Интеграция Secure Authentication Server от MFASOFT со службой каталога ALD Pro

04/07/2026

Secure Authentication Server от MFASOFT— это платформа многофакторной аутентификации, которая обеспечивает высокий уровень защиты доступа к корпоративным системам и сервисам за счёт использования современных методов подтверждения личности. Решение поддерживает широкий набор механизмов OTP, адаптивную аутентификацию и интеграцию с различными ИТ-системами, обеспечивая централизованное управление политиками безопасности и полный аудит событий.

Интеграция с **ALD Pro** даёт возможность получать актуальную информацию о пользователях и группах из единого каталога, использовать эти данные при построении политик аутентификации, автоматически назначать методы MFA и применять контекстную логику. Также реализуется прозрачная аутентификация пользователей по протоколу Kerberos, что позволяет интегрировать MFA без изменения пользовательского опыта. Администраторы домена могут получать доступ к панели управления SAS с учётом ролевой модели ALD Pro.

Инструкция подготовлена разработчиками **MFASOFT**.

Интеграция с ALD Pro

Статья описывает настройку службы каталога ALD Pro для работы с программным комплексом MFASOFT Secure Authentication Server (SAS).

В продукте SAS предусмотрена возможность интеграции со службами каталогов, поддерживающими протокол LDAP (или его защищенную версию LDAPS). Эта интеграция позволяет:

- синхронизировать учетные записи и группы из каталога LDAP в базу данных SAS;
- автоматически назначать им (а также отзывать у них) токены и административные роли;
- использовать пароль LDAP как временный пароль для приостановленных токенов;
- вводить пароль LDAP вместо ПИН-кода в одной строке с OTP (если это задано политикой токенов);
- использовать двухэтапную аутентификацию (пароль LDAP перед одноразовым паролем, или наоборот) с токенами типа «запрос-ответ», в том числе в сценариях с адаптивной (условной) аутентификацией, где цепочка (последовательность шагов) аутентификации будет зависеть от выполнения условий;
- усиливать вход по паролю LDAP проверкой одноразового пароля или подтверждением пуш-уведомления при интеграции через агент LDAP-прокси.

Чтобы интегрировать программный комплекс MFASOFT SAS со службой каталога ALD Pro и задействовать все эти возможности, нужно выполнить следующее:

- выбрать пользователей и группы для синхронизации с ПК MFASOFT SAS;
- создать сервисную учетную запись для подключения по LDAP:
- установить и настроить агент(ы) синхронизации LDAP;
- включить синхронизацию LDAP;
- включить LDAP-аутентификацию на сервере аутентификации SAS;
- включить политики использования LDAP-пароля вместо ПИН-кода для выбранных типов токенов;
- включить предварительную аутентификацию и настроить ее правила на сервере аутентификации SAS;
- включить предварительную аутентификацию и настроить ее правила на агенте для FreeRADIUS;
- установить и настроить агент(ы) LDAP-прокси.

Выбор пользователей и групп

Чтобы подготовить каталог на базе ALD Pro к интеграции с программным комплексом MFASOFT SAS, для **каждого** виртуального сервера аутентификации выполните следующее:

1. Войдите на портал управления ALD Pro с учетными данными администратора каталога.
2. Найдите пользователей и группы, которые будут синхронизироваться в данный виртуальный сервер.
3. Убедитесь, что все необходимые для синхронизации свойства синхронизируемых пользователей (имя, фамилия, логин, электронная почта) заполнены и соответствуют

форматам этих свойств в SAS, а логины не совпадают с логинами локальных (созданных вручную или импортом из файла) пользователей в этом виртуальном сервере SAS.

4. Выберите или создайте базу поиска (подразделение, в котором или под которым должны находиться все синхронизируемые пользователи и группы).
5. Включите каждого синхронизируемого пользователя в одну или несколько синхронизируемых групп.

Синхронизируются только пользователи, входящие хотя бы в одну из синхронизируемых групп (непосредственно или в группы, вложенные в синхронизируемые).

Создание сервисной учетной записи

Для подключения сервера и агентов к каталогу по протоколу LDAP (для синхронизации объектов и аутентификации пользователей) нужно создать сервисную учетную запись в ALD Pro. Эта запись не будет POSIX-пользователем, не получит прав на вход в компьютеры домена и не будет отображается в портале управления ALD Pro, а будет имеет права только на чтение LDAP. Для этого:

1. Подключитесь по SSH к контроллеру домена.
2. Создайте файл с именем srv-sas-bind.update.
3. Добавьте в файл строки:

```
dn: uid=srv-sas-bind,cn=sysaccounts,cn=etc,dc=mfasoft,dc=local
add:objectclass: account
add:objectclass: simplesecurityobject
add:uid: srv-sas-bind
add:userPassword: $Password1
add:passwordExpirationTime: 20380119031407Z
add:nsIdleTimeout: 0
```

4. Добавьте эту запись в каталог:

```
# kinit admin && ipa-ldap-updater srv-sas-bind.update
```

Установка LSA

Установите и настройте агент(ы) синхронизации LDAP (LSA) в соответствии с документом «Secure Authentication Server. Синхронизация LDAP», выбрав в файле config.ini схему FreeIPA и указав созданную ранее сервисную учетную запись и ее пароль:

```
scheme = freeipa.map
login = srv-sas-bind,cn=sysaccounts,cn=etc,dc=mfasoft,dc=local
password = $Password1
```

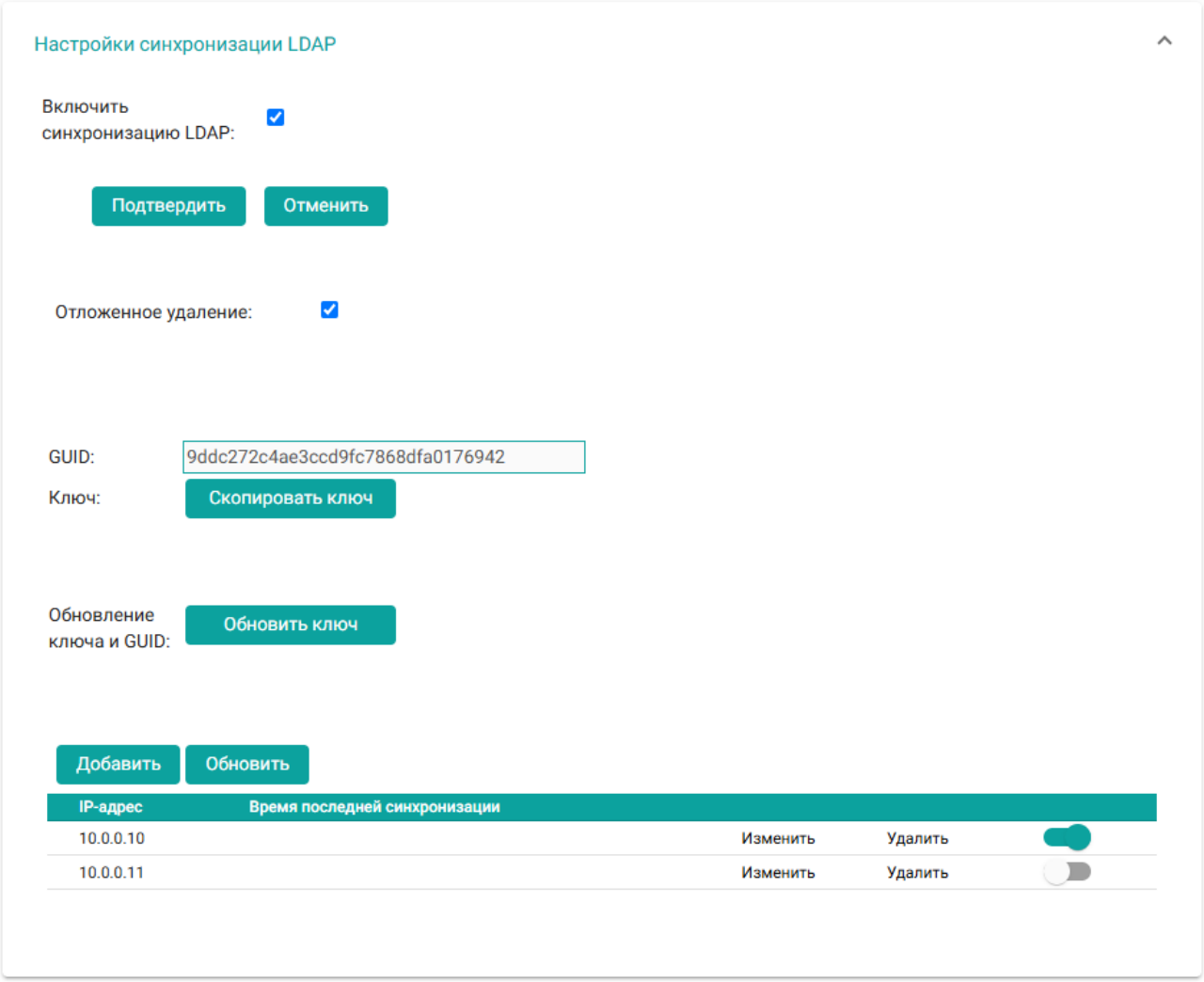
Включение синхронизации LDAP

Secure Authentication Server поддерживает автоматическую синхронизацию пользователей и групп из каталогов LDAP. В консоли можно настроить (или проверить) параметры подключения агентов LDAP к модулю синхронизации LDAP.

Для пользователей и групп, синхронизируемых через LDAP, можно установить отложенное удаление, чтобы после удаления из LDAP-источника они удалялись из базы SAS не сразу, а через 24 часа. Если пользователи и группы были удалены по ошибке, то достаточно вернуть их в LDAP-источник, и после повторной синхронизации пометка на удаление в базе SAS будет снята.

Чтобы включить синхронизацию LDAP в выбранные виртуальные серверы, для **каждого** из этих серверов:

1. Войдите в консоль с учетными данными оператора этого виртуального сервера.
2. Выберите на вкладке **Виртуальные серверы** нужный.
3. Выберите вкладку второго ряда **Настройки**.
4. Раскройте панель **Настройки синхронизации LDAP**.
5. Установите флажок **Включить синхронизацию LDAP**.
6. Если нужно, установите флажок **Отложенное удаление**.
7. Нажмите кнопку **Добавить**.
8. Введите IP-адрес машины, на которой запущен агент LDAP.
9. Нажмите кнопку **Сохранить**.
10. Передвиньте вправо переключатель в появившейся строке с адресом агента.
11. Повторите пункты 7 – 10 для остальных агентов, данные от которых будут синхронизироваться на выбранный виртуальный сервер.



Если между модулем синхронизации LDAP и агентом LDAP используется трансляция сетевых адресов (NAT), то в качестве IP-адреса агента нужно указывать интерфейс маршрутизатора NAT, через который запросы приходят к модулю синхронизации LDAP.

Отложенное удаление действует только на те учетные записи пользователей и групп, которые были синхронизированы, когда отложенное удаление было включено.

Можно временно выключить синхронизацию данных с определенных агентов, не удаляя при этом синхронизированные объекты (пользователей и группы). Для этого сделайте следующее:

1. Войдите в консоль с учетными данными оператора виртуального сервера.
2. Выберите на вкладке **Виртуальные серверы** нужный.
3. Выберите вкладку второго ряда **Настройки**.
4. Раскройте панель **Настройки синхронизации LDAP**.
5. Передвиньте вправо переключатель в строке с адресом нужного агента.

Включение аутентификации LDAP

Если требуется, включите аутентификацию LDAP в **корневом** сервере и проверьте ее настройки в выбранных виртуальных серверах. Для этого:

1. Войдите в консоль с учетными данными оператора корневого виртуального сервера.
2. Выберите на вкладке **Виртуальные серверы** нужный.
3. Выберите вкладку второго ряда **Настройки**.
4. Раскройте панель **Общие настройки**.
5. Нажмите кнопку **Изменить**.
6. Отметьте флажок **LDAP аутентификация***.
7. Нажмите кнопку **Подтвердить**.

Параметры подключения к серверу LDAP передаются в процессе синхронизации пользователей агентом LSA на сервер SAS, если включен параметр send_ldap_config в файле config.ini агента LSA:

```
send_ldap_config = yes
```

После сохранения изменений параметров можно выполнить тестовую аутентификацию на первом и втором сервере LDAP, нажав кнопку **Тест** для первого и второго узлов LDAP соответственно.

Параметр	Описание
LDAP сервер №1	Адрес или имя основного сервера LDAP
LDAP сервер №2	Адрес или имя резервного сервера LDAP
Уникальный идентификатор	Сервисная учетная запись для доступа к каталогу LDAP
Область поиска	База поиска в каталоге LDAP
Порт	Номер порта протокола LDAP
Использовать SSL	Использовать ли для подключения LDAP через SSL (LDAPS)
Время переключения на первый узел LDAP (сек)	Интервал между попытками возврата на основной сервер LDAP после переключения на резервный:
Время ожидания ответа (сек)	Тайм-аут подключения к серверам LDAP

Включение политики LDAP-пароля вместо ПИН-кода

Если требуется, включите политики использования LDAP-пароля вместо ПИН-кода в выбранных виртуальных серверах для выбранных типов токенов. Для этого для **каждого** выбранного виртуального сервера:

1. Войдите в консоль с учетными данными оператора этого виртуального сервера.
2. Выберите на вкладке **Виртуальные серверы** нужный.
3. Выберите вкладку второго ряда **Политики**.
4. Раскройте по очереди панели **Политика аппаратного токена**, **Политика программного токена** и **Политика SMS/Telegram/почтового токена**.
5. Нажмите кнопку **Изменить**.
6. Установите флажок **Использовать LDAP пароль в качестве ПИН-кода**.
7. Нажмите кнопку **Подтвердить**.
8. Повторите шаги 4 – 7 для каждого выбранного типа токенов.

Настройка предварительной аутентификации на SAS

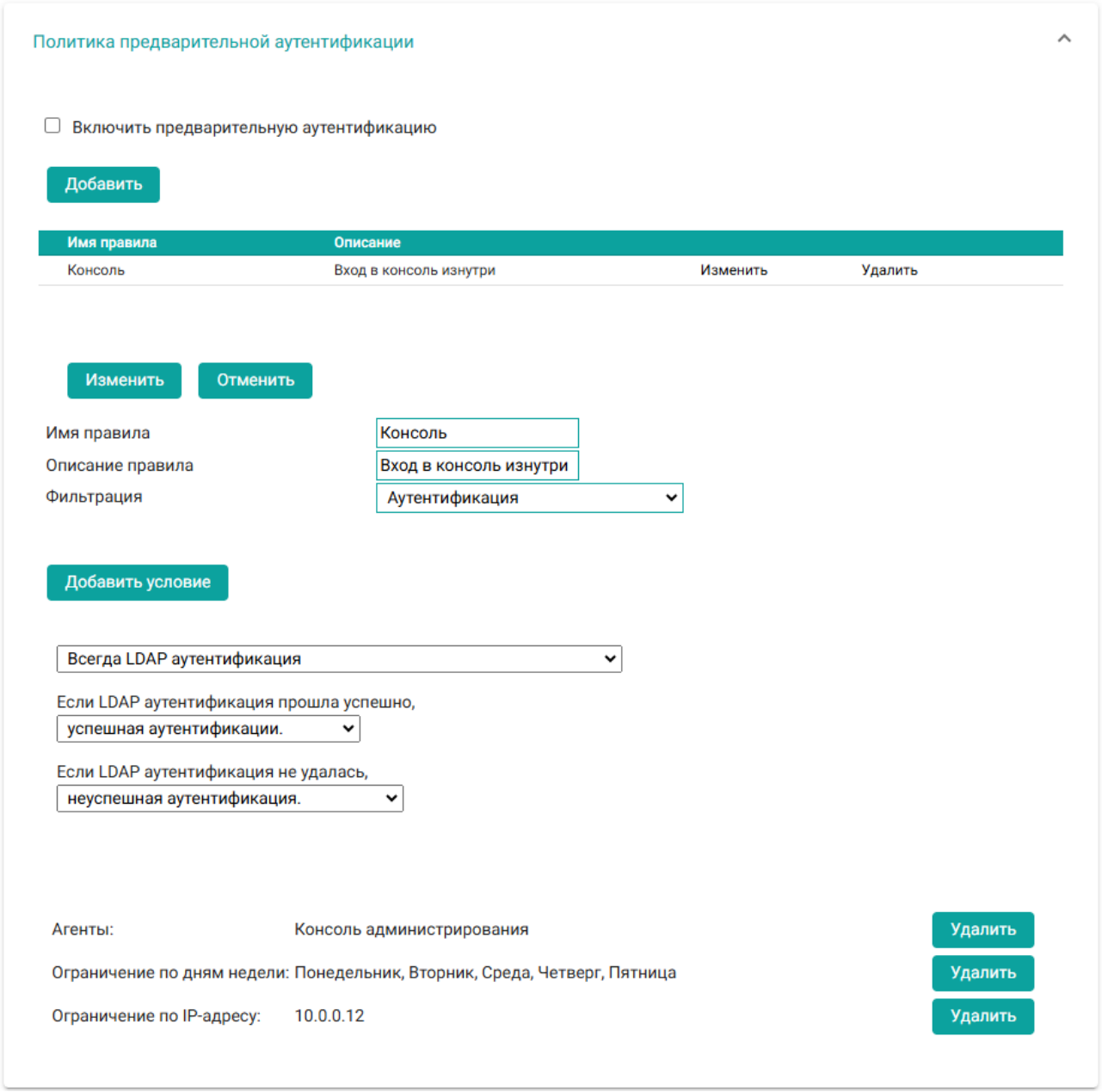
Политика предварительной аутентификации задает условия, при соблюдении которых будет разрешена аутентификация по одноразовым паролям или пуш-уведомлениям. Политика состоит из правил, каждое из которых состоит из одного или нескольких условий. К условиям в правиле применяется логическое И, а к самим правилам – логическое ИЛИ, поэтому значение имеет порядок следования правил – выполниться первое из правил, для которого выполняются все условия, при этом сортируются правила по их названиям. Доступны следующие фильтры:

Условия	Возможные значения
Агенты	Одно из: • **API** • **RADIUS** • **Портал самообслуживания** • **Консоль администрирования** • **ADFS** • **KEYCLOAK** • **LDAP прокси**
Ограничение по дате	Любые из: • **Начальная дата** • **Конечная дата**
Ограничение по дням недели	Любые из: • **Понедельник** • **Вторник** • **Среда** • **Четверг** • **Пятница** • **Суббота** • **Воскресенье**
Ограничение по IP-адресу	Одно из: • **Список IP-адресов** • **Диапазон IP-адресов** • **Маска подсети IP-адреса**
Группы	Все из:

	• **Логика** (пользователь принадлежит одной или всем группам) • **Для групп** (**Синхронизированных** или **Локальных**)
Тип токена	Одно из: • **Аппаратный** • **Программный** • **Мобильный пуш** • **SMS** • **Почта** • **Telegram**
Аутентификация	Все из: • Условие проверки пароля LDAP: ○ **Всегда LDAP аутентификация** (пароль LDAP проверяется всегда) ○ **Когда у пользователя нет токенов LDAP аутентификация** ○ **Когда у пользователя нет активных токенов LDAP аутентификация** ○ **Аутентификация без верификации** (пароль LDAP не проверяется никогда) ○ **Сперва HOTP/TOTP, затем LDAP аутентификация** (пароль LDAP проверяется после успешной проверки одноразового пароля) • Действие при успешной аутентификации LDAP: ○ **успешная аутентификация.** (не проверять второй фактор) ○ **запрос на аутентификацию в SAS.** (с токеном «запрос-ответ») • Действие при неуспешной аутентификации LDAP: ○ **неуспешная аутентификация.** ○ **перенаправить аутентификацию в SAS.** (с токеном «запрос-ответ»)

Чтобы настроить политику предварительной аутентификации:

1. Войдите в консоль с учетными данными оператора виртуального сервера.
2. Выберите на вкладке **Виртуальные серверы** нужный.
3. Выберите вкладку второго ряда **Политики**.
4. Раскройте панель **Политика предварительной аутентификации**.
5. Нажмите кнопку **Добавить** для добавления нового правила.
6. Заполните обязательное поле **Имя правила** и необязательное поле **Описание правила**.
7. Выберите тип фильтра и задайте условия.
8. После добавления каждого фильтра нажмите кнопку **Добавить условие**
9. После того, как добавлено последнее условие, нажмите кнопку **Добавить**.
10. Повторите пункты 5 – 9 для остальных правил.
11. Установите флажок Включить предварительную аутентификацию.



Если включить политику предварительной аутентификации, но не задать ни одного правила, то аутентификация (включая вход в консоль) на виртуальном сервере будет полностью заблокирована.

Если не включена LDAP-аутентификация, то в условиях аутентификации будет доступна только аутентификация без верификации.

Если отключить предварительную аутентификацию, то сами правила с их фильтрами не удалятся.

Настройка предварительной аутентификации на FRA

Эта возможность доступна только начиная с версии FRA 1.9

Агент FRA позволяет настроить правила предварительной аутентификации на самом агенте (по аналогии с правилами предварительной аутентификации сервера аутентификации SAS). Для настройки правил предварительной аутентификации необходимо включить эту опцию в секции [preauth]:

```
enable = yes
```

Далее необходимо создать правила предварительной аутентификации, которые будут определены в параметре rule[], где квадратные скобки обязательны. Параметры правила должны разделяться точкой с запятой. Общий шаблон правила имеет вид:

rule[] = [список IP-адресов через запятую или пусто];[список групп LDAP через запятую или пусто];[логическая операция для правил групп LDAP или пусто];[тип аутентификатора или пусто];[тип операции]

Список логических операций:

- 0 – логическое ИЛИ (пользователь принадлежит хотя бы одной из групп)
- 1 – логическое И (пользователь принадлежит всем группам)

Список доступных значений параметра типа аутентификатора:

- h – аппаратный токен
- g – программный токен
- s – SMS-токен
- e – почтовый токен
- t – токен Telegram
- p – программный токен к режиме пуш
- пусто – любой токен

Список доступных операций:

- 0 – проброс запроса в SAS
- 1 – только LDAP-аутентификация
- 2 – в случае успешной LDAP-аутентификации запрос в SAS
- 3 – в случае неуспешной LDAP-аутентификации запрос в SAS
- 4 – всегда возвращать успешную аутентификация (Access-Accept)
- 5 – всегда возвращать неуспешную аутентификацию (Access-Reject)
- 6 – аутентификация LDAP+OTP в одну строку

Пример правил:

- rule[]=;;;;5 – агент всегда возвращает Access-Reject;
- rule[]=10.0.0.100;VPN1,VPN2,VPN3;0;t;2 – при запросе с хоста с IP-адресом 10.0.0.100 под учетной записью, входящей в хотя бы одну из групп, необходимо выполнить LDAP-аутентификацию и в случае успеха выполнить аутентификацию в SAS через токен Telegram;

- rule[]=10.0.0.100,10.0.0.101;Admins,VPN;1;;2 – при запросе с хостов с IP-адресами 10.0.0.100 или 10.0.0.101 под учетной записью, входящей в группы Admins и VPN, необходимо выполнить LDAP-аутентификацию и в случае успеха выполнить аутентификацию в SAS одним из токенов типа «запрос-ответ»;
- rule[]=10.0.0.100;NO_2FA_USERS;;;1 – при запросе с хоста с IP-адресом 10.0.0.100 под учетной записью, входящей в группу NO_2FA, выполнить только LDAP-аутентификацию и вернуть результат.

При обновлении FRA с версий младше 1.9 в файл config.ini потребуется добавить новые параметры:

```
#LDAP enable
ldap_enable = yes
#LDAP_Server1
ldap_server_1 = 10.0.0.10
#LDAP_Server2
ldap_server_2 = 10.0.0.11
#LDAP timeout (seconds)
ldap_timeout = 10
# Time out to restore to first ldap (seconds)
timeout_to_restore_to_first_ldap = 180
# LDAP SSL
ldap_ssl = no
#LDAP port
ldap_port = 389
#LDAP scheme (active_directory, freeipa)
ldap_scheme = freeipa
#LDAP search base
search_base = OU=2FA,DC=MFASOFT,DC=LOCAL
#LDAP login
login = CN=SRV-SAS-BIND,CN=SYSACCOUNTS,CN=ETC,DC=MFASOFT,DC=LOCAL
#LDAP password
password = $Password1
#LDAP group name field
ldap_group_name_field = cn
#LDAP login field
ldap_login_field = sAMAccountName
#OTP digits
otp_digits = 10
#LDAP password is prefix
ldap_prefix = yes
```

Установка LPA

Если требуется, установите и настройте агент(ы) LDAP-прокси (LPA) в соответствии с документом «Secure Authentication Server. Интеграция через LDAP», выбрав в файле config.ini схему FreeIPA и указав созданную ранее сервисную учетную запись и ее пароль:

```
ldap_server_scheme = 2
login = srv-sas-bind,CN=sysaccounts,CN=etc,DC=mfasoft,DC=local
password = $Password1
```