Infrascope

Infrascope (https://ngrsoftlab.ru/infrascope) – это комплексный продукт для управления привилегированным доступом класса Privileged Access Management (PAM).

Подключение Infrascope к Blitz Identity Provider выполняется по протоколу *Radius* и состоит из двух этапов:

- Этап 1. Настройки на стороне Blitz Identity Provider
- Этап 2. Настройки на стороне Infrascope

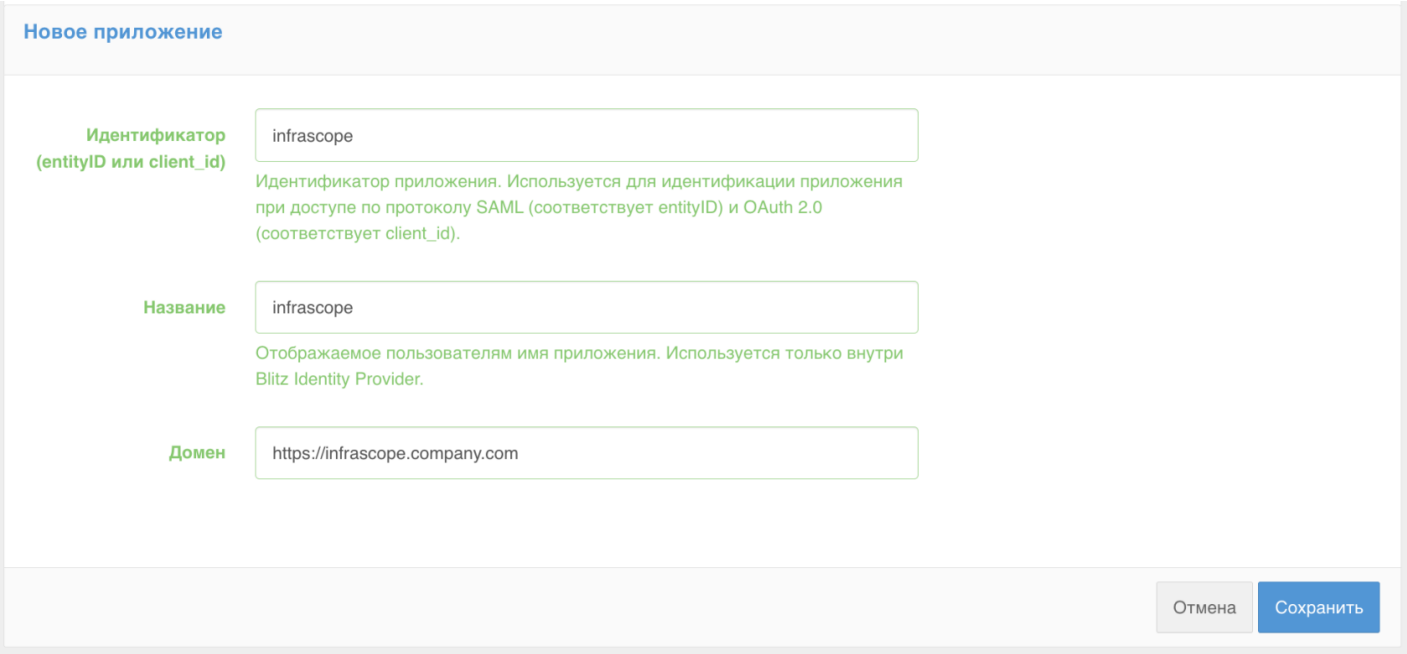
> **Важно:**
>
> В инструкции для примера указано, что Infrascope расположен на домене `https://infrascope.company.com`, а Blitz IDP установлен на домене `https://login.company.com`. Уточните ваши адреса перед применением инструкции.

Этап 1. Настройки на стороне Blitz Identity Provider

В консоли управления *Blitz Identity Provider* перейдите в раздел **Приложения** и выполните следующие действия:

1. **Создайте** новое приложение, задав его базовые настройки:

- **Идентификатор (entityID или client_id)**: введите client_id
- **Название**: имя приложения Infrascope, которое будет отображаться на стороне Blitz IDP
- **Домен**: `https://infrascope.company.com`

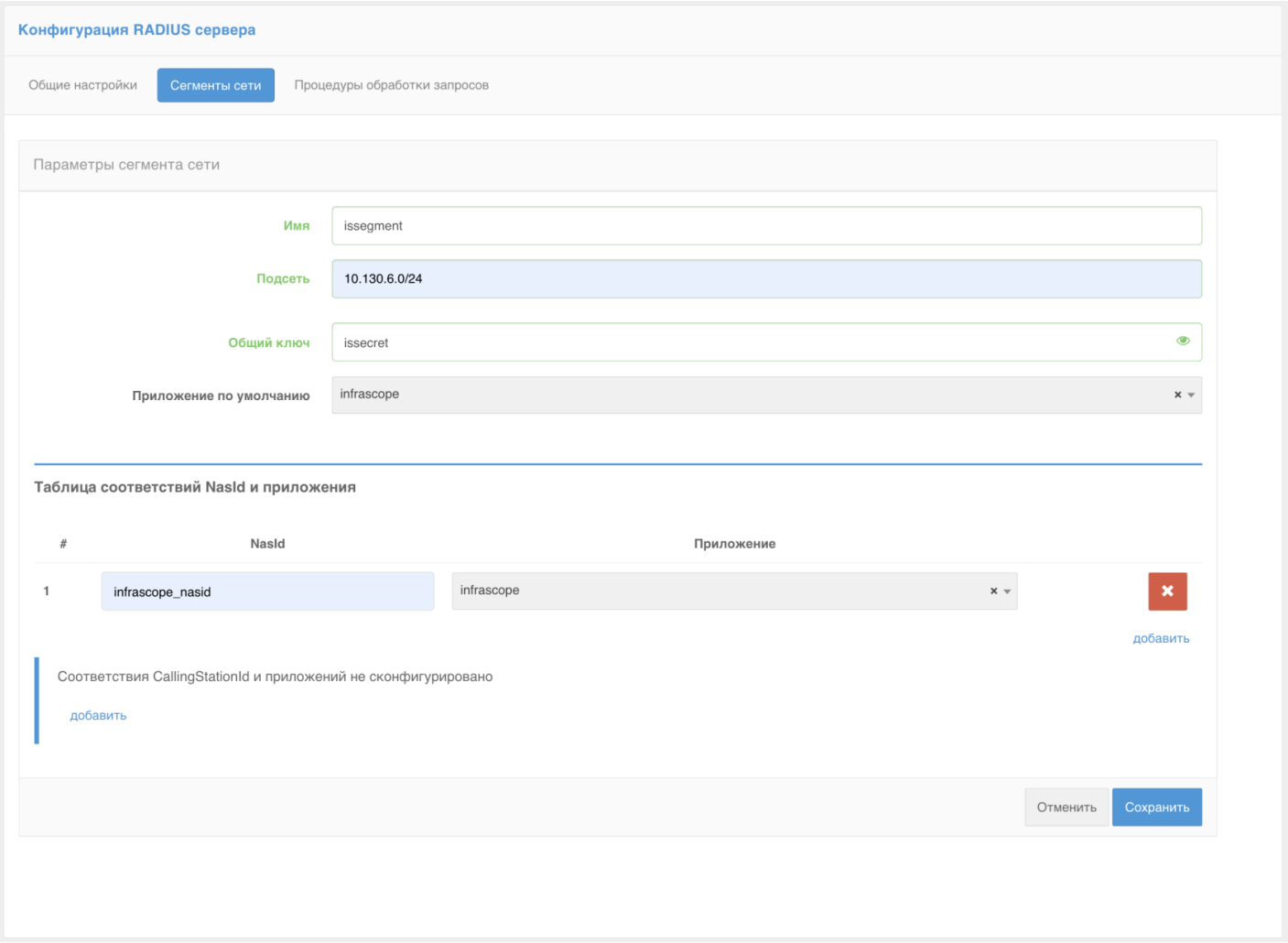


2. Нажмите **Сохранить**.

В консоли управления *Blitz Identity Provider* перейдите в раздел **Radius** и выполните следующие действия:

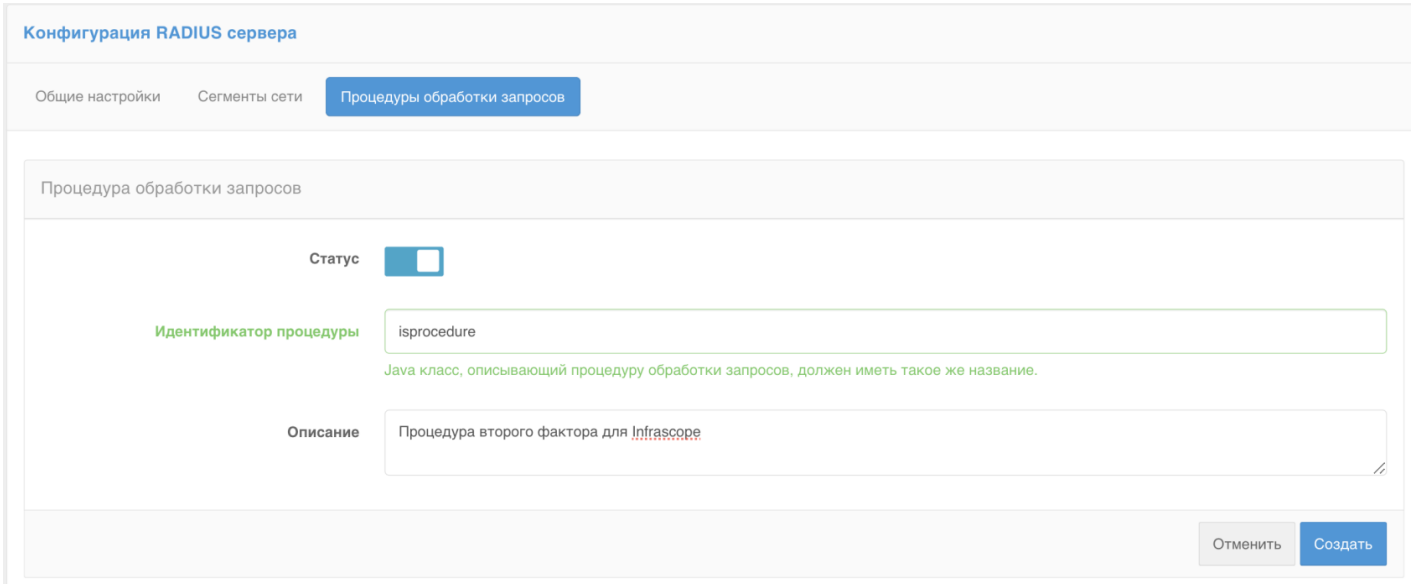
1. Перейдите на вкладку **Общие настройки** и нажмите **Сконфигурировать**. Нажмите **Сохранить** и обновите страницу.
2. Далее перейдите на вкладку **Сегменты сети** и нажмите **Добавить сегмент**. Введите следующие параметры:

- **Имя**: `issegment`
- **Подсеть**: `10.130.6.0/24`
- **Общий ключ**: введите собственный секрет. В данном случае используется `issecret`
- **Приложение по умолчанию**: `infrascope`
- В строке **Соответствия NasId и приложений не сконфигурировано** нажмите **Добавить**.
- **NasId**: `infrascope_nasid`
- **Приложение**: `infrascope`

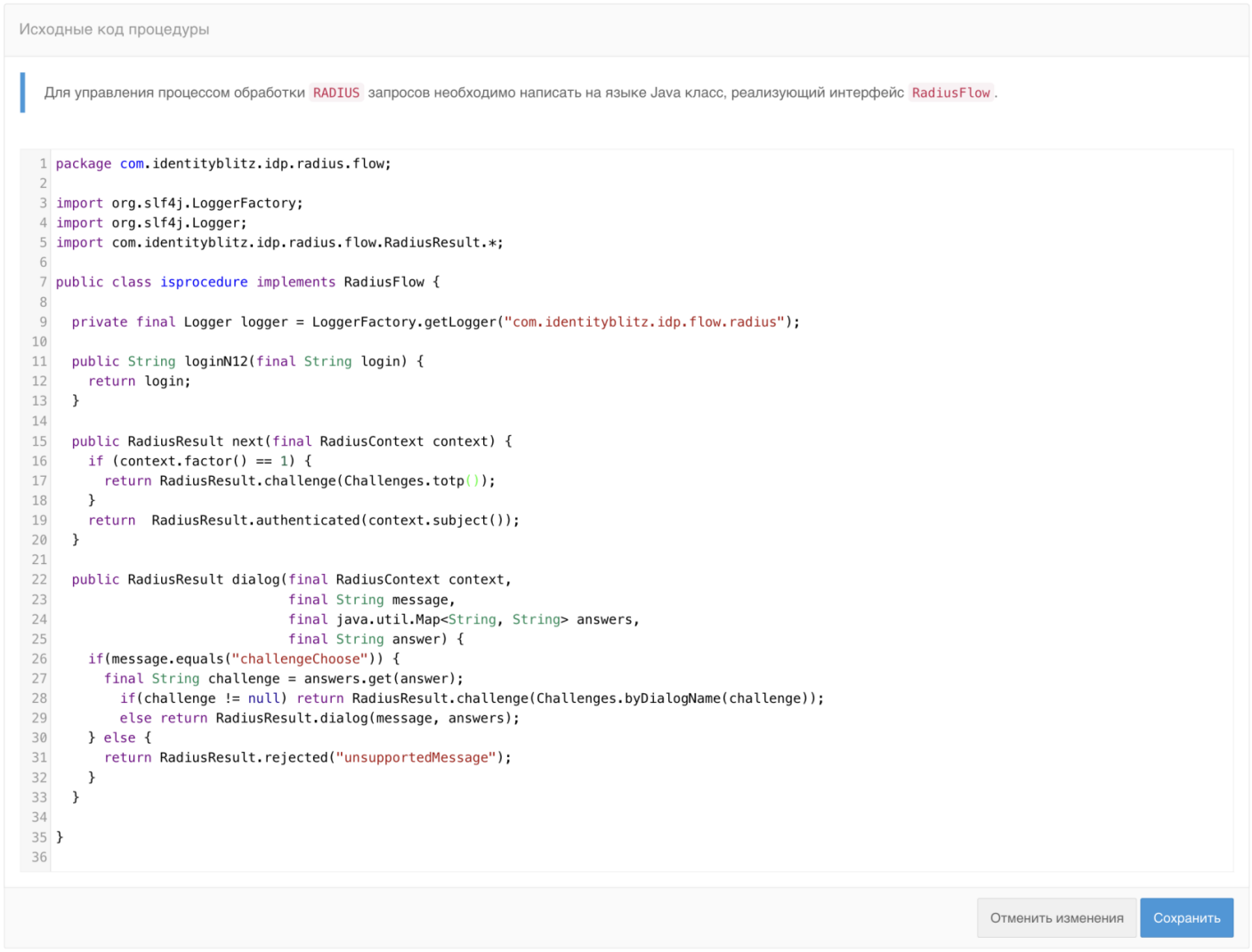


3. Нажмите **Сохранить**.
4. Перейдите на вкладку **Процедуры обработки запросов** и нажмите **Создать новую процедуру запросов**.
5. Укажите параметры:

- **Статус**: сместите ползунок, чтобы параметр стал включенным.
- **Идентификатор процедуры**: `isprocedure`
- **Описание**: введите собственное описание. Например: `Процедура второго фактора для Infrascope`



6. Нажмите **Сохранить** и перейдите в настройки на данной вкладке.
7. В 17 строке измените `return RadiusResult.challenge(Challenges.password());` на `return RadiusResult.challenge(Challenges.totp());`.

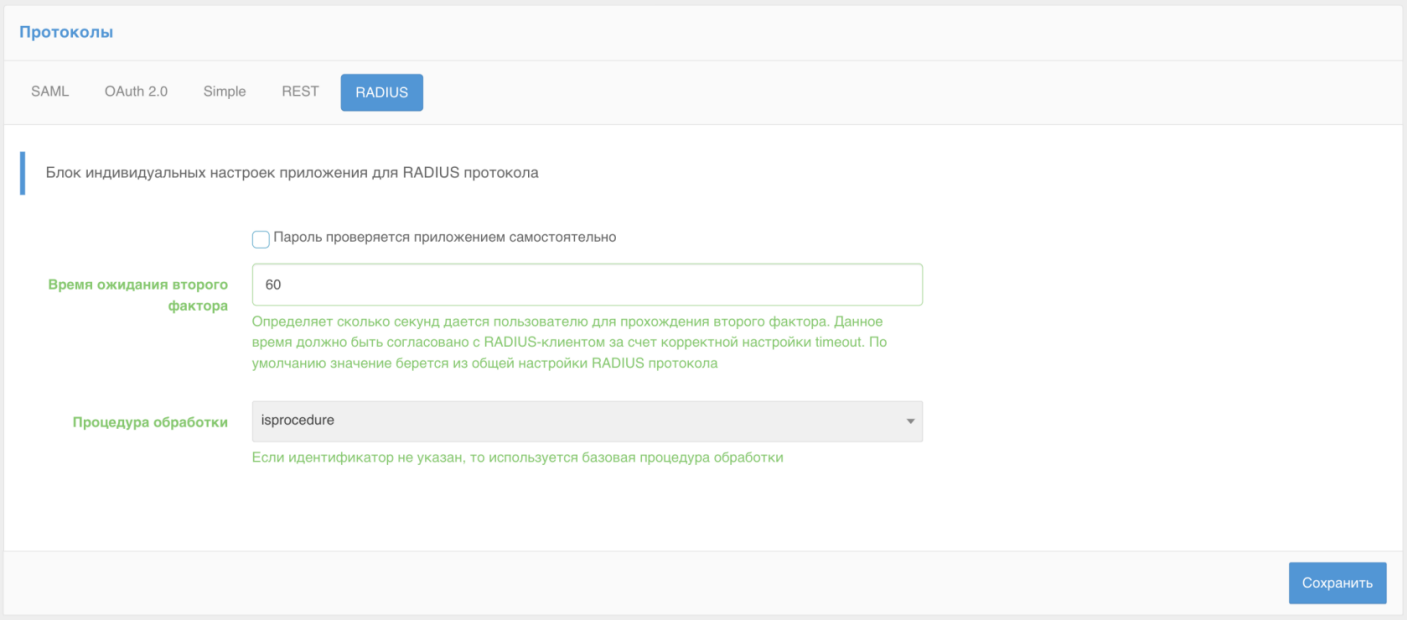


8. Нажмите **Сохранить**.

Далее в консоли управления *Blitz Identity Provider* перейдите в раздел **Приложения** и выполните следующие действия:

1. Нажмите кнопку **Параметры**  у предложения Infrascope и отредактируйте параметры приложения:

- **Протоколы**: выберите `Radius` и нажмите **Сконфигурировать**.
- В параметрах укажите следующие данные:
  - Установите флажок на **Пароль проверяется приложением самостоятельно**, если данная настройка актуальна;
  - **Время ожидания второго фактора**: введите нужное число. Например, `60`
  - **Процедура обработки**: выберите из всплывающего списка название процедуры, которое ввели ранее.

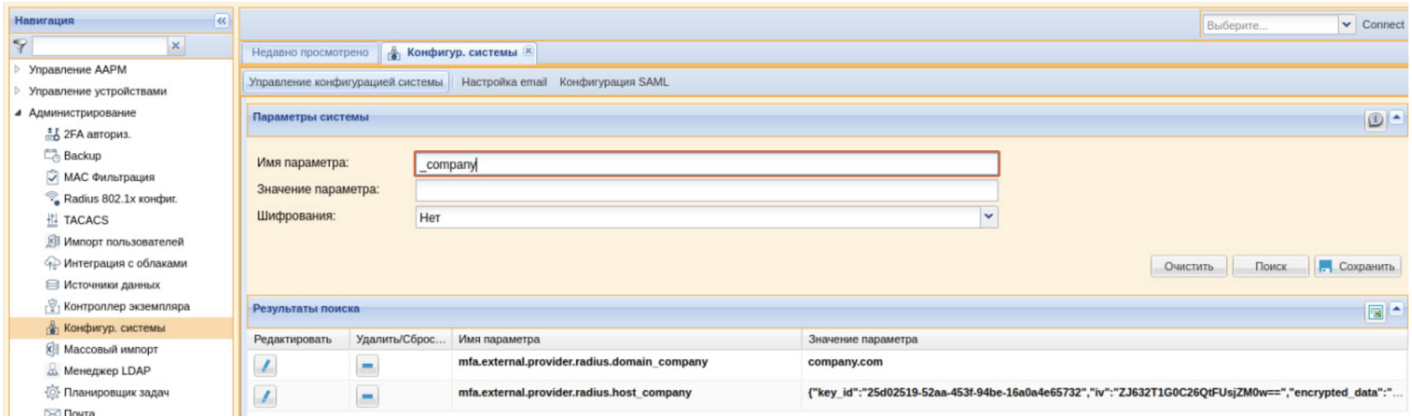


2. Нажмите **Сохранить**.

Этап 2. Настройки на стороне Infrascope

Выполните следующие действия:

1. Войдите в свой профиль Infrascope. Перейдите на вкладку *System Config Man*. Добавьте необходимую версию приложения и параметры.
2. Параметр `mfa.external.provider.radius.host_bltest3` = `radius://blsecret@10.130.100.82/bltest3_nasid?auth-protocol=pap,timeout=500,priority=100;` должен быть сохранен в зашифрованном виде. Параметр создается по формуле `radius://<secret>@<radius.host1>/<nas-id>?auth-protocol=pap,timeout=500,priority=100;radius://<secret>@<radius.host2>/<nas-id>?auth-protocol=pap,timeout=500,priority=100;`, где `secret` и `nasid` созданы в настройках Radius (Вкладка **Параметры сети**) в Blitz IDP.



Совет:

После прохождения всех шагов рекомендуем проверить корректность входа в Infrascope: https://infrascope.company.com

---

Версия #8
Admin создал 2025-06-18 09:07:23 UTC
Обновлено 2025-10-30 16:40:28 UTC