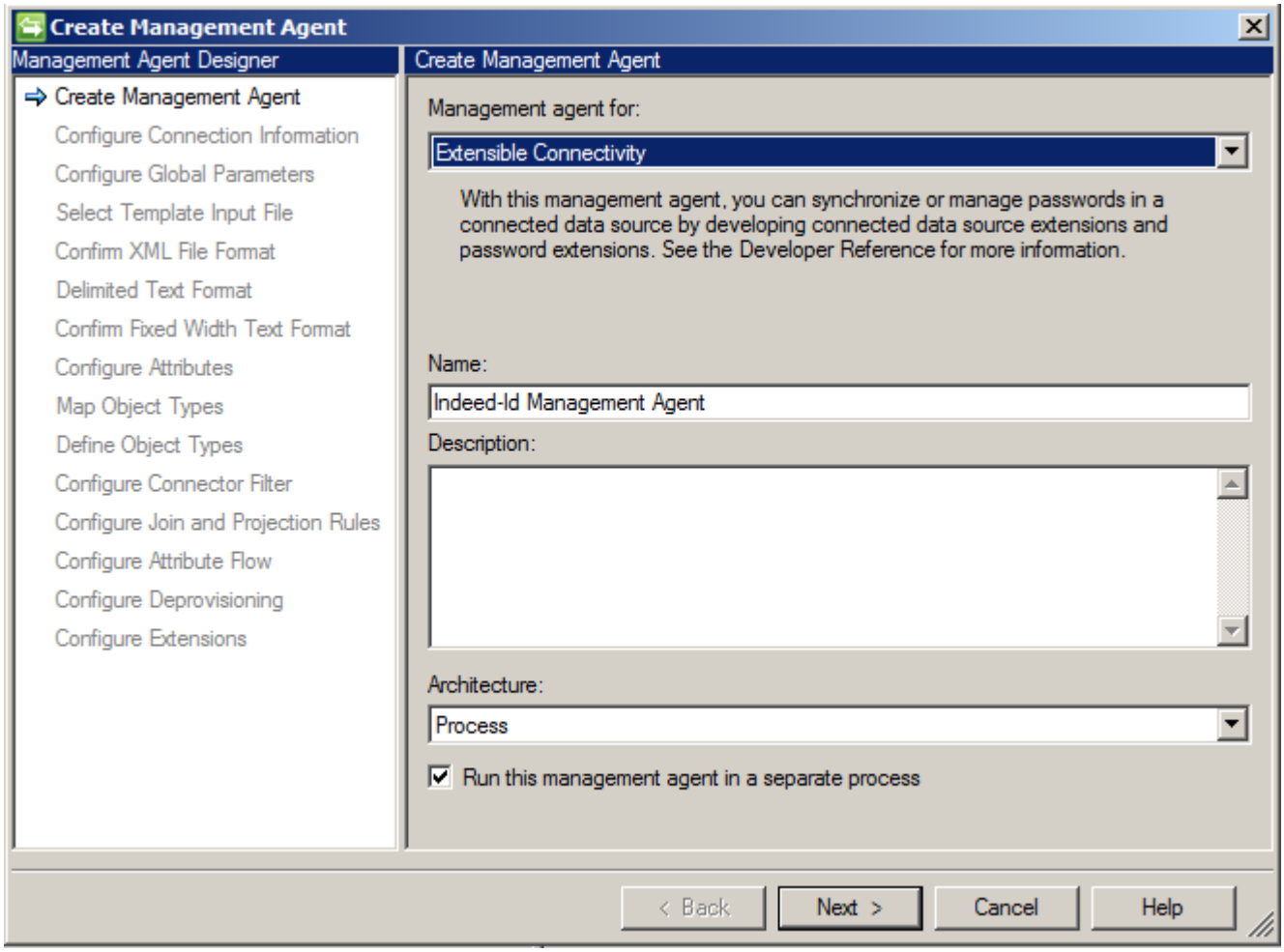



Рисунок 1.

4. В окне создания Management Agent в разделе Configure Connection Information выполните следующее (Рисунок 2):
    a. В списке поддерживаемых интерфейсов выберите **Import and Export**;
    b. В качестве типа режима экспорта выберите **Call-based**;

c. Укажите файл **IndeedID.SSO.MA.dll** (входит в состав дистрибутива Indeed-Id FIM Connector) в поле Connected data source extension name;
d. Нажмите Next.

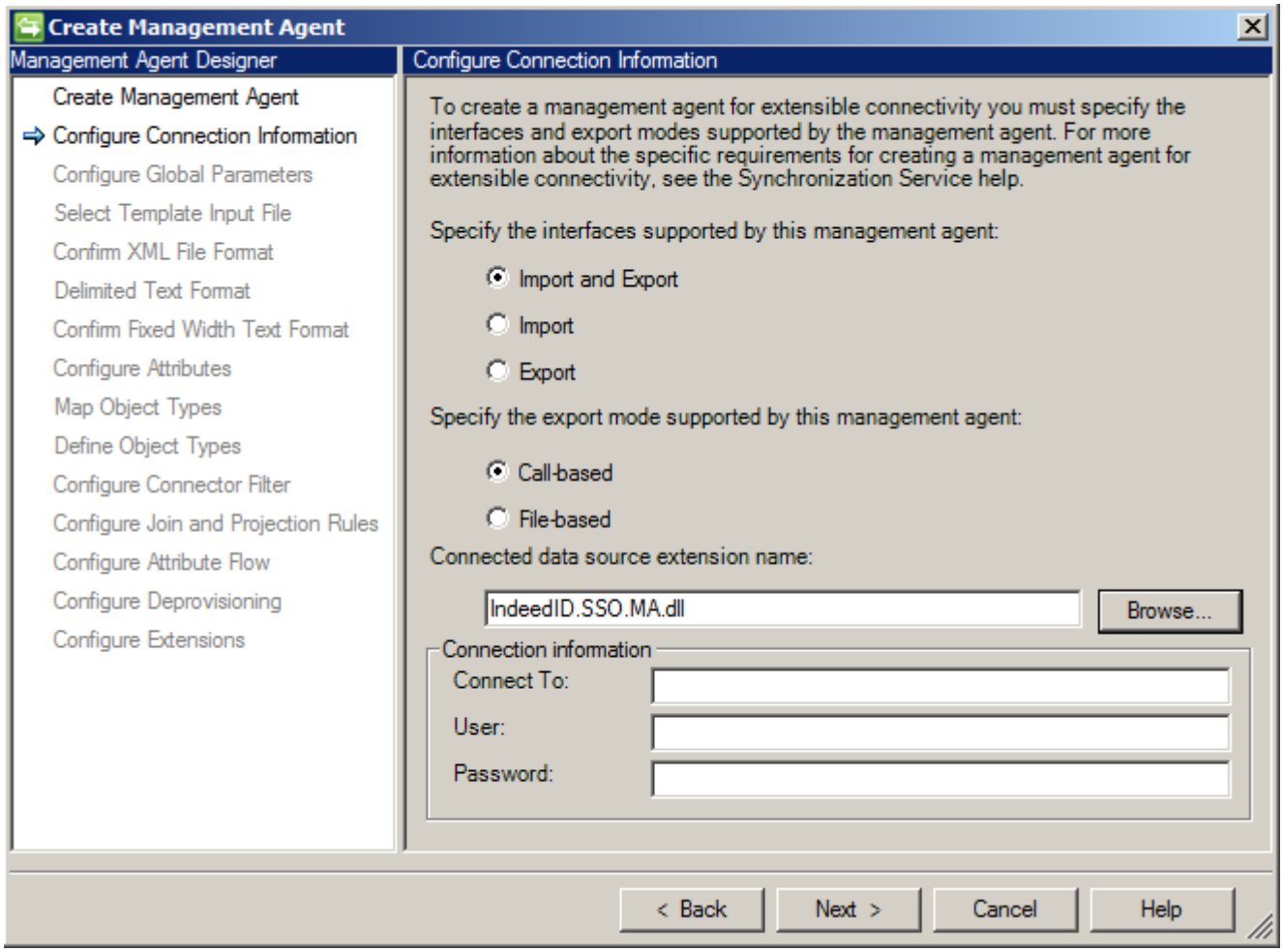



Рисунок 2.

5. В окне создания Management Agent в разделе Configure Global Parameters выполните настройку следующих параметров (Рисунок 3):
   a. Путь к экземпляру системы Indeed-Id в домене.
      Параметр: **rootPath**.
      Значение: строка, содержащая путь к экземпляру системы (например, для экземпляра системы Indeed-Id в корне домена indeed-id.local значение параметра rootPath будет dc=indeed-id,dc=local). Является обязательным параметром.
   b. Идентификатор провайдера, для которого будет автоматически обучаться аутентификатор пользователя (на данный момент поддерживается только провайдер eToken Pass).
      Параметр: **providerId**.
      Значение: EA588135-CED1-4922-B640-924C94A91904. Является обязательным параметром.
   c. Имя компании, используемое в имени контейнера экземпляра системы Indeed-Id в домене (для случая, когда экземпляр системы создан в формате company\product).
      Параметр: **companyName**.
      Значение: строка с именем компании (пустая строка в случае экземпляра системы с именем Indeed-ID).

d. Имя продукта, используемое в имени подконтейнера экземпляра системы Indeed-Id в домене (для случая, когда экземпляр системы создан в формате company\product).
   Параметр: **productName**.
   Значение: строка с именем продукта (в случае экземпляра системы с именем Indeed-ID, значение параметра следует задать Indeed-ID).
e. Захват лицензии Indeed-Id Windows Logon.
   Параметр: **takeLfwLicense**.
   Значение: 1 – захватывать, 0 – нет.
f. Захват лицензии Indeed-Id Enterprise SSO.
   Параметр: **takeEssoLicense**.
   Значение: 1 – захватывать, 0 – нет.
g. Включение опции "Генерировать случайный пароль Active Directory".
   Параметр: **generateRandomPassword**.
   Значение: 1 – генерировать, 0 – нет.

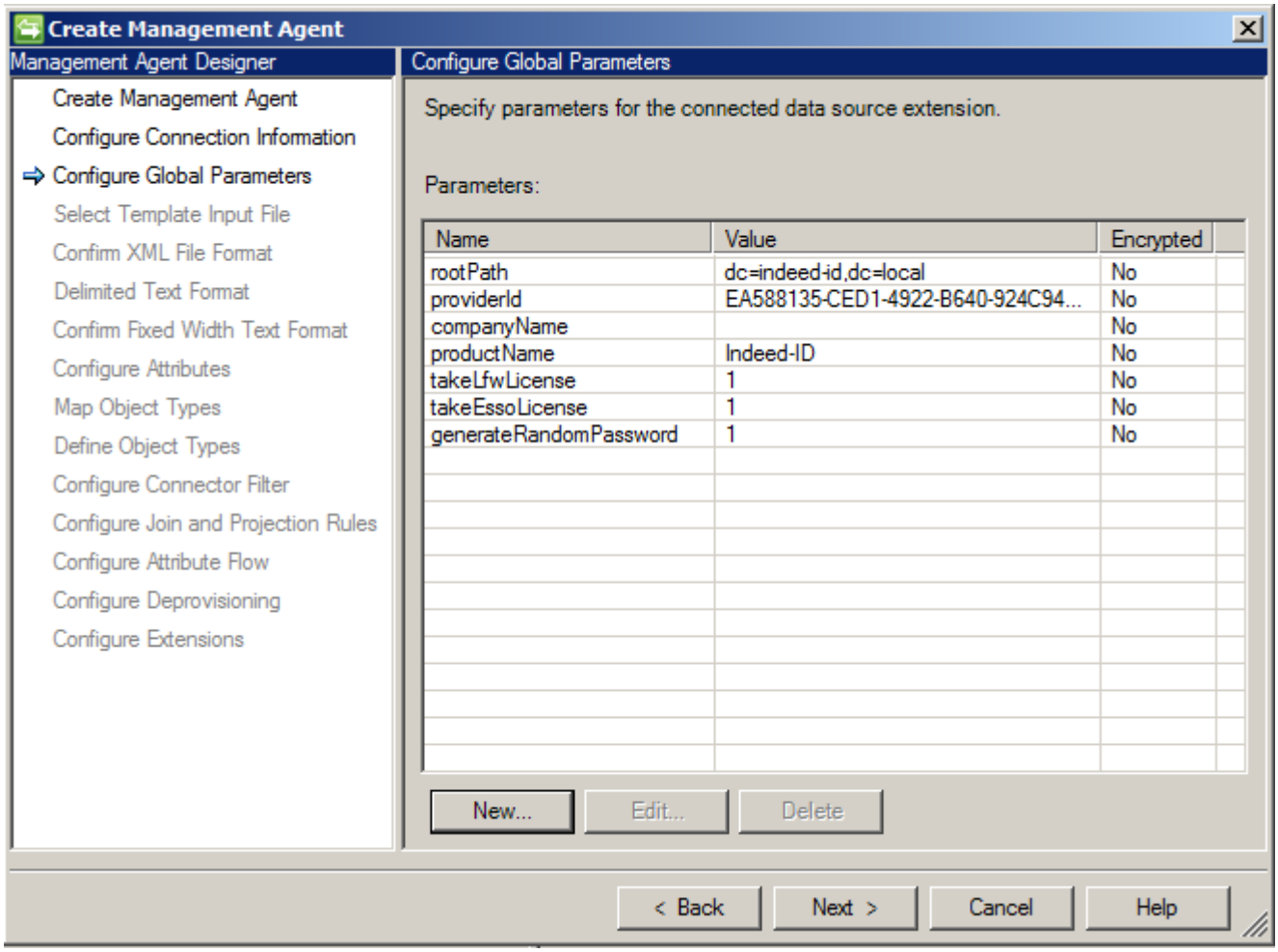



Рисунок 3.

6. В окне создания Management Agent в разделе Select Template Input File выполните следующее (Рисунок 4):
   a. Укажите путь до файла **scheme.txt** (входит в состав дистрибутива Indeed-Id FIM Connector) в поле Template Input File;
   b. Выберите Unicode в качестве Code Page;
   c. Укажите AVP в качестве File format;
   d. Нажмите Next.

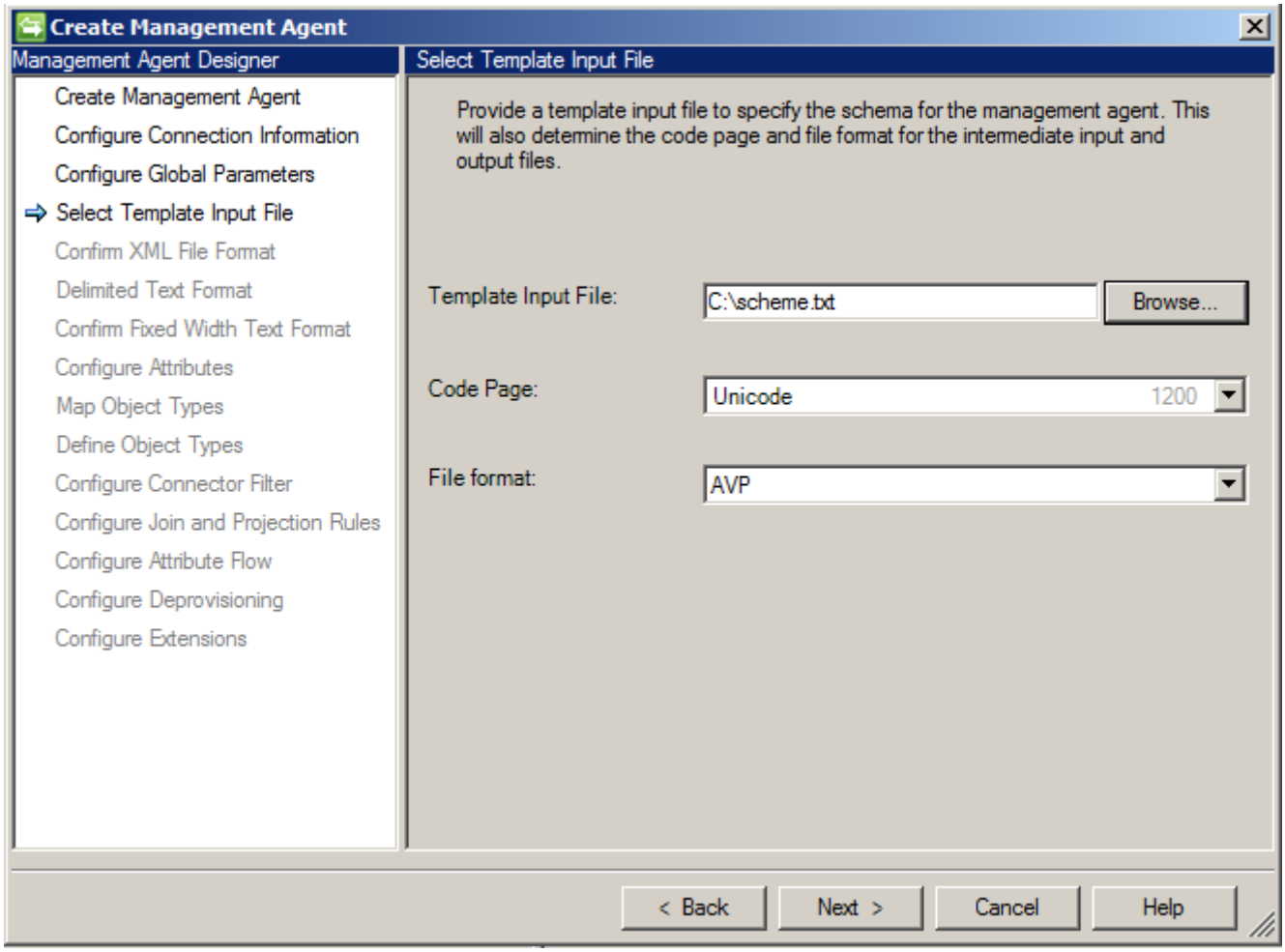



Рисунок 4.

7. В окне создания Management Agent в разделе Configure Attributes выполните следующее:
   a. Нажмите кнопку Set Anchor… и выберите в качестве якоря атрибут id;
   b. Нажмите кнопку Advanced…. В открывшемся окне в разделе Define object class выберите опцию Object class attribute и укажите атрибут objectType в качестве определяющего атрибута. Нажмите ОК (Рисунок 5а).

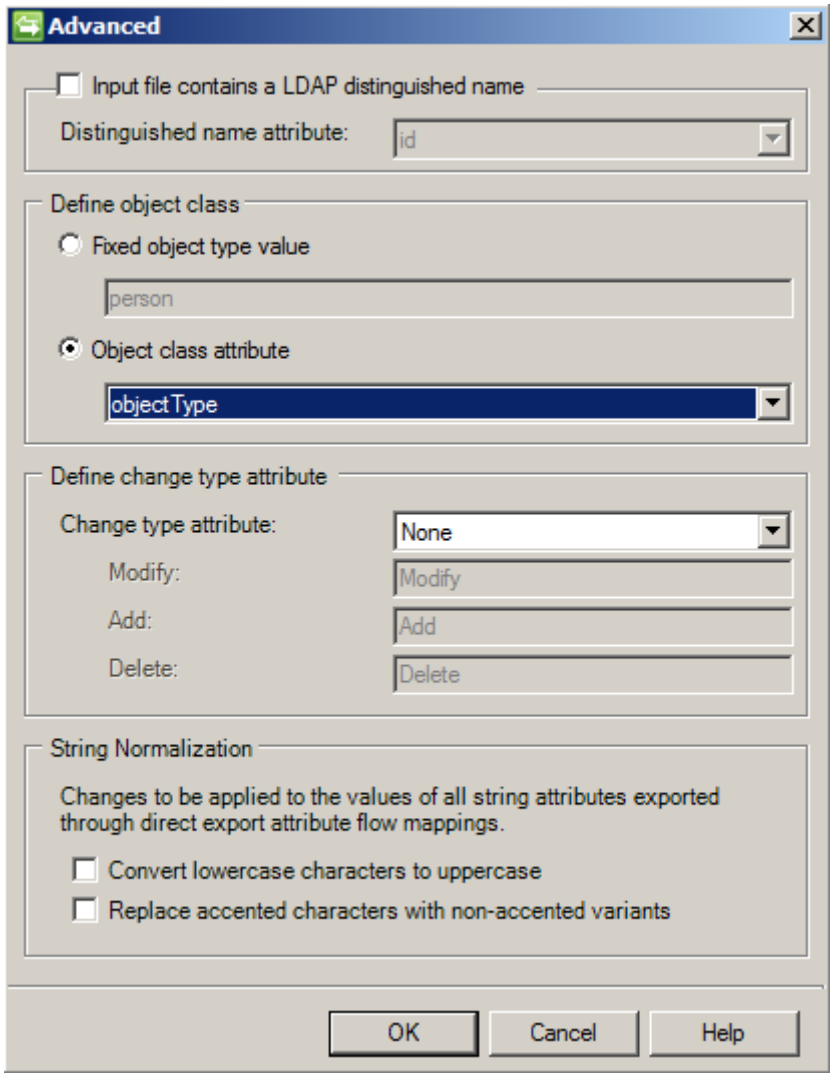



Рисунок 5a.

c. Выберите атрибут userRef и нажмите кнопку Edit…
d. В открывшемся окне измените тип атрибута со String на Reverence (DN). Нажмите OK (Рисунок 5b).

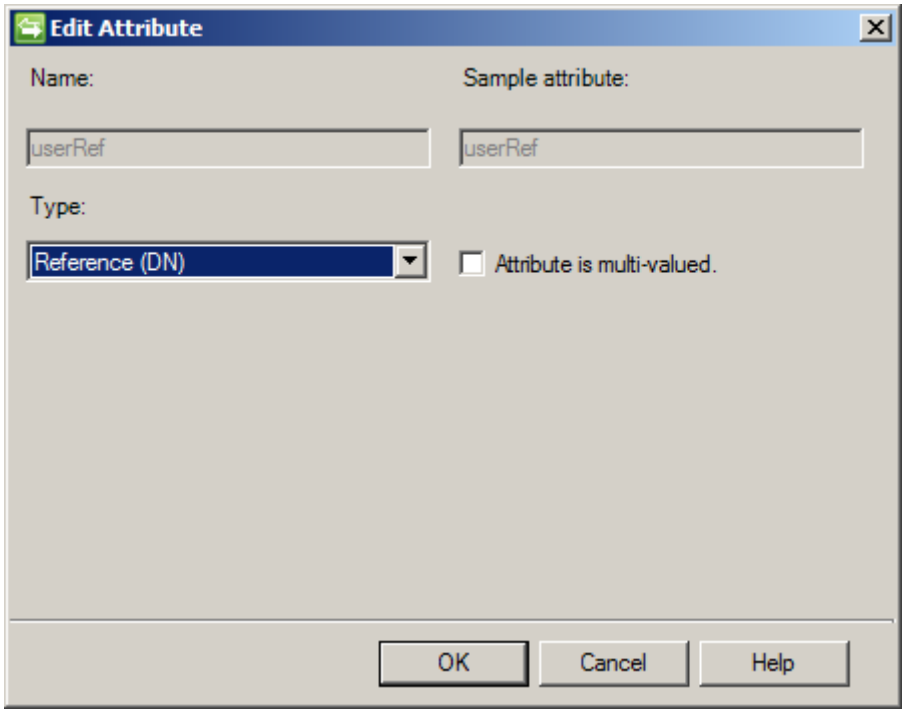



Рисунок 5b.

e. Нажмите Next (Рисунок 5c).

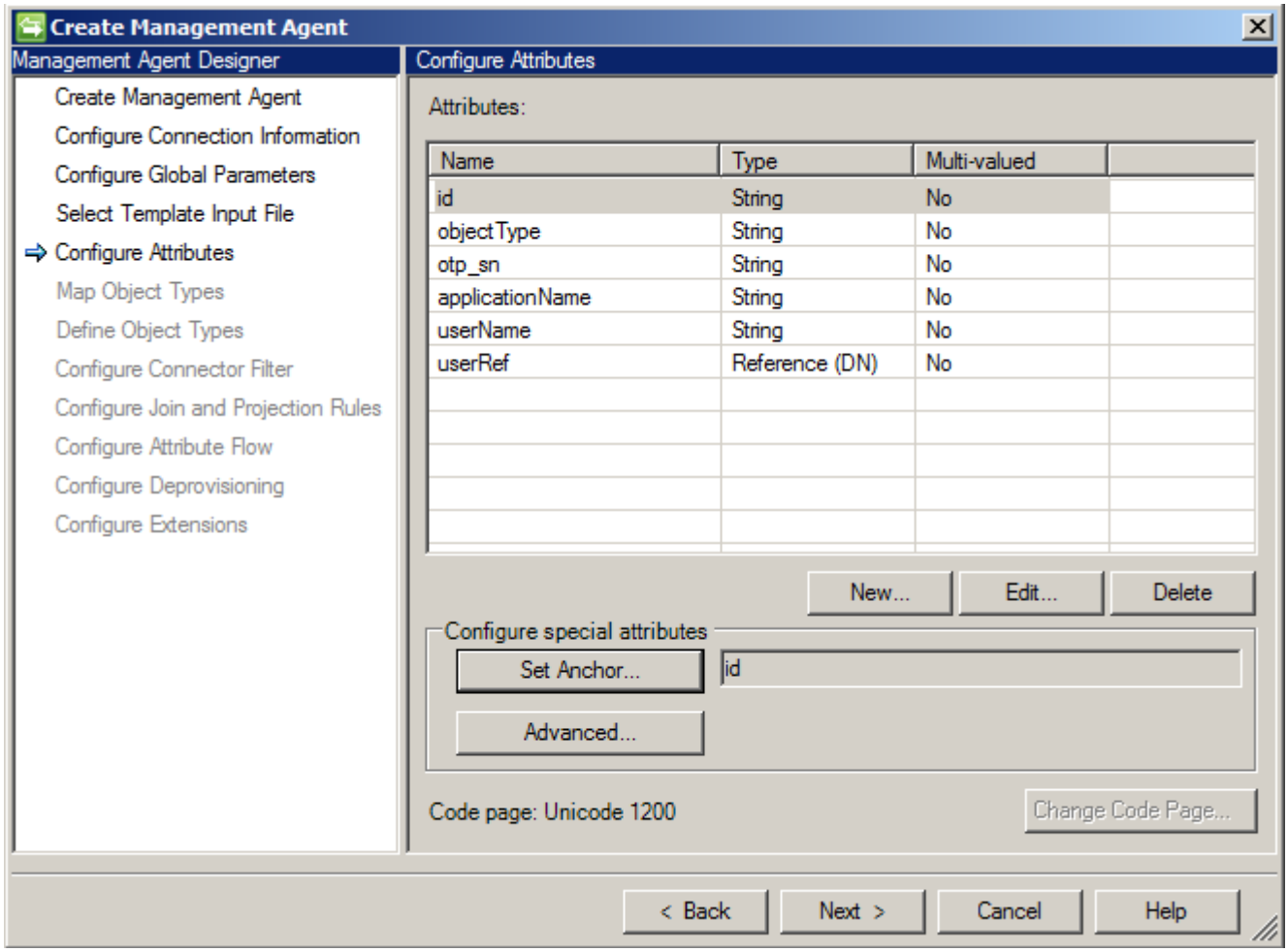



Рисунок 5c.

7. В окне создания Management Agent в разделе Map Object Types нажмите Next.
8. В окне создания Management Agent в разделе Define Object Types нажмите Next.

9. В разделах Configure Connector Filter, Configure Join and Projection Rules, Configure Attribute Flow, Configure Deprovisioning выполните настройки в соответствии с планом использования/коннектора в вашей инфраструктуре.
10. В окне создания Management Agent в разделе Configure Extensions выполните следующее (Рисунок 6):
    a. Выберите опцию Enable password management.
    b. Укажите IndeedID.SSO.MA.dll в качестве Extension name.
    c. Выберите опцию Set only.
    d. Нажмите Finish.

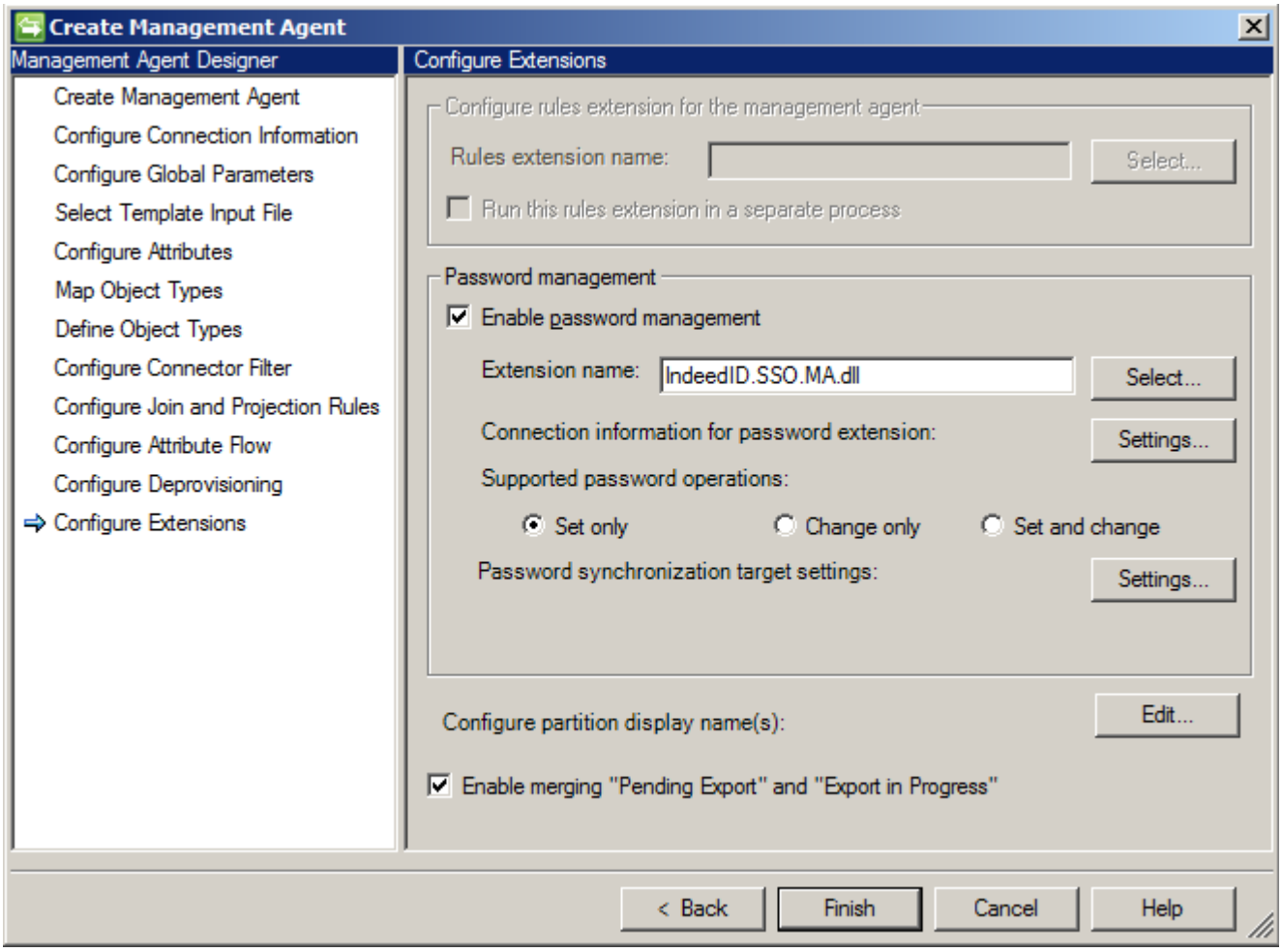



Рисунок 6.

**Описание схемы данных коннектора (файл scheme.txt).**

1. Атрибут **objectType** определяет тип объекта. Может иметь значение user или ssoaccount.
2. objectType:**user** – объект пользователя Indeed-Id. Привязывается к доменному пользователю по его SID через атрибут id.
   Атрибуты:
   - **id** – SID учетной записи пользователя в Active Directory. Формат String. Заполняется на стороне FIM. Обязательное поле.
   - **otp_sn** – серийный номер eToken PASS. Формат String. Необязательное поле.
3. objectType:**ssoaccount** – объект учетной записи приложения SSO. Привязывается к объекту user. Связь реализована через атрибут userRef. К одному объекту user может быть привязано несколько ssoaccount.
   - **id** – идентификатор SSO учетной записи, заполняется коннектором в момент создания объекта. Формат String.
   - **applicationName** – идентификатор приложения в системе. Формат String.

- **username** – имя пользователя для учетной записи приложения SSO. Формат String.
- **userRef** – Reference DN, ссылка на объект пользователя (user), для которого будет создаваться учетная запись SSO. Формат Reference DN.

## Сбор программных логов

Наличие программных логов Indeed-Id позволяет специалистам службы поддержки оперативно локализовать причины возможных проблемных ситуаций и принять меры к их устранению. Сбор программных логов осуществляется с помощью утилиты Indeed-Id GetLog, поставляемой в составе решения Indeed-Id. Для получения подробной информации обратитесь к Руководству пользователя Indeed-Id GetLog.