

VIPole Corporate Server

Active Directory (AD)/LDAP Integration

Technical Manual

v.1.0



VIPole

www.vipole.com

ENCRYPTED UNIFIED COMMUNICATIONS

secure messaging, sharing, conferencing and collaboration

Windows ▪ macOS ▪ Linux ▪ Android ▪ iOS ▪ Enterprise solutions

1. Способы интеграции с AD/LDAP

Возможны следующие способы интеграции Microsoft Active Directory(AD)/LDAP с сервером VIPole:

1. Импорт пользователей в базу VIPole из AD/LDAP.
 - Пароли пользователей при этом не импортируются.
 - Аутентификация пользователей при подключении к серверу VIPole осуществляется с использованием сервера AD/LDAP.
2. Экспорт пользователей из AD/LDAP в CSV файл.
 - CSV файл может быть импортирован в базу сервера VIPole (возможно, если это необходимо, после редактирования).
 - Пароли в этом случае автоматически генерируются при импорте или берутся из CSV файла.

Импорт пользователей обязательно выполняется в Домен Безопасности владельцем Домена.

2. Настройка сервера VIPole

- 2.1. Для работы с AD/LDAP сервером сначала выполните настройку сервера VIPole, используя следующие параметры файла конфигурации server.config:

Включите поддержку AD/LDAP
`ldap-enabled = 1`

Укажите уникальное имя (DN) пользователя AD/LDAP, которому разрешен импорт данных из дерева AD/LDAP
`ldap-admin-dn = CN=Admin,CN=Users,DC=vipole,DC=ldap,DC=sample`

Укажите пароль пользователя, которому разрешен импорт
`ldap-admin-password = SecretPassword`

URI AD/LDAP сервера
`ldap-uri = ldap://192.168.1.155`

DN, начиная с которого начинается поиск пользователей по поддереву (в поддереве должен быть хотя бы один пользователь, чтобы сервер VIPole смог проверить корректность подключения к серверу AD/LDAP)
`ldap-users-search-base = CN=Users,DC=vipole,DC=ldap,DC=sample`

Имя атрибута, который используется как логин пользователя
`ldap-users-login-mapping=cn`

2.2. После настройки этих параметров перезапустите сервер VIPole.

3. Импорт пользователей в базу VIPole из AD/LDAP

Операции импорта пользователей выполняются с помощью консольной утилиты `vipole-ldap` или с помощью расширения «Администратор VIPole» клиентской программы VIPole для компьютера.

3.1. Импорт пользователей с помощью консольной утилиты `vipole-ldap`:

Параметры работы утилиты `vipole-ldap` задаются в командной строке:

-l [--login]

логин администратора Домена Безопасности VIPole, в который будет выполняться импорт пользователей.

--passwd

пароль администратора, указанного параметром `-login`.

--passwd-file

файл с паролем администратора (используется вместо `--passwd`).

--domain

доменное имя вашего сервера VIPole (это имя, которое добавляется к логину после символа `@`, например, `admin@example.com`)

--server-host arg (=127.0.0.1)

IP адрес сервера VIPole

--server-port arg (=37210)

порт сервера VIPole

--certificate arg

путь к файлу цепочки сертификатов сервера VIPole, который указан в параметре `certificate-chain-file` в файле `server.config`.

--security-domain arg

идентификатор Домена безопасности (необходимо указывать в случае, если у администратора домена их несколько). Идентификатор можно посмотреть при создании Домена безопасности или на вкладке «Параметры» расширения «Администратор VIPole» клиентской программы VIPole.

--admin-password arg

административный пароль для управления Доменом безопасности (этот пароль создается и вводится при запуске расширения «Администратор VIPole»).

--base-dn arg

DN, с которого начинается поиск пользователей. Если не указано – используется значение параметра **ldap-users-search-base** файла конфигурации сервера VIPole.

--filter arg

(=(&(&(objectCategory=person)(objectClass=user))(objectClass=inetOrgPerson)))

фильтр записей пользователей, в соответствии с которым происходит отбор.

Подробное описание синтаксиса и примеры см. [Active Directory: LDAP Syntax Filters](http://social.technet.microsoft.com/wiki/contents/articles/5392.active-directory-ldap-syntax-filters.aspx)

<http://social.technet.microsoft.com/wiki/contents/articles/5392.active-directory-ldap-syntax-filters.aspx>

--skip-imported [0|1] (=0)

пропуск уже существующих пользователей при импорте.

--morph-login

в случае дублирования логина пользователя добавляет в конце логина уникальное число.

-t [--timeout] arg (=300)

время ожидания отклика AD/LDAP сервера в секундах.

--dry-run

добавление пользователей в базу не производится, а выводится только информация о пользователях, которые были добавлены.

--mapping

установка соответствие полей при импорте базы LDAP и внутренней базы пользователей сервера VIPole. При импорте в базу VIPole можно заполнить следующие поля:

login, name1, name2, name3, email, nickname, comments

Например, **--mapping comments=description** устанавливает соответствие между значением атрибута **description** базы LDAP и полем **comments** базы данных пользователей сервера VIPole.

Чтобы указать соответствие нескольких полей, нужно использовать несколько параметров

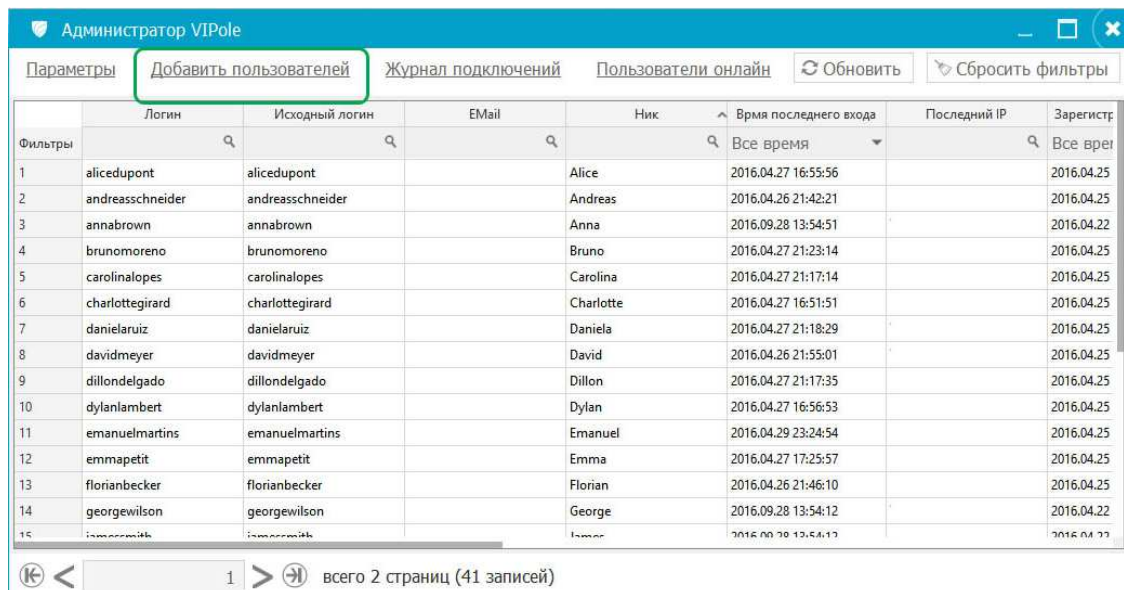
--mapping

3.2. Импорт пользователей с помощью расширения «Администратор VIPole» клиентской программы VIPole для компьютера:

3.2.1. Запустите расширение «Администратор VIPole» через Главное меню клиентской программы VIPole для компьютера.

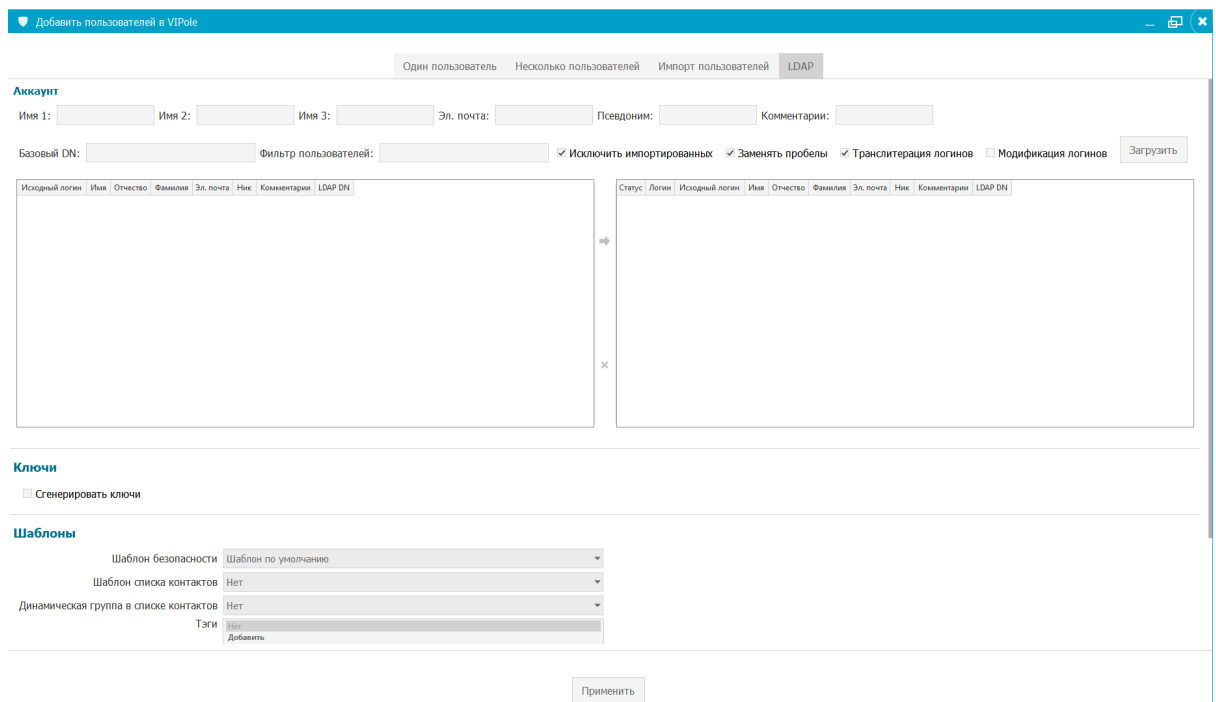
3.2.2. Введите пароль администратора.

3.2.3. Выберите вкладку «Добавить пользователей».



Филтеры	Логин	Исходный логин	EMail	Ник	Врмя последнего входа	Последний IP	Зарегистр
	alicedupont	alicedupont		Alice	2016.04.27 16:55:56		2016.04.25
	andreasschneider	andreasschneider		Andreas	2016.04.26 21:42:21		2016.04.25
	annabrown	annabrown		Anna	2016.09.28 13:54:51		2016.04.22
	brunomoreno	brunomoreno		Bruno	2016.04.27 21:23:14		2016.04.25
	carolinalopes	carolinalopes		Carolina	2016.04.27 21:17:14		2016.04.25
	charlottegirard	charlottegirard		Charlotte	2016.04.27 16:51:51		2016.04.25
	danielaruiz	danielaruiz		Daniela	2016.04.27 21:18:29		2016.04.25
	davidmeyer	davidmeyer		David	2016.04.26 21:55:01		2016.04.25
	dillondelgado	dillondelgado		Dillon	2016.04.27 21:17:35		2016.04.25
	dylanlambert	dylanlambert		Dylan	2016.04.27 16:56:53		2016.04.25
	emanuelmartins	emanuelmartins		Emanuel	2016.04.29 23:24:54		2016.04.25
	emmapetit	emmapetit		Emma	2016.04.27 17:25:57		2016.04.25
	florianbecker	florianbecker		Florian	2016.04.26 21:46:10		2016.04.25
	georgewilson	georgewilson		George	2016.09.28 13:54:12		2016.04.22
	isabelle	isabelle		Isabelle	2016.04.27 13:54:12		2016.04.22

3.2.4. Выберите вкладку LDAP и откроется окно импорта LDAP



Добавить пользователей в VIPole

Один пользователь Несколько пользователей Импорт пользователей **LDAP**

Аккаунт

Имя 1: Имя 2: Имя 3: Эл. почта: Псевдоним: Комментарий:

Базовый DN: Фильтр пользователей: ☒ Исключить импортированных ☒ Заменять пробелы ☒ Транслитерация логинов ☐ Модификация логинов Загрузить

Исходный логин Имя Отчество Фамилия Эл. почта Ник Комментарий LDAP DN

Статус Логин Исходный логин Имя Отчество Фамилия Эл. почта Ник Комментарий LDAP DN

Ключи

☐ Сгенерировать ключи

Шаблоны

Шаблон безопасности Шаблон по умолчанию

Шаблон списка контактов Нет

Динамическая группа в списке контактов Нет

Тэги Добавить

Применить

Поля «Логин», «Имя 1», «Имя 2», «Имя 3», «Эл.почта», «Псевдоним», «Комментарии» предназначены для маппинга. В них можно ввести имена полей базы LDAP, которые будут импортироваться в соответствующие поля внутренней базы пользователей сервера VIPole.

«Базовый DN» - DN, с которого начинается поиск пользователей. Если не указано – используется значение параметра `ldap-users-search-base` файла конфигурации сервера VIPole.

«Фильтр пользователей» - Фильтр записей пользователей, в соответствии с которым происходит отбор. Подробное описание синтаксиса и примеры см. **Active Directory: LDAP Syntax Filters**.

<http://social.technet.microsoft.com/wiki/contents/articles/5392.active-directory-ldap-syntax-filters.aspx>

«Исключить импортированных» - Не импортировать уже существующих пользователей


«Заменять пробелы» - пробелы в поле будут заменены на подчеркивание.

«Транслитерация логинов» - поле с кириллическими символами будет заменено на латинские символы транслитерацией.

«Модификация логинов» - в случае дублирования логина добавляется уникальное число в конце такого логина.

Для импорта обязательно заполните поле «Базовый DN». После нажатия кнопки «Загрузить» в таблице слева появится список пользователей из базы LDAP. Если поля в таблице заполняются неправильно, измените маппинг, указав в полях «Имя 1», «Имя 2», «Имя 3», «Эл.почта», «Псевдоним», «Комментарии» имена атрибутов, соответствующие вашему шаблону базы LDAP.

Выберите пользователей, которых необходимо импортировать в VIPole кликом мыши:

- Клик с нажатой клавишей Ctrl выделяет несколько строк.
- Клик с нажатой клавишей Shift выделяет диапазон строк.
- Кнопкой  перенесите выбранные записи в правую таблицу.

После нажатия клавиши «Применить» пользователи, перечисленные в таблице справа будут импортированы в базу VIPole.

Опция «Сгенерировать ключи» позволяет сразу генерировать для импортируемого пользователя ключи шифрования. При этом пароль и секретная фраза генерируются автоматически. Посмотреть их администратор может на вкладке «Безопасность» окна «Администрирование пользователя VIPole».

При импорте к пользователю могут быть применены шаблоны безопасности и шаблоны списка контактов, которые необходимо выбрать перед нажатием клавиши «Применить».

3.3. Экспорт пользователей из AD/LDAP в CSV-файл с помощью консольной утилиты vipole-ldap.

Если консольной утилите vipole-ldap среди других параметров указать параметр

--csv-file arg

то будет выполняться экспорт данных в CSV файл.

С этой опцией автоматически включается опция **--dry-run**. Таким образом, импорта пользователей в базу не происходит. Все остальные параметры работают как при импорте в базу сервера VIPole.

CSV файл может быть при необходимости отредактирован и затем импортирован в базу сервера VIPole с помощью расширения «Администратор VIPole» в клиентской программе VIPole для компьютера.

Обратите внимание, в различных реализациях AD/LDAP (в том числе AD в различных версиях Windows Server) используется различная схема именования атрибутов.

Поэтому перед импортом пользователей обязательно убедитесь в соответствии импортируемых полей.

Если вы используете импорт пользователей в базу сервера VIPole, сначала выполняйте утилиту vipole-ldap с параметром **--dry-run** и по логу программы убедитесь, что импортируются нужные пользователи и дополнительные поля заполнены правильно.

Для просмотра схемы базы LDAP, названия атрибутов и т.п. можно использовать программу [LDAP Admin](#) или подобные.

3.4. Примеры использования

Импорт новых пользователей из AD vipole.ldap.sample .

Поиск ведется среди всех пользователей, логины которых начинаются на testuser (напр. testuser04 или testusername). Пользователи импортируются как testuser04@vipole.ldap.

```
vipole-ldap \
--admin-password 1234567890 \
--base-dn CN=Users,DC=vipole,DC=ldap,DC=sample \
--certificate /etc/vipole/cacert.pk \
--domain vipole.ldap \
--login sd_admin --passwd 12345678 \
--server-host 192.168.1.175
--filter "(CN=testuser*)" "
```

Экспорт в CSV-файл пользователей, с переносом значения атрибута «description» из записи LDAP в поле «comments» базы пользователей VIPole и логин которых заканчивается числом, большим 31 (напр. testuser_41 или testuser_55).

```

vipole-ldap --admin-password 1234567890 \
--base-dn OU=OfficeInSPB,DC=vipole,DC=ldap,DC=sample\
--certificate /etc/vipole/cacert.pk \
--domain vipole.ldap \
--login sd_admin \
--passwd 12345678 \
--server-host 192.168.1.175 \
--server-port 37210 \
--filter "(CN>=testuser_31)" \
--mapping comments=description \
--csv-file ldap-users.csv

```

Администратор VIPole							
Параметры		Добавить пользователей		Журнал подключений		Пользователи онлайн	
				Обновить		Сбросить фильтры	
Фильтры	Логин	Исходный логин	E-Mail	Ник	Время последнего входа	Последний IP	Зарегистр
	?	?	?	?	Все время	?	Все вре
1	alicedupont	alicedupont		Alice	2016.04.27 16:55:56		2016.04.25
2	andreasschneider	andreasschneider		Andreas	2016.04.26 21:42:21		2016.04.25
3	annabrown	annabrown		Anna	2016.09.28 13:54:51		2016.04.22
4	brunomoreno	brunomoreno		Bruno	2016.04.27 21:23:14		2016.04.25
5	carolinalopes	carolinalopes		Carolina	2016.04.27 21:17:14		2016.04.25
6	charlottegirard	charlottegirard		Charlotte	2016.04.27 16:51:51		2016.04.25
7	danielaruiz	danielaruiz		Daniela	2016.04.27 21:18:29		2016.04.25
8	davidmeyer	davidmeyer		David	2016.04.26 21:55:01		2016.04.25
9	dillondelgado	dillondelgado		Dillon	2016.04.27 21:17:35		2016.04.25
10	dylanlambert	dylanlambert		Dylan	2016.04.27 16:56:53		2016.04.25
11	emanuelmartins	emanuelmartins		Emanuel	2016.04.29 23:24:54		2016.04.25
12	emmapetit	emmapetit		Emma	2016.04.27 17:25:57		2016.04.25
13	florianbecker	florianbecker		Florian	2016.04.26 21:46:10		2016.04.25
14	georgewilson	georgewilson		George	2016.09.28 13:54:12		2016.04.22
15	ismacsmith	ismacsmith		Isaac	2016.04.27 13:54:12		2016.04.22

1 > всего 2 страниц (41 записей)