

Руководство по установке и эксплуатации  
программного обеспечения  
**SimpleNMS**

ООО «ОРБСОФТ»  
Москва  
2026

## Введение

Данное руководство предназначено для администраторов программы для ЭВМ «SimpleNMS».

Руководство содержит сведения об установке и первичной настройке системы, активации лицензии, подключении сетевых устройств, резервном копировании и сравнении конфигураций, правилах red flags, а также о настройке каталога, ролей и контроля команд TACACS+/HWTACACS и работе с журналом аудита.

## Оглавление

|                                                           |    |
|-----------------------------------------------------------|----|
| Введение .....                                            | 2  |
| 1. Область применения .....                               | 4  |
| 2. Возможности .....                                      | 4  |
| 3. Установка во внутреннем контуре .....                  | 4  |
| 3.1. Состав поставки .....                                | 4  |
| 3.2. Требования к серверу .....                           | 5  |
| 3.3. Сетевая доступность .....                            | 5  |
| 3.4. Порядок установки.....                               | 6  |
| 4. Программно-аппаратное обеспечение рабочего места ..... | 6  |
| 5. Вход в SimpleNMS .....                                 | 7  |
| 5.1. Вход через корпоративный каталог .....               | 7  |
| 5.2. Аварийный вход.....                                  | 7  |
| 6. Первичная настройка и лицензия .....                   | 8  |
| 6.1. Первичная настройка .....                            | 8  |
| 6.2. Получение лицензии .....                             | 8  |
| 6.3. Установка лицензии.....                              | 9  |
| 6.4. Состояния лицензии .....                             | 9  |
| 7. Обзор .....                                            | 10 |
| 8. Площадки, группы устройств и профили доступа .....     | 10 |
| 8.1. Площадки.....                                        | 10 |
| 8.2. Группы устройств .....                               | 11 |
| 8.3. Профили доступа .....                                | 11 |
| 9. Подключение устройства .....                           | 12 |
| 9.1. Шаг «Параметры» .....                                | 12 |
| 9.2. Шаг «Доступ».....                                    | 13 |
| 9.3. Шаг «SSH-доверие» .....                              | 13 |
| 9.4. Шаг «Определение».....                               | 13 |
| 9.5. Шаг «Backup» .....                                   | 13 |
| 9.6. Шаг «Итог».....                                      | 13 |

|                                                       |    |
|-------------------------------------------------------|----|
| 10. Список устройств и карточка устройства .....      | 14 |
| 10.1. Список устройств .....                          | 14 |
| 10.2. Карточка устройства .....                       | 14 |
| 11. Резервное копирование и версии конфигураций ..... | 15 |
| 11.1. Как создаются версии .....                      | 15 |
| 11.2. Ручной сбор .....                               | 15 |
| 11.3. Расписания .....                                | 15 |
| 11.4. Лента изменений .....                           | 16 |
| 11.5. Сравнение версий .....                          | 17 |
| 11.6. Просмотр конфигурации .....                     | 17 |
| 12. Правила red flags .....                           | 18 |
| 12.1. Создание правила .....                          | 18 |
| 12.2. Срабатывания и проверки .....                   | 19 |
| 13. Каталог и роли .....                              | 20 |
| 13.1. Требования к каталогу .....                     | 20 |
| 13.2. Добавление провайдера .....                     | 20 |
| 13.3. Роли .....                                      | 21 |
| 13.4. Назначение ролей группам каталога .....         | 21 |
| 14. Контроль команд TACACS+/HWTACACS .....            | 22 |
| 14.1. Принцип работы .....                            | 22 |
| 14.2. Разрешения команд .....                         | 22 |
| 14.3. Настройка TACACS+ для устройства .....          | 23 |
| 14.4. Режимы «Только аудит» и «Контроль» .....        | 23 |
| 14.5. Настройка устройства .....                      | 24 |
| 15. Журнал аудита .....                               | 24 |
| 15.1. Команды .....                                   | 24 |
| 15.2. Сессии .....                                    | 25 |
| 15.3. Ошибки доступа .....                            | 26 |
| 16. Информация о разработчике .....                   | 26 |

## 1. Область применения

Программа для ЭВМ «SimpleNMS» (далее – SimpleNMS) предназначена для резервного копирования и версионирования конфигураций сетевого оборудования, контроля изменений и централизованного контроля действий администраторов сетевых устройств.

Система по расписанию и по запросу получает конфигурации устройств по SSH, хранит их в зашифрованном виде, выявляет изменения и сопоставляет их с сессиями администраторов. Встроенный сервер TACACS+/HWTACACS выполняет аутентификацию администраторов через корпоративный каталог Active Directory, покомандную авторизацию и учёт выполненных команд. Пользовательские правила red flags выявляют нежелательные команды и настройки.

SimpleNMS устанавливается во внутреннем контуре организации и после установки не требует доступа в Интернет.

## 2. Возможности

В SimpleNMS администратор имеет возможность:

- вести реестр сетевых устройств с распределением по площадкам и группам;
- подключать устройства с обязательной проверкой SSH host key и автоматическим определением модели, версии ПО и серийного номера;
- выполнять резервное копирование конфигураций вручную и по расписанию;
- просматривать версии конфигураций с контролем целостности по SHA-256;
- отслеживать ленту изменений и построчно сравнивать версии;
- сопоставлять изменения конфигураций с сессиями администраторов;
- задавать правила red flags для команд и конфигураций и просматривать срабатывания;
- аутентифицировать администраторов сетевых устройств через каталог Active Directory;
- разрешать и запрещать команды на устройствах по ролям в режимах «Только аудит» и «Контроль»;
- просматривать журнал команд, административных сессий и ошибок доступа;
- управлять ролями и правами пользователей веб-интерфейса;
- просматривать состояние системы и лицензии.

## 3. Установка во внутреннем контуре

Настоящий раздел описывает порядок установки SimpleNMS на сервер во внутреннем контуре организации. Подробный порядок действий с проверками приведён в документе «Установка SimpleNMS на Linux» из комплекта поставки.

### 3.1. Состав поставки

SimpleNMS поставляется одним архивом `simplenms-<версия>-linux-amd64.tar.gz`. После установки на сервере работают пять контейнеров одного проекта Docker Compose:

- PostgreSQL – база данных;

- Secure Core – хранилище ключей, секретов и лицензии;
- backend – сервер приложения и сервер TACACS+/HWTACACS;
- frontend – веб-интерфейс администратора;
- reverse proxy – TLS-терминация и публикация веб-интерфейса.

На сервер не устанавливаются Java, PostgreSQL, Nginx или иные компоненты: всё необходимое находится внутри образов контейнеров.

### 3.2. Требования к серверу

| Параметр                | Требование                                                                          |
|-------------------------|-------------------------------------------------------------------------------------|
| Операционная система    | Debian 12 и выше либо Ubuntu 22.04 и выше, архитектура amd64                        |
| Процессор               | 4 vCPU                                                                              |
| Оперативная память      | 8 ГБ                                                                                |
| Диск                    | 250 ГБ SSD                                                                          |
| Программное обеспечение | Python 3.10+, Docker Engine 29+, Docker Compose 5+                                  |
| Сетевой адрес           | Статический IPv4-адрес либо DNS-имя, доступное клиентам и самому серверу            |
| Время                   | Синхронизация с NTP-сервером организации                                            |
| TLS                     | Сертификат на адрес SimpleNMS от удостоверяющего центра организации и закрытый ключ |

**Важно.** Сертификат должен содержать точное имя (для DNS-имени) либо точный IP-адрес (для IPv4) в поле Subject Alternative Name. Самоподписанный сертификат установщиком отклоняется. В файл цепочки включите все сертификаты вплоть до корневого: установщик проверяет собственный адрес по этому файлу, не обращаясь к системному хранилищу.

### 3.3. Сетевая доступность

До установки согласуйте следующие направления сетевого доступа:

| Направление | Протокол и порт | Назначение                            |
|-------------|-----------------|---------------------------------------|
| К серверу   | TCP/22          | SSH для администратора сервера        |
| К серверу   | TCP/443         | Веб-интерфейс                         |
| К серверу   | TCP/49          | TACACS+/HWTACACS от сетевых устройств |
| От сервера  | TCP/636         | LDAPS к каталогу Active Directory     |
| От сервера  | TCP/22          | SSH к сетевым устройствам             |
| От сервера  | TCP и UDP/53    | DNS                                   |
| От сервера  | UDP/123         | NTP                                   |
| От сервера  | ICMP            | Проверка доступности устройств        |

### 3.4. Порядок установки

1. Скопируйте архив поставки на сервер по контролируемому каналу и распакуйте его в каталог `/opt/simplenms/releases/simplenms-<версия>`.
2. Подготовьте конфигурацию установщика в каталоге `/etc/simplenms`: файл `installer.env` с публичным адресом системы, файлы секретов и файлы TLS-сертификата и ключа.
3. Перейдите в каталог распакованного релиза и выполните проверку архива:

```
sudo ./install.sh verify
```

4. Выполните проверку сервера на соответствие требованиям:

```
sudo ./install.sh preflight
```

5. Запустите установку и подтвердите состав поставки ответом да:

```
sudo ./install.sh install
```

6. Проверьте состояние установленной системы:

```
sudo /opt/simplenms/current/status.sh
```

Успешная установка завершается сообщением `SimpleNMS installed and healthy; current release activated`, а проверка состояния – сообщением `SimpleNMS current release is healthy`.

Повторный запуск `install.sh install` того же релиза безопасен: он сверяет уже установленные компоненты и сохраняет данные. Обновление на новую версию выполняется скриптом `current/update.sh` с новым архивом.

**Важно.** Не удаляйте тома `Docker simplenms-*` и не переустанавливайте систему начисто: идентификатор установки хранится в `Secure Core`, и его потеря делает установленную лицензию недействительной.

## 4. Программно-аппаратное обеспечение рабочего места

Работа администратора SimpleNMS осуществляется через веб-интерфейс по адресу, заданному при установке. Рекомендуемые параметры рабочего места:

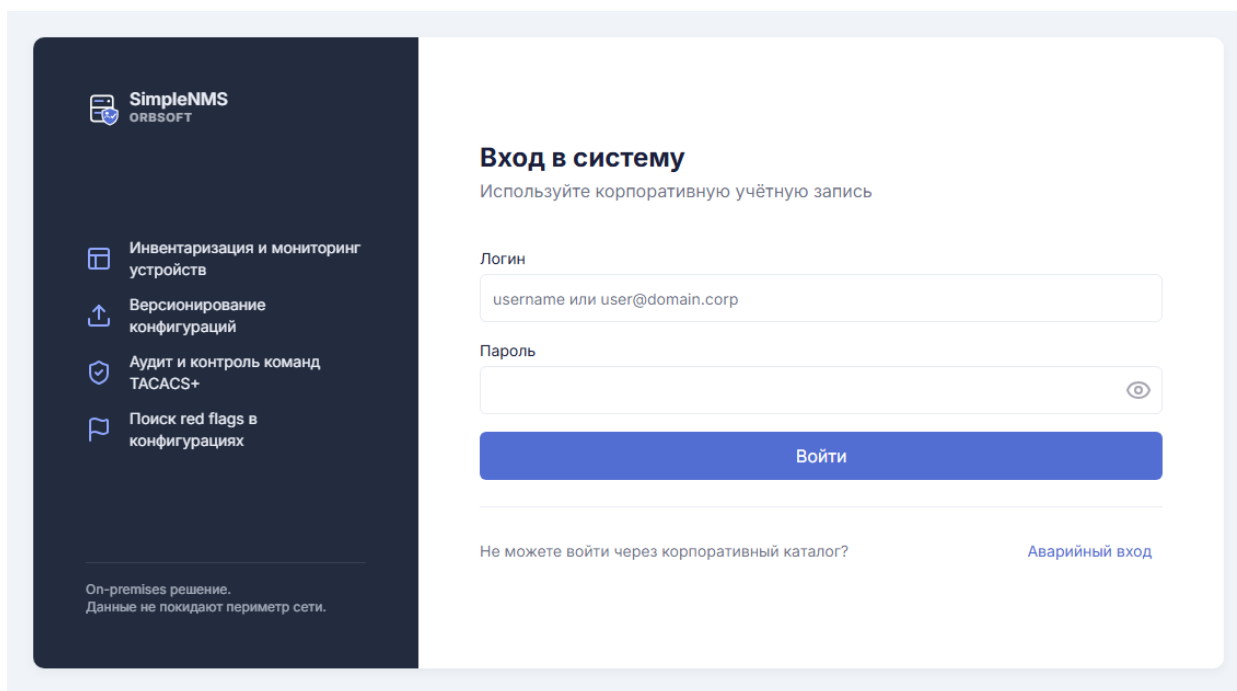
- современный браузер: Google Chrome, Яндекс.Браузер, Microsoft Edge или Mozilla Firefox актуальной версии;
- разрешение экрана не менее 1440×900;
- доступ по 443/TCP к адресу, на котором развёрнут SimpleNMS;
- сертификат удостоверяющего центра организации, выпустившего сертификат SimpleNMS, должен быть доверенным на рабочем месте.

## 5. Вход в SimpleNMS

### 5.1. Вход через корпоративный каталог

Администраторы входят в SimpleNMS под учётными записями корпоративного каталога Active Directory. Права определяются ролями, назначенными группам каталога (см. раздел 13).

1. Откройте в браузере адрес SimpleNMS.
2. Введите логин в формате `username` или `user@domain.corp` и пароль учётной записи каталога.
3. Нажмите «Войти».



### 5.2. Аварийный вход

Локальная аварийная учётная запись создаётся при первичной настройке и предназначена для доступа к системе, когда каталог недоступен или ещё не настроен. Через обычную форму входа эта учётная запись не принимается.

1. На странице входа нажмите «Аварийный вход».
2. Введите логин и пароль локальной учётной записи.
3. Нажмите «Войти».

**Важно.** Каждое использование аварийной учётной записи фиксируется в журнале аудита. Используйте её только для восстановления доступа и первоначальной настройки.

## 6. Первичная настройка и лицензия

### 6.1. Первичная настройка

При первом открытии веб-интерфейса после установки система находится в состоянии «требуется первичная настройка». Для её выполнения:

1. Получите одноразовый секрет первичной настройки из файла `/etc/simplenms/secrets/initial-setup-secret` на сервере. Файл доступен только администратору сервера с правами `root`.
2. Откройте адрес SimpleNMS в браузере и введите секрет.
3. Задайте логин и пароль локальной аварийной учётной записи.
4. Завершите настройку.

Первичная настройка выполняется один раз; повторный запуск блокируется.

### 6.2. Получение лицензии

SimpleNMS работает по офлайн-лицензии, привязанной к конкретной установке. Лицензия выпускается ООО «ОРБСОФТ» по идентификатору установки, который появляется только после первичной настройки.

1. На панели слева выберите раздел «Настройки» → «Система». Откроется страница «Система и лицензия».
2. Скопируйте показанный идентификатор установки (`installationId`).
3. Передайте идентификатор в ООО «ОРБСОФТ» вместе с наименованием организации, требуемым сроком действия и максимальным числом устройств.

#### 4. Получите файл лицензии .snlic.

### Система и лицензия

Диагностика, офлайн-лицензия и защищённые резервные копии SimpleNMS.

Режим SimpleNMS Работает

База данных проверено 21.09.2026, 12:24:32 Доступно

Защищённое ядро Хранилище секретов Доступно

Контроль лицензии Офлайн-проверка лицензии Действительна

#### Состояние системы NORMAL

##### Диагностика

|                     |                       |
|---------------------|-----------------------|
| Объём хранилища     | 1 006,9 ГиБ           |
| Доступно            | 949,6 ГиБ             |
| Использовано        | 5,7%                  |
| Первичная настройка | <span>Включено</span> |
| Всего устройств     | 3                     |
| Вне лицензии        | 0                     |

#### ОФЛАЙН-ЛИЦЕНЗИЯ Действительна

##### SimpleNMS Local

Идентификатор лицензии  
81043203-b18e-46aa-a6ef-38380bcc2772  
Идентификатор установки  
d53b2053-9361-47b1-8168-1f51b77c7d16

|                 |                      |
|-----------------|----------------------|
| Лимит устройств | 25                   |
| Действует с     | 18.09.2026, 16:16:21 |
| Истекает        | 18.09.2031, 16:16:21 |
| Ревизия         | 1                    |

Установить лицензиюВосстановить время лицензии

#### РУЧНОЕ РАСПРЕДЕЛЕНИЕ 3/3

##### Распределение лицензии

Устройства вне лимита останутся видимыми, но для них не выполняются backup, проверка доступности и поиск red flags.

acc-sw-spb-03 acc-sw-msk-02 core-sw-msk-01

Настроить места

### 6.3. Установка лицензии

1. На странице «Система и лицензия» в блоке «Офлайн-лицензия» нажмите «Установить лицензию».
2. Откройте файл .snlic как текст и скопируйте всю строку целиком, без изменений.
3. Вставьте строку в поле «Compact JWS» и отправьте форму.
4. Убедитесь, что состояние лицензии стало VALID, а лимит устройств и срок действия соответствуют ожидаемым.

Продление выполняется той же процедурой с новым файлом лицензии. Новая лицензия выпускается на тот же идентификатор установки; повторная установка той же или более старой лицензии отклоняется.

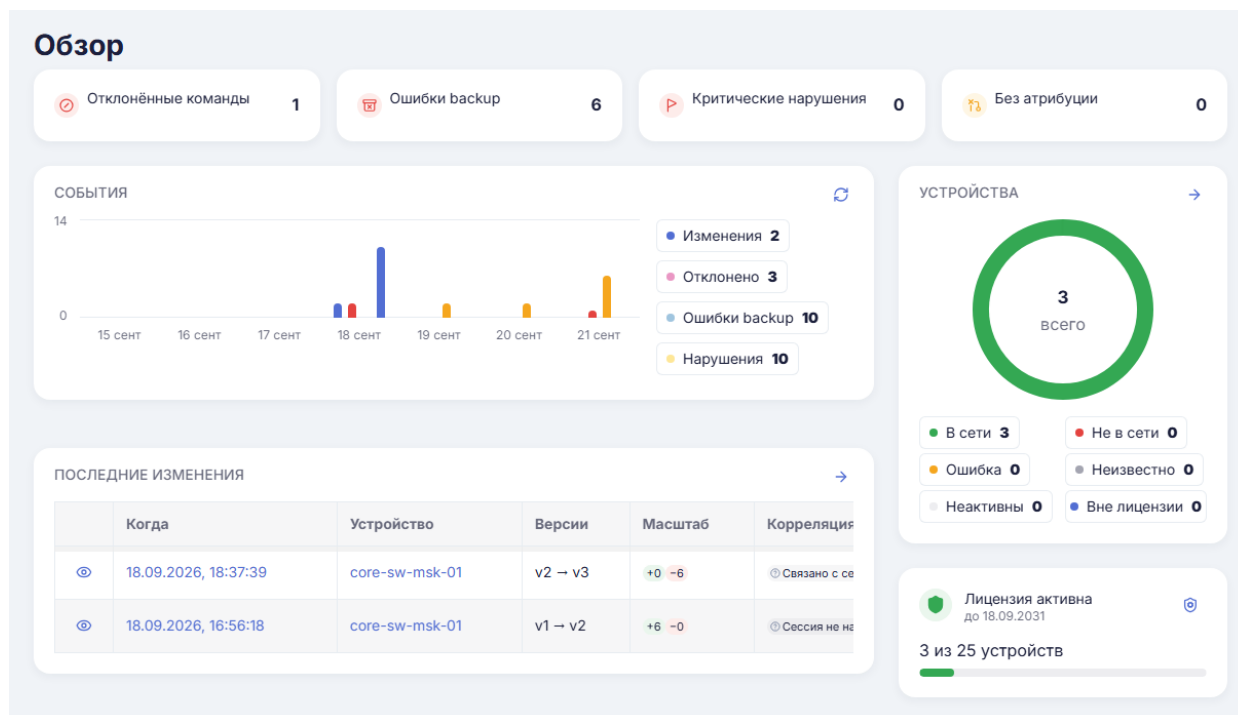
### 6.4. Состояния лицензии

| Состояние     | Значение                                                               |
|---------------|------------------------------------------------------------------------|
| VALID         | Лицензия действует                                                     |
| MISSING       | Лицензия для текущей установки не установлена                          |
| NOT_YET_VALID | Срок действия ещё не наступил; проверьте время сервера                 |
| EXPIRED       | Срок действия истёк; установите продление                              |
| INVALID       | Лицензия не прошла проверку; обратитесь к разработчику с кодом причины |

Без действующей лицензии вход в систему, просмотр сохранённых данных и установка новой лицензии остаются доступны, однако операции с сетевыми устройствами – сбор конфигураций и обслуживание TACACS+ – блокируются.

## 7. Обзор

Раздел «Обзор» открывается после входа и показывает сводное состояние системы: число устройств, изменения конфигураций за период, изменения без установленного автора, активные red flags, состояние лицензии и последние события.



Счётчик «Без атрибуции» показывает изменения конфигураций, которые система зафиксировала, но не смогла связать с сессией администратора (см. раздел 11.4).

## 8. Площадки, группы устройств и профили доступа

До подключения устройств рекомендуется заполнить справочники: площадки, группы устройств и профили доступа. Все они также могут быть созданы непосредственно в мастере подключения устройства.

### 8.1. Площадки

Площадка – физическое или логическое место размещения оборудования. Для добавления площадки:

1. На панели слева выберите раздел «Настройки» → «Площадки».
2. Нажмите кнопку «Добавить» в правой верхней части экрана.
3. Укажите название площадки.
4. Сохраните изменения.

...

Площадки

Площадки

Физические и логические места размещения оборудования.

+ Добавить

|  | Площадка                      | Состояние |
|--|-------------------------------|-----------|
|  | Москва, ЦОД Северный          | Включено  |
|  | Санкт-Петербург, офис Пулково | Включено  |

## 8.2. Группы устройств

Группа устройств объединяет оборудование с общими правилами контроля команд и расписаниями сбора. Для добавления группы:

1. На панели слева выберите раздел «Настройки» → «Группы устройств».
2. Нажмите кнопку «Добавить» в правой верхней части экрана.
3. Укажите необходимые данные:
  - **Название** – краткое обозначение группы;
  - **Режим команд** – режим контроля команд TACACS+ для устройств группы: «Только аудит» – запрещённые команды выполняются, но фиксируются как нарушения; «Контроль» – запрещённые команды отклоняются.
4. Сохраните изменения.

...

Группы устройств

Группы устройств

Группировка устройств и режим контроля команд.

+ Добавить

|  | Группа                   | Режим команд |
|--|--------------------------|--------------|
|  | Доступ — Москва          | Только аудит |
|  | Доступ — Санкт-Петербург | Только аудит |
|  | Ядро сети                | Контроль     |

**Важно.** Новые группы создавайте в режиме «Только аудит». Переход в режим «Контроль» выполняется после проверки журнала команд и настройки разрешений (см. раздел 14.4).

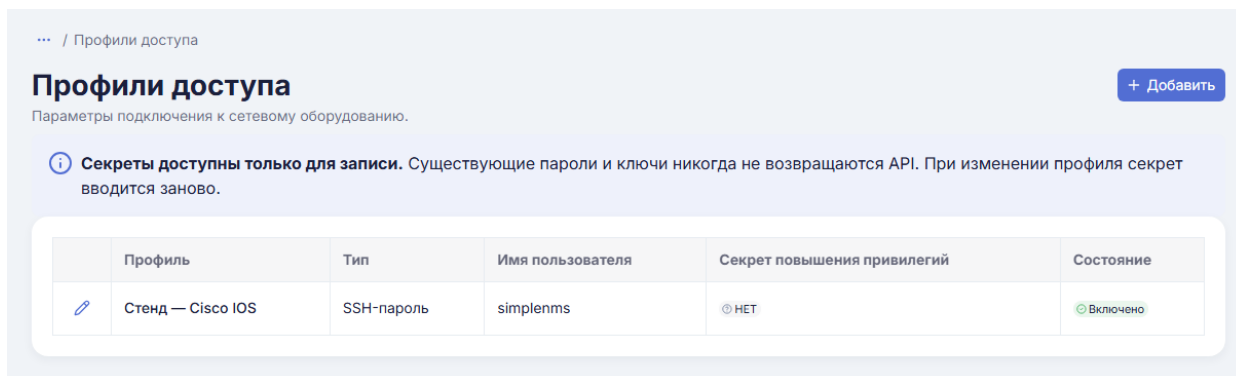
## 8.3. Профили доступа

Профиль доступа – учётные данные, под которыми SimpleNMS подключается к устройствам по SSH. Один профиль может использоваться для нескольких устройств. Для добавления профиля:

1. На панели слева выберите раздел «Настройки» → «Профили доступа».
2. Нажмите кнопку «Добавить» в правой верхней части экрана.
3. Укажите необходимые данные:
  - **Название** – краткое обозначение профиля;

- **Тип** – способ аутентификации: «Пароль» или «Приватный SSH-ключ»;
- **Имя пользователя** – учётная запись на устройстве;
- **Пароль или приватный ключ** – секрет для выбранного способа аутентификации;
- **Секрет повышения привилегий** – пароль режима enable, если он требуется для чтения конфигурации (необязательно).

4. Сохраните изменения.



Секреты хранятся в зашифрованном виде и после сохранения не отображаются.

Рекомендуется выделить для SimpleNMS отдельную учётную запись с правами только на чтение конфигурации.

**Важно.** Если на устройстве включена аутентификация через TACACS+ (см. раздел 14), учётная запись профиля доступа должна существовать в каталоге Active Directory и входить в группу с разрешениями на команды сбора конфигурации.

## 9. Подключение устройства

Устройство подключается мастером из шести шагов: «Параметры», «Доступ», «SSH-доверие», «Определение», «Backup» и «Итог». Результаты каждого шага сохраняются сразу: если закрыть страницу, мастер можно продолжить позже из карточки устройства.

1. На панели слева выберите раздел «Устройства».
2. Нажмите кнопку «Добавить» в правой верхней части экрана. Откроется страница «Добавить устройство».

### 9.1. Шаг «Параметры»

На первом шаге показано состояние лицензии и число свободных мест. Укажите необходимые данные:

- **Название** – уникальное имя устройства, как правило – его hostname;
- **IP / hostname** – адрес для подключения по SSH;
- **SSH-порт** – порт SSH, по умолчанию 22;
- **Вендор** – производитель оборудования: определяет команды сбора конфигурации;
- **Площадка** – площадка размещения; новую можно создать здесь же;
- **Группа устройств** – группа контроля команд и расписаний; новую можно создать здесь же.

Нажмите «Создать и продолжить».

**Важно.** Устройство создаётся уже на этом шаге и занимает место в лицензии, даже если мастер не пройден до конца. Неиспользуемые записи удаляйте из карточки устройства.

## 9.2. Шаг «Доступ»

Выберите существующий профиль доступа либо создайте новый (поля описаны в разделе 8.3). Учётные данные на этом шаге ещё не передаются на устройство.

## 9.3. Шаг «SSH-доверие»

SimpleNMS подключается к устройству только после явного подтверждения его SSH host key. До подтверждения учётные данные на устройство не передаются.

1. Нажмите «Считать host key». Система получит ключ устройства без передачи учётных данных и покажет его тип и отпечаток SHA-256 в состоянии PENDING\_CONFIRMATION.
2. Сверьте отпечаток по доверенному каналу: с отпечатком, полученным от владельца оборудования, либо с вычисленным на самом устройстве.
3. При совпадении нажмите «Подтвердить именно этот ключ». Состояние доверия станет PINNED.

Если отпечаток заранее получен от владельца оборудования, вместо считывания можно использовать «Закрепить fingerprint вручную».

**Важно.** Сверяйте отпечаток целиком – копированием и поиском, а не визуально: в большинстве шрифтов символы 1 и l, V и 8 неразличимы. Подтверждение непроверенного отпечатка делает возможной подмену устройства.

## 9.4. Шаг «Определение»

Нажмите «Определить». Система выполнит на устройстве команды только для чтения и заполнит модель, версию ПО, серийный номер и признак совместимости. Эти данные вручную не редактируются. На этом шаге впервые используются учётные данные профиля доступа; при недействительной лицензии шаг не выполняется.

## 9.5. Шаг «Backup»

Нажмите «Создать первый backup». Система получит конфигурацию устройства и сохранит её как версию v1. Успешное завершение отмечается результатом SUCCESS\_CREATED.

## 9.6. Шаг «Итог»

На последнем шаге показан итоговый список проверок. При полном прохождении мастера индикатор показывает «6 из 6», а устройство переходит в состояние «Готово». Здесь же доступна настройка TACACS+/HWTACACS для устройства (см. раздел 14.3).

Устройства / ... / Завершение подключения

## Завершение подключения

Состояние восстановлено из сохранённых ресурсов. Страницу можно безопасно закрыть.

Открыть карточку

Устройство уже создано. Постоянная ссылка: [карточка устройства](#).

### Настройка сохранённого устройства

11 из 11 обязательных проверок завершено

Готово

✓ Параметры 2 Доступ ✓ SSH-доверие ✓ Определение ✓ Backup ✓ TACACS 7 Итог

#### Итоговый checklist

Каждый незавершённый пункт ведёт к месту исправления.

- ✓ Устройство в лицензии Готово →
- ✓ SSH доступен Готово →
- ✓ Host key подтверждён Готово →
- ✓ Модель и версия определены Готово →
- ✓ Compatibility gate пройден →

## 10. Список устройств и карточка устройства

### 10.1. Список устройств

Раздел «Устройства» показывает все подключённые устройства: название, модель, число активных red flags, класс, адрес, площадку и группу. Доступны поиск по названию, фильтры и постраничная навигация.

### Устройства

+ Добавить

Имя устройства

Фильтры

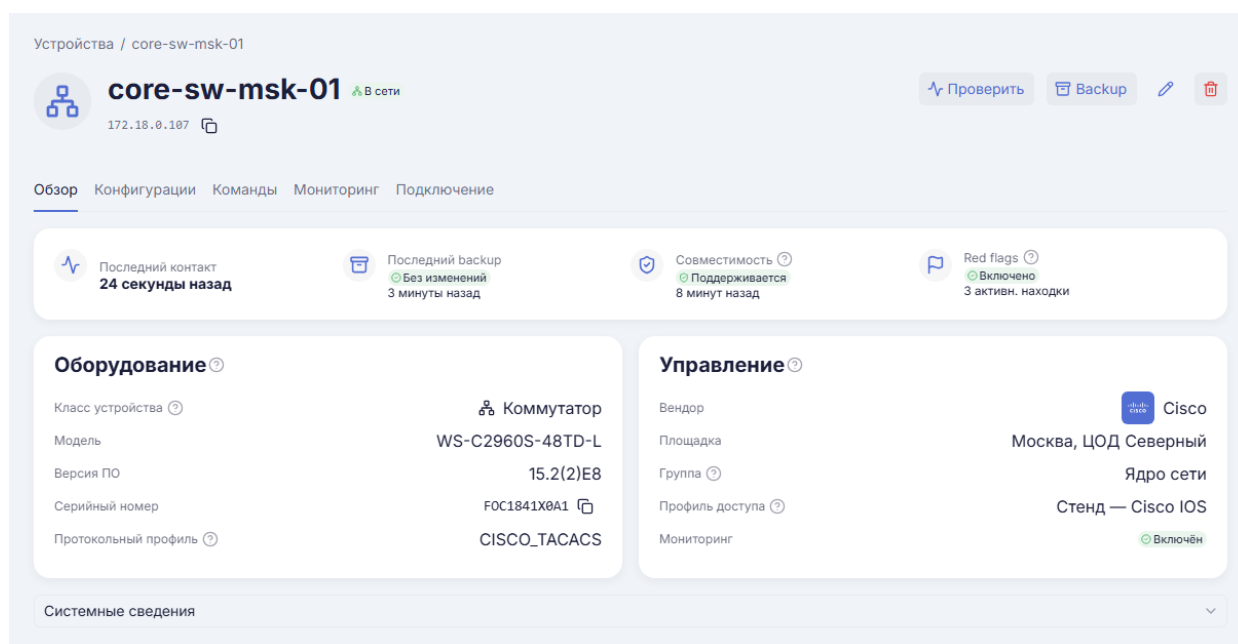
|   | Устройство                                                                                                                                                                                                                                                                                                                                                                  | Класс | Адрес | Площадка | Группа |
|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|-------|----------|--------|
| 👁 |  acc-sw-msk-02 WS-C2960S-48TD-L  2  Коммутатор 172.18.0.108 Москва, ЦОД Северный Доступ — Москва                   |       |       |          |        |
| 👁 |  acc-sw-spb-03 WS-C2960S-48TD-L  2  Коммутатор 172.18.0.109 Санкт-Петербург, офис Пулково Доступ — Санкт-Петербург |       |       |          |        |
| 👁 |  core-sw-msk-01 WS-C2960S-48TD-L  3  Коммутатор 172.18.0.107 Москва, ЦОД Северный Ядро сети                        |       |       |          |        |

Строк на страницу 1-3 из 3

Класс устройства (например, «Коммутатор») система определяет самостоятельно по модели; вручную он не задаётся.

### 10.2. Карточка устройства

Карточка открывается из списка по названию устройства и содержит вкладки «Обзор», «Конфигурации», «Команды», «Мониторинг» и «Подключение». В шапке карточки доступны действия «Проверить» – разовая проверка доступности – и «Backup» – внеплановый сбор конфигурации.



Вкладка «Обзор» показывает состояние устройства: время последнего контакта, совместимость, результат последнего сбора конфигурации и число активных red flags. Ниже расположены два блока:

- **Оборудование** – данные, определённые системой: класс, модель, версия ПО, серийный номер, протокольный профиль. Не редактируются.
- **Управление** – решения администратора: вендор, площадка, группа, профиль доступа, включение мониторинга. Редактируются.

Вкладка «Конфигурации» содержит историю версий устройства, «Команды» – команды, выполненные на устройстве через TACACS+, «Подключение» – параметры SSH-доверия и TACACS+/HWTACACS.

## 11. Резервное копирование и версии конфигураций

### 11.1. Как создаются версии

Каждый сбор конфигурации записывается в журнал запусков, но новая версия v.N создаётся только при первом получении конфигурации или при её изменении. Повторный сбор без изменений новую версию не создаёт. Нумерация версий ведётся отдельно для каждого устройства; для каждой версии вычисляется контрольная сумма SHA-256.

### 11.2. Ручной сбор

Внеплановый сбор конфигурации запускается кнопкой «Backup» в шапке карточки устройства либо кнопкой «Ручной backup» в разделе «Настройки» → «Расписания backup». Такой запуск фиксируется в журнале с триггером MANUAL.

### 11.3. Расписания

Расписание задаёт автоматический сбор конфигураций для группы устройств или отдельного устройства. Для добавления расписания:

1. На панели слева выберите раздел «Настройки» → «Расписания backup».

2. Нажмите кнопку «Добавить» в правой верхней части экрана.
3. Укажите необходимые данные:
  - **Название** – краткое обозначение расписания;
  - **Тип цели** – «Группа» или «Устройство»;
  - **Группа или Устройство** – цель сбора;
  - **Cron** – выражение из пяти полей в UTC; интервал не менее 15 минут. Ниже показываются следующие запуски для проверки.
4. Сохраните изменения.

### Расписания и запуски

Пятичасовой слот, минимальный интервал 15 минут. Часовой пояс устройства не используется.

[Расписания](#)
[Журнал запусков](#)
[Обнаруженные откаты](#)

|  | Расписание                  | Цель            | Cron        | Следующий запуск     |
|--|-----------------------------|-----------------|-------------|----------------------|
|  | Ночной сбор — доступ Москва | Доступ — Москва | 30 22 * * * | 22.09.2026, 03:30:00 |
|  | Ночной сбор — ядро сети     | Ядро сети       | 0 22 * * *  | 22.09.2026, 03:00:00 |

**Важно.** Время в расписании указывается в UTC. Ночной сбор в 01:00 по московскому времени записывается как 0 22 \* \* \*.

Рекомендуется задавать расписания для групп, а не для отдельных устройств: новое устройство, добавленное в группу, попадает под сбор автоматически. Ниже списка расписаний ведётся журнал запусков с фильтрами по устройству, триггеру и результату.

## 11.4. Лента изменений

Раздел «Конфигурации» → «Изменения» показывает по всему парку новые версии конфигураций: устройство, версию, масштаб изменений (число добавленных и удалённых строк), число red flags, автора изменения и время получения.

### Изменения

Версии конфигураций и изменения относительно предыдущего слепка.

[Сравнить](#)

Фильтры

|  | Устройство     | Версия | Изменения     | Red flags | Кто изменил       | Получена             |
|--|----------------|--------|---------------|-----------|-------------------|----------------------|
|  | core-sw-msk-01 | v3     | +0 -6         | 3         | Иван Орлов        | 18.09.2026, 18:37:39 |
|  | core-sw-msk-01 | v2     | +6 -0         | 3         | Сессия не найдена | 18.09.2026, 16:56:18 |
|  | acc-sw-spb-03  | v1     | Первая версия | 2         | —                 | 18.09.2026, 16:55:06 |
|  | acc-sw-msk-02  | v1     | Первая версия | 2         | —                 | 18.09.2026, 16:55:06 |
|  | core-sw-msk-01 | v1     | Первая версия | 2         | —                 | 18.09.2026, 16:53:55 |

Для первой версии устройства в колонке изменений указано «Первая версия». Колонка «Кто изменил» заполняется по сессиям TACACS+, пересекающимся по времени с изменением.

Значение «Сессия не найдена» означает, что конфигурация была изменена вне контролируемого доступа – например, через консоль устройства или до включения TACACS+. Такие изменения учитываются на странице «Обзор» счётчиком «Без атрибуции» и требуют внимания администратора.

## 11.5. Сравнение версий

Открыв строку ленты изменений, вы увидите построчное сравнение предыдущей и новой версии с номерами строк «Было» и «Стало». Добавленные строки отмечены знаком +, удалённые – знаком –. Строки, на которых сработали правила red flags, помечены маркером RED FLAG непосредственно в сравнении.

Изменения / Сравнение

18.09.2026, 18:37:39

**core-sw-msk-01 · v2 → v3**

+0 -6 Связано с сессией

ПОСТРОЧНОЕ СРАВНЕНИЕ

27 строк

| Было | Стало | Конфигурация                                                                   |
|------|-------|--------------------------------------------------------------------------------|
| 1    | 1     | Building configuration...                                                      |
| 2    | 2     |                                                                                |
| 3    | 3     | Current configuration : 912 bytes                                              |
| 4    | 4     | !                                                                              |
| 5    | 5     | ! Sanitized fixture. All identities, addresses and credentials are fictitious. |
| 6    | 6     | !                                                                              |
| 7    | 7     | version 15.2                                                                   |
| 8    | 8     | hostname core-sw-msk-01                                                        |
| 9    | 9     | !                                                                              |
| 10   | 10    | interface GigabitEthernet1/0/1                                                 |
| 11   | 11    | description fixture-uplink                                                     |
| 12   | 12    | no shutdown                                                                    |
| 13   | 13    | !                                                                              |
| 14   | 14    | interface Vlan1                                                                |
| 15   | 15    | ip address 192.0.2.22 255.255.255.0                                            |
| 16   | 16    | !                                                                              |
| 17   | 17    | aaa new-model                                                                  |
| 18   | 18    | ip ssh version 2                                                               |
| 19   | 19    | !                                                                              |
| 20   | -     | logging host 192.0.2.10                                                        |
| 21   | -     | ip domain-name corp.example                                                    |
| 22   | -     | !                                                                              |
| 23   | -     | line vty 0 4                                                                   |
| 24   | -     | transport input telnet                                                         |

## 11.6. Просмотр конфигурации

Страница версии конфигурации показывает контрольную сумму SHA-256, время получения, триггер сбора и полный текст конфигурации с номерами строк. Текст отображается в исходном виде – ровно так, как его отдало устройство, без преобразований.

Устройства / ... / v3

СЛЕПОК КОНФИГУРАЦИИ

**Версия v3**

18.09.2026, 18:37:39 · POST\_SESSION · CISCO\_IOS\_XE:cisco-ios-xe-qualification-v1:v2

54b0f4ebf1eb725eb1b4659b55d4e35a53432e672c2f1aa035eb07e80bbaebd3

18.09.2026, 18:37:39

Red flags Завершено · 3 срабатываний

Диагностика сканирования

ID 5690e511-3b38-4592-b0e9-92a2fa3d132c

**Конфигурация** 21 строк

Исходный payload без преобразований

```

1 Building configuration...
2
3 Current configuration : 912 bytes
4 !
5 ! Sanitized fixture. All identities, addresses and credentials are fictitious.
6 !

```

## 12. Правила red flags

Правила red flags выявляют нежелательные команды и настройки. Встроенного каталога правил нет: набор правил создаёт администратор под политику своей организации.

### 12.1. Создание правила

1. На панели слева выберите раздел «Настройки» → «Правила red flags».
2. Нажмите кнопку «Создать правило» в правой верхней части экрана.
3. Укажите необходимые данные:
  - **Название** – краткое обозначение правила;
  - **Цель** – «Команда» – правило проверяет команды, выполненные через TACACS+; «Конфигурация» – правило проверяет текст конфигурации;
  - **Тип шаблона** – «Подстрока» или «Регулярное выражение»;
  - **Шаблон** – искомый текст либо регулярное выражение;
  - **Условие конфигурации** – «Присутствует» – нарушение, если шаблон найден; «Отсутствует» – нарушение, если строка отсутствует;
  - **Область** – «Весь парк», «Группа» или «Вендор» с указанием группы либо вендора;
  - **Критичность** – от «Информационная» до «Критическая»;
  - **Комментарий** – пояснение для администраторов.
4. Сохраните изменения.

## Red flags

Пользовательские правила для команд и конфигураций. Встроенного каталога нет.

Правила
Срабатывания
Проверки

Запустить проверку

+ Создать правило

Фильтры

|  | Правило                                                                   | Цель         | Условие             | Область   | Критичность |
|--|---------------------------------------------------------------------------|--------------|---------------------|-----------|-------------|
|  | Контроль: точная строка logging host 192.0.2.10 · logging host 192.0.2.10 | Конфигурация | Подстрока · ABSENT  | Весь парк | INFO        |
|  | Модель AAA не активирована · aaa new-model                                | Конфигурация | Подстрока · ABSENT  | Весь парк | Высокая     |
|  | SSH версии 2 не включён · ip ssh version 2                                | Конфигурация | Подстрока · ABSENT  | Весь парк | Высокая     |
|  | Telnet разрешён на линиях VTY · transport input telnet                    | Конфигурация | Подстрока · PRESENT | Весь парк | Критическая |
|  | Не задан сервер журналирования · logging host                             | Конфигурация | Подстрока · ABSENT  | Весь парк | MEDIUM      |
|  | Не включено шифрование паролей · service password-encryption              | Конфигурация | Подстрока · ABSENT  | Весь парк | Высокая     |

**Важно.** Условие «Отсутствует» проверяет наличие строки, точно равной шаблону, а не вхождение подстроки. Правила вида «должно быть настроено» записывайте полной строкой конфигурации, как она выглядит на устройстве. Так, при наличии в конфигурации строки `logging host 192.0.2.10` правило с шаблоном `logging host` и условием «Отсутствует» работает, а с шаблоном `logging host 192.0.2.10` – нет.

## 12.2. Срабатывания и проверки

Раздел «Конфигурации» → «Red flags» показывает срабатывания правил: время, критичность, цель и правило. Цель срабатывания бывает двух видов: «Конфигурация» – нарушение в конкретной версии конфигурации, «Изменение» – нарушение, появившееся в конкретном изменении.

## Red flags

Пользовательские правила для команд и конфигураций. Встроенного каталога нет.

Правила
Срабатывания
Проверки

Запустить проверку

+ Создать правило

Фильтры

|  | Правило                                                                   | Цель         | Условие             | Область   | Критичность |
|--|---------------------------------------------------------------------------|--------------|---------------------|-----------|-------------|
|  | Контроль: точная строка logging host 192.0.2.10 · logging host 192.0.2.10 | Конфигурация | Подстрока · ABSENT  | Весь парк | INFO        |
|  | Модель AAA не активирована · aaa new-model                                | Конфигурация | Подстрока · ABSENT  | Весь парк | Высокая     |
|  | SSH версии 2 не включён · ip ssh version 2                                | Конфигурация | Подстрока · ABSENT  | Весь парк | Высокая     |
|  | Telnet разрешён на линиях VTY · transport input telnet                    | Конфигурация | Подстрока · PRESENT | Весь парк | Критическая |
|  | Не задан сервер журналирования · logging host                             | Конфигурация | Подстрока · ABSENT  | Весь парк | MEDIUM      |
|  | Не включено шифрование паролей · service password-encryption              | Конфигурация | Подстрока · ABSENT  | Весь парк | Высокая     |

Анализ выполняется автоматически после каждого сбора конфигурации. Новое правило не применяется к ранее собранным конфигурациям само по себе: для этого нажмите «Запустить проверку» на вкладке «Проверки».

## 13. Каталог и роли

### 13.1. Требования к каталогу

SimpleNMS аутентифицирует пользователей веб-интерфейса и администраторов сетевых устройств через каталог Active Directory по протоколу LDAPS. Для подключения требуются:

- адрес контроллера домена и порт LDAPS (как правило, 636);
- сервисная учётная запись каталога с правом чтения пользователей и групп;
- сертификат удостоверяющего центра, выпустившего сертификат контроллера домена, в формате PEM;
- группы каталога, которым будут назначены роли SimpleNMS.

**Важно.** Каталог должен быть Active Directory: система использует атрибуты sAMAccountName, userPrincipalName, memberOf и objectGUID. Каталоги с иной схемой не поддерживаются.

### 13.2. Добавление провайдера

1. На панели слева выберите раздел «Настройки» → «LDAP-провайдеры».
2. Нажмите кнопку «Добавить провайдера» в правой верхней части экрана.
3. Укажите необходимые данные:
  - **Название** – краткое обозначение провайдера;
  - **Адреса LDAPS через запятую** – адреса контроллеров домена в формате ldaps://host:636;
  - **Базовый DN** – корень поиска пользователей и групп, например DC=corp,DC=example;
  - **DN сервисной учётной записи** – учётная запись для подключения к каталогу;
  - **Пароль сервисной учётной записи** – пароль этой учётной записи; после сохранения не отображается;
  - **Доверенный сертификат СА (PEM)** – сертификат удостоверяющего центра каталога.
4. Сохраните изменения.
5. Откройте провайдера и нажмите «Проверка подключения». Для каждого адреса должен быть показан успешный результат.

...

Каталог и аутентификация

Провайдеры аутентификации

LDAPS-подключения и назначения ролей SimpleNMS по внешним группам.

+ Добавить провайдера

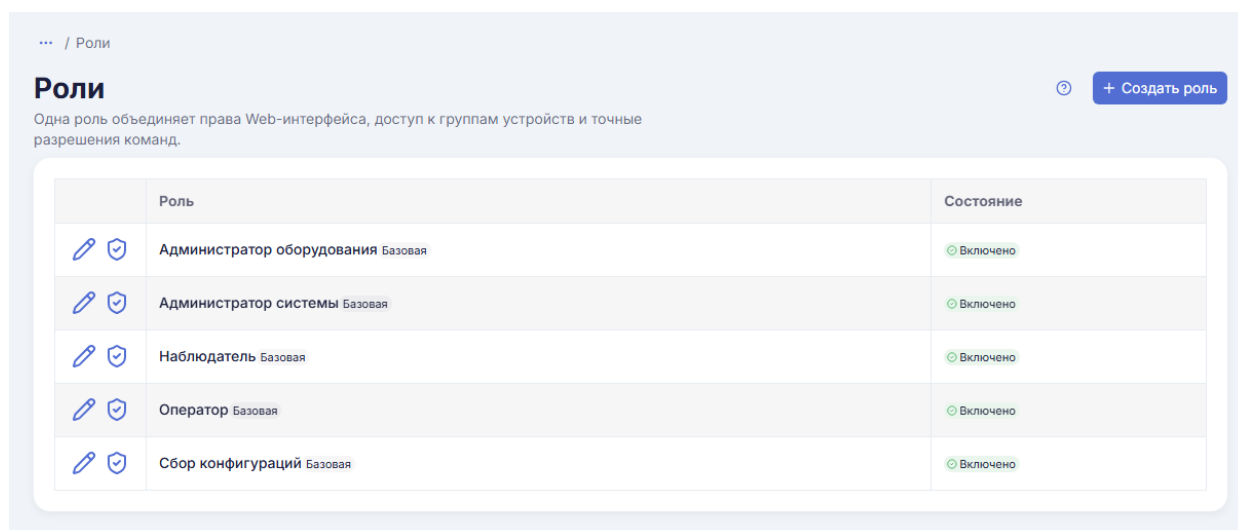
|                                                                                                                                                                         | Провайдер                                                                                                    | Адреса LDAPS         | Назначения ролей |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|----------------------|------------------|
|   | Стенд — Active Directory  | ldaps://stand-dc:636 | 3                |

### 13.3. Роли

После установки в системе есть пять базовых ролей:

| Роль                       | Назначение                                                                                     |
|----------------------------|------------------------------------------------------------------------------------------------|
| Администратор системы      | Полное управление SimpleNMS                                                                    |
| Администратор оборудования | Управление устройствами и выполнение команд на них                                             |
| Оператор                   | Сбор и просмотр конфигураций                                                                   |
| Наблюдатель                | Только просмотр                                                                                |
| Сбор конфигураций          | Техническая роль для учётной записи, под которой SimpleNMS собирает конфигурации через TACACS+ |

Роли доступны в разделе «Настройки» → «Роли». Базовые роли можно переименовывать и изменять их права, но нельзя удалять. Права роли задаются в области «Система» либо для отдельной группы устройств.



### 13.4. Назначение ролей группам каталога

Пользователи получают роли по членству в группах каталога. Для назначения:

1. На панели слева выберите раздел «Настройки» → «LDAP-провайдеры» и откройте провайдера.
2. В блоке «Назначения ролей» нажмите «Добавить назначение».
3. Найдите группу каталога по названию и выберите её.
4. В поле «Роль SimpleNMS» выберите роль.
5. Сохраните изменения.

Пример распределения:

| Группа каталога          | Роль SimpleNMS             |
|--------------------------|----------------------------|
| SimpleNMS-Network-Admins | Администратор оборудования |
| SimpleNMS-Operators      | Оператор                   |
| SimpleNMS-Viewers        | Наблюдатель                |

Роли применяются при входе пользователя; отдельно заводить пользователей в SimpleNMS не требуется. Индивидуальные назначения ролей конкретным пользователям выполняются в разделе «Настройки» → «Пользователи».

## 14. Контроль команд TACACS+/HWTACACS

### 14.1. Принцип работы

При включённом TACACS+ устройство передаёт SimpleNMS каждую команду администратора до её выполнения и получает решение: разрешить или запретить. Решение принимается по ролям администратора и группе устройства. Действует принцип «запрещено всё, что не разрешено явно». Все команды, сессии и попытки входа записываются в журнал аудита.

Для работы контроля команд должны быть выполнены следующие условия:

1. Настроен провайдер каталога с успешной проверкой подключения (раздел 13.2).
2. Группам каталога назначены роли SimpleNMS (раздел 13.4).
3. Для роли в группе устройств заданы разрешения команд (раздел 14.2).
4. В настройках устройства включён TACACS+ и задан общий секрет (раздел 14.3).
5. На самом устройстве настроено обращение к SimpleNMS по TACACS+ (раздел 14.5).

### 14.2. Разрешения команд

Разрешение выдаётся роли для конкретной группы устройств. Для добавления разрешения:

1. На панели слева выберите раздел «Настройки» → «TACACS+ / HWTACACS», вкладка «Разрешения команд».
2. Нажмите кнопку «Добавить разрешение» в правой верхней части экрана.
3. Укажите необходимые данные:
  - **Роль** – роль, которой выдаётся разрешение;
  - **Группа устройств** – группа, в которой действует разрешение;
  - **Точная команда** – имя команды – первое слово командной строки;
  - **Аргументы по порядку** – остальные слова командной строки;
  - **Влияние** – «Только чтение» или «Изменяющая» – характер команды для журнала и правил;
  - **Комментарий** – пояснение для администраторов.
4. Сохраните изменения.

... / TACACS+ / HWTACACS

## TACACS+ / HWTACACS и контроль команд

Точные разрешения для системных ролей и состояние TACACS-настроек устройств.

Разрешения команд
Устройства

Команда

Роль

Группа устройств

Политика

|                                                                                                         |                            |           |                                                                                                   |
|---------------------------------------------------------------------------------------------------------|----------------------------|-----------|---------------------------------------------------------------------------------------------------|
|  show · running-config | Администратор оборудования | Ядро сети | Только чтение  |
|  show · version        | Администратор оборудования | Ядро сети | Только чтение  |
|  terminal · length 0   | Администратор оборудования | Ядро сети | Только чтение  |

+ Добавить разрешение

**Важно.** Команда и аргументы сопоставляются точно. Команда `show version` – это имя `show` и аргумент `version`; разрешение на `show` без аргументов не разрешает `show version`.

Для сбора конфигураций через TACACS+ роли «Сбор конфигураций» (или роли учётной записи профиля доступа) необходим минимальный набор команд драйвера устройства. Для Cisco IOS это `terminal length 0`, `show version` и `show running-config`.

### 14.3. Настройка TACACS+ для устройства

- Откройте карточку устройства, вкладку «Подключение», блок «TACACS-настройка устройства». Тот же блок доступен на шаге «Итог» мастера подключения.
- Укажите необходимые данные:
  - Исходный IP-адрес** – точный адрес, с которого устройство обращается к SimpleNMS. Это не адрес SimpleNMS и не обязательно адрес управления устройством;
  - Протокол** – Cisco TACACS+ либо Huawei HWTACACS;
  - Общий секрет** – ключ, одинаковый в SimpleNMS и на устройстве, длиной не менее 32 символов; после сохранения не отображается;
  - Состояние** – «Активна» – TACACS+ для устройства включён.
- Нажмите «Сохранить TACACS-настройку».

**Важно.** Общий секрет короче 32 символов отклоняется без пояснения причины. При смене секрета одинаковое новое значение указывается и в SimpleNMS, и на устройстве.

### 14.4. Режимы «Только аудит» и «Контроль»

Режим задаётся для группы устройств (раздел 8.2) и определяет, что происходит с командой, на которую нет разрешения:

| Режим        | Команда без разрешения  | Запись в журнале                  |
|--------------|-------------------------|-----------------------------------|
| Только аудит | Выполняется             | Нарушение с вердиктом «разрешено» |
| Контроль     | Отклоняется устройством | Отказ с вердиктом «запрещено»     |

Рекомендуемый порядок внедрения:

- Включите TACACS+ на устройствах группы в режиме «Только аудит».

2. В течение контрольного периода просматривайте журнал команд и дополняйте разрешения командами, которые администраторы действительно используют.
3. Убедитесь, что для сервисной учётной записи разрешены команды сбора конфигурации.
4. Проверьте аварийный доступ к устройствам в обход TACACS+ (консоль или локальная учётная запись).
5. Переведите группу в режим «Контроль» в разделе «Настройки» → «Группы устройств».

**Важно.** Режим «Контроль» действует только для устройств, прошедших квалификацию на него; она подтверждается первой успешной сессией в режиме «Только аудит». Повторное определение устройства – например, после смены его SSH host key – квалификацию сбрасывает, и в группе с режимом «Контроль» такое устройство перестаёт принимать администраторов и отдавать конфигурацию, а в журнале ошибок доступа записей не появляется. В этом случае переведите группу в «Только аудит», дождитесь успешной сессии и верните «Контроль».

## 14.5. Настройка устройства

На устройстве настраивается обращение к SimpleNMS как к серверу TACACS+ по адресу SimpleNMS и порту TCP/49 с тем же общим секретом. Команды зависят от вендора и приведены в его документации. Пример для Cisco IOS:

```
aaa new-model
tacacs server SIMPLENMS
  address ipv4 <адрес SimpleNMS>
  key <общий секрет>
aaa group server tacacs+ SIMPLENMS-GROUP
  server name SIMPLENMS
aaa authentication login default group SIMPLENMS-GROUP local
aaa authorization exec default group SIMPLENMS-GROUP local
aaa authorization commands 15 default group SIMPLENMS-GROUP local
aaa accounting commands 15 default start-stop group SIMPLENMS-GROUP
ip tacacs source-interface <интерфейс с исходным IP-адресом>
```

**Важно.** Сохраняйте локальную учётную запись как резервный способ входа (local в конце списка методов) и проверяйте доступ через консоль до отключения от текущей сессии. Первую настройку выполняйте при наличии консольного доступа к устройству.

## 15. Журнал аудита

Раздел «Аудит» объединяет команды администраторов, административные сессии и ошибки доступа. Для просмотра на панели слева выберите раздел «Аудит».

### 15.1. Команды

Вкладка «Команды» показывает каждую команду, переданную устройством на проверку: администратора и время, устройство, команду и результат. Результат отображается двумя значками: режим группы – щит для режима «Контроль» и глаз для режима «Только аудит» – и вердикт: зелёный – разрешено, красный – запрещено. Доступны поиск по администратору и фильтры по устройству, периоду и результату.



## 15.3. Ошибки доступа

Вкладка «Ошибки доступа» показывает неуспешные попытки входа на устройства через TACACS+: имя пользователя, время, устройство, адрес источника и код причины, например INVALID\_CREDENTIALS – неверный пароль или несуществующий пользователь.

### Журнал аудита

Команды, сессии администраторов и ошибки доступа.

Команды Сессии Ошибки доступа

Фильтры

|   | Администратор  | Время                | Устройство     | Источник      | Причина               |
|---|----------------|----------------------|----------------|---------------|-----------------------|
| ⊕ | ivanov-unknown | 18.09.2026, 18:43:51 | core-sw-msk-01 | 198.51.100.20 | ⊕ INVALID_CREDENTIALS |
| ⊕ | orlov          | 18.09.2026, 18:43:50 | core-sw-msk-01 | 198.51.100.20 | ⊕ INVALID_CREDENTIALS |

Успешный вход на устройство не означает права на выполнение команд: администратор, роль которого не имеет разрешений в группе устройства, войдёт на устройство, но его команды будут отклонены и отражены на вкладке «Команды».

## 16. Информация о разработчике

Программа для ЭВМ «SimpleNMS»

ООО «ОРБСОФТ»

Россия, Москва, р-н Троицк, д. Станиславль, 13

Телефон: (495) 150-80-59

E-mail: [info@orbsoft.ru](mailto:info@orbsoft.ru)