Инструкция по быстрому запуску СКДПУ НТ Шлюз доступа

Данная инструкция предназначена для администраторов, проводящих первоначальную настройку СКДПУ НТ Шлюз доступа 7 и выше.

Далее в тексте СКДПУ НТ Шлюз доступа для упрощения обозначается как "СКДПУ".

1. Подготовка к проведению работ

Чтобы провести настройки, необходимо подготовить следующие параметры:

- IP адрес, маска подсети и шлюз для настройки на виртуальной машине. Если требуется включение нескольких интерфейсов – подготовить настройки и для них.
- адреса серверов NTP, DNS.
- при наличии источника централизованной авторизации (Active Directory, LDAP и т.п) подготовить адрес и учетные данные для подключения. При использовании Active Directory желательно иметь возможность создать в структуре AD 2-3 группы (Security – Global Distribution) для подключения пользователей с привязкой к группам
- адрес и учетные данные сервера SMTP для отправки уведомлений.
- При необходимости настраивать межсетевые экраны, роутинг и систему виртуализации необходимо обрести соответствующие права или контакты необходимых специалистов.
- Подготовить таблицу с адресами, протоколами доступа и учетными данными на тестовых целевых серверах.
- Подготовить АРМ администратора (обычно это Windows 7, 10. Можно и Linux), где будут доступны современный браузер, ssh и RDP клиенты, почтовый клиент для приема оповещений.

1.1. Подключение СКДПУ в исполнении ПАК

Для подключения СКДПУ в исполнении ПАК к инфраструктуре объекта необходимо:

1. Распаковать ПАК из транспортной тары.
2. Подключить ПАК к сети электропитания.
3. Подключить к разъемам ПАК необходимые периферийные устройства (монитор, клавиатура)
4. Подключить сетевой интерфейс в необходимый коммутатор посредством сетевого кабеля.
5. Подготовить АРМ администратора (обычно это Windows 7-10 или Linux), где будут доступны современный браузер, ssh и RDP клиенты, почтовый клиент для приема оповещений.

1.2. Подключение СКДПУ в исполнении VA

Для подключения СКДПУ в исполнении VA к виртуальной инфраструктуре объекта необходимо:

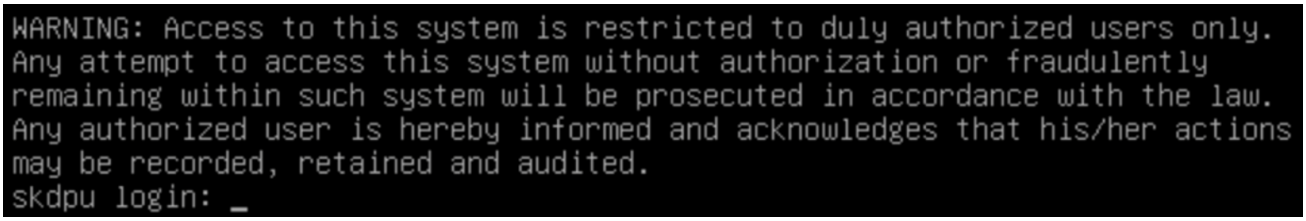
1. Требуется подготовить целевой сервер системы виртуализации, выделив на нем необходимые ресурсы в зависимости от предполагаемой нагрузки. В минимальной конфигурации параметры следующие: 3-4 ядра, 4-6 Гб RAM, 80 Гб диска, 1 сетевой интерфейс.
2. Скачать и сохранить готовую виртуальную машину по предоставленной ссылке.
3. Импортировать предоставленную виртуальную машину в систему виртуализации.
4. Подключить виртуальный сетевой интерфейс в необходимый виртуальный коммутатор.
5. Подготовить АРМ администратора (обычно это Windows 7-10 или Linux), где будут доступны современный браузер, ssh и RDP клиенты, почтовый клиент для приема оповещений.

2. Порядок запуска и первоначальной настройки

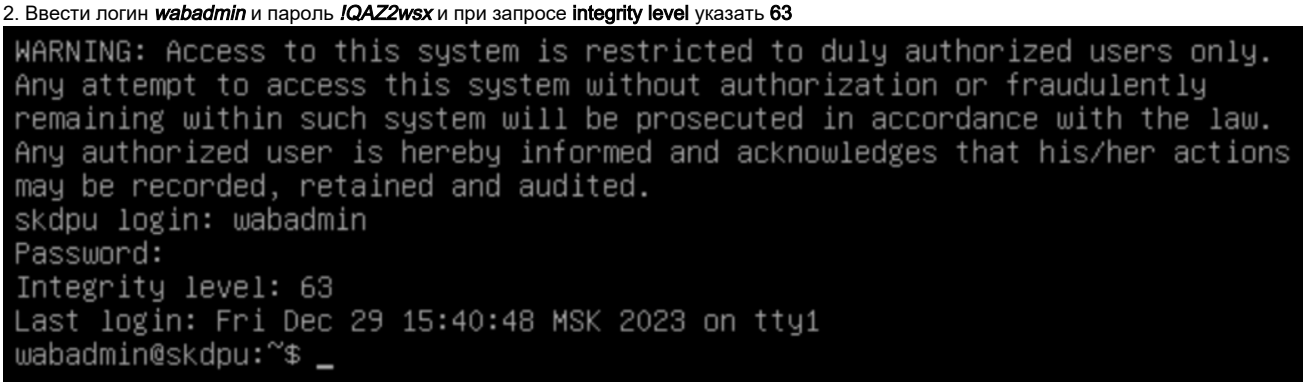
Данный пункт идентичен для каждого из вариантов исполнения СКДПУ.

Запустить ПАК/виртуальную машину.

1. После подключения к консоли дождаться приглашения операционной системы.



2. Ввести логин ***wabadmin*** и пароль ***!QAZ2wsx*** и при запросе **integrity level** указать **63**



3. Получить права суперпользователя:

- выполнить команду ***super*** и ввести пароль ***!QAZ2wsx***
- выполнить команду ***sudo -i*** и снова ввести пароль ***!QAZ2wsx***

```
WARNING: Access to this system is restricted to duly authorized users only.
Any attempt to access this system without authorization or fraudulently
remaining within such system will be prosecuted in accordance with the law.
Any authorized user is hereby informed and acknowledges that his/her actions
may be recorded, retained and audited.
skdpu login: wabadmin
Password:
Integrity level: 63
Last login: Fri Dec 29 15:40:48 MSK 2023 on tty1
wabadmin@skdpu:~$ super
[sudo] password for wabsuper:
wabsuper@skdpu:/home/wabadmin$ sudo -i
[sudo] password for wabsuper:
root@skdpu:~#
```

4. Настроить сетевой интерфейс в файле /etc/network/interfaces

- открыть файл ***/etc/network/interfaces*** с помощью текстового редактора (например, nano или vim)

```
root@skdpu:~# nano /etc/network/interfaces
```

Пример конфигурационного файла для **динамической** IP-адресации:

```
  GNU nano 2.7.4               File: /etc/network/interfaces

auto lo
iface lo inet loopback


auto eth0
iface eth0 inet dhcp
```

Пример конфигурационного файла для **статической** IP-адресации:

```
  GNU nano 2.7.4                                File: /etc/network/interfaces

auto lo
iface lo inet loopback


auto eth0
iface eth0 inet static
   address 10.0.128.100
   netmask 255.255.0.0
   gateway 10.0.0.1
```

5. Ввести команду **systemctl restart networking** для перезапуска сетевой службы.

```
root@skdpu:~# systemctl restart networking
```

6. Ввести команду **ifconfig** для проверки сетевых настроек.

```
root@skdpu:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.128.100  netmask 255.255.0.0  broadcast 10.0.255.255
        ether 00:50:56:96:0d:86  txqueuelen 1000  (Ethernet)
        RX packets 319  bytes 20707 (20.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 21  bytes 1688 (1.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 7722  bytes 974244 (951.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7722  bytes 974244 (951.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

7. После перезагрузки системы проверить SSH-соединение к консоли СКДПУ при помощи команды **ssh wabadmin@<ip-адрес хоста> -p 2242**

```
C:\Users\Администратор>ssh wabadmin@10.0.128.100 -p 2242
The authenticity of host '[10.0.128.100]:2242 ([10.0.128.100]:2242)' can't be established.
ECDSA key fingerprint is SHA256:[redacted]
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.0.128.100]:2242' (ECDSA) to the list of known hosts.
wabadmin@10.0.128.100's password:
Last login: Mon Jan  8 21:13:28 2024 from 172.16.136.246
wabadmin@skdpu:~$
```

8. Проверить доступность web-интерфейса, перейдя по IP-адресу хоста СКДПУ в браузере АРМ администратора (см. следующий пункт).

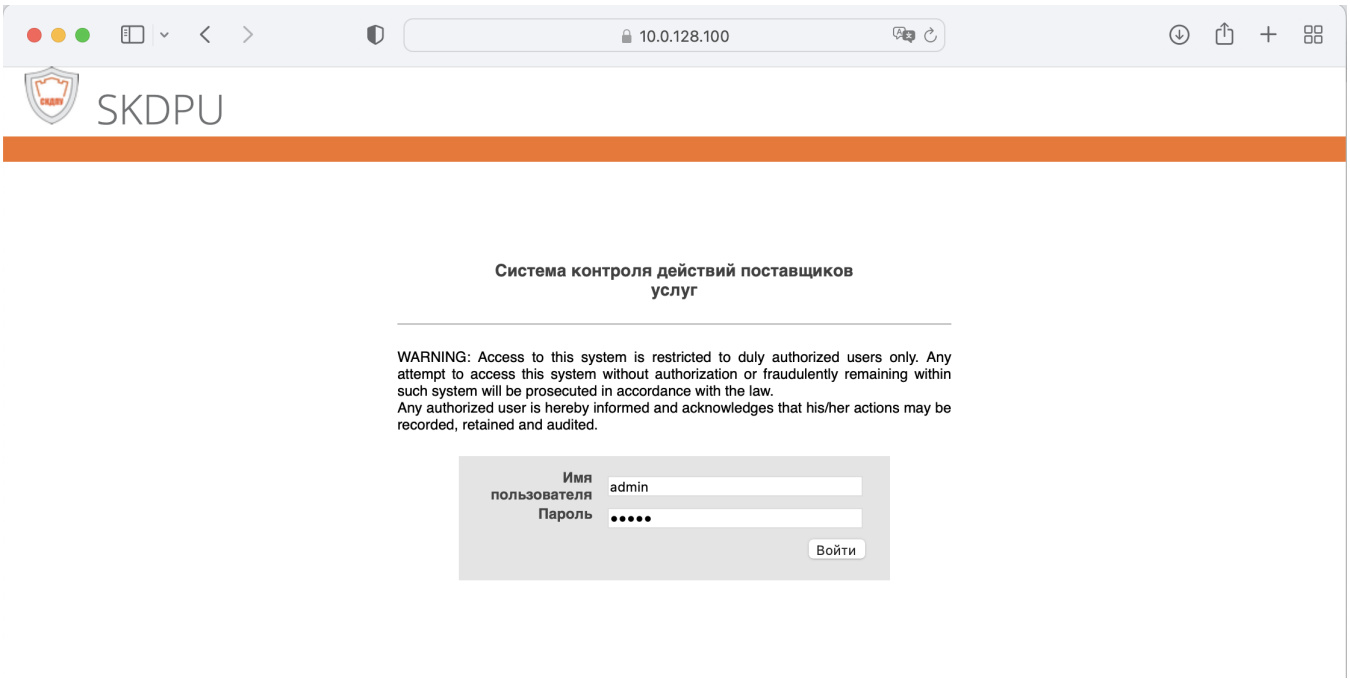
3. Настройка системы в веб-интерфейсе

3.1. Первичный вход

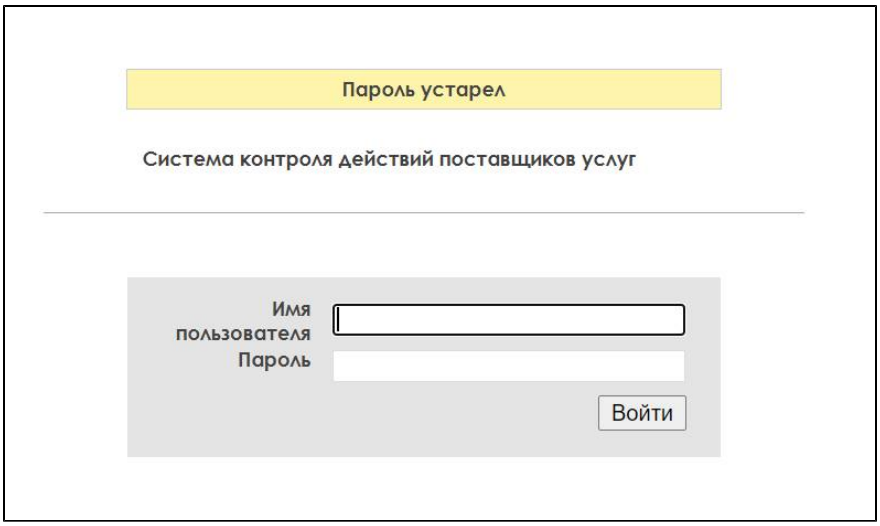
Пройдите по ссылке **https://<ip хоста СКДПУ>**

> **Параметры доступа по умолчанию**
>
> **Логин** – ***admin***
> **Пароль** – ***admin***

Откроется интерфейс первичной инициализации устройства.



Если этого не произошло, а появилось предупреждение "Пароль устарел", необходимо выполнить рекомендации раздела **"Устранение возможных проблем"** данной инструкции.



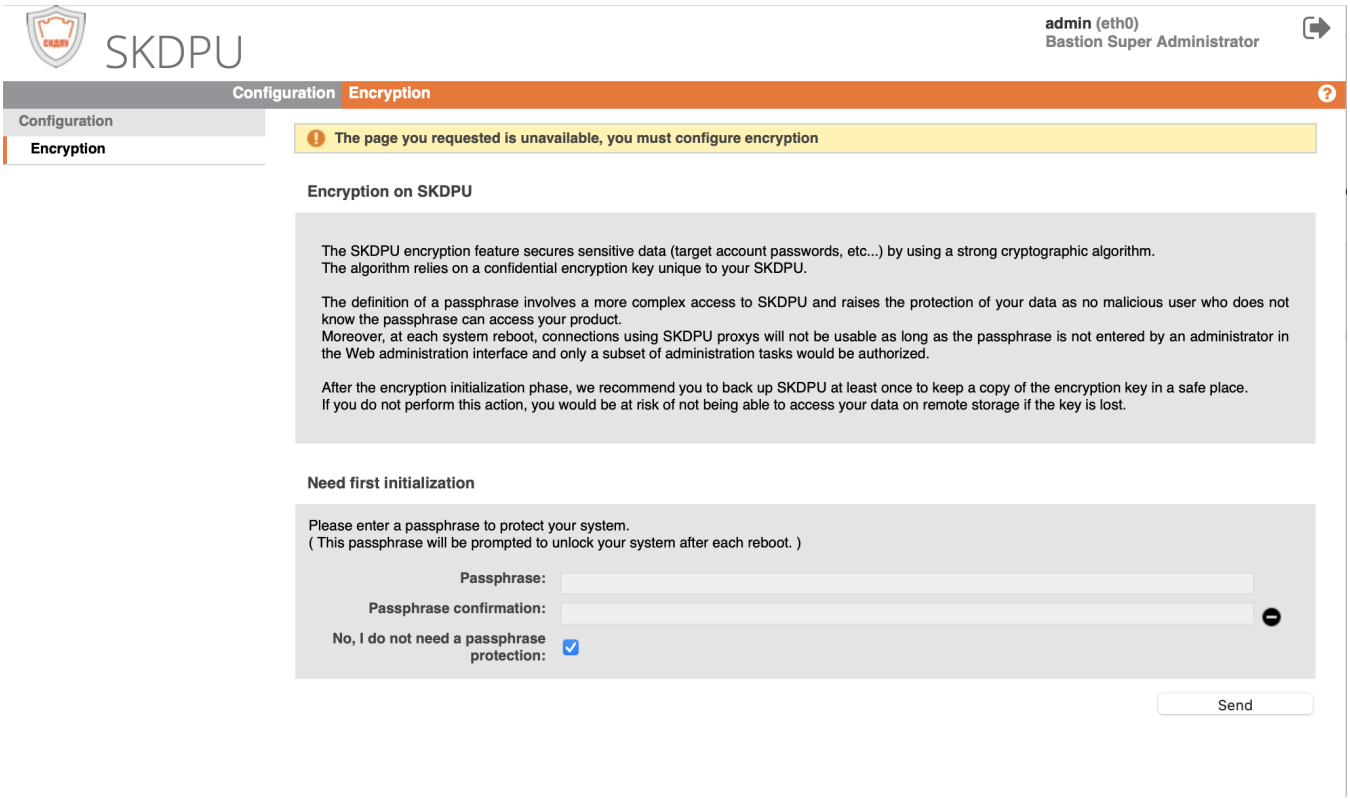
3.2. Настройка шифрования

Настройка данного параметра обеспечивает повышенный уровень защищенности данный системы, препятствующий восстановлению и доступу к данным в случае несанционированного доступа к резервным копиям, а также к самой ВМ системы.

В случае утери ранее введенной ***Passphrase*** восстановление и доступ к БД системы будет невозможен!

В демо-зонах шифрование диска рекомендуется не применять, поэтому выберите пункт ***No, i don't need***... и нажмите ***Send***.

В случае если данный параметр является требованием безопасности – введите ***Passphrase*** и нажните ***Send***.



С этого момента активируется демо-лицензия и будет доступен полный функционал системы в течение 30 дней, для 5 сессий и 15 устройств.

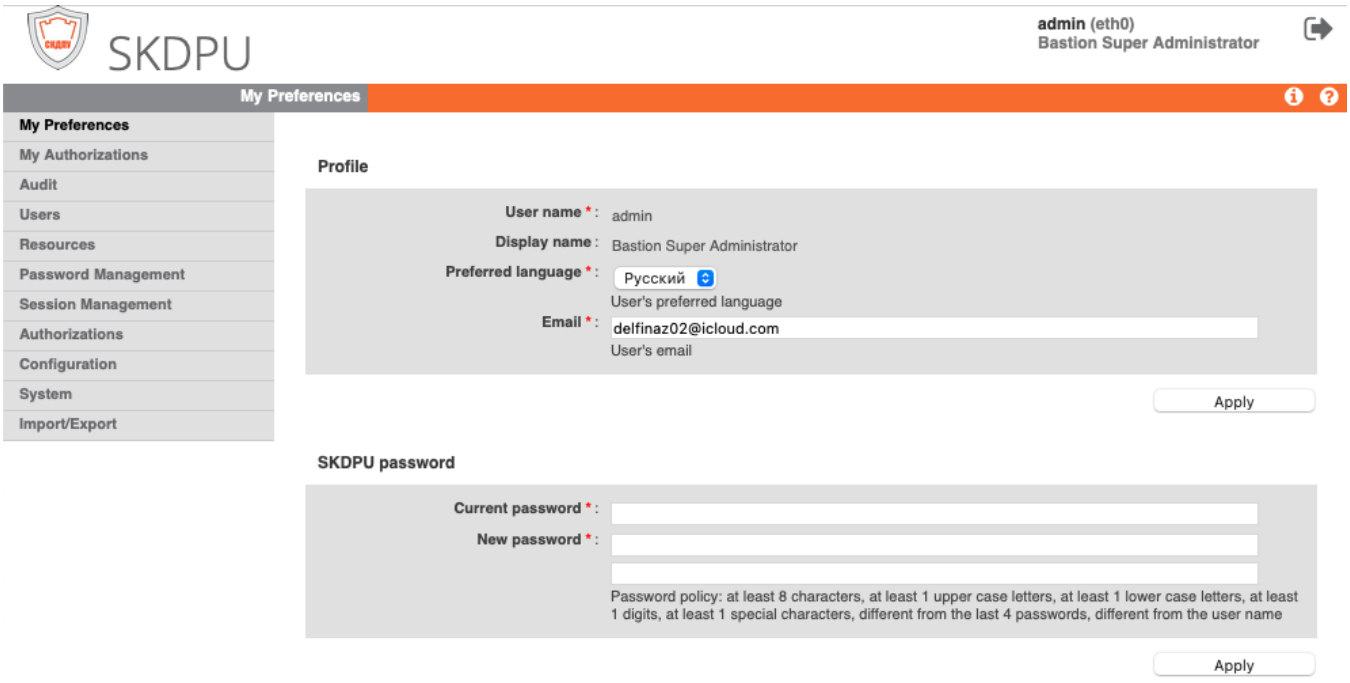
При необходимости обратитесь за расширенной демо-лицензией по email support@it-bastion.com.

Далее, необходимо установить системные настройки устройства (см. следующий пункт)

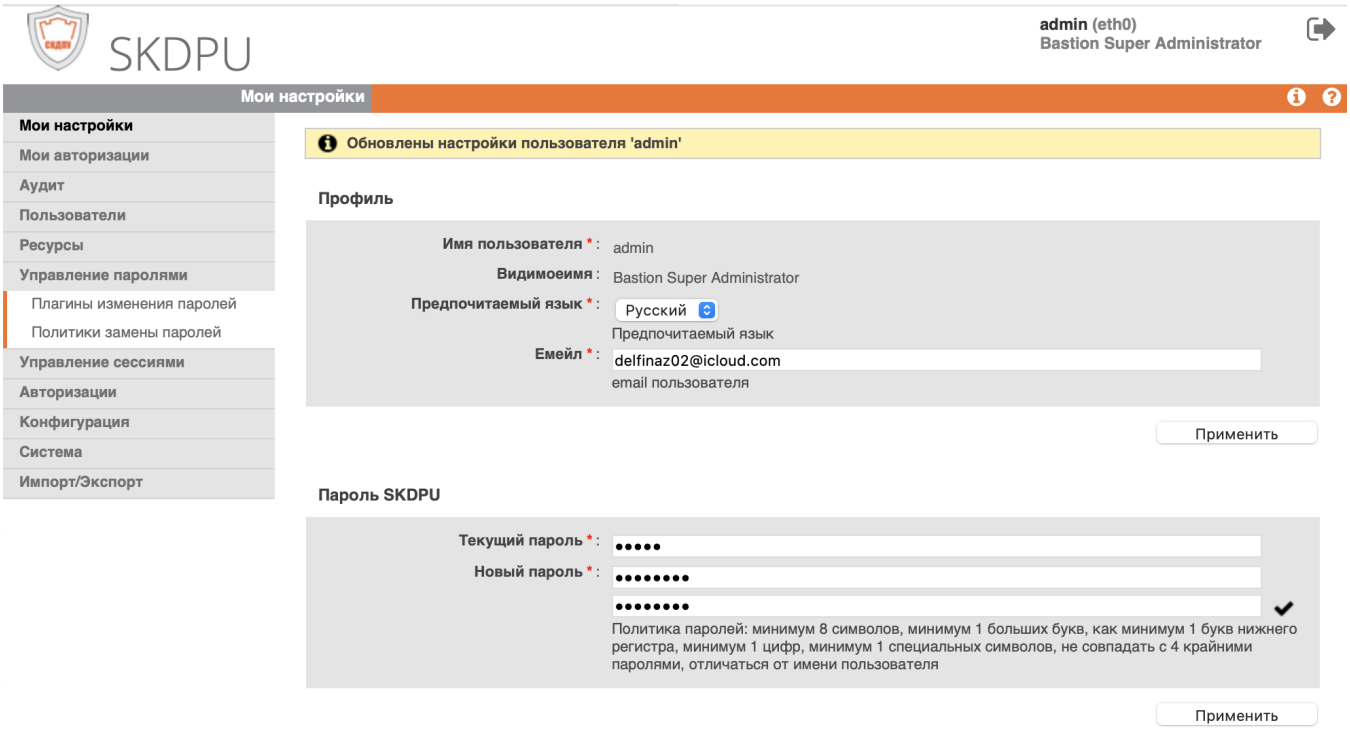
4. Системные настройки устройства

4.1. Замена пароля администратора

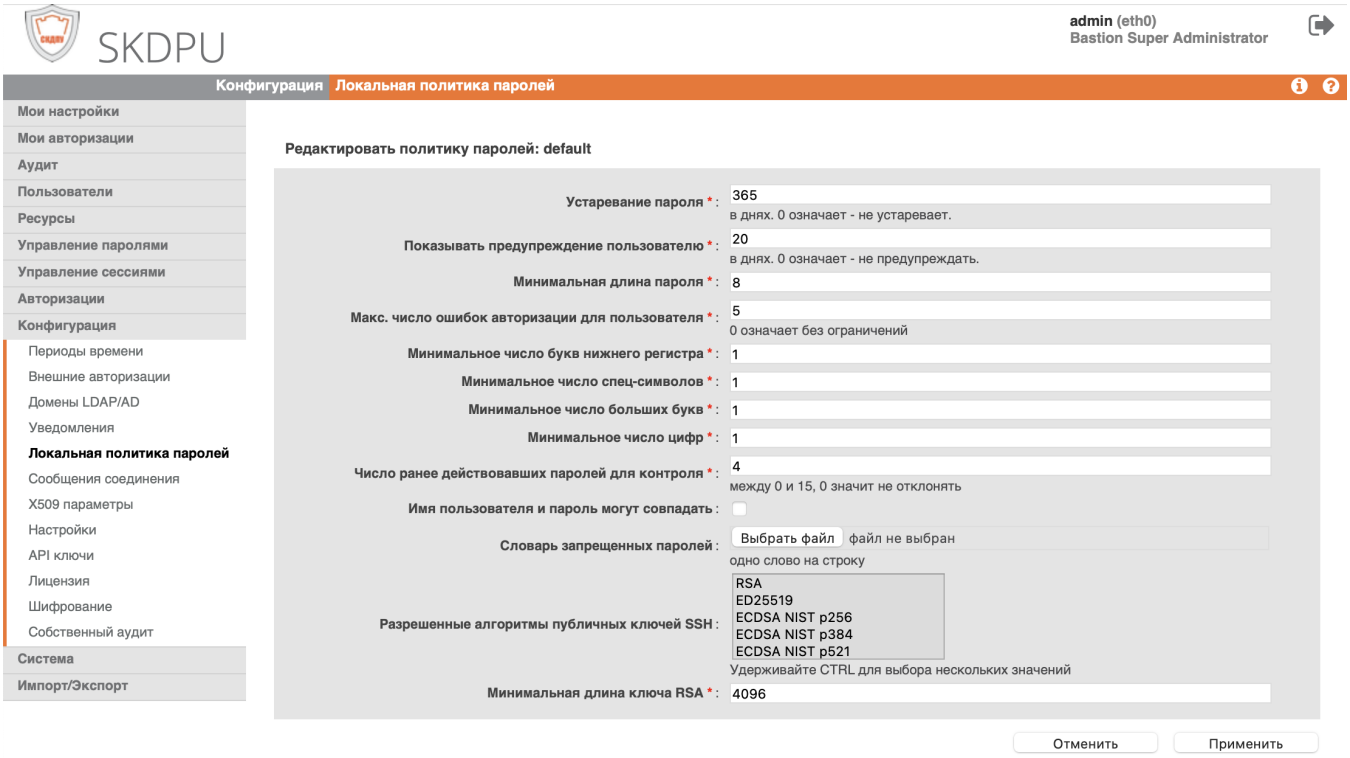
В разделе **My Preferences** укажите email администратора, необходимый язык интерфейса и примените настройки.



Далее, смените пароль с дефолтного на подходящий для администратора. Система не даст сохранить слабый пароль.



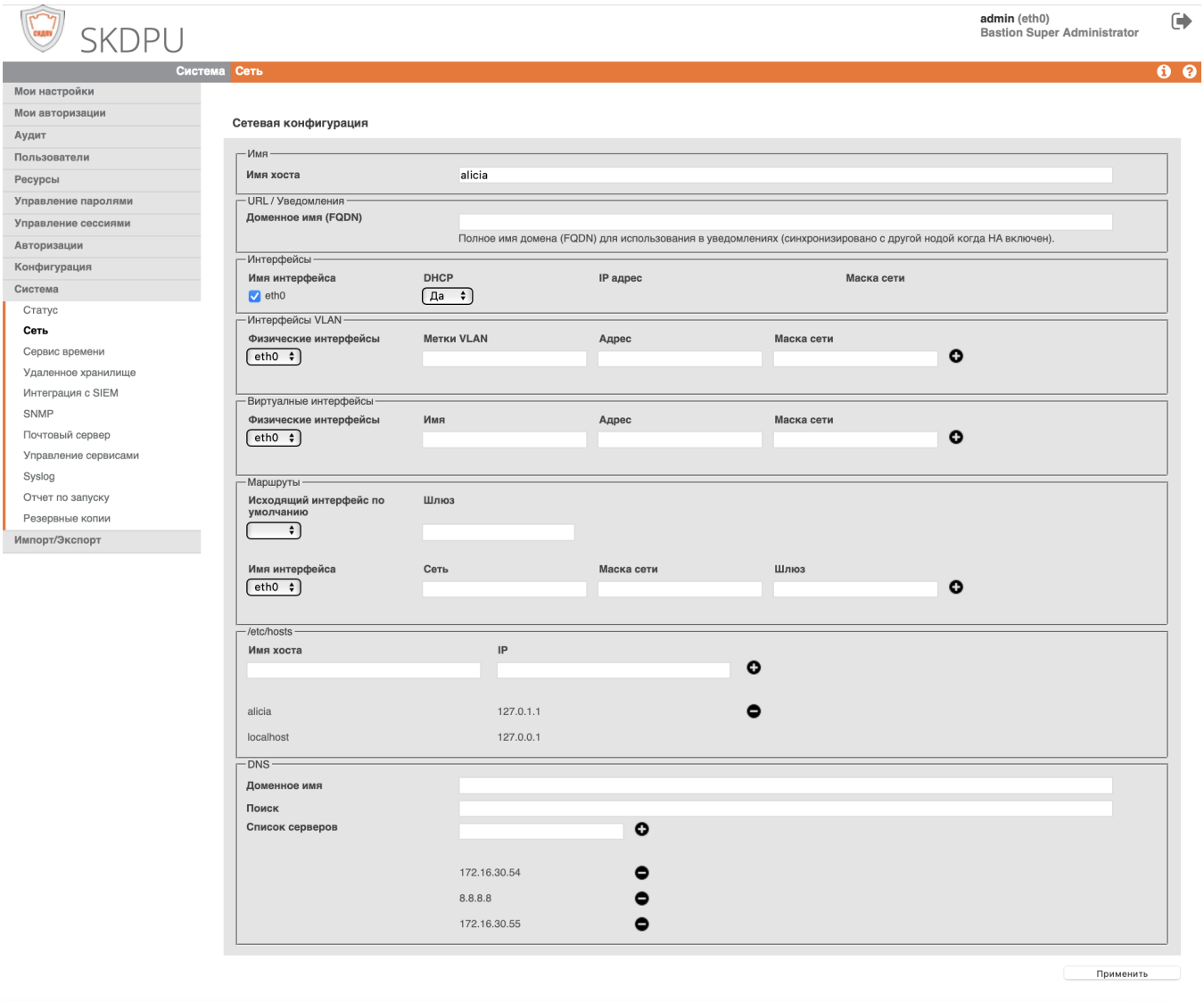
При необходимости, Вы можете изменить локальную политику паролей СКДПУ в разделе **Configuration → Local Password Policy**



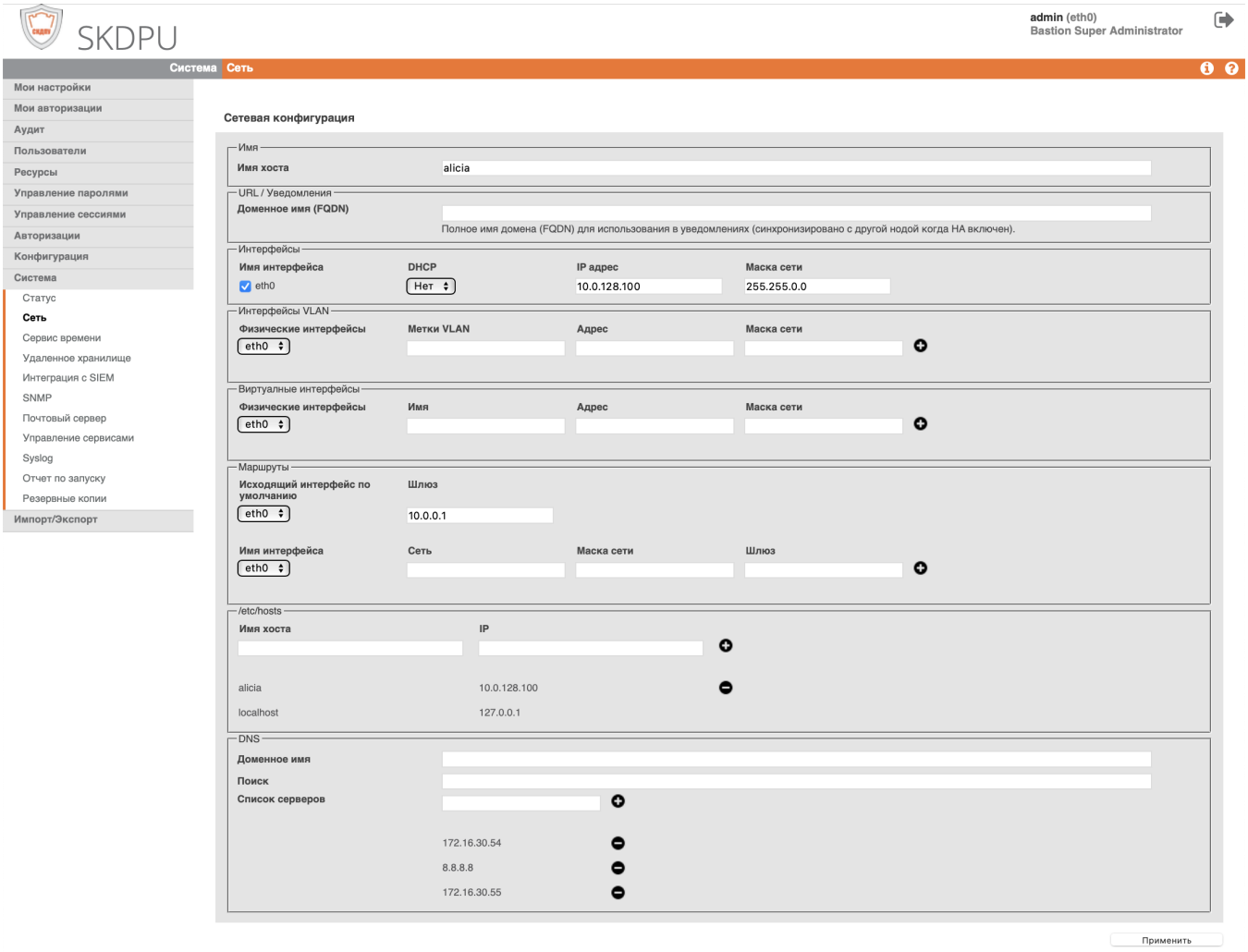
4.2. Настройка сети

В разделе **Система → Сеть** проверьте настройки сетевых интерфейсов.

Сетевая конфигурация для **динамической** IP-адресации:

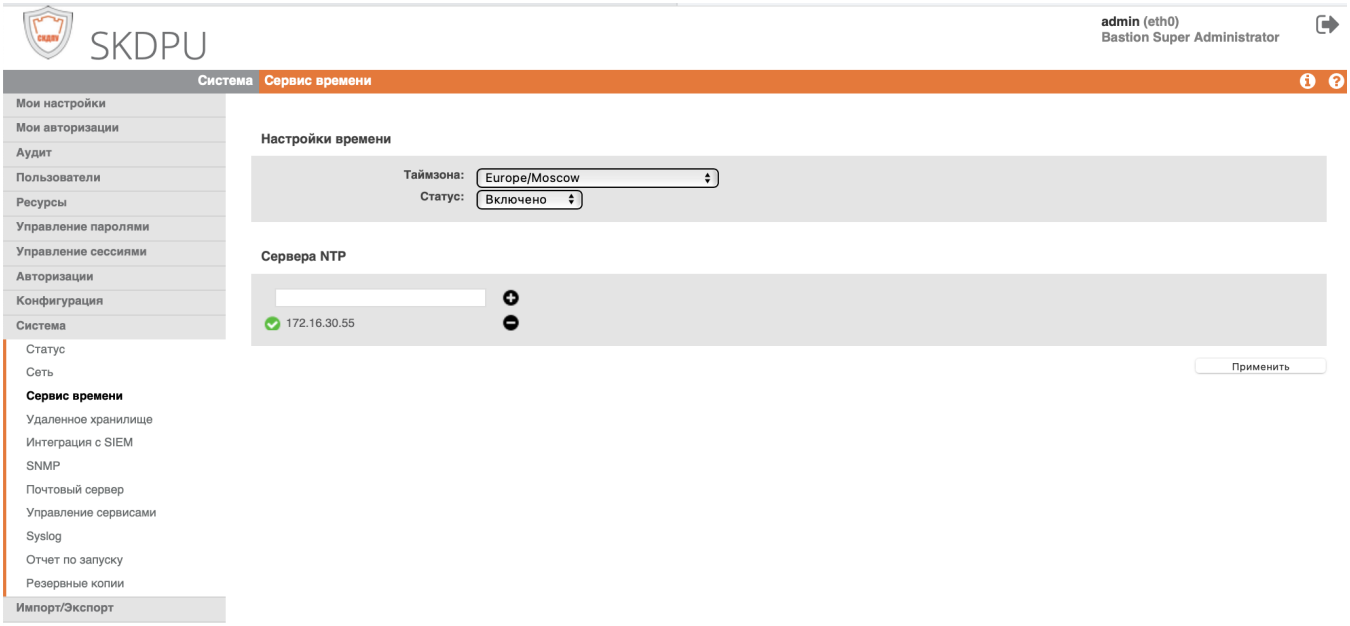


Сетевая конфигурация для **статической** IP-адресации:



4.3. Настройка подсистемы точного времени

Рекомендуется указать действующий сервер точного времени для устройства в разделе **Система → Сервис времени**, т. к. от актуальности настроек времени будет зависеть стабильная работа смежных систем, например, передача логов во внешние SIEM-системы.

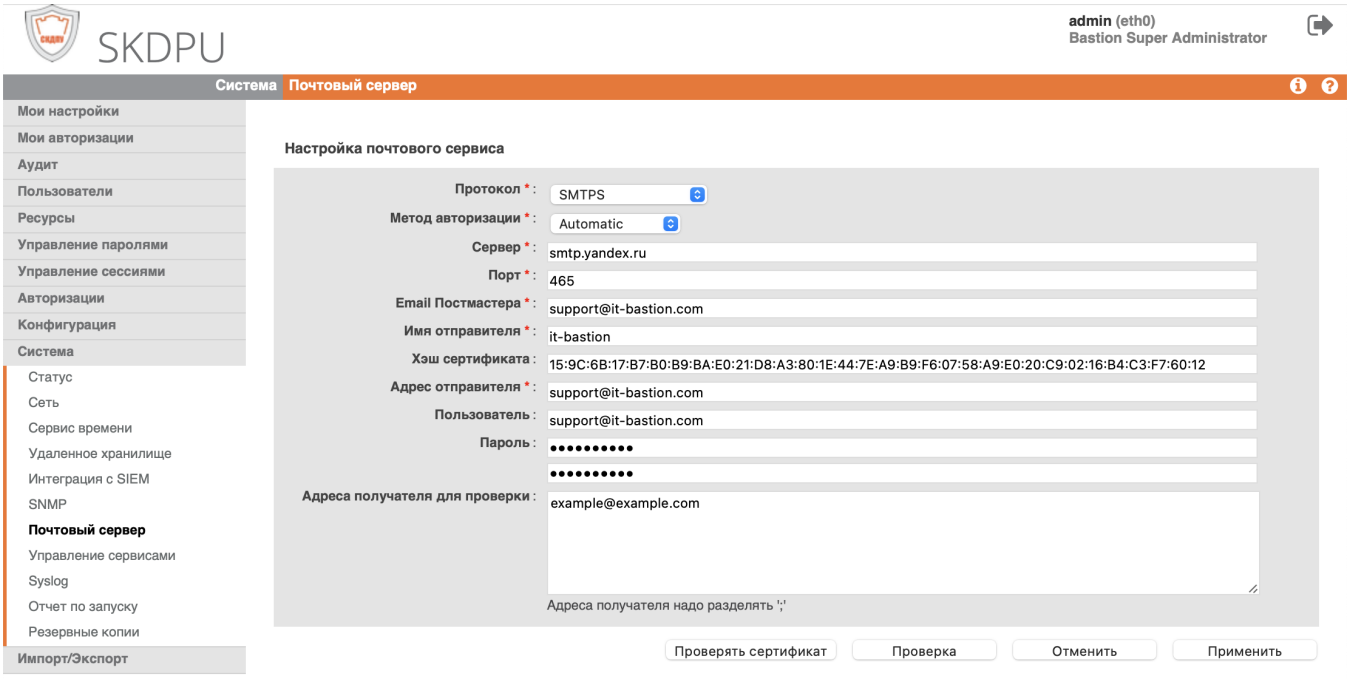


4.4. Настройка подсистемы оповещений

В разделе **Система → Почтовый сервер** укажите настройки почтовой подсистемы. Здесь же можно отправить тестовое сообщение для проверки.

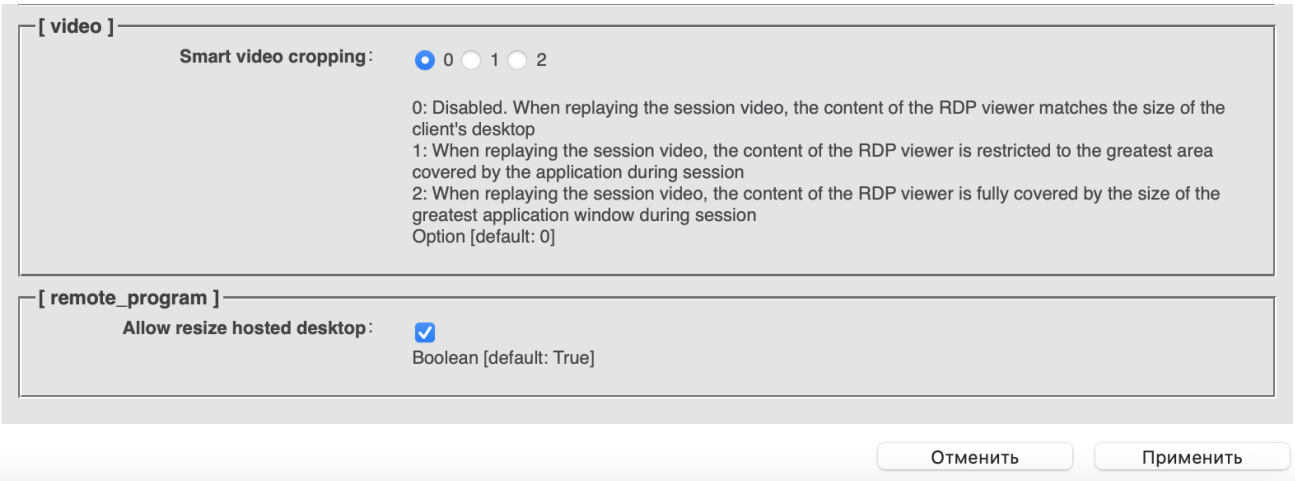
В настройках в СКДПУ 7 присутствует так же строка хэш сертификата. При использовании зашифрованного соединения с сервером почты, для того что бы сверять сертификат система запоминает его хэш. Для получения хэша есть кнопка **"Проверить сертификат"**. После связи и авторизации на целевом сервере система записывает себе данные сертификата.

> Не нужно пытаться в ручную прописать контрольную сумму сертификата - это неверные данные. Если система по какой-то причине не получила хэш сертификата, проверьте корректность указанных параметров почтового сервера и данные авторизации на нем. В случае использования символьного имени – проверьте, настроен ли DNS.

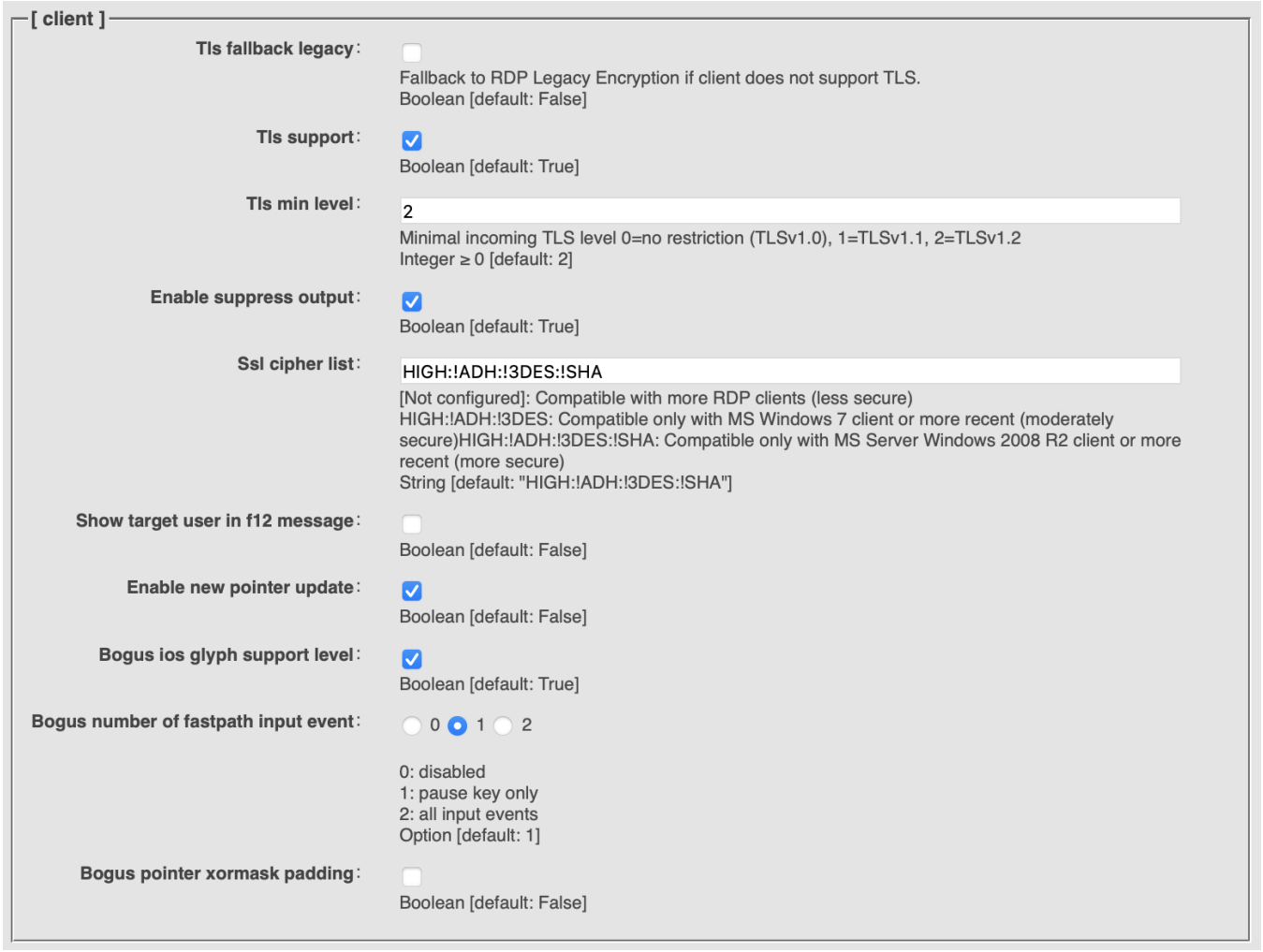


4.5. Подстройка параметров конфигурации для оптимальной работы.

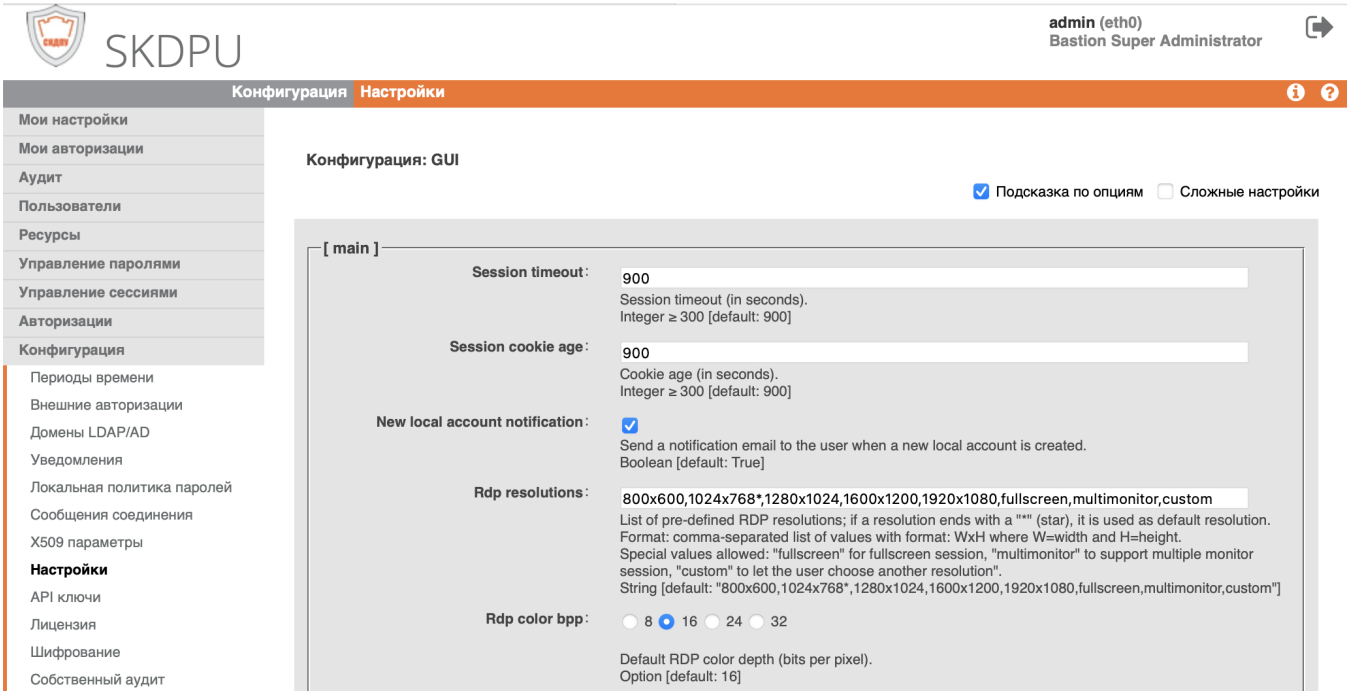
В разделе **Конфигурация → Настройки** выберите раздел **RDP proxy**. В секции [video] переключите значения в 0.



Если Вы работаете на компьютере с операционной системой MacOS, необходимо **в этом же разделе** в секции [**client**] установить значение **"Enable new pointer update"**

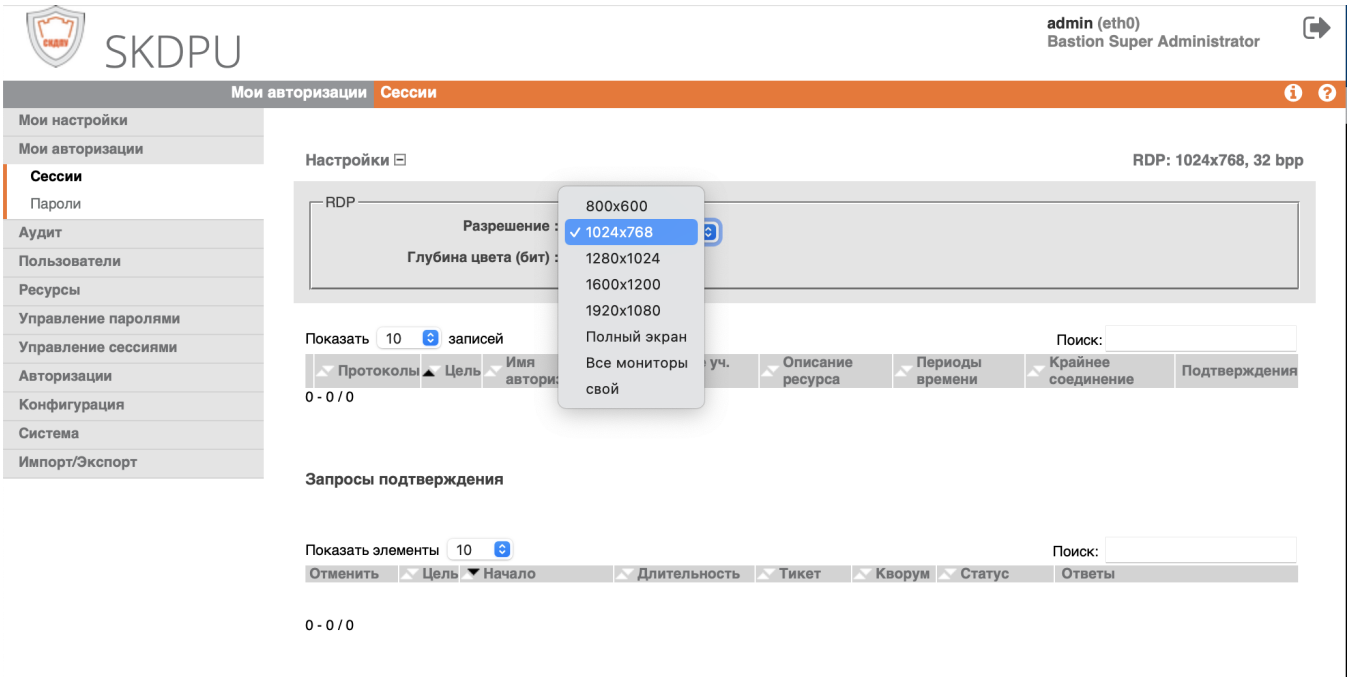


В разделе **Конфигурация → Настройки** выберите раздел **GUI**. Укажите оптимальное разрешение для окон RDP клиента. В версии 7 можно задать несколько доступных разрешений экрана.

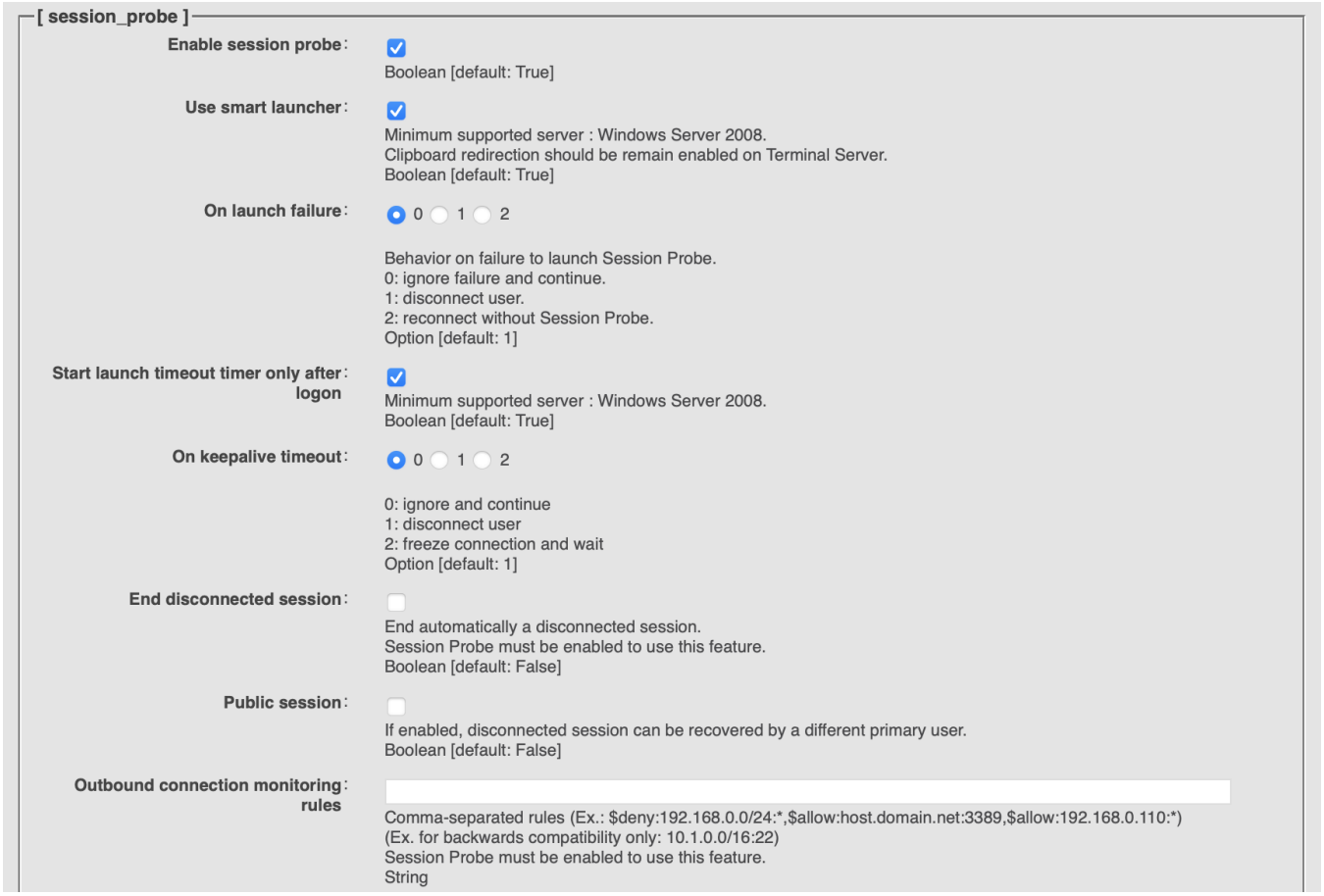


Если Вы работаете на компьютере с операционной системой MacOS, потребуется **в этом же разделе** для параметра "**Rdp other os filetype**" выставить значение "**rdp**" для просмотра сессий RDP

Настройка разрешения экрана при подключении к сессии производится в разделе **Мои авторизации → Сессии** во вкладке "**Настройки**".



В разделе **Управление сессиями → Параметры соединения → RDP** переключите в секции [**session_probe**] параметры **"On launch failure" и "On keepalive timeout"** на 0



Если позволяют политики безопасности в контуре инфраструктуры, можно выключить строгий контроль TLS-сертификатов в RDP-сессиях. Для этого в разделе **Управление сессиями → Параметры соединения → RDP** переключите в секции [**server_cert**] параметр **"Server cert check"** на 3. Это позволит избежать ошибки подключения и невозможности установить сессию в случае, если на стороне контроллируемого целевого устройства изменился сертификат.

4.6. Завершение первоначальной настройки.

На данном шаге, СКДПУ НТ Шлюз доступа готов к работе. Рекомендуется сделать снимок (snapshot) в рамках системы виртуализации и продолжать настройки в части политики.

При необходимости возможно сменить пароли для системных пользователей wabadmin, wabsuper в консоли системы – от root с помощью команд passwd wabadmin, passwd wabsuper.

Рекомендуется новые пароли записать и сохранить в сейф – они потребуются для эксплуатации системы в дальнейшем и восстанавливать их нетривиально.

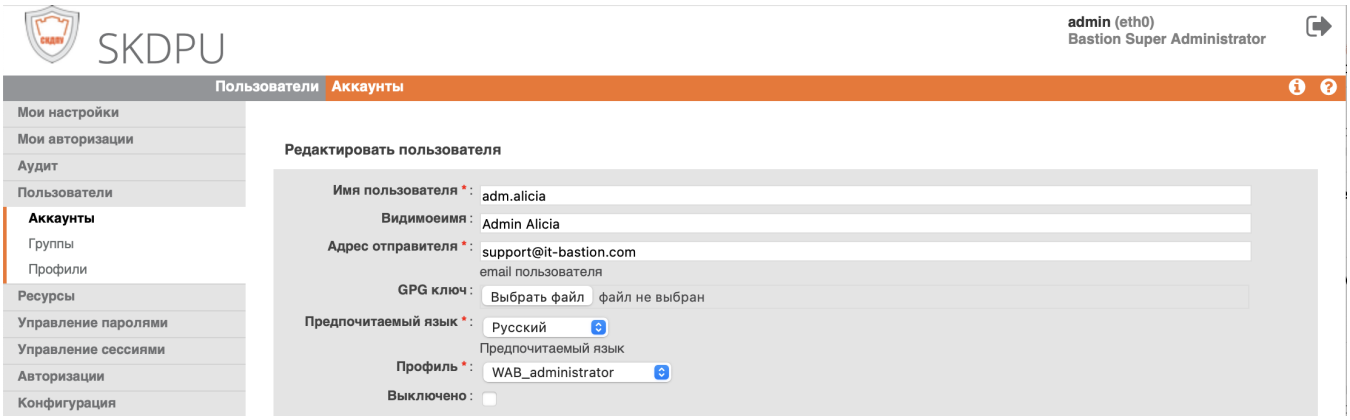
ВАЖНО. Все пароли системы по умолчанию чувствительны к перебору и блокируются после 5 попыток

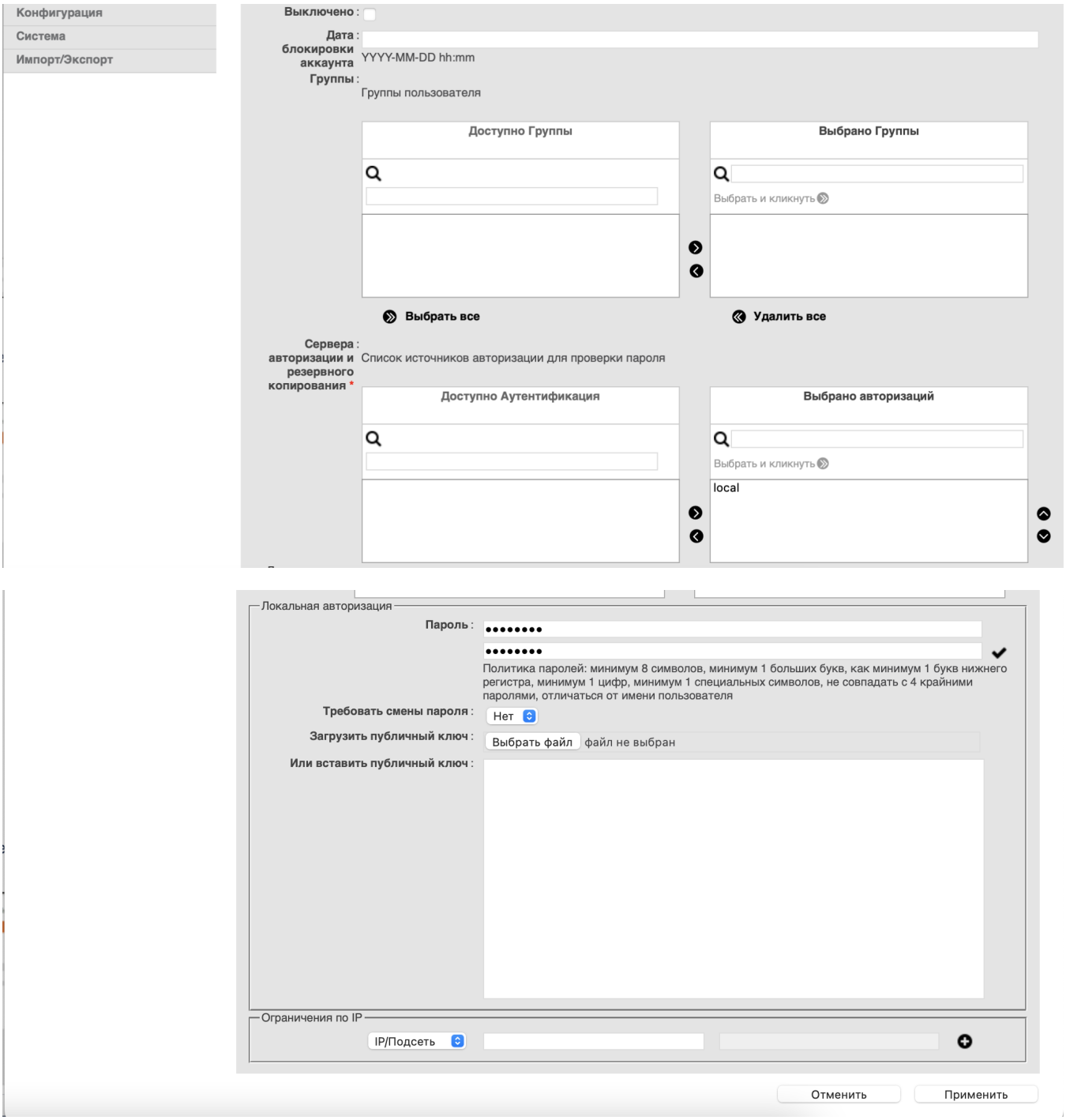
5. Настройка минимальной необходимой политики доступов

Добавление пользователей, устройств, групп и авторизаций.

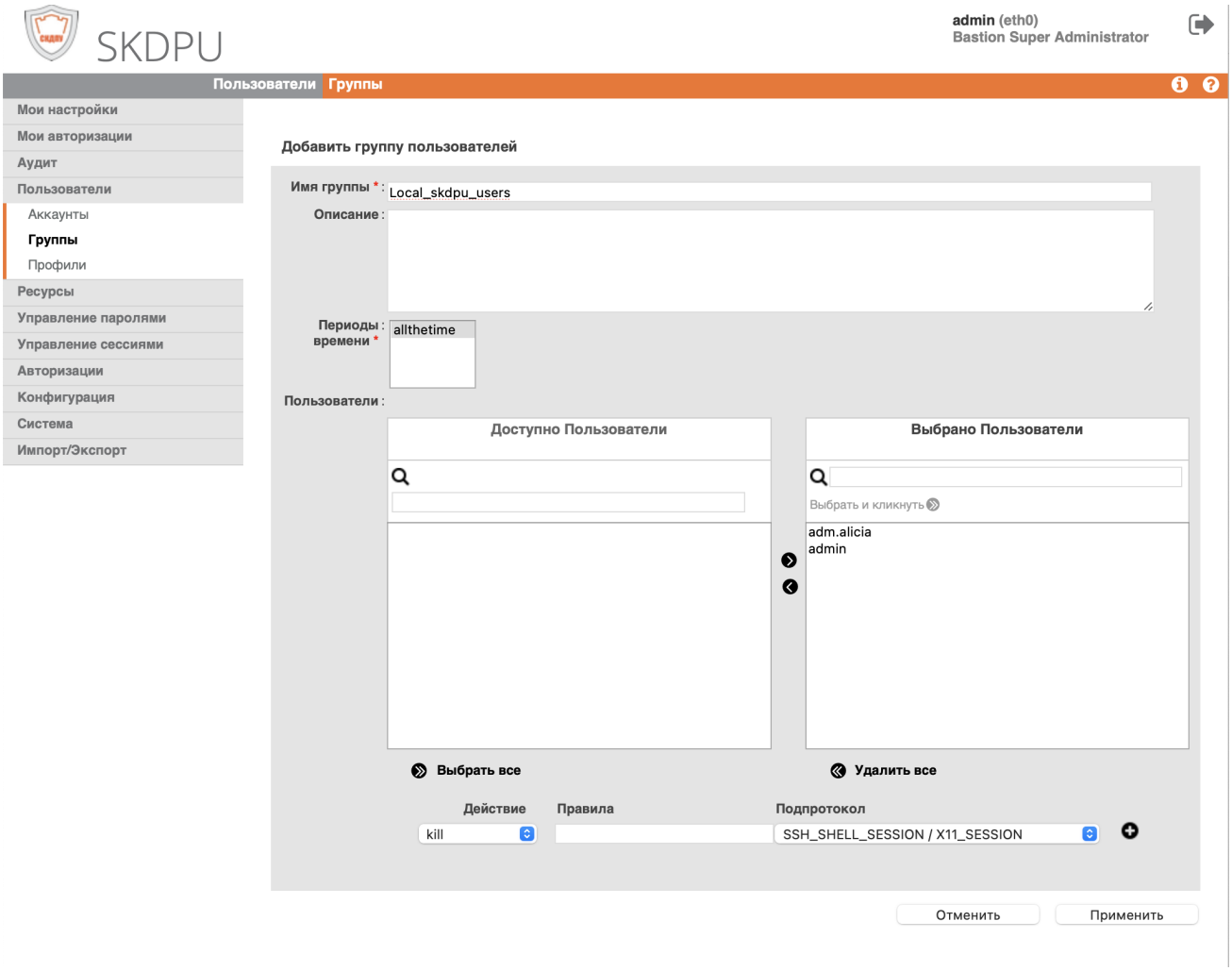
В разделе **Пользователи → Аккаунты** создать пользователя с правами администратора (WAB_administrator). Авторизация "**local**" уже выбрана по умолчанию, поэтому нужно задать новому пользователю пароль в разделе "**Локальная авторизация**".

> **Примечание**
>
> Здесь и далее примером дополнительной учётной записи с правами администратора используется **adm.alicia**



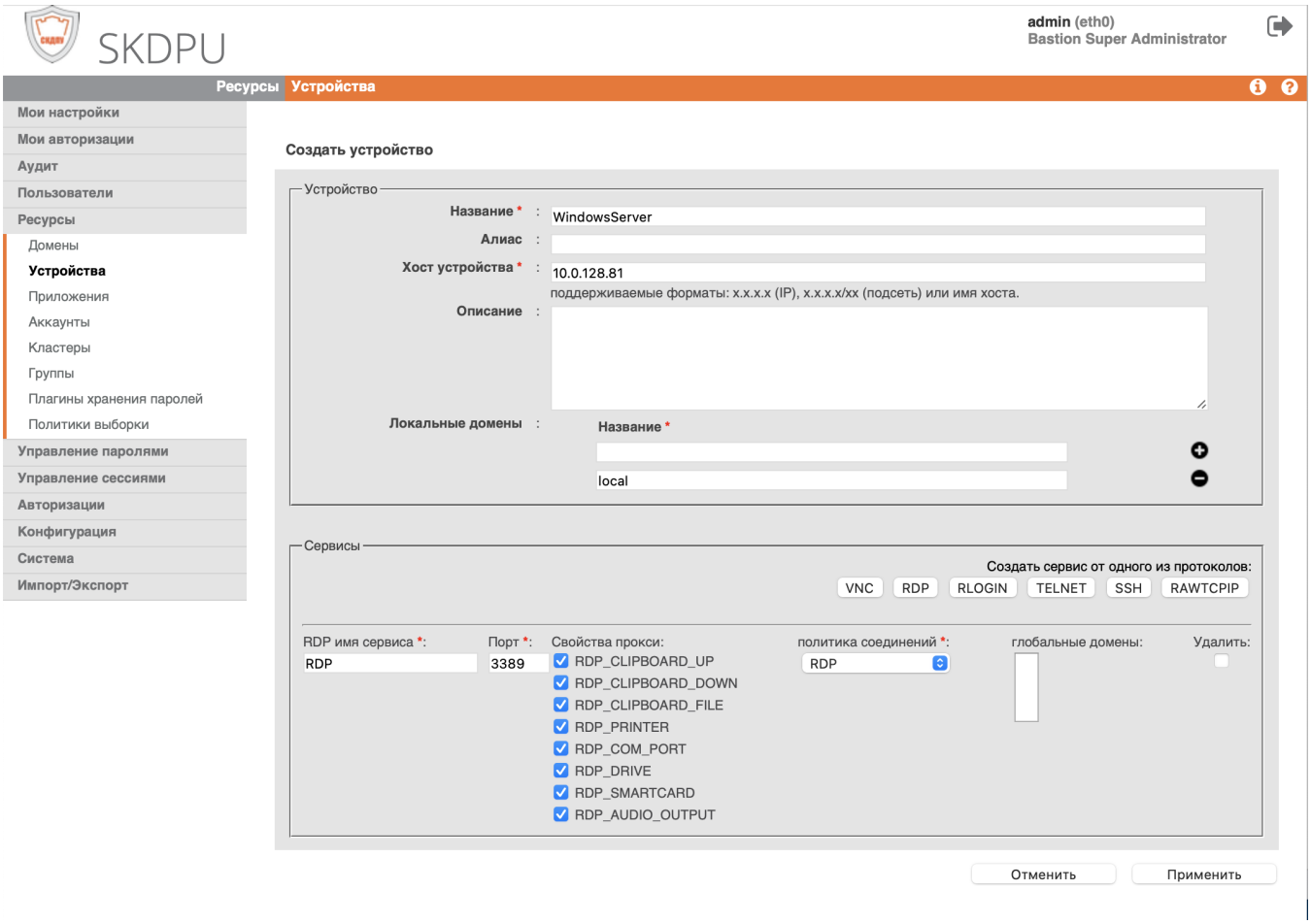


В разделе **Пользователи → Группы** создать группу, например "**Local_skdpu_users**", и добавить в нее пользователей **admin, adm.alicia**

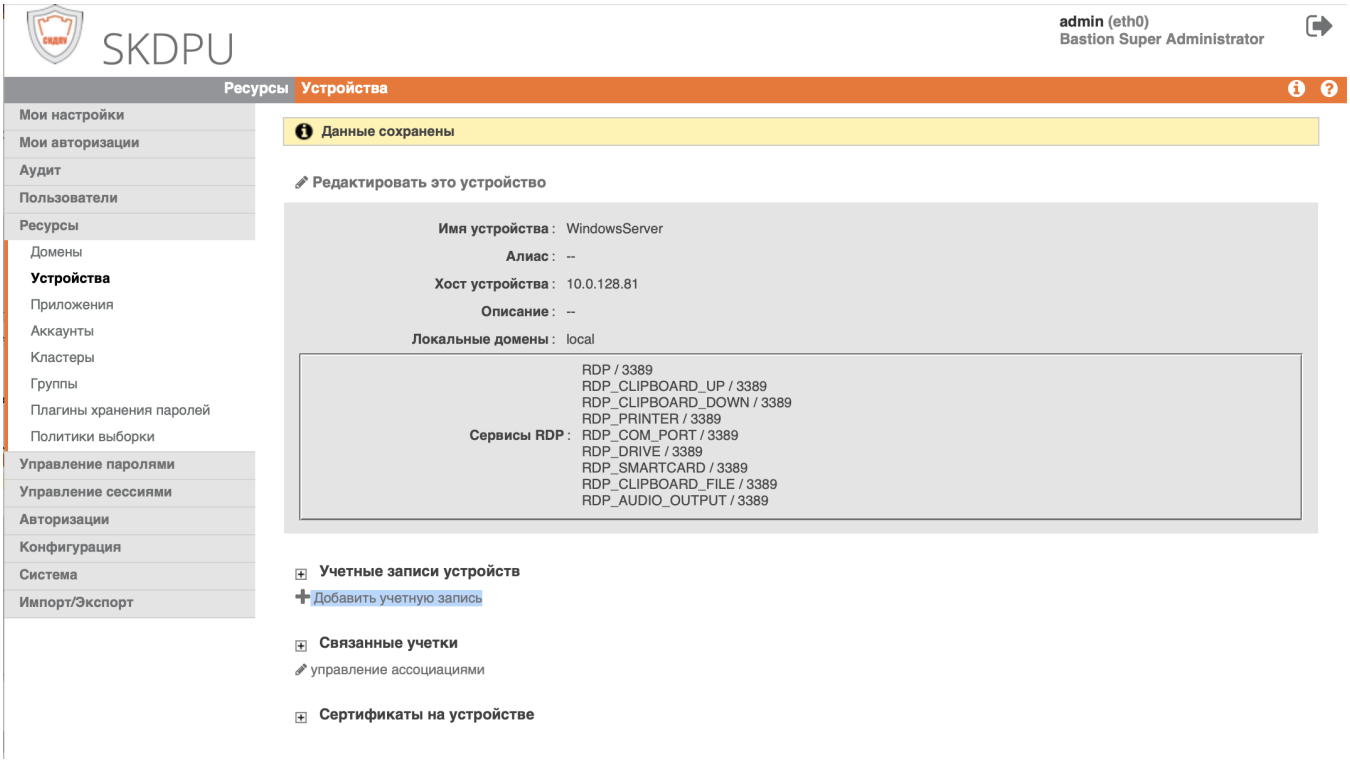


В разделе **Ресурсы → Устройства** необходимо добавить профиль соединения с RDP хостом.

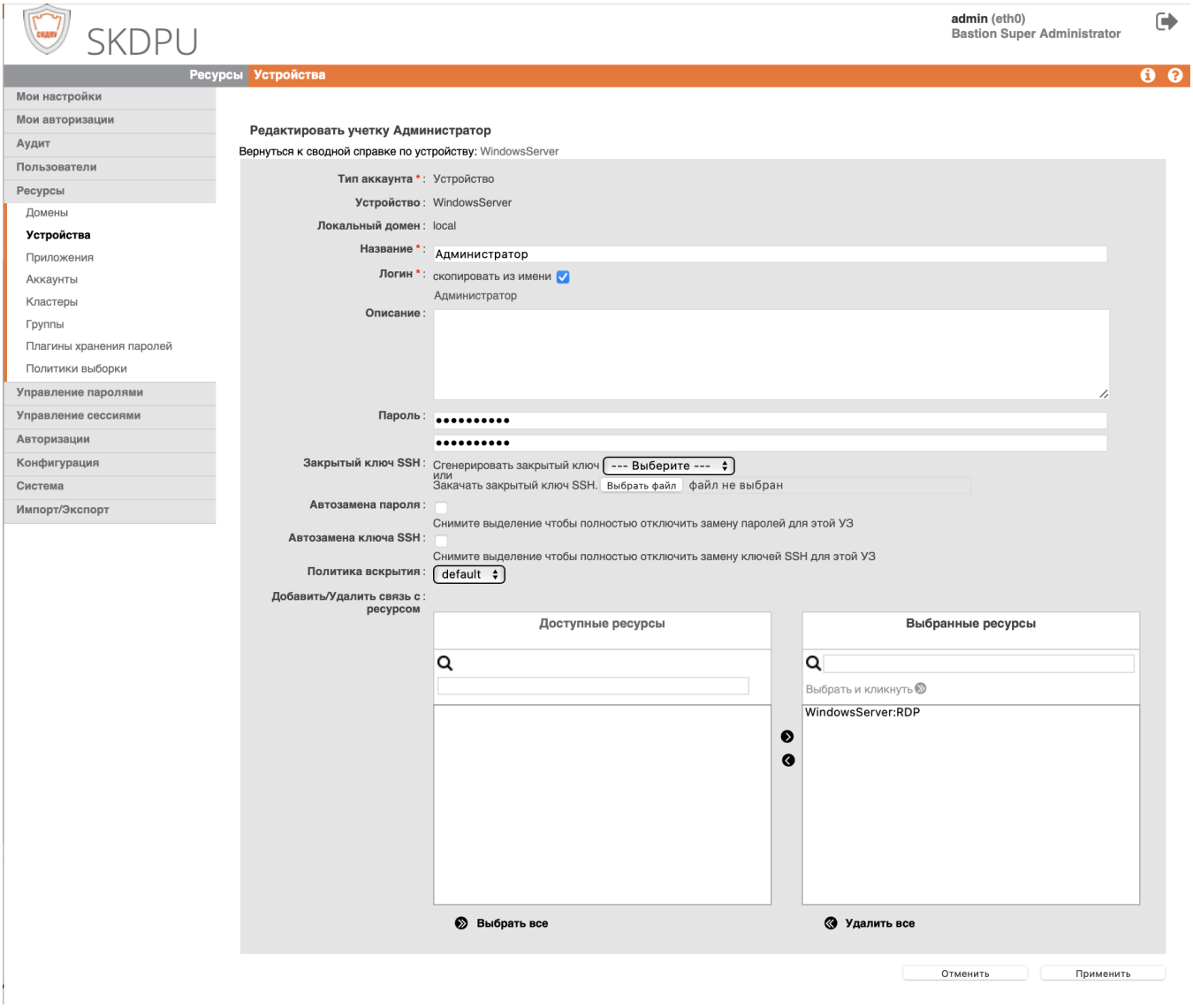
Указать **адрес** Вашего хоста RDP, в локальные домены занести строчку **"local"**, выбрать протокол **RDP** и применить настройки устройства



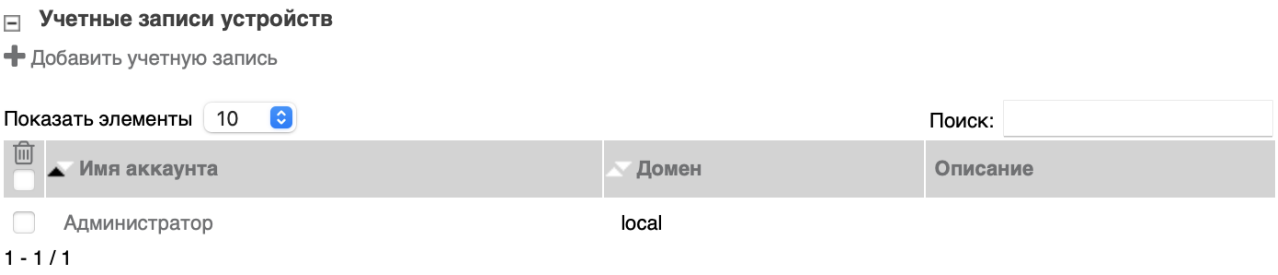
Далее можно добавить учетную запись для соединения с целевым сервером и повышения прав исполнителя



Внесите данные **учетной записи целевого устройства** и сохраните. Обычно добавляют **административные** УЗ, чтобы не выдавать на руки исполнителям пароли от них.



Добавленная учётная запись должна выглядеть следующим образом



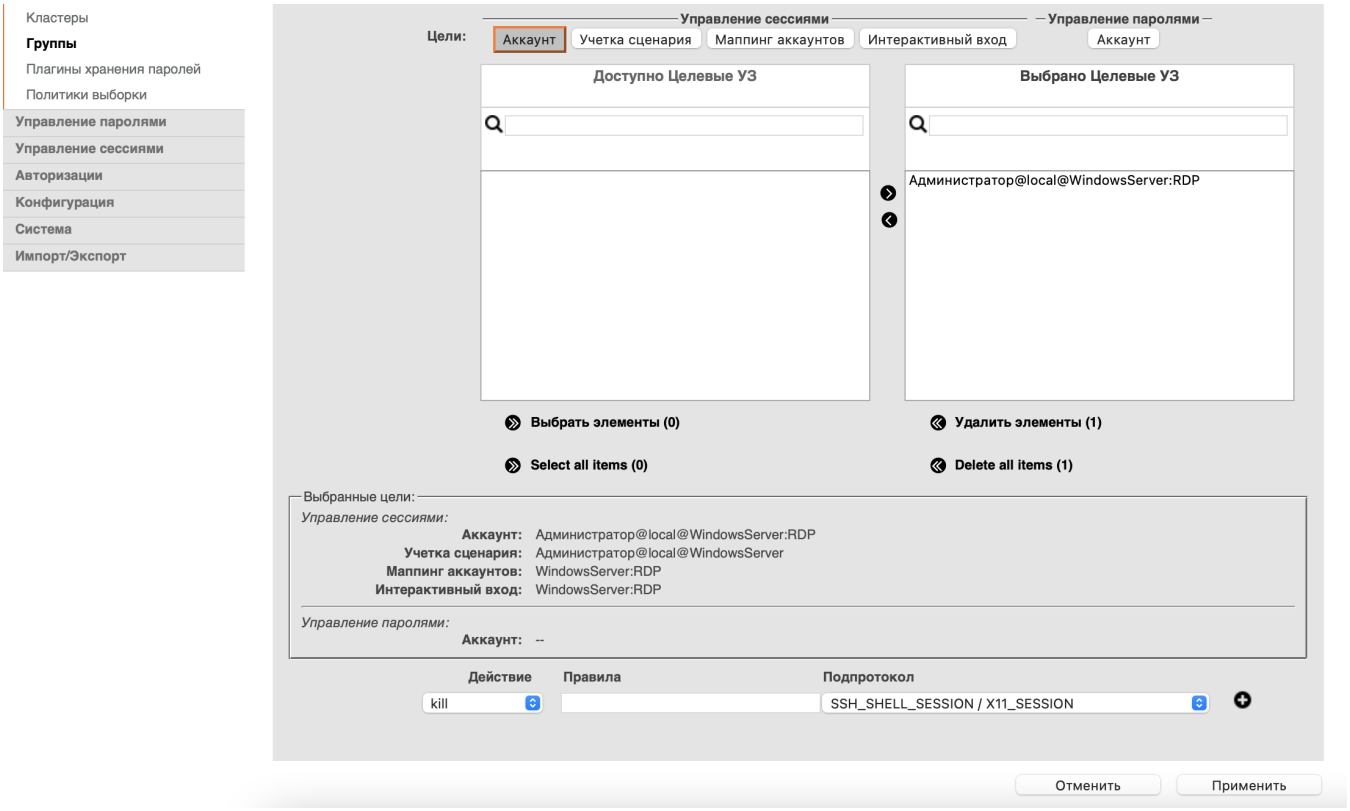
Система поддерживает 3 варианта доступа к системе:

- При входе **по сохраненной УЗ (по учетной записи управления сессиями и учётке сценария)** целевой вход будет от пользователя Администратор@local в нашем примере (предполагается, что такая УЗ на целевой системе есть).
- При входе **через маппинг аккаунтов** вход будет от УЗ, с которой пользователь вошел на СКДПУ (admin или adm.alicia в нашем примере, предполагается, что такие УЗ присутствуют в целевой системе).

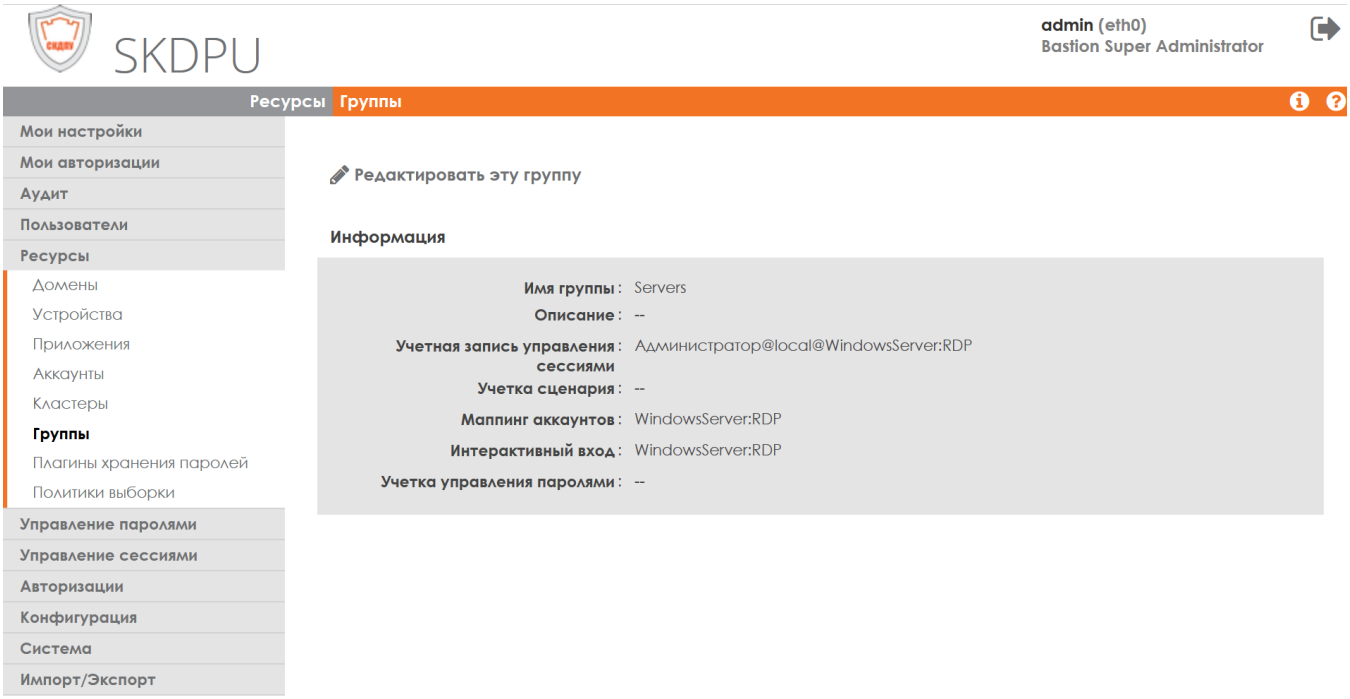
- При **интерактивном входе** СКДПУ используется последовательная авторизация при условии, что пользователь знает УЗ локального пользователя СКДПУ и, *в нашем случае*, УЗ AD Windows Server. *СКДПУ будет записывать все действия при таком входе.

В разделе **Ресурсы → Группы** добавим группу ресурсов "**Servers**".

Добавить **разрешения** использовать ресурс. Можно добавить любое сочетание вариантов доступа к системе для каждого хоста.

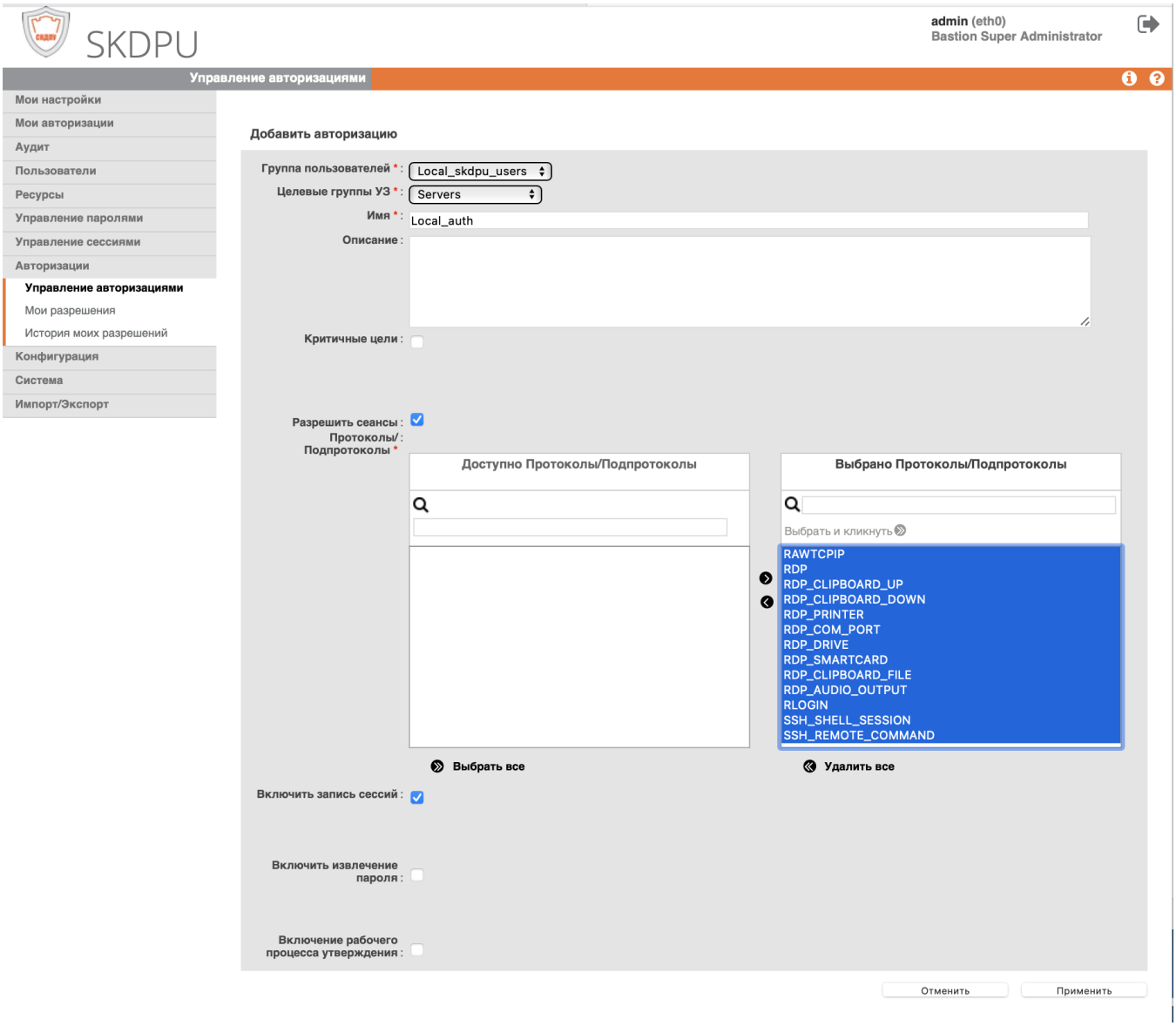


Добавим их все и сохраним группу ресурсов.



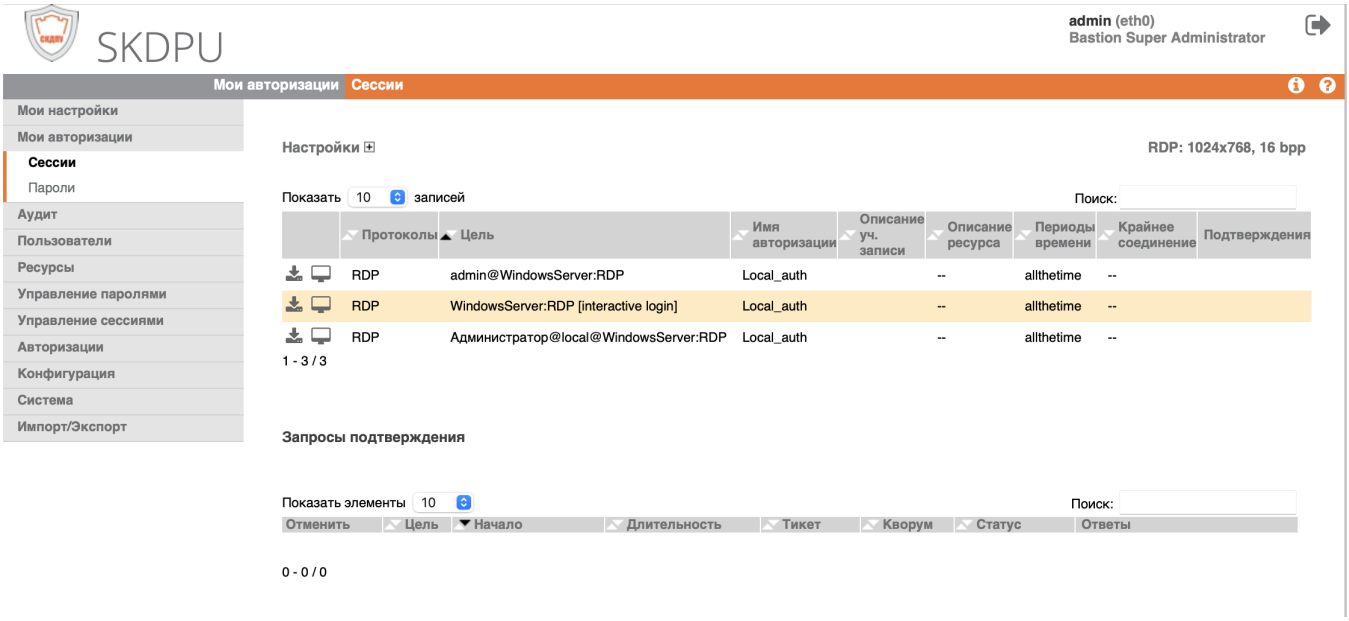
Добавление хоста SSH идентично принципам добавления хоста RDP, описанным в предыдущих пунктах.

В разделе **Авторизации → Управление авторизациями** добавим правило "**Local_auth**", разрешающее группе пользователей "**Local_skdpu_users**" использовать ресурсы из группы "**Servers**" и все необходимые **протоколы и подпротоколы**. Также необходимо включить **запись сессий**.



Авторизация "Local_auth" для группы "Local_skdpu_users" должна выглядеть следующим образом

Если все сделано правильно, то в разделе **Мои авторизации → Сессии** будет представлен список доступных данному пользователю целевых ресурсов:

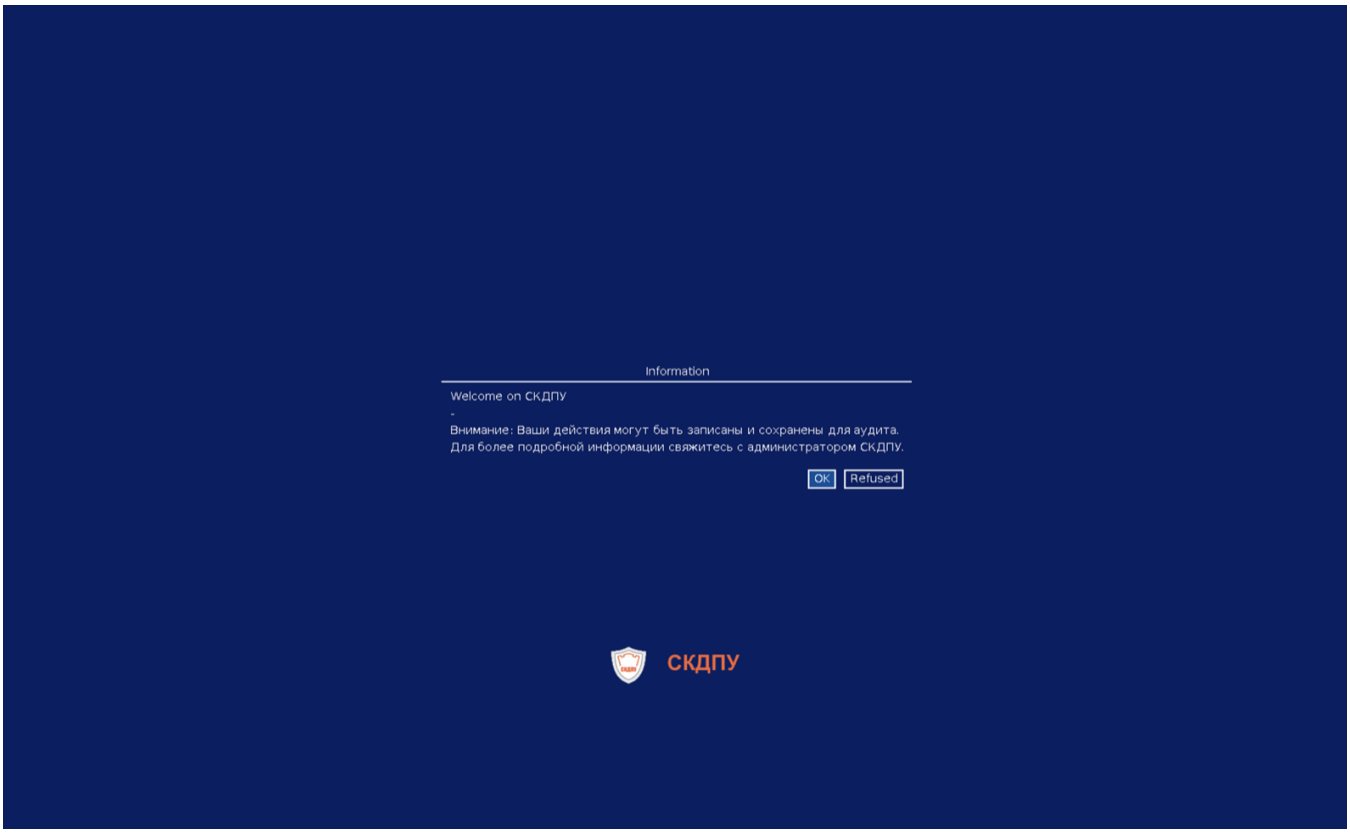


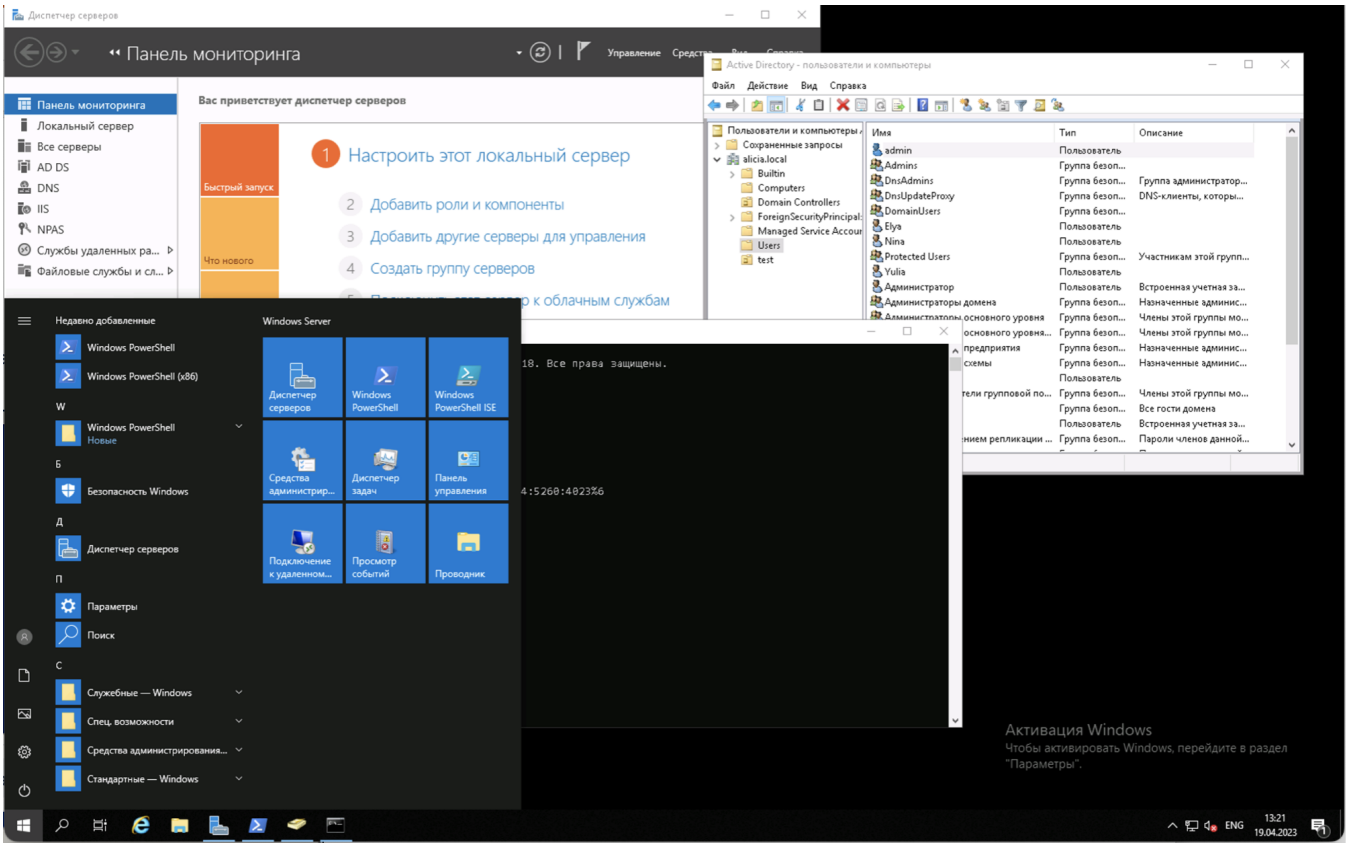
6. Соединение через СКДПУ

6.1. Подключение по протоколу RDP

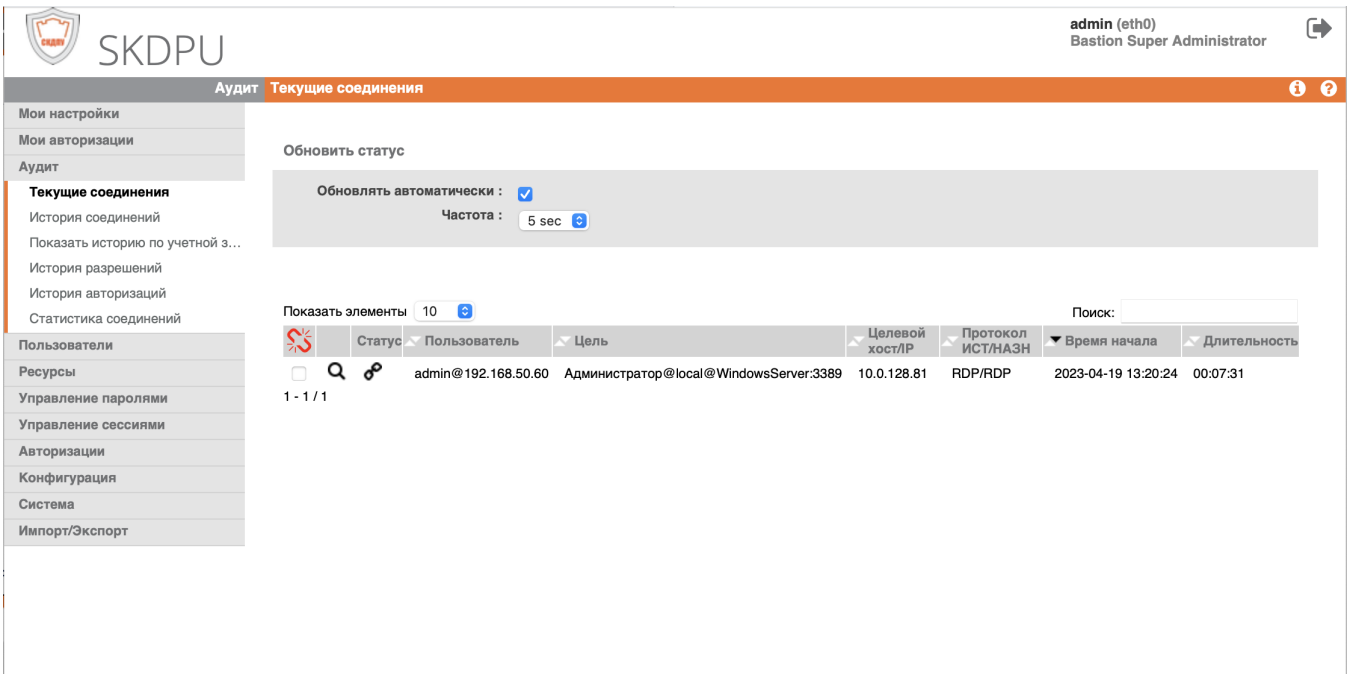
6.1.1. Подключение из интерфейса системы

Выберите в разделе **Мои авторизации → Сессии** вариант входа с сохраненной УЗ - Администратор@local@WindowsServer:RDP, скачайте и запустите ярлык запуска ***mstsc*** **(либо Microsoft Remote Desktop на MacOS)**.

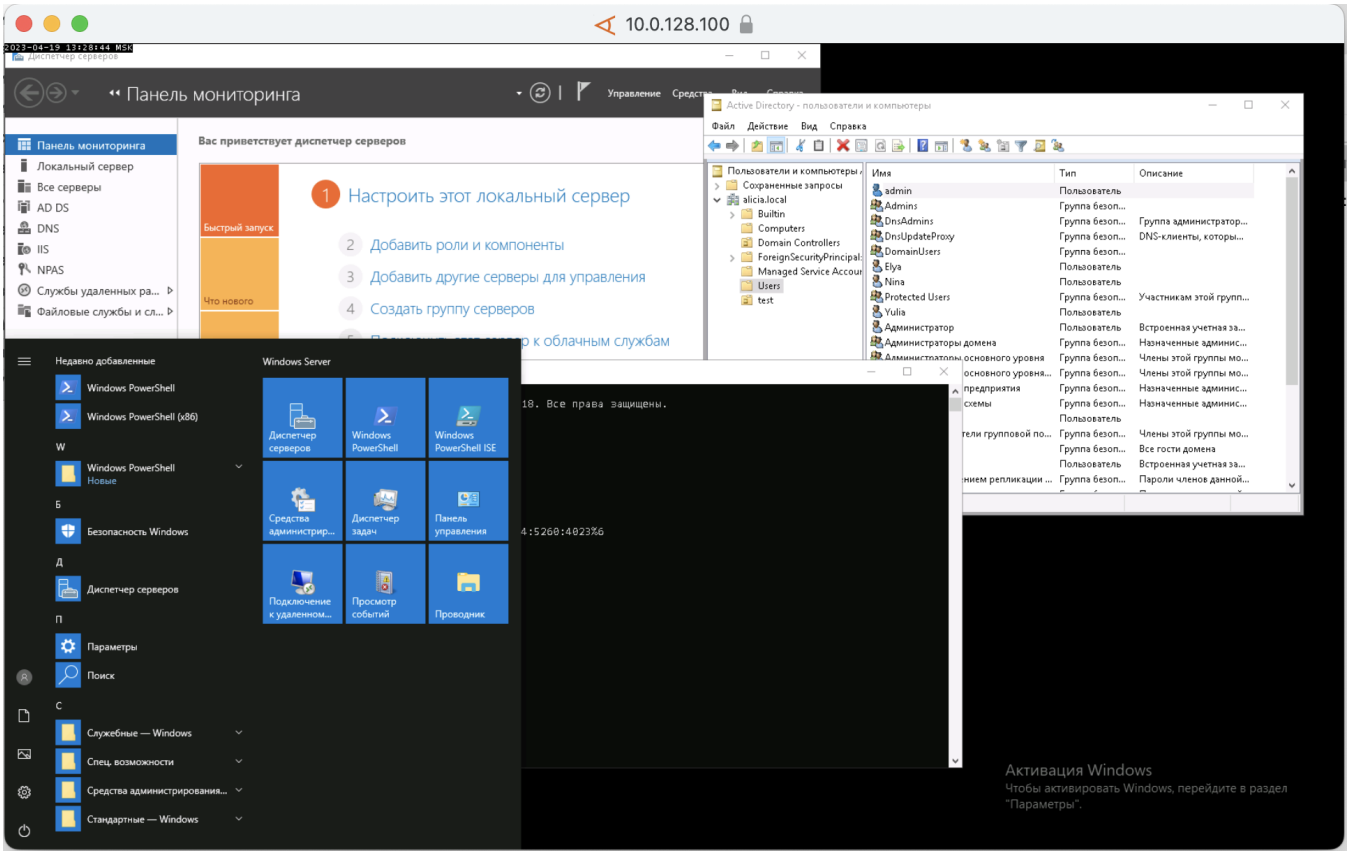




Пока сессия открыта, в разделе **Аудит → Текущие соединения** доступны сведения о происходящем.



Система позволяет оперативно наблюдать происходящее в рамках сессии по клику на 

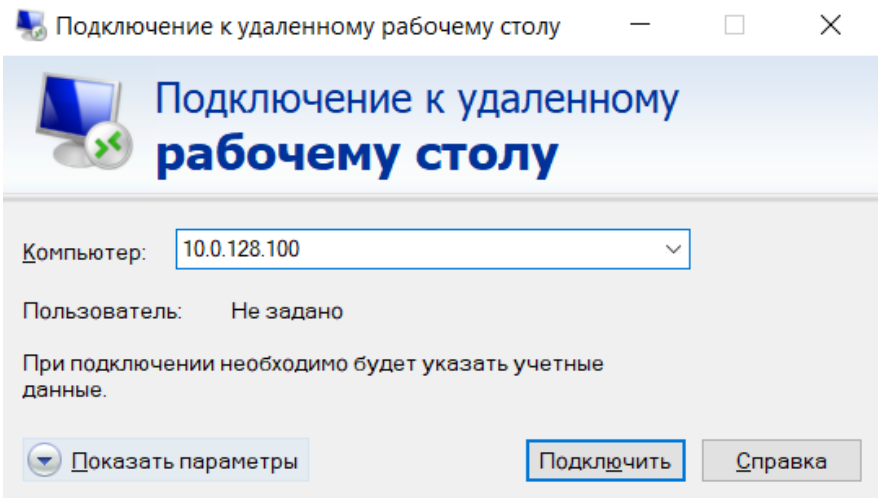


Закройте сессию.

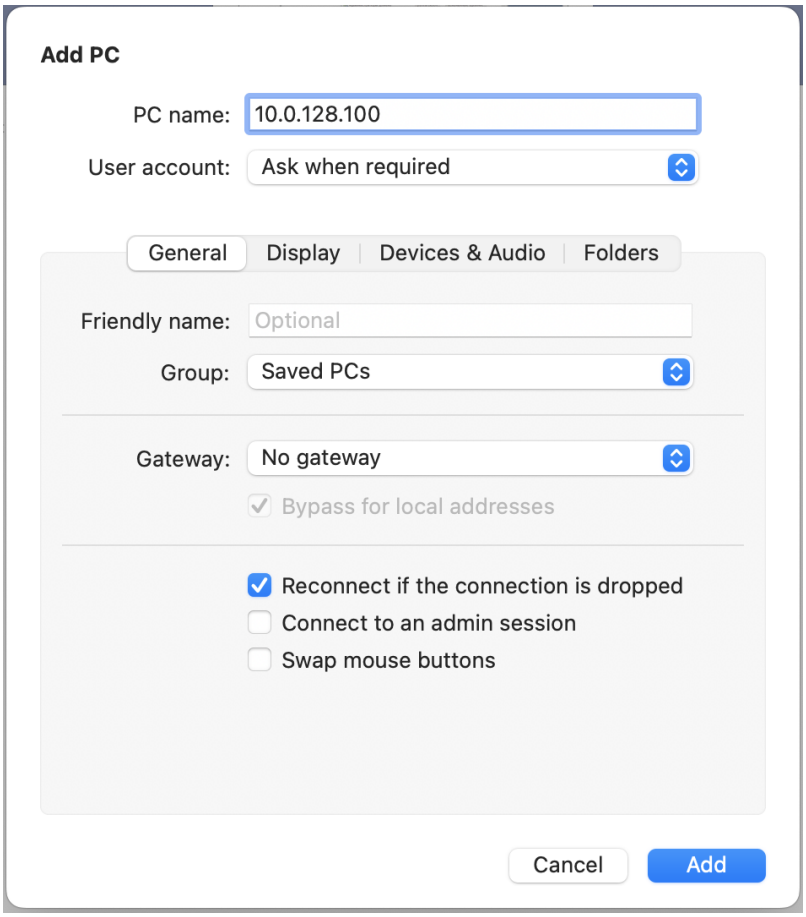
6.1.2. Подключение при помощи клиента удаленного доступа mstsc или Microsoft Remote Desktop

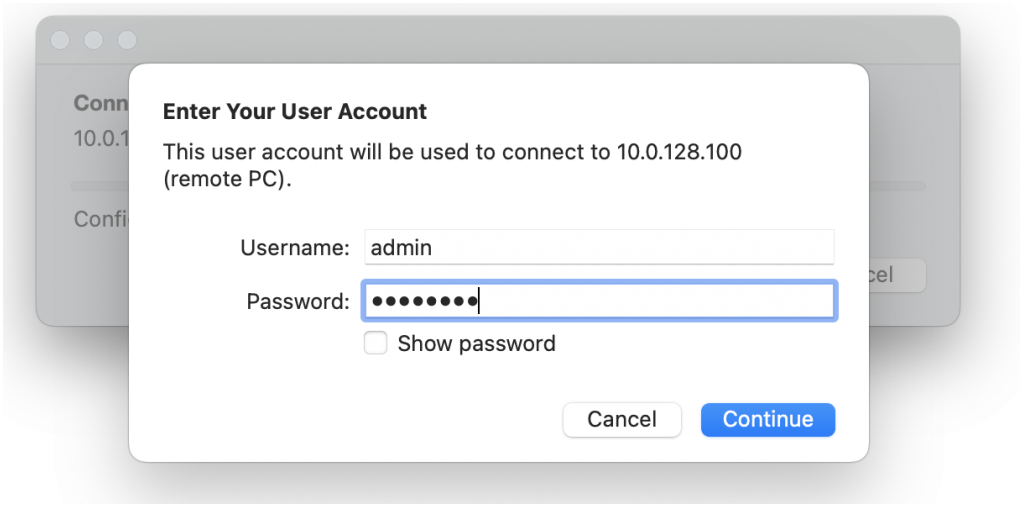
Вход на систему можно осуществить и без входа в веб-интерфейс, например, можно запустить клиент напрямую на адрес СКДПУ и выбрать нужную целевую систему после авторизации:

Вход через mstsc:

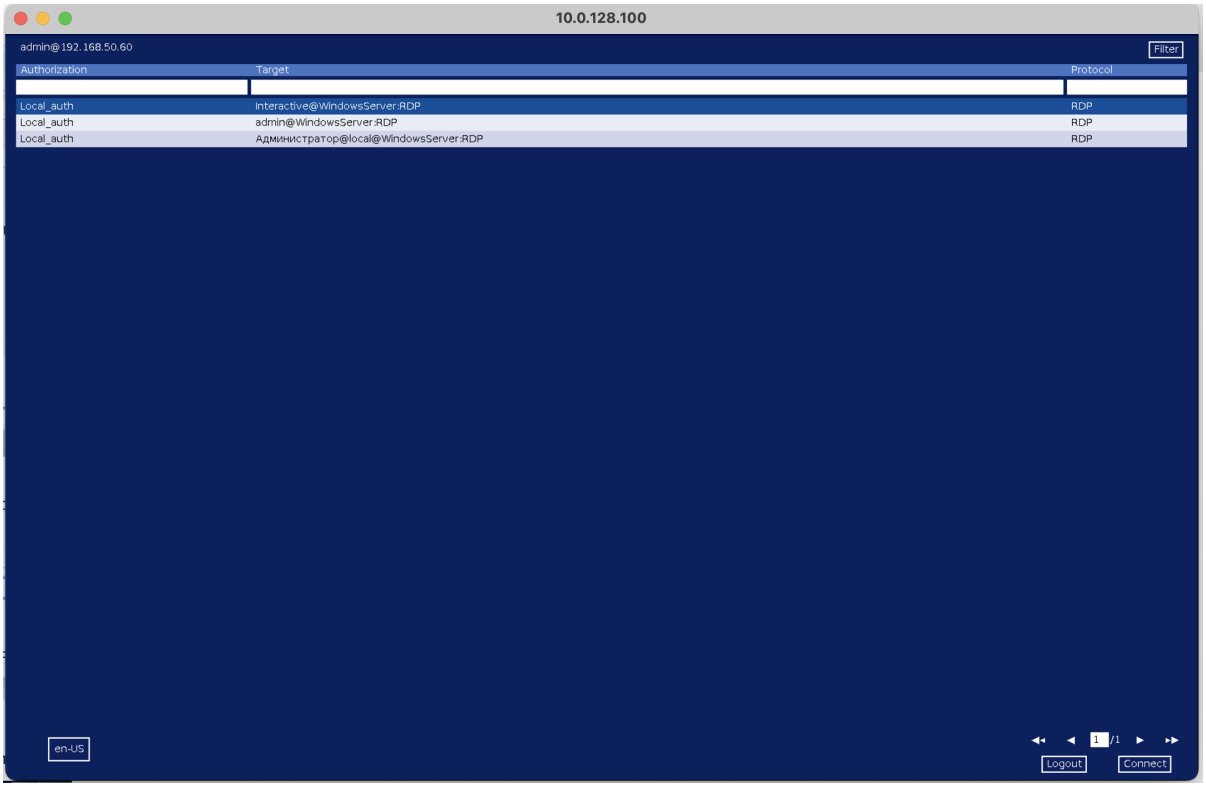


В нашем случае, вход будет осуществляться при помощи Microsoft Remote Desktop

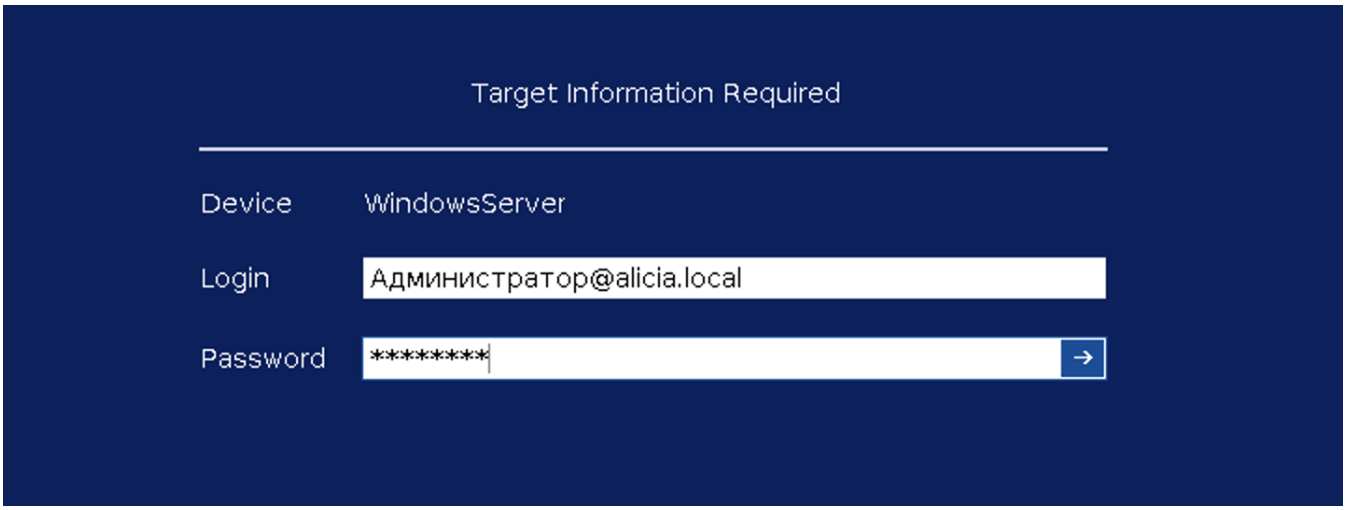




После авторизации система выдаст меню доступных вариантов подключения по протоколам RDP или VNC для данного пользователя



Подключение к УЗ "Администратор" при помощи интерактивного входа реализуется так:

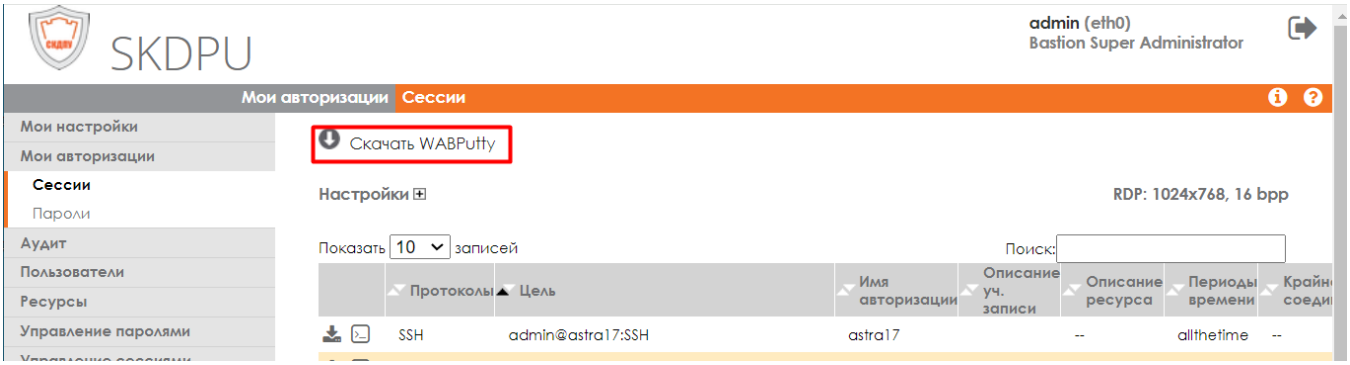


Протестируйте остальные варианты входа на целевое устройства.

6.2. Подключение по протоколу SSH

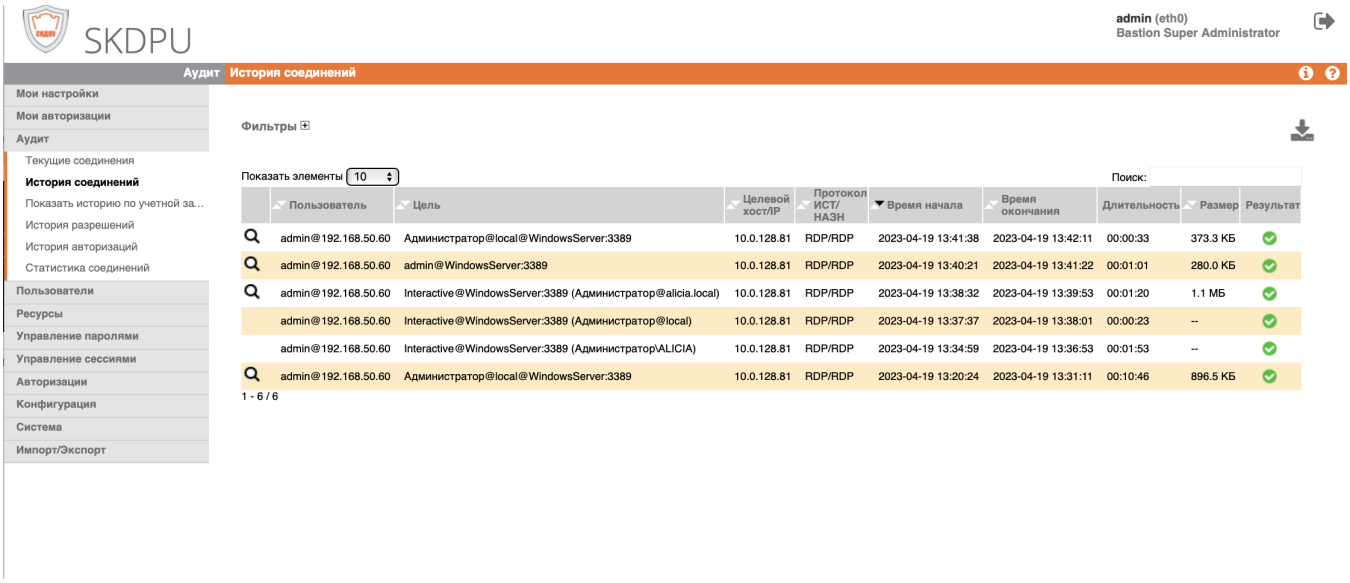
Такой же механизм работает и для SSH подключений.

Для того, чтобы открывать соединения с SSH системами из веб-интерфейса, необходимо установить клиента WABPutty, который идет в поставке системы. Ссылка на него появляется при добавлении первой целевой системы с протоколом ssh.



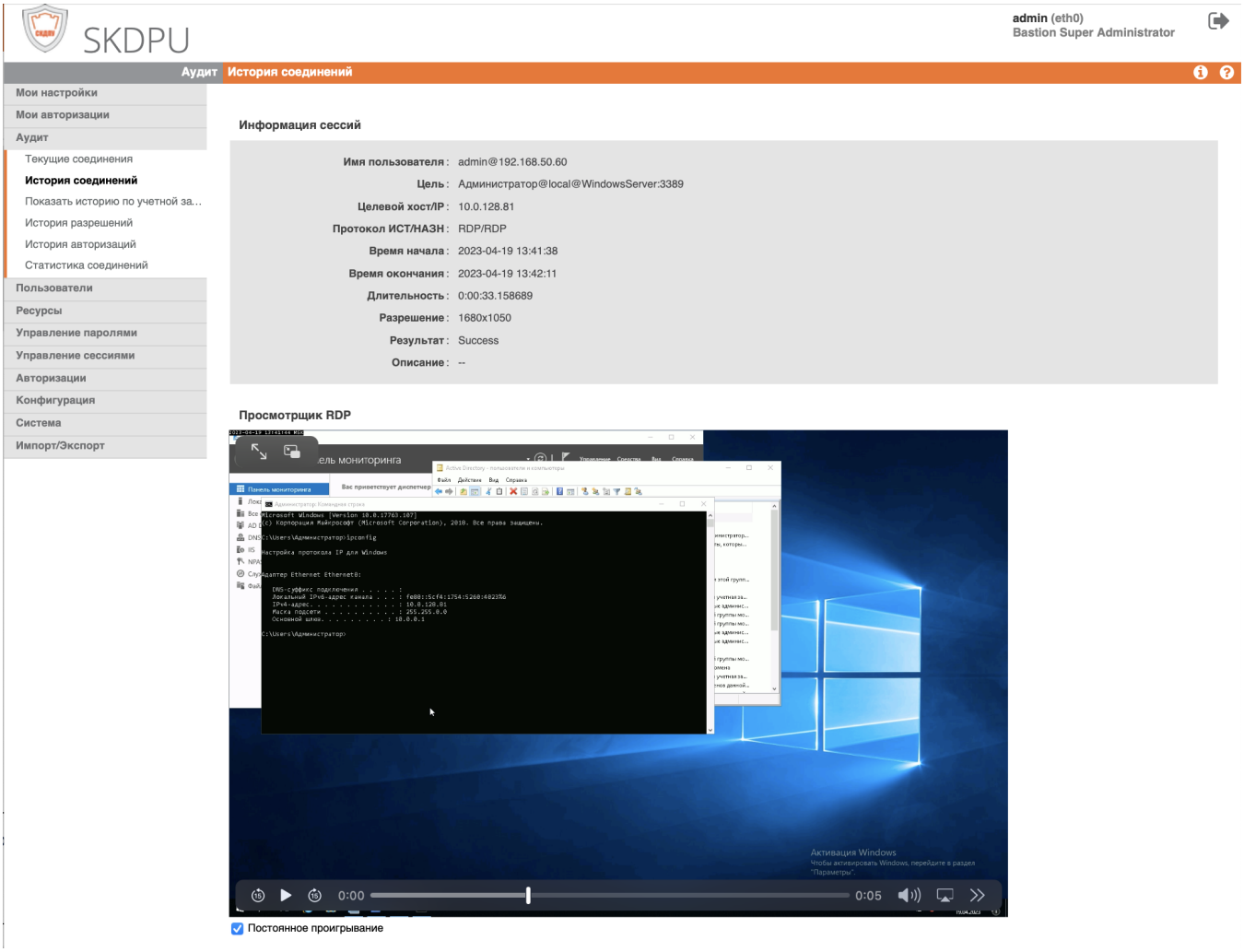
7. Аудит сессий пользователей

В разделе **Аудит → История соединений** доступен список обработанных системой сессий администрирования.

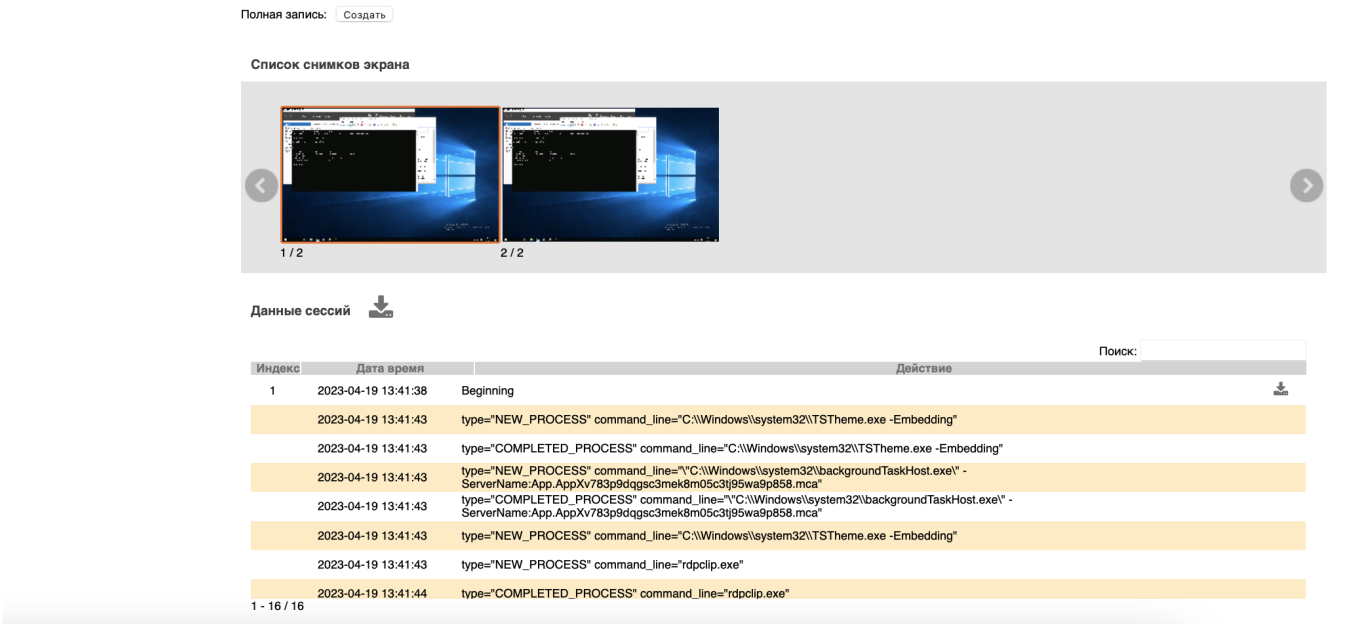


Подробнее Вы можете изучить информацию о сессии , кликнув на  .

В данном диалоге, доступны мета-данные о сессии, видео-поток, который можно полностью скачать,



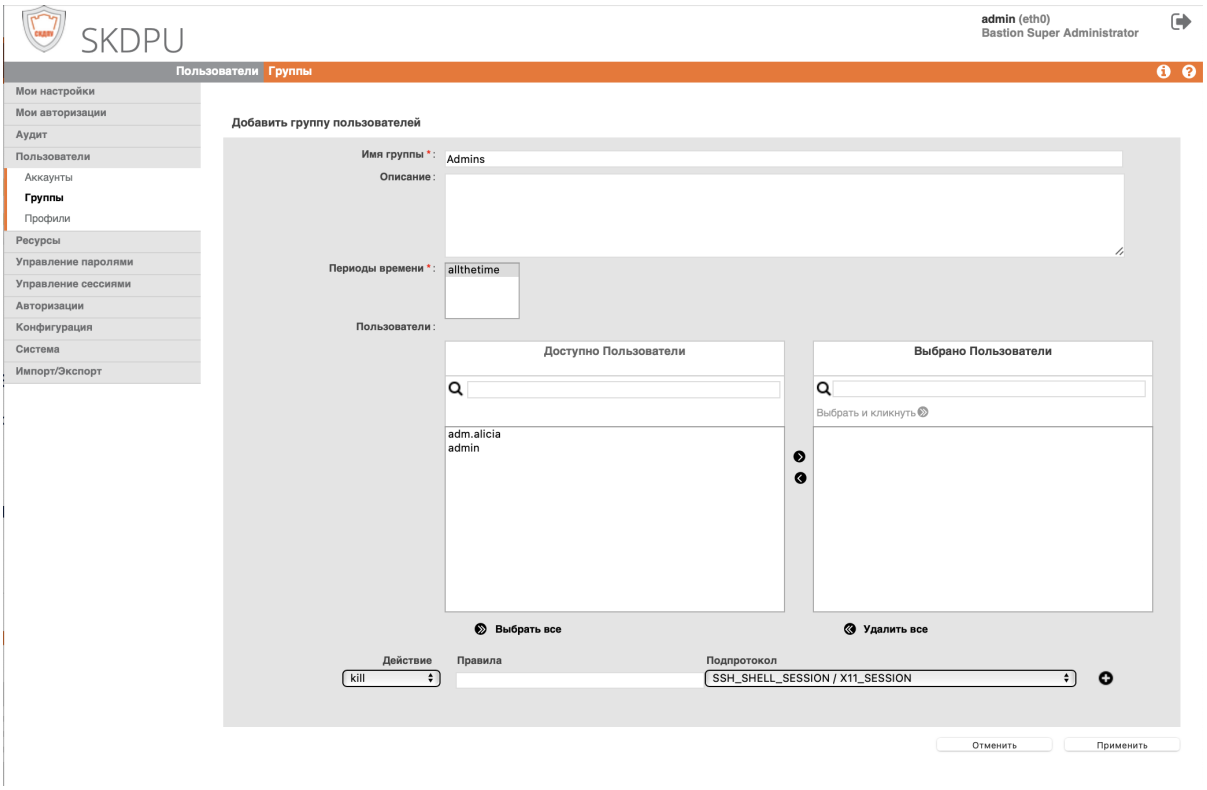
а также оглавление в виде ключевых кадров и список сохраненных системой событий, которые исполнил пользователь, работавший в рамках сессии.

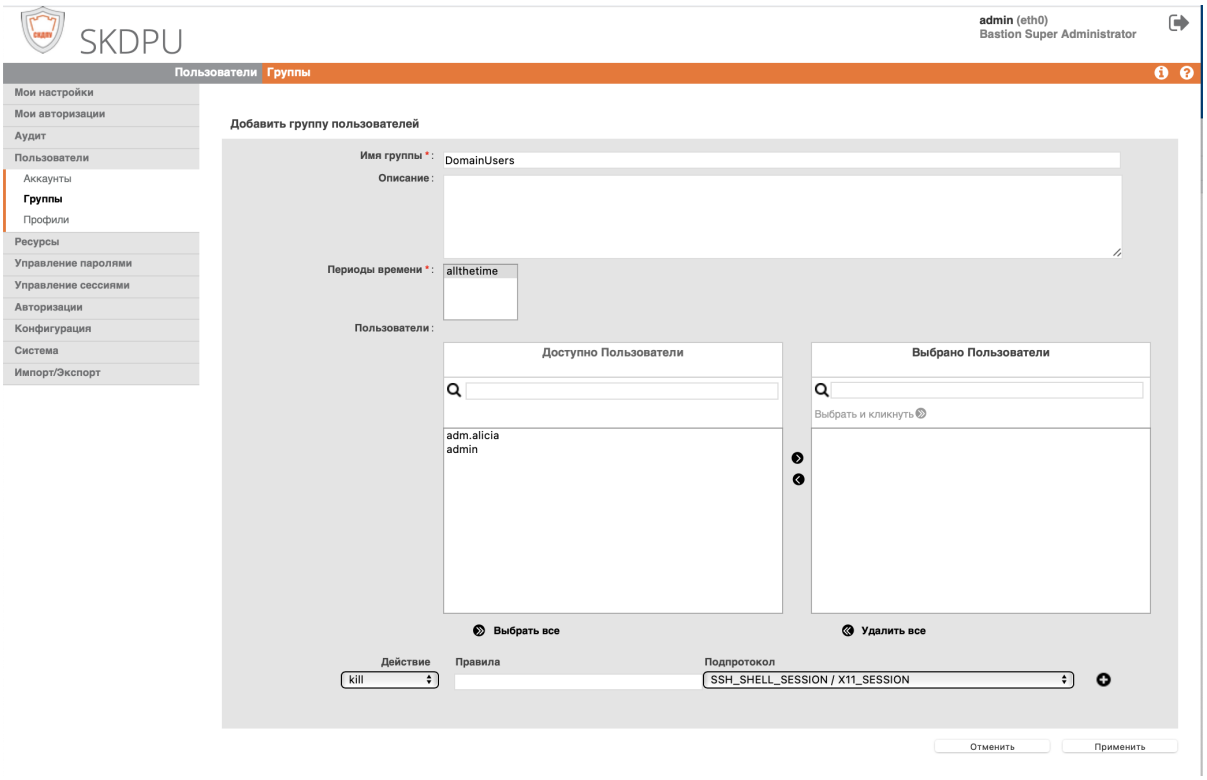


8. Подключение внешних каталогов пользователей

8.1. Настройки Active Directory для авторизации исполнителей

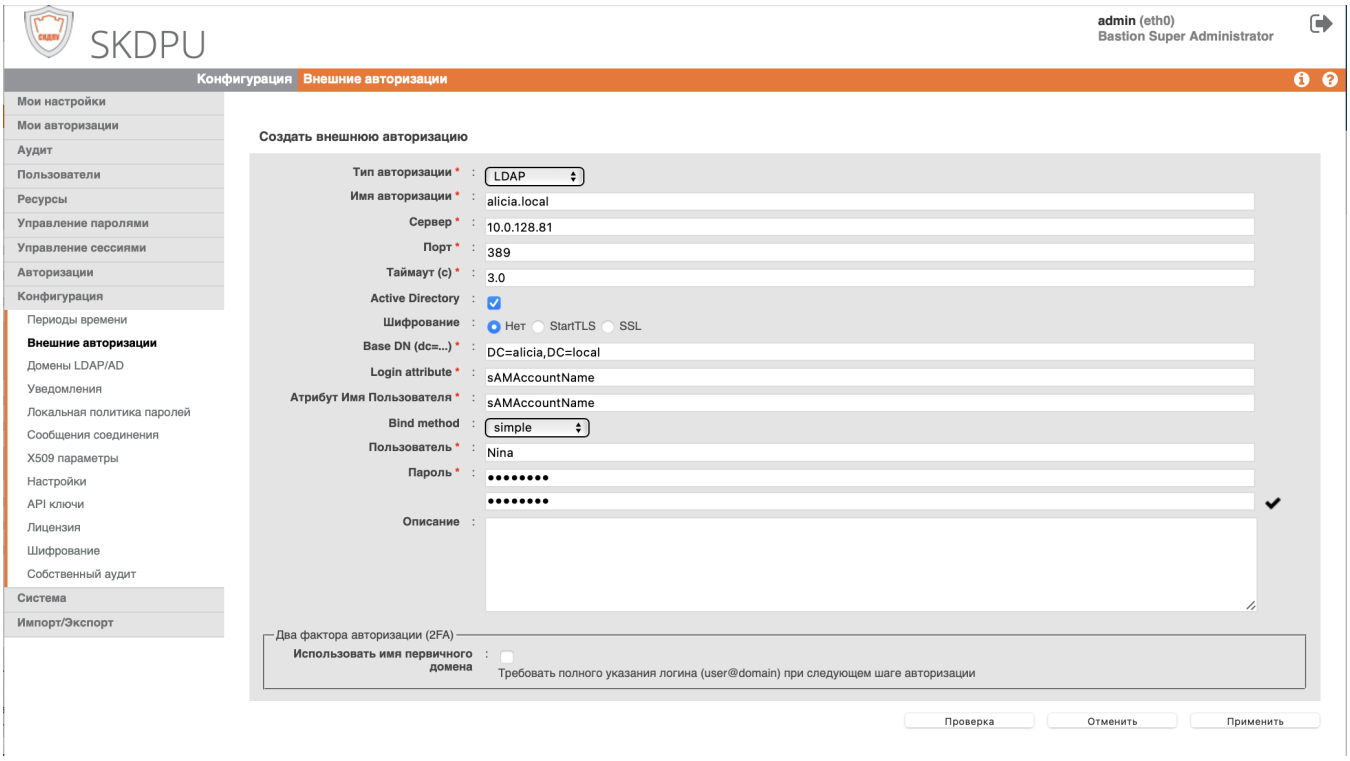
Добавим новые группы Admins и Domain Users в разделе **Пользователи → Группы.**



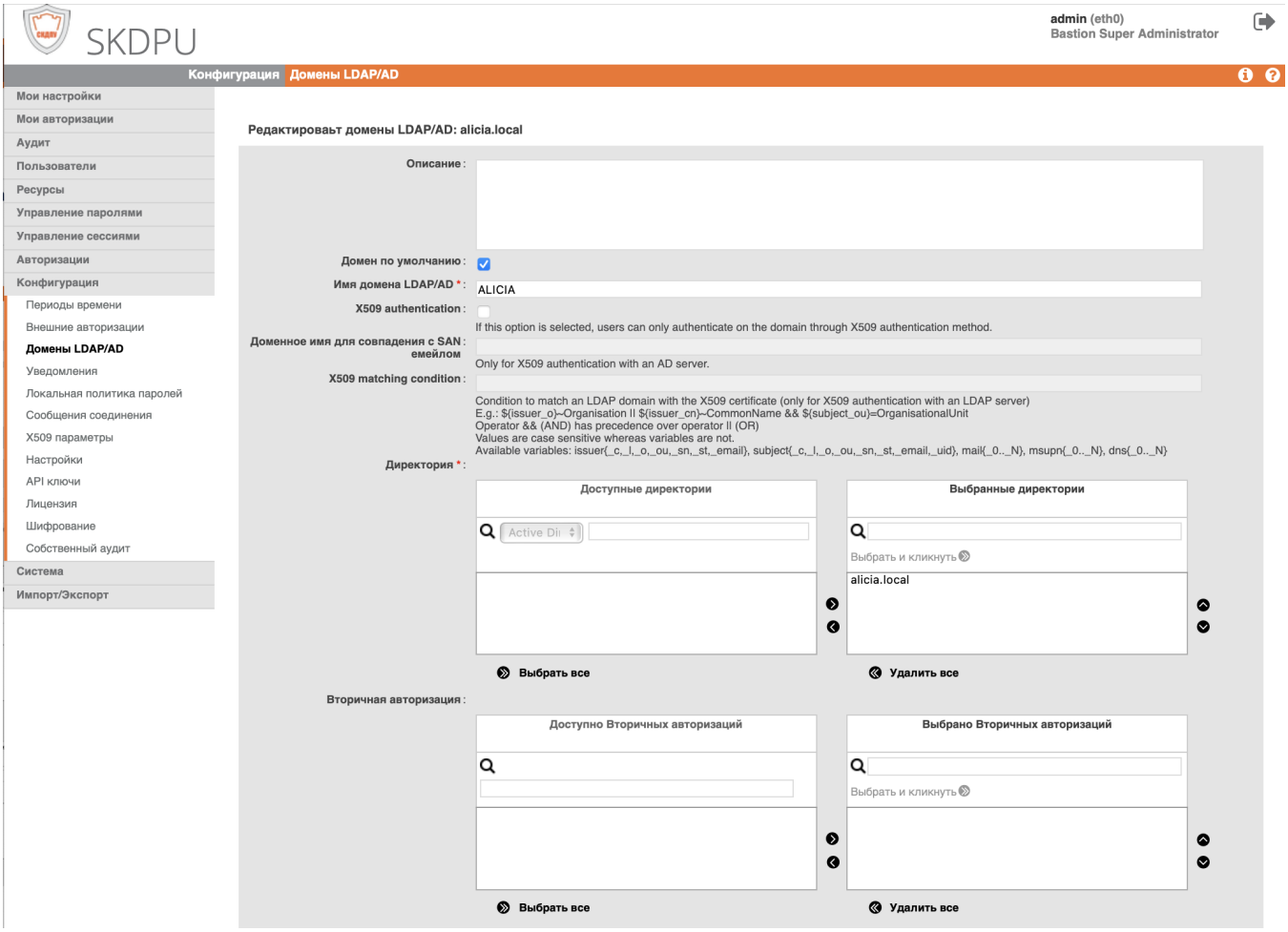


В разделе **Конфигурация → Внешние авторизации** нужно добавить профиль LDAP сервера для работы с AD.

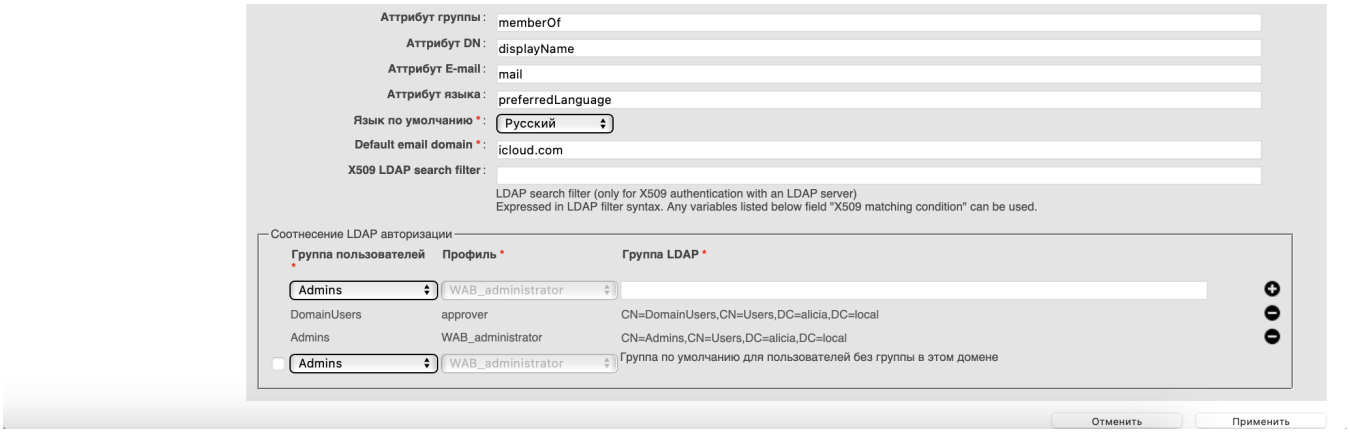
ВАЖНО! Пользователь AD должен обладать достаточными для чтения списка пользователей домена правами, при этом не рекомендуется добавлять самого Администратора домена для авторизации LDAP.



Далее, в разделе **Конфигурация → Домены LDAP\AD** создаем профиль домена и используем в его настройке только что созданный профиль LDAP сервера

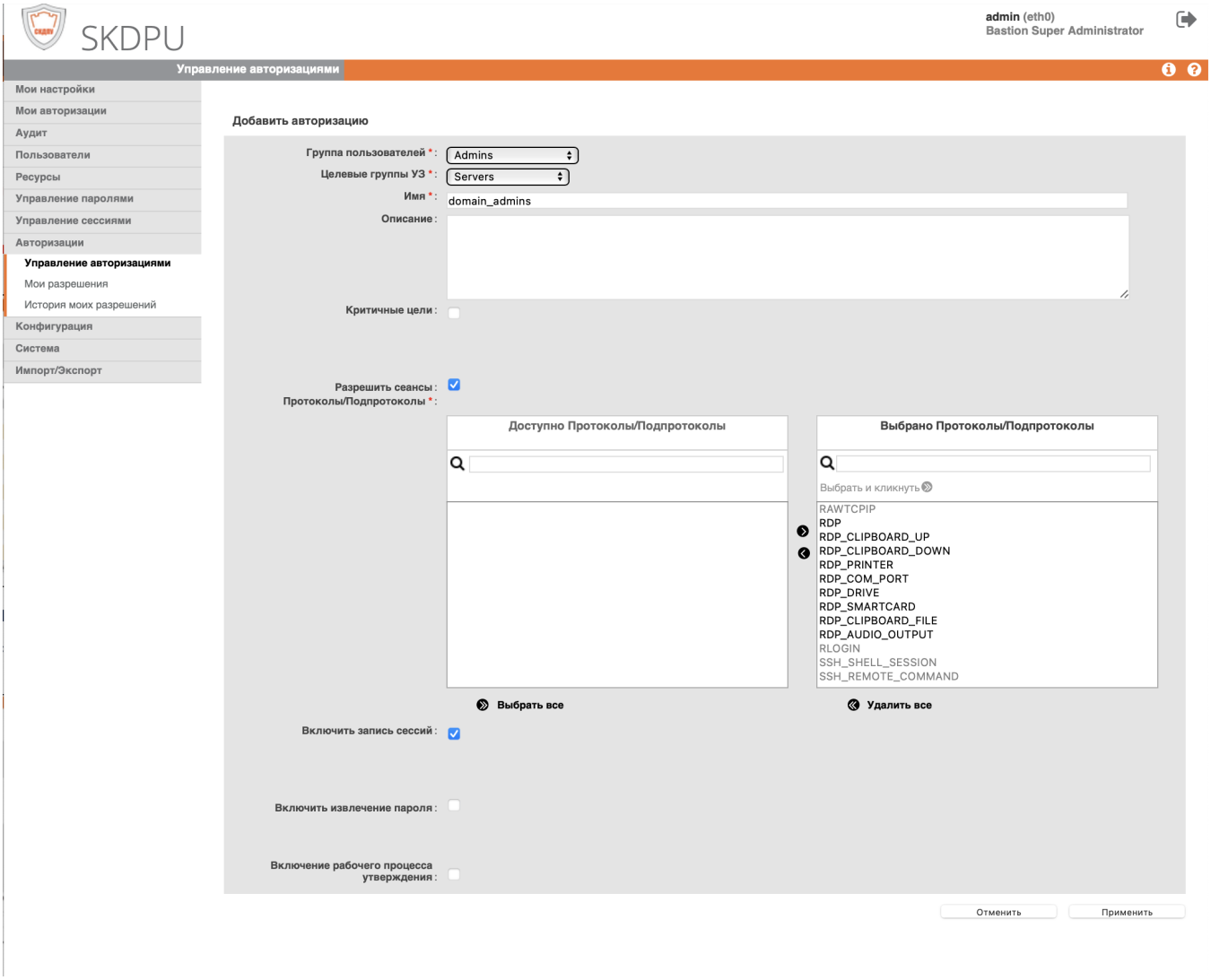


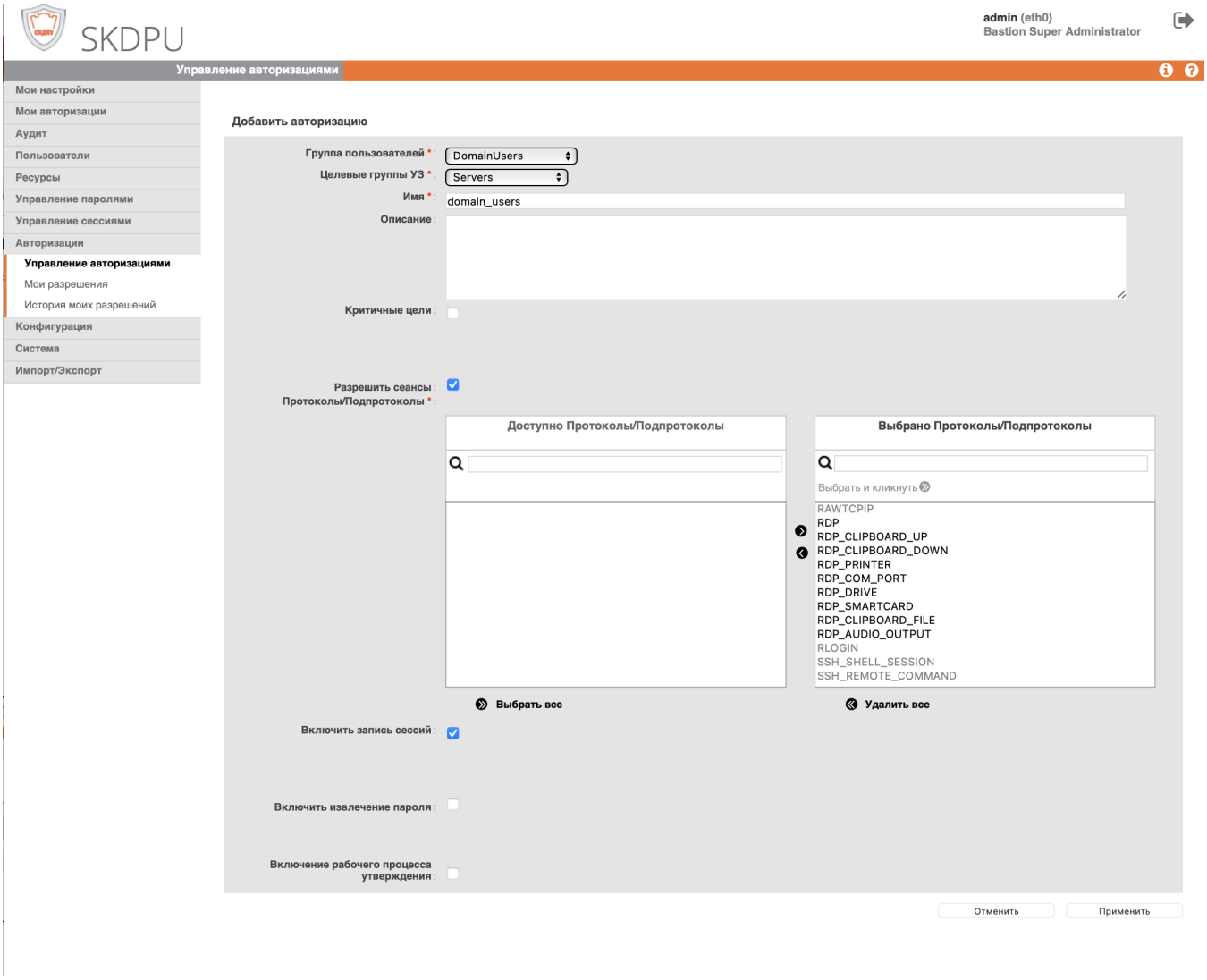
Добавим соотнесение LDAP авторизации. Для созданных групп СКДПУ (в нашем примере, DomainUsers и Admins) укажем атрибуты (CN, OU, DC) групп LDAP Windows Server, которые мы хотим связать с локальными в СКДПУ, и сохраним созданный профиль.



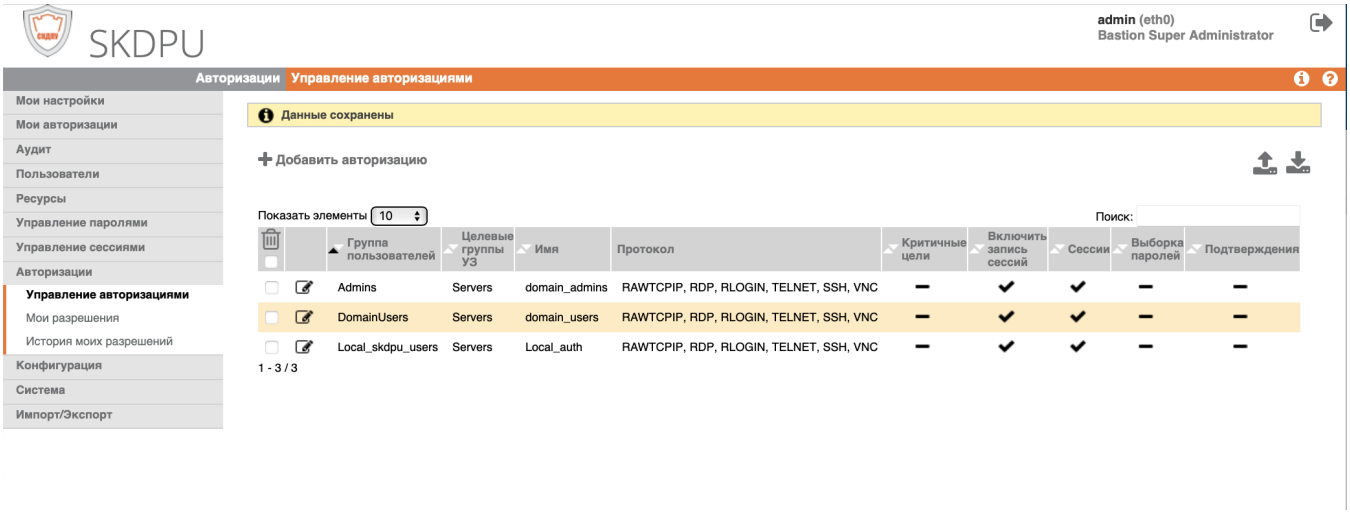
Следующий обязательный шаг – задать соотнесение доменных групп с локальными группами СКДПУ.

В разделе **Авторизации → Управление авторизациями** добавляем правила с использованием групп Admins и DomainUsers.

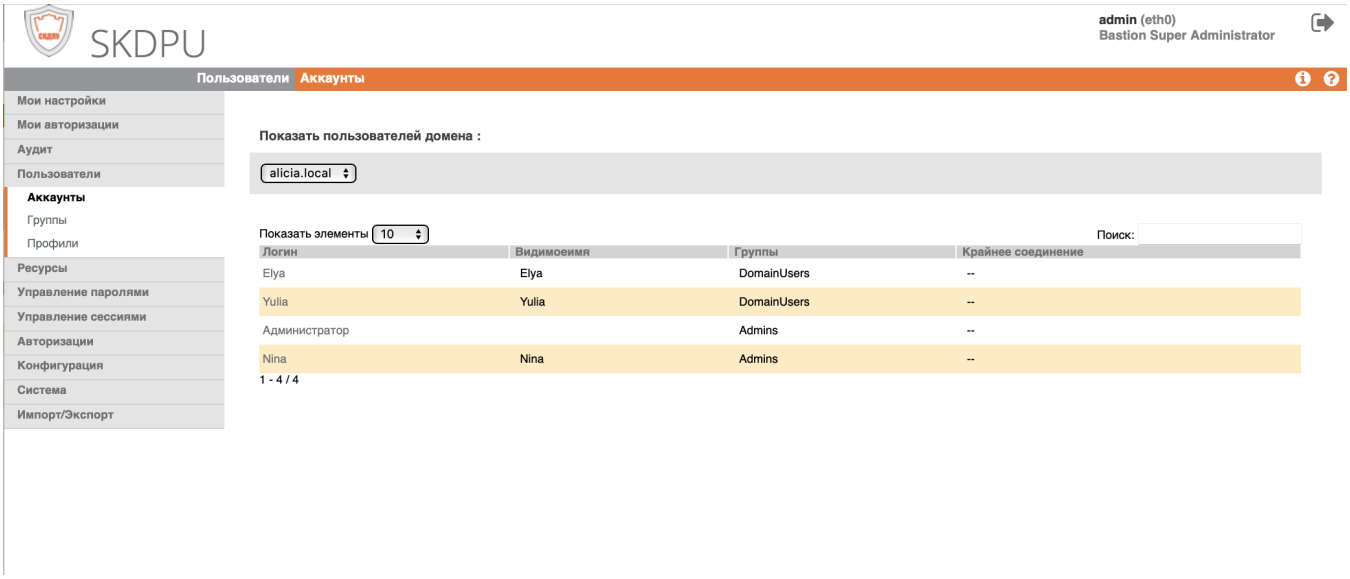

SKDPU
admin (eth0)
Bastion Super Administrator
Управление авторизациями
Мои настройки
Мои авторизации
Аудит
Пользователи
Ресурсы
Управление паролями
Управление сессиями
Авторизации
Управление авторизациями
Мои разрешения
История моих разрешений
Конфигурация
Система
Импорт/Экспорт
Добавить авторизацию
Группа пользователей *: Admins
Целевые группы УЗ *: Servers
Имя *: domain_admins
Описание:
Критичные цели:
Разрешить сеансы:
Протоколы/Подпротоколы *:
Доступно Протоколы/Подпротоколы
Выбрано Протоколы/Подпротоколы
Выбрать и кликнуть
RAWTCPIP
RDP
RDP_CLIPBOARD_UP
RDP_CLIPBOARD_DOWN
RDP_PRINTER
RDP_COM_PORT
RDP_DRIVE
RDP_SMARTCARD
RDP_CLIPBOARD_FILE
RDP_AUDIO_OUTPUT
RLOGIN
SSH_SHELL_SESSION
SSH_REMOTE_COMMAND
Выбрать все
Удалить все
Включить запись сессий:
Включить извлечение пароля:
Включение рабочего процесса утверждения:
Отменить
Применить



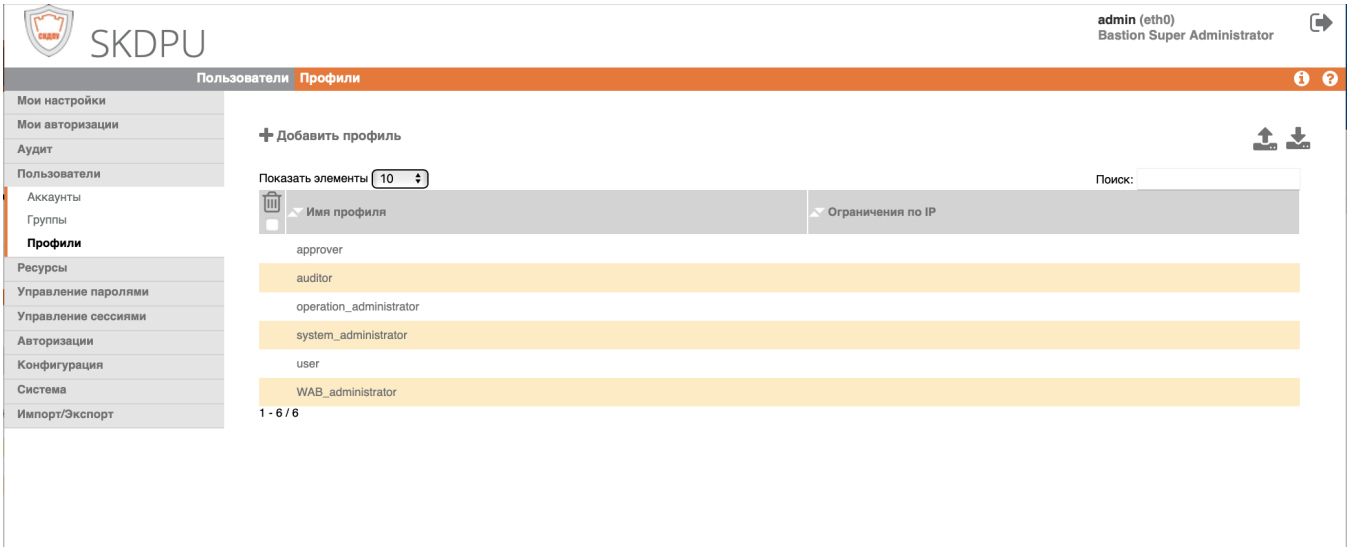
Теперь авторизации должны выглядеть следующим образом



Сохраняем настройки. Если мы все указали правильно, в разделе **Пользователи → Аккаунты** появится возможность переключения между локальными учетными записями и пользователями домена. Для доменных пользователей, входящих в ранее указанные доменные группы, должны указываться локальные группы СКДПУ, с которыми выполнено соотнесение. Если это не так, то возможными причинами могут быть ошибки в настройках – недоступный хост домена, некорректные учетные данные учётной записи для чтения списка пользователей домена, не созданы соответствующие группы, некорректно настроенное соотнесение доменных и локальных групп и т.п.



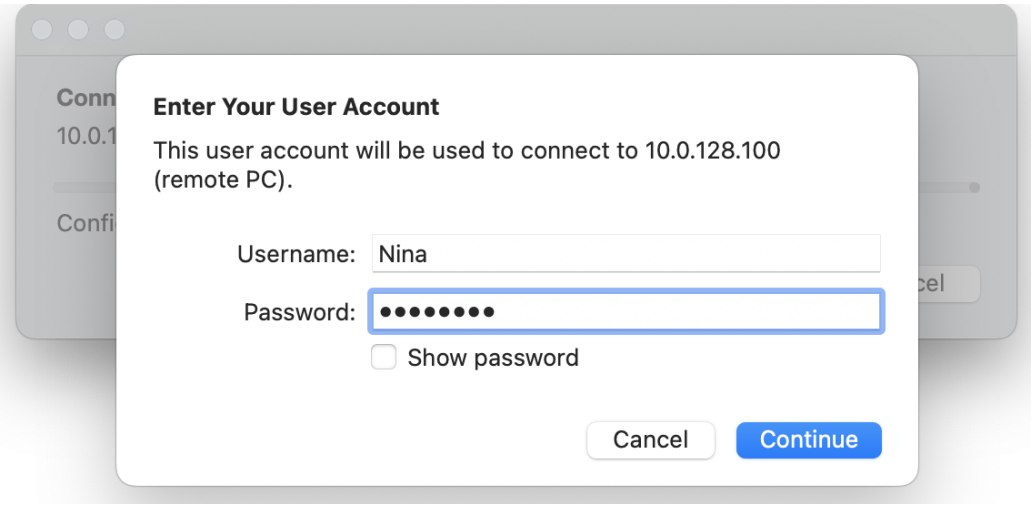
Допустимые профили пользователей описаны в разделе **Пользователи → Профили**, там же можно создать свои профили с удобными ограничениями и разрешениями.

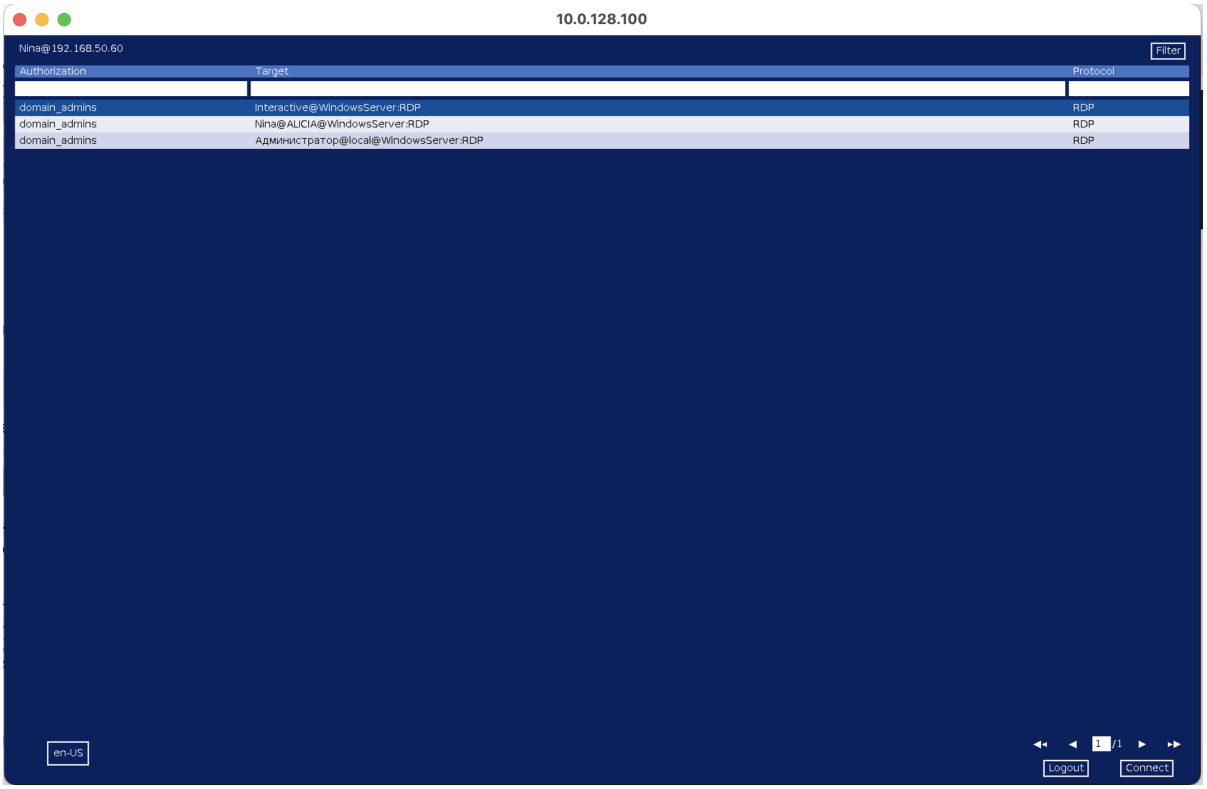


И сможете войти как доменный пользователь как на веб-интерфейс, так и залогиниться непосредственно в клиенте при соединении с СКДПУ.

Логин можно указывать и как DOMAIN\user, и как user@domain.name. Во многом это зависит от сервера домена

Если при создании домена LDAP указывался параметр "Домен по умолчанию", то можно зайти в СКДПУ под пользователем в формате <user> без указания домена





9. Устранение возможных проблем

9.1. Пароль пользователя admin устарел

Для того, чтобы сбросить пароль учетной записи admin требуется:

1. Войти по ssh на систему по порту 2242
2. Повысить привилегии до пользователя root командами

```
super
Password: !QAZ2wsx
sudo -i
Password: !QAZ2wsx
```

3. Ввести команду для сброса пароля:

```
/opt/wab/bin/WABRestoreDefaultAdmin
```

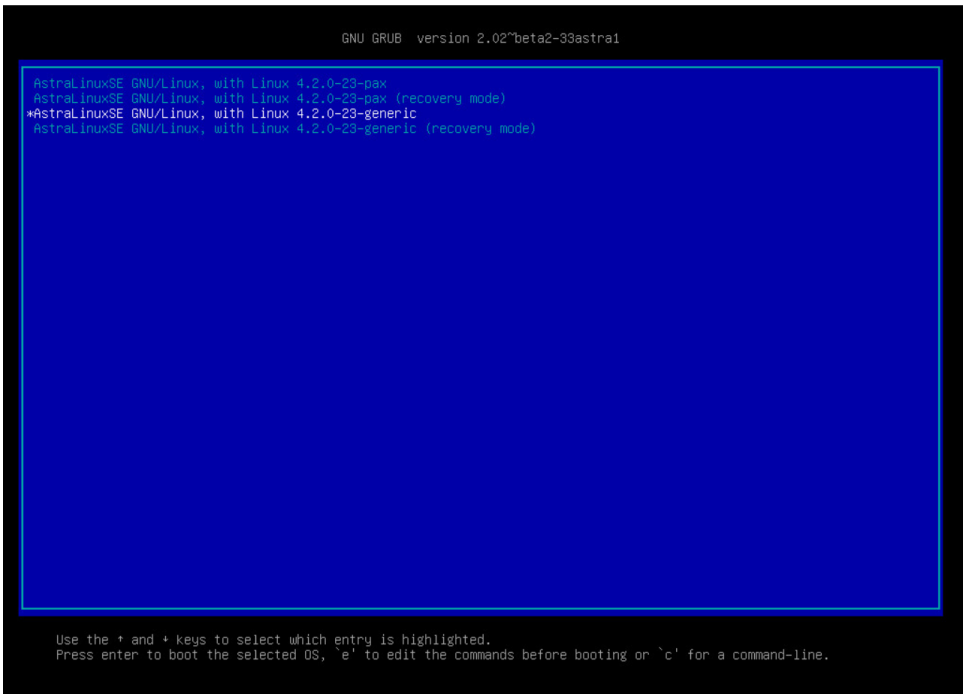
После этого пароль станет стандартным:

Логин -- ***admin***
Пароль -- ***admin***

9.2. Восстановление пароля учетной записи wabadmin

В случае, если при попытке авторизации учетной записи wabadmin возникают ошибки ("Login incorrect", "Access denied", "Password incorrect") или пароль данной учетной записи был утерян, для возобновления доступа к консоли устройства необходимо произвести восстановление пароля. Для этого нужно загрузится в single mode:

1. Перезагрузить сервер командой ***reboot*** сервер, дождаться экрана загрузчика GRUB;



2. Войти в режим редактирования нажатием клавиши "e";
3. Выбрать строку, которая начинается со слова linux или kernel;
4. Удалить из нее слова ***quiet*** и ***splash*** и дописать в конец

```
single init=/bin/bash
```

5. Нажать Ctrl+X. Произойдёт перезагрузка системы, после которой она будет загружена под управлением учетной записи **root.**
6. Войти в консоль, ввести следующие команды:

```
mount -a
pam_tally --user wabadmin --reset
pam_tally2 --user wabadmin --reset
```

7. Перезагрузить устройство командой ***reboot.***
8. После перезагрузки попробовать войти под учетной записью **wabadmin (**пароль: **!QAZ2wsx).**
9. Чтобы получить права суперпользователя, после авторизации ввести следующие команды:

```
super
Password: !QAZ2wsx
sudo -i
Password: !QAZ2wsx
```

10. Если авторизация все ещё невозможна, повторить шаги 1-5.
11. После загрузки системы ввести следующие команды:

```
mount -a
parsec_pam del
passwd wabadmin (  )
parsec_pam add
```

12. Перезагрузить устройство командой reboot и повторить шаги 8-9.

9.3. Восстановления начального состояния системы

Возможны ситуации, когда требуется восстановить начальное состояние системы, для этого необходимо войти в консоль и выполнить следующие команды:

```
/etc/init.d/wab-gui stop
/etc/init.d/wabcore stop
/etc/init.d/wabengine stop
/etc/init.d/postgresql restart
WABSqlInit -f -y
reboot
```