Интеграция Secret Cloud Enterprise со службой каталога ALD Pro

04/07/2026

Secret Cloud Enterprise (SCE) - это защищённая платформа для совместной работы и хранения файлов, обеспечивающая безопасный обмен данными, управление доступом и поддержку корпоративных политик безопасности.

Интеграция позволяет централизованно вести базу пользователей в домене ALD Pro, обеспечивая аутентификацию и авторизацию через LDAP и Kerberos. SCE использует LDAP Bind для получения информации о пользователях и группах из каталога ALD Pro, а Kerberos обеспечивает безопасный и прозрачный вход с поддержкой сквозной авторизации (SSO). Такой подход устраняет необходимость дублирования учётных записей, упрощает администрирование и обеспечивает единое управление доступом к корпоративным сервисам.

Инструкция по интеграции разработана командой Secret Cloud Enterprise.

Руководство по настройке интеграции со службой каталога ALD Pro в системе **Secret Cloud Enterprise**

SecretTechnologies

Вкладка «Каталог»

На вкладке «Каталог» подраздела «Интеграции» (Рисунок 1) администратор может добавить интеграции со службами каталога, подключаемыми по протоколу LDAP/LDAPS:

- MS Active Directory или аналогичных, включая отечественные службы каталогов, такие как ALD Pro,
- KeyCloak в режиме каталога или провайдера SSO.

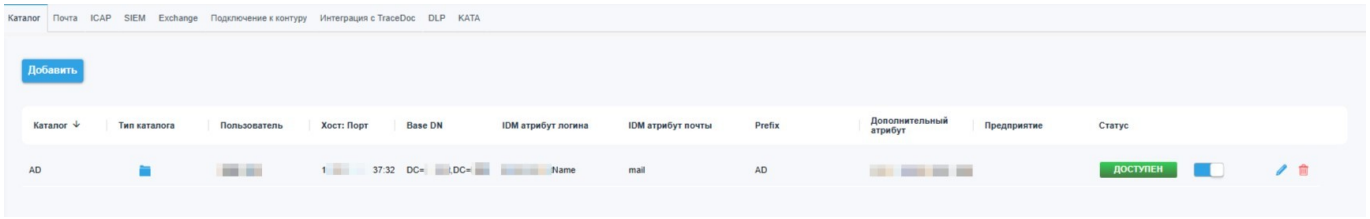

Рисунок 1. Вкладка «Каталог»

Для добавленных каталогов доступна следующая информация:

- Каталог — название каталога;
- Тип каталога — индикация типа подключённого каталога;
- Пользователь — имя учётной записи, использованной для добавления каталога;
- Хост:порт — IP-адрес и порт контроллера домена;
- Base DN — корневой элемент;
- IDM атрибут логина;
- IDM атрибут почты;
- Prefix — позволяет отметить и разграничить добавленных через синхронизацию с несколькими каталогами пользователей в списке на вкладке «Пользователи», например, для разграничения учётных записей пользователей с одинаковой фамилией, работающих
  в разных филиалах компании и записанных в разных каталогах AD;
- Дополнительный атрибут — идентификатор одного из дополнительных атрибутов, используемого в каталоге AD, для указания требуемых данных в дополнительном поле («Дополнительная информация» в рассматриваемом примере

на вкладке «Пользователи» и «Настройки пользователей» подраздела «Пользователи»), например, для указания должности сотрудника, отдела или филиала компании;

- Предприятие — индикация назначения предприятия для всех пользователей, администраторов и (или) контрагентов, импортируемых посредством интеграции с данным каталогом;
- Статус — индикация доступности каждой из служб каталогов;
- Переключатель активации интеграции со службой каталога;
- Пиктограмма редактирования параметров интеграции со службой каталога «»;
- Пиктограмма удаления интеграции со службой каталога «».

Обратите внимание: при удалении или отключении уже настроенной интеграции со службой каталога доменные пользователи потеряют доступ к системе SCE. Перед отключением или удалением интеграции со службой каталога будет выведено предупреждение с запросом подтверждения действия (Рисунок 2).

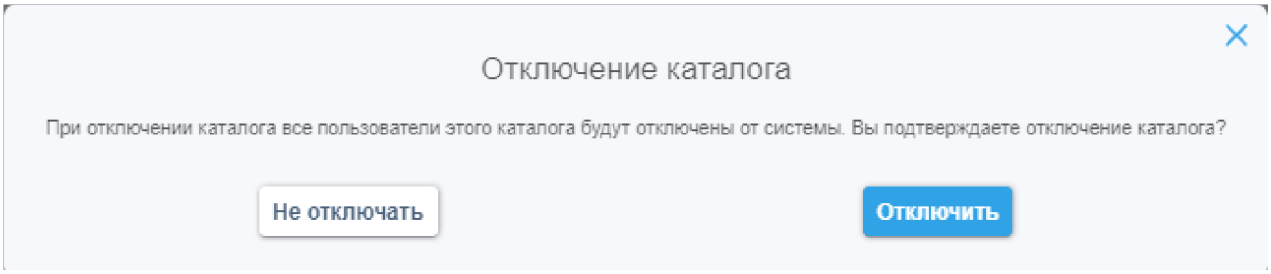

Рисунок 2. Запрос подтверждения на отключение каталога

Общая информация по добавлению новой интеграции с каталогом

Для добавления интеграции с новым каталогом используется кнопка «Добавить», расположенная в левом верхнем углу вкладки. В открывшемся всплывающем окне добавления нового каталога (Рисунок 3) идентификаторы полей снабжены пиктограммами «», при наведении курсора на которые будет отображена всплывающая подсказка по заполнению соответствующих полей.

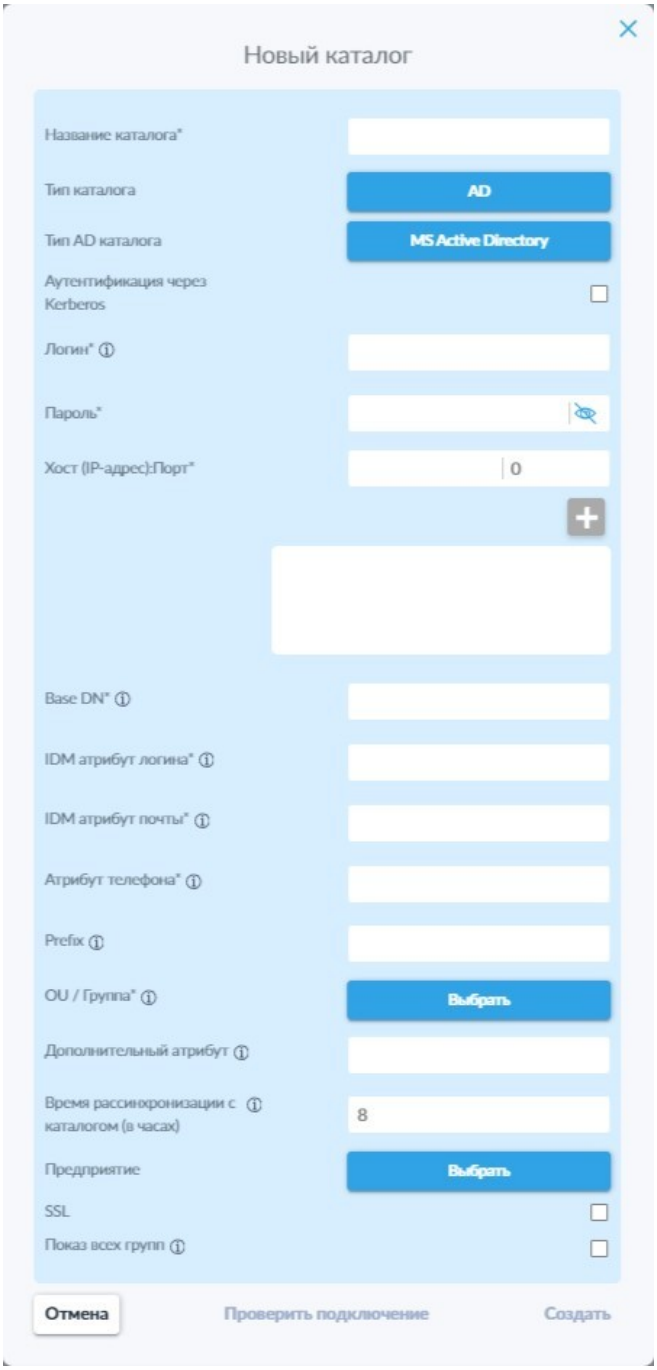

Рисунок 3. Окно добавления нового каталога

В данном окне требуется указать следующие данные (обязательные для заполнения поля отмечены символом «*»):

- Название каталога* — данное поле предоставляет возможность задать уникальное имя для данной интеграции в системе для удобного распознавания, в случае наличия нескольких интеграций;
- Тип каталога — кнопка выбора типа подключаемого каталога. Позволяет выбрать один из двух типов поддерживаемых

каталогов: «AD» или «KEY CLOAK». При выборе варианта «KEY CLOAK» часть полей ниже не отображается;

- Тип AD каталога — кнопка выбора типа подключаемого каталога Active Directory. Отображается только в том случае, если в пункте выбран вариант «AD». Позволяет выбрать тип подключаемого каталога Active Directory из двух доступных вариантов: «MS Active Directory» или «Free IPA».

> **Обратите внимание:** в случае необходимости подключения каталога «ALD Pro» используется вариант «Free IPA».

- Аутентификация через Kerberos — переключатель для использования протокола аутентификации Kerberos при авторизации и аутентификации пользователей, добавленных посредством данной интеграции с каталогом;
- Логин учётной записи* — логин пользователя, от имени которого будет выполняться интеграция.;
- Пароль учётной записи*;
- Хост (IP-адрес):Порт* — IP-адрес и порт контроллера домена. После ввода адреса и порта для подключения необходимо нажать на пиктограмму «  », которая активируется только после ввода действительных значений в данные поля. Это добавляет пару «IP-адрес:Порт» в список, расположенный в поле под данной пиктограммой;
- Base DN* — корневой элемент каталога. *Не отображается для типа каталога «KEY CLOAK»*;
- IDM атрибут логина* — название атрибута, в котором содержится логин пользователя на LDAP-сервере. *Не отображается для типа каталога «KEY CLOAK»*;
- IDM атрибут почты* — название атрибута, в котором содержится адрес электронной почты пользователя. *Не отображается для типа каталога «KEY CLOAK»*;

- Атрибут телефона* — название атрибута, которое будет браться для заполнения телефонов пользователей. *Не отображается для типа каталога «KEY CLOAK»*;
- Prefix – уникальное название, которое используется для разделения ресурсов одного каталога от ресурсов другого. *Не отображается для типа каталога «KEY CLOAK»*;
- OU/Группа* — кнопка выбора типа элементов, которые будут синхронизированы как группы пользователей. *При выборе типа каталога «KEY CLOAK» название данного пункта меняется на «Группа»*;
- Дополнительный атрибут — название атрибута для синхронизации дополнительного поля;
- Время рассинхронизации с каталогом (в часах) — задержка перед удалением пользователей каталога из системы при невозможности подключения к каталогу;
- Предприятие — возможность назначения предприятия для данной интеграции с каталогом, что позволит администратору предприятия использовать её для добавления пользователей в систему напрямую в выбранное предприятие посредством механизма синхронизации списка пользователей на соответствующей вкладке;
- SSL — переключатель, активация которого необходима в случае необходимости настройки SSL-соединения с каталогом;
- Показ всех групп — переключатель, активация которого включает древовидное отображение групп каталога в окнах импорта учётных записей пользователей.

Обратите внимание: данный функционал может работать некорректно, если хотя бы одна из групп заблокирована для получения от имени указанного выше пользователя.

После заполнения необходимых полей требуется нажать активировавшуюся кнопку «Проверить подключение».

В случае успешной проверки корректности данных и доступности каталога будет отображено всплывающее сообщение о доступности каталога (Рисунок 4).

Рисунок 4. Всплывающее окно успешной проверки подключения к каталогу

После этого необходимо нажать активировавшуюся кнопку «Сохранить», чтобы добавить интеграцию с каталогом в список активных и отобразить её на вкладке «Каталог» (Рисунок 1).

Обратите внимание: после добавления новой интеграции её необходимо включить с использованием соответствующего переключателя в строке интеграции, чтобы обеспечить возможность импорта пользователей из добавленного каталога.

Добавление интеграции со службой каталога ALD Pro

Для использования интеграции со службой каталога ALD Pro необходимо произвести следующие настройки системы Secret Cloud Enterprise:

1. Настройка сервисной учетной записи

   Для этого нужно подключиться по SSH к контроллеру домена и выполнить следующие шаги:

   a. Создать файл с именем ldap-bind.update.

   b. Внести в файл следующее содержимое:

dn: uid=ldap-bind,cn=sysaccounts,cn=etc,dc=ald,dc=company,dc=lan
add:objectclass: account
add:objectclass: simplesecurityobject
add:uid: ldap-bind
add:userPassword: securePassword
add:passwordExpirationTime: 20380119031407Z
add:nsIdleTimeout: 0

Разъяснения:

dn — уникальный идентификатор записи пользователя в LDAP,

add:objectclass: account — добавляет базовый класс для учётной записи,

add:objectclass: simplesecurityobject — добавляет класс для хранения пароля и других атрибутов безопасности,

add:uid: ldap-bind — уникальный идентификатор пользователя,

add:userPassword: securePassword — пароль для учётной записи, заменить на желаемый,

add:passwordExpirationTime: 20380119031407Z — время истечения пароля (можно адаптировать под политики безопасности),

add:nsIdleTimeout: 0 — отключает таймаут простоя для этой учетной записи.

c. Выполнить добавление пользователя следующей командой:

kinit admin && ipa-ldap-updater ldap-bind.update

2. Открыть веб-интерфейс системы SCE.

3. Перейти в раздел «Интеграция» («Настройки» → «Администрирование» → «Интеграция» → «Каталог») и нажать кнопку «Добавить» в верхнем левом углу вкладки.

1. В открывшемся окне ввести следующие параметры подключения:

- «Название каталога» — произвольное название службы каталога ALD Pro;
- «Тип каталога» — «AD»;
- «Тип AD каталога» — «Free IPA»;

«Логин» — логин сервисной учётной записи имеющей право на чтение каталога. В зависимости от настроек службы каталога может потребоваться указать логин в формате «uid,cn,dc», например: «uid=ldap-bind,cn=sysaccounts,cn=etc,dc=ald,dc=company,dc=lan» (без кавычек и пробелов);

- «Пароль» — пароль от используемой учётной записи;

- «Хост (IP-адрес) – Порт» — указать в полях адрес службы каталога и порт подключения, после чего нажать кнопку «+»;
- «Base DN» — корневой элемент каталога указывается в формате «dc=<имя_домена>», должно совпадать с доменом, использованным в логине учётной записи, например «dc=freeipa» для использованного выше примера логина;
- «IDM атрибут логина» — название атрибута, в котором содержится логин пользователя, в данном случае – «uid»;
- «IDM атрибут почты» — название атрибута, в котором содержится адрес электронной почты пользователя, например – «mail»;
- «Атрибут почты» — название атрибута, в котором содержится номер телефона пользователя, например – «phone»;
- «Prefix» — уникальное название, которое используется для разделения ресурсов одного каталога от ресурсов другого, можно оставить пустым, если планируется использование одной интеграции;
- «OU/Группа» — выбрать вариант «Группы»;
- «Дополнительный атрибут» — опционально, название атрибута для синхронизации поля дополнительной информации (произвольных полей информации из каталога);
- «Время рассинхронизации с каталогом (в часах)» — «8»;
- «Область безопасности» — указать область безопасности службы каталога, в которой размещается импортируемая группа (например, «*master*» (без кавычек));
- «Идентификатор клиента» — указать название импортируемой группы;
- «SSL» — активировать переключатель;
- «Показ всех групп» — опционально, включает древовидное отображение групп каталога в окнах импорта учётных записей,

Обратите внимание: данная настройка может вызывать ошибки отображения, если для учётной записи, используемой для синхронизации, недоступно чтение всех групп каталога;

- Нажать кнопку «Проверить подключение» — при успешном подключении будет отображено уведомление об успешной проверке соединения со службой каталога A LD Pro;
- Нажать кнопку «Сохранить» в нижней части окна.

4. После создания интеграции с каталогом необходимо активировать её с помощью соответствующего переключателя в строке созданной интеграции.

5. Перейти в раздел «Пользователи», нажать кнопку «Синхронизировать из каталога». В открывшемся окне в левом столбце выбрать название созданной службы каталога. Справа в строке поиска ввести имя группы и нажать кнопку «Поиск». Найденная группа отобразится в поле ниже. Поставить отметку в строке группы и нажать кнопку «Сохранить». Будет запущен процесс импорта учётных записей из указанной группы. После завершения импорта будет отображено уведомление об успешном импорте пользователей.