

Интеграция 1IDM со службой каталога ALD Pro



06/10/2025

Содержание

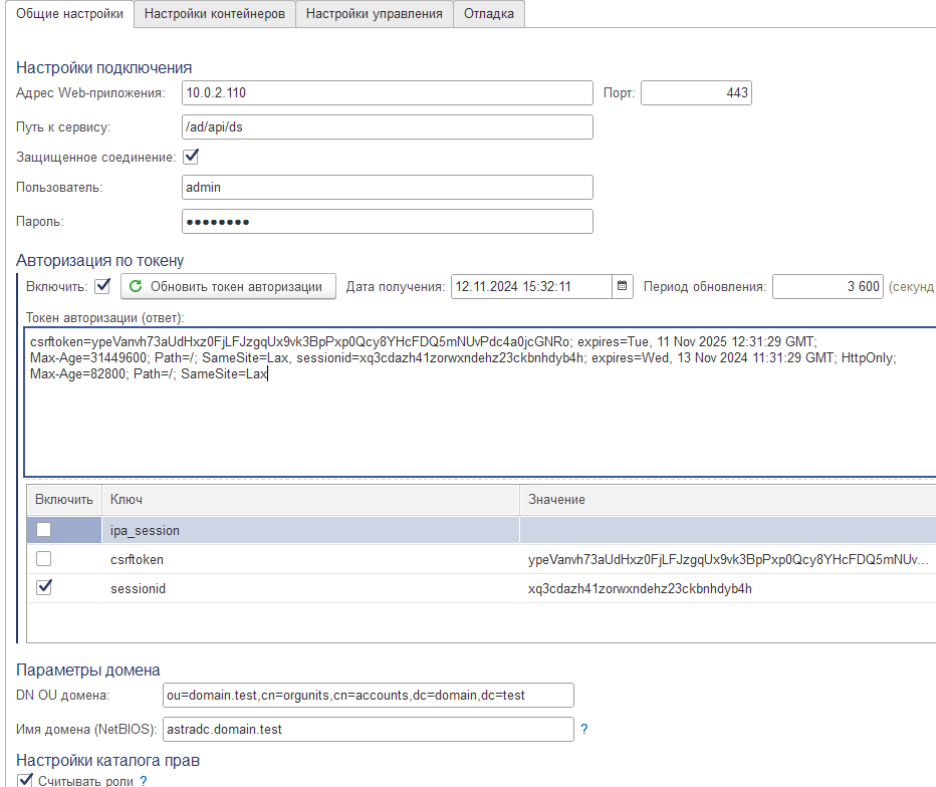
1	Общие настройки	3
2	Настройки контейнеров.....	5
2.1	Контейнеры для считывания.....	5
2.2	Шаблоны контейнеров	6
3	Настройки управления	8
3.1	Атрибуты УЗ	8
3.2	Операции.....	8
4	Принятые сокращения	10

1IDM — это IDM-система, построенная на платформе 1С и предназначенная для интеграции бизнес-процессов из 1С с внешними сервисами предприятия.

В настоящей инструкции описана процедура интеграции 1IDM со службой каталога ALD Pro. Данная интеграция позволяет централизованно управлять пользователями домена: создавать и блокировать учётные записи, изменять атрибуты, управлять членством в группах и назначать роли. Взаимодействие реализовано через REST-API ALD Pro, что обеспечивает гибкую и автоматизированную синхронизацию между системами.

1 Общие настройки

На вкладке **Общие настройки** выполняются настройки подключения и общие настройки коннектора (рис. 1).



Общие настройки | Настройки контейнеров | Настройки управления | Отладка

Настройки подключения

Адрес Web-приложения: Порт:

Путь к сервису:

Защищенное соединение:

Пользователь:

Пароль:

Авторизация по токenu

Включить: Обновить токен авторизации Дата получения: Период обновления: (секунд)

Токен авторизации (ответ):

```
csrfToken=ypeVanvh73aUdHxz0FjLFJzggUx9vk3BpPxp0Qcy8YHcFDQ5mNUVdc4a0jcGNRo; expires=Tue, 11 Nov 2025 12:31:29 GMT;
Max-Age=31449600; Path=/; SameSite=Lax; sessionId=xq3cdazh41zorwxndehz23ckbnhdyb4h; expires=Wed, 13 Nov 2024 11:31:29 GMT; HttpOnly;
Max-Age=62800; Path=/; SameSite=Lax
```

Включить	Ключ	Значение
<input type="checkbox"/>	ipa_session	
<input type="checkbox"/>	csrfToken	ypeVanvh73aUdHxz0FjLFJzggUx9vk3BpPxp0Qcy8YHcFDQ5mNUV...
<input checked="" type="checkbox"/>	sessionId	xq3cdazh41zorwxndehz23ckbnhdyb4h

Параметры домена

DN OU домена:

Имя домена (NetBIOS): ?

Настройки каталога прав

Считать роли ?

Рисунок 1 – Общие настройки коннектора Astra Linux Directory Pro

Настройки подключения

Адрес Web-приложения – адрес сервера, на котором находится система ALD Pro.

Путь к сервису – адрес размещения интеграционного сервиса.

Защищенное соединение open SSL – признак устанавливается, если используется защищенное соединение .

Пользователь – логин в системе ALD Pro.

Пароль – пароль в системе ALD Pro.

Авторизация по токenu

Для авторизации по токenu необходимо включить соответствующую опцию в настройках коннектора. Токен обновляется автоматически перед выполнением запроса.

Обновить токен авторизации – обновление токена вручную.

Период обновления – можно задать вручную, по умолчанию задан период 3600 секунд.

Параметры домена

DN OU домена – DN корневого подразделения домена.

Имя домена (NetBIOS) – Net BIOS Name домена

Настройки каталога прав

Считывать роли – опция включает считывание ролей пользователей в каталог прав 1IDM, а также показывает в карточке учетной записи наличие привилегий вида «Роль пользователя».

2 Настройки контейнеров

2.1 Контейнеры для считывания

На вкладке **Настройки контейнеров** настраиваются контейнеры для получения групп и учетных записей пользователей (рис.2).

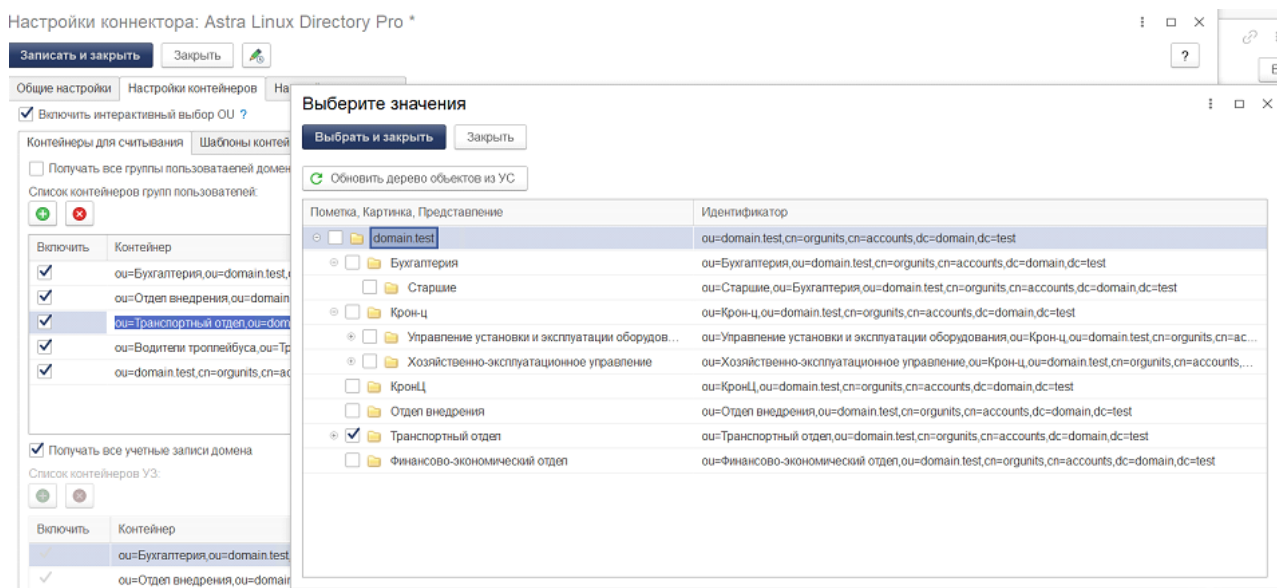


Рисунок 2 – Настройка контейнеров для считывания УЗ и групп пользователей коннектора Astra Linux Directory Pro

Поле **Контейнер** возможно заполнять как вручную, так и интерактивно, выбирая необходимое значение из дерева объектов, предоставляемого управляемой системой ALD Pro.

Чтобы задействовать интерактивный выбор контейнеров, необходимо активировать опцию **Включить интерактивный выбор OU**. Далее при добавлении либо изменении поля **Контейнер** будет появляться окно с отображением дерева подразделений.

Если заполнение идет в режиме добавления в список новых контейнеров, то будет возможность выбрать несколько контейнеров.

Команда **Обновить дерево объектов УС** предназначена для принудительного обновления дерева подразделений из ALD Pro.

Включить интерактивный выбор OU – опция позволяет выбирать контейнер подразделения из списка.

Получать все группы пользователей домена – рекомендуется включить, если необходимо загружать все «Группы пользователей», существующие в ALDPro.

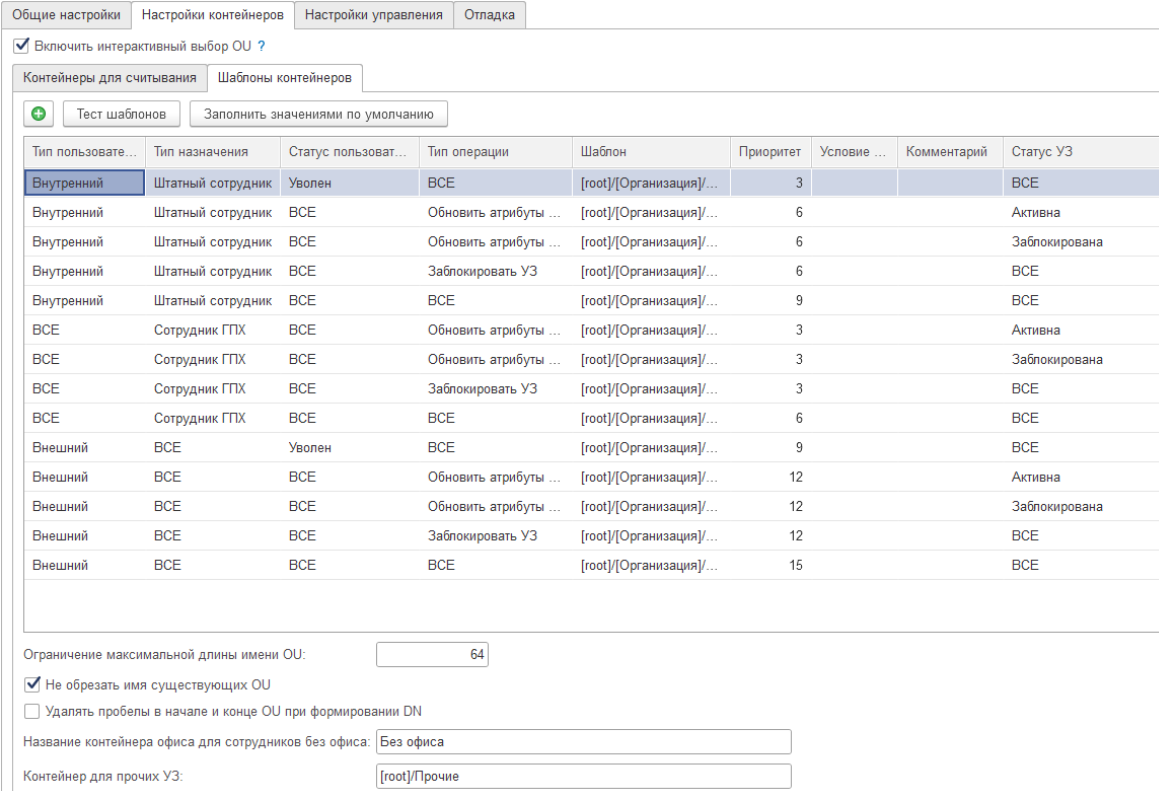
Список контейнеров групп пользователей – необходимо заполнять, если отключена опция **Получать все группы пользователей домена**.

Получать все учетные записи домена – рекомендуется включить, если необходимо загружать все УЗ, существующие в ALDPro.

Список контейнеров УЗ – необходимо заполнить, если отключена опция **Получать все учетные записи домена**.

2.2 Шаблоны контейнеров

Настройки для формирования контейнеров по шаблонам (рис. 3). Табличную часть шаблонов контейнеров рекомендуется заполнять значениями по умолчанию командой **Заполнить значениями по умолчанию**.



Тип пользовате...	Тип назначения	Статус пользоват...	Тип операции	Шаблон	Приоритет	Условие ...	Комментарий	Статус УЗ
Внутренний	Штатный сотрудник	Уволен	ВСЕ	[root]/[Организация]/...	3			ВСЕ
Внутренний	Штатный сотрудник	ВСЕ	Обновить атрибуты ...	[root]/[Организация]/...	6			Активна
Внутренний	Штатный сотрудник	ВСЕ	Обновить атрибуты ...	[root]/[Организация]/...	6			Заблокирована
Внутренний	Штатный сотрудник	ВСЕ	Заблокировать УЗ	[root]/[Организация]/...	6			ВСЕ
Внутренний	Штатный сотрудник	ВСЕ	ВСЕ	[root]/[Организация]/...	9			ВСЕ
ВСЕ	Сотрудник ГПХ	ВСЕ	Обновить атрибуты ...	[root]/[Организация]/...	3			Активна
ВСЕ	Сотрудник ГПХ	ВСЕ	Обновить атрибуты ...	[root]/[Организация]/...	3			Заблокирована
ВСЕ	Сотрудник ГПХ	ВСЕ	Заблокировать УЗ	[root]/[Организация]/...	3			ВСЕ
ВСЕ	Сотрудник ГПХ	ВСЕ	ВСЕ	[root]/[Организация]/...	6			ВСЕ
Внешний	ВСЕ	Уволен	ВСЕ	[root]/[Организация]/...	9			ВСЕ
Внешний	ВСЕ	ВСЕ	Обновить атрибуты ...	[root]/[Организация]/...	12			Активна
Внешний	ВСЕ	ВСЕ	Обновить атрибуты ...	[root]/[Организация]/...	12			Заблокирована
Внешний	ВСЕ	ВСЕ	Заблокировать УЗ	[root]/[Организация]/...	12			ВСЕ
Внешний	ВСЕ	ВСЕ	ВСЕ	[root]/[Организация]/...	15			ВСЕ

Ограничение максимальной длины имени OU:

Не обрезать имя существующих OU

Удалять пробелы в начале и конце OU при формировании DN

Название контейнера офиса для сотрудников без офиса:

Контейнер для прочих УЗ:

Рисунок 3 – Настройка шаблонов контейнеров коннектора Astra Linux Directory Pro

Тест шаблонов – команда выполняется, когда требуется проверить какой шаблон будет использоваться для определенного сотрудника (УЗ) и при определенной операции.

Для выполнения проверки требуется выбрать сотрудника и тип операции, затем выполнить команду **Сформировать результат**. Дополнительно для выбранного сотрудника можно указать учетную запись.

Колонки *Тип пользователя*, *Тип назначения*, *Статус пользователя*, *Тип операции*, *Статус УЗ* содержат условия, при одновременном выполнении которых определяется шаблон, по которому будет сформирован путь при текущей операции с УЗ. Значения, которые можно выбрать в колонках, предопределены программно.

Если условия могут одновременно выполняться более чем в одной строке, то будет выбран шаблон той строки, где наивысшее значение поля *Приоритет*.

Приоритет со значением 1 – наивысший приоритет. Чем выше значение, тем меньше приоритет у данной строки шаблона.

Поле *Условие (И)* – поле для ввода выражения на встроенном языке, которое возвращает логическое значение «Истина» или «Ложь», необязательно для заполнения, используется для расширения возможностей (более тонкой настройки) как дополнительное условие в выборе шаблона контейнера.

В колонке «Шаблон» допускается ввод пути, по которому следует помещать УЗ, если выполняются все условия, заданные в текущей строке.

Ограничение максимальной длины имени OU – если значение указано, то при создании нового контейнера (OU) для учетных записей в AD, проверяется длина имени на соответствие указанному значению, и если длина больше, то имя обрезается.

Не обрезать имена у существующих OU – если признак установлен, то при формировании контейнера (OU) для УЗ, если такой контейнер в AD уже существует, длина имени сохраняется, даже если превышает значение реквизита **Ограничение максимальной длины имени OU**.

Удалять пробелы в начале и конце OU при формировании DN – если признак установлен, то при создании УЗ в строке distinguishedName в формируемых наименованиях контейнеров (OU) будут отсутствовать пробелы в начале и в конце.

Название контейнера для сотрудников без офиса – название данного OU будет взято для сотрудников без офиса.

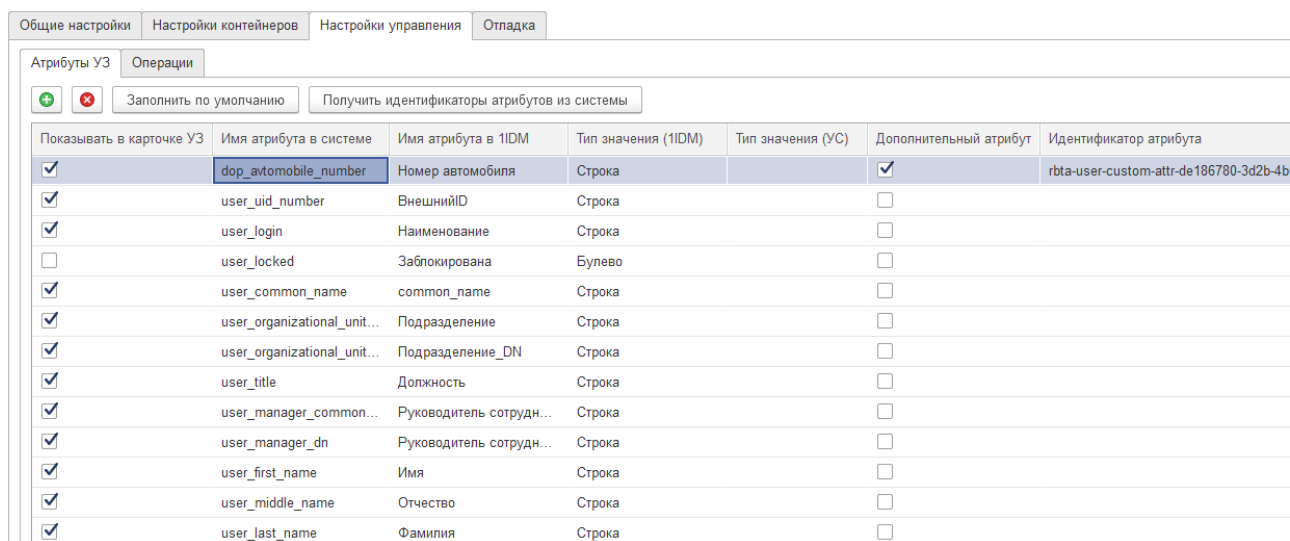
Контейнер для прочих УЗ – здесь прописываются параметры контейнера, куда определяются УЗ, которые не отвечают ни одному из условий в табличной части **Шаблоны контейнеров**.

3 Настройки управления

3.1 Атрибуты УЗ

В таблице заполняются настройки соответствия атрибутов УЗ (рис.4). Возможно указать как основные атрибуты (из схемы ALD Pro), так и дополнительные.

Если планируется управлять дополнительными атрибутами УЗ, то необходимо также заполнить поле **Идентификатор атрибута**.



Показывать в карточке УЗ	Имя атрибута в системе	Имя атрибута в 1IDM	Тип значения (1IDM)	Тип значения (УС)	Дополнительный атрибут	Идентификатор атрибута
<input checked="" type="checkbox"/>	dop_automobile_number	Номер автомобиля	Строка		<input checked="" type="checkbox"/>	rbta-user-custom-attr-de186780-3d2b-4b
<input checked="" type="checkbox"/>	user_uid_number	ВнешнийID	Строка		<input type="checkbox"/>	
<input checked="" type="checkbox"/>	user_login	Наименование	Строка		<input type="checkbox"/>	
<input type="checkbox"/>	user_locked	Заблокирована	Булево		<input type="checkbox"/>	
<input checked="" type="checkbox"/>	user_common_name	common_name	Строка		<input type="checkbox"/>	
<input checked="" type="checkbox"/>	user_organizational_unit...	Подразделение	Строка		<input type="checkbox"/>	
<input checked="" type="checkbox"/>	user_organizational_unit...	Подразделение_DN	Строка		<input type="checkbox"/>	
<input checked="" type="checkbox"/>	user_title	Должность	Строка		<input type="checkbox"/>	
<input checked="" type="checkbox"/>	user_manager_common...	Руководитель сотрудн...	Строка		<input type="checkbox"/>	
<input checked="" type="checkbox"/>	user_manager_dn	Руководитель сотрудн...	Строка		<input type="checkbox"/>	
<input checked="" type="checkbox"/>	user_first_name	Имя	Строка		<input type="checkbox"/>	
<input checked="" type="checkbox"/>	user_middle_name	Отчество	Строка		<input type="checkbox"/>	
<input checked="" type="checkbox"/>	user_last_name	Фамилия	Строка		<input type="checkbox"/>	

Рисунок 4 – Настройка атрибутов учетных записей коннектора Astra Linux Directory Pro

Заполнить по умолчанию – команда для заполнения табличной части значениями по умолчанию.

Получить идентификаторы атрибутов из системы – команда для автоматического заполнения идентификаторов дополнительных атрибутов.

Настройки в табличной части:

Показывать в карточке УЗ – настройка отображения атрибута в карточке УЗ;

Имя Атрибута в системе– исходное наименование атрибута в Управляемой системе;

Имя Атрибута 1IDM – наименование атрибута в 1IDM;

Тип Значения 1IDM / УС – тип значения атрибута. Может принимать значения: *Строка, Число, Булево, Дата, Массив*;

Дополнительный атрибут – указывает, что текущий атрибут является дополнительным атрибутом УЗ в управляемой системе;

Идентификатор атрибута – поле, обязательное к заполнению для дополнительных атрибутов УЗ. Заполняется автоматически по команде **Получить идентификаторы атрибутов системы**.

3.2 Операции

Настройки для выполнения операций (рис.5).

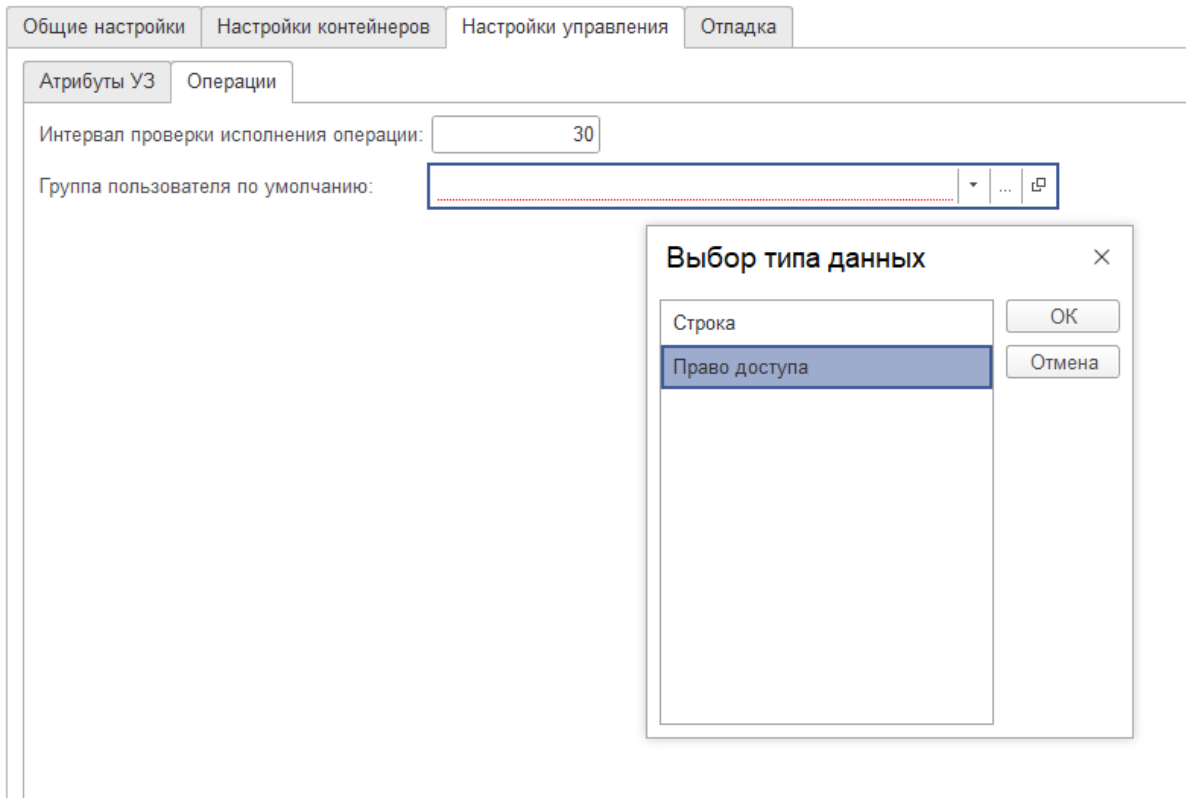


Рисунок 5 – Настройка операций коннектора Astra Linux Directory Pro

Интервал проверки исполнения операции – задаёт задержку перед считыванием системой 1 IDM результата запущенных процессов изменения для контроля применения изменений.

Группа пользователя по умолчанию – группа, которая автоматически назначается системой ALD Pro при создании УЗ. (данный функционал пока не реализован).

Группа настроек на вкладке **Отладка** – предназначена для разработчика.

 **Внимание!**

Не рекомендуется использовать в продуктивной среде!

4 Принятые сокращения

УС – управляемая система

ALD Pro – Astra Linux Directory Pro

УЗ – учетная запись/учетные записи

OU – organizational unit – подразделение (в системе ALD Pro)

DN OU – distinguished name, отличительное имя подразделения

Приложение – элемент справочника 1С «Приложение»

Коннектор – логическая структура, обеспечивающая интеграцию 1IDM с определенной управляемой системой.