Интеграция Базис.Virtual Security со службой каталога ALD Pro

06/04/2025

Базис.Virtual Security – это сертифицированное ФСТЭК РФ средство защиты информации систем виртуализации и облачных платформ.

Интеграция позволяет настроить единую точку входа (Single Sign-On, SSO), при которой пользователи могут аутентифицироваться один раз и получать доступ к нескольким приложениям или сервисам без необходимости повторного ввода учетных данных; появляется возможность централизованного управления пользователями, ролями и правами доступа. Также решение позволяет настраивать различные сценарии аутентификации, включая многофакторную аутентификацию (MFA), условный доступ и кастомизацию форм входа.

Инструкция по интеграции разработана вендором Базис.Virtual Security, который также оказывает поддержку по проведению пилотного тестирования и внедрению своего программного продукта.

Интеграция ALD Pro с Базис.Virtual Security v.3.3.0

Москва

04/03/2025

Содержание

Введение

Данная инструкция содержит информацию о настройке федерации ALD Pro с BVS по протоколу LDAP.

Интеграция ALD Pro в режиме федерации в Базис Virtual Security предоставляет несколько важных преимуществ, которые упрощают управление аутентификацией и авторизацией в распределенных системах.
Основные преимущества включают:

1. Единая точка входа (Single Sign-On, SSO). Пользователи могут аутентифицироваться один раз и получать доступ к нескольким приложениям или сервисам без необходимости повторного ввода учетных данных. Это улучшает пользовательский опыт и снижает нагрузку на пользователей, особенно в системах с большим количеством приложений.
2. Централизованное управление пользователями. Подобная интеграция позволяет централизованно управлять пользователями, ролями и правами доступа. Это упрощает администрирование, так как не нужно дублировать учетные записи в разных системах.
3. Гибкость в настройке аутентификации. Решение позволяет настраивать различные сценарии аутентификации, включая многофакторную аутентификацию (MFA), условный доступ и кастомизацию форм входа. Это повышает безопасность и адаптирует процесс аутентификации под нужды бизнеса.
4. Безопасность. Интеграция гарантирует высокий уровень безопасности, включая поддержку шифрования, управление сессиями, защиту от различных атак и возможность настройки политик паролей. Это обеспечивает соответствие требованиям безопасности и стандартам ФСТЭК.

Добавление сертификата в хранилище Java

Если предполагается использовать протокол LDAPS в качестве протокола подключения к ALD Pro перед настройкой федерации необходимо добавить используемый им сертификат (если это самоподписанный вариант) или сертификат CA в хранилище CA-сертификатов в Java.

Если используется самоподписанный сертификат, то выполните команду получения сертификата ALD Pro:

```
 echo -n | openssl s_client -connect ALD_PRO_DOMAIN:636 | sed -ne '/-BEGIN
CERTIFICATE-/,/-END CERTIFICATE-/p' > ldapserver.pem
```

Полученный файл сертификата добавьте в хранилище CA-сертификатов Java:

```
/opt/basis/java/bin/keytool -importcert -alias aldprocert -keystore /opt/basis/java/lib/
security/cacerts -storepass changeit -file ldapserver.pem
```

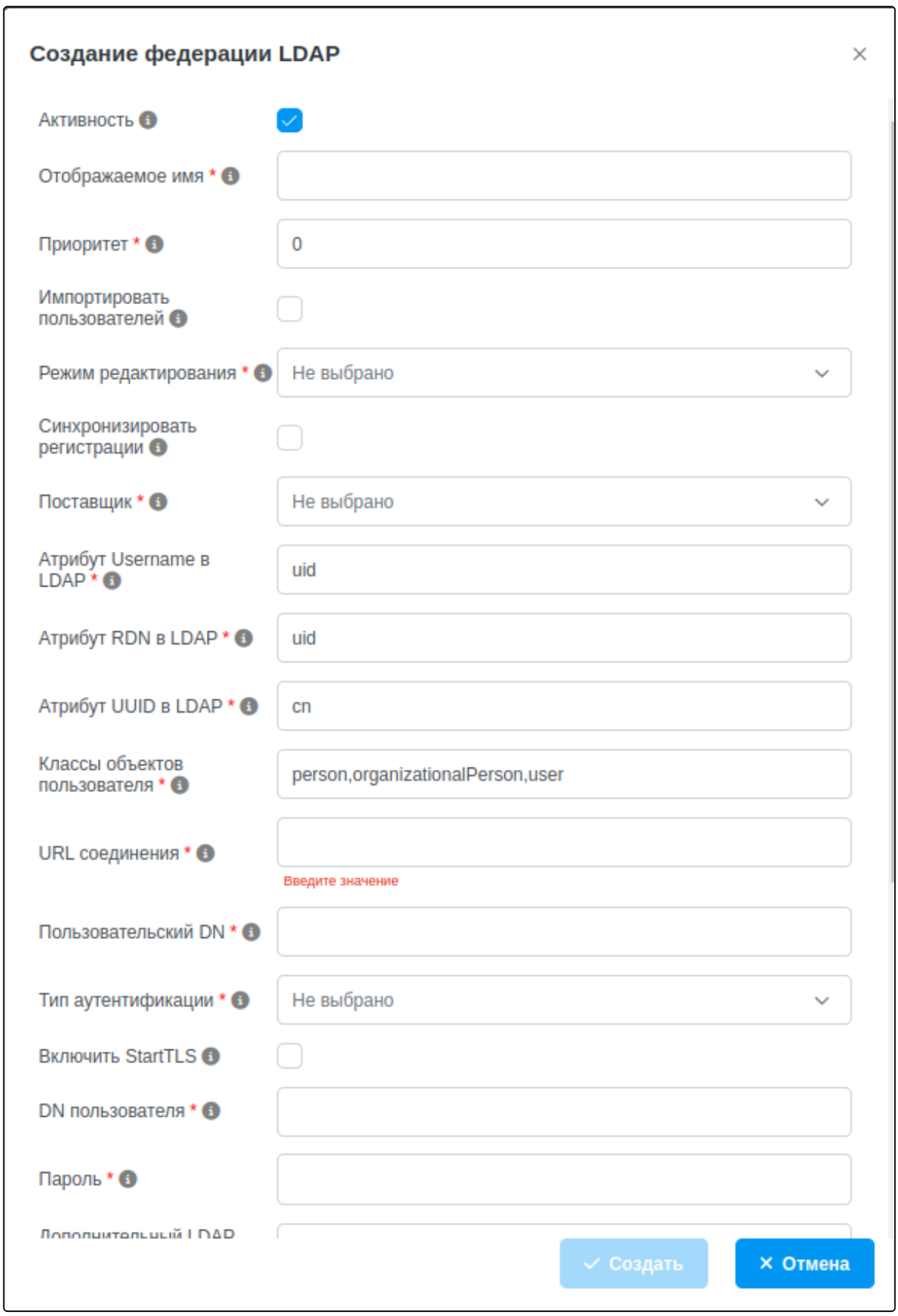
Если используется сертификат, выпущенный с помощью CA-сертификата, то достаточно импортировать сам файл CA-сертификата, без получения сертификата с ALD Pro:

```
/opt/basis/java/bin/keytool -importcert -alias aldprocert -keystore /opt/basis/java/lib/
security/cacerts -storepass changeit -file ca.crt
```

Настройка федерации в BVS

Перейдите на страницу: *Имя домена -> Безопасность -> Федерации.*

Нажмите на кнопку «Создать» и выберите тип федерации «LDAP». Заполните основную конфигурационную информацию о федерации, каждое поле снабжено подсказкой:



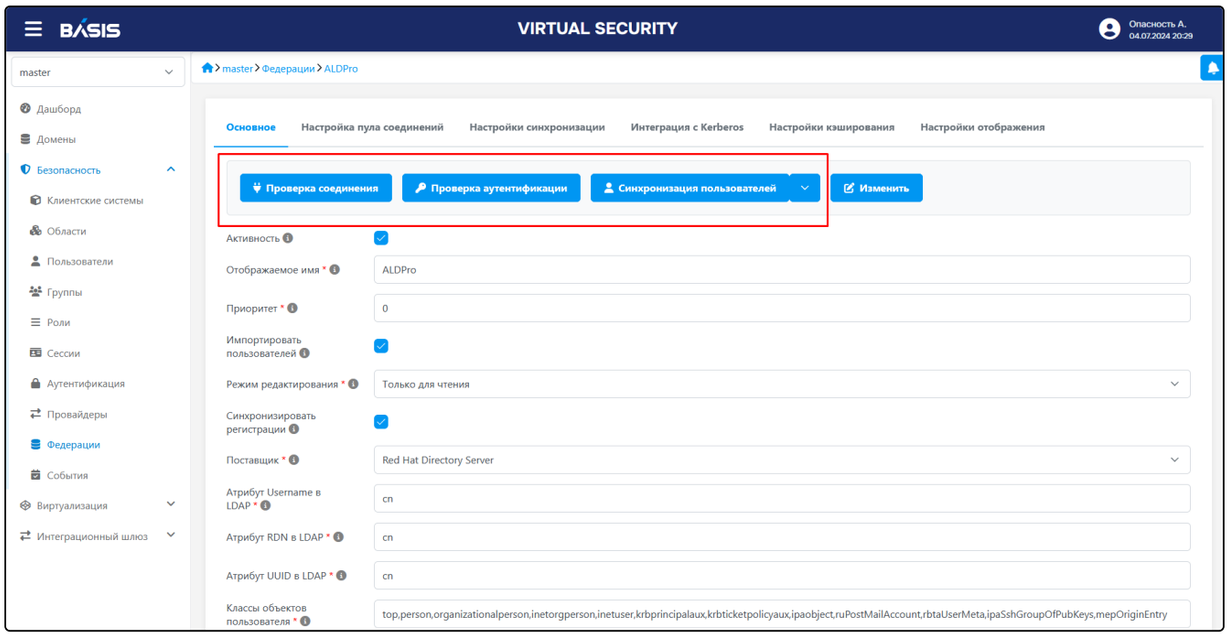
Окно создания федерации LDAP

Укажите параметры:

Параметр	Описание
Активность	Параметр определяет состояние федерации. Если параметр выключен, то федерация не будет учитываться для запросов, а импортированные пользователи будут отключены и доступны только для чтения. Включите функцию.
Отображаемое имя	Укажите имя федерации.
Приоритет	Укажите приоритет - `0`.
Импортировать пользователей	Включите функцию.
Режим редактирования	Режим "С возможностью записи" не поддерживается. Используйте режимы: "Только для чтения" или "Несинхронизированный".
Синхронизировать регистрации	Включите функцию.
Поставщик	Укажите - `Red Hat Directory Server`.
Атрибут Username в LDAP	Укажите - `uid`.
Атрибут RDN в LDAP	Укажите - `uid`.
Атрибут UUID в LDAP	Укажите - `cn`.
Классы объектов пользователя	Укажите - `top,person,organizationalperson,inetorgperson,inetuser`.
URL соединения	Укажите: `ldap://DNS_ДОМЕН_ALD_PRO:389`, где: • `DNS_ДОМЕН_ALD_PRO` – должен быть доступен из сети узлов управления BVS; • допускается указание адреса ldaps://, в этом случае следует указать порт 636. Перед подключением выполните шаг добавления сертификата в хранилище Java, иначе BVS не сможет подключиться к ALD Pro.
Пользовательский DN	Укажите `cn=users,cn=accounts,dc=aldpro,dc=loc`, где вместо `dc=aldpro` и `dc=loc` укажите свое наименование домена ALD Pro.
Тип аутентификации	Укажите - `simple`.
Включить StartTLS	Выключите функцию.

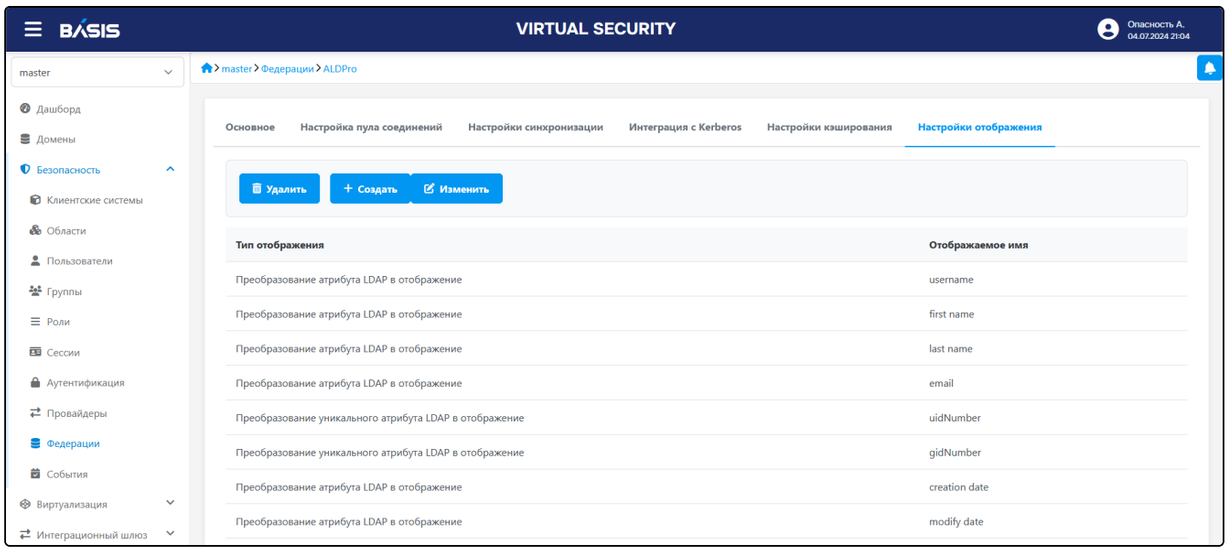
Параметр	Описание
DN пользователя	Укажите `uid=system,cn=users,cn=accounts,dc=basis,dc=loc`, где: • вместо `dc=aldpro` и `dc=loc` укажите свое наименование домена ALD Pro; • в `uid` указывается имя сервисной учетной записи с правами чтения, предназначенной для входа в ALD Pro; • для возможности использования этого пользователя необходимо хотя бы один раз осуществить вход этим пользователем в ALD Pro.
Пароль	Укажите пароль от DN-пользователя ALD Pro.
Дополнительный LDAP фильтр	Оставьте пустым.
Область поиска	Укажите - Поддерево.
Проверка пароля на требования	Выключите функцию.
Подтверждение E-mail	Выключите функцию.
Использовать Truststore SPI	Используйте режимы: "Только для ldaps" или "Никогда".
Таймаут соединения, мс	Укажите "-1".
Таймаут чтения, мс	Укажите "-1".
Постраничный режим	Выключите функцию.

После успешного сохранения основных настроек, убедитесь, что успешно выполняются следующие проверки: "Проверка соединения", "Проверка аутентификации", "Синхронизация пользователей".



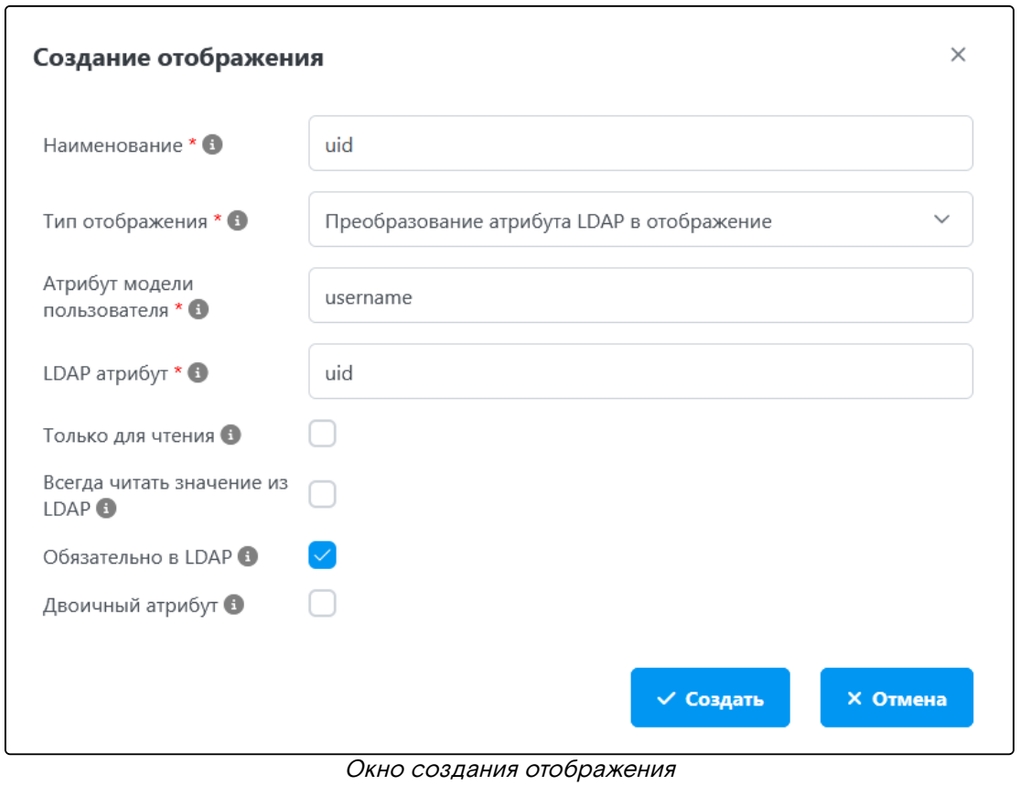
Изменение отображения. LDAP атрибут

Перейдите в настройки отображения федерации:



Настройки отображения федерации

Создайте новое отображение:



Окно создания отображения

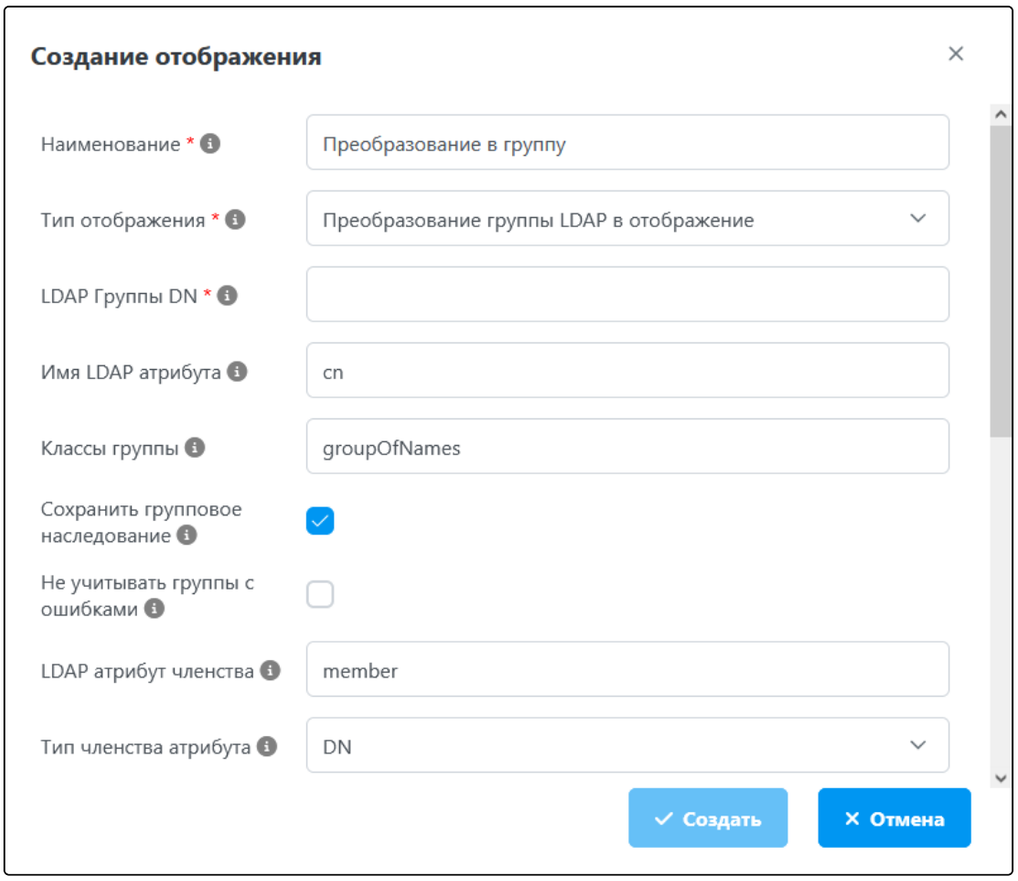
Укажите следующие параметры:

Параметр	**Описание**
Наименование	Укажите - `uid`.
Тип	Укажите "Преобразование атрибута LDAP в отображение".
Атрибут модели пользователя	Укажите - `username`.
LDAP атрибут	Укажите - `uid`.
Только для чтения	Выключите функцию.
Всегда читать значение из LDAP	Выключите функцию.

Параметр	Описание
Обязательно в LDAP	Включите функцию.
Двоичный атрибут	Выключите функцию.

Настройка отображения групп ALD Pro в BVS

Для синхронизации групп из ALD Pro в BVS требуется настройка отображения "Преобразование группы LDAP в отображение". Для этого перейдите во вкладку "Настройка отображения" в параметрах федерации и нажмите кнопку "+ Создать".



Форма создания отображения

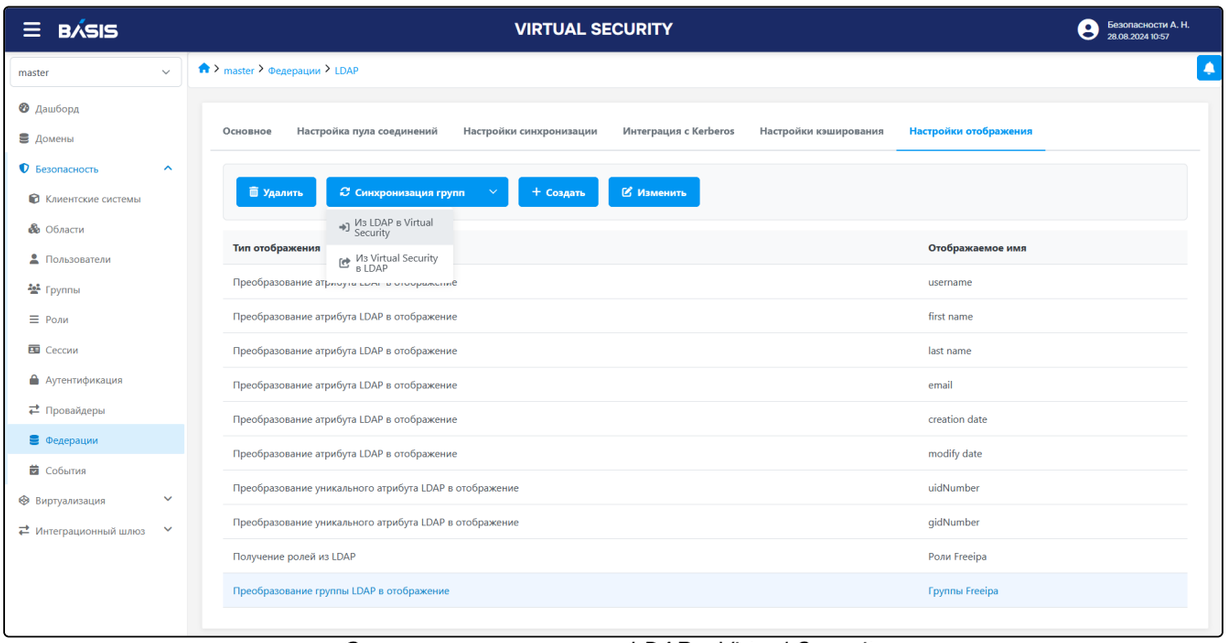
В форму укажите следующие параметры:

Параметр	Описание
Наименование	Имя настройки отображения. Можно указать любое.
Тип отображения	Выберите пункт "Преобразование группы LDAP в отображение".
LDAP группы DN	Укажите путь LDAP, откуда необходимо получить список групп.
Имя LDAP атрибута	Укажите - `cn`.
Классы группы	Укажите - `groupOfNames.`
Сохранить групповое наследование	Включите опцию.
Не учитывать группы с ошибками	Выключите опцию.
LDAP атрибут членства	Укажите - `member`.
Тип членства атрибута	Укажите - `DN`.

Параметр	Описание
LDAP атрибут членства пользователя	Укажите - `uid`.
Атрибут UUID в LDAP	Укажите - `gidNumber`.
Фильтр	По умолчанию оставьте пустым, укажите его, если требуется дополнительная фильтрация списков групп (например, по отдельному objectclass). Правило фильтрации использует стандартный формат фильтрации для LDAP;
Режим	Укажите "Только LDAP".
Стратегия извлечения групп пользователей	Укажите "Получение групп из атрибута memberOf".
LDAP атрибут Member-Of	Укажите - `memberOf`.
Отображение атрибутов группы	Укажите - `gidNumber`;
Удалить несуществующие группы	Выключите опцию.

После указания всех параметров нажмите "Создать".

После сохранения отображения выделите его в списке. Появятся дополнительные кнопки в панели, в том числе кнопка "Синхронизация групп". Нажмите на нее, и в вплывающем списке выберите "Из LDAP в Virtual Security" для получения группы с ALD Pro в BVS:



Синхронизация групп из LDAP в Virtual Security

После выполнения этой операции BVS покажет уведомление с краткой информацией о результате синхронизации групп.

> ⚠ Синхронизация групп из BVS в LDAP не поддерживается.

Перейдите в "Безопасность - Группы", чтобы убедиться в наличии групп ALD Pro в BVS.