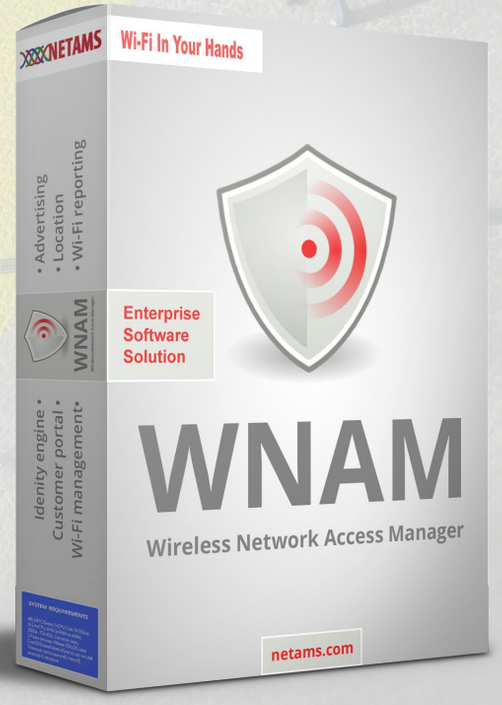
Корпоративная авторизация в проводных и беспроводных сетях

Ваша сеть В ВАШИХ РУКАХ

www.netams.com info@netams.com +7 (499) 346-76-60

О компании «Нетамс»

- Программное обеспечение и оборудование для сетей
- Работаем с 2008 года
- 13 лет опыта внедрения системы авторизации WNAM
- + новый продукт каждый год
- 250+ клиентов:
  - операторы связи
  - частный бизнес | банки | нефтяные компании | IT
  - государственные организации
- Служба технической поддержки
- Сеть партнеров



NETAMS

Наши клиенты

Ростелеком

ТТК

orange Business Services

UZTELECOM

ГЭС-2

Яндекс

FIFA WORLD CUP RUSSIA 2018

Т БАНК

РСХБ

Sk Сколково

2ГИС

ЛСР

ТАТТЕЛЕКОМ

ВТБ

cloud.ru

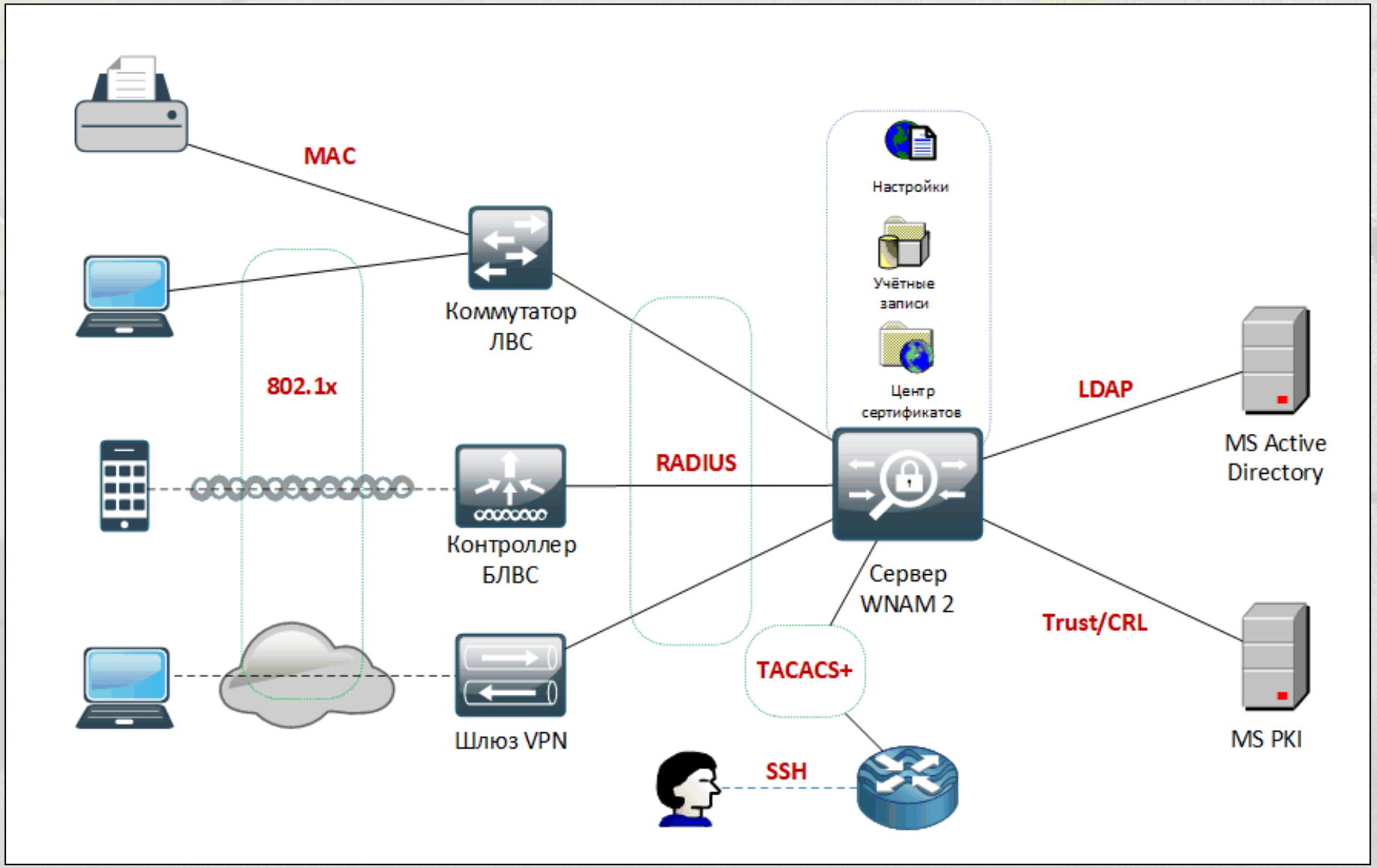
Для вашей сети

Собственные решения компании «Нетамс»

- Локальная разработка | ФИПС | Реестр Минцифры
- On-premises установка «без облаков»
- Бессрочная лицензия | Поддержка

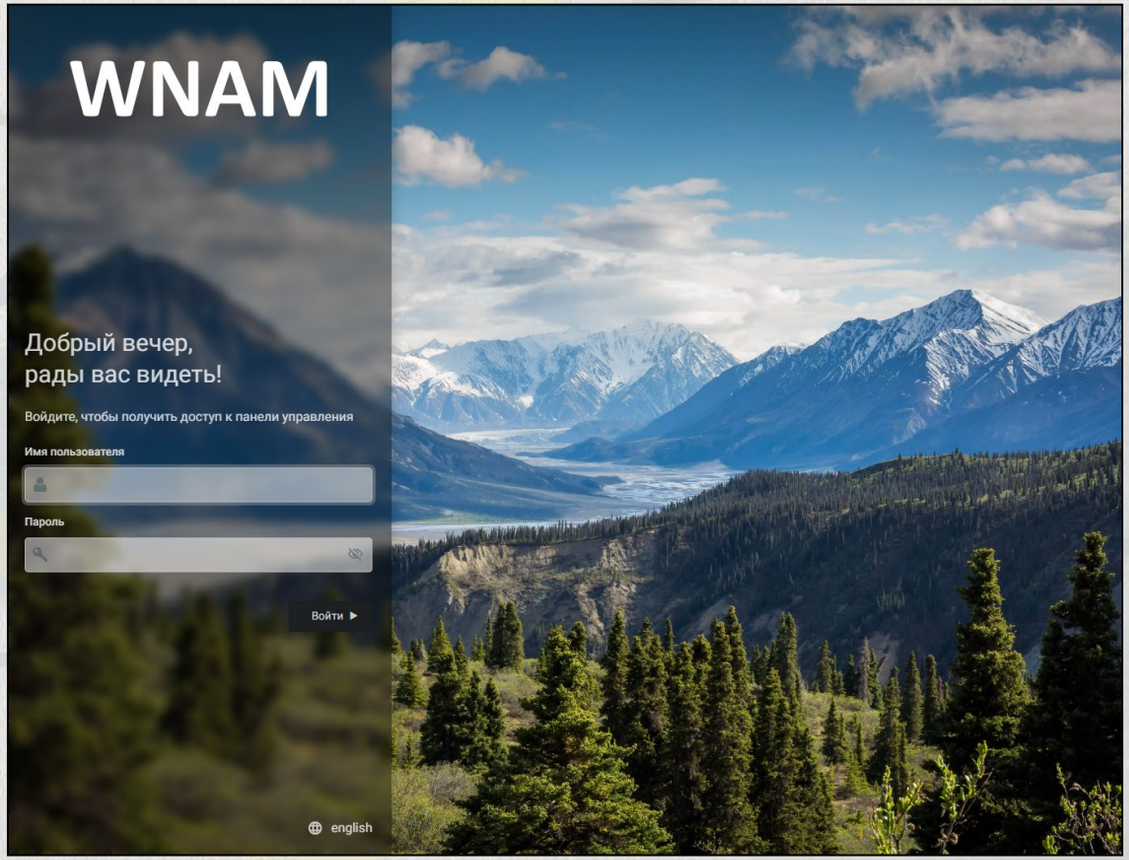
1. Гостевой беспроводной доступ
   - ✓ WNAM (Wireless Network Access Manager)
2. Корпоративная авторизация
   - ✓ Дополнительный модуль для WNAM 1.6
   - ✓ **Новая Система сетевой авторизации WNAM 2**
3. Контроль качества Wi-Fi
   - ✓ WNAM Quality of Wireless
4. Контроллер беспроводных точек доступа Wi-Fi
   - ✓ WiCo

Архитектура корпоративной авторизации



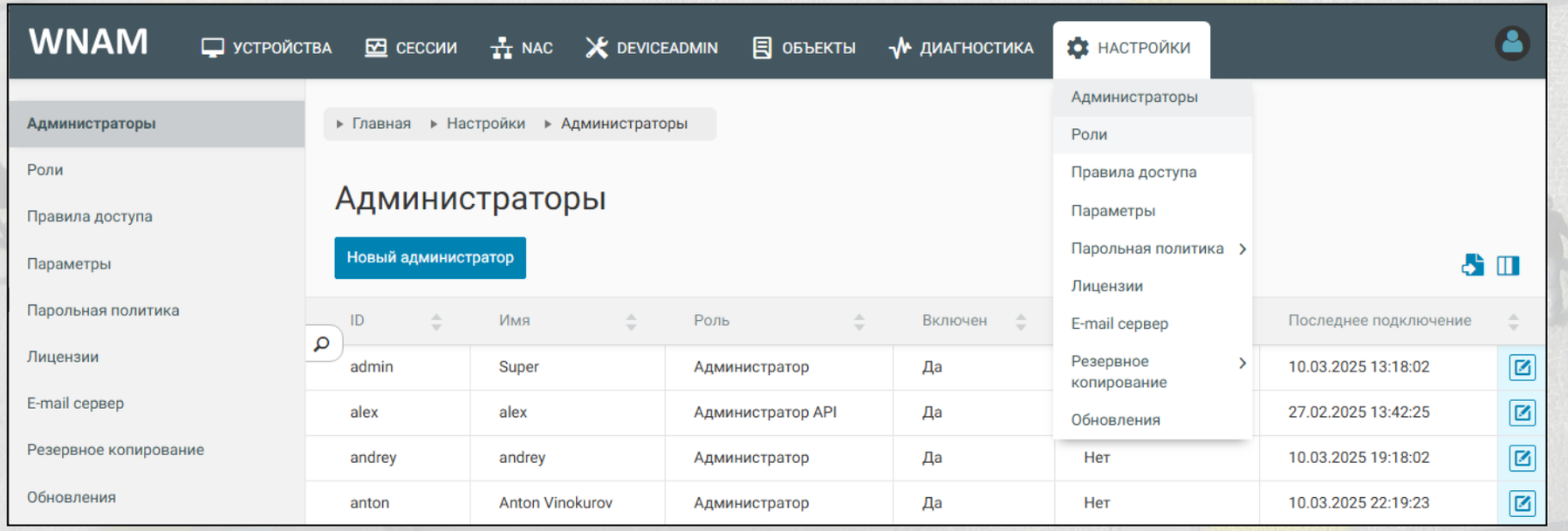
Корпоративная авторизация WNAM

- Контроль доступа
  - В закрытых сетях Wi-Fi
  - Проводных подключений к ЛВС
  - VPN подключений
  - Администраторов к оборудованию
- Собственный RADIUS-сервер
  - Поддержка MAC bypass (MAB)
  - Поддержка EAP-TLS и EAP-PEAP/MSCHAPv2
- Гибкая система конфигурации через браузер
- Отказоустойчивость и кластеризация
- Диагностика и траблшутинг
- Российское ПО для Linux, в Реестре Минцифры



Альтернатива проприетарным Cisco ISE/ACS,
Microsoft NPS, Aruba ClearPass, Ruckus Cloudpath
Альтернатива опенсорсу FreeRADIUS/PacketFence/tac_plus

Удобство управления



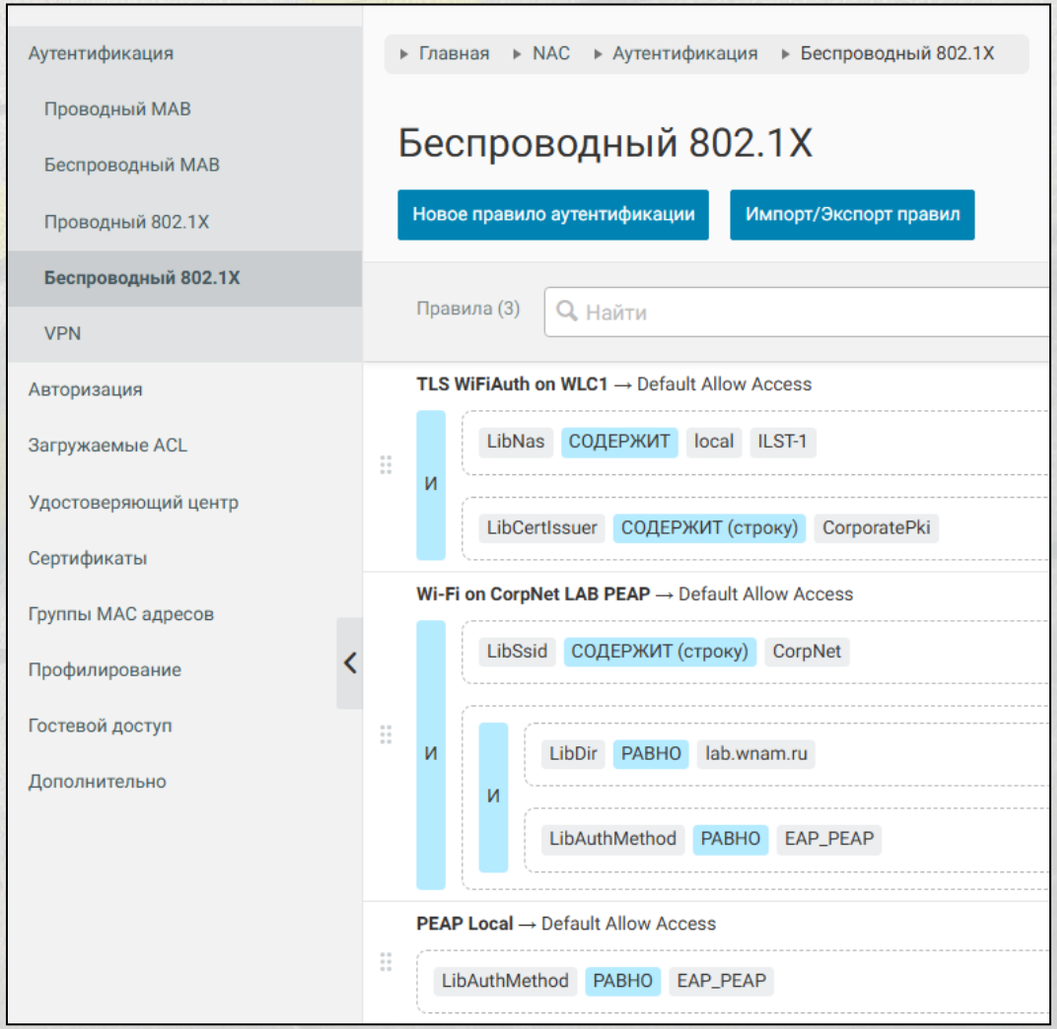
- Центральный дашборд – сводка всего, что происходит. Виджеты
- Устройства (клиенты, эндпоинты) и их сессии подключений (RADIUS, TACACS+)
- Функции NAC – сетевой авторизации: правила, сертификаты, ACL и профайлер
- Функции DeviceAdmin – авторизации администраторов: учётки, правила, группы, наборы команд
- Общесистемные объекты: NAS, категории, службы каталога, уведомления
- Диагностика: аудит, события, алерты, статус нод кластера
- Общие настройки: лицензии, обновления, парольные политики, доступ в UI

Сетевой доступ: модель правил

- Разделение на 5 возможных типов RADIUS
- Гибкий конструктор правил с логическими выражениями
- Проверка источника и способа подключения
- Проверка «личности» подключающегося:
  - Локальная база данных
  - Взаимодействие с PKI
    - Действительность сертификата
    - Поля в сертификате
  - Взаимодействие со службами каталога
    - Проверка хэша пароля
    - Членство в группах и OU
    - LDAP-атрибуты
- Проверка результатов профилирования
- История прошлых подключений

Выбирается наиболее подходящий профиль

- Применяется связанное правило авторизации

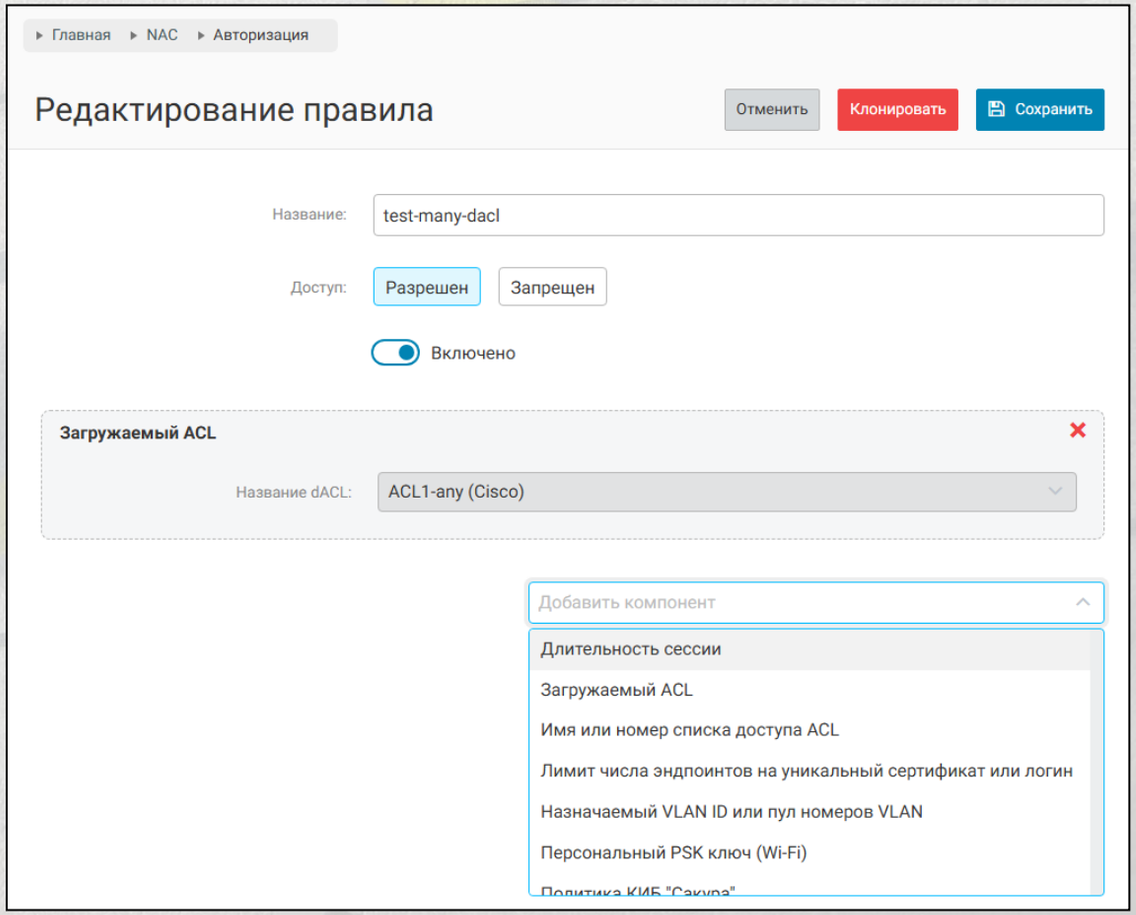


Сетевой доступ: авторизация

- Вернуть сетевому оборудованию:
  - Номер VLAN
  - Фильтр
  - Загружаемый ACL
  - Ограничения доступа
  - Редирект на портал самообслуживания
  - Произвольные RADIUS-атрибуты
- Формирование профиля эндпоинта
- Проверка статуса защищенности APM («Сакура»)
- Запрос второго фактора
- Протоколирование события авторизации (+SIEM)

Применяется наиболее подходящий профиль

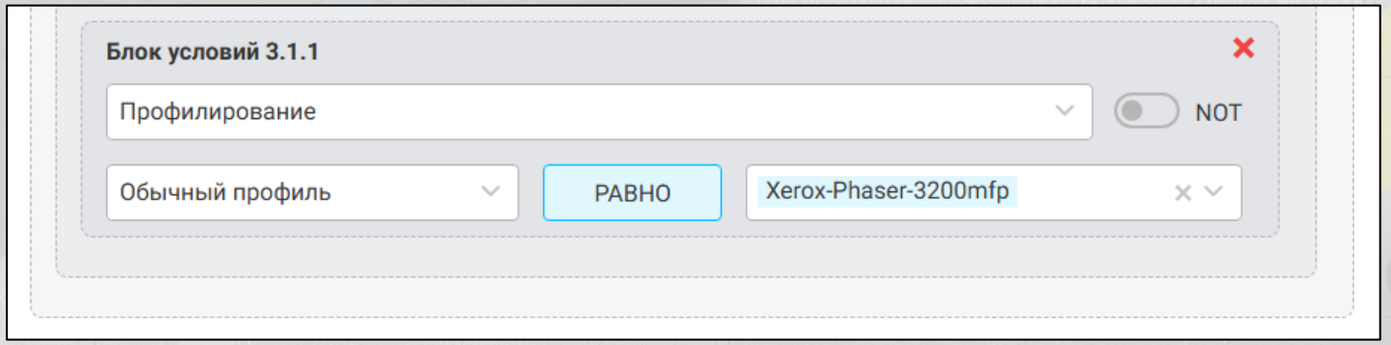
- Параметризация (конкретный VLAN ID)
- По умолчанию: отказ в доступе

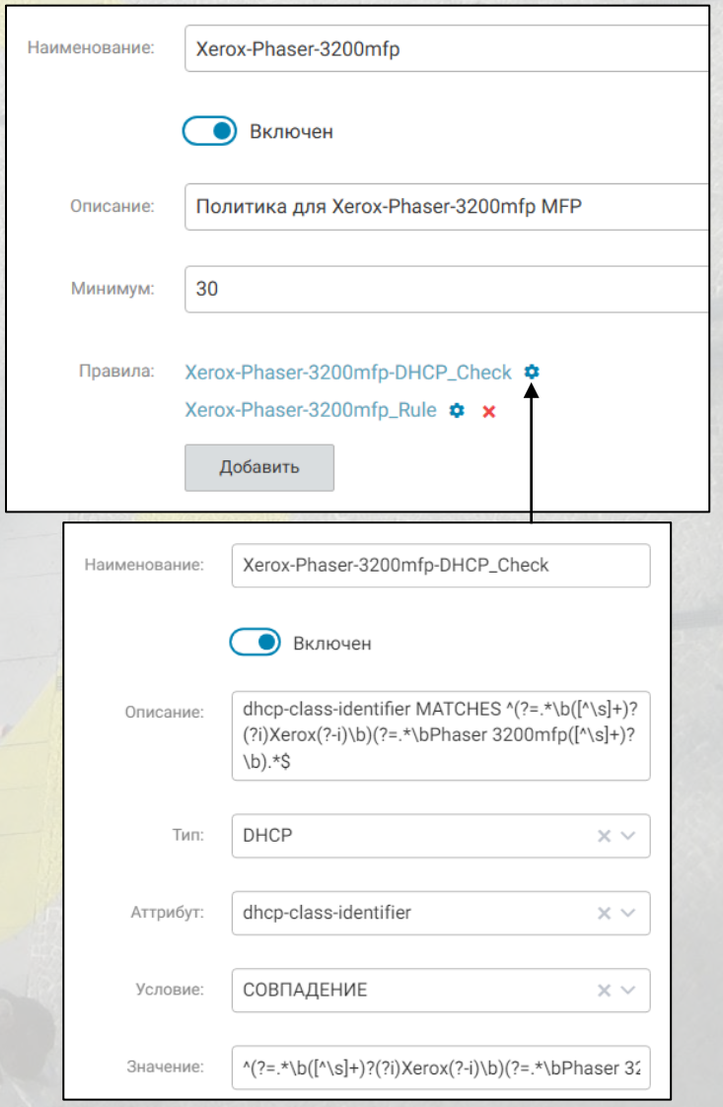


Профилирование устройств

- Работает при MAC-авторизации (MAB)
- Применяется в правилах аутентификации
- Источники данных:
  - По вендорам, по таблицам MAC адресов
  - DHCP, CDP, LLDP данные от Cisco Device Sensor
  - SNMP опрос коммутаторов
  - Анализ DHCP Options запроса клиента Linux-агентом
- CoA (сброс порта) при смене профиля, помещение в карантин

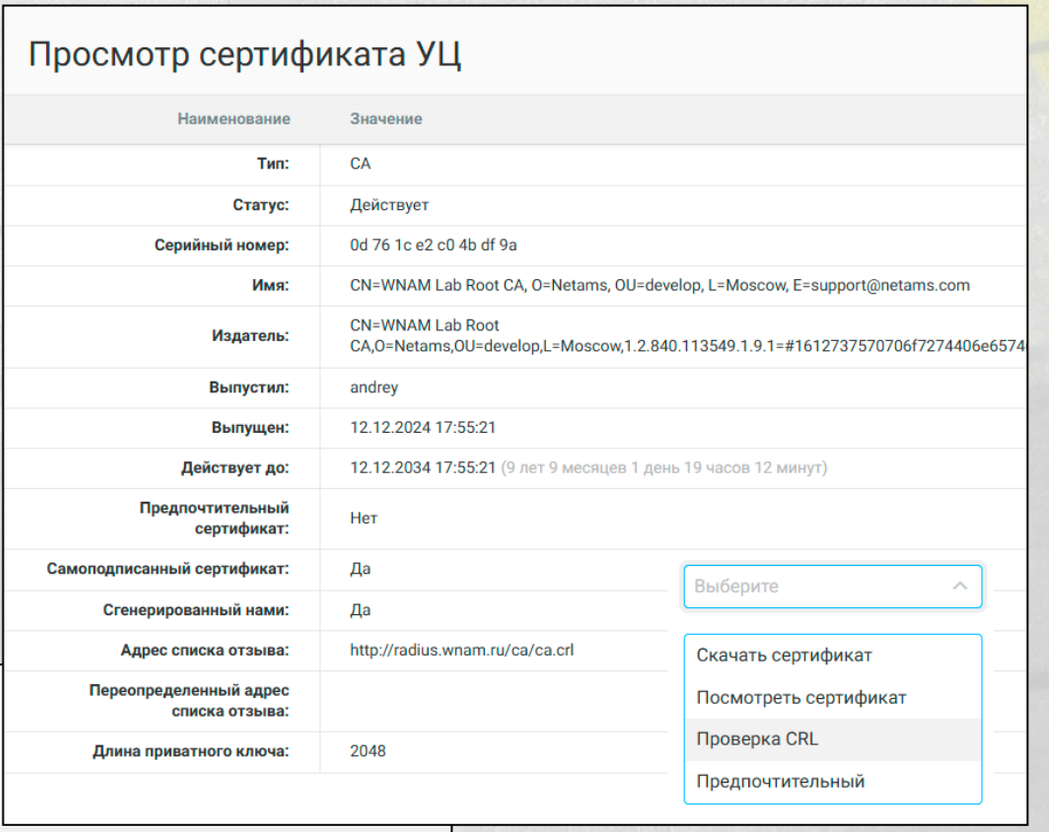
1000+ встроенных правил, можно создавать свои

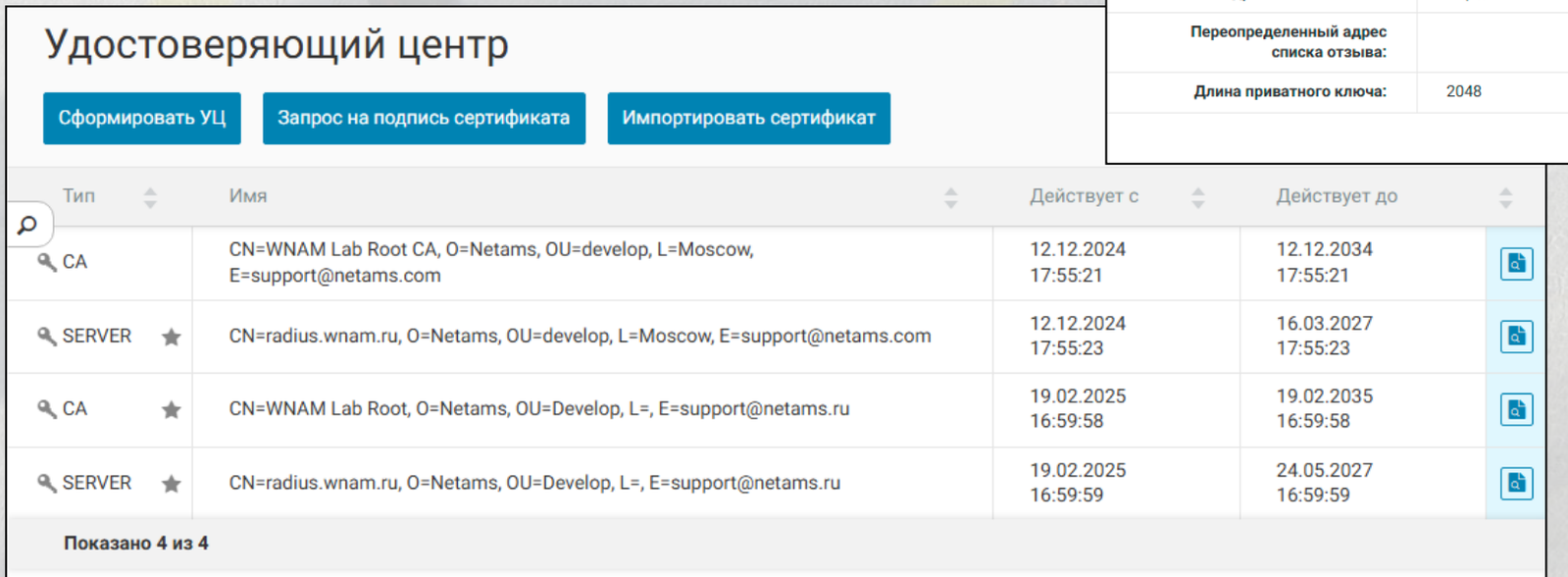




Работа с сертификатами

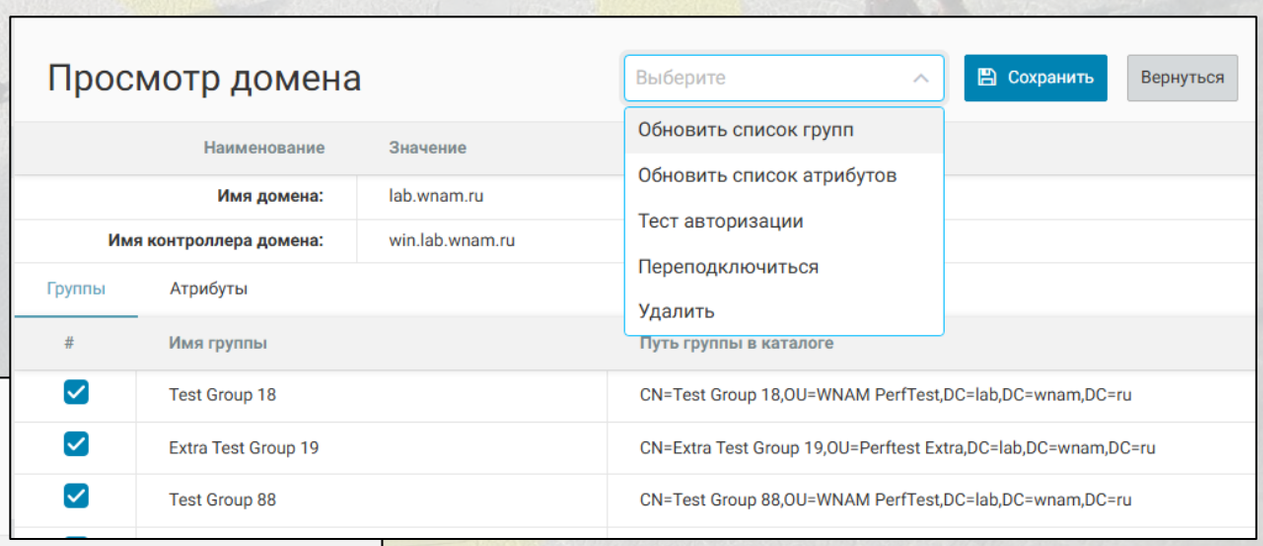
- Встроенный корневой УЦ
- Подчиненные сертификаты от УЦ вашего предприятия (PKI)
- Запрос на подпись сертификата CSR в вашем УЦ
- Проверка списков отзыва
- Для работы RADIUS-сервера WNAM (802.1X)
- Формирование клиентских сертификатов доступа
- Аутентификация и авторизация по EAP-TLS

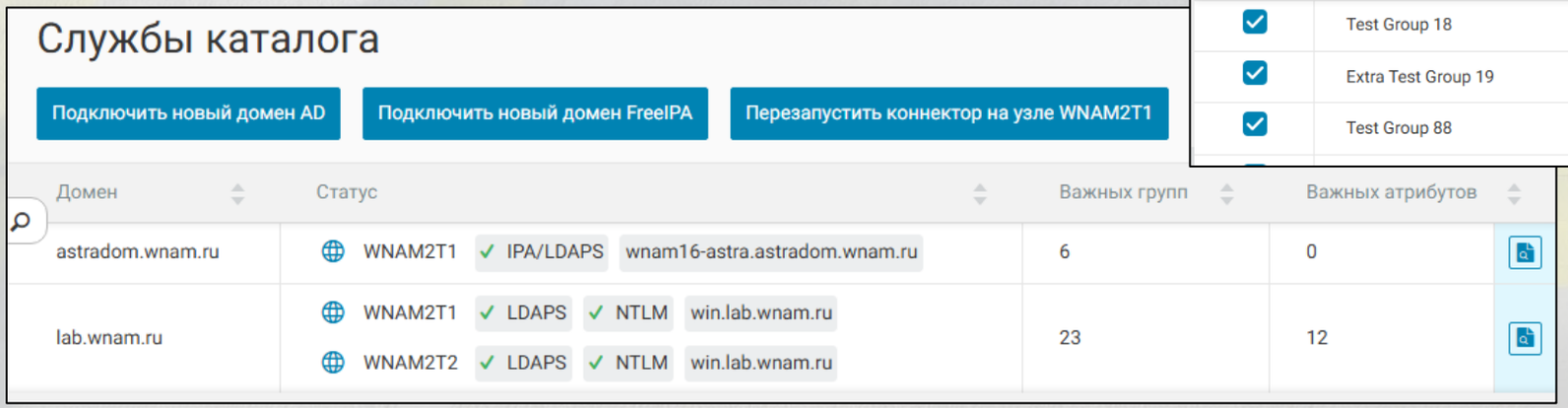




Взаимодействие со службами каталога

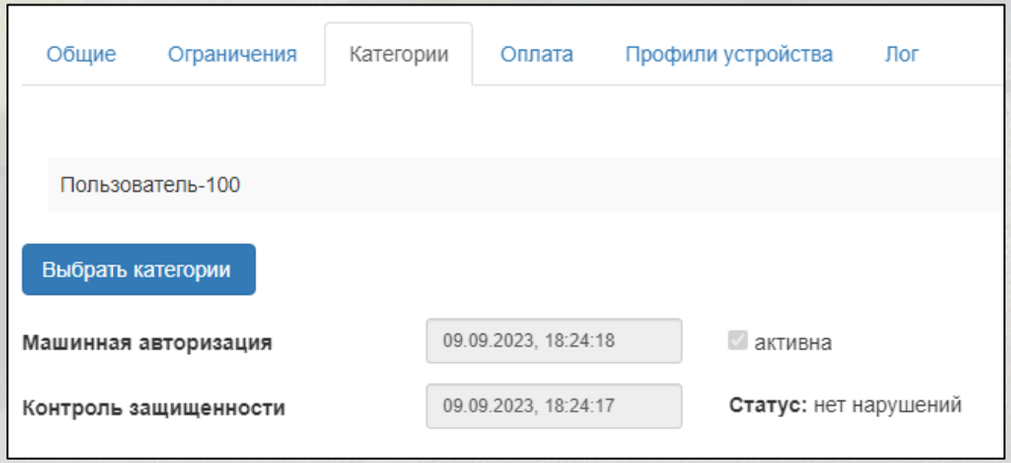
- MS Active Directory, FreeIPA (ALD Pro), ALT Домен
- Получение списка групп и атрибутов. Установка «важных» вам.
- Проверка групп и атрибутов учетной записи в момент авторизации
- Вложенные группы
- EAP-PEAP/MSCHAPv2
- NTLM-проверка пароля
- Мульти-домен
- Кластерная конфигурация

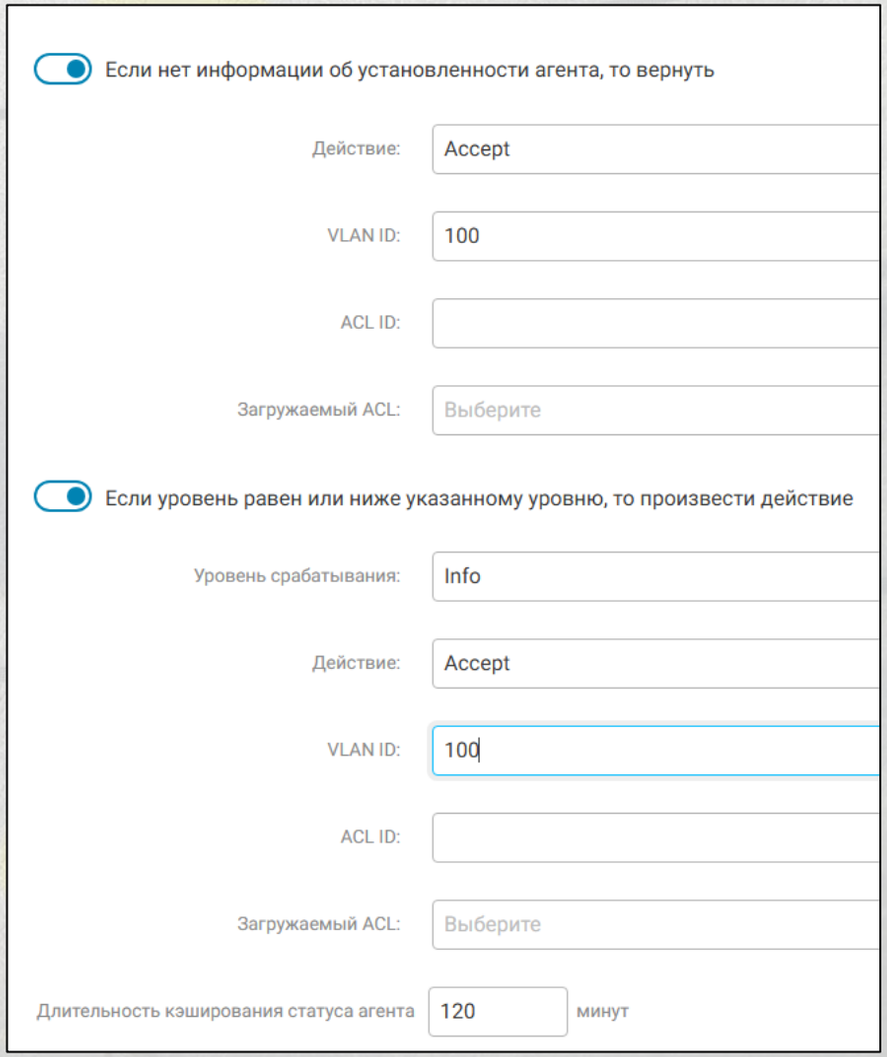




Контроль защищенности АРМ

- Проверка наличия антивируса, обновлений, процессов
- Замена Cisco Anyconnect Posture
- КИБ «Сакура» от IT Expertise. Windows, Mac, Linux
- Сервер «Сакура» контролирует агентов
- Изменение статуса агента направляется на WNAM
- Статус защищенности эндпоинта (IP, MAC)
- Отправка команды переавторизации порта. RADIUS CoA.
- Назначение карантинных VLAN, ACL, dACL
- «Излечение эндпоинта» - повторение процесса. Целевой VLAN.



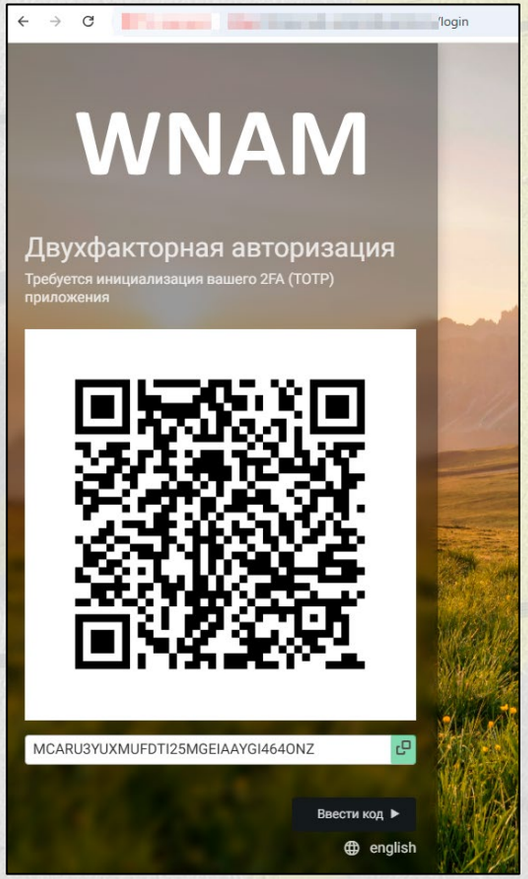


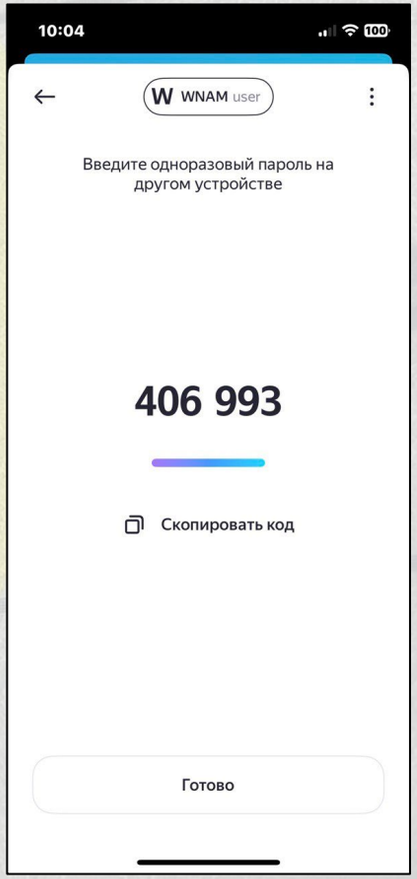
Двухфакторная авторизация

- Защита административного доступа к UI
- VPN авторизация

- Провайдеры:
  - Multifactor (RADIUS)
  - MFASOFT (API)
  - Собственный, встроенный

В планах:
- TACACS+ подключения
- 802.1X
  - Push в 2FA-приложение
  - Редирект на портал, TOTP код

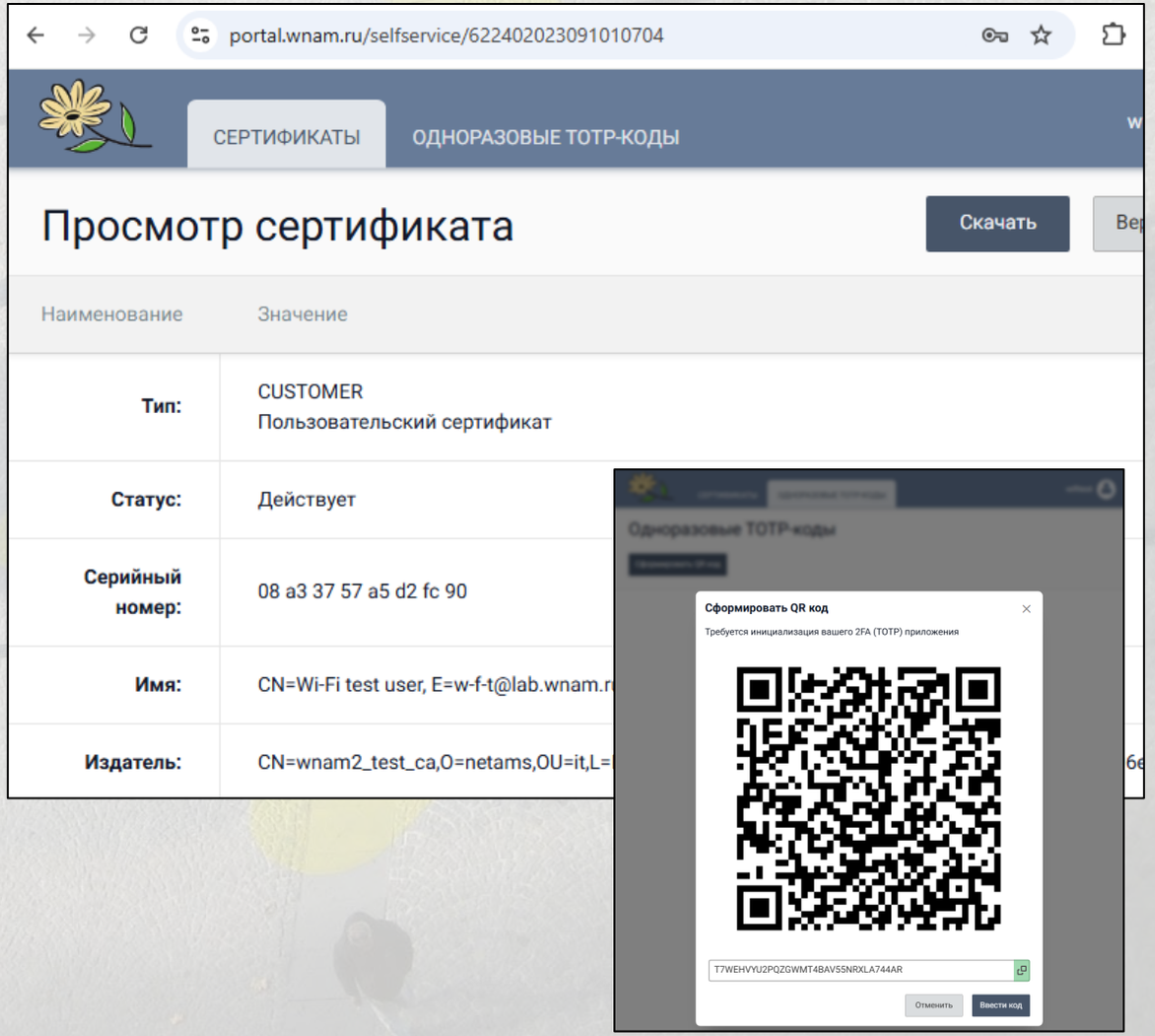




Самообслуживание

- Ссылка с корпоративного портала предприятия
- Редирект при Wi-Fi подключении (онбоардинг)
  https://wnam2.corp.int/selfservice

- Формирование и выгрузка
  сертификата для EAP-TLS через:
  - Встроенный УЦ
  - Внешний УЦ предприятия (MS, SCEP)
- Инициализация 2FA-приложения
- Согласие с условиями доступа к сети

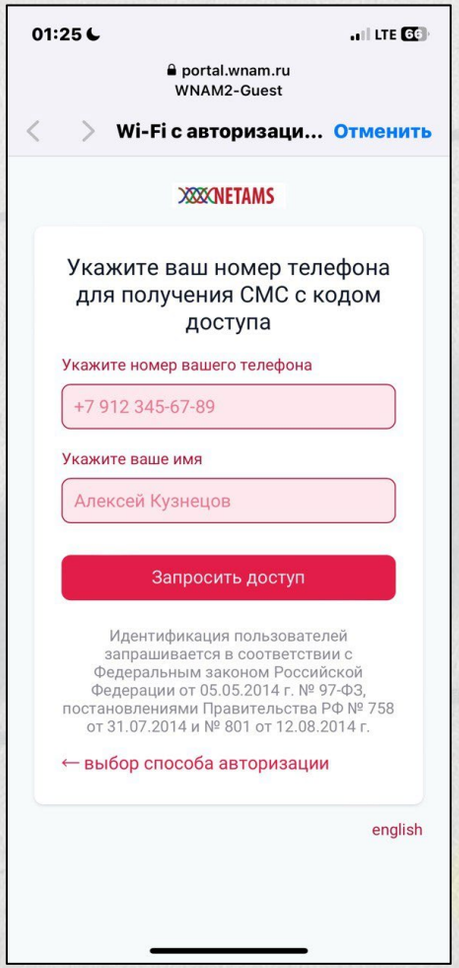


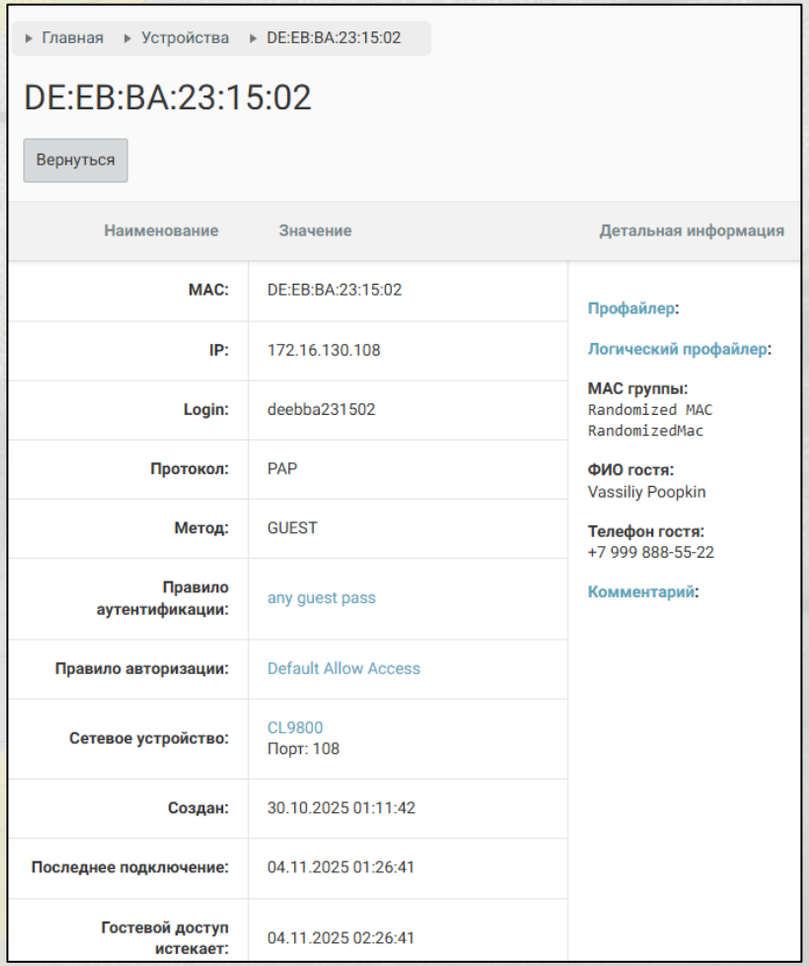
Гостевой доступ Wi-Fi

- Подтверждение спонсором
- Звонок на платформу (SIP)
- Отправка СМС-кода (HTTP, script)
- Ввод кода ваучера
- Ввод логина и пароля
  - Локальные учетные записи
  - Из домена, по группе

- Русский и английский языки
- Опционально: запрос ФИО

- Cisco WLC, 9800-CL
- Huawei (RADIUS, CMPP)
- Mikrotik
- Unifi





Гостевые эндпоинты не занимают лицензий!

Траблшутинг

- Детальный лог подключения
  - Атрибуты запроса
- Ход всех проверок и запросов
- Совпавшие правила и профили
- Применённые атрибуты ACL, VLAN
- Аккаунтинг трафика

- Причина отказа в подключении

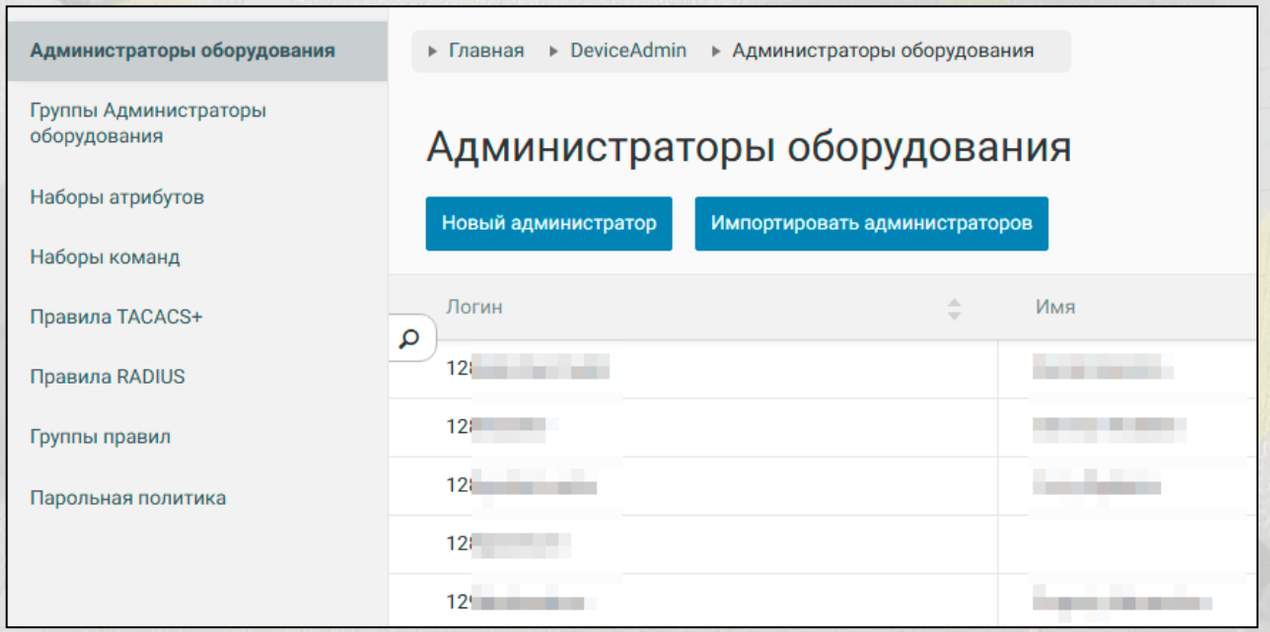
Наименование	Значение	Детальная информация
IP	172.16.137.252	+-23 ms: **fillFromRadiusAttributes** password: present in request +0 ms: **fillFromRadiusAttributes** ap: '38:1C:1A:C0:CD:92', ssid: '' +1 ms: **fillFromRadiusAttributes** identity: '44d1faef2211', portType: EthernetMAB +0 ms: **fillFromRadiusAttributes** mac: '44:D1:FA:EF:22:11' +1 ms: **fillFromRadiusAttributes** session id: 'AC10890800002869A221FF7C' +0 ms: **radius** received 17 attributes in the request: Service-Type = Call-Check EAP-Key-Name = NAS-IP-Address = 172.16.137.8 NAS-Port-Id = GigabitEthernet1/0/18 NAS-Port-Type = Ethernet Framed-MTU = 1500 User-Name = 44d1faef2211 Cisco-AVPair-method = mab Calling-Station-Id = 44-D1-FA-EF-22-11 User-Password = ******** Cisco-AVPair-service-type = Call Check Cisco-AVPair-audit-session-id = AC10890800002869A221FF7C Framed-IP-Address = 172.16.137.252 Message-Authenticator = 0xe6350fd88ed7ea6fee83d112770de6 Called-Station-Id = 38-1C-1A-C0-CD-92 Unknown-Sub-Attribute-2 = 0x476967616269744574686572 6e65 NAS-Port = 50118 +2 ms: **fillFromRadiusAttributes** nas: 'Cisco d20', ip: 172.16.137.8, id: 67c58f863dfee823b89f +16 ms: **authentication** final result: Allow with policy 'test4' and authorization 'P +2 ms: **radius** send RADIUS ACCEPT with 1 attributes +1 ms: **radius** attribute: Message-Authenticator = 0x0bbc3aadecff40eb17b
MAC	44:D1:FA:EF:22:11	
Логин	44d1faef2211	
Узел кластера	stress-test-wnam.lab.wnam.ru	
Длительность аутентификации	24 мс. (10.03.2025 19:14:51.758 — 10.03.2025 19:14:51.782)	
Сетевое устройство	Cisco d20	
Правило аутентификации	test4	
Правило авторизации	Разрешить	
Успех	Да	

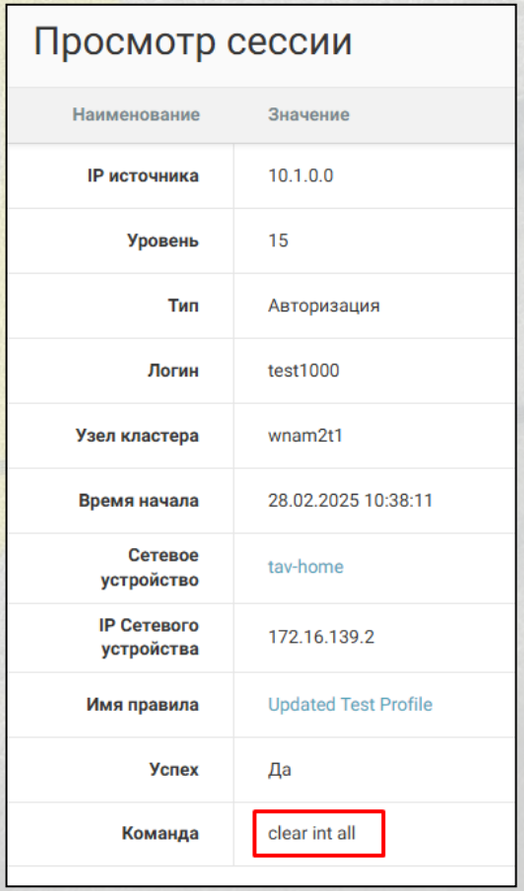
Сессии RADIUS

Время начала	MAC	IP	Логин	Сетевое устройство	Метод	Успех			
10.03.2025 19:14:51	44:D1:FA:EF:22:11	172.16.137.252	44d1faef2211	Cisco d20	PAP	✓			
10.03.2025 19:14:49	44:D1:FA:EF:22:11	172.16.137.252	44d1faef2211	Cisco d20	PAP	✓	test4	Разрешить	10 19
10.03.2025 16:22:17	44:D1:FA:EF:22:11	172.16.137.252	44d1faef2211	Cisco d20	PAP	✓	test4	Разрешить	10 16

Контроль авторизаций администраторов: TACACS+

- Авторизация доступа к сетевому оборудованию (также RADIUS)
- Локальная база учётных записей, групп, или пользователи служб каталога
- Примененные атрибуты и ограничения
- Разрешенные и запрещенные команды и их группы
- Лог набранных администратором команд
- Поиск «кто это сделал?»





Отказоустойчивость

- Поддержка кластерной конфигурации
- Репликация данных (брокер)
- Поддержка гео-распределенной конфигурации

Работает под управлением ОС Linux, в том числе Astra Linux и RedOS

Поддерживается любая виртуализация

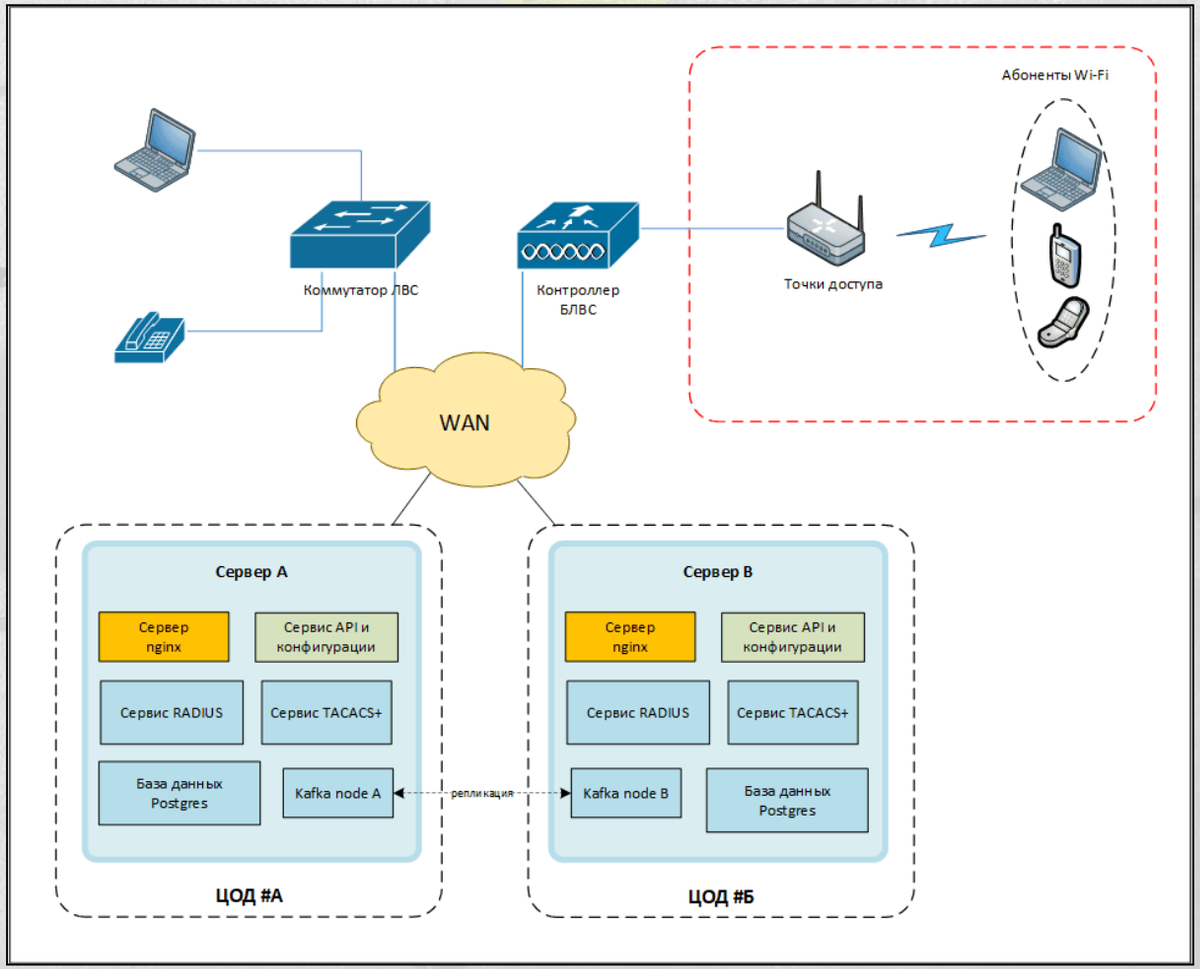
Поставляется в виде:

- Установочный ISO
- Образ VM

Установка подписанных обновлений

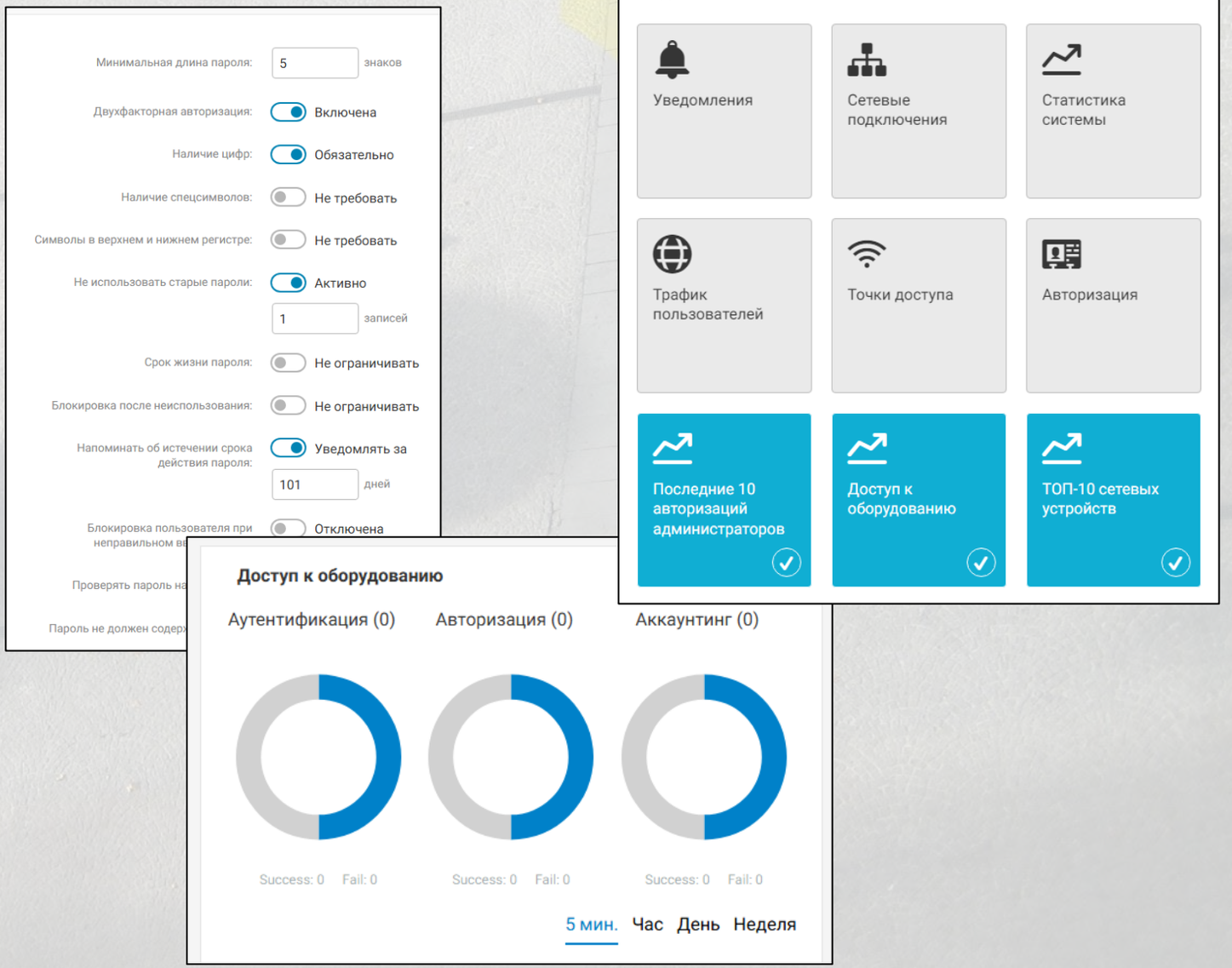
Лицензируется:

- Эндпоинты
- Управляемые устройства



Интерфейс

- Ролевая модель доступа в UI
- Доступ администраторов из домена
- 2FA для доступа в UI
- 4 парольные политики
- Дашборды и отчеты по типам авторизации, правилам и т.п.
- Аккаунтинг сессий и трафика
- Импорт из ISE:
  - Эндпоинты, их группы и профили
  - NAS и их категории
  - TACACS+ администраторы
- Экспорт данных в CSV
- Весь кластер управляем с любого узла
- Полное управление через API



Сравнение с аналогами

Cisco ISE

Чего у нас нет:

- SGT меток, TrustSEC
- FIPS Mode
- EAP-TEAP, TLS v1.3
- Posturing (средствами AnyConnect)
- MDM

Что у нас есть:

- Проверенный MAB/802.1X/TACACS+ с отечественными вендорами
- Контроль защищенности АРМ через интеграцию с КИБ «Сакура»
- Поддержка 2FA (отечественные решения, + доступ в UI)
- Расширенные опции карантина
- SNMP опрос оборудования
- Потенциал интеграции с различным гостевым Wi-Fi
- Возможность напрямую обратиться к вендору, а не отправить «тикет-в-Индию»

Сравнение с аналогами

Microsoft NPS

Чего у нас нет:

- Нативной поддержки взаимодействия с AD

Что у нас есть:

- Нормальные средства диагностики, статистики и отчетов
- Профайлер для MAB методов
- Гостевая авторизация
- BYOD
- TACACS+
- Кластерная конфигурация

Сравнение с аналогами

FreeRADIUS и PacketFence; tac_plus

Чего у нас нет:

- Бесплатной версии
- Рестарта сервиса на каждое изменение правил
- Необходимости лазить в CLI

Что у нас есть:

- Web GUI
- Нормальные средства настройки, диагностики, статистики
- Профайлер для MAB методов
- Гостевая авторизация
- BYOD
- TACACS+
- Кластерная конфигурация
- Мульти-доменное подключение к AD
- Техническая поддержка

Сравнение с аналогами

ГазИнформСервис «Efros Defense Operations»
Deck.Auth
AxelNAC
Eltex NAICE
Blazar NAC

- Наша система WNAM 2 ориентирована на решение сложных задач с особыми требованиями заказчиков к кластеризации, надежности, работе под высокой нагрузкой. Мы не «перекрашиваем опенсорс», а делаем всё сами «с нуля», детально разбираясь в тонкостях процессов авторизации.
- Мы реализуем десятки тонких настроек, специальных кейсов, недоступных в альтернативных системах.
- Наша система авторизации проверена установкой у десятков заказчиков.
- Обратитесь за деталями к нам.

Сравнение с аналогами

Deck.Auth

Чего у нас нет:

- Подписочной модели сервиса

Что у нас есть:

- Реально работающая поддержка кластерной конфигурации
- Мульти-домен
- TACACS+ сервер
- Бессрочная лицензия
- Настоящий профайлер для MAB, активный/пассивный контроль эндпоинтов

AxelNAC, Eltex NAICE, BlazarNAC

Чего у нас нет:

- Перевода на русский opensource-продуктов под капотом

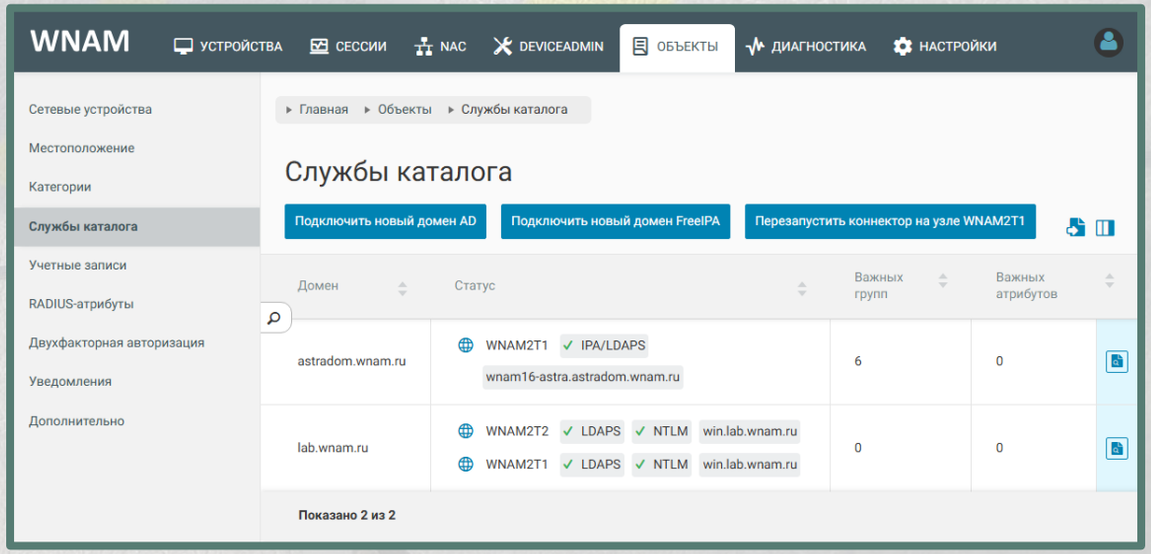
Что у нас есть:

- Мы понимаем, как всё работает внутри, так как написали каждую строчку кода сами. Эти системы основаны на опенсорсе FreeRADIUS/Packetfence, который архитектурно не подходит корпоративному заказчику (рестарты после изменения конфигурации, работа к кластере и т.п.)

Планы развития 2025/2026

Система управления сетевым доступом WNAM 2

- Зарегистрировано в ФИПС, в Реестре Минцифры (РПО): запись №26381 от 12.02.2025
- Первый релиз с поддержкой авторизации администраторов (DeviceAdmin): январь 2025.
- Релиз с поддержкой авторизации клиентов (NAC): 12 мая 2025.
- Текущий релиз: WNAM2-NAC-UPD2
- Выход релиза WNAM2-NAC-UPD3: ноябрь 2025
- Более 50 задач и подзадач в роадмапе
  (обратитесь за деталями к нам)



Дальше

Поддержка продаж, пуско-наладка и дальнейшее обслуживание ведется с привлечением авторизованных системных интеграторов

1. Запросите опросный лист, заполните его, получите оценку проекта
2. Запросите демо-ключ, подготовьте стенд
3. Разверните систему. Мы поможем с настройкой
4. Выполните проектирование и разработайте план миграции
5. Купите бессрочную лицензию WNAM 2
6. Внедрите систему на вашем предприятии

Техническая поддержка
- Работа по регламенту в соответствии с согласованным SLA

Доработки
- Оперативное устранение выявленных замечаний
- Расширение функционала системы по запросу заказчика

Оборудование и программное обеспечение компании «Нетамс»

Дополняет вашу сеть полезными сервисами

- Система управления сетевым доступом WNAM 2
  - 802.1X, MAB, TACACS+ доступ на основе политик
- Гостевая авторизация WNAM (Wireless Network Access Manager)
  - Полное соответствие требованиям законодательства
  - Реклама, статистика, опросы
- Сенсор качества Wi-Fi – WNAM Quality of Wireless
  - Проактивный мониторинг и контроль SLA
  - Инструменты для инженеров
- Контроллер точек доступа Wi-Fi для предприятий WiCo

На все продукты – бессрочная лицензия!

Всё запускается на ваших серверах, без облаков!

Узнать больше:

https://www.netams.com/corp_auth/

Запросить условия:

info@netams.com

+7 (499) 346-76-60