VK WorkSpace

Интеграция с Active Directory в Почте

Инструкция для администраторов

Оглавление

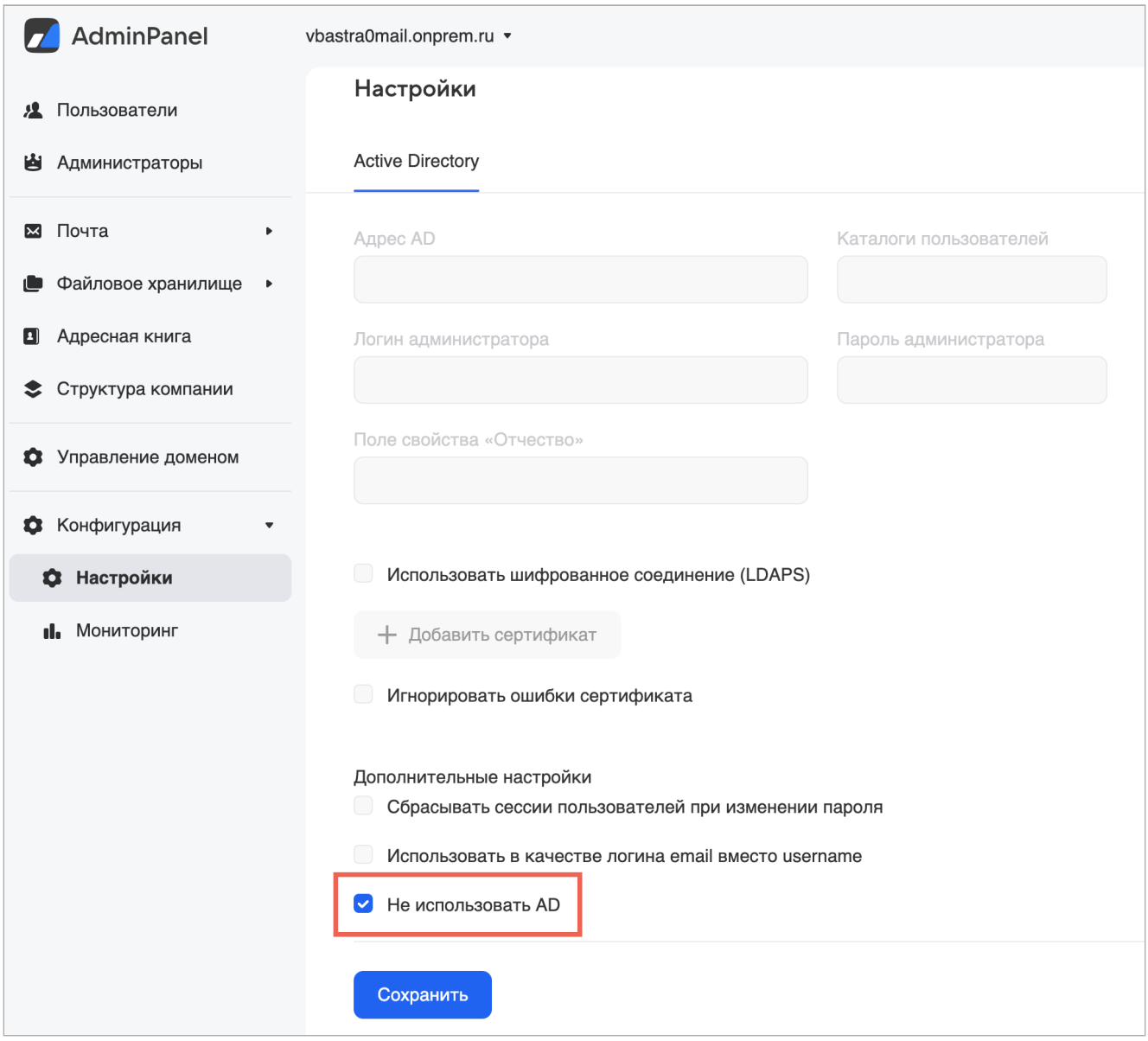
Назначение документа

В документе описан процесс настройки интеграции с Active Directory.

Настроить интеграцию с Active Directory

Почта переносит из Acitve Directory список пользователей, группы рассылок и контакты. При этом Почта не хранит пароли пользователей, то есть вся цепочка аутентификации происходит на стороне AD (LDAP-провайдера). Для каждого домена интеграция с AD настраивается отдельно. Чтобы настроить интеграцию:

1. Перейдите в панель администратора по адресу `biz.<почтовый домен>`.
2. Перейдите в раздел **Конфигурация** → **Настройки**.
3. Уберите чекбокс **Не использовать AD**.



4. Заполните поля:

   Адрес AD — адрес вашего каталога Active Directory.

   Каталоги пользователей — введите значение поля **distinguishedName** из списка атрибутов каталога. Например, `OU=demoapp.DC=presale.DC=local`.

   > **Примечание**
   >
   > Если вам нужно указать больше одного каталога пользователей, обратитесь к представителю VK.

   Логин администратора — логин пользователя Active Directory с правами на чтение каталога и авторизацию пользователей.

   Пароль администратора — пароль пользователя Active Directory с правами на чтение каталога и авторизацию пользователей.

   Поле свойства «Отчество» — если вы используете свойство **Отчество**, введите его значение в это поле.

   Использовать шифрованное соединение (LDAPS) — есть возможность добавления сертификата LDAPS с помощью кнопки **Добавить сертификат**.

   Игнорировать ошибки сертификата — отметьте этот чекбокс, если у вас самоподписанный SSL-сертификат.

   Сбрасывать сессии пользователей при изменении пароля — если чекбокс отмечен, при изменении пароля пользователя в Active Directory будет сбрасываться сессия в Почте.

   Использовать в качестве логина email вместо username — в текущей версии поле не используется.

5. Нажмите на кнопку **Сохранить**.

Синхронизация с AD выполняется один раз в час. Если AD содержит много данных, то одного часа может быть недостаточно для синхронизации всего объема. В этом случае через час после настройки подключения в разделе Пользователи отобразятся не все пользователи из AD, а только часть. Просто подождите еще час.

> **Внимание**
>
> Если объем данных в AD очень большой, при синхронизации может временно отображаться ошибка 502 (или 504). Не переживайте, дождитесь окончания синхронизации.

Если пользователи не появились в Почте, нужно проверить корректность настроек синхронизации с Active Directory с помощью консольной команды:

```
sudo journalctl -fu onpremise-container-adloader1.service
```