Документация Privileged Access Manager 3.0

Table of contents:

- Каталоги пользователей
- Администраторы ролей
- Аутентификация пользователей
- Сервер доступа
- Логирование
- События
- Резервная копия
- Установка PAM

- Основная на Linux
  - Запуск мастера
  - Сценарий
  - Схема хостов
  - Порты
  - Сертификаты
  - Базы данных
  - Хранилище данных
  - Каталоги пользователей
  - Администраторы ролей
  - Аутентификация пользователей
  - Сервер доступа
  - Логирование
  - События
  - Резервная копия
  - Установка PAM
- Отказоустойчивая на Windows
  - Запуск мастера
  - Сценарий
  - Схема хостов
  - Порты
  - Сертификаты
  - Базы данных
  - Хранилище данных
  - Каталоги пользователей
  - Администраторы ролей
  - Аутентификация пользователей
  - Сервер доступа
  - Логирование
  - События

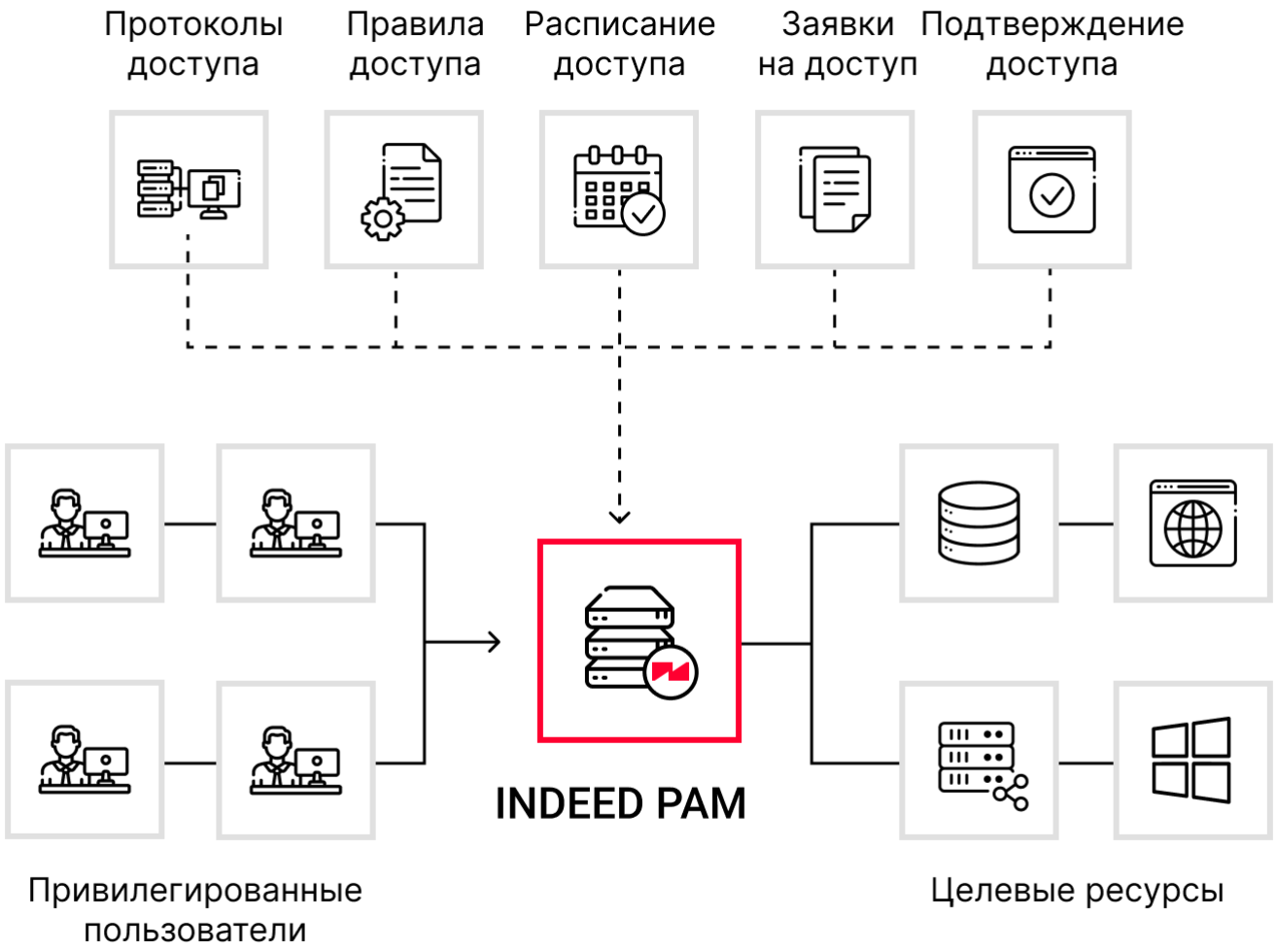
- Резервные учетные записи
- Шифрование паролей и секретов
  - Утилита на Windows
    - Снятие шифрования
    - Шифрование
  - Скрипт на Linux
    - Снятие шифрования
    - Шифрование
  - О механизме шифрования
- Фильтрация процессов и ФС
  - Запрет запуска процессов
  - Защита критичных файлов
- Шифрование материалов сессии
- Политики безопасности сервера доступа
  - Назначение прав пользователя
  - Параметры безопасности
    - Учетные записи
    - Аудит
    - Устройства
    - Интерактивный вход в систему
    - Клиент сети Microsoft
    - Доступ к сети / Сетевой доступ
    - Сетевая безопасность
    - Завершение работы
    - Параметры системы
    - Контроль учетных записей
    - Прочие
  - Журнал событий
  - Системные службы
  - Файловая система
    - %SystemRoot%\System32\config
    - %SystemRoot%\System32\config\RegBack
  - Реестр
    - MACHINE\SOFTWARE
    - MACHINE\SYSTEM
    - MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg
  - Конфигурация расширенной политики аудита
    - Вход учетной записи

- Разрешения
  - Поиск разрешений
    - Быстрый поиск
    - Расширенный поиск
  - Профиль разрешения
- Создание разрешений
  - Подразделение
  - Пользователь
  - Ресурс
  - Учетная запись
  - Ограничения времени
  - Параметры разрешения
- Операции над разрешениями
  - Копирование
  - Отзыв
  - Приостановка
  - Возобновление
- Массовые операции над разрешениями
  - Отзыв
  - Приостановка
  - Возобновление
- Запросы сессий
  - Поиск запросов
    - Быстрый поиск
    - Расширенный поиск
  - Функции Запросов
    - Подтверждение запроса
    - Отклонение запроса
  - Профиль запроса
- Активные сессии
- Все сессии
  - Поиск сессий
    - Быстрый поиск
    - Расширенный поиск
  - Выгрузка журнала сессий в файл
  - Профиль сессии
- Операции над сессиями
  - Прерывание сессии

О продукте

Программный комплекс Indeed Privileged Access Manager (Indeed PAM) — продукт для управления доступом привилегированных пользователей к ИТ-системам компании.

Единая точка доступа привилегированных пользователей к целевым ресурсам.



Термины

Каталог пользователей

Область домена Active Directory, из которой Indeed PAM получает данные о сотрудниках. Возможна работа с несколькими доменами Active Directory.

> **ИНФОРМАЦИЯ**
>
> Кроме Active Directory поддерживаются следующие службы каталогов:
>
> - FreeIPA (PAM 2.9 и выше)
> - OpenLDAP (PAM 2.10 и выше)
> - ALD Pro (PAM 2.10 и выше)

Пользователи

Сотрудники, чьи личные учетные записи Active Directory входят в каталог пользователей.

Учетные записи

Локальные учетные записи различных систем или доменные учетные записи Active Directory, от которых Indeed PAM получил пароль.

Ресурсы

Различные системы, к которым необходимо получить доступ от имени учетных записей.

Домены

Домены предназначены для получения и автоматического добавления в Indeed PAM доменных компьютеров и доменных учетных записей.

Подразделение

Организационная единица необходимая для объединения в Indeed PAM по формальным признакам пользователей, ресурсов, учетных записей, разрешений для доступа к защищаемым объектам и т.д. Подразделения предназначены для разделения полномочий администраторов Indeed PAM, что позволяет выполнять работы только в рамках конкретного подразделения без возможности вмешаться в работу других администраторов Indeed PAM.

Хранилище данных

Для хранения данных Indeed PAM может использовать СУБД:

- Microsoft SQL Server
- PostgreSQL
- PostgreSQL Pro
- Jatoba

Сервисное подключение

Сервисное подключение к ресурсу позволяет выполнять следующие операции:

- Проверка соединения
- Синхронизация учетных записей
- Синхронизация групп безопасности учетных записей
- Проверка паролей (SSH-ключей) учетных записей
- Изменение паролей (SSH-ключей) учетных записей
- Синхронизация версии ОС или версии СУБД
- Синхронизация компьютеров в Active Directory

Следующие типы ресурсов поддерживают сервисное подключение:

- Microsoft Active Directory
- ОС Windows
- ОС *nix
- Microsoft SQL Server

- MySQL
- PostgreSQL
- OracleDB
- Cisco (OC IOS XE)
- Inspur BMC (IPMI-модуль)

Также доступно добавление собственных типов сервисных подключений.

Пользовательское подключение

Пользовательское подключение является свойством ресурса и позволяет открывать сессии (RDP, SSH и telnet) или сессии через RemoteApp приложения. Поддерживаются следующие типы подключений:

- RDP
- SSH
- Telnet
- RemoteApp
- PostgreSQL

Ресурс может иметь один или более типов пользовательских подключений.

Также доступно добавление собственных типов пользовательских подключений.

Разрешения

Разрешения используются для управления доступом. Любому сотруднику из каталога пользователей может быть выдано разрешение на доступ к ресурсу.
Состав разрешения:

- **Пользователь** — сотрудник, чья личная учетная запись входит в состав каталога пользователей.
- **Учетная запись** — локальная или доменная учетная запись от имени которой пользователь будет открывать сессию на ресурсе.
- **Ресурс** — ресурс, на котором будет открыта сессия.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**

Разрешение не может быть изменено в процессе эксплуатации. Отозванные разрешения не могут быть восстановлены.

Политики

Набор настроек, распределяемых на множество объектов системы. Для одного объекта может быть назначена только одна политика одного типа.

Компоненты

Сервер управления

Indeed PAM Core

Центральный компонент реализующий логику комплекса Indeed PAM.

Среда выполнения:

- ОС Windows Server 2016 – 2022 → web-сервере Internet Information Services (IIS)
- ОС Linux → Docker → Web-сервер Nginx

Состав:

- Web-приложение — core

Задачи:

- Управление пользователями, привилегированными учетными записями, доступом, паролями.

Indeed PAM IdP

Центр идентификации пользователей и компонентов Indeed PAM.

Среда выполнения:

- ОС Windows Server 2016 – 2022 → web-сервере Internet Information Services (IIS)
- ОС Linux → Docker → Web-сервер → Nginx

Состав:

- Web-приложение — idp

Задачи:

- Управление аутентификацией пользователей, выдача и проверка 2fa, проверка подлинности компонентов Indeed PAM.

Indeed PAM Management Console

Административный интерфейс для управления Indeed PAM.

Среда выполнения:

- ОС Windows Server 2016 – 2022 → web-сервере Internet Information Services (IIS)
- ОС Linux → Docker → Web-сервер Nginx

Состав:

- Web-приложение — mc

Задачи:

- Список задач см. в разделе руководство администратора.

Indeed PAM User Console

Пользовательский интерфейс для доступа к защищаемым объектам Indeed PAM.

Среда выполнения:

- ОС Windows Server 2016 – 2022 → web-сервере Internet Information Services (IIS)
- ОС Linux → Docker → Web-сервер Nginx

Состав:

- Web-приложение — uc

Задачи:

- Список задач см. в разделе руководство пользователя.

Indeed Log Server

Единая платформа для работы с событиями Indeed PAM.

Среда выполнения:

- ОС Windows Server 2016 – 2022 → web-сервере Internet Information Services (IIS)

- ОС Linux → Docker → Web-сервер Nginx

Состав:

- Web-приложение — ls

Задачи:

- Сбор, хранение и выдача событий.

Indeed PAM EventLog

Дополнительный модуль для Indeed Log Server.

Среда выполнения:

- ОС Windows Server 2016 – 2022

Состав:

- Файлы и библиотеки для Indeed Log Server

Задачи:

- Реализует запись событий в Windows Event Log

Сервер доступа

Indeed PAM Gateway

Набор компонентов реализующих функции jump server'a, средств аудита сессий и механизмов защиты.

Среда выполнения:

- ОС Windows Server 2016 – 2022

Состав:

- Приложение — ProxyApp.exe

- Драйвер для работы с файловой системой — Pam.FsFilter
- Служба взаимодействия с Pam.FsFilter — Pam.Service
- Модифицированный SSH клиент — Putty.exe
- Расширение для mstsc.exe
- Набор утилит и библиотек — FFmpeg
- Библиотеки контроля процессов

Задачи:

- Предоставление доступа по протоколам RDP/SSH/Telnet и прочим в режиме RemoteApp.
- Ведение записи видео и снимков экрана, перехвата текста и перехвата передаваемых файлов.
- Обработка и сохранение артефактов сессий.
- Проверка состояния клиентских компонентов.
- Контроль запуска процессов и доступа к файловой системе.

Indeed PAM SSH Proxy

Прокси-сервер для SSH-сессий.

Среда выполнения:

- ОС Linux → Docker

Состав:

- Приложение — Pam.SshProxy.Service (ОС Linux)

Задачи:

- Предоставление доступа по протоколам SSH\SCP\SFTP.
- Ведение перехвата текста и перехвата передаваемых файлов.
- Обработка и сохранение артефактов сессии.

Indeed PAM PostgreSQL Proxy

Прокси-сервер для PostgreSQL-сессий.

Среда выполнения:

- ОС Linux → Docker

Состав:

- Приложение — Pam.PostgreSQLProxy.Service (ОС Linux)

Задачи:

- Ведение перехвата текста SQL-запросов, запускаемых пользователем.

Indeed PAM RDP Proxy

Прокси-сервер для RDP-сессий.

Среда выполнения:

- ОС Linux → Docker

Состав:

- Приложение — Pam.RdpProxy.Service (ОС Linux)

Задачи:

- Предоставление доступа по протоколу RDP.
- Ведение перехвата текста, видео, скриншотов и перехвата передаваемых файлов.
- Обработка и сохранение артефактов сессии.

Indeed ESSO Agent и Indeed Admin Pack

Набор компонентов для реализации SSO-доступа.

Среда выполнения:

- ОС Windows Server 2016 – 2022

Состав:

- Набор приложений, служб и инструментов для взаимодействия с формами аутентификации и компонентами Indeed PAM.
- Расширения для браузеров: Internet Explorer; Google Chrome; EDGE.

Задачи:

- Перехват и заполнение форм аутентификации web и настольных приложений.

Ресурсы Windows

Indeed PAM Agent

Компонент для текстового логирования RDP-сессий.

Среда выполнения:

- ОС Windows Server 2012R2 – 2022/Windows XP SP3 X64 – 11

Состав:

- Приложение Pam.Proxy.WindowsAgent

Задачи:

- Фиксация смены активных окон, запуска процессов и клавиатурного ввода.

> ⓘ **К СВЕДЕНИЮ**
>
> Компонент Indeed PAM Agent является необязательным, так как Indeed PAM полностью безагентское решение, дополнительные компоненты используются только для решения специальных задач.

Ресурсы Linux

Indeed PAMSU

Компонент для выполнения команд с привилегией root, аналогично sudo используется команда pamsu. Отличие заключается в том, что аутентификация будет запрашиваться у пользователя PAM, а не привилегированной УЗ от имени которой открыта сессия.

Среда выполнения:

- ОС Linux

Состав:

- deb или rpm пакет

Задачи:

- Выполнение команд с повышением привилегий от имени пользователя PAM

> **К СВЕДЕНИЮ**
>
> Компонент Indeed PAMSU является необязательным, так как Indeed PAM полностью безагентское решение, дополнительные компоненты используются только для решения специальных задач.

Рабочее место пользователя Indeed PAM

Indeed PAM Desktop Console

Дополнительный инструмент для получения доступа к защищаемым объектам Indeed PAM.

Состав:

- Модифицированный mRemoteNG.exe

Задачи:

- Список задач см. в разделе руководство пользователя.

Упрощенная на Windows

Для ознакомления с Indeed PAM

Упрощенная на Linux

Для ознакомления с Indeed PAM

Основная

Для внедрения и эксплуатации в промышленной среде

Отказоустойчивая

Для внедрения и эксплуатации в промышленной среде (с дублированием серверов)

Упрощенная на Windows

Компоненты Indeed PAM устанавливаются на два сервера. Рекомендуется для ознакомления и тестирования.

Компоненты

Сервер управления/Сервер доступа (RDP/RemoteApp)

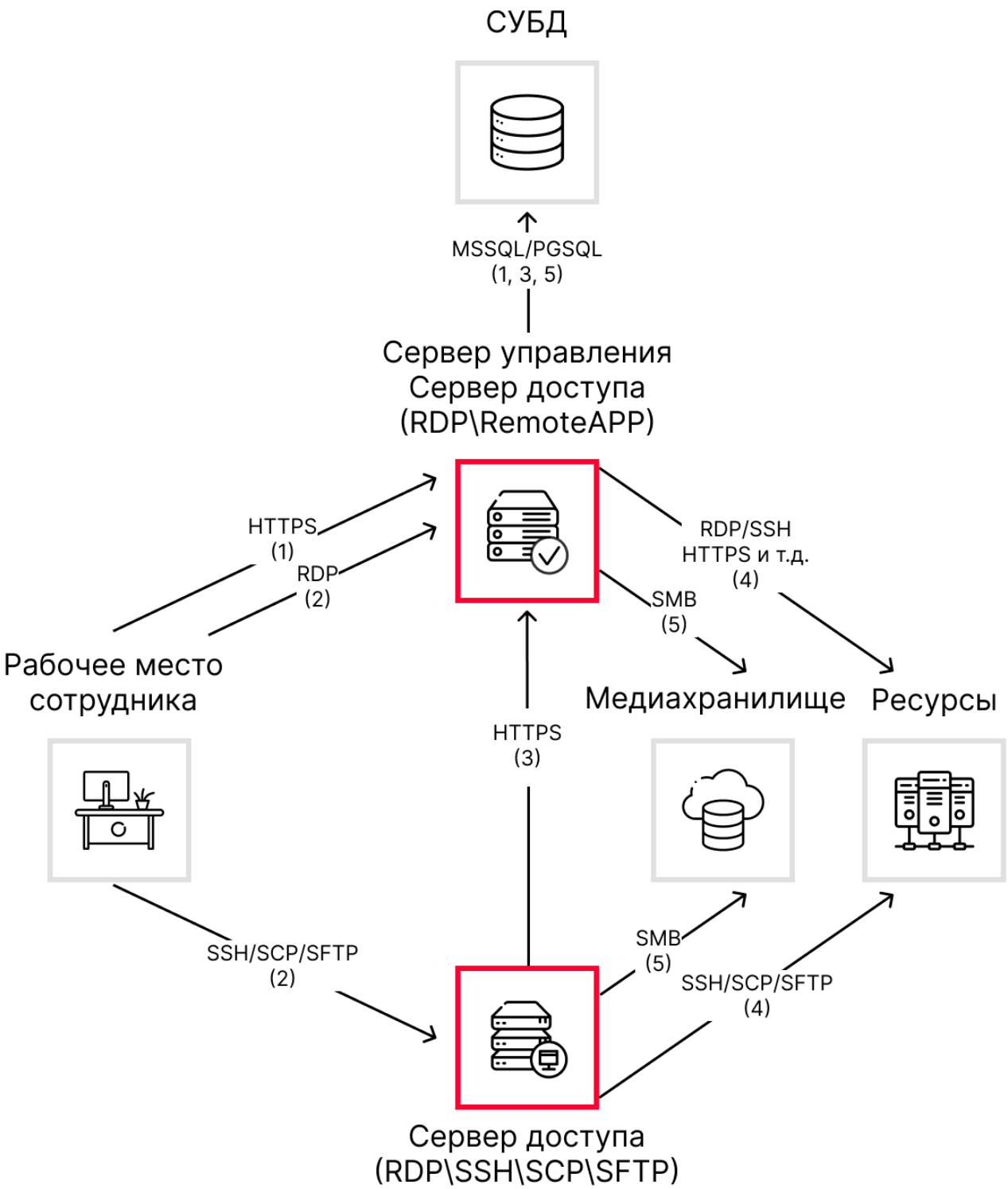
- Indeed PAM Core
- Indeed PAM IdP
- Indeed PAM Management Console
- Indeed PAM User Console
- Indeed Log Server
- Indeed PAM EventLog
- Indeed PAM Gateway
- Indeed ESSO Admin Pack
- Indeed ESSO Agent

Сервер доступа (SSH/SCP/SFTP)

- Indeed PAM SSH Proxy
- Indeed PAM RDP Proxy
- Indeed PAM PostgreSQL Proxy

Сценарии работы

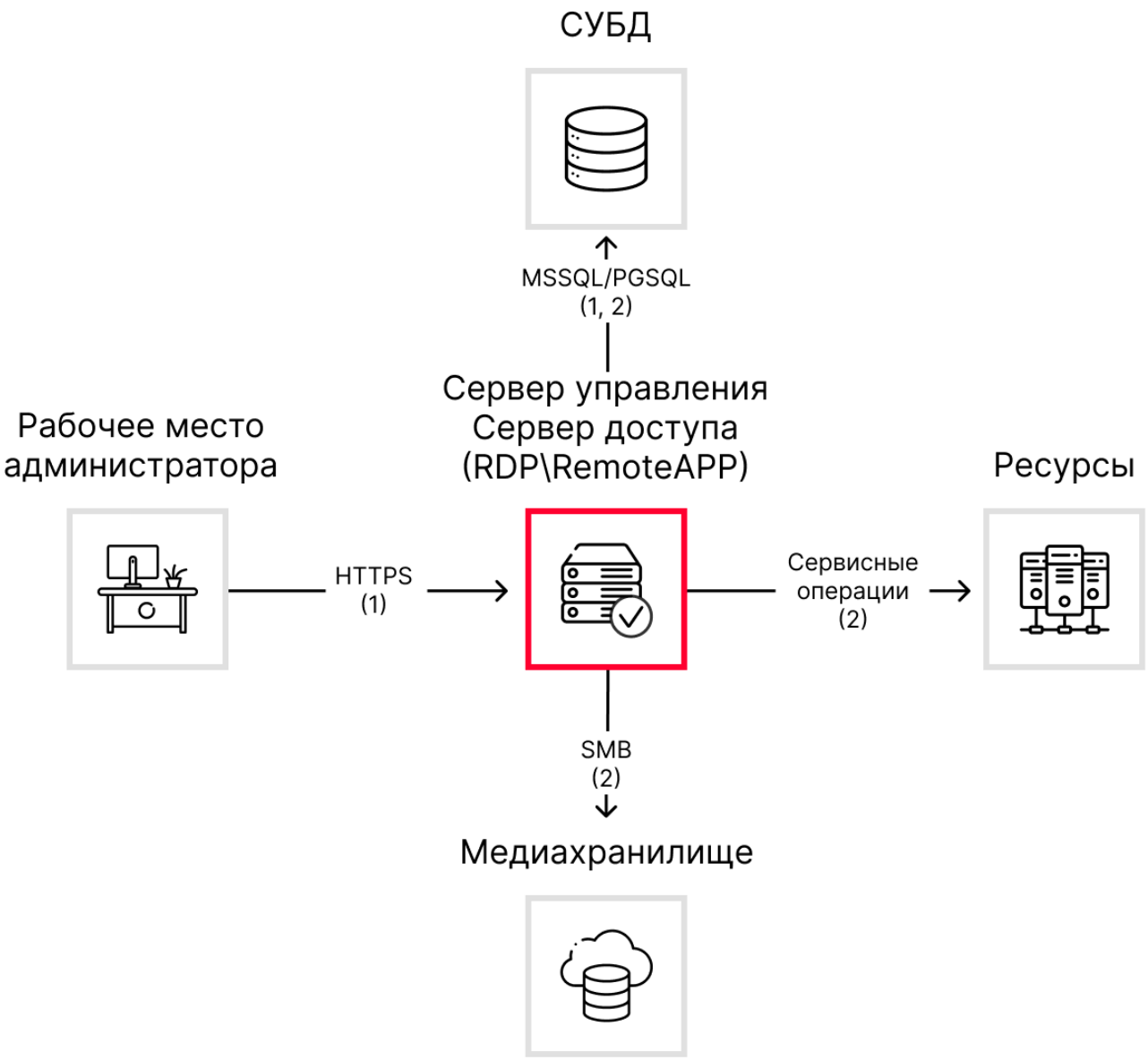
Пользовательский



1. Подключение к личному кабинету пользователя через браузер или запуск Indeed PAM Desktop Console. Доменная аутентификация и регистрация/предоставление второго фактора. Проверка пользователя в БД IdP. Получение списка ресурсов из БД Core. Получение RDP-файла для подключения к ресурсу.

2. Подключение к серверу доступа (RDP\RemoteApp) при помощи RDP-файла, Indeed PAM Desktop Console или подключение к серверу доступа (RDP\SSH\SCP\SFTP) при помощи RDP-файла или отдельного SSH-клиента.
3. Доменная аутентификация и предоставление второго фактора. Проверка пользователя БД IdP. Проверка разрешения на доступ в БД Core. Извлечение из СУБД логина и пароля сервисной учетной записи для работы с медиахранилищем. Извлечение из СУБД логина и пароля привилегированной учетной записи для подключения к ресурсу.
4. Подключение к ресурсу.
5. Сохранение видео и скриншотов в медиахранилище. Сохранение текстового лога в БД Core.

Административный



1. Подключение к кабинету администратора. Доменная аутентификация и регистрация/ предоставление второго фактора. Проверка пользователя в БД IdP.
2. Получение, добавление и редактирование объектов системы. Выполнение сервисных операций.

Упрощенная на Linux

Компоненты Indeed PAM устанавливаются на два сервера. Рекомендуется для ознакомления и тестирования.

Компоненты

Сервер управления/Сервер доступа (RDP/SSH/SCP/SFTP)

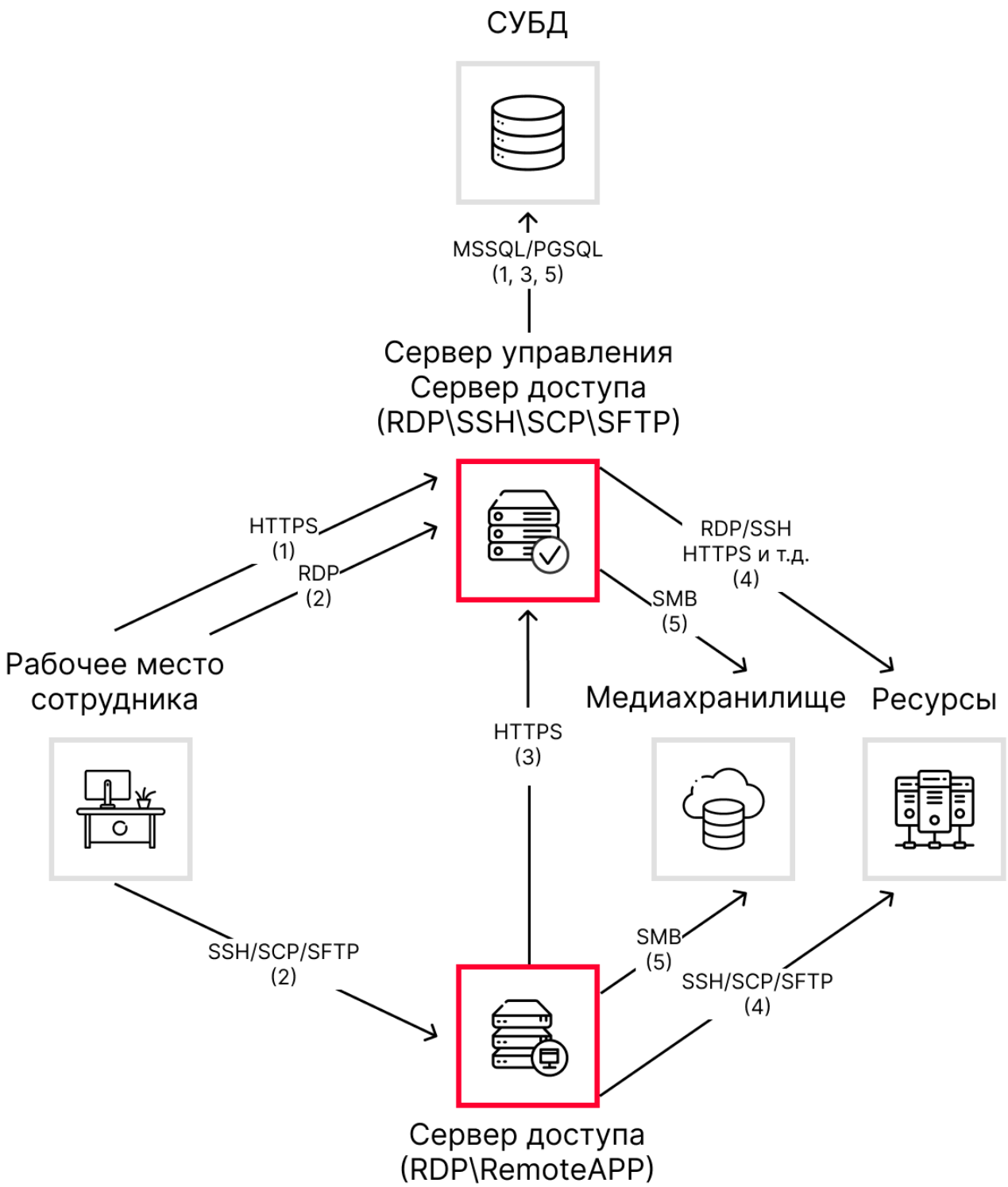
- Indeed PAM Core
- Indeed PAM IdP
- Indeed PAM Management Console
- Indeed PAM User Console
- Indeed Log Server
- Indeed PAM SSH Proxy
- Indeed PAM RDP Proxy
- Indeed PAM PostgreSQL Proxy

Сервер доступа (RDP/RemoteApp)

- Indeed PAM Gateway
- Indeed ESSO Admin Pack
- Indeed ESSO Agent

Сценарии работы

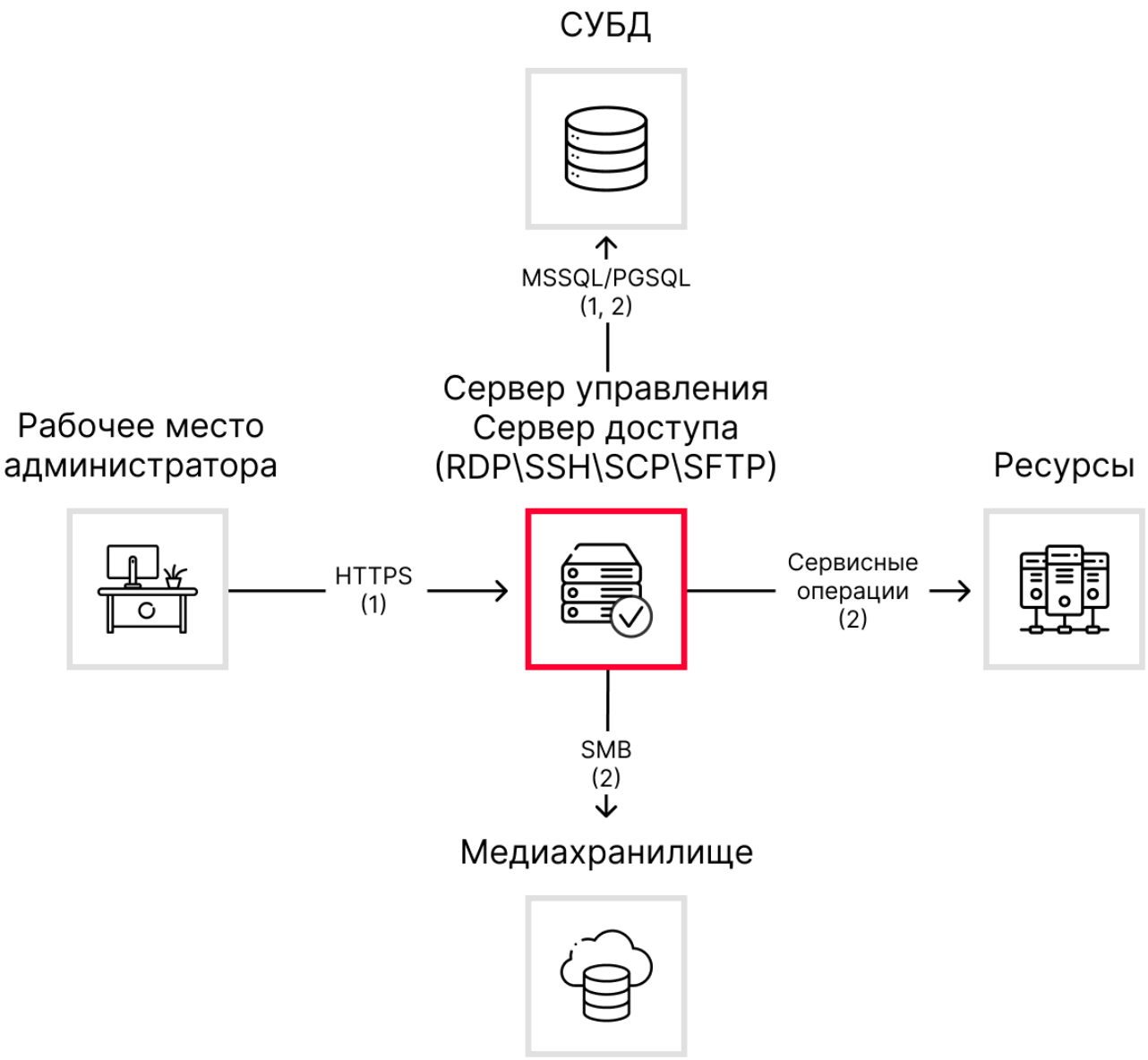
Пользовательский



1. Подключение к личному кабинету пользователя через браузер или запуск Indeed PAM Desktop Console. Доменная аутентификация и регистрация/предоставление второго фактора. Проверка пользователя в БД IdP. Получение списка ресурсов из БД Core. Получение RDP-файла для подключения к ресурсу.

2. Подключение к серверу доступа (RDP/RemoteApp) при помощи RDP-файла, Indeed PAM Desktop Console или подключение к серверу доступа (RDP/SSH/SCP/SFTP) при помощи RDP-файла или отдельного SSH-клиента.
3. Доменная аутентификация и предоставление второго фактора. Проверка пользователя БД IdP. Проверка разрешения на доступ в БД Core. Извлечение из СУБД логина и пароля сервисной учетной записи для работы с медиахранилищем. Извлечение из СУБД логина и пароля привилегированной учетной записи для подключения к ресурсу.
4. Подключение к ресурсу.
5. Сохранение видео и скриншотов в медиахранилище. Сохранение текстового лога в БД Core.

Административный



1. Подключение к кабинету администратора. Доменная аутентификация и регистрация/ предоставление второго фактора. Проверка пользователя в БД IdP.
2. Получение, добавление и редактирование объектов системы. Выполнение сервисных операций.

Основная

Компоненты Indeed PAM устанавливаются на три сервера. Этот тип установки позволяет отделить логику системы от компонентов предоставляющих доступ. Рекомендуется для внедрения и эксплуатации в промышленной среде.

Компоненты

Сервер управления

- Indeed PAM Core
- Indeed PAM IdP
- Indeed PAM Management Console
- Indeed PAM User Console
- Indeed Log Server
- Indeed PAM EventLog

Сервер доступа (RDP/RemoteApp)

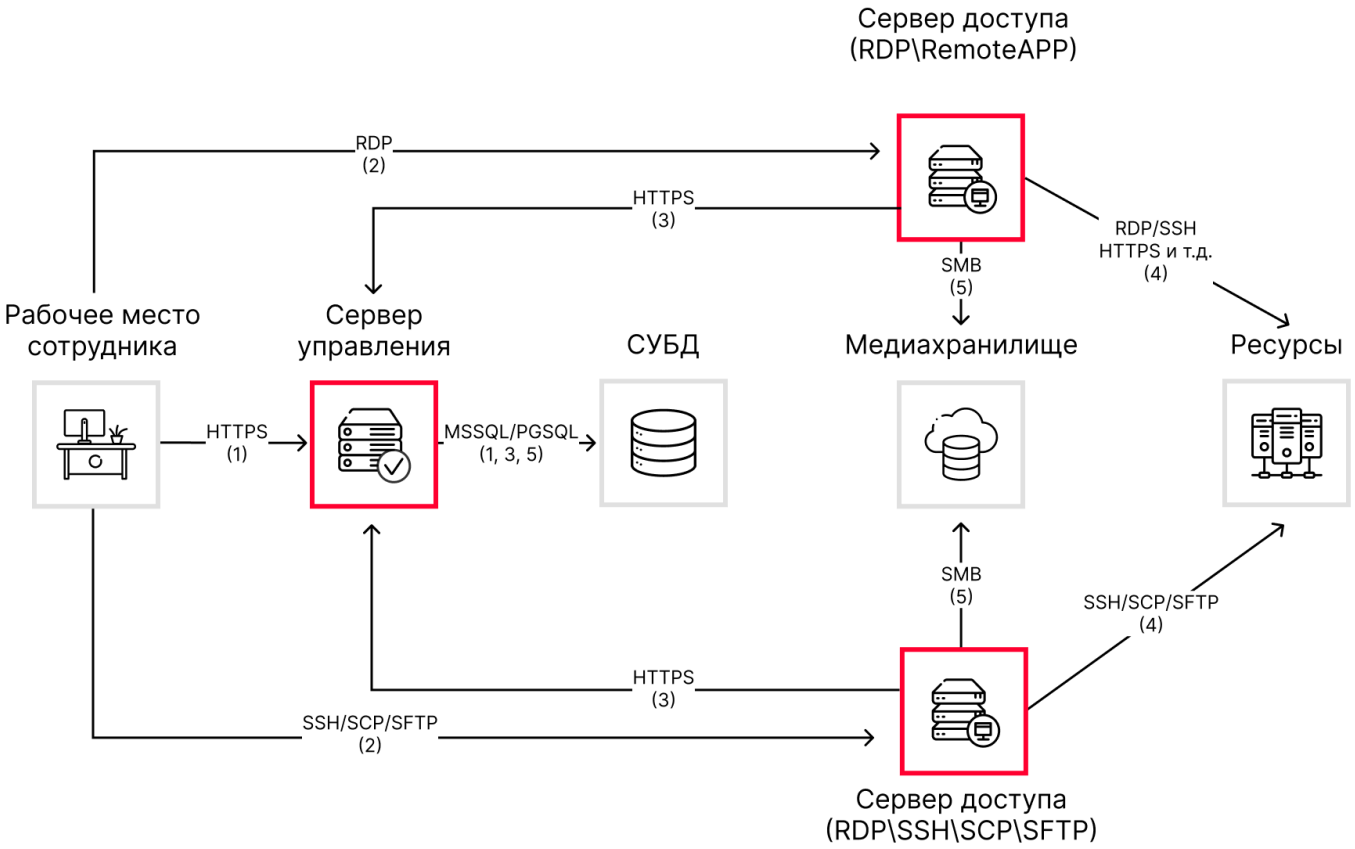
- Indeed PAM Gateway
- Indeed ESSO Admin Pack
- Indeed ESSO Agent

Сервер доступа (RDP/SSH/SCP/SFTP)

- Indeed PAM SSH Proxy
- Indeed PAM RDP Proxy
- Indeed PAM PostgreSQL Proxy

Сценарии работы

Пользовательский



1. Подключение к личному кабинету пользователя через браузер или запуск Indeed PAM Desktop Console. Доменная аутентификация и регистрация/предоставление второго фактора. Проверка пользователя в БД IdP. Получение списка ресурсов из БД Core. Получение RDP-файла для подключения к ресурсу.
2. Подключение к серверу доступа (RDP\RemoteApp) при помощи RDP-файла, Indeed PAM Desktop Console или подключение к серверу доступа (RDP\SSH\SCP\SFTP) при помощи RDP-файла или отдельного SSH-клиента.
3. Доменная аутентификация и предоставление второго фактора. Проверка пользователя в БД IdP. Проверка разрешения на доступ в БД Core. Извлечение из СУБД логина и пароля сервисной учетной записи для работы с медиахранилищем. Извлечение из СУБД логина и пароля привилегированной учетной записи для подключения к ресурсу.
4. Подключение к ресурсу.
5. Сохранение видео и скриншотов в медиахранилище. Сохранение текстового лога в БД Core.

Административный

1. Подключение к кабинету администратора. Доменная аутентификация и регистрация/ предоставление второго фактора. Проверка пользователя в БД IdP.
2. Получение, добавление и редактирование объектов системы. Выполнение сервисных операций.

Отказоустойчивая

Компоненты Indeed PAM устанавливаются на разные серверы, каждый сервер дублируется для организации отказоустойчивости. Рекомендуется использовать для внедрения и эксплуатации в промышленной среде.

Компоненты

Сервер управления

- Indeed PAM Core
- Indeed PAM IdP
- Indeed PAM Management Console
- Indeed PAM User Console
- Indeed Log Server
- Indeed PAM EventLog

Сервер доступа (RDP/RemoteApp)

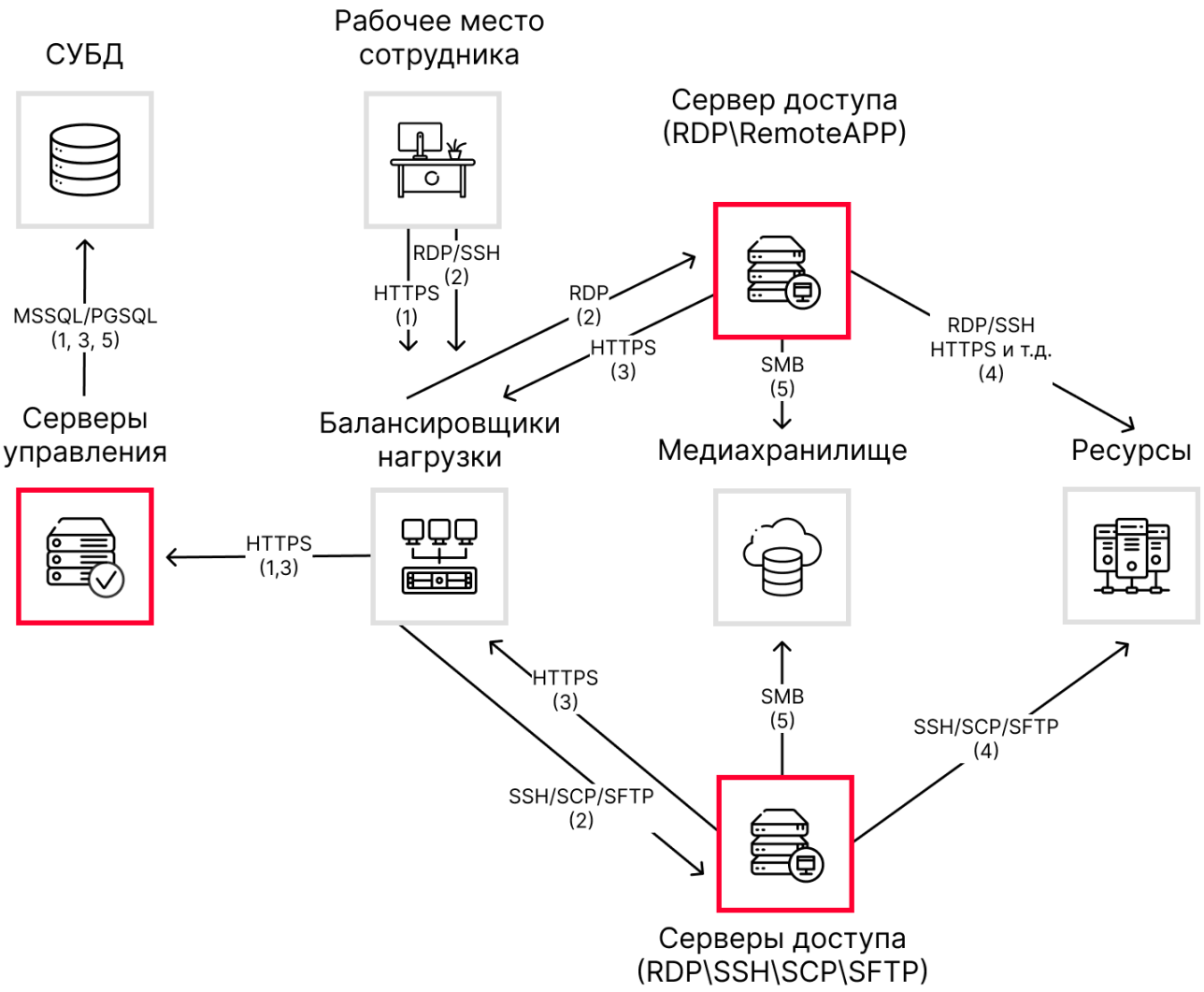
- Indeed PAM Gateway
- Indeed ESSO Admin Pack
- Indeed ESSO Agent

Сервер доступа (RDP/SSH/SCP/SFTP)

- Indeed PAM SSH Proxy
- Indeed PAM RDP Proxy
- Indeed PAM PostgreSQL Proxy

Сценарии работы

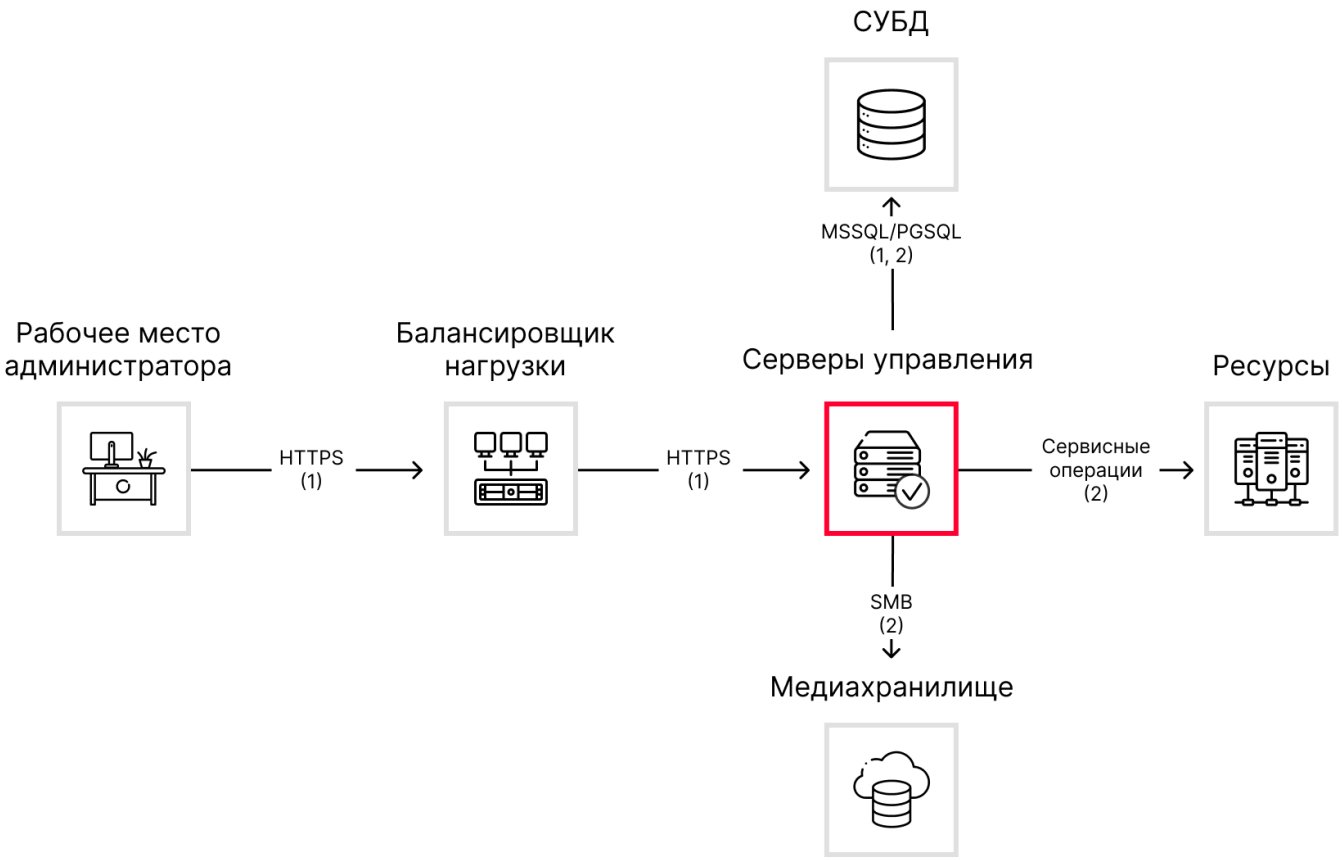
Пользовательский



1. Подключение к личному кабинету пользователя через браузер или запуск Indeed PAM Desktop Console. Доменная аутентификация и регистрация/предоставление второго фактора. Проверка пользователя в БД IdP. Получение списка ресурсов из БД Core. Получение RDP-файла для подключения к ресурсу.
2. Подключение к серверу доступа (RDP/RemoteApp) при помощи RDP-файла, Indeed PAM Desktop Console или подключение к серверу доступа (RDP/SSH/SCP/SFTP) при помощи RDP-файла или отдельного SSH-клиента.
3. Доменная аутентификация и предоставление второго фактора. Проверка пользователя в БД IdP. Проверка разрешения на доступ в БД Core. Извлечение из СУБД логина и пароля сервисной учетной записи для работы с медиахранилищем. Извлечение из СУБД логина и пароля привилегированной учетной записи для подключения к ресурсу.
4. Подключение к ресурсу.

5. Сохранение видео и скриншотов в медиахранилище. Сохранение текстового лога в БД Core.

Административный



1. Подключение к кабинету администратора. Доменная аутентификация и регистрация/ предоставление второго фактора.
2. Получение, добавление и редактирование объектов системы. Выполнение сервисных операций.

Для ОС Windows

Аппаратные и программные требования для установки Indeed PAM на ОС Windows

Для ОС Linux

Аппаратные и программные требования для установки Indeed PAM на ОС Linux

К СУБД

Аппаратные требования к СУБД

Для ОС Windows

Сервер управления

Аппаратные требования

Параметры	50 сессий	100 сессий	200 сессий
CPU	8 Cores	16 Cores	32 Cores
RAM	8 GB	16 GB	32 GB
HDD/SSD	120 GB	120 GB	120 GB
Network adapter	1 Gb	1 Gb	1 Gb

Программные требования

Операционная система:

- Windows Server 2016 – 2022

Домен:

- В составе домена Microsoft Active Directory

Веб-сервер:

- Internet Information Services 8.5 – 10.0

Модули для веб-сервера Internet Information Services:

- Обычная проверка подлинности (Basic Authentication)
- Проверка подлинности Windows (Windows Authentication)
- Статическое содержимое (Static Content)
- Перенаправление HTTP (HTTP Redirection)

- ASP.NET Core Runtime
- Расширения ISAPI (ISAPI Extensions)
- Расширяемость .NET (.NET Extensibility)
- Фильтры ISAPI (ISAPI Filters)
- Консоль управления службами IIS (IIS Management Console)

Дополнительные компоненты Microsoft:

- Microsoft .NET Core 8
- URL Rewrite

Сетевое взаимодействие

Входящие **Исходящие**

Протокол	Порт	Описание
TCP	443	Работа с личными кабинетами, API и IdP

Сервер доступа (RDP)

Аппаратные требования

Параметры	10 RDP/SSH сессий	50 RDP/SSH сессий	100 RDP/SSH сессий
CPU	8 Cores	16 Cores	32 Cores
RAM	12 GB	32 GB	64 GB
HDD/SSD	160 GB + 5 GB на каждого пользователя PAM	320 GB + 5 GB на каждого пользователя PAM	520 GB + 5 GB на каждого пользователя PAM

Параметры	10 RDP/SSH сессий	50 RDP/SSH сессий	100 RDP/SSH сессий
Network adapter	1 Gb	1 Gb	1 Gb

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Требования рассчитаны для выделенного физического сервера. Тестирование выполнялось для сессий RDP и SSH.
>
> Для поддержания заявленного количества одновременных сессий необходим процессор с поддержкой Simultaneous multithreading (AMD) или Hyper-Threading (Intel).
>
> Заявленное количество одновременных сессий поддерживается при условии захвата видео с одного монитора в разрешении HD. Разрешение видео определяется настройками монитора на стороне клиента. При увеличении разрешения или количества мониторов максимальное заявленное количество одновременных сессий снизится.
>
> Использование клиентских приложений запускаемых с сервера Indeed PAM в режиме RemoteApp снижает максимальное количество одновременных сессий. Влияние каждого приложения на максимальное количество одновременных сессий индивидуально и определяется при тестировании.
>
> Если развертывание выполняется в конкурентной виртуальной среде, то количество одновременных сессий может быть меньше. Для поддержки заявленного количества одновременных сессий виртуальный сервер должен иметь зарезервированные MHz и RAM эквивалентные физическому серверу.

Программные требования

Операционная система:

- Windows Server 2016 – 2022

Домен:

- В составе домена Microsoft Active Directory

Дополнительные компоненты Microsoft:

- Microsoft .NET Desktop Runtime x64 версия 8
- Microsoft C++ 2015 – 2019 Redistributable

Браузер:

- Google Chrome
- Microsoft EDGE

Роли Remote Desktop Services:

- Remote Desktop Services Broker (RDCB)
- Remote Desktop Services Host (RDSH)
- Remote Desktop Web Access (RDWA)

Сетевое взаимодействие

Входящие **Исходящие**

Протокол	Порт	Описание
TCP	3389	Подключение к серверу доступа
TCP	5443	Просмотр стрима сессии

Для ОС Linux

Сервер управления

Аппаратные требования

Параметры	50 сессий	100 сессий	200 сессий
CPU	2 Cores	2 Cores	2 Cores
RAM	4 GB	4 GB	4 GB
HDD/SSD	120 GB	120 GB	120 GB
Network adapter	1 Gb	1 Gb	1 Gb

Программные требования

Операционная система:

- ОС Linux

Контейнеризация:

- Docker не ниже 18.09
- Docker Compose не ниже 1.29.2

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Docker должен быть установлен из репозитория дистрибутива.

▼ Альтернативный способ установки Docker (не рекомендуется)

В крайних случаях (когда нет доступа к репозиториям операционной системы и Docker) возможна установка Docker из статических бинарных файлов.

Если вы используете операционную систему, отличную от перечисленных по ссылке, то при установке этим способом не установится необходимый для работы Indeed PAM пакет с модулем SELinux. В большинстве систем этот пакет называется **container-selinux**.

Установите его вручную в соответствии с документацией используемой операционной системы. Сделать это нужно **перед** запуском скрипта установки **run-deploy.sh**.

Сетевое взаимодействие

Входящие **Исходящие**

Протокол	Порт	Описание
TCP	443	Работа с личными кабинетами, API и IdP

Сервер доступа (SSH)

Аппаратные требования

Параметры	50 SSH сессий	100 SSH сессий	200 SSH сессий
CPU	2 Cores	2 Cores	2 Cores
RAM	2 GB	2 GB	4 GB
HDD/SSD	120 GB	120 GB	120 GB
Network adapter	1 Gb	1 Gb	1 Gb

Программные требования

Операционная система:

- ОС Linux

Контейнеризация:

- Docker не ниже 18.09
- Docker Compose 1.29.2

Сетевое взаимодействие

Входящие **Исходящие**

Протокол	Порт	Описание
TCP	2222	Подключение к серверу доступа

Сервер доступа (RDP)

Аппаратные требования

Параметры	10 RDP сессий	50 RDP сессий	100 RDP сессий
CPU	4 Cores	12 Cores	16 Cores
RAM	4 GB	12 GB	40 GB
HDD/SSD	120 GB	120 GB	120 GB
Network adapter	1 Gb	1 Gb	1 Gb

Программные требования

Операционная система:

- ОС Linux

Контейнеризация:

- Docker не ниже 18.09
- Docker Compose 1.29.2

Сетевое взаимодействие

Входящие **Исходящие**

Протокол	Порт	Описание
TCP	3390	Подключение к серверу доступа
TCP	8443	Просмотр стрима сессии

Настройки безопасности CIS Benchmark

На серверах PAM необходимо применить настройки безопасности CIS Benchmark, описанные в PDF-файле. Получить файл можно одним из способов:

- скачать файл здесь
- получить файл на официальном сайте cisecurity

К СУБД

Поддерживаемые СУБД

- Microsoft SQL Server 2012SP2 – 2022 с поддержкой Full-Text and Semantic Extractions for Search
- PostgreSQL 12–16
- Postgres Pro Standard 12–16
- Postgres Pro Enterprise
- Jatoba 4–5

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> При использовании Microsoft SQL Server обязательно должен быть установлен дополнительный модуль — полнотекстовый и семантический поиск (Full-Text and Semantic Extractions for Search).

Аппаратные требования

Параметры	50 сессий	100 сессий	200 сессий
CPU	2 Cores	2 Cores	2 Cores
RAM	2 GB	4 GB	4 GB
HDD	1 TB	1 TB	1 TB
Network adapter	1 Gb	1 Gb	1 Gb

Программные требования

- В соответствии с официальной документацией производителя

Сетевое взаимодействие

- В соответствии с официальной документацией производителя

Лицензирование

В Indeed Privileged Access Manager (Indeed PAM) есть две схемы лицензирования:

- По пользователям и ресурсам.
- По сессиям (одновременным подключениям).

> ⚠ **ОБРАТИТЕ ВНИМАНИЕ**
>
> Вы можете выбрать только одну схему лицензирования в рамках одной инсталляции Indeed PAM.

Отдельно (вне схем лицензирования) можно приобрести лицензию на Application to Application Password Management (AAPM). Эта лицензия влияет только на доступ к функциям AAPM и не влияет на возможность пользователей установить сессию через PAM или на возможность администратора добавить пользователю разрешение.

Лицензирование по пользователям и ресурсам

При выборе этой схемы лицензирования вам нужно определить количество пользователей и количество ресурсов в вашей инсталляции Indeed PAM.

Они задаются количеством лицензий следующих типов:

- Пользовательская — определяет количество пользователей, которые смогут использовать Indeed PAM.
- Ресурсная — определяет количество ресурсов, которые можно создать в Indeed PAM.

При выборе этой схемы лицензирования количество сессий (одновременных подключений) не ограничено. Пользовательские лицензии можно перераспределить между сотрудниками (отозвать лицензии у одних сотрудников и выделить другим). Ресурсные лицензии можно освободить и занять другими ресурсами.

> 💡 **ИНФОРМАЦИЯ**
>
> Любые лицензии можно докупить.

Выдача лицензии

Пользовательская лицензия

Чтобы выдать пользовательскую лицензию, добавьте пользователю хотя бы одно активное разрешение. После этого лицензия автоматически будет считаться занятой этим пользователем. Если все пользовательские лицензии исчерпаны, добавить разрешение новому пользователю нельзя.

Ресурсная лицензия

Чтобы выдать ресурсную лицензию, создайте или восстановите ресурс в Indeed PAM. После этого лицензия автоматически будет считаться занятой этим ресурсом. Если все ресурсные лицензии исчерпаны, создать новый ресурс нельзя.

Отзыв (освобождение) лицензии

Пользовательская лицензия

Пользовательская лицензия освобождается, когда у пользователя не остается ни одного активного разрешения, т.е. в результате таких действий с разрешениями, как:

- Отзыв
- Приостановка
- Истечение срока

Ресурсная лицензия

Ресурсная лицензия освобождается при удалении ресурса.

Срок действия лицензии

По сроку действия лицензии бывают:

- Не ограниченные по времени
- Ограниченные конкретной календарной датой
  - Пробный период
  - Подписка

После истечения срока действия лицензии следующие операции станут недоступны:

- Добавить ресурс
- Добавить пользователя (даже при наличии свободных лицензий)
- Открыть сессию (подключиться к ресурсу)

> **ВНИМАНИЕ**
>
> Если нет неограниченных лицензий, то после истечения срока действия лицензий подключения станут недоступны.

Лицензирование по сессиям

При выборе этой схемы лицензирования вам нужно задать количество сессий, т.е. одновременных подключений, которые можно открыть в Indeed PAM.

При выборе этой схемы лицензирования количество пользователей и количество ресурсов Indeed PAM не ограничено.

Выдача и освобождение лицензии

Сессионная лицензия считается занятой в момент открытия сессии и освобождается в момент завершения сессии (причина завершения не важна).

Срок действия лицензии

По сроку действия лицензии бывают:

- Не ограниченные по времени
- Ограниченные конкретной календарной датой
  - Пробный период
  - Подписка

После истечения срока действия лицензии станет нельзя открывать сессии.

После истечения срока действия лицензии останутся доступны следующие операции:

- Редактирование разрешений
- Редактирование созданных ресурсов

- Редактирование учетных записей

> **ВНИМАНИЕ**
>
> Если нет неограниченных лицензий, то после истечения срока действия лицензий подключения станут недоступны.

Лицензия на Application to Application Password Management

Лицензия на AAPM позволяет использовать сценарии получения секретов учетных записей из Indeed PAM сторонними приложениями.

В этой лицензии вам нужно задать количество учетных записей, к которым можно получить доступ при помощи механизма AAPM.

Количество приложений, пользователей приложений и разрешений не ограничено.

> **ИНФОРМАЦИЯ**
>
> Лицензия на AAPM не зависит от выбранной схемы лицензирования.
>
> Лицензию на AAPM можно докупить или удалить в любой момент.

Выдача и освобождение лицензии

Лицензия на AAPM считается занятой в момент добавления учетной записи первого разрешения для приложения.

Лицензия на AAPM освобождается в момент отзыва всех разрешений у учетной записи.

> **ОБРАТИТЕ ВНИМАНИЕ**
>
> Приостановка разрешений не освобождает лицензию на AAPM.

Срок действия лицензии

По сроку действия лицензии бывают:

- Не ограниченные по времени
- Ограниченные конкретной календарной датой
  - Пробный период
  - Подписка

После истечения срока действия лицензии вам станут недоступны следующие операции:

- Добавить новые разрешения на приложения
- Использовать сценарии получения секретов учетных записей из Indeed PAM сторонними приложениями

Общий план внедрения

Подготовка инфраструктуры

1. Предоставление серверных и клиентских ресурсов в соответствии с их системно-аппаратными требованиями.
2. Установка и настройка **Служб удаленных рабочих столов** (Remote Desktop Services).
3. Установка дополнительных компонентов Microsoft для корректной работы серверных компонентов Indeed PAM.
4. Настройка сетевого взаимодействия серверных и клиентских компонентов в соответствии с требованиями.
5. Настройка хранилища данных Indeed PAM:

- Предоставление доступа к экземпляру Microsoft SQL/PostgreSQL, PostgreSQL Pro.
- Создание баз данных и настройка сервисной учетной записи или предоставление доступа к имеющейся учетной записи.

6. Определение LDAP-путей контейнеров и подразделений, в которых будет расположен каталог пользователей Indeed PAM в иерархии Active Directory.
7. Создание и настройка сервисной учетной записи для работы с каталогом пользователей Indeed PAM или предоставление доступа к имеющейся учетной записи.
8. Создание и настройка сервисной учетной записи для сервисных операций в Active Directory или предоставление доступа к имеющейся учетной записи.

Установка и настройка серверных компонентов Indeed PAM

Windows

1. Сервер управления (Windows)
2. Сервер доступа (RDP\RemoteApp)
3. Сервер доступа (SSH Proxy)

Linux

1. Сервер управления (Linux)
2. Сервер доступа (RDP/RemoteApp)
3. Сервер доступа (SSH Proxy)

Установка и настройка клиентских компонентов Indeed PAM

1. Установка и настройка PamSu
2. Установка и настройка Indeed PAM Agent
3. Установка и настройка Indeed PAM Desktop Console

Тестовый запуск Indeed PAM

1. Проверка серверных и клиентских компонентов.
2. Проверка сценариев заказчика:

- Настройка сервисных операций для ресурсов с ОС Windows.
- Настройка сервисных операций для ресурсов с ОС *nix.
- Настройка пользовательских подключений.

3. Устранение ошибок.

Завершающий этап

1. Демонстрация.
2. Обучение.
3. Тестирование.

Учетные записи каталога пользователей

Создайте учетные записи для работы с каталогом пользователей и для сервисных операций

Сертификаты

Подготовьте сертификаты перед установкой Indeed PAM

Базы данных

Создайте базы данных и учетные записи для работы с хранилищем данных

Медиахранилище

Создайте и настройте файловое хранилище

Серверы

Добавьте RDS роль (для Windows) или установите необходимые компоненты (для Linux)

Учетные записи для установки PAM через мастер

Просмотрите список учетных записей, которые требуются для работы с мастером

Учетные записи каталога пользователей

Взаимодействие Indeed PAM с конечными пользователями выполняется за счет учетной записи, которая будет получать список пользователей и их атрибуты.

Учетная запись для работы с каталогом пользователей

Active Directory | **FreeIPA** | **ALD Pro** | **OpenLDAP**

1. Запустите оснастку **Active Directory — пользователи и компьютеры** (Active Directory Users and Computers).
2. Вызовите контекстное меню контейнера или подразделения.
3. Выберите пункт **Создать** (Create) — **Пользователь** (User).
4. Укажите имя, например, **IPAMADReadOps**.
5. Заполните обязательные поля и завершите создание учетной записи.

Учетная запись для сервисных операций

Active Directory | **FreeIPA** | **ALD Pro** | **OpenLDAP**

1. Запустите оснастку **Active Directory — пользователи и компьютеры**(Active Directory Users and Computers).
2. Откройте контекстное меню контейнера или подразделения.
3. Выберите пункт **Создать**(Create) — **Пользователь** (User).
4. Укажите имя, например, **IPAMADServiceOps**.
5. Заполните обязательные поля и завершите создание учетной записи.
6. Откройте контекстное меню контейнера, подразделения или корня домена.
7. Выберите пункт **Свойства** (Properties).

8. Перейдите на вкладку **Безопасность** (Security).
9. Нажмите **Добавить** (Add).
10. Выберите учетную запись **IPAMADServiceOps** и нажмите **Ок**.
11. Нажмите **Дополнительно** (Advanced).
12. Выберите учетную запись **IPAMADServiceOps** и нажмите **Изменить**(Edit).
13. Установите для поля **Применяется к:**(Applies to:) значение **Дочерние объекты: Пользователь** (Descendant User objects).
14. В разделе **Разрешения:** (Permissions:) отметьте **Сброс пароля** (Reset password).
15. Сохраните внесенные изменения.

Сертификаты

Подготовьте сертификаты перед установкой Indeed PAM. У всех сертификатов должен быть один и тот же пароль.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Все сертификаты, кроме сертификата удостоверяющего центра, должны быть в формате `.pfx`.
>
> Сертификат удостоверяющего центра должен быть в формате `.crt`.

Инсталляция без балансировки | **Отказоустойчивая инсталляция с HAProxy** | **Отказоустойчивая инсталляция со сторонним балансировщиком**

Вам понадобятся следующие сертификаты:

- Сертификат удостоверяющего центра без приватного ключа в формате PEM (Base64) с расширением `.crt`.
- Сертификат на FQDN PAM с приватным ключом в формате `.pfx`.
- Сертификаты на все серверы доступа RDP, RDS и PostgreSQL с приватным ключом в формате `.pfx`. Кроме случая, когда сервер доступа установлен на одном хосте с сервером управления.

> ⓘ **ИНФОРМАЦИЯ**
>
> Доступно использование wildcard-сертификата. В этом случае сертификат должен быть выпущен на весь домен или иметь в альтернативных именах адреса всех хостов PAM.

Для корректной работы LDAPS поместите корневой сертификат в **IndeedPAM_3.0_RU\indeed-pam\state\ca-certificates** перед запуском мастера.

Базы данных

Для хранения данных Indeed PAM использует следующие БД:

- **Core** — БД компонента Indeed PAM Core, используется для хранения данных привилегированных учетных записей, ресурсов, разрешений, и прочих сервисных данных Indeed PAM.
- **CoreJobs** — БД компонента Indeed PAM Core, используется для хранения задач по расписанию.
- **Idp** — БД компонента Indeed PAM IdP, используется для хранения аутентификаторов пользователей и администраторов Indeed PAM.
- **IdpJobs** — БД компонента Indeed PAM IdP, используется для хранения задач по расписанию.
- **ILS** — БД компонента Indeed Log Server, используется для хранения события Indeed PAM.

Создание баз данных

MSSQL **PostgreSQL**

1. Запустите **Microsoft SQL Management Studio**(SSMS) и выполните подключение к экземпляру Microsoft SQL Server.
2. Откройте контекстное меню пункта **Базы данных** (Databases).
3. Выберите пункт **Новая база данных** (New Database).
4. Укажите имя базы данных, например: **Core**, **CoreJobs**, **Idp**, **IdpJobs**, **ILS**.
5. Нажмите **Ок**.

Создание и назначение учетной записи для работы с хранилищем данных

MSSQL **PostgreSQL**

1. Запустите **Microsoft SQL Management Studio**(SSMS) и выполните подключение к экземпляру Microsoft SQL Server.
2. Раскройте пункт **Безопасность** (Security).

3. Откройте контекстное меню пункта **Имена для входа** (Logins).
4. Выберите пункт **Создать имя для входа** (Create login).
5. Укажите имя, например, **IPAMSQLServiceOps**.
6. Выберите тип **Проверка подлинности SQL Server** (SQL Server authentication) и заполните необходимые поля.
7. Перейдите в пункт **Сопоставление пользователей** (User Mapping).
8. Отметьте БД **Core**, **CoreJobs**, **Idp**, **IdpJobs**, **ILS**.
9. Отметьте права **db_owner**, **db_datareader** и **db_datawriter**.
10. Нажмите **Ок**.

> ⓘ **ПРИМЕЧАНИЕ**
>
> Права **db_owner** для Microsoft SQL Server требуются только для первого обращения к БД.

> ⓘ **ПРИМЕЧАНИЕ**
>
> Для работы PAM необходимо выполнить установку сертификата для инстанса MSSQL

Медиахранилище

Файловые хранилища необходимы для агрегации и долгосрочного хранения видеозаписей, снимков экрана и передаваемых в сессиях файлов.

Создание и настройка файлового хранилища

1. Выполните вход на сервер, который будет выступать в роли файлового хранилища.
2. Создайте каталог, например, **IPAMStorage**.
3. Вызовите контекстное меню каталога, выберите пункт **Предоставить доступ к** (Give access to) и **Отдельные люди** (Specific people).
4. Введите имя учетной записи, например, **IPAMStorageOps** и нажмите кнопку **Добавить** (Add).
5. Выберите **IPAMStorageOps** из списка добавленных. Измените **Уровень разрешений** (Permission level) на **Чтение и запись** (Read/Write).
6. Нажмите **Поделиться** (Share).

Серверы

Windows **Linux**

Все серверы, на которые планируется установка компонентов PAM должны находиться в одном домене, в одной сети и обращаться к одному DNS серверу.

Сервер доступа

Сервер доступа принимает удаленные подключения пользователей PAM и автоматически открывает удаленные подключения к конечным ресурсам от имени привилегированных учетных записей.

Для разворачивания роли RDS необходим "чистый" Windows Server в составе домена:

- к нему **не применяются** групповые политики, связанные с удаленным доступом
- на нем **отсутствуют** любые из компонентов роли RDS (RDCB, RDG, RDL, RDSH, RDVH, RDWA)

Разворачивание роли Remote Desktop Services

1. Откройте **Server Manager** (Диспетчер серверов), в меню **Manage** (Управление) выберите пункт **Add Roles and Features** (Добавить роли и компоненты)
2. На шаге **Installation Type** (Типы установки) выберите пункт **Remote Desktop Services installation** (Установка служб удаленных рабочих столов)
3. На шаге **Deployment type** (Типы развертывания) выберите пункт **Standard deployment** (Стандартное развертывание)
4. На шаге **Deployment scenario**(Сценарий развертывания) выберите пункт **Session-based desktop deployment** (Развертывание рабочих столов на основе сеансов)
5. На шагах **RD Connection Broker** (Посредник подключений), **RD Web Access** (Веб-доступ), **RD Session Host** (Узел сеансов) выберите имя текущего сервера
6. На шаге **Confirmation** (Подтверждение) отметьте галочкой **Restart the destination server automatically if required** (Автоматически перезапускать конечный сервер, если это потребуется), выберите **Deploy** (Развернуть) и дождитесь перезагрузки сервера.

Учетные записи для установки PAM через мастер

Перед переходом к разделу Установка убедитесь, что вы подготовили все описанные ниже учетные записи и их пароли. Без этих учетных записей установка Indeed PAM невозможна.

- Учетные записи хостов (отдельные или общая доменная учетная запись).

  <details>
  <summary>Подробнее</summary>

  Эти учетные записи будут применяться для установки компонентов PAM на хосты.

  Для хостов под управлением Windows должна быть возможность подключения по WinRM, а учетная запись должна иметь права локального администратора. Для Linux должна быть возможность подключения по SSH, а учетная запись должна иметь права root.

  Учетные данные этих записей будут сохранены в резервной копии мастера для использования при последующих операциях с мастером, таких как изменение конфигурации или обновление Indeed PAM.
  </details>

- Учетные записи балансировщиков, если планируется отказоустойчивая инсталляция.
- Учетная запись СУБД (например, **IPAMSQLServiceOps**).
- Учетная запись для доступа к медиахранилищу, если выбран тип хранилища SMB.
- Учетная запись для чтения каталога пользователей (например, **IPAMADReadOps**).
- Учетная запись администратора ролей — пользователя, которому будут выданы права на управление ролями PAM. Этот пользователь сможет выдать права на доступ к консоли управления PAM другим пользователям.
- Учетная запись для аутентификации на SMTP-сервере, если планируется выбрать Email в качестве второго фактора.

Основная на Windows

Установите Indeed PAM в соответствии с основной схемой развертывания без балансировки с сервером управления на Windows

Основная на Linux

Установите Indeed PAM в соответствии с основной схемой развертывания без балансировки с сервером управления на Linux

Отказоустойчивая на Windows

Установите Indeed PAM в соответствии с отказоустойчивой схемой развертывания с сервером управления на Windows

Отказоустойчивая на Linux

Установите Indeed PAM в соответствии с отказоустойчивой схемой развертывания с сервером управления на Linux

Основная на Windows

Компоненты Indeed PAM устанавливаются на три сервера. Этот тип установки позволяет отделить логику системы от компонентов, предоставляющих доступ. Подходит для внедрения и эксплуатации в промышленной среде. Схема развертывания без балансировки.

Перед началом установки выполните подготовку окружения.

Запуск мастера

Мастер — это веб-приложение, которое позволяет установить, обновить версию или изменить конфигурацию Indeed PAM. Мастер поставляется в составе дистрибутива PAM. Чтобы использовать мастер, потребуется запустить его в Docker-контейнере с помощью специального скрипта.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Мастер должен быть запущен на том хосте, на котором будет установлена одна из ролей PAM (сервер управления или сервер доступа), иначе попытка установки PAM приведет к ошибке.

1. Загрузите и распакуйте дистрибутив PAM на Linux-машину и перейдите в директорию дистрибутива.

2. Выполните команду:

   ```
   sudo bash run-wizard.sh
   ```

3. Дождитесь выполнения скрипта.

4. После выполнения скрипта перейдите по URL, указанному в консоли.

5. В поле **Код доступа** введите `AutenticationCode`, указанный в консоли после выполнения скрипта.
   Пример кода: `vVHyTVRyKX5pxUKM6e1ZgCWEnOdXFdOy`.

   > ⓘ **ИНФОРМАЦИЯ**

> По умолчанию код будет запрошен снова через 2 часа, то есть за это время нужно успеть выполнить всю работу.

6. Нажмите **Войти** и переходите к работе с мастером.

Сценарий

1. Выберите **Новая инсталляция PAM**.
2. Нажмите **Далее** для перехода к следующему шагу мастера.

<details>
<summary>Подробнее о сценариях</summary>

Мастер используется для выполнения одного из трех сценариев:

- **Новая инсталляция PAM** — установка Indeed PAM.
- **Обновление PAM** — обновление всех компонентов Indeed PAM до новой версии. Например, с 2.10 до 3.0. Во время обновления PAM будет недоступен. Все текущие сессии будут прерваны.
- **Изменение конфигурации PAM** — внесение изменений в текущую инсталляцию PAM. Например, изменение состава хостов. Версия PAM останется той же. Во время обновления PAM будет недоступен. Все текущие сессии будут прерваны.
</details>

Схема хостов

Под хостом понимается физический или виртуальный сервер, на котором располагаются компоненты PAM.

1. На шаге **Схема хостов** введите полное доменное имя сервера управления в поле **FQDN PAM**. Пример: pam.my-company.local.

2. Добавьте сервер управления, сервер доступа RDS, сервер доступа SSH, сервер доступа PostgreSQL. Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.

<details>
<summary>Сервер управления</summary>
</details>

1. Нажмите **Добавить хост**.
2. Для переключателя **Операционная система хоста** выберите **Windows**.
3. Включите опцию **Сервер управления**.
4. Введите IP-адрес или DNS в поле **Адрес хоста**. Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.
5. Укажите порт в поле **Порт**.
6. Выберите тип учетной записи для хоста: **общая доменная учетная запись** или **отдельная учетная запись для этого хоста**.
7. Введите **Логин** в формате UPN или SAM и **Пароль** для указанной учетной записи.
8. Нажмите **Добавить**.

▼ Сервер доступа RDS

1. Нажмите **Добавить хост**.
2. Для переключателя **Операционная система хоста** выберите **Windows**.
3. Включите опцию **Сервер доступа RDS**.
4. Введите IP-адрес или DNS в поле **Адрес хоста**. Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.
5. Укажите порт в поле **Порт**.
6. Выберите тип учетной записи для хоста: **общая доменная учетная запись** или **отдельная учетная запись для этого хоста**.
7. Введите **Логин** в формате UPN или SAM и **Пароль** для указанной учетной записи.
8. Нажмите **Добавить**.

▼ Сервер доступа SSH

1. Нажмите **Добавить хост**.
2. Для переключателя **Операционная система хоста** выберите **Linux**.
3. Включите опцию **Сервер доступа SSH**.
4. Введите IP-адрес или DNS в поле **Адрес хоста**. Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.
5. Укажите порт в поле **Порт**.
6. Выберите способ аутентификации учетной записи на хосте: **по паролю** или **по SSH-ключу**.
7. Если на предыдущем шаге выбрали **по паролю**, то введите **Логин** и **Пароль**. Если на

предыдущем шаге выбрали **по SSH-ключу**, то введите **Логин**, **Пароль sudo**, **SSH-ключ** и **Парольную фразу**.
8. Нажмите **Добавить**.

▼ Сервер доступа PostgreSQL

1. Нажмите **Добавить хост**.
2. Для переключателя **Операционная система хоста** выберите **Linux**.
3. Включите опцию **Сервер доступа PostgreSQL**.
4. Введите IP-адрес или DNS в поле **Адрес хоста**. Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.
5. Укажите порт в поле **Порт**.
6. Выберите способ аутентификации учетной записи на хосте: **по паролю** или **по SSH-ключу**.
7. Если на предыдущем шаге выбрали **по паролю**, то введите **Логин** и **Пароль**. Если на предыдущем шаге выбрали **по SSH-ключу**, то введите **Логин**, **Пароль sudo**, **SSH-ключ** и **Парольную фразу**.
8. Нажмите **Добавить**.

ИНФОРМАЦИЯ

Сервер управления и сервер доступа RDS могут располагаться на одном хосте.
Сервер доступа RDP, сервер доступа SSH, сервер доступа PostgreSQL могут располагаться на одном хосте.

3. Просмотрите таблицу хостов и проверьте правильность заполненных данных. Если требуется отредактировать данные хоста, нажмите на строку с этим хостом, внесите изменения и нажмите кнопку **Сохранить**. Если требуется удалить хост, нажмите  рядом с этим хостом.

4. Для переключателя **Балансировщик** выберите значение **Не использовать**.

5. Нажмите **Далее** для перехода к следующему шагу мастера.

Порты

> **ИНФОРМАЦИЯ**
>
> Порты компонентов PAM должны быть уникальными.

1. Укажите порты для компонентов PAM в соответствии с вашей сетевой архитектурой или оставьте значения по умолчанию.

Компонент	Порт по умолчанию
SSH Proxy	2222
RDP Proxy	3390
PostgreSQL Proxy	5432
MC/UC HTTP	80
MC/UC HTTPS	443
Gateway Service	8443

2. Нажмите **Далее** для перехода к следующему шагу мастера.

Сертификаты

На этом шаге требуется загрузить заранее подготовленные сертификаты.

1. Загрузите сертификат удостоверяющего центра без приватного ключа в формате PEM (Base64) с расширением `.crt`.
2. Загрузите сертификаты для хостов с расширением `.pfx` или wildcard-сертификат и укажите пароль.
3. Нажмите **Далее** для перехода к следующему шагу мастера.

Базы данных

1. Выберите **Тип сервера** Microsoft SQL.

2. Введите **Адрес сервера** и **Имя инстанса MSSQL**.
3. Включите опцию **Безопасное подключение к СУБД**.
4. Введите имя пользователя и пароль учетной записи для работы с базами данных.
5. Для переключателя **Ключи шифрования** выберите значение **Сгенерировать новый**.
6. Введите названия баз данных, которые вы создали на шаге подготовки к установке:
    - БД для привилегированных УЗ
    - БД для аутентификаторов пользователей PAM
    - БД для событий PAM
    - БД для задач по расписанию Core
    - БД для задач по расписанию Idp
7. Нажмите **Далее** для перехода к следующему шагу мастера.

Хранилище данных

1. Выберите **Тип хранилища** Файловая система.
2. Если требуется измените значение в поле **Корневая директория хранилища**.
3. Нажмите **Далее** для перехода к следующему шагу мастера.

▼ Другие типы хранилищ

При выборе SMB заполните поля:

- Сетевой путь
- Домен
- Имя пользователя
- Пароль

При выборе S3 заполните поля:

- Сетевой адрес S3 сервера
- Путь до корневой директории хранилища на S3-сервере
- Идентификатор ключа доступа (access key id)
- Секретный ключ доступа (secret access key)
- Регион (необязательное поле)

- Ограничение локации (необязательное поле)

Каталоги пользователей

1. Нажмите **Добавить каталог**.
2. В поле **Служба каталогов** выберите значение **Active Directory**.
3. Введите значение в поле **ID каталога**.
4. Введите значение в поле **DNS домена**.
5. Введите значение в поле **DN контейнера пользователей**.
6. Введите имя пользователя и пароль учетной записи.
7. Включите опцию **Использовать LDAPS**.
8. Если требуется, измените соответствие атрибутов пользователей и/или атрибутов групп пользователей.
9. Нажмите **Добавить**.
10. Нажмите **Далее** для перехода к следующему шагу мастера.

> ⓘ **ИНФОРМАЦИЯ**
>
> Можно добавить несколько каталогов пользователей.

Администраторы ролей

> ⓘ **ИНФОРМАЦИЯ**
>
> В мастере можно указать только одного администратора ролей.

1. Выберите из каталога учетную запись пользователя, которому будут выданы права на управление ролями PAM. Этот пользователь сможет выдать права на доступ к консоли управления PAM другим пользователям.
2. Нажмите **Далее** для перехода к следующему шагу мастера.

Аутентификация пользователей

1. Для поля **Механизм аутентификации** выберите значение **Windows**.
2. Включите опцию **Включить двухфакторную аутентификацию для всех пользователей по умолчанию**.
3. Для переключателя **Тип второго фактора** выберите значение **TOTP**.
4. Отметьте компоненты, для которых требуется включить кеширование второго фактора:
   - Management Console
   - User Console
   - Desktop Console
   - SSH Proxy
   - RDP Proxy
   - RDS Proxy
5. Если требуется, отредактируйте значение в поле **Время кеширования**.
6. Нажмите **Далее** для перехода к следующему шагу мастера.

<details>
<summary>Второй фактор аутентификации по Email</summary>

При выборе Email в качестве второго фактора заполните следующие поля:

- SMTP-сервер
- Адрес почты отправителя (адрес, с которого будет отправлено письмо)
- Порт
- Имя пользователя (логин для авторизации на сервере)
- Пароль
</details>

<details>
<summary>Аутентификация по RADIUS</summary>

При выборе RADIUS в качестве механизма аутентификации потребуется указать данные RADIUS-сервера.

1. Нажмите **Добавить сервер RADIUS**.
2. Выберите схему аутентификации. Возможные значения: `PAP`, `CHAP`, `MSCHAPV2`. Не рекомендуется выбирать схему `PAP`, т.к. она является небезопасной, потому что пароль передается в открытом виде.
3. Укажите **Адрес сервера**, **Порт** и **Секрет**.
</details>

4. Оставьте включенной опцию **Проверять атрибут Message-Authenticator**. Этот атрибут используется для обеспечения целостности пакетов и защиты их от подделки. Оставлять опцию выключенной допустимо только в том случае, если используемое программное обеспечение не поддерживает работу с этим атрибутом.
5. Выберите **Формат имени для аутентификации**. Выбирайте значение **Имя без домена** для аутентификации во FreeRadius. Выбирайте **Имя в формате SAM** или **Имя в формате UPN** для аутентификации в NPS RADIUS.

Можно указать несколько серверов RADIUS, чтобы обеспечить отказоустойчивость системы. В этом случае PAM посылает запрос серверам RADIUS последовательно, в порядке указания серверов. То есть если не удалось подключиться к первому серверу RADIUS, то PAM попытается подключиться к следующему.

Сервер доступа

1. Если требуется, измените значения полей **Максимальное время ответа агента** и **Интервал healthcheck агента**.
2. Нажмите **Далее** для перехода к следующему шагу мастера.

Логирование

1. Если требуется, измените **Уровень логирования**, максимальное количество лог-файлов сервера управления и максимальное количество лог-файлов сервера доступа.
2. Нажмите **Далее** для перехода к следующему шагу мастера.

События

1. Если требуется, добавьте Syslog-сервер.

▼ Syslog-сервер

Syslog-сервер используется для интеграции с SIEM-системой. События и текстовые логи записываются на Syslog-сервер в режиме реального времени, то есть в процессе активного удаленного подключения, а не после его завершения. Это позволяет максимально быстро

выявлять инциденты и аномалии, связанные с действиями привилегированных пользователей.

При добавлении Syslog-сервера потребуется заполнить следующие поля:
- Адрес сервера
- Сетевой протокол (TCP или RDP)
- Порт
- Формат событий (CEF или LEEF)
- Версия Syslog (RFC3164 или RFC5424)

2. Нажмите **Далее** для перехода к следующему шагу мастера.

Резервная копия

Резервная копия мастера — это зашифрованный файл, который используется для восстановления состояния мастера. Этот файл потребуется вам в будущем для обновления PAM на новую версию или для изменения конфигурации текущей версии PAM.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Сохраните файл резервной копии мастера и запомните пароль.
>
> Без этого файла и пароля к нему вы не сможете в будущем изменить конфигурацию вашей инсталляции PAM или обновить PAM до новой версии через мастер.

1. Задайте пароль для резервной копии мастера.
2. Нажмите **Скачать резервную копию**.
3. Нажмите **Далее** для перехода к следующему шагу мастера.

Установка PAM

1. Для переключателя **Способ установки** выберите значение **Из мастера**.
2. Нажмите **Установить PAM**.
3. Отслеживайте процесс установки с помощью прогресс-бара. Дождитесь завершения установки.
4. Откройте в новой вкладке консоль управления, чтобы настроить Indeed PAM. Проходите аутентификацию в консоли с теми учетными данными, которые указали на шаге Администраторы

ролей. Подробную информацию о первоначальной настройке смотрите на странице Первый запуск.

5. Нажмите **Завершить работу мастера** или выполните следующую команду в терминале:

```
sudo bash stop-wizard.sh
```

<details>
<summary>Ручная установка</summary>

При выборе ручной установки появляется возможность скачать конфигурационные файлы PAM. Эти файлы потребуется разложить по серверам самостоятельно, а также запустить скрипт развертывания PAM на каждом сервере отдельно.
</details>

Основная на Linux

Компоненты Indeed PAM устанавливаются на три сервера. Этот тип установки позволяет отделить логику системы от компонентов, предоставляющих доступ. Подходит для внедрения и эксплуатации в промышленной среде. Схема развертывания без балансировки.

Перед началом установки выполните подготовку окружения.

Запуск мастера

Мастер — это веб-приложение, которое позволяет установить, обновить версию или изменить конфигурацию Indeed PAM. Мастер поставляется в составе дистрибутива PAM. Чтобы использовать мастер, потребуется запустить его в Docker-контейнере с помощью специального скрипта.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Мастер должен быть запущен на том хосте, на котором будет установлена одна из ролей PAM (сервер управления или сервер доступа), иначе попытка установки PAM приведет к ошибке.

1. Загрузите и распакуйте дистрибутив PAM на Linux-машину и перейдите в директорию дистрибутива.

2. Выполните команду:

   ```
   sudo bash run-wizard.sh
   ```

3. Дождитесь выполнения скрипта.

4. После выполнения скрипта перейдите по URL, указанному в консоли.

5. В поле **Код доступа** введите `AutenticationCode`, указанный в консоли после выполнения скрипта.
   Пример кода: `vVHyTVRyKX5pxUKM6e1ZgCWEnOdXFdOy`.

   > ⓘ **ИНФОРМАЦИЯ**

> По умолчанию код будет запрошен снова через 2 часа, то есть за это время нужно успеть выполнить всю работу.

6. Нажмите **Войти** и переходите к работе с мастером.

Сценарий

1. Выберите **Новая инсталляция PAM**.
2. Нажмите **Далее** для перехода к следующему шагу мастера.

▼ Подробнее о сценариях

Мастер используется для выполнения одного из трех сценариев:

- **Новая инсталляция PAM** — установка Indeed PAM.
- **Обновление PAM** — обновление всех компонентов Indeed PAM до новой версии. Например, с 2.10 до 3.0. Во время обновления PAM будет недоступен. Все текущие сессии будут прерваны.
- **Изменение конфигурации PAM** — внесение изменений в текущую инсталляцию PAM. Например, изменение состава хостов. Версия PAM останется той же. Во время обновления PAM будет недоступен. Все текущие сессии будут прерваны.

Схема хостов

Под хостом понимается физический или виртуальный сервер, на котором располагаются компоненты PAM.

1. На шаге **Схема хостов** введите полное доменное имя сервера управления в поле **FQDN PAM**. Пример: pam.my-company.local.

2. Добавьте сервер управления, сервер доступа RDP, сервер доступа SSH, сервер доступа PostgreSQL. Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.

▼ Сервер управления

1. Нажмите **Добавить хост**.
2. Для переключателя **Операционная система хоста** выберите **Linux**.
3. Включите опцию **Сервер управления**.
4. Введите IP-адрес или DNS в поле **Адрес хоста**. Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.
5. Укажите порт в поле **Порт**.
6. Выберите способ аутентификации учетной записи на хосте: **по паролю** или **по SSH-ключу**.
7. Если на предыдущем шаге выбрали **по паролю**, то введите **Логин** и **Пароль**. Если на предыдущем шаге выбрали **по SSH-ключу**, то введите **Логин**, **Пароль sudo**, **SSH-ключ** и **Парольную фразу**.
8. Нажмите **Добавить**.

▼ Сервер доступа RDP

1. Нажмите **Добавить хост**.
2. Для переключателя **Операционная система хоста** выберите **Linux**.
3. Включите опцию **Сервер доступа RDP**.
4. Введите IP-адрес или DNS в поле **Адрес хоста**. Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.
5. Укажите порт в поле **Порт**.
6. Выберите способ аутентификации учетной записи на хосте: **по паролю** или **по SSH-ключу**.
7. Если на предыдущем шаге выбрали **по паролю**, то введите **Логин** и **Пароль**. Если на предыдущем шаге выбрали **по SSH-ключу**, то введите **Логин**, **Пароль sudo**, **SSH-ключ** и **Парольную фразу**.
8. Нажмите **Добавить**.

▼ Сервер доступа SSH

1. Нажмите **Добавить хост**.
2. Для переключателя **Операционная система хоста** выберите **Linux**.
3. Включите опцию **Сервер доступа SSH**.
4. Введите IP-адрес или DNS в поле **Адрес хоста**. Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.

5. Укажите порт в поле **Порт**.
6. Выберите способ аутентификации учетной записи на хосте: **по паролю** или **по SSH-ключу**.
7. Если на предыдущем шаге выбрали **по паролю**, то введите **Логин** и **Пароль**. Если на предыдущем шаге выбрали **по SSH-ключу**, то введите **Логин**, **Пароль sudo**, **SSH-ключ** и **Парольную фразу**.
8. Нажмите **Добавить**.

▼ Сервер доступа PostgreSQL

1. Нажмите **Добавить хост**.
2. Для переключателя **Операционная система хоста** выберите **Linux**.
3. Включите опцию **Сервер доступа PostgreSQL**.
4. Введите IP-адрес или DNS в поле **Адрес хоста**. Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.
5. Укажите порт в поле **Порт**.
6. Выберите способ аутентификации учетной записи на хосте: **по паролю** или **по SSH-ключу**.
7. Если на предыдущем шаге выбрали **по паролю**, то введите **Логин** и **Пароль**. Если на предыдущем шаге выбрали **по SSH-ключу**, то введите **Логин**, **Пароль sudo**, **SSH-ключ** и **Парольную фразу**.
8. Нажмите **Добавить**.

ИНФОРМАЦИЯ

Сервер управления, сервер доступа RDP, сервер доступа SSH, сервер доступа PostgreSQL могут располагаться на одном хосте.

3. Просмотрите таблицу хостов и проверьте правильность заполненных данных. Если требуется отредактировать данные хоста, нажмите на строку с этим хостом, внесите изменения и нажмите кнопку **Сохранить**. Если требуется удалить хост, нажмите  рядом с этим хостом.

4. Для переключателя **Балансировщик** выберите значение **Не использовать**.

5. Нажмите **Далее** для перехода к следующему шагу мастера.

Порты

> **ИНФОРМАЦИЯ**
>
> Порты компонентов PAM должны быть уникальными.

1. Укажите порты для компонентов PAM в соответствии с вашей сетевой архитектурой или оставьте значения по умолчанию.

Компонент	Порт по умолчанию
SSH Proxy	2222
RDP Proxy	3390
PostgreSQL Proxy	5432
MC/UC HTTP	80
MC/UC HTTPS	443
Gateway Service	8443

2. Нажмите **Далее** для перехода к следующему шагу мастера.

Сертификаты

На этом шаге требуется загрузить заранее подготовленные сертификаты.

1. Загрузите сертификат удостоверяющего центра без приватного ключа в формате PEM (Base64) с расширением `.crt`.
2. Загрузите сертификаты для хостов с расширением `.pfx` или wildcard-сертификат и укажите пароль.
3. Нажмите **Далее** для перехода к следующему шагу мастера.

Базы данных

1. Выберите **Тип сервера** PostgreSQL.
2. Введите **Адрес сервера**.
3. Включите опцию **Безопасное подключение к СУБД**.
4. Введите имя пользователя и пароль учетной записи для работы с базами данных.
5. Для переключателя **Ключи шифрования** выберите значение **Сгенерировать новый**.
6. Введите названия баз данных, которые вы создали на шаге подготовки к установке:
   - БД для привилегированных УЗ
   - БД для аутентификаторов пользователей PAM
   - БД для событий PAM
   - БД для задач по расписанию Core
   - БД для задач по расписанию Idp
7. Нажмите **Далее** для перехода к следующему шагу мастера.

Хранилище данных

1. Выберите **Тип хранилища** Файловая система.
2. Нажмите **Далее** для перехода к следующему шагу мастера.

▼ Другие типы хранилищ

При выборе SMB заполните поля:

- Сетевой путь
- Домен
- Имя пользователя
- Пароль

При выборе S3 заполните поля:

- Сетевой адрес S3 сервера
- Путь до корневой директории хранилища на S3-сервере
- Идентификатор ключа доступа (access key id)
- Секретный ключ доступа (secret access key)
- Регион (необязательное поле)

- Ограничение локации (необязательное поле)

Каталоги пользователей

1. Нажмите **Добавить каталог**.
2. В поле **Служба каталогов** выберите одно из значений: **ALD PRO**, **FreeIPA**, **OpenLDAP**.
3. Введите значение в поле **ID каталога**.
4. Введите значение в поле **DNS домена**.
5. Введите значение в поле **DN контейнера пользователей**.
6. Введите имя пользователя в формате DN (пример: 'uid=pamadmin,cn=users,cn=accounts,dc=my,dc=company') и пароль учетной записи.
7. Включите опцию **Использовать LDAPS**.
8. Если выбрали ALD PRO или FreeIPA, то выберите **Формат идентификатора пользователей и групп** — SID или GUID.
9. Если требуется, измените соответствие атрибутов пользователей и/или атрибутов групп пользователей.
10. Нажмите **Добавить**.
11. Нажмите **Далее** для перехода к следующему шагу мастера.

> **ИНФОРМАЦИЯ**
>
> Можно добавить несколько каталогов пользователей.

Администраторы ролей

> **ИНФОРМАЦИЯ**
>
> В мастере можно указать только одного администратора ролей.

1. Выберите из каталога учетную запись пользователя, которому будут выданы права на управление ролями PAM. Этот пользователь сможет выдать права на доступ к консоли управления PAM другим пользователям.
2. Нажмите **Далее** для перехода к следующему шагу мастера.

Аутентификация пользователей

1. Для поля **Механизм аутентификации** выберите значение **LDAP**.
2. Включите опцию **Включить двухфакторную аутентификацию для всех пользователей по умолчанию**.
3. Для переключателя **Тип второго фактора** выберите значение **TOTP**.
4. Отметьте компоненты, для которых требуется включить кеширование второго фактора:
   - Management Console
   - User Console
   - Desktop Console
   - SSH Proxy
   - RDP Proxy
   - RDS Proxy
5. Если требуется, отредактируйте значение в поле **Время кеширования**.
6. Нажмите **Далее** для перехода к следующему шагу мастера.

▼ Второй фактор аутентификации по Email

При выборе Email в качестве второго фактора заполните следующие поля:

- SMTP-сервер
- Адрес почты отправителя (адрес, с которого будет отправлено письмо)
- Порт
- Имя пользователя (логин для авторизации на сервере)
- Пароль

▼ Аутентификация по RADIUS

При выборе RADIUS в качестве механизма аутентификации потребуется указать данные RADIUS-сервера.

1. Нажмите **Добавить сервер RADIUS**.
2. Выберите схему аутентификации. Возможные значения: `PAP`, `CHAP`, `MSCHAPV2`. Не рекомендуется выбирать схему `PAP`, т.к. она является небезопасной, потому что пароль

передается в открытом виде.

3. Укажите **Адрес сервера**, **Порт** и **Секрет**.
4. Оставьте включенной опцию **Проверять атрибут Message-Authenticator**. Этот атрибут используется для обеспечения целостности пакетов и защиты их от подделки. Оставлять опцию выключенной допустимо только в том случае, если используемое программное обеспечение не поддерживает работу с этим атрибутом.
5. Выберите **Формат имени для аутентификации**. Выбирайте значение **Имя без домена** для аутентификации во FreeRadius. Выбирайте **Имя в формате SAM** или **Имя в формате UPN** для аутентификации в NPS RADIUS.

Можно указать несколько серверов RADIUS, чтобы обеспечить отказоустойчивость системы. В этом случае PAM посылает запрос серверам RADIUS последовательно, в порядке указания серверов. То есть если не удалось подключиться к первому серверу RADIUS, то PAM попытается подключиться к следующему.

Сервер доступа

1. Если требуется, измените значения полей **Максимальное время ответа агента** и **Интервал healthcheck агента**.
2. Нажмите **Далее** для перехода к следующему шагу мастера.

Логирование

1. Если требуется, измените **Уровень логирования**, максимальное количество лог-файлов сервера управления и максимальное количество лог-файлов сервера доступа.
2. Нажмите **Далее** для перехода к следующему шагу мастера.

События

1. Если требуется, добавьте Syslog-сервер.

▾ Syslog-сервер

Syslog-сервер используется для интеграции с SIEM-системой. События и текстовые логи записываются на Syslog-сервер в режиме реального времени, то есть в процессе активного удаленного подключения, а не после его завершения. Это позволяет максимально быстро выявлять инциденты и аномалии, связанные с действиями привилегированных пользователей.

При добавлении Syslog-сервера потребуется заполнить следующие поля:
- Адрес сервера
- Сетевой протокол (TCP или RDP)
- Порт
- Формат событий (CEF или LEEF)
- Версия Syslog (RFC3164 или RFC5424)

2. Нажмите **Далее** для перехода к следующему шагу мастера.

Резервная копия

Резервная копия мастера — это зашифрованный файл, который используется для восстановления состояния мастера. Этот файл потребуется вам в будущем для обновления PAM на новую версию или для изменения конфигурации текущей версии PAM.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Сохраните файл резервной копии мастера и запомните пароль.
>
> Без этого файла и пароля к нему вы не сможете в будущем изменить конфигурацию вашей инсталляции PAM или обновить PAM до новой версии через мастер.

1. Задайте пароль для резервной копии мастера.
2. Нажмите **Скачать резервную копию**.
3. Нажмите **Далее** для перехода к следующему шагу мастера.

Установка PAM

1. Для переключателя **Способ установки** выберите значение **Из мастера**.

2. Нажмите **Установить PAM**.
3. Отслеживайте процесс установки с помощью прогресс-бара. Дождитесь завершения установки.
4. Откройте в новой вкладке консоль управления, чтобы настроить Indeed PAM. Проходите аутентификацию в консоли с теми учетными данными, которые указали на шаге Администраторы ролей. Подробную информацию о первоначальной настройке смотрите на странице Первый запуск.
5. Нажмите **Завершить работу мастера** или выполните следующую команду в терминале:

```
sudo bash stop-wizard.sh
```

<details>
<summary>Ручная установка</summary>

При выборе ручной установки появляется возможность скачать конфигурационные файлы PAM. Эти файлы потребуется разложить по серверам самостоятельно, а также запустить скрипт развертывания PAM на каждом сервере отдельно.
</details>

Отказоустойчивая на Windows

Компоненты Indeed PAM устанавливаются на три сервера. Этот тип установки позволяет отделить логику системы от компонентов, предоставляющих доступ. Используется дополнительный сервер для организации отказоустойчивости. Подходит для внедрения и эксплуатации в промышленной среде. Схема развертывания с балансировкой.

Перед началом установки выполните подготовку окружения.

Запуск мастера

Мастер — это веб-приложение, которое позволяет установить, обновить версию или изменить конфигурацию Indeed PAM. Мастер поставляется в составе дистрибутива PAM. Чтобы использовать мастер, потребуется запустить его в Docker-контейнере с помощью специального скрипта.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Мастер должен быть запущен на том хосте, на котором будет установлена одна из ролей PAM (сервер управления или сервер доступа), иначе попытка установки PAM приведет к ошибке.

1. Загрузите и распакуйте дистрибутив PAM на Linux-машину и перейдите в директорию дистрибутива.

2. Выполните команду:

   ```
   sudo bash run-wizard.sh
   ```

3. Дождитесь выполнения скрипта.

4. После выполнения скрипта перейдите по URL, указанному в консоли.

5. В поле **Код доступа** введите `AutenticationCode`, указанный в консоли после выполнения скрипта.
   Пример кода: `vVHyTVRyKX5pxUKM6e1ZgCWEnOdXFdOy`.

   > ⓘ **ИНФОРМАЦИЯ**

> По умолчанию код будет запрошен снова через 2 часа, то есть за это время нужно успеть выполнить всю работу.

6. Нажмите **Войти** и переходите к работе с мастером.

Сценарий

1. Выберите **Новая инсталляция PAM**.
2. Нажмите **Далее** для перехода к следующему шагу мастера.

<details>
<summary>Подробнее о сценариях</summary>

Мастер используется для выполнения одного из трех сценариев:

- **Новая инсталляция PAM** — установка Indeed PAM.
- **Обновление PAM** — обновление всех компонентов Indeed PAM до новой версии. Например, с 2.10 до 3.0. Во время обновления PAM будет недоступен. Все текущие сессии будут прерваны.
- **Изменение конфигурации PAM** — внесение изменений в текущую инсталляцию PAM. Например, изменение состава хостов. Версия PAM останется той же. Во время обновления PAM будет недоступен. Все текущие сессии будут прерваны.
</details>

Схема хостов

Под хостом понимается физический или виртуальный сервер, на котором располагаются компоненты PAM.

1. На шаге **Схема хостов** введите полное доменное имя сервера управления в поле **FQDN PAM**. Пример: pam.my-company.local.

2. Добавьте сервер управления, сервер доступа RDS, сервер доступа SSH, сервер доступа PostgreSQL. Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.

<details>
<summary>Сервер управления</summary>
</details>

1. Нажмите **Добавить хост**.
2. Для переключателя **Операционная система хоста** выберите **Windows**.
3. Включите опцию **Сервер управления**.
4. Введите IP-адрес или DNS в поле **Адрес хоста**. Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.
5. Укажите порт в поле **Порт**.
6. Выберите тип учетной записи для хоста: **общая доменная учетная запись** или **отдельная учетная запись для этого хоста**.
7. Введите **Логин** в формате UPN или SAM и **Пароль** для указанной учетной записи.
8. Нажмите **Добавить**.

▼ Сервер доступа RDS

1. Нажмите **Добавить хост**.
2. Для переключателя **Операционная система хоста** выберите **Windows**.
3. Включите опцию **Сервер доступа RDS**.
4. Введите IP-адрес или DNS в поле **Адрес хоста**. Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.
5. Укажите порт в поле **Порт**.
6. Выберите тип учетной записи для хоста: **общая доменная учетная запись** или **отдельная учетная запись для этого хоста**.
7. Введите **Логин** в формате UPN или SAM и **Пароль** для указанной учетной записи.
8. Нажмите **Добавить**.

▼ Сервер доступа SSH

1. Нажмите **Добавить хост**.
2. Для переключателя **Операционная система хоста** выберите **Linux**.
3. Включите опцию **Сервер доступа SSH**.
4. Введите IP-адрес или DNS в поле **Адрес хоста**. Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.
5. Укажите порт в поле **Порт**.
6. Выберите способ аутентификации учетной записи на хосте: **по паролю** или **по SSH-ключу**.
7. Если на предыдущем шаге выбрали **по паролю**, то введите **Логин** и **Пароль**. Если на

предыдущем шаге выбрали **по SSH-ключу**, то введите **Логин**, **Пароль sudo**, **SSH-ключ** и **Парольную фразу**.
8. Нажмите **Добавить**.

▼ Сервер доступа PostgreSQL

1. Нажмите **Добавить хост**.
2. Для переключателя **Операционная система хоста** выберите **Linux**.
3. Включите опцию **Сервер доступа PostgreSQL**.
4. Введите IP-адрес или DNS в поле **Адрес хоста**. Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.
5. Укажите порт в поле **Порт**.
6. Выберите способ аутентификации учетной записи на хосте: **по паролю** или **по SSH-ключу**.
7. Если на предыдущем шаге выбрали **по паролю**, то введите **Логин** и **Пароль**. Если на предыдущем шаге выбрали **по SSH-ключу**, то введите **Логин**, **Пароль sudo**, **SSH-ключ** и **Парольную фразу**.
8. Нажмите **Добавить**.

> ⓘ **ИНФОРМАЦИЯ**
>
> Сервер управления и сервер доступа RDS могут располагаться на одном хосте.
> Сервер доступа RDP, сервер доступа SSH, сервер доступа PostgreSQL могут располагаться на одном хосте.

3. Просмотрите таблицу хостов и проверьте правильность заполненных данных. Если требуется отредактировать данные хоста, нажмите на строку с этим хостом, внесите изменения и нажмите кнопку **Сохранить**. Если требуется удалить хост, нажмите  рядом с этим хостом.

4. Для переключателя **Балансировщик** выберите значение **HAProxy**. Это балансировщик, поставляемый в составе PAM, который устанавливается и настраивается в процессе развертывания PAM. Можно указать максимум 2 балансировщика HAProxy.

> ⓘ **ИНФОРМАЦИЯ**

> При использовании стороннего балансировщика учитывайте, что потребуется настроить его самостоятельно. Убедитесь, что PAM доступен по адресу, указанному в поле FQDN PAM.

5. Добавьте балансировщик. Учитывайте, что нельзя добавить несколько балансировщиков с одинаковым адресом.

   ▼ Балансировщик

   1. Нажмите **Добавить балансировщик**.
   4. Введите IP-адрес или DNS в поле **Адрес балансировщика**.
   5. Укажите порт в поле **Порт**.
   6. Выберите способ аутентификации учетной записи на хосте: **по паролю** или **по SSH-ключу**.
   7. Если на предыдущем шаге выбрали **по паролю**, то введите **Логин** и **Пароль**. Если на предыдущем шаге выбрали **по SSH-ключу**, то введите **Логин**, **Пароль sudo**, **SSH-ключ** и **Парольную фразу**.
   8. Нажмите **Добавить**.

6. Нажмите **Далее** для перехода к следующему шагу мастера.

Порты

> ⓘ **ИНФОРМАЦИЯ**
>
> Порты компонентов PAM должны быть уникальными. Порты HAProxy должны быть уникальными.

1. Укажите порты для компонентов PAM в соответствии с вашей сетевой архитектурой или оставьте значения по умолчанию.

Компонент	Порт по умолчанию
SSH Proxy	2222
RDP Proxy	3390

Компонент	Порт по умолчанию
PostgreSQL Proxy	5432
MC/UC HTTP	80
MC/UC HTTPS	443
Gateway Service	8443

2. Укажите порты для HAProxy в соответствии с вашей сетевой архитектурой или оставьте значения по умолчанию.

HAProxy	Порт по умолчанию
HAProxy SSH	2222
HAProxy RDP	3390
HAProxy PostgreSQL	5432
HAProxy HTTP	80
HAProxy HTTPS	443

3. Нажмите **Далее** для перехода к следующему шагу мастера.

Сертификаты

На этом шаге требуется загрузить заранее подготовленные сертификаты.

1. Загрузите сертификат удостоверяющего центра без приватного ключа в формате PEM (Base64) с расширением `.crt`.
2. Загрузите сертификаты для хостов с расширением `.pfx` или wildcard-сертификат и укажите пароль.
3. Нажмите **Далее** для перехода к следующему шагу мастера.

Базы данных

1. Выберите **Тип сервера** Microsoft SQL.
2. Введите **Адрес сервера** и **Имя инстанса MSSQL**.
3. Включите опцию **Безопасное подключение к СУБД**.
4. Введите имя пользователя и пароль учетной записи для работы с базами данных.
5. Для переключателя **Ключи шифрования** выберите значение **Сгенерировать новый**.
6. Введите названия баз данных, которые вы создали на шаге подготовки к установке:
   - БД для привилегированных УЗ
   - БД для аутентификаторов пользователей PAM
   - БД для событий PAM
   - БД для задач по расписанию Core
   - БД для задач по расписанию Idp
7. Нажмите **Далее** для перехода к следующему шагу мастера.

Хранилище данных

1. Выберите **Тип хранилища** Файловая система.
2. Если требуется измените значение в поле **Корневая директория хранилища**.
3. Нажмите **Далее** для перехода к следующему шагу мастера.

▼ Другие типы хранилищ

При выборе SMB заполните поля:

- Сетевой путь
- Домен
- Имя пользователя
- Пароль

При выборе S3 заполните поля:

- Сетевой адрес S3 сервера
- Путь до корневой директории хранилища на S3-сервере
- Идентификатор ключа доступа (access key id)

- Секретный ключ доступа (secret access key)
- Регион (необязательное поле)
- Ограничение локации (необязательное поле)

Каталоги пользователей

1. Нажмите **Добавить каталог**.
2. В поле **Служба каталогов** выберите значение **Active Directory**.
3. Введите значение в поле **ID каталога**.
4. Введите значение в поле **DNS домена**.
5. Введите значение в поле **DN контейнера пользователей**.
6. Введите имя пользователя и пароль учетной записи.
7. Включите опцию **Использовать LDAPS**.
8. Если требуется, измените соответствие атрибутов пользователей и/или атрибутов групп пользователей.
9. Нажмите **Добавить**.
10. Нажмите **Далее** для перехода к следующему шагу мастера.

> ⓘ **ИНФОРМАЦИЯ**
>
> Можно добавить несколько каталогов пользователей.

Администраторы ролей

> ⓘ **ИНФОРМАЦИЯ**
>
> В мастере можно указать только одного администратора ролей.

1. Выберите из каталога учетную запись пользователя, которому будут выданы права на управление ролями PAM. Этот пользователь сможет выдать права на доступ к консоли управления PAM другим пользователям.
2. Нажмите **Далее** для перехода к следующему шагу мастера.

Аутентификация пользователей

1. Для поля **Механизм аутентификации** выберите значение **Windows**.
2. Включите опцию **Включить двухфакторную аутентификацию для всех пользователей по умолчанию**.
3. Для переключателя **Тип второго фактора** выберите значение **TOTP**.
4. Отметьте компоненты, для которых требуется включить кеширование второго фактора:
   - Management Console
   - User Console
   - Desktop Console
   - SSH Proxy
   - RDP Proxy
   - RDS Proxy
5. Если требуется, отредактируйте значение в поле **Время кеширования**.
6. Нажмите **Далее** для перехода к следующему шагу мастера.

▼ Второй фактор аутентификации по Email

При выборе Email в качестве второго фактора заполните следующие поля:

- SMTP-сервер
- Адрес почты отправителя (адрес, с которого будет отправлено письмо)
- Порт
- Имя пользователя (логин для авторизации на сервере)
- Пароль

▼ Аутентификация по RADIUS

При выборе RADIUS в качестве механизма аутентификации потребуется указать данные RADIUS-сервера.

1. Нажмите **Добавить сервер RADIUS**.
2. Выберите схему аутентификации. Возможные значения: `PAP`, `CHAP`, `MSCHAPV2`. Не рекомендуется выбирать схему `PAP`, т.к. она является небезопасной, потому что пароль

передается в открытом виде.

3. Укажите **Адрес сервера**, **Порт** и **Секрет**.
4. Оставьте включенной опцию **Проверять атрибут Message-Authenticator**. Этот атрибут используется для обеспечения целостности пакетов и защиты их от подделки. Оставлять опцию выключенной допустимо только в том случае, если используемое программное обеспечение не поддерживает работу с этим атрибутом.
5. Выберите **Формат имени для аутентификации**. Выбирайте значение **Имя без домена** для аутентификации во FreeRadius. Выбирайте **Имя в формате SAM** или **Имя в формате UPN** для аутентификации в NPS RADIUS.

Можно указать несколько серверов RADIUS, чтобы обеспечить отказоустойчивость системы. В этом случае PAM посылает запрос серверам RADIUS последовательно, в порядке указания серверов. То есть если не удалось подключиться к первому серверу RADIUS, то PAM попытается подключиться к следующему.

Сервер доступа

1. Если требуется, измените значения полей **Максимальное время ответа агента** и **Интервал healthcheck агента**.
2. Нажмите **Далее** для перехода к следующему шагу мастера.

Логирование

1. Если требуется, измените **Уровень логирования**, максимальное количество лог-файлов сервера управления и максимальное количество лог-файлов сервера доступа.
2. Нажмите **Далее** для перехода к следующему шагу мастера.

События

1. Если требуется, добавьте Syslog-сервер.

▾ Syslog-сервер

Syslog-сервер используется для интеграции с SIEM-системой. События и текстовые логи записываются на Syslog-сервер в режиме реального времени, то есть в процессе активного удаленного подключения, а не после его завершения. Это позволяет максимально быстро выявлять инциденты и аномалии, связанные с действиями привилегированных пользователей.

При добавлении Syslog-сервера потребуется заполнить следующие поля:
- Адрес сервера
- Сетевой протокол (TCP или RDP)
- Порт
- Формат событий (CEF или LEEF)
- Версия Syslog (RFC3164 или RFC5424)

2. Нажмите **Далее** для перехода к следующему шагу мастера.

Резервная копия

Резервная копия мастера — это зашифрованный файл, который используется для восстановления состояния мастера. Этот файл потребуется вам в будущем для обновления PAM на новую версию или для изменения конфигурации текущей версии PAM.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Сохраните файл резервной копии мастера и запомните пароль.
>
> Без этого файла и пароля к нему вы не сможете в будущем изменить конфигурацию вашей инсталляции PAM или обновить PAM до новой версии через мастер.

1. Задайте пароль для резервной копии мастера.
2. Нажмите **Скачать резервную копию**.
3. Нажмите **Далее** для перехода к следующему шагу мастера.

Установка PAM

1. Для переключателя **Способ установки** выберите значение **Из мастера**.

2. Нажмите **Установить PAM**.
3. Отслеживайте процесс установки с помощью прогресс-бара. Дождитесь завершения установки.
4. Откройте в новой вкладке консоль управления, чтобы настроить Indeed PAM. Проходите аутентификацию в консоли с теми учетными данными, которые указали на шаге Администраторы ролей. Подробную информацию о первоначальной настройке смотрите на странице Первый запуск.
5. Нажмите **Завершить работу мастера** или выполните следующую команду в терминале:

```
sudo bash stop-wizard.sh
```

<details>
<summary>Ручная установка</summary>

При выборе ручной установки появляется возможность скачать конфигурационные файлы PAM. Эти файлы потребуется разложить по серверам самостоятельно, а также запустить скрипт развертывания PAM на каждом сервере отдельно.
</details>

Отказоустойчивая на Linux

Компоненты Indeed PAM устанавливаются на три сервера. Этот тип установки позволяет отделить логику системы от компонентов, предоставляющих доступ. Используется дополнительный сервер для организации отказоустойчивости. Подходит для внедрения и эксплуатации в промышленной среде. Схема развертывания с балансировкой.

Перед началом установки выполните подготовку окружения.

Запуск мастера

Мастер — это веб-приложение, которое позволяет установить, обновить версию или изменить конфигурацию Indeed PAM. Мастер поставляется в составе дистрибутива PAM. Чтобы использовать мастер, потребуется запустить его в Docker-контейнере с помощью специального скрипта.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Мастер должен быть запущен на том хосте, на котором будет установлена одна из ролей PAM (сервер управления или сервер доступа), иначе попытка установки PAM приведет к ошибке.

1. Загрузите и распакуйте дистрибутив PAM на Linux-машину и перейдите в директорию дистрибутива.

2. Выполните команду:

   ```
   sudo bash run-wizard.sh
   ```

3. Дождитесь выполнения скрипта.

4. После выполнения скрипта перейдите по URL, указанному в консоли.

5. В поле **Код доступа** введите `AutenticationCode`, указанный в консоли после выполнения скрипта.
   Пример кода: `vVHyTVRyKX5pxUKM6e1ZgCWEnOdXFdOy`.

   > ⓘ **ИНФОРМАЦИЯ**

> По умолчанию код будет запрошен снова через 2 часа, то есть за это время нужно успеть выполнить всю работу.

6. Нажмите **Войти** и переходите к работе с мастером.

Сценарий

1. Выберите **Новая инсталляция PAM**.
2. Нажмите **Далее** для перехода к следующему шагу мастера.

<details>
<summary>Подробнее о сценариях</summary>

Мастер используется для выполнения одного из трех сценариев:

- **Новая инсталляция PAM** — установка Indeed PAM.
- **Обновление PAM** — обновление всех компонентов Indeed PAM до новой версии. Например, с 2.10 до 3.0. Во время обновления PAM будет недоступен. Все текущие сессии будут прерваны.
- **Изменение конфигурации PAM** — внесение изменений в текущую инсталляцию PAM. Например, изменение состава хостов. Версия PAM останется той же. Во время обновления PAM будет недоступен. Все текущие сессии будут прерваны.
</details>

Схема хостов

Под хостом понимается физический или виртуальный сервер, на котором располагаются компоненты PAM.

1. На шаге **Схема хостов** введите полное доменное имя сервера управления в поле **FQDN PAM**. Пример: pam.my-company.local.

2. Добавьте сервер управления, сервер доступа RDP, сервер доступа SSH, сервер доступа PostgreSQL. Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.

<details>
<summary>Сервер управления</summary>
</details>

1. Нажмите **Добавить хост**.
2. Для переключателя **Операционная система хоста** выберите **Linux**.
3. Включите опцию **Сервер управления**.
4. Введите IP-адрес или DNS в поле **Адрес хоста**. Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.
5. Укажите порт в поле **Порт**.
6. Выберите способ аутентификации учетной записи на хосте: **по паролю** или **по SSH-ключу**.
7. Если на предыдущем шаге выбрали **по паролю**, то введите **Логин** и **Пароль**. Если на предыдущем шаге выбрали **по SSH-ключу**, то введите **Логин**, **Пароль sudo**, **SSH-ключ** и **Парольную фразу**.
8. Нажмите **Добавить**.

▼ Сервер доступа RDP

1. Нажмите **Добавить хост**.
2. Для переключателя **Операционная система хоста** выберите **Linux**.
3. Включите опцию **Сервер доступа RDP**.
4. Введите IP-адрес или DNS в поле **Адрес хоста**. Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.
5. Укажите порт в поле **Порт**.
6. Выберите способ аутентификации учетной записи на хосте: **по паролю** или **по SSH-ключу**.
7. Если на предыдущем шаге выбрали **по паролю**, то введите **Логин** и **Пароль**. Если на предыдущем шаге выбрали **по SSH-ключу**, то введите **Логин**, **Пароль sudo**, **SSH-ключ** и **Парольную фразу**.
8. Нажмите **Добавить**.

▼ Сервер доступа SSH

1. Нажмите **Добавить хост**.
2. Для переключателя **Операционная система хоста** выберите **Linux**.
3. Включите опцию **Сервер доступа SSH**.
4. Введите IP-адрес или DNS в поле **Адрес хоста**. Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.

5. Укажите порт в поле **Порт**.
6. Выберите способ аутентификации учетной записи на хосте: **по паролю** или **по SSH-ключу**.
7. Если на предыдущем шаге выбрали **по паролю**, то введите **Логин** и **Пароль**. Если на предыдущем шаге выбрали **по SSH-ключу**, то введите **Логин**, **Пароль sudo**, **SSH-ключ** и **Парольную фразу**.
8. Нажмите **Добавить**.

▼ Сервер доступа PostgreSQL

1. Нажмите **Добавить хост**.
2. Для переключателя **Операционная система хоста** выберите **Linux**.
3. Включите опцию **Сервер доступа PostgreSQL**.
4. Введите IP-адрес или DNS в поле **Адрес хоста**. Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.
5. Укажите порт в поле **Порт**.
6. Выберите способ аутентификации учетной записи на хосте: **по паролю** или **по SSH-ключу**.
7. Если на предыдущем шаге выбрали **по паролю**, то введите **Логин** и **Пароль**. Если на предыдущем шаге выбрали **по SSH-ключу**, то введите **Логин**, **Пароль sudo**, **SSH-ключ** и **Парольную фразу**.
8. Нажмите **Добавить**.

> ⓘ **ИНФОРМАЦИЯ**
>
> Сервер управления, сервер доступа RDP, сервер доступа SSH, сервер доступа PostgreSQL могут располагаться на одном хосте.

3. Просмотрите таблицу хостов и проверьте правильность заполненных данных. Если требуется отредактировать данные хоста, нажмите на строку с этим хостом, внесите изменения и нажмите кнопку **Сохранить**. Если требуется удалить хост, нажмите  рядом с этим хостом.
4. Для переключателя **Балансировщик** выберите значение **HAProxy**. Это балансировщик, поставляемый в составе PAM, который устанавливается и настраивается в процессе развертывания PAM. Можно указать максимум 2 балансировщика HAProxy.

> **ИНФОРМАЦИЯ**
>
> При использовании стороннего балансировщика учитывайте, что потребуется настроить его самостоятельно. Убедитесь, что PAM доступен по адресу, указанному в поле FQDN PAM.

5. Добавьте балансировщик. Учитывайте, что нельзя добавить несколько балансировщиков с одинаковым адресом.

   ▼ Балансировщик

   1. Нажмите **Добавить балансировщик**.
   4. Введите IP-адрес или DNS в поле **Адрес балансировщика**.
   5. Укажите порт в поле **Порт**.
   6. Выберите способ аутентификации учетной записи на хосте: **по паролю** или **по SSH-ключу**.
   7. Если на предыдущем шаге выбрали **по паролю**, то введите **Логин** и **Пароль**. Если на предыдущем шаге выбрали **по SSH-ключу**, то введите **Логин**, **Пароль sudo**, **SSH-ключ** и **Парольную фразу**.
   8. Нажмите **Добавить**.

6. Нажмите **Далее** для перехода к следующему шагу мастера.

Порты

> **ИНФОРМАЦИЯ**
>
> Порты компонентов PAM должны быть уникальными. Порты HAProxy должны быть уникальными.

1. Укажите порты для компонентов PAM в соответствии с вашей сетевой архитектурой или оставьте значения по умолчанию.

Компонент	Порт по умолчанию
SSH Proxy	2222
RDP Proxy	3390

Компонент	Порт по умолчанию
PostgreSQL Proxy	5432
MC/UC HTTP	80
MC/UC HTTPS	443
Gateway Service	8443

2. Укажите порты для HAProxy в соответствии с вашей сетевой архитектурой или оставьте значения по умолчанию.

HAProxy	Порт по умолчанию
HAProxy SSH	2222
HAProxy RDP	3390
HAProxy PostgreSQL	5432
HAProxy HTTP	80
HAProxy HTTPS	443

3. Нажмите **Далее** для перехода к следующему шагу мастера.

Сертификаты

На этом шаге требуется загрузить заранее подготовленные сертификаты.

1. Загрузите сертификат удостоверяющего центра без приватного ключа в формате PEM (Base64) с расширением `.crt`.
2. Загрузите сертификаты для хостов с расширением `.pfx` или wildcard-сертификат и укажите пароль.
3. Нажмите **Далее** для перехода к следующему шагу мастера.

Базы данных

1. Выберите **Тип сервера** PostgreSQL.
2. Введите **Адрес сервера**.
3. Включите опцию **Безопасное подключение к СУБД**.
4. Введите имя пользователя и пароль учетной записи для работы с базами данных.
5. Для переключателя **Ключи шифрования** выберите значение **Сгенерировать новый**.
6. Введите названия баз данных, которые вы создали на шаге подготовки к установке:
   - БД для привилегированных УЗ
   - БД для аутентификаторов пользователей PAM
   - БД для событий PAM
   - БД для задач по расписанию Core
   - БД для задач по расписанию Idp
7. Нажмите **Далее** для перехода к следующему шагу мастера.

Хранилище данных

1. Выберите **Тип хранилища** Файловая система.
2. Нажмите **Далее** для перехода к следующему шагу мастера.

▼ Другие типы хранилищ

При выборе SMB заполните поля:

- Сетевой путь
- Домен
- Имя пользователя
- Пароль

При выборе S3 заполните поля:

- Сетевой адрес S3 сервера
- Путь до корневой директории хранилища на S3-сервере
- Идентификатор ключа доступа (access key id)
- Секретный ключ доступа (secret access key)

- Регион (необязательное поле)
- Ограничение локации (необязательное поле)

Каталоги пользователей

1. Нажмите **Добавить каталог**.
2. В поле **Служба каталогов** выберите одно из значений: **ALD PRO**, **FreeIPA**, **OpenLDAP**.
3. Введите значение в поле **ID каталога**.
4. Введите значение в поле **DNS домена**.
5. Введите значение в поле **DN контейнера пользователей**.
6. Введите имя пользователя в формате DN (пример: 'uid=pamadmin,cn=users,cn=accounts,dc=my,dc=company') и пароль учетной записи.
7. Включите опцию **Использовать LDAPS**.
8. Если выбрали ALD PRO или FreeIPA, то выберите **Формат идентификатора пользователей и групп** — SID или GUID.
9. Если требуется, измените соответствие атрибутов пользователей и/или атрибутов групп пользователей.
10. Нажмите **Добавить**.
11. Нажмите **Далее** для перехода к следующему шагу мастера.

> ⓘ **ИНФОРМАЦИЯ**
>
> Можно добавить несколько каталогов пользователей.

Администраторы ролей

> ⓘ **ИНФОРМАЦИЯ**
>
> В мастере можно указать только одного администратора ролей.

1. Выберите из каталога учетную запись пользователя, которому будут выданы права на управление ролями PAM. Этот пользователь сможет выдать права на доступ к консоли управления PAM другим пользователям.
2. Нажмите **Далее** для перехода к следующему шагу мастера.

Аутентификация пользователей

1. Для поля **Механизм аутентификации** выберите значение **LDAP**.
2. Включите опцию **Включить двухфакторную аутентификацию для всех пользователей по умолчанию**.
3. Для переключателя **Тип второго фактора** выберите значение **TOTP**.
4. Отметьте компоненты, для которых требуется включить кеширование второго фактора:
   - Management Console
   - User Console
   - Desktop Console
   - SSH Proxy
   - RDP Proxy
   - RDS Proxy
5. Если требуется, отредактируйте значение в поле **Время кеширования**.
6. Нажмите **Далее** для перехода к следующему шагу мастера.

▼ Второй фактор аутентификации по Email

При выборе Email в качестве второго фактора заполните следующие поля:

- SMTP-сервер
- Адрес почты отправителя (адрес, с которого будет отправлено письмо)
- Порт
- Имя пользователя (логин для авторизации на сервере)
- Пароль

▼ Аутентификация по RADIUS

При выборе RADIUS в качестве механизма аутентификации потребуется указать данные RADIUS-сервера.

1. Нажмите **Добавить сервер RADIUS**.
2. Выберите схему аутентификации. Возможные значения: `PAP`, `CHAP`, `MSCHAPV2`. Не рекомендуется выбирать схему `PAP`, т.к. она является небезопасной, потому что пароль

передается в открытом виде.

3. Укажите **Адрес сервера**, **Порт** и **Секрет**.
4. Оставьте включенной опцию **Проверять атрибут Message-Authenticator**. Этот атрибут используется для обеспечения целостности пакетов и защиты их от подделки. Оставлять опцию выключенной допустимо только в том случае, если используемое программное обеспечение не поддерживает работу с этим атрибутом.
5. Выберите **Формат имени для аутентификации**. Выбирайте значение **Имя без домена** для аутентификации во FreeRadius. Выбирайте **Имя в формате SAM** или **Имя в формате UPN** для аутентификации в NPS RADIUS.

Можно указать несколько серверов RADIUS, чтобы обеспечить отказоустойчивость системы. В этом случае PAM посылает запрос серверам RADIUS последовательно, в порядке указания серверов. То есть если не удалось подключиться к первому серверу RADIUS, то PAM попытается подключиться к следующему.

Сервер доступа

1. Если требуется, измените значения полей **Максимальное время ответа агента** и **Интервал healthcheck агента**.
2. Нажмите **Далее** для перехода к следующему шагу мастера.

Логирование

1. Если требуется, измените **Уровень логирования**, максимальное количество лог-файлов сервера управления и максимальное количество лог-файлов сервера доступа.
2. Нажмите **Далее** для перехода к следующему шагу мастера.

События

1. Если требуется, добавьте Syslog-сервер.

▾ Syslog-сервер

Syslog-сервер используется для интеграции с SIEM-системой. События и текстовые логи записываются на Syslog-сервер в режиме реального времени, то есть в процессе активного удаленного подключения, а не после его завершения. Это позволяет максимально быстро выявлять инциденты и аномалии, связанные с действиями привилегированных пользователей.

При добавлении Syslog-сервера потребуется заполнить следующие поля:
- Адрес сервера
- Сетевой протокол (TCP или RDP)
- Порт
- Формат событий (CEF или LEEF)
- Версия Syslog (RFC3164 или RFC5424)

2. Нажмите **Далее** для перехода к следующему шагу мастера.

Резервная копия

Резервная копия мастера — это зашифрованный файл, который используется для восстановления состояния мастера. Этот файл потребуется вам в будущем для обновления PAM на новую версию или для изменения конфигурации текущей версии PAM.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Сохраните файл резервной копии мастера и запомните пароль.
>
> Без этого файла и пароля к нему вы не сможете в будущем изменить конфигурацию вашей инсталляции PAM или обновить PAM до новой версии через мастер.

1. Задайте пароль для резервной копии мастера.
2. Нажмите **Скачать резервную копию**.
3. Нажмите **Далее** для перехода к следующему шагу мастера.

Установка PAM

1. Для переключателя **Способ установки** выберите значение **Из мастера**.

2. Нажмите **Установить PAM**.
3. Отслеживайте процесс установки с помощью прогресс-бара. Дождитесь завершения установки.
4. Откройте в новой вкладке консоль управления, чтобы настроить Indeed PAM. Проходите аутентификацию в консоли с теми учетными данными, которые указали на шаге Администраторы ролей. Подробную информацию о первоначальной настройке смотрите на странице Первый запуск.
5. Нажмите **Завершить работу мастера** или выполните следующую команду в терминале:

```
sudo bash stop-wizard.sh
```

<details>
<summary>Ручная установка</summary>

При выборе ручной установки появляется возможность скачать конфигурационные файлы PAM. Эти файлы потребуется разложить по серверам самостоятельно, а также запустить скрипт развертывания PAM на каждом сервере отдельно.
</details>

Настройка IIS

Добавьте запись в реестр и настройте IIS (для Windows)

Установка и настройка клиентских компонентов

Установите и настройте PamSu, PAM Agent и PAM Desktop Console

Настройка RADIUS

Отредактируйте файл конфигурации appsettings.json

Настройка подписи RDP файла

Отредактируйте файл конфигурации appsettings.json

Настройка одноразового пароля по Email

Отредактируйте файл конфигурации appsettings.json (опционально)

Включение перезапуска контейнеров сервисов прокси

Включите перезапуск контейнеров для серверов доступа RDP Proxy и SSH Proxy (опционально)

Интеграция со сторонними каталогами пользователей

Настройте интеграцию с каталогами пользователей FreeIPA, OpenLDAP, ALD Pro (опционально)

Настройка PAM для использования с NFS

Количество глав: 2

Настройка IIS

При развертывании Сервера управления на Windows Server и IIS выполните следующие действия:

1. Добавьте следующие записи реестра:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HTTP\Parameters]
"MaxFieldLength"=dword:8000 (hex)
"MaxRequestBytes"=dword:8000 (hex)
```

2. Запустите IIS на сервере управления и перейдите в раздел **Default Web Site**.
3. Откройте **Редактор конфигурации** (англ. — *Configuration Editor*) в разделе **Управление** (англ. — *Manage*).
4. Раскройте выпадающий список **Раздел:** (англ. — *Section:*) и выберите **system.webServer\security\requestFiltering**.
5. Раскройте элемент **requestLimits**, установите для параметра **maxQueryString** значение **8192**.
6. Нажмите **Применить** (англ. — *Apply*) в разделе **Действия** (англ. — *Actions*).
7. Перейдите в раздел **Default Web Site\core**.
8. Откройте **Редактор конфигурации** (англ. — *Configuration Editor*) в разделе **Управление** (англ. — *Manage*).
9. Раскройте выпадающий список **Раздел:** (англ. — *Section:*) и выберите **system.webServer\serverRuntime**.
10. Установите для параметра **uploadReadAheadSize** значение **1048576**.
11. Нажмите **Применить** (англ. — *Apply*) в разделе **Действия** (англ. — *Actions*).
12. Перезагрузите сервер.

Установка и настройка клиентских компонентов

PamSu

Компонент PamSu позволяет пользователям Indeed PAM запускать команды с правами root, используя пароль своей собственной учетной записи пользователя Active Directory.

Установка выполняется вручную на Linux-ресурсах, где необходимо запускать команды с правами root.

Установка PamSu

Компоненты расположены в папке: **IndeedPAM_3.0_RU\indeed-pam-tools\pamsu**.

> ⓘ **ПРИМЕЧАНИЕ**
>
> Установка утилиты PamSu выполняется на ресурсы ОС *nix.

Загрузите установочный пакет на ресурс и выполните команду:

Установка на Debian-based ОС

```
$ sudo dpkg -i Indeed.PAM.PamSu*.deb
```

Установка на RedHat-based ОС

```
$ sudo rpm -i Indeed.PAM.PamSu*.rpm
```

Настройка PamSu

На ресурсе необходимо настроить доверие сертификату веб-сервера core и idp. Проверить корректность работы с сертификатами можно выполнив команду:

```
```

```
$ curl https://pam.indeed-id.local
```

Откройте файл /etc/pamsu.conf в любом редакторе с правами локального администратора, укажите настройки idp_url, api_url, log_path и log_level:

- **idp_url** — адрес idp
- **core_url** — адрес core
- **log_path** — путь к каталогу с файлами логов
- **log_level** — уровень логирования, может принимать значения INFO, WARN, ERROR, FATAL

```
Set idp_url https://pam.indeed-id.local/idp
Set core_url https://pam.indeed-id.local/core
Set log_path /var/log
Set log_level INFO
```

На некоторых системах ssh server не разрешает по умолчанию переменные окружения **LC_***. Для корректной работы приложения следует в файле /etc/ssh/sshd_config добавить строку **AcceptEnv LC_PAM_USER LC_PAM_SESSION_ID**, либо маской **LC_***.

> ⓘ **ПРИМЕЧАНИЕ**
>
> Для разрешения выполнения команды pamsu необходимо включить в политике, в разделе **SSH** опцию **Разрешить выполнять pamsu**.

Indeed PAM Agent

Indeed PAM Agent следует устанавливать непосредственно на ресурсы для включения возможности текстового логирования RDP сессий.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> При отсутствии агента на ресурсе и включении опции сохранения текстовых логов в Политике подключений пользовательская **сессия завершится автоматически через минуту.**

После установки Indeed PAM Agent потребуется выполнить перезагрузку или повторный вход в ОС. Дополнительная настройка не требуется.

Indeed PAM Desktop Console

Настройка Indeed Pam Desktop Console для доменных машин

1. Скопируйте содержимое папки **indeed-pam-tools\desktop-console\PolicyDefinitions** на контроллер домена в каталог **C:\Windows\sysvol\domain\policies\PolicyDefinitions**
2. На контроллере домена запустите оснастку **Управление групповой политикой** (Group Policy Management Console)
3. Выберите необходимый объект групповой политики, перейдите в раздел **Computer Configuration\Policies\Administrative Templates\Indeed PAM\General** (Конфигурация компьютера\Политики\Административные шаблоны\Indeed PAM\Общие)
4. Включите и настроите **PAM connection settings** (Настройки подключения с PAM)
5. Обновить групповые политики на клиентском ПК

Настройка для машин, к которым не применяются доменные политики

1. Скопируйте содержимое папки **indeed-pam-tools\desktop-console\PolicyDefinitions** в каталог **C:\Windows\PolicyDefinitions**
2. Запустите редактор локальной групповой политики **gpedit.msc**
3. Перейдите в раздел **Computer Configuration\Policies\Administrative Templates\Indeed PAM\General** (Конфигурация компьютера\Политики\Административные шаблоны\Indeed PAM\Общие)
4. Включите и настроите **PAM connection settings** (Настройки подключения с PAM)

Настройка записи событий в Syslog

Windows **Linux**

1. Перейдите в каталог **C:\inetpub\wwwroot\ls\targetConfigs**, создайте копию файла **sampleSyslog.config** и переименуйте ее в **Pam.Syslog.config**, затем отредактируйте `<Settings> … </Settings>` в соответствии с настройками ниже:
    - **HostName** — имя Syslog-сервера
    - **Port** — порт Syslog-сервера
    - **Protocol** — тип подключения к Syslog-серверу: TCPoverTLS, TCP, UDP

- **Format** — формат логов: Plain, CEF, LEEF
- **SyslogVersion** — спецификация протокола: RFC3164, RFC5424

C:\inetpub\wwwroot\ls\targetConfigs

```
<Settings HostName="localhost" Port="5081" Protocol="TCP" Format="CEF"
SyslogVersion="RFC3164" />
```

2. В файле **C:\inetpub\wwwroot\ls\clientApps.config** отредактируйте секцию `pam` для работы с файлом **Pam.Syslog.config** — добавьте новый `TargetId` для `WriteTarget`:

C:\inetpub\wwwroot\ls\clientApps.config

```
1  <Application Id="pam" SchemaId="Pam.Schema">
2    <ReadTargetId>Pam.TargetDb</ReadTargetId>
3    <WriteTargets>
4      <TargetId>Pam.TargetDb</TargetId>
5      <TargetId>Pam.Syslog</TargetId>
6    </WriteTargets>
7    <AccessControl>
8      <!--<CertificateAccessControl CertificateThumbprint="001122...AA11"
   Rights="Read" />-->
9    </AccessControl>
10 </Application>
```

3. Далее в этом же файле в секции `Targets` добавьте новый элемент:

C:\inetpub\wwwroot\ls\clientApps.config

```
1  <Targets>
2    ...
3    <Target Id="Pam.TargetDb" Type="mssql"/>
4    <Target Id="Pam.Syslog" Type="syslog"/>
5  </Targets>
```

В `Target Id="Pam.TargetDb"` пропишите `Type` в зависимости от используемой БД: `mssql` или `pgsql`.

Настройка RADIUS

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Все URL указываются в нижнем регистре.
>
> Формат JSON не допускает наличия комментариев в файле, поэтому необходимо удалить строки, начинающиеся с символов "//".

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> После внесения изменений в файл конфигурации необходимо перезагрузить пул приложений IdP в IIS Manager.

Перейдите в каталог **C:\inetpub\wwwroot\idp** и отредактируйте файл **appsettings.json**.

Секция IdentitySettings

- **DirectoryMechanism** — механизм работы аутентификации.
- **Authentication** — параметр указывает поставщиков аутентификации в IDP.

Секция IdentitySettings в конфигурационном файле appsettings.json

```
"IdentitySettings": {
...
"DirectoryMechanism": "Radius",
"Authentication": "Local",
...
}
```

Секция Radius

- **AuthenticationScheme** — схема аутентификации в RADIUS. Возможные значения: 'PAP', 'CHAP', 'MSCHAPV2'. Схема PAP является небезопасной, потому что пароль передается в открытом виде.

- **AuthenticationUserName** — формат имени для аутентификации.

Возможные значения:

  - NameWithoutDomain — имя без домена (для аутентификации в FreeRadius).
  - SamCompatibleName — имя в формате INDEED\\user.
  - PrincipalName — имя в формате user@indeed.domain.

- **Secret** — секрет для дополнительной аутентификации компонента.
- **Timeout** — время ожидания ответа от сервера RADIUS.
- **RemoteEndpoint:**
  - **Address** — адрес сервера RADIUS для подключения.
  - **Port** — адрес сервера RADIUS для подключения (по умолчанию 1812).

Секция Radius в конфигурационном файле appsettings.json (один сервер RADIUS)

```
"Radius": {
  "AuthenticationScheme": "MSCHAPV2",
  "AuthenticationUserName": "PrincipalName",

"Secret":"ENCRYPTED_CfDJ8MPJ7V58kgpLvtoHgdiuk5VKMK_hf3r437uZdHjdZAfve5wtVvgDZPjjDm7bgjC
  "Timeout": 10,
  "RemoteEndpoint": {
    "Address": "PAM_RADIUS_SERVER_1",
    "Port": 1812
  }
```

Можно указать несколько серверов RADIUS, чтобы обеспечить отказоустойчивость системы. В этом случае PAM посылает запрос серверам RADIUS последовательно, в порядке указания серверов в конфигурационном файле. То есть если не удалось подключиться к первому серверу RADIUS, то PAM попытается подключиться к следующему.

Секция Radius в конфигурационном файле appsettings.json (два сервера RADIUS)

```
"Radius": {
  "Timeout": 10,
  "RemoteEndpoints": [
    {
      "Address": "10.11.4.28",
      "Port": 1812,
```

```
      "Secret": "123",
      "AuthenticationScheme": "MSCHAPV2",
      "AuthenticationUserName": "PrincipalName"
    },
    {
      "Address": "10.11.4.128",
      "Port": 1812,
      "Secret": "123",
      "AuthenticationScheme": "MSCHAPV2",
      "AuthenticationUserName": "PrincipalName"
    }
  ]
},
```

Настройка подписи RDP файла

Включение подписи RDP файла

Чтобы включить подпись RDP-файла, требуется отредактировать раздел `Rdp` файла конфигурации Core, который находится по пути:

C:\inetpub\wwwroot\core — для Windows

```
"Rdp": {
   "UseRemoteApp": false,
   "SignRdpFile": true,
   "Certificate": "16c214ba7dec702a7ce5e4ac727502b0c0d448e2",
   "Password": ""
 },
```

/etc/indeed/indeed-pam/core — для Linux

```
"Rdp": {
   "UseRemoteApp": false,
   "SignRdpFile": true,
   "Certificate": "/etc/",
   "Password": "1234"
 },
```

Секция Rdp

- `SignRdpFile` — включение подписи RDP-файла.
- `Certificate` — отпечаток сертификата или путь до самого сертификата.
- `Password` — пароль сертификата. Заполняется, если в параметре `Certificate` был указан путь до сертификата.

После редактирования файла конфигурации требуется перезапустить компонент Core.

Windows

Перезапустить IIS

Linux

Перейти в папку **/etc/indeed/indeed-pam**:

```
cd /etc/indeed/indeed-pam
```

Перезапустить компонент Indeed PAM Core:

```
sudo docker compose -f docker-compose.management-server.yml up -d core --force-recreate
```

или

```
sudo docker-compose -f docker-compose.management-server.yml up -d core --force-recreate
```

Настройка сертификата

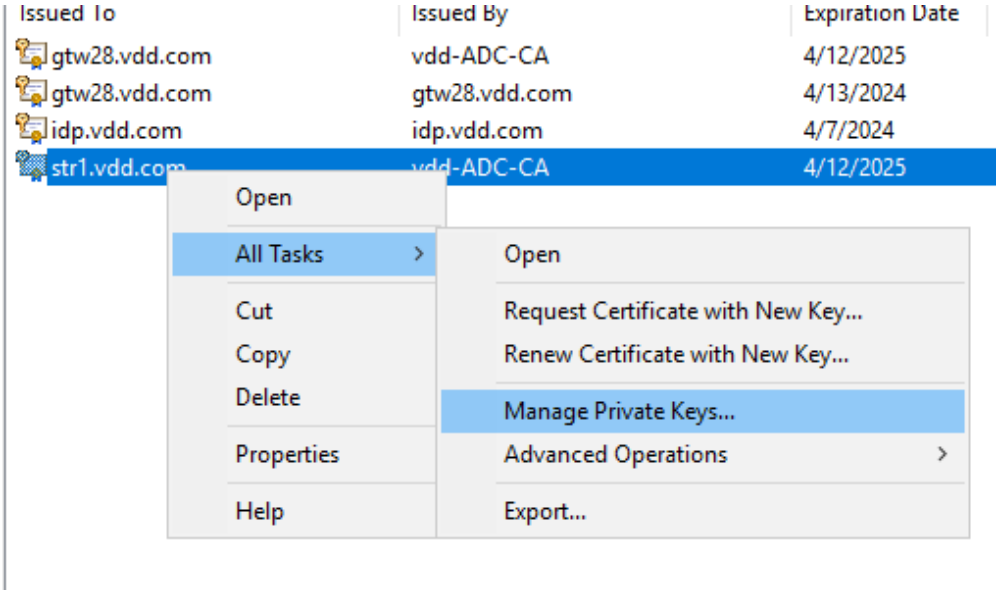
Для включения подписи RDP-файла требуется сертификат, выданный удостоверяющим центром сертификации.

> ⓘ **ПРИМЕЧАНИЕ**
>
> Все действия, описанные ниже, проходят на сервере управления с установленным компонентом Core.

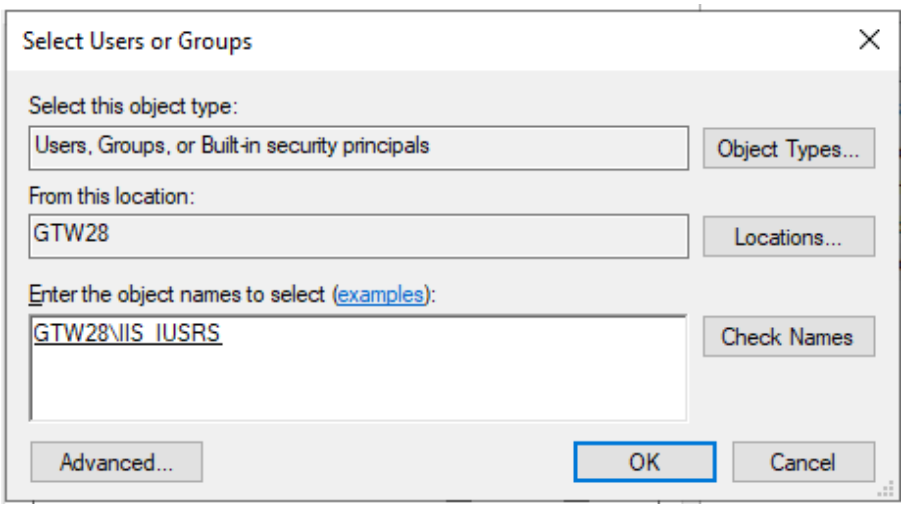
Windows с отпечатком

1. Добавьте сертификат в личное хранилище компьютера.

2. Откройте меню сертификата **Все задачи** (All Tasks) → **Управление закрытыми ключами** (Manage Private Keys...).



3. Нажмите **Добавить...** (Add...). В открывшемся окне нажмите **Размещение...** (Locations...), выберите **локальный компьютер** → **ОК**.
4. В поле введите имя IIS_IUSRS → **ОК**.



5. Отредактируйте файл конфигурации, указав отпечаток сертификата без пароля.

Linux с импортированием ключа формате PFX

1. Импортируйте в папку **/etc/indeed/indeed-pam/keys/rdp-sign.pfx** сертификат в формате PFX с приватным ключом и паролем.
2. Отредактируйте файл конфигурации, указав путь к сертификату и пароль.
3. Отредактируйте файл **/etc/indeed/indeed-pam/docker-compose.management-server.yml** добавив строчку `./keys/rdp-sign.pfx:/etc/indeed/indeed-pam/keys/rdp-sign.pfx` в разделе `core` → `volumes` для проброса сертификата в контейнер:

```
volumes:
  - ./core/events:/var/lib/indeed/indeed-pam/events
  - ./core/appsettings.json:/app/appsettings.json:ro
  - ./keys/shared/protector:/etc/indeed/indeed-pam/keys/shared/protector:ro
  - ./keys/core:/etc/indeed/indeed-pam/keys/core:ro
  - ./ca-certificates:/usr/local/share/ca-certificates:ro
  - ./logs/core:/app/logs
  - ./keys/rdp-sign.pfx:/etc/indeed/indeed-pam/keys/rdp-sign.pfx
```

Настройка одноразового пароля по Email

Данная функция позволяет получать второй фактор через почту. Почта берется из данных учетной записи в Active Directory.

На Windows-сервере — перейдите в каталог **C:\inetpub\wwwroot\idp** и отредактируйте файл **appsettings.json**.

На Linux-сервере — перейдите в каталог **/etc/indeed/indeed-pam/idp** и отредактируйте файл **appsettings.json**.

Поменяйте `TOTP` на `EMAIL`.

Секция IdentitySettings

```
"IdentitySettings": {
  ...
  "SecondFaType": "TOTP",
  ...
}
```

Секция Smtp

```
"Smtp": {
  "Address": "PAM_SMTP_ADDRESS",
  "Port": 587,
  "SenderAddress": "PAM_SMTP_SENDER_ADDRESS",
  "Username": "PAM_SMTP_USERNAME",
  "Password": "",
  "EncryptionMethod": "TLS"
  "AllowedSslProtocols": "Tls12,Tls13"
}
```

- `Address` — адрес SMTP сервера.
- `Port` — порт SMTP сервера.
- `SenderAddress` — адрес, с которого будет отправлено письмо.

- `Username` — логин для авторизации на сервере.
- `Password` — пароль для авторизации на сервере(шифруется).
- `EncryptionMethod` — метод шифрования, поддерживается только TLS.
- `AllowedSslProtocols` — поддерживаемые версии TLS.

Включение перезапуска контейнеров сервисов прокси

Docker-контейнерам SSH Proxy и RDP Proxy требуется периодический перезапуск (ротация) для устранения эффектов утечки памяти, потоков и дескрипторов. В Indeed PAM это реализовано специальным скриптом, который запускается автоматически по расписанию. Остановка работы PAM при этом не происходит (сессии пользователей не прерываются).

По умолчанию перезапуск выключен. Чтобы его включить, нужно изменить значение параметра в файле конфигурации и перезапустить сервер доступа.

Включение перезапуска в файле конфигурации

1. Откройте файл ./scripts/ansible/vars.yml.
2. В секции `proxy_recycling` поменяйте значение параметра `enabled` с `false` на `true`.
3. Переходите к перезапуску сервера доступа.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> При использовании на сервере доступа SELinux в режиме Enforcing вам потребуется вручную добавить контекст для скрипта, вы увидите сообщение об этом:
>
> ```
> TASK [Warn about SELinux mode] ************************
>
> msg:
>
> 'Warning: SELinux is in enforcing mode. Add script context manually:'
> semanage fcontext -a -t bin_t /etc/indeed/indeed-pam/scripts/recycle-proxy.sh &&
> restorecon -Fv /etc/indeed/indeed-pam/scripts/recycle-proxy.sh
> ```
>
> Поэтому выполните следующую команду:

```
semanage fcontext -a -t bin_t /etc/indeed/indeed-pam/scripts/recycle-proxy.sh &&
restorecon -Fv /etc/indeed/indeed-pam/scripts/recycle-proxy.sh
```

Дополнительные настройки

В файле ./scripts/ansible/vars.yml, в секции `proxy_recycling` есть еще несколько параметров. Укажите их значения (опционально) или используйте значения по умолчанию.

- `replicas` — количество Master-реплик (активных реплик, которые принимают соединения). По умолчанию 1.
- `proxies` — типы прокси, для которых будет выполняться перезапуск. Представляет из себя массив. По умолчанию [rdp,ssh].
- `rotation_hours` — время ротации реплик в часах. По умолчанию 168.
- `session_hours` — максимальная длительность сессии в часах для реплики в состоянии `DRAIN` (когда сервер не принимает новые соединения, но обрабатывает существующие). По умолчанию 24.

Перезапуск сервера доступа

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Запускайте команды из папки /etc/indeed/indeed-pam.

Для перезапуска компонентов сервера доступа Indeed PAM используйте следующие команды:

```
sudo docker compose -f docker-compose.access-server.yml down
sudo docker compose -f docker-compose.access-server.yml up -d
```

или

```
sudo docker-compose -f docker-compose.access-server.yml down
sudo docker-compose -f docker-compose.access-server.yml up -d
```

Пример перезапуска компонента RDP Proxy

```
sudo docker compose -f docker-compose.access-server.yml up -d Pam.RdpProxy.Service --
force-recreate
```

или

```
sudo docker-compose -f docker-compose.access-server.yml up -d Pam.RdpProxy.Service --
force-recreate
```

Пример перезапуска компонента SSH Proxy

```
sudo docker compose -f docker-compose.access-server.yml up -d Pam.SshProxy.Service --
force-recreate
```

или

```
sudo docker-compose -f docker-compose.access-server.yml up -d Pam.SshProxy.Service --
force-recreate
```

Интеграция со сторонними каталогами пользователей

На этой странице описано, как настроить интеграцию продукта Indeed PAM с каталогами пользователей Active Directory, FreeIPA, OpenLDAP и ALD Pro.

Для изменения параметров чтения каталога пользователей требуется отредактировать секцию `UserCatalog` в конфигурационных файлах Core и Idp.

Путь до файла конфигурации Core:

Windows	C:\inetpub\wwwroot\core\appsettings.json
Linux	/etc/indeed/indeed-pam/core/appsettings.json

Путь до файла конфигурации IdP:

Windows	C:\inetpub\wwwroot\idp\appsettings.json
Linux	/etc/indeed/indeed-pam/idp/appsettings.json

Настройка интеграции с Active Directory

Файлы конфигурации изначально содержат настройки для интеграции с Active Directory, дополнительных изменений не требуется.

Настройка поиска пользователей в группе безопасности

Для настройки поиска пользователей из определенной группы безопасности требуется настроить параметр `CatalogFilter`.

Пример настройки параметра для одной группы безопасности

```
"CatalogFilter": "memberOf=cn=Admins,CN=Builtin,DC=vdd,DC=com"
```

Пример настройки для нескольких групп безопасности

```
"CatalogFilter": "(|(memberOf=cn=Admins,CN=Builtin,DC=vdd,DC=com)
(memberOf=cn=PrivelledgeAccounts,OU=Groups,DC=vdd,DC=com)
(memberOf=cn=Admins1,OU=PAMUsers,DC=vdd,DC=com))"
```

Параметр `ContainerPath` также должен быть заполнен, т.к. считываться будут только те пользователи, которые состоят в OU, который вы указали в значении параметра `CatalogFilter`.

▼ Пример заполненной секции UserCatalog с указанием группы безопасности

```
"UserCatalog": {
  "RootProvider": "ad1",
  "Providers": {
    "Ldap": [
      {
        "Id": "ad1",
        "ConnectorType": "Ldap",
        "LdapServerType": "ActiveDirectory",
        "Domain": "indeed.test",
        "Port": 636,
        "AuthType": "Basic",
        "SecureSocketLayer": true,
        "ContainerPath": "OU=UsersPAM,DC=indeed,DC=test",
        "CatalogFilter":
"memberOf=cn=SecurityGroup,OU=PAMUsers,DC=indeed,DC=test",
        "UserName": "IPAMADReadOps@indeed.test",
        "Password": "qwe123",
        "UserMapRules": {
          "Settings": [
            {
              "Category": "person",
              "Class": "user"
            }
          ]
        }
      }
    ]
```

```
  }
}
```

Дополнительную информацию по настройке параметра `CatalogFilter` можно прочитать в документации Microsoft.

Настройка интеграции с FreeIpa или AldPro

Для настройки интеграции с каталогом пользователей FreeIPA или AldPro пользователи каталога должны иметь следующие атрибуты:

- `entryUUID` или `ipaUniqueID`
- `cn`
- `entryDn`
- `ipaNTSecurityIdentifier`
- `krbPrincipalName`
- `uid`

▼ Пример заполненной секции UserCatalog для каталога пользователей FreeIPA или AldPro

```
{
  "Id": "ad",
  "ConnectorType": "Ldap",
  "LdapServerType": "FreeIpa", //Заменить на AldPro при настройке на AldPro
  "Domain": "ald.sup", //Имя домена или конкретного контроллера
  "Port": 389, //389 для подключения по LDAP, 636 для подключения по LDAPS
  "AuthType": "Basic",
  "SecureSocketLayer": false,//false для подключения по LDAP, true для подключения по LDAPS
  "ContainerPath": "dc=ald,dc=sup", //Путь до контейнера пользователей
  "UserName": "uid=pamread,cn=users,cn=accounts,dc=ald,dc=sup", //Учетные данные для доступа к домену. Должны быть в формате distigushedName, УЗ должна иметь права на чтение необходимых атрибутов
  "Password": "Q1w2e3r4", //Пароль УЗ для доступа к домену
  "GroupMapRules": {
    "Settings": [
     {
      "Category": "",
```

```
      "Class": "ipantgroupattrs"
      }
    ],
    "Attributes": {
      "Id": "ipaUniqueID",
      "Name": "cn",
      "SamAccountName": "cn",
      "CanonicalName": "cn",
      "DistinguishedName": "entryDn",
      "SidBytes": "ipaNTSecurityIdentifier"
     }
    },
    "UserMapRules": {
      "Settings": [
       {
        "Category": "",
        "Class": "person"
       }
      ],
      "Attributes": {
        "Id": "ipaUniqueID",
        "Name": "cn",
        "PrincipalName": "krbPrincipalName",
        "SamAccountName": "uid",
        "DistinguishedName": "entryDn",
        "SidBytes": "ipaNTSecurityIdentifier",
        "ThumbnailPhoto": "jpegPhoto",
        "JpegPhoto": "jpegPhoto"
       }
    }
}
```

Если у пользователей каталога есть атрибут `entryUUID` и нет атрибута `ipaUniqueID`, то в секциях `GroupMapRules` и `UserMapRules` в разделе `Attributes` необходимо удалить параметр `"Id": "ipaUniqueID"`.

Настройка интеграции с OpenLDAP

Для настройки интеграции с каталогом пользователей OpenLDAP пользователи каталога должны иметь следующие атрибуты:

- `cn`

- `entryDn`
- `uid`

▼ Пример заполненной секции UserCatalog для каталога пользователей OpenLDAP

```
{
  "Id": "oldap",
  "ConnectorType": "Ldap",
  "LdapServerType": "OpenLdap",
  "Domain": "oldap.local", //Имя домена или конкретного контроллера
  "Port": 389, //389 для подключения по LDAP, 636 для подключения по LDAPS
  "AuthType": "Basic",
  "SecureSocketLayer": false, //false для подключения по LDAP, true для подключения по LDAPS
  "ContainerPath": "DC=oldap,DC=local", //Путь до контейнера пользователей
  "UserName": "cn=IPAMADReadOps,dc=oldap,dc=local", //Учетные данные для доступа к домену. Должны быть в формате distigushedName, УЗ должна иметь права на чтение необходимых атрибутов
  "Password": "QWEqwe123", //Пароль УЗ для доступа к домену
  "GroupMapRules": {
    "Settings": [
      {
        "Category": "",
        "Class": "groupOfUniqueNames"
      }
    ],
    "Attributes": {
      "Name": "cn",
      "SamAccountName": "cn",
      "CanonicalName": "cn",
      "DistinguishedName": "entryDn",
      "Members": "uniqueMember"
    }
  },
  "UserMapRules": {
    "Settings": [
      {
        "Category": "",
        "Class": "inetOrgPerson"
      }
    ],
    "Attributes": {
      "Name": "cn",
```

```
        "SamAccountName": "uid",
        "DistinguishedName": "entryDn",
        "ThumbnailPhoto": "photo",
        "JpegPhoto": "photo"
      }
    }
}
```

Настройка интеграции с несколькими каталогами пользователей

Для настройки интеграции с несколькими каталогами пользователей выполните следующие действия:

1. Поменяйте значение параметра `RootProvider` на "orUCP".
2. В секции `Ldap` перечислите через запятую каталоги пользователей, с которыми необходима интеграция. Id провайдеров не должны совпадать. Id провайдеров, с которыми до этого работал PAM, не должны меняться.
3. Добавьте секцию `Or` из примера ниже, в которой пропишите Id секций провайдеров.

▼ Пример секции UserCatalog, настроенной на работу с двумя каталогами пользователей

```
"UserCatalog": {
    "RootProvider": "orUCP",
    "Providers": {
      "Ldap": [
        {
          "Id": "ad",
          "ConnectorType": "Ldap",
          "LdapServerType": "ActiveDirectory",
          "Domain": "indeed.test",
          "Port": 636,
          "AuthType": "Basic",
          "SecureSocketLayer": true,
          "ContainerPath": "OU=UsersPAM,DC=indeed,DC=test",
          "UserName": "IPAMADReadOps@indeed.test",
          "Password": "qwe123",
          "UserMapRules": {
            "Settings": [
```

```
            {
              "Category": "person",
              "Class": "user"
            }
          ]
        }
      },
      {
        "Id": "ad2",
        "ConnectorType": "Ldap",
        "LdapServerType": "ActiveDirectory",
        "Domain": "indeed.test",
        "Port": 636,
        "AuthType": "Basic",
        "SecureSocketLayer": true,
        "ContainerPath": "OU=UsersPAM,DC=indeed,DC=test",
        "UserName": "IPAMADReadOps@indeed.test",
        "Password": "qwe123",
        "UserMapRules": {
          "Settings": [
            {
              "Category": "person",
              "Class": "user"
            }
          ]
        }
      },
      {
        "Id": "ipa",
        "ConnectorType": "Ldap",
        "LdapServerType": "FreeIpa",
        "Domain": "ipa.redos",
        "Port": 389,
        "AuthType": "Basic",
        "SecureSocketLayer": false,
        "ContainerPath": "DC=ipa,DC=redos",
        "UserName": "uid=IPAMADReadOps,cn=users,cn=accounts,dc=ipa,dc=redos",
        "Password": "qwe123",
        "GroupMapRules": {
          "Settings": [
            {
              "Category": "",
              "Class": "ipantgroupattrs"
            }
          ],
          "Attributes": {
```

```
                "Name": "cn",
                "SamAccountName": "cn",
                "CanonicalName": "cn",
                "DistinguishedName": "entryDn",
                "SidBytes": "ipaNTSecurityIdentifier"
              }
            },
            "UserMapRules": {
                "Settings": [
                  {
                    "Category": "",
                    "Class": "person"
                  }
                ],
                "Attributes": {
                    "Name": "cn",
                    "PrincipalName": "krbPrincipalName",
                    "SamAccountName": "uid",
                    "DistinguishedName": "entryDn",
                    "SidBytes": "ipaNTSecurityIdentifier",
                    "ThumbnailPhoto": "jpegPhoto",
                    "JpegPhoto": "jpegPhoto"
                }
            }
          }
        ],
        "Or": [
          {
            "Id": "orUCP",
            "Providers": {
              "ad": {"IgnoreExceptions": true},
              "ad2": {"IgnoreExceptions": true},
              "ipa": {"IgnoreExceptions": true}
            }
          }
        ]
      }
    }
```

Подготовка NFS-медиахранилища

Выполните описанные здесь шаги на сервере NFS

Настройка PAM для работы с NFS

Выполните описанные здесь шаги на сервере PAM

Подготовка NFS-медиахранилища

RPM DEB

1. **Установите необходимые пакеты:**

```
sudo dnf install nfs-utils
```

2. **Запустите службы NFS-сервера:**

```
sudo systemctl start nfs-server.service
sudo systemctl enable nfs-server.service
sudo systemctl status nfs-server.service
```

3. **Создайте файловые системы для экспорта или обмена на сервере NFS и задайте владельца и группу:**

```
sudo mkdir -p /mnt/data_storage/
sudo chown -R 23041:23041 /mnt/data_storage/
```

4. **Экспортируйте файловые системы в файл конфигурации сервера NFS — `/etc/exports`, чтобы определить локальные физические файловые системы, доступные для клиентов NFS:**

Шаблон пути
/mnt/data_storage/ <IP-адрес_клиента/сеть/маска/*> (rw,sync,all_squash,anonuid=23041,anongid=23041)

Пример пути
/mnt/data_storage/ 192.168.131.0/24(rw,sync,all_squash,anonuid=23041,anongid=23041)

5. **После внесения изменений, чтобы они вступили в силу, выполните команду:**

```
sudo exportfs -arv
```

6. **Обход встроенных утилит безопасности:**

   В дистрибутивах на основе RPM (например, CentOS, RHEL, Fedora) утилита безопасности SELinux может блокировать доступ к NFS, если он не настроен должным образом.

   - Чтобы временно отключить SELinux для тестирования:

     ```
     sudo setenforce 0
     ```

   - Чтобы настроить SELinux для работы с NFS:

     ```
     sudo setsebool -P nfs_export_all_rw 1
     sudo setsebool -P nfs_export_all_ro 1
     ```

   Также убедитесь, что firewall не блокирует порты, необходимые для работы NFS. Откройте их:

```
sudo firewall-cmd --permanent --add-service=nfs
sudo firewall-cmd --permanent --add-service=rpc-bind
sudo firewall-cmd --permanent --add-service=mountd
sudo firewall-cmd --reload
```

Настройка PAM для работы с NFS

Перед настройкой PAM для работы с NFS необходимо выполнить установку и настройку NFS-медиахранилища.

Linux **Windows**

1. **Создайте папку для монтирования медиахранилища на сервере.** Также можете использовать готовую папку, например, /etc/indeed/indeed-pam/media-temp.

```
sudo mkdir -p /mnt/pamstorage/
```

2. **Установите клиент для монтирования NFS:**

   - **RPM:**

```
sudo yum install nfs-utils
```

   - **DEB:**

```
sudo apt install nfs-common
```

3. **Выполните монтирование хранилища:**

Шаблон команды

```
sudo mount -t nfs <fqdn_or_ip_nfs_server>:/путь/до/медихранилища /путь/до/папки/монтирования
```

Пример команды

```
sudo mount -t nfs 192.168.131.200:/mnt/data_storage/ /mnt/pamstorage/
```

4. **Добавьте монтирование хранилища в автозапуск:**

   Чтобы автоматически монтировать NFS при старте системы, добавьте запись в файл **/etc/fstab**:

   Шаблон команды

   ```
   <fqdn_or_ip_nfs_server>:/путь/до/медихранилища /путь/до/папки/монтирования nfs defaults 0 0
   ```

   Пример файла:

   Пример команды

   ```
   192.168.131.200:/mnt/data_storage/ /mnt/pamstorage/ nfs defaults 0 0
   ```

   Для проверки монтирования выполните команду:

   ```
   sudo mount
   ```

5. **Внесите изменения в секции volumes в docker-compose файлах для Core и Gateway-Service:**

   - **Core**: Путь до файла на сервере управления: /etc/indeed/indeed-pam/docker-compose.management-server.yml
   - **Gateway-Service**: Путь до файла на сервере доступа: /etc/indeed/indeed-pam/docker-compose.access-server.yml

   В секцию `volumes` необходимо добавить путь к монтированному хранилищу:

   ```
   - /путь/до/папки/монтирования:/mnt/storage:rw,z
   ```

   Пример для Core

   ```
   core:
     image: nexus.indeed-id.hq:5050/pam/indeed-pam-core:${TAG}
     container_name: pam-core
     extends:
   ```

```
    file: docker-compose.common-services.yml
    service: base
  pids_limit: 5000
  depends_on:
    - ca-certificates
    - pgsql
  environment:
    - COMPlus_EnableDiagnostics=0
  user: root
  read_only: false
  security_opt:
    - apparmor=pam-management
  volumes:
    - ./core/events:/var/lib/indeed/indeed-pam/events:rw,Z
    - ./core/appsettings.json:/app/appsettings.json:ro,z
    - ./keys/shared/protector:/etc/indeed/indeed-pam/keys/shared/protector:ro,z
    - ./keys/core:/etc/indeed/indeed-pam/keys/core:ro,Z
    - ./logs/core:/app/logs:rw,Z
    - /mnt/pamstorage:/mnt/storage:rw,z  # Пример монтирования NFS
    - pam-core-temp-data:/var/lib/indeed/indeed-pam:rw
    - pam-ca-cert-store:${CERT_STORE}:ro
  tmpfs:
    - /tmp
  networks:
    - pam-core-network
    - pam-ls-network
```

6. **Внесите изменения в секции Storage конфигурационных файлов Core и Gateway-Service:**

   - **Core**: Путь до конфигурационного файла на сервере управления: /etc/indeed/indeed-pam/core/appsettings.json
   - **Gateway-Service**: Путь до конфигурационного файла на сервере доступа: /etc/indeed/indeed-pam/gateway-service/appsettings.json

   В обоих файлах необходимо указать путь до монтированного хранилища:

```
"Storage": {
  "Type": "FileSystem",
  "Settings": {
    "Root": "/mnt/storage"
  }
}
```

7. **Перезагрузите контейнеры с помощью следующей команды:**

```
sudo bash /etc/indeed/indeed-pam/scripts/run-pam.sh
```

Изменение конфигурации PAM

Изменение конфигурации текущей инсталляции PAM выполняется с помощью мастера. Для изменения конфигурации вам понадобится файл резервной копии, который был сгенерирован во время прошлого использования мастера.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Во время изменения конфигурации PAM будет недоступен. Все текущие сессии будут прерваны.

Запуск мастера

Мастер — это веб-приложение, которое позволяет установить, обновить версию или изменить конфигурацию Indeed PAM. Мастер поставляется в составе дистрибутива PAM. Чтобы использовать мастер, потребуется запустить его в Docker-контейнере с помощью специального скрипта.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Мастер должен быть запущен на том хосте, на котором будет установлена одна из ролей PAM (сервер управления или сервер доступа), иначе попытка установки PAM приведет к ошибке.

1. Загрузите и распакуйте дистрибутив PAM на Linux-машину и перейдите в директорию дистрибутива.
2. Выполните команду:

   ```
   sudo bash run-wizard.sh
   ```

3. Дождитесь выполнения скрипта.
4. После выполнения скрипта перейдите по URL, указанному в консоли.
5. В поле **Код доступа** введите `AutenticationCode`, указанный в консоли после выполнения скрипта.
   Пример кода: `vVHyTVRyKX5pxUKM6e1ZgCWEnOdXFdOy`.

> **ИНФОРМАЦИЯ**
>
> По умолчанию код будет запрошен снова через 2 часа, то есть за это время нужно успеть выполнить всю работу.

6. Нажмите **Войти** и переходите к работе с мастером.

Сценарий

1. Выберите **Изменение конфигурации PAM**.
2. Нажмите **Далее**.

<details>
<summary>Подробнее о сценариях</summary>

Мастер используется для выполнения одного из трех сценариев:

- **Новая инсталляция PAM** — установка Indeed PAM.
- **Обновление PAM** — обновление всех компонентов Indeed PAM до новой версии. Например, с 2.10 до 3.0. Во время обновления PAM будет недоступен. Все текущие сессии будут прерваны.
- **Изменение конфигурации PAM** — внесение изменений в текущую инсталляцию PAM. Например, изменение состава хостов. Версия PAM останется той же. Во время обновления PAM будет недоступен. Все текущие сессии будут прерваны.
</details>

Загрузка файла резервной копии

1. Приложите файл резервной копии и введите пароль.
2. Нажмите **Проверить резервную копию**.
3. После успешного завершения проверки нажмите **Далее**.

Изменение предзаполненных значений мастера

Благодаря файлу резервной копии, который вы загрузили на предыдущем шаге, в мастере предзаполнены поля с настройками вашей инсталляции Indeed PAM. Измените необходимые параметры и/или состав хостов и переходите к следующему этапу обновления PAM.

Учитывайте ряд ограничений:

- Удаление PAM с хостов, которые были исключены из списка хостов, не реализовано в мастере. Удаление PAM с хостов выполняется вручную, без использования мастера.
- Пароли, восстановленные из файла резервной копии, невозможно посмотреть. Заменить на другие можно.

Сохранение файла резервной копии

На этом шаге вам потребуется скачать новый файл резервной копии, который потребуется вам при следующем обновлении PAM на новую версию или для изменения конфигурации текущей версии PAM.

1. Задайте пароль для резервной копии мастера.
2. Нажмите **Скачать резервную копию**.
3. Нажмите **Далее** для перехода к следующему шагу мастера.

Изменение конфигурации PAM

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Во время применения изменений PAM будет недоступен. Все текущие сессии будут прерваны.

1. Для переключателя **Способ изменения конфигурации** выберите значение **Из мастера**.
2. Нажмите **Применить изменения**.
3. Отслеживайте процесс применения изменений с помощью прогресс-бара. Дождитесь завершения применения изменений.
4. После завершения применения изменений нажмите **Завершить работу мастера** или выполните следующую команду в терминале:

   ```
   sudo bash stop-wizard.sh
   ```

▼ Применение изменений вручную

При выборе изменения конфигурации вручную появляется возможность скачать конфигурационные файлы PAM. Эти файлы потребуется разложить по серверам самостоятельно, а также запустить скрипт развертывания PAM на каждом сервере отдельно.

Резервные учетные записи

Выделите резервную учетную запись для каждого ресурса

Шифрование паролей и секретов

Зашифруйте файлы конфигурации после окончания настройки инсталляции

Фильтрация процессов и ФС

Добавьте разрешенные для запуска процессы в файл конфигурации processprotection.settings.json (опционально)

Шифрование материалов сессии

Ознакомьтесь с информацией о шифровании материалов сессии

Политики безопасности сервера доступа

Импортируйте набор рекомендуемых политик на сервер доступа

Настройки безопасности сервера доступа

Примените необходимые настройки безопасности на сервере доступа

Смена ключа шифрования БД PAM

Смените ключ шифрования в случае его компрометации

Резервные учетные записи

База данных и сервис Indeed PAM Core — это критические элементы. Повреждение базы данных или отказ сервиса приведет к потере доступа к ресурсам, так как пароли учетных записей неизвестны конечным пользователям и администраторам.

Поэтому рекомендуется для каждого ресурса выделить резервную учетную запись с правами локального администратора (ОС Windows) или с правами на выполнение команды SUDO (ОС *nix). Назначьте уполномоченного сотрудника, который будет отвечать за сохранность резервных учетных записей и паролей.

Эта мера позволит восстановить доступ к ресурсам в случае выхода из строя базы данных или сервиса.

Шифрование паролей и секретов

По умолчанию, для дополнительной защиты системы, во время установки компонентов происходит автоматическое шифрование файлов конфигурации.

Для защиты системы рекомендуется выполнять шифрование файлов конфигурации после внесения окончательных правок.

Во время работы с системой может потребоваться редактирование фалов конфигурации. Для этого понадобится снятие шифрования и дальнейшее шифрование файлов конфигурации.

Это можно сделать с помощью утилиты на Windows или скрипта на Linux.

Шифрованию подлежат конфигурационные файлы компонентов Core, IdP, ProxyApp и Log Server.

Утилита на Windows

Снятие шифрования

- Перейдите в каталог с дистрибутивом PAM по пути **IndeedPAM_3.0_RU\indeed-pam-tools\configuration-protector**.
- Запустите PowerShell от имени администратора.
- Для снятия шифрования со всех файлов конфигурации, расположенных в стандартных директориях, выполните команду:

  ```
  .\Pam.Tools.Configuration.Protector.exe unprotect
  ```

- Для снятия шифрования с файлов конфигурации отдельных компонентов выполните команду:

  ```
  .\Pam.Tools.Configuration.Protector.exe unprotect --component Имя_компонента
  ```

  Например:

  ```
  
  ```

```
.\Pam.Tools.Configuration.Protector.exe unprotect --component core
```

- Снятие шифрования с файла, расположенного вне стандартной директории:

```
.\Pam.Tools.Configuration.Protector.exe unprotect --component Имя_компонента --file
путь_к_файлу
```

Например:

```
.\Pam.Tools.Configuration.Protector.exe unprotect --component Core --file
C:\inetpub\wwwroot\core\appsettings.json
```

> ⓘ **ПРИМЕЧАНИЕ**
>
> Стандартной директорией файлов конфигурации является директория C:\inetpub\wwwroot\имя_компонента\appsettings.json.

Шифрование

- Перейдите в каталог с дистрибутивом PAM по пути **IndeedPAM_3.0_RU\indeed-pam-tools\configuration-protector**.
- Запустите PowerShell от имени администратора.
- Для шифрования всех файлов конфигурации, расположенных в стандартных директориях, выполните команду:

```
.\Pam.Tools.Configuration.Protector.exe protect
```

- Для шифрования файлов конфигурации отдельных компонентов выполните команду:

```
.\Pam.Tools.Configuration.Protector.exe protect --component Имя_компонента
```

Например:

```
```

```
.\Pam.Tools.Configuration.Protector.exe protect --component core
```

- Шифрование файла, расположенного вне стандартной директории:

```
.\Pam.Tools.Configuration.Protector.exe protect --component Имя_компонента --file
путь_к_файлу
```

Например:

```
.\Pam.Tools.Configuration.Protector.exe protect --component Core --file
C:\inetpub\wwwroot\core\appsettings.json
```

> ⓘ **ПРИМЕЧАНИЕ**
>
> Стандартной директорией файлов конфигурации является директория C:\inetpub\wwwroot\имя_компонента\appsettings.json

Скрипт на Linux

Снятие шифрования

- Перейдите в директорию с файлом протектора

```
cd /etc/indeed/indeed-pam/tools
```

- Для снятия шифрования со всех файлов конфигурации, расположенных в стандартных директориях, выполните команду:

```
bash protector.sh unprotect
```

- Для снятия шифрования с файлов конфигурации отдельных компонентов выполните команду:

```
bash protector.sh unprotect –component Имя_компонента
```

Например:

```
bash protector.sh unprotect -component core
```

Шифрование

- Перейдите в директорию с файлом протектора:

```
cd /etc/indeed/indeed-pam/tools
```

- Для шифрования всех файлов конфигурации, расположенных в стандартных директориях, выполните команду:

```
bash protector.sh protect
```

- Для шифрования файлов конфигурации отдельных компонентов выполните команду:

```
bash protector.sh protect -component Имя_компонента
```

Например:

```
bash protector.sh protect -component core
```

О механизме шифрования

Шифрование конфигурационных файлов (критичных файлов) Indeed PAM выполняется при помощи ключа шифрования AES-256 сгенерированного Data Protection API. Ключ сохраняется на сервере Indeed PAM и дополнительно шифруется Windows Data Protection API.

Расположение ключа:

- ОС Windows Server — %ProgramData%\Indeed\Keys
- ОС Linux — /etc/indeed/indeed-pam/keys

Право на использование директории предоставляется только приложениям Indeed PAM.

Фильтрация процессов и ФС

Запрет запуска процессов

Для PAM Gateway реализован механизм запрета запуска процессов пользователями.

При каждом запуске процесса выполняется ряд проверок. Запуск процесса разрешен, если хотя бы одна из проверок пройдена:

- Если пользователь это `LOCAL_SYSTEM`, `LOCAL_SERVICE` или `NETWORK_SERVICE`.
- Если пользователь является администратором на сервере RDS.
- Если родительским процессом является один из известных системных (`svchost.exe`, `winlogon.exe`, `userinit.exe`, `rdpinit.exe`).
- Старт процесса разрешен в конфигурационном файле `processprotection.settings.json`.

Если ни одна из проверок не пройдена, то запуск процесса запрещен.

Конфигурация разрешенных процессов настраивается в файле:
`C:\Program Files\Indeed PAM\Gateway\ProcessCreateHook\processprotection.settings.json`

Пример файла processprotection.settings.json

```
{
  "BlackListRules": [
    {
      "Comment": "Common, iexplore from shortcut",
      "ParentProcessPaths": [
        "C:\\Windows\\System32\\svchost.exe"
      ],
      "ApplicationPaths": [
        "C:\\Program Files\\Internet Explorer\\IEXPLORE.EXE",
        "C:\\Program Files (x86)\\Internet Explorer\\IEXPLORE.EXE"
      ]
    }
  ],

  "WhiteListRules": [
    {
      "Comment": "Common, record video",
```

```
      "ParentProcessPaths": [
        "C:\\Program Files\\Axidian\\Axidian Privilege\\Gateway\\ProxyApp\\Pam.Proxy.App.exe"
      ],
      "ApplicationPaths": [
        "C:\\Program Files\\Axidian\\Axidian Privilege\\Gateway\\ProxyApp\\ffmpeg.exe"
        "C:\\Program Files\\Axidian\\Axidian Privilege\\Gateway\\ProxyApp\\ffprobe.exe
      ]
    },
    {
      "Comment": "Common, UserInit process",
      "ParentProcessPaths": [
        "C:\\Windows\\System32\\userinit.exe"
      ],
      "ApplicationPaths": [
        "C:\\Windows\\system32\\rdpinit.exe",
        "C:\\Program Files\\Axidian\\Axidian Privilege\\Gateway\\ProxyApp\\Pam.Proxy.App.exe"
      ]
    },
    {
      "Comment": "Common, RdpInit process",
      "ParentProcessPaths": [
        "C:\\Windows\\system32\\rdpinit.exe"
      ],
      "ApplicationPaths": [
        "C:\\Windows\\system32\\rdpshell.exe",
        "C:\\Program Files\\Axidian\\Axidian Privilege\\Gateway\\ProxyApp\\Pam.Proxy.App.exe"
      ]
    },
    {
      "Comment": "Common, start WebView for authentication on IDP",
      "ParentProcessPaths": [
        "C:\\Program Files\\Axidian\\Axidian Privilege\\Gateway\\ProxyApp\\Pam.Proxy.App.exe",
        "C:\\Program Files\\Axidian\\Axidian Privilege\\Gateway\\ProxyApp\\Microsoft.WebView2.FixedVersionRuntime\\msedgewebview2.e
      ],
      "ApplicationPaths": [
        "C:\\Program Files\\Axidian\\Axidian Privilege\\Gateway\\ProxyApp\\Microsoft.WebView2.FixedVersionRuntime\\msedgewebview2.e
      ]
    },
    {
      "Comment": "RDP",
```

```
58        "ParentProcessPaths": [
59          "C:\\Program Files\\Axidian\\Axidian
    Privilege\\Gateway\\ProxyApp\\Pam.Proxy.App.exe"
60        ],
61        "ApplicationPaths": [
62          "C:\\Windows\\system32\\mstsc.exe",
63          "C:\\Windows\\SysWOW64\\mstsc.exe"
64        ]
65      },
66      {
67        "Comment": "SSH",
68        "ParentProcessPaths": [
69          "C:\\Program Files\\Axidian\\Axidian
    Privilege\\Gateway\\ProxyApp\\Pam.Proxy.App.exe"
70        ],
71        "ApplicationPaths": [
72          "C:\\Program Files\\Axidian\\Axidian
    Privilege\\Gateway\\SshClient\\Pam.Putty.exe"
73        ]
74      }
75    ]
76  }
```

- `BlackListRules` — правила для запрещенных процессов.
- `WhiteListRules` — правила для разрешенных процессов.

Параметры правил:

- `Comment` — комментарий для правила.
- `ApplicationPaths` — пути до исполняемых файлов, которые можно запускать.
- `ParentProcessPaths` — пути до исполняемых файлов, процессы которых могут запускать приложения из `ApplicationPaths`.

Защита критичных файлов

Для PAM Gateway реализован механизм разграничения прав для доступа к файлам на уровне процессов.

Пользователи локальной группы администраторов имеют доступ к любым файлам из любых процессов. Остальные пользователи могут открывать любые файлы из любых процессов, кроме

уязвимых файлов. Для уязвимых файлов выполняется проверка процесса: если процесс находится в списке разрешенных, то доступ разрешается, иначе — запрещается.

Конфигурация защиты уязвимых файлов настраивается в файле:
`C:\Program Files\Indeed PAM\Gateway\Service\filesprotection.settings.json`

По умолчанию в конфигурационный файл добавлены уязвимые файлы PAM, дополнительная настройка не требуется.

Пример файла filesprotection.settings.json

```
{
    "VulnerableFiles": [
        {
            "Path": "C:\\Program Files\\Indeed PAM\\Gateway\\ProxyApp\\appsettings.json",
            "AllowedProcesses": [
                "C:\\Program Files\\Indeed PAM\\Gateway\\ProxyApp\\Pam.Proxy.App.exe"
            ]
        },
        {
            "Path": "C:\\Program Files\\Indeed PAM\\SSH Proxy\\SshProxy\\",
            "AllowedProcesses": [
                "C:\\Program Files\\Indeed PAM\\SSH Proxy\\SshProxy\\Pam.SshProxy.Service.exe"
            ]
        }
    ]
}
```

Параметры:

- `VulnerableFiles –` список уязвимых файлов.
- `Path` — путь к уязвимому файлу. Можно указывать как конкретный файл, так и директорию.
- `AllowedProcesses –` список процессов, которым разрешен доступ к файлу. Указываются конкретные исполняемые модули.

После изменения конфигурационного файла требуется перезапуск службы Pam.Service.

Шифрование материалов сессии

Предоставление доступа к защищаемым привилегированным учетным записям является не единственной задачей Indeed PAM. Для максимального обеспечения безопасности учетной записи и процесса работы применяются средства протоколирования. В процессе работы выполняется фиксация действий при помощи видео и снимков экрана. Отснятые материалы являются критичными с точки зрения информационной безопасности, так как используются для исследования инцидентов и часто носят конфиденциальный характер.

Для обеспечения безопасности отснятых материалов в Indeed PAM реализован механизм шифрования позволяющий безопасно хранить и использовать в рамках решения. Шифрование выполняется при помощи алгоритма AES256, сам ключ уникален для каждой отдельной сессии.

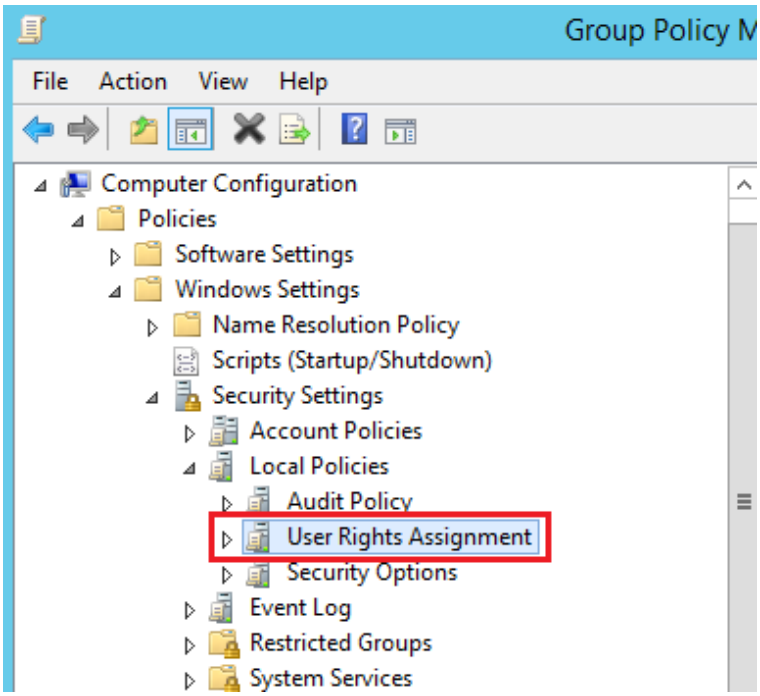
Политики безопасности сервера доступа

Набор стандартных групповых политик домена Active Directory, рекомендуемых к применению на сервер, который выполняет роль Indeed PAM Gateway, для обеспечения безопасности.

Назначение прав пользователя

Путь: **Конфигурация компьютера → Политики → Конфигурация Windows → Параметры безопасности → Локальные политики → Назначение прав пользователя**

(англ. — *Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → User Rights Assignment*)



▼ Описание политик

Политика	Описание	Значения
Access Credential Manager as a trusted	Этот параметр используется диспетчером учетных данных в ходе	Не определено

Политика	Описание	Значения
caller (Доступ к диспетчеру учетных данных от имени доверенного вызывающего)	архивации и восстановления. Эта привилегия не должна предоставляться учетным записям, поскольку она предоставляется только Winlogon. Сохраненные пользователями учетные данные могут быть скомпрометированы, если эта привилегия предоставляется другим субъектам.	
Act as part of the operating system (Работа в режиме операционной системы)	Это право пользователя позволяет процессу олицетворять любого пользователя без проверки подлинности. Процесс, таким образом, может получать доступ к тем же локальным ресурсам, что и пользователь. Процессы, для которых требуется такая привилегия, должны использовать уже содержащую эту привилегию учетную запись LocalSystem, а не отдельную учетную запись пользователя с этой привилегией. Если в организации используются только серверы с операционными системами семейства Windows Server 2003, нет необходимости назначать эту привилегию пользователям. Однако если в организации используются серверы под управлением операционных систем Windows 2000 или Windows NT 4.0, назначение этой привилегии может потребоваться для использования приложений, обменивающихся паролями в обычном текстовом формате. Внимание!	Не определено

Политика	Описание	Значения
	Назначение этого права пользователю может представлять угрозу безопасности. Назначайте такие права только доверенным пользователям.	
Adjust memory quotas for a process (Настройка квот памяти для процесса)	Эта привилегия определяет, кто может изменять максимальный объем памяти, используемый процессом. Это право пользователя определено в объекте групповой политики (GPO) контроллера домена по умолчанию и в локальной политике безопасности рабочих станций и серверов. Примечание. Эта привилегия полезна при настройке системы, но его использование может нанести вред, например, в случае атак типа "отказ в обслуживании".	NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE, BUILTIN\Administrators
Allow log on locally (Локальный вход в систему)	Этот параметр определяет пользователей, которые могут входить в систему на компьютере.	BUILTIN\Administrators
Allow log on through Remote Desktop Services (Разрешать вход в систему через службы удаленных рабочих столов)	Этот параметр безопасности определяет, у каких пользователей или групп есть разрешение на вход в систему в качестве клиента служб удаленных рабочих столов.	BUILTIN\Administrators, группа пользователей PAM
Back up files and directories (Архивация файлов и каталогов)	Это право пользователя определяет, какие пользователи могут игнорировать разрешения для файлов, каталогов, реестра и других постоянных объектов с целью архивации системы. В частности, это	BUILTIN\Administrators

Политика	Описание	Значения
	право пользователя подобно предоставлению следующих разрешений пользователю или группе для всех папок и файлов в системе: Обзор папок/Выполнение файлов Содержимое папки/Чтение данных Чтение атрибутов Чтение расширенных атрибутов Чтение разрешений Внимание! Назначение этого права пользователю может представлять угрозу безопасности. Поскольку невозможно точно знать, что именно пользователь делает с данными - создает архив, крадет или копирует с целью распространения - назначайте это право только доверенным пользователям.	
Bypass traverse checking (Обход перекрестной проверки)	Это право пользователя определяет, какие пользователи могут производить обзор деревьев каталога, даже если у этих пользователей отсутствуют разрешения на каталог. Эта привилегия не позволяет пользователям просматривать содержимое каталога, а позволяет только выполнять обзор.	BUILTIN\Administrators, NT AUTHORITY\Authenticated Users, NT AUTHORITY\LOCAL SERVICE, NT AUTHORITY\NETWORK SERVICE
Change the system time (Изменение системного времени)	Это право пользователя определяет, какие пользователи и группы могут изменять время и дату внутренних часов компьютера. Пользователи с данным правом могут влиять на вид журналов событий. Если системное время было изменено, записи отслеженных событий отразят новое	BUILTIN\Administrators, NT AUTHORITY\LOCAL SERVICE

Политика	Описание	Значения
	время, а не действительное время совершения событий.	
Change the time zone (Изменение часового пояса)	Это пользовательское право определяет, какие пользователи и группы могут изменять часовой пояс, используемый компьютером для отображения местного времени, которое представляет собой сумму системного времени компьютера и смещения часового пояса. Само по себе системное время является абсолютным и не изменяется при изменении часового пояса.	BUILTIN\Administrators, NT AUTHORITY\LOCAL SERVICE
Create a token object (Создание маркерного объекта)	Этот параметр безопасности определяет, какие учетные записи могут быть использованы процессами для создания маркеров, которые затем могут быть использованы для получения доступа к любым локальным ресурсам, если для создания маркера доступа процесс использует внутренний интерфейс (API). Данное право используется операционной системой для внутренних целей. Если нет необходимости, не предоставляйте это право никаким пользователям, группам или процессам кроме пользователя "Локальная система". Внимание! Назначение этого права пользователю может представлять угрозу безопасности. Не назначайте это право пользователю, группе или	Не определено

Политика	Описание	Значения
	процессу, которым нежелательно позволять управлять системой.	
Create global objects (Создание глобальных объектов)	Этот параметр безопасности определяет, могут ли пользователи создавать глобальные объекты, доступные для всех сеансов. Пользователи по-прежнему могут создавать отдельные объекты для их сеансов, не имея данного права. Создание глобальных объектов может влиять на процессы, выполняемые в сеансах других пользователей, ведя к ошибкам приложений и повреждению данных. Внимание! Назначение этого права пользователя может представлять угрозу безопасности. Назначайте его только доверенным пользователям.	BUILTIN\Administrators, NT AUTHORITY\SERVICE
Create permanent shared objects (Создание постоянных общих объектов)	Это право пользователя определяет, какие учетные записи могут использоваться процессами для создания объекта каталога при помощи диспетчера объектов. Это право пользователя используется внутри операционной системы и полезно для компонентов в режиме ядра, расширяющих пространство имен объекта. Поскольку это право уже назначено компонентам, выполняющимся в режиме ядра, его не нужно специально назначать.	Не определено
Create symbolic links (Создание	Эта привилегия определяет для пользователя возможность создавать	BUILTIN\Administrators

Политика	Описание	Значения
символических ссылок)	символьные ссылки с компьютера, на который он вошел. Внимание! Эту привилегию следует предоставлять только доверенным пользователям. Символические ссылки могут обнажить уязвимые места в приложениях, которые не рассчитаны на их обработку.	
Debug programs (Отладка программ)	Это право пользователя определяет, какие пользователи могут подключать отладчик к любому процессу или ядру. Это право не нужно назначать разработчикам, выполняющим отладку собственных приложений. Оно потребуется разработчикам для отладки новых системных компонентов. Это право пользователя обеспечивает полный доступ к важным компонентам операционной системы. Внимание! Назначение этого права пользователя может представлять угрозу безопасности. Назначайте его только доверенным пользователям.	BUILTIN\Administrators
Deny access to this computer from the network (Отказать в доступе к этому компьютеру из сети)	Этот параметр безопасности определяет, каким пользователям будет отказано в доступе к компьютеру из сети. Этот параметр заменяет параметр политики "Разрешить доступ к компьютеру из сети", если к учетной записи пользователя применяются обе политики.	BUILTIN\Guests
Deny log on as a batch job (Отказать	Этот параметр безопасности определяет, каким учетным записям	BUILTIN\Guests

Политика	Описание	Значения
во входе в качестве пакетного задания)	будет отказано во входе в систему в виде пакетного задания. Данный параметр замещает параметр "Разрешить вход в систему как пакетному заданию", если к учетной записи пользователя применяются оба параметра.	
Deny log on as a service (Отказать во входе в качестве службы)	Этот параметр безопасности определяет, каким учетным записям служб будет отказано в регистрации процесса как службы. Этот параметр политики заменяет параметр "Разрешить вход в систему как службе", если к учетной записи применяются об политики. Примечание. Этот параметр безопасности не применяется к учетным записям "Система", "Локальная служба" или "Сетевая служба".	BUILTIN\Guests
Deny log on locally (Запретить локальный вход)	Этот параметр безопасности определяет, каким пользователям будет отказано во входе в систему. Этот параметр политики заменяет параметр "Разрешить локальный вход в систему", если к учетной записи применяются обе политики. Внимание! Если этот параметр безопасности применяется к группе "Все", никто не сможет войти в систему локально.	BUILTIN\Guests
Deny log on through Terminal Services (Запретить вход в	Этот параметр безопасности определяет, каким пользователям и группам будет запрещено входить в	BUILTIN\Guests

Политика	Описание	Значения
систему через службу удаленных рабочих столов)	систему как клиенту служб удаленных рабочих столов.	
Enable computer and user accounts to be trusted for delegation (Разрешение доверия к учетным записям компьютеров и пользователей при делегировании)	Этот параметр безопасности определяет, какие пользователи могут устанавливать параметр "Делегирование разрешено" для пользователя или объекта-компьютера. Пользователь или объект, получившие эту привилегию, должны иметь доступ на запись к управляющим флагам учетной записи пользователя или объекта-компьютера. Серверный процесс, выполняемый на компьютере (или в пользовательском контексте), которому разрешено делегирование, может получить доступ к ресурсам другого компьютера, используя делегированные учетные данные клиента, пока в учетной записи клиента не будет установлен управляющий флаг "Учетная запись не может быть делегирована". Это право пользователя определено в объекте групповой политики (GPO) контроллера домена по умолчанию и в локальной политике безопасности рабочих станций и серверов. Внимание! Неправильное применение этого права пользователя или параметра "Делегирование разрешено" может сделать сеть уязвимой к изощренным атакам с помощью вредоносных программ типа	BUILTIN\Administrators

Политика	Описание	Значения
	"Троянский конь", которые имитируют входящих клиентов и используют их учетные данные для получения доступа к сетевым ресурсам.	
Force shutdown from a remote system (Принудительное удаленное завершение работы)	Этот параметр безопасности определяет, каким пользователям разрешено удаленное завершение работы компьютера. Неправильное применение этого права пользователя может стать причиной отказа в обслуживании. Это право пользователя определено в объекте групповой политики (GPO) контроллеров домена по умолчанию и в локальной политике безопасности рабочих станций и серверов.	BUILTIN\Administrators
Generate security audits (Создание аудитов безопасности)	Этот параметр безопасности определяет, какие учетные записи могут быть использованы процессом для добавления записей в журнал безопасности. Журнал безопасности используется для отслеживания несанкционированного доступа в систему. Неправильное применение этого права пользователя может стать причиной формирования множества событий аудита, которые могут скрыть свидетельства атаки или вызвать отказ в обслуживании, если включен параметр безопасности "Аудит: немедленно завершить работу системы при невозможности протоколирования аудита безопасности". Дополнительные	NT AUTHORITY\LOCAL SERVICE, NT AUTHORITY\NETWORK SERVICE

Политика	Описание	Значения
	сведения см. в разделе "Аудит: немедленно завершить работу системы при невозможности протоколирования аудита безопасности"	
Impersonate a client after authentication (Имитация клиента после проверки подлинности)	Выдача пользователю этой привилегии позволяет программам, выполняемым от имени этого пользователя, олицетворять клиента. Требование этого права для подобного олицетворения не позволяет неавторизованному пользователю убедить клиента подключиться (например, через вызов удаленной процедуры (RPC) или именованные каналы) к созданной им службе, а затем олицетворить клиента, что даст возможность повысить его полномочия до административного или системного уровня. Внимание! Назначение этого права пользователю может представлять угрозу безопасности. Назначайте такие права только доверенным пользователям. Примечание. По умолчанию к токенам доступа служб, запущенных диспетчером управления службами, добавляется встроенная группа "Служба". Встроенная группа "Служба" также добавляется к токенам доступа COM-серверов, запущенных COM-инфраструктурой и настроенных на выполнение под определенной учетной записью. Поэтому данные службы получают это	BUILTIN\Administrators, NT AUTHORITY\SERVICE

Политика	Описание	Значения
	пользовательское право при запуске. Кроме того, пользователь может олицетворять токен доступа и при выполнении любого из следующих условий. Олицетворяемый токен доступа назначен данному пользователю. В данном сеансе входа пользователь создал токен доступа, явно указав учетные данные при входе. Запрошенный уровень ниже, чем "Олицетворять", например:"Анонимный" или "Идентифицировать". Поэтому пользователям обычно не требуется это пользовательское право. Дополнительные сведения можно найти поиском SeImpersonatePrivilege в Microsoft Platform SDK. Внимание! Включение этого параметра может привести к потере привилегии "Олицетворять" программами, имеющим эту привилегию, и заблокировать их выполнение.	
Increase scheduling priority (Увеличение приоритета выполнения)	Этот параметр безопасности определяет, какие учетные записи могут использовать процесс, имеющий право доступа "Запись свойства" для другого процесса, для повышения приоритета выполнения, назначенного другому процессу. Пользователь, имеющий данную привилегию, может изменять приоритет выполнения процесса через пользовательский интерфейс диспетчера задач.	BUILTIN\Administrators

Политика	Описание	Значения
Load and unload device drivers (Загрузка и выгрузка драйверов устройств)	Это право пользователя определяет, какие пользователи могут динамически загружать и выгружать драйверы устройств или другой код в режиме ядра. Это право пользователя не применяется к драйверам устройств Plug and Play. Не рекомендуется назначать эту привилегию другим пользователям. Внимание! Назначение этого права пользователю может представлять угрозу безопасности. Не назначайте это право пользователю, группе или процессу, которым нежелательно позволять управлять системой.	BUILTIN\Administrators
Lock pages in memory (Блокировка страниц в памяти)	Этот параметр безопасности определяет, какие учетные записи могут использовать процессы для сохранения данных в физической памяти для предотвращения сброса этих данных в виртуальную память на диске. Применение этой привилегии может существенно повлиять на производительность системы, снижая объем доступной оперативной памяти (RAM).	Не определено
Log on as a batch job (Вход в качестве пакетного задания)	Этот параметр безопасности позволяет пользователю входить в систему при помощи средства, использующего очередь пакетных заданий, и предоставляется только для совместимости с предыдущими версиями Windows. Например, если пользователь передает задание при	BUILTIN\Administrators

Политика	Описание	Значения
	помощи планировщика заданий, последний регистрирует этого пользователя в системе как пользователя с пакетным входом, а не как интерактивного пользователя.	
Manage auditing and security log (Управлять аудитом и журналом безопасности)	Этот параметр безопасности определяет, какие пользователи могут указывать параметры аудита доступа к объектам для отдельных ресурсов, таких как файлы, объекты Active Directory и разделы реестра. Данный параметр безопасности не разрешает пользователю включить аудит доступа к файлам и объектам в целом. Для включения такого аудита нужно настроить параметр доступа к объекту "Аудит" в пути "Конфигурация компьютера\Параметры Windows\Параметры безопасности\Локальные политики\Политики аудита". События аудита можно просмотреть в журнале безопасности средства просмотра событий. Пользователь с данной привилегией может также просматривать и очищать журнал безопасности.	BUILTIN\Administrators
Modify an object label (Изменение метки объекта)	Эта привилегия определяет, каким учетным записям пользователей разрешается изменять метки целостности объектов, таких как файлы, разделы реестра или процессы, владельцами которых являются другие пользователи.	Не определено

Политика	Описание	Значения
	Процессы, выполняющиеся под учетной записью пользователя, без этой привилегии могут понижать уровень метки объекта, владельцем которого является данный пользователь.	
Modify firmware environment values (Изменение параметров среды изготовителя)	Этот параметр безопасности определяет, кто может изменять значения параметров аппаратной среды. Переменные аппаратной среды - это параметры, сохраняемые в энергонезависимой памяти компьютеров, архитектура которых отлична от x86. Действие параметра зависит от процессора. На компьютерах архитектуры x86 единственное значение аппаратной среды, которое можно изменить назначением данного права пользователя, - это параметр "Последняя удачная конфигурация", который должен изменяться только системой. В компьютерах на базе процессоров Itanium загрузочные данные хранятся в энергонезависимой памяти. Данное право пользователя должно назначаться пользователям для выполнения программы bootcfg.exe и изменения параметра "Операционная система по умолчанию" компонента "Загрузка и восстановление" диалогового окна свойств системы. На всех компьютерах это право пользователя требуется для установки и обновления Windows.	BUILTIN\Administrators

Политика	Описание	Значения
	Примечание. Этот параметр безопасности не влияет на пользователей, которые могут изменять системные и пользовательские переменные среды, отображаемые на вкладке "Дополнительно" диалогового окна свойств системы. Сведения о том, как изменять эти переменные, см. в разделе "Добавление или изменение значения переменных среды".	
Perform volume maintenance tasks (Выполнение задач по обслуживанию томов)	Этот параметр безопасности определяет пользователей и группы, которые могут выполнять задачи по обслуживанию томов, например, удаленную дефрагментацию. При назначении этого права пользователя следует соблюдать осторожность. Пользователи, имеющие данное право, могут просматривать диски и добавлять файлы в память, занятую другими данными. После открытия дополнительных файлов пользователь может читать изменять запрошенные данные.	BUILTIN\Administrators
Profile single process (Профилирование одного процесса)	Этот параметр безопасности определяет пользователей, которые могут использовать средства мониторинга производительности для отслеживания производительности несистемных процессов.	BUILTIN\Administrators
Profile system performance	Этот параметр безопасности определяет пользователей, которые	BUILTIN\Administrators

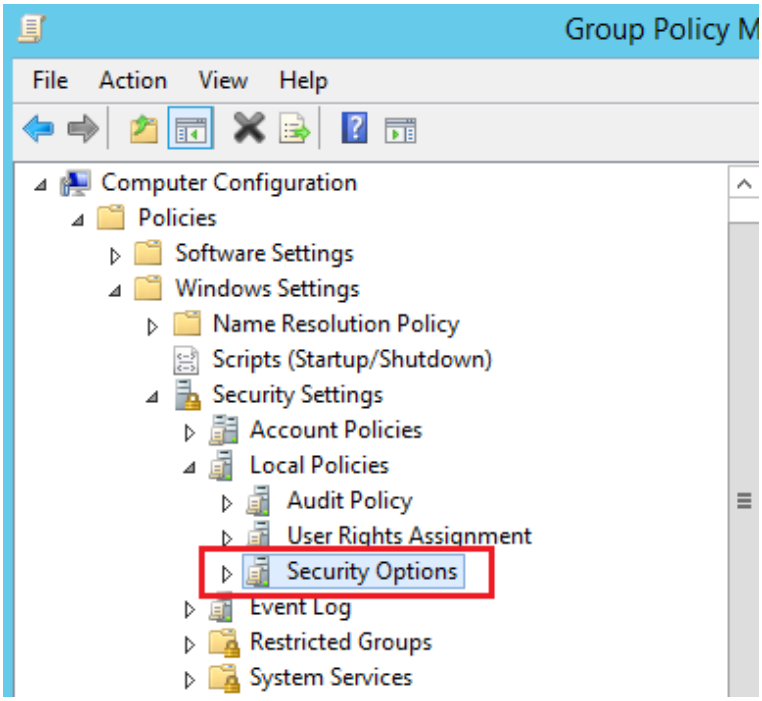
Политика	Описание	Значения
(Профилирование производительности системы)	могут использовать средства мониторинга производительности для отслеживания производительности системных процессов.	
Replace a process level token (Замена маркеров уровня процесса)	Этот параметр безопасности определяет учетные записи пользователей, которые могут вызывать процедуру API-интерфейса CreateProcessAsUser() для того, чтобы одна служба могла запускать другую. Планировщик заданий - это пример процесса, использующего данное право пользователя. Сведения о планировщике заданий см. в обзоре "Планировщик заданий".	NT AUTHORITY\LOCAL SERVICE, NT AUTHORITY\NETWORK SERVICE
Restore files and directories (Восстановление файлов и каталогов)	Этот параметр безопасности определяет пользователей, которые могут обойти разрешения на файлы, каталоги, реестр и другие постоянные объекты при восстановлении архивных копий файлов и каталогов, а также пользователей, которые могут назначить любого действительного субъекта безопасности владельцем объекта. В частности, это право пользователя подобно предоставлению следующих разрешений пользователю или группе для всех папок и файлов в системе: Обзор папок/Выполнение файлов Запись Внимание! Назначение этого права пользователя может представлять угрозу безопасности. Так как оно дает возможность	BUILTIN\Administrators

Политика	Описание	Значения
	перезаписывать параметры реестра, скрывать данные и получать во владение системные объекты, назначать его следует только доверенным пользователям.	
Shut down the system (Завершение работы системы)	Этот параметр безопасности определяет пользователей, которые после локального входа в систему могут завершить работу операционной системы при помощи команды "Завершить работу". Неправильное применение этого права пользователя может стать причиной отказа в обслуживании.	BUILTIN\Administrators
Take ownership of files or other objects (Смена владельцев файлов и других объектов)	Этот параметр безопасности определяет пользователей, которые могут стать владельцем любого защищаемого объекта системы, в том числе: объектов Active Directory, файлов и папок, принтеров, разделов реестра, процессов и потоков. Внимание! Назначение этого права пользователя может представлять угрозу безопасности. Так как объекты полностью контролируются их владельцами, назначать данное право следует только доверенным пользователям.	BUILTIN\Administrators

Параметры безопасности

Путь: **Конфигурация компьютера → Политики → Конфигурация Windows → Параметры безопасности → Локальные политики → Параметры безопасности**

(англ. — *Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → Security Options*)



Учетные записи

(англ. — *Accounts*)

▼ Описание политик

Политика	Описание	Значение
Accounts: Administrator account status (Учетные записи: Состояние учетной записи 'Администратор')	Этот параметр безопасности определяет, включена или отключена учетная запись локального администратора. Примечания При несоответствии пароля текущего администратора требованиям к паролю повторно включить учетную запись администратора, если ранее она была отключена, будет нельзя. В этом случае, пароль учетной записи администратора должен быть сброшен другим членом группы администраторов. Сведения о том, как	Enabled (Включен)

Политика	Описание	Значение
	сбросить пароль, см. в разделе "Сброс пароля". Отключение учетной записи администратора при некоторых обстоятельствах может затруднить обслуживание. При перезагрузке в безопасном режиме отключенную учетную запись администратора можно включить только в том случае, если компьютер не присоединен к домену и отсутствуют другие активные учетные записи локального администратора. Если компьютер присоединен к домену, отключенная учетная запись администратора не может быть включена.	
Accounts: Guest account status (Учетные записи: Состояние учетной записи 'Гость')	Этот параметр безопасности определяет, включена или отключена учетная запись гостя. Примечание. Если учетная запись гостя отключена, а для параметра безопасности "Сетевой доступ: модель общего доступа и безопасности для локальных учетных записей" установлено значение "Только гости", попытки входа в сеть, выполняемые, например, сервером сетей Майкрософт (служба SMB), завершатся неудачно.	Disabled (Отключен)
Accounts: Limit local account use of blank passwords to console logon only (Учетные записи: разрешить использование пустых паролей только при консольным входе)	Этот параметр безопасности определяет, могут ли локальные учетные записи, не защищенные паролем, использоваться для входа в систему из местоположений, отличных от физической консоли компьютера. Если параметр включен, то для локальных учетных записей, не защищенных паролем, вход в систему возможен только с клавиатуры компьютера. Внимание! К компьютерам, находящимся в физически незащищенных местах, всегда должны принудительно применяться параметры надежных паролей для всех локальных учетных записей пользователей. В противном случае любой пользователь, имеющий физический доступ к компьютеру, может войти в систему при помощи	Enabled (Включен)

Политика	Описание	Значение
	пользовательской учетной записи, не имеющей пароля. Это особенно важно для портативных компьютеров. Если этот параметр безопасности применяется к группе "Все", никто не сможет войти в систему через службы удаленных рабочих столов. Примечания Данный параметр не оказывает влияния, если при входе в систему используются учетные записи домена. Приложения, использующие удаленный интерактивный вход в систему, могут обойти этот параметр.	

Аудит

(англ. — *Audit*)

▼ Описание политик

Политика	Описание	Значение
Audit: Audit the use of Backup and Restore privilege (Аудит: аудит использования привилегии на архивацию и восстановление)	Этот параметр безопасности определяет, будет ли выполняться аудит использования всех привилегий пользователя, в том числе на архивацию и восстановление, если действует политика "Выполнять аудит использования привилегий". Если эта политика действует, включение данного параметра создает событие аудита для каждого файла, с которым выполняются операции архивации или восстановления. Если эта политика отключена, аудит использования привилегии на архивацию и восстановление не выполняется даже при включенном параметре "Выполнять аудит использования привилегий". Примечание. В версиях Windows, предшествующих Vista, изменения в результате настройки этого параметра безопасности вступят в силу только после	Enabled (Включен)

Политика	Описание	Значение
	перезагрузки Windows. Включение этого параметра может вызвать очень много событий (иногда несколько сот в секунду) во время архивации.	

Устройства

(англ. — *Devices*)

▼ Описание политик

Политика	Описание	Значение
Devices: Allowed to format and eject removable media (Устройства: разрешить форматирование и извлечение съемных носителей)	Этот параметр безопасности определяет, кому разрешено форматирование и извлечение съемных NTFS-носителей.	Administrators (Администраторы)
Devices: Prevent users from installing printer drivers (Устройства: запретить пользователям установку драйверов принтера)	Чтобы локальный компьютер мог использовать общий принтер, на нем должен быть установлен драйвер этого общего принтера. Этот параметр безопасности определяет, кому разрешено устанавливать драйвер принтера при добавлении общего принтера. Если этот параметр включен, при добавлении общего принтера драйвер принтера могут устанавливать только администраторы. Если параметр отключен, устанавливать драйвер принтера при добавлении общего принтера может любой пользователь. Примечания Этот параметр не	Enabled (Включен)

Политика	Описание	Значение
	влияет на возможность добавления локального принтера. Параметр не затрагивает администраторов.	
Devices: Restrict CD-ROM access to locally logged-on user only (Устройства: разрешить доступ к дисководам компакт-дисков только локальным пользователям)	Этот параметр безопасности определяет, будет ли дисковод компакт-дисков доступен одновременно и локальным, и удаленным пользователям. Если данный параметр включен, доступ к компакт-дискам разрешен только пользователям, вошедшим в систему интерактивно. Если данный параметр включен, но никто не вошел в систему интерактивно, дисковод компакт-дисков будет доступен через сеть.	Enabled (Включен)
Devices: Restrict floppy access to locally logged-on user only (Устройства: разрешить доступ к дисководам гибких дисков только локальным пользователям)	Этот параметр безопасности определяет, будет ли съемный дисковод гибких дисков доступен одновременно и локальным, и удаленным пользователям. Если данный параметр включен, доступ к съемным дисководам гибких дисков разрешен только пользователям, вошедшим в систему интерактивно. Если данный параметр включен, но никто не вошел в систему интерактивно, дисковод гибких дисков будет доступен через сеть.	Enabled (Включен)

Интерактивный вход в систему

(англ. — *Interactive Logon*)

▼ Описание политик

Политика	Описание	Значение
Interactive logon: Do not display last user name (Интерактивный вход в систему: не отображать последнее имя пользователя при входе в систему Интерактивный вход в систему: не отображать учетные данные последнего пользователя)	Этот параметр безопасности определяет, будет ли на экране входа в Windows отображаться имя последнего пользователя, выполнившего вход на этом компьютере. Если эта политика включена, имя пользователя не будет отображаться.	Enabled (Включен)
Interactive logon: Do not require CTRL+ALT+DEL (Интерактивный вход в систему: не требовать нажатия CTRL+ALT+DEL)	Этот параметр безопасности определяет, требуется ли нажатие клавиш CTRL+ALT+DEL перед входом в систему. Если эта политика включена, нажатие клавиш CTRL+ALT+DEL перед входом в систему не требуется. Отсутствие необходимости нажимать клавиши CTRL+ALT+DEL перед входом в систему делает пользователей уязвимыми для атак с попыткой перехвата паролей. Обязательное нажатие клавиш CTRL+ALT+DEL перед входом в систему гарантирует передачу данных по доверенному каналу при вводе паролей пользователями. Если эта политика отключена, нажатие клавиш CTRL+ALT+DEL обязательно для любого пользователя перед входом в Windows.	Disabled (Отключен)
Interactive logon: Number of previous logons to cache (in case domain controller is not available) (Интерактивный вход в систему: количество	Сведения о входе в систему каждого уникального пользователя кэшируются локально, чтобы обеспечить возможность входа в систему в случае отсутствия доступа к контроллеру домена во время последующих попыток входа. Хранятся кэшированные сведения о входе в систему из предыдущего сеанса. Если доступ к контроллеру	0 logons (0 входов в систему)

Политика	Описание	Значение
предыдущих подключений к кэшу (в случае отсутствия доступа к контроллеру домена))	домена отсутствует, а сведения о входе в систему для данного пользователя не кэшированы, выводится сообщение: В настоящее время нет доступных серверов входа для обслуживания запроса входа в систему. В этом параметре политики значение 0 отключает кэширование входа в систему. При любом значении выше 50 кэшируется только 50 попыток входа в систему. Windows поддерживает не более 50 записей кэша, при этом число потребляемых записей на пользователя зависит от учетных данных. Например, в системе Windows может быть кэшировано до 50 уникальных учетных записей пользователя с паролями, но не более 25 учетных записей пользователя со смарт-картой, так как сохраняются сведения как о пароле, так и о смарт-карте. При повторном входе в систему пользователя с кэшированными сведениями о входе сведения данного пользователя в кэше заменяются.	
Interactive logon: Require Domain Controller authentication to unlock workstation (Интерактивный вход в систему: требовать проверки на контроллере домена для отмены блокировки компьютера)	Для разблокировки блокированного компьютера необходимо предоставить данные входа. Для учетных записей доменов этот параметр безопасности определяет, необходимо ли установить связь с контроллером домена для разблокировки компьютера. Если этот параметр отключен, пользователь может разблокировать компьютер с помощью кэшированных учетных данных. Если этот параметр включен, используемая для разблокировки компьютера учетная запись домена должна быть проверена контроллером домена на подлинность.	Enabled (Включен)

Клиент сети Microsoft

(англ. — *Microsoft Network Client*)

Описание политик

Политика	Описание	Значение
Microsoft network client: Send unencrypted password to third-party SMB servers (Клиент сети Microsoft: отправлять незашифрованный пароль сторонним SMB-серверам)	Если этот параметр безопасности включен, перенаправителю блока сообщений сервера (SMB) разрешено отправлять пароли открытым текстом на серверы SMB, не принадлежащие Майкрософт, которые не поддерживают шифрование паролей во время проверки подлинности. Отправка незашифрованных паролей представляет риск для безопасности.	Disabled (Отключен)

Доступ к сети / Сетевой доступ

(англ. — *Network Access*)

Описание политик

Политика	Описание	Значение
Network access: Allow anonymous SID/Name translation (Доступ к сети: разрешить трансляцию анонимного SID в имя)	Этот параметр политики определяет, может ли анонимный пользователь запрашивать атрибуты идентификатора безопасности (SID) другого пользователя. Если эта политика включена, то анонимный пользователь может запросить идентификатор безопасности любого другого пользователя. Например, анонимный пользователь, знающий идентификатор безопасности администратора, может подключиться к компьютеру, на котором включена эта политика, и получить имя администратора.	Disabled (Отключен)

Политика	Описание	Значение
	Данный параметр влияет как на преобразование идентификатора безопасности в имя, так и на обратное преобразование (имя в идентификатор безопасности). Если этот параметр политики отключен, анонимный пользователь не может запрашивать идентификатор безопасности другого пользователя.	
Network access: Do not allow anonymous enumeration of SAM accounts (Сетевой доступ: не разрешать перечисление учетных записей SAM анонимными пользователями.)	Этот параметр безопасности определяет, какие дополнительные разрешения будут даны анонимным подключениям к этому компьютеру. Windows разрешает анонимным пользователям совершать определенные действия, такие как перечисление имен учетных записей домена и общих сетевых ресурсов. Это удобно, например, когда администратору требуется предоставить доступ пользователям в доверенном домене, не поддерживающем взаимное доверие. Этот параметр безопасности позволяет накладывать дополнительные ограничения на анонимные подключения. Включен: не разрешать перечисление учетных записей SAM. Этот параметр заменяет параметр "Все" на параметр "Прошедшие проверку" в разрешениях безопасности для ресурсов. Отключен: нет дополнительных ограничений. Используются разрешения по умолчанию.	Enabled (Включен)
Network access: Do not allow anonymous enumeration of SAM accounts and shares (Сетевой доступ: не разрешать перечисление учетных записей	Этот параметр безопасности определяет, разрешено ли перечисление учетных записей SAM и общих ресурсов анонимными пользователями. Windows разрешает анонимным пользователям совершать некоторые действия (например, перечисление имен учетных записей домена и общих папок). Это удобно в случае, если администратор хочет предоставить доступ	Enabled (Включен)

Политика	Описание	Значение
SAM и общих ресурсов анонимными пользователями)	пользователям в доверенном домене, не поддерживающем взаимное доверие. Чтобы запретить перечисление учетных записей SAM и общих ресурсов анонимными пользователями, включите этот параметр.	
Network access: Do not allow storage of passwords and credentials for network authentication (Сетевой доступ: не разрешать хранение паролей или учетных данных для сетевой проверки подлинности)	Этот параметр безопасности определяет, сохраняются ли диспетчером учетных данных пароли и учетные данные при проверке подлинности доменом (для последующего использования). Если данный параметр включен, то сохранение паролей и учетных данных диспетчером учетных данных на данном компьютере не производится. Если данный параметр политики выключен или значение для него не задано, то диспетчер учетных данных будет сохранять пароли и учетные данные на этом компьютере (для использования в будущем при проверке подлинности доменом). Примечание. Изменения в конфигурации этого параметра безопасности вступят в силу только после перезагрузки Windows.	Enabled (Включен)
Network access: Let Everyone permissions apply to anonymous users (Сетевой доступ: разрешать применение разрешений "Для всех" к анонимным пользователям)	Этот параметр безопасности определяет, какие дополнительные разрешения будут даны анонимным подключениям к компьютеру. Windows разрешает анонимным пользователям совершать некоторые действия (например, перечисление имен учетных записей домена и общих папок). Это удобно в случае, если администратор хочет предоставить доступ пользователям в доверенном домене, не поддерживающем взаимное доверие. По умолчанию идентификатор безопасности "Для всех" удаляется из токена, созданного для анонимных соединений. Таким образом,	Disabled (Отключен)

Политика	Описание	Значение
	разрешения группы "Для всех" не затрагивают анонимных пользователей. Если этот параметр установлен, анонимные пользователи имеют доступ только к тем ресурсам, доступ к которым им разрешен явным образом. Если этот параметр включен, идентификатор безопасности "Для всех" добавляется к токену, созданному для анонимных соединений. В этом случае анонимные пользователи имеют доступ к любому ресурсу, разрешенному для группы "Для всех".	
Network access: Named Pipes that can be accessed anonymously (Сетевой доступ: разрешать анонимный доступ к именованным каналам)	Этот параметр безопасности определяет, какие сеансы связи (каналы) будут иметь атрибуты и разрешения, дающие право анонимного доступа.	Не определено
Network access: Remotely accessible registry paths (Сетевой доступ: удаленно доступные пути реестра)	Этот параметр безопасности определяет, какие пути реестра могут быть доступны через сеть вне зависимости от пользователей или групп пользователей, указанных в списке управления доступом (ACL) раздела реестра winreg.	Не определено
Network access: Remotely accessible registry paths and sub-paths (Сетевой доступ: удаленно доступные пути и	Этот параметр безопасности определяет, какие пути и вложенные пути реестра могут быть доступны через сеть вне зависимости от пользователей или групп пользователей, указанных в списке управления доступом (ACL) раздела реестра winreg.	Не определено

Политика	Описание	Значение
вложенные пути реестра.)		
Network access: Restrict anonymous access to Named Pipes and Shares (Сетевой доступ: запретить анонимный доступ к именованным каналам и общим ресурсам)	Если этот параметр безопасности включен, он ограничивает анонимный доступ к общим ресурсам и именованным каналам в соответствии со значениями следующих параметров: Сетевой доступ: разрешать анонимный доступ к именованным каналам Сетевой доступ: разрешать анонимный доступ к общим ресурсам	Enabled (Включен)
Network access: Shares that can be accessed anonymously (Сетевой доступ: разрешать анонимный доступ к общим ресурсам)	Этот параметр безопасности определяет, к каким общим ресурсам могут получать доступ анонимные пользователи.	Не определено
Network access: Sharing and security model for local accounts (Сетевой доступ: модель общего доступа и безопасности для локальных учетных записей.)	Этот параметр безопасности определяет, каким образом проверяется подлинность при входе в сеть с использованием локальных учетных записей. Если данный параметр имеет значение "Обычная", при входе в сеть с учетными данными локальной учетной записи выполняется проверка подлинности по этим учетным данным. Обычная модель позволяет более гибко управлять доступом к ресурсам. С ее помощью можно предоставить разным пользователям разные типы доступа к одному и тому же ресурсу. Если этот параметр имеет значение "Гостевая", операции входа в сеть с учетными данными	Classic - local users authenticate as themselves (Обычная - локальные пользователи удостоверяются как они сами)

Политика	Описание	Значение
	локальных учетных записей автоматически сопоставляются с учетной записью гостя. При использовании гостевой модели между пользователями нет различий. Все пользователи проходят проверку подлинности с учетной записью гостя и получают одинаковый уровень доступа к данному ресурсу — "Только чтение" или "Изменение". По умолчанию на компьютерах домена: Обычная. По умолчанию на автономных компьютерах: Гостевая. Внимание! Если используется гостевая модель, любой пользователь, имеющий доступ к компьютеру по сети (включая анонимных пользователей Интернета), может получить доступ к общим ресурсам. Для защиты компьютера от несанкционированного доступа необходимо использовать брандмауэр Windows или другую аналогичную программу. Кроме того, при использовании обычной модели локальные учетные записи должны быть защищены паролем, чтобы их невозможно было использовать для доступа к общим ресурсам системы. Примечание Этот параметр не влияет на операции интерактивного входа в систему, которые выполняются удаленно с помощью таких служб, как Telnet или служб удаленных рабочих столов.	

Сетевая безопасность

(англ. — *Network Security*)

▼ Описание политик

Политика	Описание	Значение
Network security: Do not store LAN Manager hash value on next password change (Сетевая безопасность: не хранить хэш-значения LAN Manager при следующей смене пароля)	Этот параметр безопасности определяет, нужно ли при следующей смене пароля сохранять хэш-значение диспетчера LAN (LM) для нового пароля. Хэш LM является относительно слабым и уязвимым для атак по сравнению с более криптостойким хэшем Windows NT. Поскольку хэш LM хранится в базе данных безопасности на локальном компьютере, в случае атаки на базу данных безопасности пароли могут быть расшифрованы.	Enabled (Включен)
Network security: Force logoff when logon hours expire (Сетевая безопасность: Принудительный вывод из сеанса по истечении допустимых часов работы)	Этот параметр безопасности определяет, будут ли отключаться пользователи при подключении к локальному компьютеру вне времени входа, заданного для их учетной записи. Этот параметр влияет на компонент блока сообщений сервера (SMB). Если эта политика включена, после истечения времени входа клиента сеансы клиента с сервером SMB принудительно разрываются. Если эта политика отключена, после истечения времени входа клиента его сеанс сохраняется. Примечание. Этот параметр безопасности применяется так же, как политика учетной записи. Для учетных записей домена может существовать только одна политика учетных записей. Политика учетной записи должна быть определена в политике домена по умолчанию; она применяется контроллерами данного домена. Контроллер домена всегда получает политику учетной записи из объекта групповой политики (GPO) политики домена по умолчанию, даже если существует другая политика учетной записи, которая применяется к подразделению, содержащему этот контроллер домена. По умолчанию рабочие	Enabled (Включен)

Политика	Описание	Значение
	станции и серверы, входящие в домен, получают ту же политику учетной записи для своих локальных учетных записей. Однако политики локальных учетных записей таких компьютеров могут отличаться от политики учетной записи домена, если определена политика учетной записи для подразделения, в которое входят эти компьютеры. Параметры Kerberos не применяются к таким компьютерам.	
Network security: LAN Manager authentication level (Сетевая безопасность: уровень проверки подлинности LAN Manager)	Этот параметр безопасности определяет, какие протоколы проверки подлинности с запросом и ответом используются для сетевого входа в систему. Значение этого параметра влияет на уровень протокола проверки подлинности, который используют клиенты, на уровень согласованной безопасности сеанса, а также на уровень проверки подлинности, принимаемой серверами, следующим образом. Отправлять ответы LM и NTLM: клиенты используют проверку подлинности LM и NTLM и никогда не используют сеансовую безопасность NTLMv2; контроллеры домена принимают проверку подлинности LM, NTLM и NTLMv2. Отправлять LM и NTLM - использовать сеансовую безопасность NTLMv2 при согласовании: клиенты используют проверку подлинности LM и NTLM, а также сеансовую безопасность NTLMv2, если сервер ее поддерживает; контроллеры домена принимают проверку подлинности LM, NTLM и NTLMv2. Отправлять только NTLM-ответ: клиенты используют только проверку подлинности NTLM, а также сеансовую безопасность NTLMv2, если сервер ее поддерживает; контроллеры домена принимают проверку подлинности LM, NTLM и NTLMv2. Отправлять только NTLMv2-ответ:	Send NTLMv2 response only. Refuse LM & NTLM (Отправлять только NTLMv2-ответ. Отказывать LM и NTLM)

Политика	Описание	Значение
	клиенты используют только проверку подлинности NTLMv2, а также сеансовую безопасность NTLMv2, если сервер ее поддерживает; контроллеры домена принимают проверку подлинности LM, NTLM и NTLMv2. Отправлять только NTLMv2-ответ и отказывать LM: клиенты используют только проверку подлинности NTLMv2, а также сеансовую безопасность NTLMv2, если сервер ее поддерживает; контроллеры домена отклоняют LM (принимая только проверку подлинности NTLM и NTLMv2). Отправлять только NTLMv2-ответ и отказывать LM и NTLM: клиенты используют только проверку подлинности NTLMv2, а также сеансовую безопасность NTLMv2, если сервер ее поддерживает; контроллеры домена отклоняют LM и NTLM (принимая только проверку подлинности NTLMv2).	
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients (Сетевая безопасность: минимальная сеансовая безопасность для клиентов на базе NTLM SSP (включая безопасный RPC).)	Этот параметр безопасности позволяет клиенту требовать согласования 128-разрядного шифрования и (или) сеансовой безопасности NTLMv2. Эти значения зависят от значения параметра безопасности "Уровень проверки подлинности LAN Manager". Доступны следующие варианты. Требовать сеансовую безопасность NTLMv2. Если протокол NTLMv2 не согласован, подключение не будет установлено. Требовать 128-разрядное шифрование. Если стойкое (128-разрядное) шифрование не согласовано, подключение не будет установлено.	Require NTLMv2 session security: Enabled Require 128-bit encryption: Enabled (Требовать сеансовую безопасность NTLMv2: Включен Требовать 128-битное шифрование: Включен)
Network security: Minimum session	Этот параметр безопасности позволяет серверу требовать согласования 128-разрядного	Require NTLMv2 session security:

Политика	Описание	Значение
security for NTLM SSP based (including secure RPC) servers (Сетевая безопасность: минимальная сеансовая безопасность для серверов на базе NTLM SSP (включая безопасный RPC).)	шифрования и (или) сеансовой безопасности NTLMv2. Эти значения зависят от значения параметра безопасности "Уровень проверки подлинности LAN Manager". Доступны следующие варианты. Требовать сеансовую безопасность NTLMv2. Если целостность сообщений не согласована, подключение не будет установлено. Требовать 128-битное шифрование. Если стойкое (128-разрядное) шифрование не согласовано, подключение не будет установлено.	Enabled Require 128-bit encryption: Enabled (Требовать сеансовую безопасность NTLMv2: Включен Требовать 128-битное шифрование: Включен)

Завершение работы

(англ. — *Shutdown*)

▼ Описание политик

Политика	Описание	Значение
Shutdown: Allow system to be shut down without having to log on (Завершение работы: разрешить завершение работы системы без выполнения входа в систему.)	Этот параметр безопасности определяет, можно ли завершить работу компьютера, не выполняя вход в систему Windows. Если эта политика включена, команду "Завершение работы" можно выбрать на экране входа в Windows. Если эта политика отключена, команда "Завершение работы" не отображается на экране входа в Windows. В этом случае, чтобы завершить работу системы, пользователю необходимо успешно выполнить вход в систему и он должен иметь право на завершение работы системы.	Disabled (Отключен)

Политика	Описание	Значение
Shutdown: Clear virtual memory pagefile (Завершение работы: очистка файла подкачки виртуальной памяти)	Этот параметр безопасности определяет, будет ли выполняться очистка файла подкачки виртуальной памяти при завершении работы системы. Поддержка виртуальной памяти использует файл подкачки системы для выгрузки страниц памяти на диск, когда они не используются. Во время работы системы файл подкачки открыт операционной системой в монопольном режиме и хорошо защищен. Однако если система настроена так, что допускает загрузку других операционных систем, необходимо убедиться, что при завершении работы системы выполняется очистка ее файла подкачки. Это гарантирует, что уязвимые сведения из памяти процессов, которые могли попасть в файл подкачки, не станут доступны пользователям, получившим прямой несанкционированный доступ к этому файлу. Если эта политика включена, при корректном завершении работы системы выполняется очистка файла подкачки системы. Если этот параметр безопасности включен, также выполняется обнуление файла режима гибернации (hiberfil.sys), когда этот режим отключен.	Enabled (Включен)

Параметры системы

(англ. — *System Settings*)

▼ Описание политик

Политика	Описание	Значение
System settings: Optional subsystems (Параметры системы: необязательные подсистемы)	Этот параметр безопасности определяет, какие дополнительные подсистемы могут быть запущены для поддержки приложений. С помощью этого параметра можно указать все подсистемы, которые необходимы для поддержки приложений в соответствии с требованиями среды.	Не определено
System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies (Параметры системы: использовать правила сертификатов для исполняемых файлов Windows для политик ограниченного использования программ)	Этот параметр безопасности определяет, выполняется ли обработка цифровых сертификатов, когда пользователь или процесс пытается запустить программу с расширением имени файла EXE. Он позволяет включить или отключить правила сертификатов — тип правил политик ограниченного использования программ. С помощью таких политик вы можете создать правило сертификатов, которое разрешает или запрещает запуск программы, подписанной с помощью Authenticode, в зависимости от того, какой цифровой сертификат ей соответствует. Чтобы применить правила сертификатов, необходимо включить данный параметр безопасности. Если правила сертификатов включены, политики ограниченного использования программ проверяют список отзыва сертификатов (CRL), чтобы убедиться, что сертификат и подпись программы действительны. Это может привести к снижению производительности при запуске подписанных программ. Вы можете отключить эту функцию. В окне свойств доверенного издателя снимите флажки "Издатель" и "Отметка времени". Дополнительные сведения см. в разделе "Задание параметров доверенного издателя".	Enabled (Включен)

Контроль учетных записей

(англ. — *User Account Control*)

▼ Описание политик

Политика	Описание	Значение
User Account Control: Admin Approval Mode for the Built-in Administrator account (Контроль учетных записей: режим одобрения администратором для встроенной учетной записи администратора)	Этот параметр политики определяет характеристики режима одобрения администратором для встроенной учетной записи администратора. Возможные значения Включено. Для встроенной учетной записи администратора используется режим одобрения администратором. По умолчанию любая операция, требующая повышения привилегий, предлагает пользователю подтвердить операцию. Отключено (по умолчанию). Встроенная учетная запись администратора выполняет все приложения с полными привилегиями администратора.	Enabled (Включен)
User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop (Контроль учетных записей: разрешать UIAccess-приложениям запрашивать повышение прав, не используя безопасный рабочий стол.)	Этот параметр политики определяет, могут ли UIAccess-приложения (UIA-программы) автоматически отключать безопасный рабочий стол для запросов на повышение, используемых обычным пользователем. Включено. UIA-программы, в том числе удаленный помощник Windows, автоматически отключают безопасный рабочий стол для запросов на повышение прав. Если не отключен параметр политики "Контроль учетных записей: переключение к безопасному рабочему столу при выполнении запроса на повышение прав", приглашение появится на интерактивном рабочем столе пользователя, а не на безопасном рабочем столе. Отключено (по умолчанию). Безопасный рабочий стол может быть отключен только пользователем интерактивного	Disabled (Отключен)

Политика	Описание	Значение
	рабочего стола или путем отключения параметра политики "Контроль учетных записей: переключение к безопасному рабочему столу при выполнении запроса на повышение прав".	
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode (Контроль учетных записей: поведение запроса на повышение прав для администраторов в режиме одобрения администратором)	Этот параметр политики определяет поведение запроса на повышение привилегий для администраторов. Возможные значения Повышение без запроса. Позволяет привилегированным учетным записям выполнить операцию, требующую повышения привилегий, без подтверждения согласия или ввода учетных данных. Примечание. Этот вариант должен использоваться только в средах с максимальными ограничениями. Запрос учетных данных на безопасном рабочем столе. Для любой операции, требующей повышения привилегий, на безопасном рабочем столе выводится приглашение ввести имя и пароль привилегированного пользователя. Если вводятся привилегированные учетные данные, операция продолжается продолжена с максимальными доступными привилегиями пользователя. Запрос согласия на безопасном рабочем столе. Для любой операции, требующей повышения привилегий, на безопасном рабочем столе выводится приглашение выбрать: "Разрешить" или "Запретить". Если пользователь выбирает "Разрешить", операция продолжается с максимальными доступными привилегиями пользователя. Запрос учетных данных. Для любой операции, требующей повышения привилегий, выводится приглашение ввести имя пользователя и пароль учетной записи администратора. Если вводятся допустимые учетные данные, операция продолжается с соответствующими привилегиями.	Prompt for consent for non-Windows binaries (Запрос согласия для исполняемых файлов, отличных от Windows)

Политика	Описание	Значение
	Запрос согласия. Для любой операции, требующей повышения привилегий, пользователю предлагается выбрать: "Разрешить" или "Запретить". Если пользователь выбирает "Разрешить", операция продолжается с максимальными доступными привилегиями пользователя. Запрос согласия для сторонних двоичных файлов (не Windows) (по умолчанию). Когда операция для приложения стороннего (не Майкрософт) производителя требует повышения привилегий, на безопасном рабочем столе выводится приглашение выбрать: "Разрешить" или "Запретить". Если пользователь выбирает "Разрешить", операция продолжается с максимальными доступными привилегиями пользователя.	
User Account Control: Behavior of the elevation prompt for standard users (Контроль учетных записей: поведение запроса на повышение прав для обычных пользователей)	Этот параметр политики определяет поведение запроса на повышение привилегий для обычных пользователей. Возможные значения Запрос учетных данных (по умолчанию). Когда операция требует повышения привилегий, выводится приглашение ввести имя пользователя и пароль учетной записи пользователя с привилегиями администратора. Если пользователь вводит действительные учетные данные, операция продолжается с соответствующими привилегиями. Автоматическое отклонение запросов на повышение привилегий. Когда операция требует повышения привилегий, отображается сообщение об ошибке отказа в доступе. Организации, настольные компьютеры которых используются обычными пользователями, могут выбрать этот параметр политики для уменьшения числа обращений в службу поддержки. Запрос учетных данных на безопасном рабочем столе. Когда	Prompt for credentials on the secure desktop (Запрос учетных данных на безопасном рабочем столе)

Политика	Описание	Значение
	операция требует повышения привилегий, на безопасном рабочем столе выводится приглашение ввести имя и пароль другого пользователя. Если пользователь вводит допустимые учетные данные, операция продолжается с соответствующими привилегиями.	
User Account Control: Only elevate UIAccess applications that are installed in secure locations (Контроль учетных записей: повышать права для UIAccess-приложений, только при установке в безопасных местах)	Контроль учетных записей: повышать права только для UIAccess-приложений, установленных в безопасном местоположении Этот параметр политики управляет тем, должны ли приложения, запрашивающие выполнение на уровне целостности UIAccess, находиться в безопасной папке файловой системы. Безопасными считаются только следующие папки: …\Program Files\, включая вложенные папки …\Windows\system32\ …\Program Files (x86)\, включая вложенные папки для 64-разрядных версий Windows Примечание. Windows принудительно проводит обязательную проверку подписей PKI для любого интерактивного приложения, запрашивающего выполнение на уровне целостности UIAccess, вне зависимости от состояния данного параметра безопасности. Возможные значения. Включено (по умолчанию). Приложение будет запускаться с уровнем целостности UIAccess только в том случае, если оно находится в безопасной папке файловой системы. Отключено. Приложение будет запускаться с уровнем целостности UIAccess, даже если оно не находится в безопасной папке файловой системы.	Enabled (Включен)
User Account Control: Run all administrators in Admin Approval Mode (Контроль	Этот параметр политики определяет характеристики всех политик контроля учетных записей для компьютера. При изменении этого параметра политики необходимо перезагрузить	Enabled (Включен)

Политика	Описание	Значение
учетных записей: все администраторы работают в режиме одобрения администратором)	компьютер. Возможные значения Включено (по умолчанию). Режим одобрения администратором включен. Чтобы разрешить встроенной учетной записи администратора и всем остальным пользователям, являющимся участниками группы "Администраторы", работать в режиме одобрения администратором, эта политика должна быть включена, а все связанные политики управления учетными записями также должны быть установлены соответствующим образом. Отключено. Режим одобрения администратором и все соответствующие параметры политики контроля учетных записей будут отключены. Примечание. Если этот параметр политики отключен, центр обеспечения безопасности выдаст уведомление, что общая безопасность операционной системы снизилась.	
User Account Control: Switch to the secure desktop when prompting for elevation (Контроль учетных записей: переключение к безопасному рабочему столу при выполнении запроса на повышение прав)	Этот параметр политики определяет, будут ли запросы на повышение прав выводиться на интерактивный рабочий стол пользователя или на безопасный рабочий стол. Возможные значения. Включено (по умолчанию). Все запросы на повышение прав выводятся на безопасный рабочий стол независимо от параметров политики поведения приглашения для администраторов и обычных пользователей. Отключено: все запросы на повышение прав выводятся на интерактивный рабочий стол пользователя. Используются параметры политики поведения приглашения для администраторов и обычных пользователей.	Enabled (Включен)
User Account Control: Virtualize file and registry write failures to per-user locations	Этот параметр политики управляет перенаправлением сбоев записи приложений в определенные расположения в реестре и файловой системе. Этот параметр политики	Enabled (Включен)

Политика	Описание	Значение
(Контроль учетных записей: при сбоях записи в файл или реестр виртуализация в размещение пользователя)	позволяет уменьшить опасность приложений, которые выполняются от имени администратора и во время выполнения записывают данные в папку %ProgramFiles%, %Windir%; %Windir%\system32 или HKLM\Software... Возможные значения. Включено (по умолчанию). Сбои записи приложений перенаправляются во время выполнения в определенные пользователем расположения в файловой системе и реестре. Отключено. Выполнение приложений, записывающих данные в безопасные расположения, заканчивается ошибкой.	

Прочие

(англ. — *Other*)

▼ Описание политик

Политика	Описание	Значение
Accounts: Block Microsoft accounts (Учетные записи: блокировать учетные записи Майкрософт)	Этот параметр политики не позволяет пользователям добавлять новые учетные записи Майкрософт на данном компьютере. Если выбрать вариант "Пользователи не могут добавлять учетные записи Майкрософт", пользователи не смогут создавать новые учетные записи Майкрософт на этом компьютере, преобразовывать локальные учетные записи в учетные записи Майкрософт, а также подключать учетные записи домена к учетным записям Майкрософт. Этот вариант предпочтителен, если требуется ограничить число используемых учетных записей Майкрософт в организации. Если выбрать вариант "Пользователи не могут добавлять	Users can't add Microsoft accounts (Пользователи не могут добавлять учетные записи Майкрософт)

Политика	Описание	Значение
	учетные записи Майкрософт и использовать их для входа", существующие пользователи учетных записей Майкрософт не смогут войти в систему Windows. Выбор этого параметра может сделать вход в систему и управление ею недоступным для существующего администратора на данном компьютере. Если эта политика отключена или не настроена (рекомендуется), пользователи смогут использовать учетные записи Майкрософт в Windows.	
Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings (Аудит: принудительно переопределяет параметры категории политики аудита параметрами подкатегории политики аудита (ОС Windows Vista или более поздние версии).)	ОС Windows Vista и более поздние версии Windows позволяют точнее управлять политикой аудита при помощи подкатегорий политики аудита. Установка политики аудита на уровне категории переопределит новую функцию политики аудита подкатегории. Чтобы обеспечить управление политикой аудита при помощи подкатегорий без необходимости изменения групповой политики, в Windows Vista и более поздних версиях предусмотрено новое значение реестра (SCENoApplyLegacyAuditPolicy), запрещающее применение политики аудита уровня категории из групповой политики и из средства администрирования "Локальная политика безопасности". Если установленная здесь политика аудита уровня категории не согласуется с формируемыми событиями, то причина может быть в том, что установлен этот раздел реестра.	Enabled (Включен)
Domain member: Disable machine account password changes (Член домена: отключить изменение	Определяет, производится ли периодическое изменение пароля учетной записи компьютера члена домена. При включении этого параметра член домена не пытается изменить пароль учетной записи компьютера. Если этот параметр отключен, член домена пытается изменить пароль учетной записи компьютера согласно значению параметра "Член	Disabled (Отключен)

Политика	Описание	Значение
пароля учетных записей компьютера)	домена: максимальный срок действия пароля учетной записи компьютера", имеющего по умолчанию значение "каждые 30 дней". По умолчанию: Отключено. Примечания Не следует включать этот параметр безопасности. Пароли учетных записей используются для установления безопасных каналов связи между членами домена и контроллерами домена, а также между самими контроллерами внутри домена. После установления связи безопасный канал используется для передачи конфиденциальных данных, необходимых для выполнения проверки подлинности и авторизации. Этот параметр не следует использовать для поддержки сценариев двойной загрузки, использующих одну и ту же учетную запись компьютера. Для двойной загрузки двух установок, объединенных в одном домене, присвойте этим установкам разные имена компьютеров.	
Domain member: Maximum machine account password age (Член домена: максимальный срок действия пароля учетных записей компьютера)	Этот параметр безопасности определяет, как часто член домена будет пытаться изменить пароль учетной записи компьютера.	30 дней
Domain member: Require strong (Windows 2000 or later) session key (Член домена: требовать стойкий	Этот параметр безопасности определяет, требуется ли для зашифрованных данных безопасного канала 128-разрядный ключ. При присоединении компьютера к домену создается учетная запись компьютера. После этого при запуске системы для создания безопасного канала с контроллером домена используется пароль учетной записи компьютера.	Enabled (Включен)

Политика	Описание	Значение
сеансовый ключ (Windows 2000 или выше))	Этот безопасный канал используется для совершения таких операций, как сквозная проверка подлинности NTLM, поиск имени или ИД безопасности LSA и т. д. В зависимости от версии Windows, используемой на контроллере домена, с которым осуществляется соединение, а также от значений параметров: Член домена: всегда требуется цифровая подпись или шифрование данных безопасного канала Член домена: шифровать данные безопасного канала, когда это возможно Будут зашифрованы все или некоторые данные, передаваемые по безопасному каналу. Этот параметр политики определяет, требуется ли для зашифрованных данных безопасного канала 128-разрядный ключ. Если этот параметр включен, безопасное соединение будет установлено только в том случае, если возможно 128-разрядное шифрование. Если этот параметр отключен, стойкость ключа согласуется с контроллером домена.	
Interactive logon: Display user information when the session is locked (Интерактивный вход в систему: отображать сведения о пользователе, если сеанс заблокирован.)	Этот параметр определяет, будут ли такие дополнительные сведения, как адрес электронной почты или домен/имя пользователя, отображаться вместе с именем пользователя на экране входа в систему. У клиентов, использующих Windows 10 версий 1511 и 1507 (RTM), этот параметр работает так же, как и в предыдущих версиях Windows. Ввиду добавления нового параметра конфиденциальности в Windows 10 версии 1607 этот параметр применяется к таким клиентам иначе. Изменения в Windows 10 версии 1607 Начиная с версии 1607 в Windows 10 имеется новая функциональная возможность, благодаря которой можно по умолчанию скрывать такие сведения пользователя, как адрес электронной почты, и изменять стандартные настройки, чтобы эти сведения отображались. Настроить данную	User display name only (Только имя пользователя)

Политика	Описание	Значение
	функциональную возможность можно с помощью нового параметра конфиденциальности в разделе «Параметры» > «Учетные записи» > «Параметры входа». По умолчанию параметр конфиденциальности выключен, а дополнительные сведения пользователя скрыты. Данный параметр групповой политики определяет эту же функциональную возможность. Данному параметру можно присваивать следующие значения: Выводимое имя пользователя, имена домена и пользователя: в случае осуществления локального входа отображается полное имя пользователя. Если пользователь входит через учетную запись Майкрософт, отображается адрес электронной почты пользователя. В случае входа в домен отображается домен/имя_пользователя. Только имя пользователя: отображается полное имя пользователя, заблокировавшего сеанс. Не отображать сведения о пользователе: никакие имена не отображаются, однако во всех версиях Windows старше Windows 10 на экране смены пользователя будут отображаться полные имена пользователей. Начиная с версии 1607 Windows 10, эта функция не поддерживается. Если выбрано данное значение, на экране будет отображаться полное имя пользователя, заблокировавшего сеанс. Данное изменение обеспечивает соответствие этого параметра новому параметру конфиденциальности. Чтобы на экране не отображалось никакой информации о пользователе, включите параметр групповой политики "Интерактивный вход": не отображать данные пользователя, последним входившим в систему. Пусто: стандартное значение. Означает «Не определено», однако на экране будет отображаться полное имя пользователя точно так же, как и при выборе значения «Только имя пользователя».	

Политика	Описание	Значение
	Исправление для Windows 10 версии 1607 В случае использования Windows 10 версии 1607 данные пользователя не будут отображаться на экране входа в систему, даже если выбрано значение «Выводимое имя пользователя, имена домена и пользователя», поскольку отключен параметр конфиденциальности. Если включить этот параметр, данные появятся на экране. Групповое изменение настроек параметра конфиденциальности невозможно. Вместо этого можно применить KB4013429 к клиентам с Windows 10 версии 1607, чтобы система действовала аналогично предыдущим версиям Windows. Взаимодействие с командой «Запретить пользователю отображать данные учетной записи на экране входа» Во всех версиях Windows 10 по умолчанию отображается только имя пользователя. Если задано значение «Запретить пользователю отображать данные учетной записи на экране входа», на экране входа будет отображаться только выводимое имя пользователя независимо от настроек групповой политики. Пользователи не смогут выводить на экран свои сведения. Если значение «Запретить пользователю отображать данные учетной записи на экране входа» не задано, можно задать для параметра «Интерактивный вход в систему: отображать сведения о пользователе, если сеанс заблокирован» значение «Выводимое имя пользователя, имена домена и пользователя », чтобы на экране входа в систему отображались такие дополнительные сведения пользователя, как домен\имя пользователя. В этом случае на клиентских компьютерах с Windows 10 версии 1607 необходимо применить KB4013429. Пользователи не смогут скрыть дополнительные сведения. Рекомендации Возможности применения этой политики зависят от ваших требований безопасности	

Политика	Описание	Значение
	в отношении отображаемых учетных данных для входа. Если вы работаете с компьютерами, на которых хранится конфиденциальная информация, а мониторы находятся в незащищенных местах, либо если к вашим компьютерам с конфиденциальной информацией имеется удаленный доступ, то отображение полных имен вошедших в систему пользователей или имен учетной записи домена может противоречить вашей общей политике безопасности. С учетом вашей политики безопасности может быть целесообразным установление значения «Интерактивный вход в систему: не отображать учетные данные последнего пользователя».	
Interactive logon: Machine account lockout threshold (Интерактивный вход в систему: пороговое число неудачных попыток входа)	Этот параметр безопасности определяет количество неудачных попыток входа в систему, после которого компьютер перезагружается. Компьютеры, на которых для защиты томов ОС включена функция Bitlocker, будут заблокированы. Для снятия блокировки необходимо указать в консоли ключ восстановления. Убедитесь, что включены соответствующие политики восстановления доступа. Количество неудачных попыток доступа может быть задано числом от 1 до 999. Если установить это значение равным 0, компьютер никогда не будет блокироваться. Значения от 1 до 3 будут интерпретированы как 4. Неудачные попытки ввода паролей на рабочих станциях или рядовых серверах, заблокированных с помощью клавиш CTRL+ALT+DEL или с помощью защищенных паролем заставок, считаются неудачными попытками входа в систему.	5 invalid logon attempts (5 до блокировки учетной записи компьютера)
Microsoft network server: Amount of idle time required before suspending	Этот параметр безопасности определяет продолжительность отрезка времени SMB-сеанса до его приостановки по причине неактивности. Администраторы могут использовать этот параметр	15 минут

Политика	Описание	Значение
session (Сервер сети Microsoft: время бездействия до приостановки сеанса)	для управления временем приостановки неактивного SMB-сеанса компьютером. Если клиентская активность возобновляется, сеанс автоматически устанавливается заново. Для этого параметра значение "0" означает отсоединение сеанса сразу, как только это представится возможным. Максимальное значение - 99999, что составляет 208 дней; в действительности такое значение отключает этот параметр. По умолчанию: параметр не определен; это означает, что система рассматривает параметр как имеющий значение "15" для серверов и неопределенное значение для рабочих станций.	
Microsoft network server: Attempt S4U2Self to obtain claim information (Сетевой сервер (Майкрософт): попытка S4U2Self получить информацию об утверждении)	Этот параметр безопасности предназначен для поддержки клиентов с системами, выпущенными до Windows 8, которые пытаются получить доступ к общему файловому ресурсу, требующему заявку пользователя. Он определяет, будет ли локальный файловый сервер пытаться использовать функцию Kerberos Service-For-User-To-Self (S4U2Self) для получения заявок субъекта клиента сети из домена учетной записи клиента. Этот параметр необходимо включать только в том случае, если файловый сервер использует заявки пользователей для управления доступом к файлам и если он будет поддерживать субъекты клиентов, учетные записи которых находятся в домене с клиентскими компьютерами и контроллерами домена под управлением операционной системы, выпущенной до Windows 8. Для этого параметра нужно задать значение "Автоматически" (используется по умолчанию), чтобы файловый сервер мог автоматически определять, требуется ли для пользователя заявка. Для этого параметра нужно явно задавать значение "Включено" только в том случае, если есть политики доступа к локальным файлам, включающие заявки	Disabled (Отключено)

Политика	Описание	Значение
	пользователей на доступ. Если этот параметр безопасности включен, файловый сервер Windows будет анализировать маркер доступа субъекта сетевого клиента, прошедшего проверку подлинности, и определять, присутствует ли информация о заявке. Если заявок нет, файловый сервер будет использовать функцию Kerberos S4U2Self для связи с контроллером домена Windows Server 2012 в домене учетной записи клиента и получения маркера доступа, поддерживающего заявки, для субъекта клиента. Маркер, поддерживающий заявки на доступ, может потребоваться для доступа к файлам и папкам, к которым применена политика управления доступом на основе заявок. Если этот параметр отключен, файловый сервер Windows не будет пытаться получить маркер доступа на основе заявок для субъекта клиента.	
Microsoft network server: Disconnect clients when logon hours expire (Сервер сети Microsoft: отключать клиентов по истечении разрешенных часов входа)	Этот параметр безопасности определяет, будут ли отключаться пользователи, подключенные к локальному компьютеру, по истечении разрешенного времени входа, заданного для их учетной записи. Этот параметр влияет на компонент протокола SMB. Если этот параметр включен, по истечении разрешенного времени входа клиента сеансы клиента со службой SMB принудительно разрываются. Если этот параметр отключен, по истечении разрешенного времени входа клиента его сеанс сохраняется.	Enabled (Включен)
Microsoft network server: Server SPN target name validation level (Сетевой сервер (Майкрософт):	Этот параметр политики управляет уровнем проверки, выполняемой компьютером с общими папками или принтерами (сервером) над именем субъекта-службы, предоставляемым клиентским компьютером при установлении последним сеанса с помощью протокола SMB. Протокол SMB предоставляет основу	Off (Откл.)

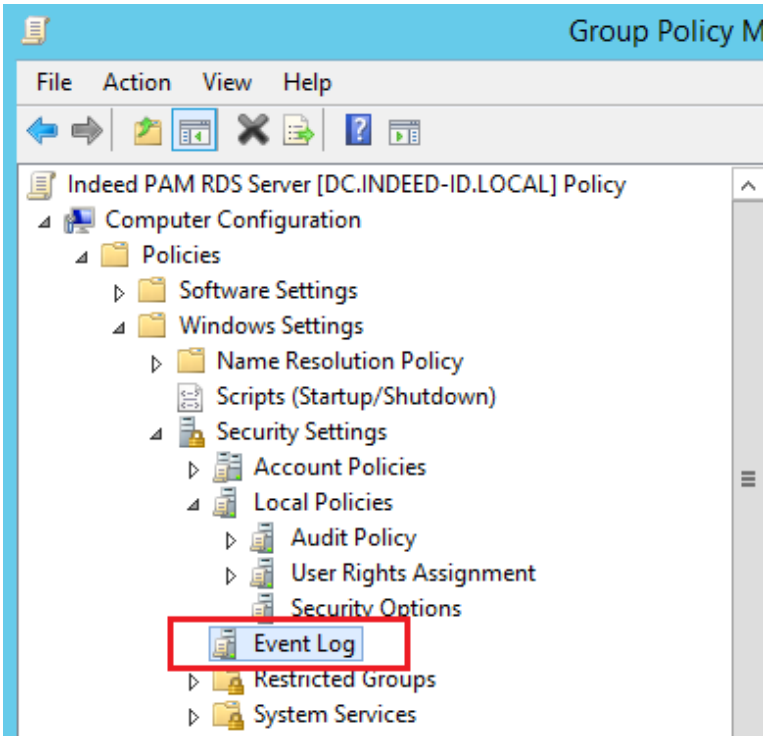
Политика	Описание	Значение
уровень проверки сервером имени участника-службы конечного объекта)	для совместного доступа к файлам и принтерам, а также для других сетевых операций, например для удаленного администрирования Windows. Протокол SMB поддерживает проверку имени субъекта-службы SMB-сервера в большом двоичном объекте, предоставляемом SMB-клиентом, для предотвращения класса атак против SMB-серверов, называемых атаками с перехватами. Этот параметр влияет на SMB1 и SMB2. Этот параметр безопасности определяет уровень проверки, выполняемой SMB-сервером над именем субъекта-службы, предоставляемым SMB-клиентом при установлении последним сеанса с SMB-сервером. Параметры: Откл. - имя субъекта-службы SMB-клиента не требуется (не проверяется) SMB-сервером. Принимать, если предоставлено клиентом - SMB-сервер принимает и проверяет имя субъекта-службы, предоставляемое SMB-клиентом, и разрешает сеанс, если оно совпадает со списком имен субъектов-служб SMB-сервера. Если имя НЕ совпадает, то сеанс для SMB-клиента отклоняется. Требовать от клиента - SMB-клиент ДОЛЖЕН отправить имя субъекта-службы при настройке сеанса, а указанное имя ДОЛЖНО совпадать с SMB-сервером, на который отправлен запрос на подключение. Если имя субъекта-службы не указано клиентом или оно не совпадает, сеанс отклоняется.	
Recovery console: Allow automatic administrative logon (Консоль восстановления: разрешить автоматический	Этот параметр безопасности определяет, нужно ли указывать пароль учетной записи "Администратор" для получения доступа к системе. Если этот параметр включен, консоль восстановления не требует ввода пароля, позволяя выполнять вход в систему автоматически.	Disabled (Отключен)

Политика	Описание	Значение
вход администратора)		
Recovery console: Allow floppy copy and access to all drives and all folders (Консоль восстановления: разрешить копирование дискет и доступ ко всем дискам и папкам.)	При включении этого параметра безопасности становится доступной команда SET консоли восстановления, которая позволяет задать следующие переменные среды консоли восстановления. AllowWildCards: позволяет использовать подстановочные знаки для некоторых команд (например, для команды DEL). AllowAllPaths: разрешает доступ к любым файлам и папкам компьютера. AllowRemovableMedia: позволяет копировать файлы на съемные носители, например на дискеты. NoCopyPrompt: отменяет выдачу предупреждения при перезаписи существующих файлов.	Disabled (Отключен)

Журнал событий

Путь: **Конфигурация компьютера → Политики → Конфигурация Windows → Параметры безопасности → Журнал событий**

(англ. — *Computer Configuration → Policies → Windows Settings → Security Settings → Event Log*)



▼ Описание политик

Политика	Описание	Значение
Maximum application log size (Максимальный размер журнала приложений)	Этот параметр безопасности определяет максимальный размер журнала событий приложений (не более 4 ГБ). На практике используется более низкое ограничение (примерно, 300 МБ). Примечания Размеры файлов журнала должны быть кратны 64 КБ. Если введено значение не кратное 64 КБ, средство просмотра событий установит размер файла журнала, кратный 64 КБ. Этот параметр отсутствует в объекте локальной политики компьютера. Размер файла и способ перезаписи событий в журнале необходимо указывать в соответствии с бизнес-требованиями и требованиями безопасности, определенными при разработке плана безопасности предприятия. Можно реализовать эти параметры журнала событий на уровне сайта, домена или	100032 КБ

Политика	Описание	Значение
	подразделения, чтобы использовать преимущества параметров групповой политики.	
Maximum security log size (Максимальный размер журнала безопасности)	Этот параметр безопасности определяет максимальный размер журнала событий безопасности (не более 4 ГБ). На практике используется более низкое ограничение (примерно, 300 МБ).	100032 КБ
Maximum system log size (Максимальный размер системного журнала)	Этот параметр безопасности определяет максимальный размер журнала событий системы (не более 4 ГБ). На практике используется более низкое ограничение (примерно, 300 МБ).	100032 КБ
Prevent local guests group from accessing application log (Запретить доступ локальной группы гостей к журналу приложений)	Этот параметр безопасности определяет, запрещен ли гостям доступ к журналу событий приложений. Примечания Этот параметр отсутствует в объекте локальной политики компьютера.	Enabled (Включен)
Prevent local guests group from accessing security log (Запретить доступ локальной группы гостей к журналу безопасности)	Этот параметр безопасности определяет, запрещен ли гостям доступ к журналу событий безопасности. Примечания Этот параметр отсутствует в объекте локальной политики компьютер	Enabled (Включен)
Prevent local guests group from	Этот параметр безопасности определяет, запрещен ли гостям доступ к журналу событий системы.	Enabled (Включен)

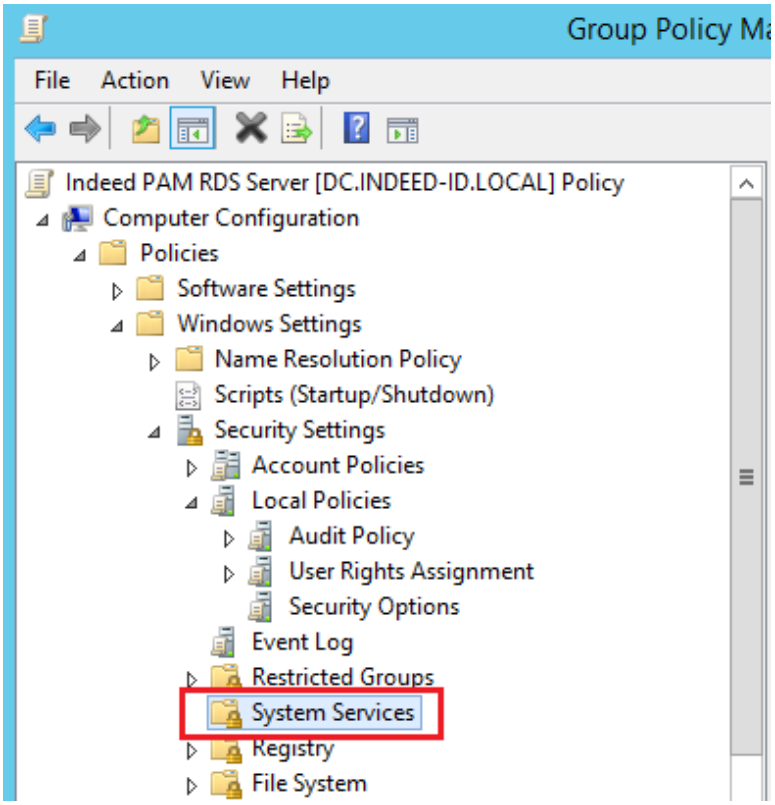
Политика	Описание	Значение
accessing system log (Запретить доступ локальной группы гостей к журналу системы)	Примечания Этот параметр отсутствует в объекте локальной политики компьютера.	
Retention method for application log (Метод сохранения событий в журнале приложений)	Этот параметр безопасности определяет способ перезаписи журнала приложений. Если архивирование журнала приложений не выполняется, установите в диалоговом окне "Свойства" этой политики флажок "Определить этот параметр политики", а затем выберите значение "Переписывать события при необходимости". Если архивирование журнала выполняется через заданные промежутки времени, установите в диалоговом окне "Свойства" этой политики флажок "Определить этот параметр политики", а затем выберите значение "Затирать старые события по дням" и укажите нужное число дней с помощью параметра "Сохранение событий в журнале приложений". Убедитесь в том, что максимальный размер журнала приложений достаточно велик, чтобы он не был достигнут в течение этого промежутка времени. Если необходимо сохранять в журнале все события, установите в диалоговом окне "Свойства" этой политики флажок "Определить этот параметр политики", а затем выберите значение "Не переписывать события (очистить журнал вручную)". При выборе этого варианта журнал необходимо очищать вручную. В этом случае после достижения максимального размера журнала новые события отклоняются. Примечание. Этот параметр отсутствует в объекте локальной политики компьютера.	As needed (Затирать старые события по необходимости)

Политика	Описание	Значение
Retention method for security log (Метод сохранения событий в журнале безопасности)	Этот параметр безопасности определяет способ перезаписи журнала безопасности. Примечания. Этот параметр отсутствует в объекте локальной политики компьютера. Чтобы получить доступ к журналу безопасности, пользователь должен обладать правом "Управление аудитом и журналом безопасности".	As needed (Затирать старые события по необходимости)
Retention method for system log (Метод сохранение событий в системном журнале)	Этот параметр безопасности определяет способ перезаписи журнала системы. Примечание. Этот параметр отсутствует в объекте локальной политики компьютера.	As needed (Затирать старые события по необходимости)

Системные службы

Путь: **Конфигурация компьютера** → **Политики** → **Конфигурация Windows** → **Параметры безопасности** → **Системные службы**

(англ. — *Computer Configuration* → *Policies* → *Windows Settings* → *Security Settings* → *System Services*)



▼ Описание политик

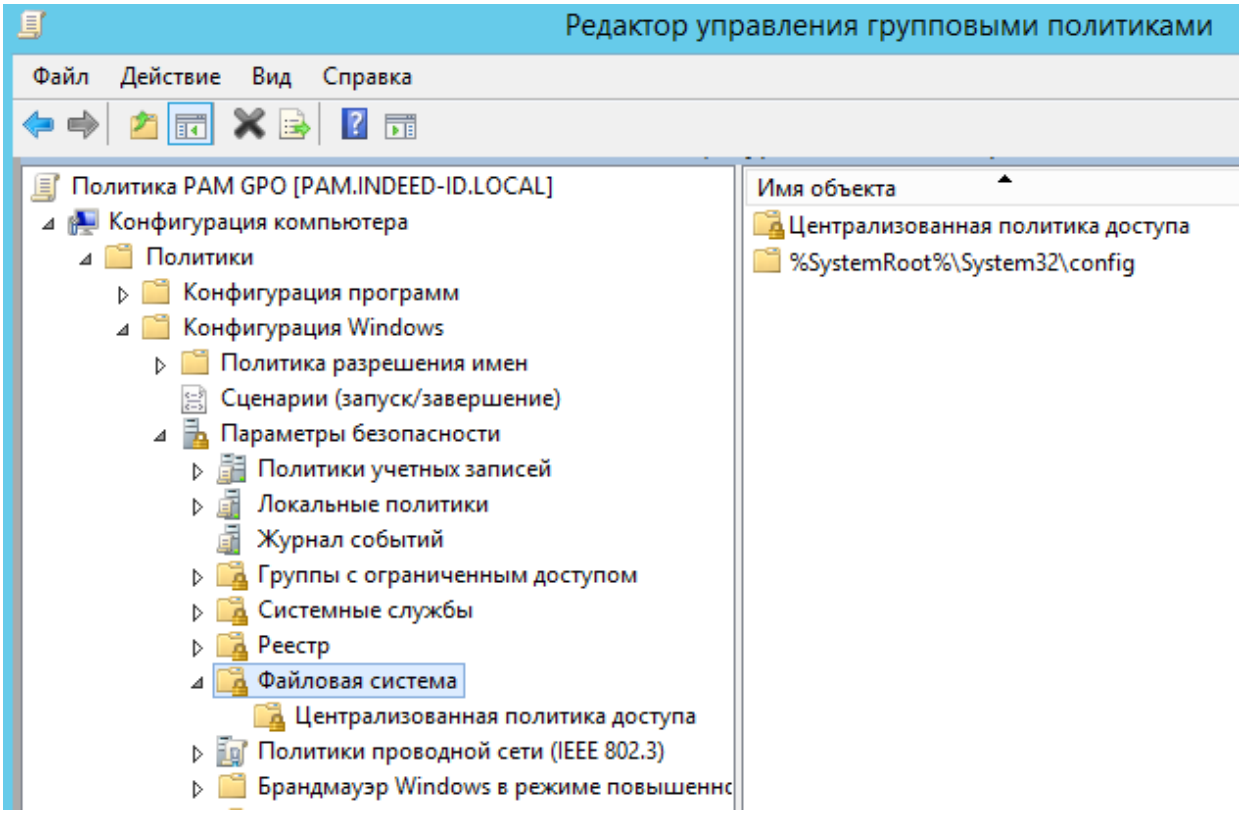
Имя службы (Режим запуска службы)	Разрешения	Аудит
Routing and Remote Access (Startup Mode: Disabled) Маршрутизация и удаленный доступ (Режим запуска: запрещен)	Не определены	Не определен
Special Administration Console Helper (Startup Mode: Disabled) Модуль поддержки специальной консоли администрирования (Режим запуска: запрещен)	Не определены	Не определен
SNMP Trap (Startup Mode: Disabled) Ловушка SNMP (Режим запуска: запрещен)	Не определены	Не определен
Telephony (Startup Mode: Disabled) Телефония (Режим запуска: запрещен)	Не определены	Не определен
Windows Error Reporting Service (Startup Mode: Disabled) Служба регистрации ошибок Windows (Режим запуска:	Не определены	Не определен

Имя службы (Режим запуска службы)	Разрешения	Аудит
запрещен)		
WinHTTP Web Proxy Auto-Discovery Service (Startup Mode: Disabled) Служба автоматического обнаружения веб-прокси WinHTTP (Режим запуска: запрещен)	Не определены	Не определен

Файловая система

Путь: **Конфигурация компьютера → Политики → Конфигурация Windows → Параметры безопасности → Файловая система**

(англ. — *Computer Configuration → Policies → Windows Settings → Security Settings → File System*)



%SystemRoot%\System32\config

▼ Описание настроек

Configure this file or folder then: Propagate inheritable permissions to all subfolders and files (Настроить разрешения для этого файла или папки, а затем: Распространить наследуемые разрешения на все подпапки и файлы)

Permissions (Разрешения)

Type (Тип)	Значение	Access (Доступ)	Applies To (Применяется к)
Allow (Разрешить)	ALL APPLICATION PACKAGES (ВСЕ ПАКЕТЫ ПРИЛОЖЕНИЙ)	Read and Execute (Чтение и выполнение)	This folder, subfolders and files (Для этой папки, вложенных папок и файлов)
Allow (Разрешить)	CREATOR OWNER (СОЗДАТЕЛЬ-ВЛАДЕЛЕЦ)	Full Control (Полный доступ)	Subfolders and files only (Только для вложенных папок и файлов)
Allow (Разрешить)	NT AUTHORITY\SYSTEM (СИСТЕМА)	Full Control (Полный доступ)	This folder, subfolders and files (Для этой папки, вложенных папок и файлов)
Allow (Разрешить)	BUILTIN\Administrators (Builtin\Администраторы)	Full Control (Полный доступ)	This folder, subfolders and files (Для этой папки, вложенных папок и файлов)

Inheritance disabled (Наследование отключено)

Auditing (Аудит)

Type (Тип)	Principal (Субъект)	Access (Доступ)	Applies To (Применяется к)
Fail (Отказ)	Everyone (Все)	Traverse Folder/Execute File, List folder / Read data, Read attributes, Read extended attributes	This folder, subfolders and files

Type (Тип)	Principal (Субъект)	Access (Доступ)	Applies To (Применяется к)
		(Обзор папок/Выполнение файлов, Содержание папки / Чтение данных, Чтение атрибутов, Чтение дополнительных атрибутов)	(Для этой папки, вложенных папок и файлов)
All (Все)	Everyone (Все)	Create files / Write data, Create folders / Append data, Write attributes, Write extended attributes, Delete subfolders and files, Delete, Change permissions, Take ownership (Создание файлов / Запись данных, Создание папок / Дозапись данных, Запись атрибутов, Запись дополнительных атрибутов, Удаление вложенных папок и файлов, Удаление, Смена разрешений, Смена владельца)	This folder, subfolders and files (Для этой папки, вложенных папок и файлов)

Inheritance enabled (Наследование включено)

%SystemRoot%\System32\config\RegBack

▼ Описание настроек

Configure this file or folder then: Propagate inheritable permissions to all subfolders and files (Настроить разрешения для этого файла или папки, а затем: Распространить наследуемые разрешения на все подпапки и файлы)

Permissions (Разрешения)

Type (Тип)	Principal (Субъект)	Access (Доступ)	Applies To (Применяется к)
Allow (Разрешить)	ALL APPLICATION PACKAGES (ВСЕ ПАКЕТЫ ПРИЛОЖЕНИЙ)	Read and Execute (Чтение и выполнение)	This folder, subfolders and files (Для этой

Type (Тип)	Principal (Субъект)	Access (Доступ)	Applies To (Применяется к)
			папки, вложенных папок и файлов)
Allow (Разрешить)	CREATOR OWNER (СОЗДАТЕЛЬ-ВЛАДЕЛЕЦ)	Full Control (Полный доступ)	Subfolders and files only (Только для вложенных папок и файлов)
Allow (Разрешить)	NT AUTHORITY\SYSTEM (СИСТЕМА)	Full Control (Полный доступ)	Subfolders and files only (Только для вложенных папок и файлов)
Allow (Разрешить)	BUILTIN\Administrators (Builtin\Администраторы)	Full Control (Полный доступ)	Subfolders and files only (Только для вложенных папок и файлов)

Inheritance disabled (Наследование отключено)

Auditing (Аудит)

Type (Тип)	Principal (Субъект)	Access (Доступ)	Applies To (Применяется к)
Fail (Отказ)	Everyone (Все)	Traverse Folder/Execute File, List folder / Read data, Read attributes, Read extended attributes (Обзор папок/Выполнение файлов, Содержание папки / Чтение данных, Чтение атрибутов, Чтение дополнительных атрибутов)	This folder, subfolders and files (Для этой папки, вложенных папок и файлов)
All (Все)	Everyone (Все)	Create files / Write data, Create folders / Append data, Write attributes, Write extended attributes, Delete subfolders and files, Delete, Change permissions, Take ownership (Создание файлов / Запись данных, Создание папок / Дозапись данных, Запись атрибутов, Запись	This folder, subfolders and files (Для этой папки, вложенных папок и файлов)

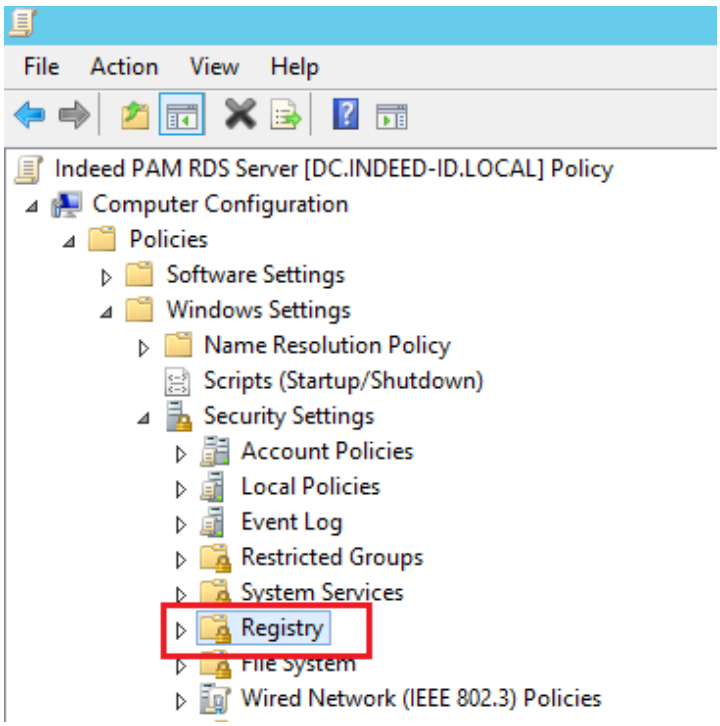
Type (Тип)	Principal (Субъект)	Access (Доступ)	Applies To (Применяется к)
		дополнительных атрибутов, Удаление вложенных папок и файлов, Удаление, Смена разрешений, Смена владельца)	

Inheritance enabled (Наследование включено)

Реестр

Путь: **Конфигурация компьютера → Политики → Конфигурация Windows → Параметры безопасности → Реестр**

(англ. — *Computer Configuration → Policies → Windows Settings → Security Settings → Registry*)



MACHINE\SOFTWARE

▼ Описание настроек

Configure this key then: Propagate inheritable permissions to all subkeys (Настроить этот раздел: Распространить наследуемые разрешения на все подразделы)

Permissions (Разрешения)

Type (Тип)	Principal (Субъект)	Access (Доступ)	Applies To (Применяется к)
Allow (Разрешить)	BUILTIN\Administrators (Builtin\Администраторы)	Full Control (Полный доступ)	This key and subkeys (Этот раздел и его подразделы)
Allow (Разрешить)	CREATOR OWNER (СОЗДАТЕЛЬ-ВЛАДЕЛЕЦ)	Full Control (Полный доступ)	Subkeys only (Только подразделы)
Allow (Разрешить)	NT AUTHORITY\SYSTEM (СИСТЕМА)	Full Control (Полный доступ)	This key and subkeys (Этот раздел и его подразделы)
Allow (Разрешить)	BUILTIN\Users (Builtin\Пользователи)	Read (Чтение)	This key and subkeys (Этот раздел и его подразделы)
Allow (Разрешить)	ALL APPLICATION PACKAGES (ВСЕ ПАКЕТЫ ПРИЛОЖЕНИЙ)	Read (Чтение)	This key and subkeys (Этот раздел и его подразделы)

Inheritance disabled (Наследование отключено)

Auditing (Аудит)

Type (Тип)	Principal (Субъект)	Access (Доступ)	Applies To (Применяется к)
All (Все)	Everyone (Все)	Create Subkey, Create Link, Delete, Read permissions, Change permissions	This key and subkeys (Этот раздел и его

Type (Тип)	Principal (Субъект)	Access (Доступ)	Applies To (Применяется к)
		(Создание подраздела, Создание связи, Удаление, Чтение разрешений, Смена разрешений)	подразделы)
Success (Успех)	Everyone (Все)	Set Value (Задание значения)	This key and subkeys (Этот раздел и его подразделы)

Inheritance enabled (Наследование включено)

MACHINE\SYSTEM

▼ Описание настроек

Configure this key then: Propagate inheritable permissions to all subkeys (Настроить этот раздел: Распространить наследуемые разрешения на все подразделы)

Permissions (Разрешения)

Type (Тип)	Principal (Субъект)	Access (Доступ)	Applies To (Применяется к)
Allow (Разрешить)	BUILTIN\Administrators (Builtin\Администраторы)	Full Control (Полный доступ)	This key and subkeys (Этот раздел и его подразделы)
Allow (Разрешить)	CREATOR OWNER (СОЗДАТЕЛЬ-ВЛАДЕЛЕЦ)	Full Control (Полный доступ)	Subkeys only (Только подразделы)
Allow (Разрешить)	NT AUTHORITY\SYSTEM (СИСТЕМА)	Full Control (Полный доступ)	This key and subkeys (Этот раздел и его подразделы)

Type (Тип)	Principal (Субъект)	Access (Доступ)	Applies To (Применяется к)
Allow (Разрешить)	BUILTIN\Users (Builtin\Пользователи)	Read (Чтение)	This key and subkeys (Этот раздел и его подразделы)
Allow (Разрешить)	ALL APPLICATION PACKAGES (ВСЕ ПАКЕТЫ ПРИЛОЖЕНИЙ)	Read (Чтение)	This key and subkeys (Этот раздел и его подразделы)

Inheritance disabled (Наследование отключено)

Auditing (Аудит)

Type (Тип)	Principal (Субъект)	Access (Доступ)	Applies To (Применяется к)
All (Все)	Everyone (Все)	Create Subkey, Create Link, Delete, Read permissions, Change permissions (Создание подраздела, Создание связи, Удаление, Чтение разрешений, Смена разрешений)	This key and subkeys (Этот раздел и его подразделы)
Success (Успех)	Everyone (Все)	Set Value (Задание значения)	This key and subkeys (Этот раздел и его подразделы)

Inheritance enabled (Наследование включено)

MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg

▼ Описание настроек

Configure this key then: Propagate inheritable permissions to all subkeys (Настроить этот раздел: Распространить наследуемые разрешения на все подразделы)

Permissions (Разрешения)

Type (Тип)	Principal (Субъект)	Access (Доступ)	Applies To (Применяется к)
Allow (Разрешить)	BUILTIN\Administrators (Builtin\Администраторы)	Full Control (Полный доступ)	This key and subkeys (Этот раздел и его подразделы)
Allow (Разрешить)	CREATOR OWNER (СОЗДАТЕЛЬ-ВЛАДЕЛЕЦ)	Full Control (Полный доступ)	Subkeys only (Только подразделы)
Allow (Разрешить)	NT AUTHORITY\SYSTEM (СИСТЕМА)	Full Control (Полный доступ)	This key and subkeys (Этот раздел и его подразделы)
Allow (Разрешить)	BUILTIN\Users (Builtin\Пользователи)	Read (Чтение)	This key and subkeys (Этот раздел и его подразделы)
Allow (Разрешить)	ALL APPLICATION PACKAGES (ВСЕ ПАКЕТЫ ПРИЛОЖЕНИЙ)	Read (Чтение)	This key and subkeys (Этот раздел и его подразделы)

Inheritance disabled (Наследование отключено)

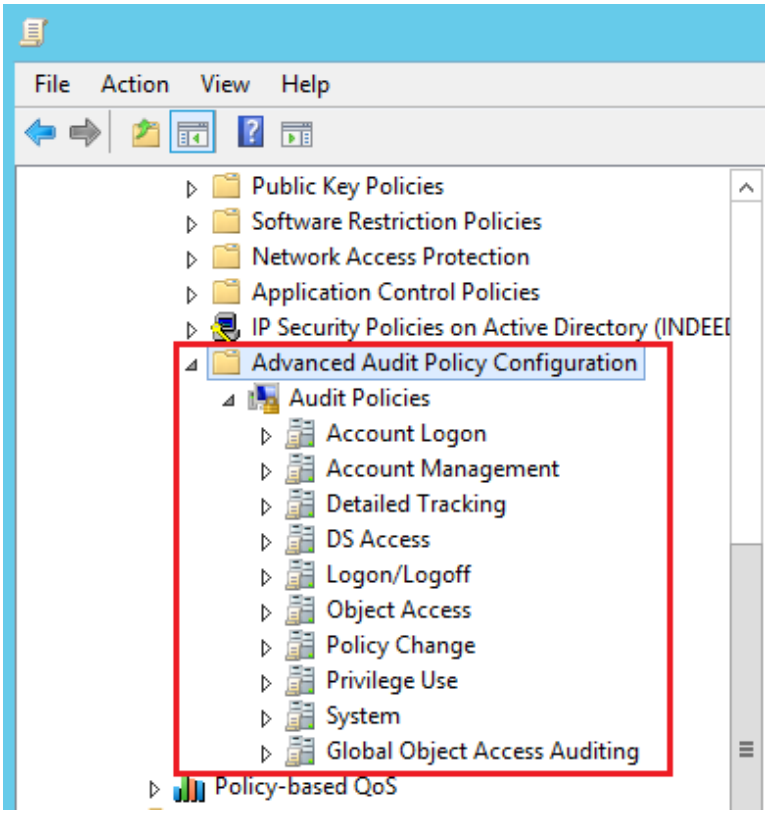
Auditing (Аудит)

No auditing specified (Не задан)

Конфигурация расширенной политики аудита

Путь: **Конфигурация компьютера → Политики → Конфигурация Windows → Параметры безопасности → Конфигурация расширенной политики аудита**

(англ. — *Computer Configuration → Policies → Windows Settings → Security Settings → Advanced Audit Configuration*)



Вход учетной записи

(англ. — *Account Logon*)

▼ Описание политик

Политика	Описание	Значение
Audit Credential Validation (Аудит проверки учетных данных)	Этот параметр политики позволяет вести аудит событий, возникающих при проверке учетных данных для входа учетной записи пользователя. События этой подкатегории возникают только на компьютерах, заслуживающих доверия для этих учетных данных. Для учетных данных домена соответствующими полномочиями обладает контроллер домена. Для локальных учетных записей соответствующими полномочиями обладает локальный компьютер.	Success, Failure (Успех, Отказ)

Политика	Описание	Значение
Audit Other Account Logon Events (Аудит других событий входа учетных записей)	Другие события входа учетных записей Этот параметр политики позволяет вести аудит событий, возникающих при получении ответов на запросы о входе учетной записи пользователя в систему, не относящиеся к проверке учетных данных и не являющиеся билетами Kerberos.	Success, Failure (Успех, Отказ)

Управление учетными записями

(англ. — *Account Management*)

▼ Описание политик

Политика	Описание	Значение
Audit Application Group Management (Аудит управления группами приложений)	Этот параметр политики позволяет вести аудит событий, возникающих при выполнении следующих изменений групп приложений: Создание, изменение или удаление группы приложений. Добавление или удаление члена в группе приложений.	Success, Failure (Успех, Отказ)
Audit Computer Account Management (Аудит управления учетными записями компьютеров)	Этот параметр политики позволяет вести аудит событий, возникающих при изменении учетных записей компьютеров, например, при их создании, изменении или удалении.	Success, Failure (Успех, Отказ)
Audit Distribution Group Management (Аудит управления группами распространения)	Этот параметр политики позволяет вести аудит событий, возникающих при выполнении следующих изменений групп распространения: Создание, изменение или удаление группы распространения. Добавление участника в группу распространения или удаление из нее. Изменение типа группы распространения.	Success, Failure (Успех, Отказ)

Политика	Описание	Значение
	Примечание. События этой подкатегории регистрируются только на контроллерах домена.	
Audit Other Account Management Events (Аудит других событий управления учетными записями)	Этот параметр политики позволяет вести аудит событий, возникающих при выполнении других изменений учетных записей пользователя, не указанных в этой категории: Обращение к хэшу пароля для учетной записи пользователя. Эта операция обычно выполняется при миграции паролей с использованием средства управления Active Directory. Вызов API проверки политики паролей. Вызов этой функции может выполняться при атаках в тех случаях, когда вредоносное приложение проверяет политику, чтобы уменьшить число попыток во время словарной атаки. Изменения групповой политики домена по умолчанию по следующим путям групповой политики: Конфигурация компьютера\Параметры Windows\Параметры безопасности\Политики учетных записей\Политики паролей Конфигурация компьютера\Параметры Windows\Параметры безопасности\Параметры учетных записей\Политика блокировки учетных записей Примечание. Событие аудита безопасности регистрируется в случае применения параметра политики. Во время изменения параметров события не регистрируются.	Success, Failure (Успех, Отказ)
Audit Security Group Management (Аудит управления группами безопасности)	Этот параметр политики позволяет вести аудит событий, возникающих при выполнении следующих изменений групп безопасности: Создание, изменение или удаление группы безопасности. Добавление участника в группу безопасности или удаление из нее. Изменение типа группы.	Success, Failure (Успех, Отказ)
Audit User Account Management (Аудит управления	Этот параметр политики позволяет вести аудит изменений, вносимых в учетные записи пользователей. Отслеживаются следующие события: Создание,	Success, Failure

Политика	Описание	Значение
учетными записями пользователей)	изменение, удаление, переименование, отключение, включение, блокировка и снятие блокировки учетных записей. Установка или изменение пароля учетной записи пользователя. Добавление идентификатора безопасности (SID) к журналу SID учетной записи пользователя. Установка пароля для режима восстановления служб каталогов. Изменение разрешений для учетных записей администраторов. Архивация или восстановление учетных данных диспетчера учетных данных.	(Успех, Отказ)

Вход / Выход

(англ. — *Logon / Logoff*)

▼ Описание политик

Политика	Описание	Значение
Audit Account Lockout (Аудит блокировки учетных записей)	Этот параметр политики позволяет выполнять аудит событий, созданных при неудачной попытке входа в блокированную учетную запись. Если этот параметр политики настроен, то в случае, когда вход в компьютер с учетной записью невозможен из-за блокировки этой учетной записи, создается событие аудита. Успешные и неудачные события аудита регистрируются в соответствующих записях. События входа в систему важны для понимания действий пользователя и обнаружения возможных атак.	Success, Failure (Успех, Отказ)
Audit Logoff (Аудит выхода из системы)	Этот параметр политики позволяет вести аудит событий, возникающих при закрытии сеанса входа в систему. Эти события возникают на компьютере, к которому осуществлялся доступ. При интерактивном выходе из системы событие аудита безопасности возникает на	Success, Failure (Успех, Отказ)

Политика	Описание	Значение
	компьютере, на который выполнен вход с использованием учетной записи пользователя. Если этот параметр политики настроен, событие аудита возникает при закрытии сеанса входа в систему. Успешные и неудачные попытки закрытия сеансов регистрируются в соответствующих записях. Если этот параметр политики не настроен, при закрытии сеанса входа в систему никакие события аудита не возникают.	
Audit Logon (Аудит входа в систему)	Этот параметр политики позволяет вести аудит событий, возникающих при попытке входа в систему с использованием учетной записи пользователя. События этой подкатегории связаны с созданием сеансов входа в систему и возникают на компьютере, к которому осуществляется доступ. При интерактивном входе в систему событие аудита безопасности возникает на компьютере, на котором выполнен вход с использованием учетной записи. При входе в сеть, например при обращении к общей папке в сети, событие аудита безопасности возникает на компьютере, на котором размещается ресурс. Отслеживаются следующие события: Успешные попытки входа в систему. Неудачные попытки входа в систему. Попытки входа в систему с использованием явно указанных учетных данных. Это событие возникает при попытке входа процесса в учетную запись с явным указанием соответствующих учетных данных. Обычно это событие возникает в конфигурациях пакетного входа в систему, например при выполнении запланированных задач или команд RUNAS. Запрет на вход в систему в результате фильтрации идентификаторов безопасности (SID).	Success, Failure (Успех, Отказ)
Audit Network Policy Server (Аудит сервера политики сети)	Этот параметр политики позволяет вести аудит событий, возникающих при выполнении запросов на доступ пользователей по протоколам RADIUS (IAS) и защиты доступа к сети (NAP). Отслеживаются запросы на предоставление, отказ, отзыв, помещение в карантин, блокировку и разблокировку. Если этот параметр политики	Success, Failure (Успех, Отказ)

Политика	Описание	Значение
	настроен, событие аудита возникает для каждого запроса на доступ пользователей по протоколу IAS или NAP. Успешные и неудачные запросы на доступ пользователей регистрируются в соответствующих записях.	
Audit Other Logon/Logoff Events (Аудит других событий входа и выхода)	Этот параметр политики позволяет вести аудит других событий входа и выхода, которые не регулируются параметром политики "Вход/выход", например: Завершение сеансов служб терминалов. Создание новых сеансов служб терминалов. Блокировка и отмена блокировки рабочей станции. Вызов заставки. Отключение заставки. Обнаружение атаки Kerberos с повторением пакетов, при которой дважды отправляется запрос Kerberos с одинаковыми данными. Это состояние может быть связано с неправильными настройками сети. Предоставление доступа к беспроводной сети учетной записи пользователя или компьютера. Предоставление доступа к проводной сети 802.1x учетной записи пользователя или компьютера.	Success, Failure (Успех, Отказ)
Audit Special Logon (Аудит специального входа)	Этот параметр политики позволяет вести аудит событий, возникающих при выполнении таких операций специального входа, как следующие: Использование специального входа, то есть входа в систему с правами, аналогичными правам администратора, который может использоваться для повышения уровня процесса. Вход в систему участника специальной группы. При использовании специальных групп обеспечивается возникновение событий аудита при входе в сеть участника конкретной группы. В реестре можно настроить список идентификаторов безопасности (SID) группы. Событие регистрируется в том случае, если к токену добавлен один из заданных идентификаторов SID и включена эта подкатегория.	Success, Failure (Успех, Отказ)

Доступ к объектам

(англ. — *Object Access*)

▾ Описание политик

Политика	Описание	Значение
Audit Application Generated (Аудит событий, создаваемых приложениями)	Этот параметр политики обеспечивает аудит приложений, которые вызывают события с использованием программных интерфейсов аудита Windows. Эта подкатегория используется для регистрации событий аудита, которые связаны с работой приложений, использующих программные интерфейсы аудита Windows. Отслеживаются следующие события этой подкатегории: Создание контекста клиента приложения. Удаление контекста клиента приложения. Инициализация контекста клиента приложения. Другие операции приложений с использованием программных интерфейсов аудита Windows.	Success, Failure (Успех, Отказ)
Audit Certification Services (Аудит служб сертификации)	Этот параметр политики обеспечивает аудит операций служб сертификации Active Directory (AD CS). К операциям AD CS относятся следующие: Запуск, завершение работы, резервное копирование и восстановление служб AD CS. Изменение списка отзыва сертификатов (CRL). Запросы новых сертификатов. Выдача сертификата. Отзыв сертификата. Изменение параметров диспетчера сертификатов для служб AD CS. Изменение конфигурации служб AD CS. Изменение шаблона служб сертификации. Импорт сертификата. Публикация сертификата центра сертификации в доменных службах Active Directory. Изменение разрешений безопасности для служб AD CS. Архивация ключа. Импорт ключа. Извлечение ключа. Запуск службы ответов OCSP. Остановка службы ответов OCSP.	Success, Failure (Успех, Отказ)

Политика	Описание	Значение
Audit Detailed File Share (Аудит сведений об общем файловом ресурсе)	Этот параметр политики позволяет вести аудит попыток доступа к файлам и папкам в общих папках. Параметр позволяет протоколировать события при любой попытке обращения к файлу или папке, в то время как параметр "Общие папки" записывает только одно событие для любого подключения, установленного между клиентом и общей папкой. В события аудита этого параметра включаются подробные сведения о разрешениях или других критериях предоставления или запрета доступа. Если этот параметр настроен, при попытке обращения к файлу или папке в общей папке возникает событие аудита. Администратор может включить выполнение аудита для успешного выполнения, отказа или того и другого. Примечание: Для общих папок не предусмотрены системные списки управления доступом (SACL). Если этот параметр политики включен, выполняется аудит доступа ко всем общим файлам и папкам системы.	Failure (Отказ)
Audit File Share (Аудит общего файлового ресурса)	Этот параметр политики позволяет вести аудит попыток доступа к общим папкам. Если этот параметр настроен, при попытке доступа к общей папке возникает событие аудита. Если этот параметр задан, администратор может указывать выполнение аудита только успешных выполнений, отказов или того и другого. Примечание. Для общих папок не предусмотрены системные списки управления доступом (SACL). Если этот параметр политики включен, осуществляется аудит доступа ко всем общим папкам в системе.	Success, Failure (Успех, Отказ)
Audit File System (Аудит файловой системы)	Этот параметр политики обеспечивает аудит попыток доступа к объектам файловой системы со стороны пользователей. События аудита безопасности возникают только для тех объектов, для которых заданы системные списки управления доступом (SACL), и только в том случае, если запрашивается тип доступа на запись, чтение или изменение и запрашивающая учетная запись	Success, Failure (Успех, Отказ)

Политика	Описание	Значение
	соответствует параметрам, установленным в списке SACL. Примечание. Чтобы задать список SACL для объекта файловой системы, воспользуйтесь вкладкой "Безопасность" диалогового окна "Свойства" объекта.	
Audit Kernel Object (Аудит объектов ядра)	Этот параметр политики обеспечивает аудит попыток доступа к ядру с использованием мьютексов и семафоров. События аудита безопасности возникают только для объектов ядра с соответствующим системным списком управления доступом (SACL). Примечание. Аудит: установленные по умолчанию списки SACL для объектов ядра управляются параметром аудита доступа глобальных системных объектов.	Success, Failure (Успех, Отказ)
Audit Registry (Аудит реестра)	Этот параметр политики обеспечивает аудит попыток доступа к объектам реестра. События аудита безопасности возникают только для тех объектов, для которых заданы системные списки управления доступом (SACL), и только в том случае, если запрашивается тип доступа на чтение, запись или изменение и запрашивающая учетная запись соответствует параметрам, установленным в списке SACL. Примечание. Чтобы задать список SACL для объекта реестра, воспользуйтесь диалоговым окном "Разрешения".	Success, Failure (Успех, Отказ)
Audit Removable Storage (Аудит съемного носителя)	Этот параметр политики позволяет проводить аудит попыток доступа пользователей к объектам файловой системы на съемном запоминающем устройстве. Событие аудита системы безопасности генерируется только для всех объектов и всех запрошенных типов доступа.	Success (Успех)
Audit SAM (Аудит диспетчера учетных записей безопасности)	Этот параметр политики обеспечивает аудит событий, возникающих при попытке доступа к объектам диспетчера учетных записей безопасности (SAM). К объектам SAM относятся следующие: SAM_ALIAS - локальная группа. SAM_GROUP - группа, не являющаяся локальной.	Success, Failure (Успех, Отказ)

Политика	Описание	Значение
	SAM_USER – учетная запись пользователя. SAM_DOMAIN – домен. SAM_SERVER – учетная запись компьютера. Примечание. Изменять можно только системный список управления доступом (SACL) для объекта SAM_SERVER.	

Изменение политики

(англ. — *Policy Change*)

▼ Описание политик

Политика	Описание	Значение
Audit Audit Policy Change (Аудит изменения политики аудита)	Этот параметр политики позволяет вести аудит изменений параметров политики аудита безопасности, таких как следующие: Установка разрешений и параметров аудита для объекта политики аудита. Изменения в политике аудита системы. Регистрация источников событий безопасности. Отмена регистрации источников событий безопасности. Изменения параметров аудита для отдельных пользователей. Изменения значения параметра CrashOnAuditFail. Изменения системного списка управления доступом для объекта файловой системы или реестра. Изменения списка специальных групп. Примечание. Аудит изменений в системном списке управления доступом (SACL) выполняется при изменении списка SACL для объекта, если при этом включена категория изменений политики. Аудит изменений в списке управления доступом на уровне пользователей (DACL) и изменений владения осуществляется в том случае, если включен аудит доступа к объектам и для списка SACL объекта настроен аудит изменений списка DACL или владения.	Success, Failure (Успех, Отказ)

Политика	Описание	Значение
Audit Authentication Policy Change (Аудит изменения политики проверки подлинности)	Этот параметр политики позволяет вести аудит событий, возникающих при выполнении изменений групп безопасности, таких как следующие: Создание отношений доверия для леса или домена. Изменение отношений доверия для леса или домена. Удаление отношений доверия для леса или домена. Изменения политики Kerberos по следующему пути: Конфигурация компьютера\Параметры Windows\Параметры безопасности\Политики учетных записей\Политика Kerberos. Предоставление пользователю или группе следующих прав: Доступ к компьютеру из сети. Локальный вход. Вход с использованием служб терминалов. Вход с использованием пакетного задания. Вход в службу. Конфликт пространств имен (например, если имя нового отношения доверия совпадает с именем существующего пространства имен). Примечание. Событие аудита безопасности регистрируется в случае применения параметра политики. Во время изменения параметров события не регистрируются.	Success, Failure (Успех, Отказ)
Audit Authorization Policy Change (Аудит изменения политики авторизации)	Этот параметр политики позволяет вести аудит событий, возникающих при выполнении изменений политики авторизации, таких как следующие: Назначение прав (привилегий) пользователей, например, SeCreateTokenPrivilege, которые не проходят аудит в подкатегории "Изменение политики проверки подлинности". Удаление прав (привилегий) пользователей, например, SeCreateTokenPrivilege, которые не проходят аудит в подкатегории "Изменение политики проверки подлинности". Изменения политики шифрованной файловой системы (EFS). Изменения атрибутов ресурса объекта. Изменения централизованной политики доступа (CAP), примененной к объекту.	Success, Failure (Успех, Отказ)
Audit Filtering Platform Policy Change (Аудит	Этот параметр политики позволяет вести аудит событий, возникающих при выполнении изменений платформы фильтрации Windows (WFP), таких как следующие:	Success, Failure

Политика	Описание	Значение
изменения политики платформы фильтрации)	Состояние служб IPsec. Изменения параметров политики IPsec. Изменения параметров политики брандмауэра Windows. Изменения поставщиков и модуля WFP.	(Успех, Отказ)
Audit MPSSVC Rule-Level Policy Change (Аудит изменения политики на уровне правил MPSSVC)	Этот параметр политики позволяет вести аудит событий, возникающих при изменении правил политики, используемых службой защиты Майкрософт (MPSSVC). Эта служба используется брандмауэром Windows. Отслеживаются следующие события: Сообщения от активных политик при запуске службы брандмауэра Windows. Изменения правил брандмауэра Windows. Изменения в списке исключений брандмауэра Windows. Изменения параметров брандмауэра Windows. Пропуск или неприменение правил службой брандмауэра Windows. Изменения параметров групповой политики брандмауэра Windows.	Success, Failure (Успех, Отказ)

Использование привилегий

(англ. — *Privilege Use*)

▼ Описание политик

Политика	Описание	Значение
Audit Non Sensitive Privilege Use (Аудит использования привилегий, не затрагивающих конфиденциальные данные)	Этот параметр политики обеспечивает аудит событий, возникающих при использовании привилегий, не затрагивающих конфиденциальные данные (права пользователя). Использование следующих привилегий не затрагивает конфиденциальные данные: Доступ к диспетчеру учетных данных от имени доверенного вызывающего. Доступ к компьютеру из сети. Добавление рабочих станций к домену. Настройка квот	Success, Failure (Успех, Отказ)

Политика	Описание	Значение
	памяти для процесса. Локальный вход в систему. Вход в систему через службу терминалов. Обход перекрестной проверки. Изменение системного времени. Создание файла подкачки. Создание глобальных объектов. Создание постоянных общих объектов. Создание символических ссылок. Запрет на доступ к компьютеру из сети. Отказ во входе в качестве пакетного задания. Отказ во входе в качестве службы. Запрет на локальный вход. Запрет на вход в систему через службу терминалов. Принудительное удаленное завершение работы. Увеличение рабочего набора процесса. Увеличение приоритета выполнения. Блокировка страниц в памяти. Вход в качестве пакетного задания. Вход в качестве службы. Изменение метки объекта. Выполнение задач по обслуживанию томов. Профилирование одного процесса. Профилирование производительности системы. Отключение компьютера от стыковочного узла. Завершение работы системы. Синхронизация данных службы каталогов.	
Audit Sensitive Privilege Use (Аудит использования привилегий, затрагивающих конфиденциальные данные)	Этот параметр политики обеспечивает аудит событий, возникающих при использовании прав, затрагивающем конфиденциальные данные (пользовательских прав), следующим образом: Вызов привилегированной службы. Вызов одной из следующих привилегий: Действие от имени компонента операционной системы. Архивация файлов и каталогов. Создание объекта-токена. Отладка программ. Включение учетных записей компьютеров и пользователей, которым разрешено делегирование. Создание аудита безопасности. Олицетворение клиента после проверки подлинности. Загрузка и выгрузка драйверов устройств. Управление журналом аудита и безопасности. Изменение значения параметров аппаратной среды. Замена	Failure (Отказ)

Политика	Описание	Значение
	токена на уровне процесса. Восстановление файлов и каталогов. Смена владельца файла или другого объекта.	

Система

(англ. — *System*)

▾ Описание политик

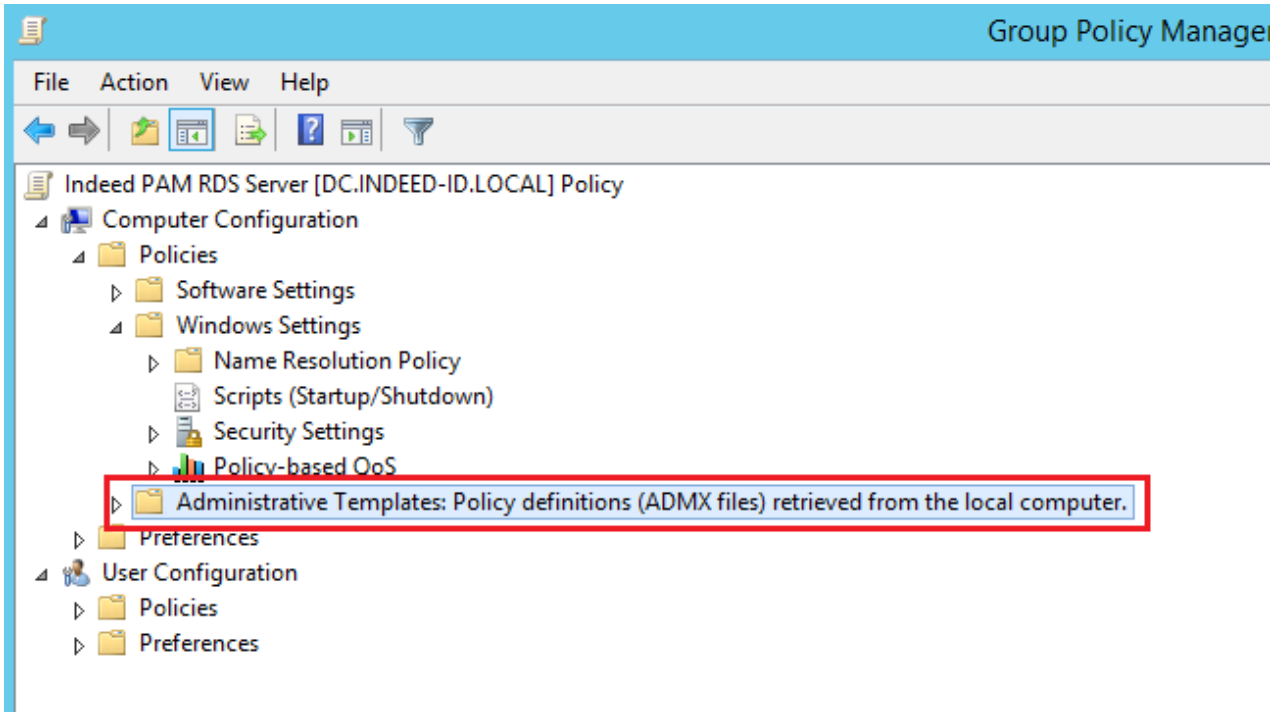
Политика	Описание	Значение
Audit Other System Events (Аудит других системных событий)	Этот параметр политики позволяет вести аудит следующих событий: Запуск и завершение работы службы и драйвера брандмауэра Windows. Обработка политики безопасности службой брандмауэра Windows. Операции с файлами ключей шифрования и операции миграции.	Success, Failure (Успех, Отказ)
Audit Security State Change (Аудит изменения состояния безопасности)	Этот параметр политики позволяет вести аудит событий, возникающих при выполнении изменений состояния безопасности компьютера, таких как следующие: Запуск и завершение работы компьютера. Изменение системного времени. Восстановление системы при событии CrashOnAuditFail, которое регистрируется после перезапуска системы в том случае, если журнал событий заполнен и настроена запись реестра CrashOnAuditFail.	Success, Failure (Успех, Отказ)
Audit Security System Extension (Аудит расширения системы безопасности)	Этот параметр политики позволяет вести аудит событий, связанных с расширением системы безопасности, таких как следующие: Загрузка расширения системы безопасности, например, пакета проверки подлинности, уведомления или безопасности, и его регистрация в системе администратора локальной безопасности (LSA). Оно используется для проверки подлинности при попытке	Success, Failure (Успех, Отказ)

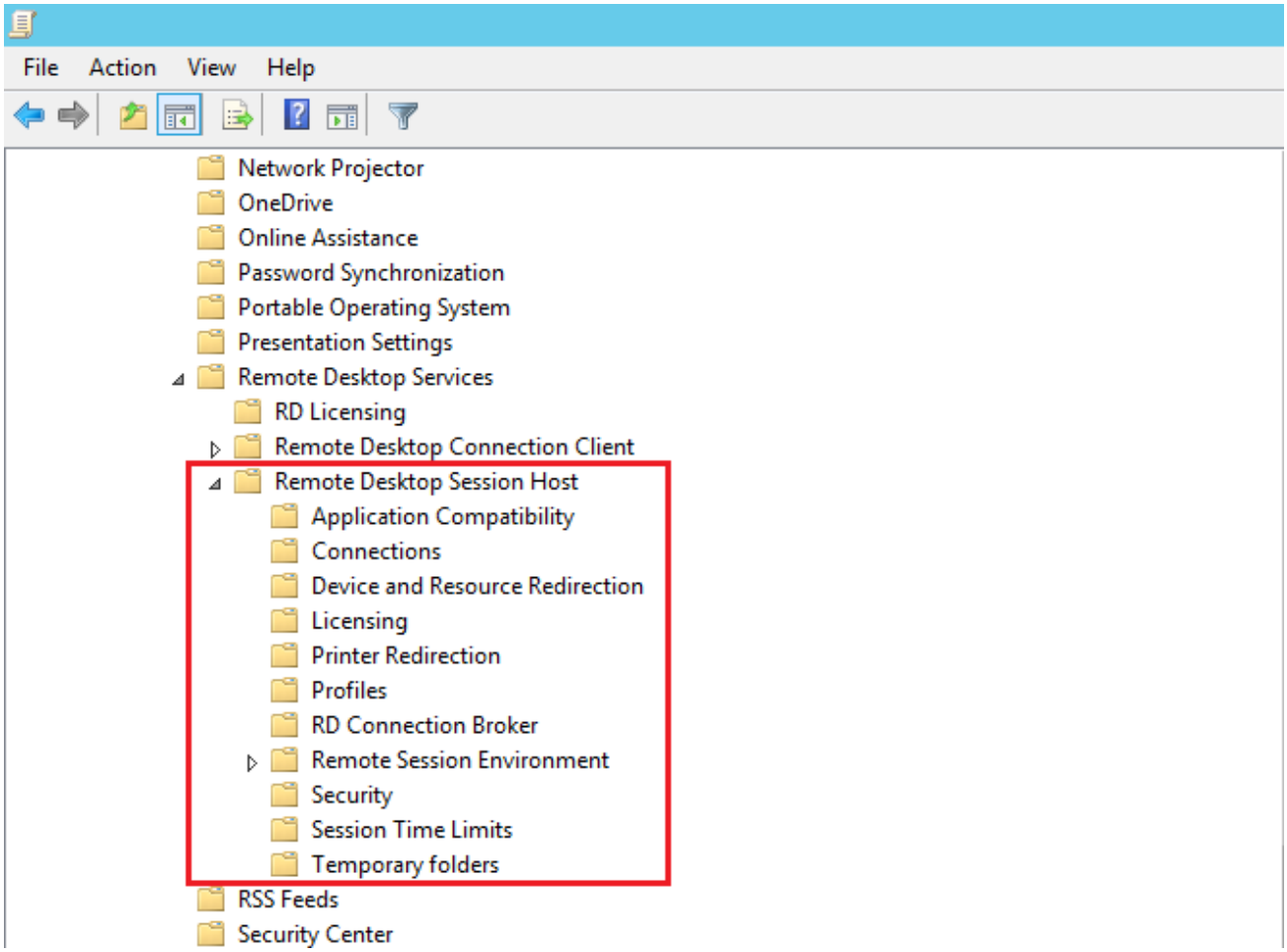
Политика	Описание	Значение
	входа, отправки запросов на вход в систему, а также при любых изменениях учетных записей или паролей. Примерами расширений системы безопасности являются Kerberos и NTLM. Установка и регистрация службы в диспетчере управления службами. В журнале аудита регистрируются сведения об имени, двоичных файлах, типе, типе запуска и учетной записи службы.	
Audit System Integrity (Аудит целостности системы)	Этот параметр политики позволяет вести аудит событий, связанных с нарушениями целостности подсистемы безопасности, такими как следующие: События, которые не удается записать в журнал событий из-за ошибок системы аудита. Процессы, использующие недопустимый порт локального вызова процедур (LPC) для олицетворения клиента посредством ответа, чтения или записи в адресном пространстве клиента. Обнаружение удаленного вызова процедур (RPC), нарушающего целостность системы. Обнаружение недопустимого значения хэша исполняемого файла средством проверки целостности кода. Операции шифрования, нарушающие целостность системы.	Success, Failure (Успех, Отказ)

Административные шаблоны

Путь: **Конфигурация компьютера** → **Политики** → **Административные шаблоны**

(англ. — *Computer Configuration* → *Policies* → *Administrative Templates*)





Подключения

Раздел **Компоненты Windows → Службы удаленных рабочих столов → Узел сеансов удаленных рабочих столов → Подключения**

(англ. — *Windows Components → Remote Desktop Services → Remote Desktop Session Host → Connections*)

▼ Описание политик

Политика	Описание	Значение
Automatic reconnection (Автоматическое переподключение)	Определяет, разрешено ли клиентам подключений к удаленному рабочему столу автоматически восстанавливать подключение к сеансам на сервере узла сеансов удаленных рабочих столов при временной недоступности сетевого подключения. По умолчанию разрешается выполнить не более 20 попыток повторного подключения с интервалом в 5 секунд. Если установлено состояние «Включен», все клиенты, на которых выполняется подключение к удаленному рабочему столу, при недоступности сетевого подключения предпринимают попытки автоматического переподключения. Если установлено состояние «Отключен», автоматические переподключения клиентов запрещены. Если установлено состояние «Не задано», автоматическое переподключение на уровне групповой политики не определено. Тем не менее пользователи могут настроить автоматическое переподключение, установив флажок «Восстановить подключение при разрыве» на вкладке «Взаимодействие» в диалоговом окне «Подключение к удаленному рабочему столу».	Disabled (Отключено)

Политика	Описание	Значение
Configure keep-alive connection interval (Настроить интервал проверяемых на активность подключений)	Этот параметр политики позволяет ввести интервал проверки активности для подтверждения того, что состояние сеанса на сервере узла сеансов удаленных рабочих столов соответствует состоянию клиента. После того как клиент сервера узла сеансов удаленных рабочих столов теряет подключение к серверу узла сеансов удаленных рабочих столов, сеанс на этом сервере может оставаться активным, а не переходить в отключенное состояние, даже если клиент физически отключен от сервера узла сеансов удаленных рабочих столов. Если клиент вновь выполняет вход на тот же сервер узла сеансов удаленных рабочих столов, то может быть установлен новый сеанс (если сервер узла сеансов удаленных рабочих столов настроен так, что допускаются множественные сеансы) и первоначальный сеанс может все еще оставаться активным. Если этот параметр политики включен, то должен быть введен интервал проверки активности. Интервал проверки активности определяет, как часто (в минутах) сервер проверяет состояние сеанса. Диапазон допустимых значений — от 1 до 999 999. Если этот параметр политики отключен или не задан, то интервал проверки активности не установлен и сервер не проверяет состояние сеанса.	Enabled Keep-Alive interval: 1 (Включено Интервал проверки активности: 1)
Set rules for remote control of Remote Desktop Services user sessions (Устанавливает правила удаленного	Если вы включаете этот параметр политики, администраторы могут взаимодействовать с сеансом служб удаленных рабочих столов пользователя в соответствии с выбранным вариантом. Выберите желаемый уровень контроля и разрешений из списка вариантов:	Enabled Options: Full Control without user's permission (Включено Параметры:

Политика	Описание	Значение
управления для пользовательских сеансов служб удаленных рабочих столов)	Удаленное управление не разрешено: запрещает администратору использовать удаленное управление или просматривать сеансы удаленных пользователей. Полный контроль с разрешения пользователя: разрешает администратору взаимодействовать с сеансом при условии согласия пользователя. Полный контроль без разрешения пользователя: разрешает администратору взаимодействовать с сеансом даже без согласия пользователя. Наблюдение за сеансом с разрешения пользователя: позволяет администратору просматривать сеанс удаленного пользователя с согласия пользователя. Наблюдение за сеансом без разрешения пользователя: позволяет администратору просматривать сеанс удаленного пользователя без согласия пользователя. Если вы отключаете этот параметр политики, администраторы могут взаимодействовать с сеансом служб удаленных рабочих столов пользователя, если пользователь даст на это согласие.	Полный контроль без разрешения пользователя)

Перенаправление устройств и ресурсов

Путь: **Компоненты Windows → Службы удаленных рабочих столов → Узел сеансов удаленных рабочих столов → Перенаправление устройств и ресурсов**

(англ. — *Windows Components → Remote Desktop Services → Remote Desktop Session Host → Device and Resource Redirection*)

▼ Описание политик

Политика	Описание	Значение
Do not allow COM port redirection (Не разрешать перенаправление COM-портов)	Определяет, следует ли отключать перенаправление данных с удаленного компьютера на клиентские COM-порты в сеансах служб удаленных рабочих столов. Этот параметр политики можно использовать для того, чтобы запретить пользователям перенаправление данных на периферийные устройства, подключенные к COM-портам, или сопоставление локальных COM-портов при подключении к сеансу служб удаленных рабочих столов. По умолчанию службы удаленных рабочих столов разрешают перенаправление данных на COM-порты. Если вы включаете этот параметр политики, пользователи не могут перенаправлять данные сервера на COM-порты локальных компьютеров. Если вы отключаете этот параметр политики, перенаправление на COM-порты всегда разрешается службами удаленных рабочих столов. Если вы не настраиваете этот параметр политики, перенаправление на COM-порты на уровне групповой политики не определено.	Enabled (Включено)
Do not allow LPT port redirection (Не разрешать перенаправление LPT-портов)	Этот параметр политики определяет, требуется ли отключать перенаправление данных на клиентские LPT-порты в сеансах служб удаленных рабочих столов. Данный параметр политики можно использовать, чтобы запретить пользователям сопоставление локальных LPT-портов и перенаправление данных с удаленного компьютера на локальные периферийные устройства, подключенные к LPT-портам. По умолчанию службы удаленных рабочих столов разрешают перенаправление LPT-портов. Если вы включаете этот параметр политики, пользователи во время сеанса служб удаленных рабочих столов не могут перенаправлять данные сервера на локальные LPT-	Enabled (Включено)

Политика	Описание	Значение
	порты. Если вы отключаете этот параметр политики, перенаправление на LPT-порты всегда разрешено. Если вы не настраиваете этот параметр политики, перенаправление на LPT-порты на уровне групповой политики не определено.	
Do not allow supported Plug and Play device redirection (Не разрешать перенаправление поддерживаемых самонастраиваемых устройств)	Этот параметр политики позволяет управлять перенаправлением поддерживаемых самонастраиваемых устройств, таких как устройства Windows Portable Device, на удаленный компьютер во время сеанса служб удаленных рабочих столов. По умолчанию службы удаленных рабочих столов разрешают перенаправление поддерживаемых самонастраиваемых устройств. Пользователи могут использовать настройку «Дополнительно» на вкладке «Локальные ресурсы» диалогового окна «Подключение к удаленному рабочему столу», чтобы выбрать поддерживаемые самонастраиваемые устройства для перенаправления на удаленный компьютер. Если вы включаете этот параметр политики, пользователи не могут перенаправлять поддерживаемые самонастраиваемые устройства на удаленный компьютер. Если вы отключаете или не настраиваете этот параметр политики, пользователи могут перенаправлять поддерживаемые самонастраиваемые устройства на удаленный компьютер. Примечание. При помощи параметров политики в папке «Конфигурация компьютера\Административные шаблоны\Система\Установка устройств\Ограничения на установку устройств» можно запретить перенаправление определенных типов поддерживаемых самонастраиваемых устройств.	Enabled (Включено)

Среда удаленных сеансов

Путь: **Компоненты Windows → Службы удаленных рабочих столов → Узел сеансов удаленных рабочих столов → Среда удаленных сеансов**

(англ. — *Windows Components → Remote Desktop Services → Remote Desktop Session Host → Remote Session Environment*)

▼ Описание политик

Политика	Описание	Значение
Remove "Disconnect" option from Shut Down dialog (Удалить элемент "Отключение сеанса" из диалога завершения работы)	Этот параметр политики позволяет удалить элемент «Отключение сеанса» из диалогового окна «Завершение работы Windows» в сеансах служб удаленных рабочих столов. С помощью этого параметра политики можно запретить пользователям применять этот знакомый способ отключения клиентского компьютера от сервера узла сеансов удаленных рабочих столов. Если этот параметр политики включен, вариант «Отключение сеанса» не отображается в раскрывающемся списке в диалоговом окне «Завершение работы Windows». Если этот параметр политики отключен или не настроен, элемент «Отключение сеанса» не удаляется из списка в диалоговом окне «Завершение работы Windows». Примечание. Этот параметр политики влияет только на диалоговое окно «Завершение работы Windows». Он не запрещает пользователям применять другие методы для отключения от сеанса служб удаленных рабочих столов. Этот параметр политики также не запрещает отключение сеансов на сервере. Можно задать период времени, в течение которого отключенный сеанс будет оставаться активным на сервере, с помощью настройки параметра политики «Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Службы удаленных рабочих столов\Узел сеансов удаленных рабочих столов\Ограничения сеансов по времени\Задать ограничение по времени для отключенных сеансов».	Enabled (Включено)

Политика	Описание	Значение
Remove Windows Security item from Start menu (Удалить элемент "Безопасность Windows" из меню "Пуск")	Определяет, следует ли удалить элемент «Безопасность Windows» из меню «Параметры» на клиентах служб удаленных рабочих столов. Этот параметр политики можно использовать, чтобы не допустить отключения недостаточно опытных пользователей из служб удаленных рабочих столов по недосмотру. Если установлено состояние «Включено», то пункт «Безопасность Windows» не отображается в меню «Пуск». В результате для того, чтобы открыть диалоговое окно «Безопасность Windows» на клиентском компьютере, пользователь должен использовать специальное сочетание клавиш (CTRL+ALT+END). Если установлено состояние «Отключено» или «Не задано», то пункт «Безопасность Windows» остается в меню «Пуск».	Enabled (Включено)

Безопасность

Путь: **Компоненты Windows → Службы удаленных рабочих столов → Узел сеансов удаленных рабочих столов → Безопасность**

(англ. — *Windows Components → Remote Desktop Services → Remote Desktop Session Host → Security*)

▼ Описание политик

Политика	Описание	Значение
Require secure RPC communication (Требовать безопасное RPC-подключение)	Указывает, требует ли сервер узла сеансов удаленных рабочих столов безопасные RPC-подключения от всех клиентов либо допускает небезопасные подключения. Этот параметр можно использовать для повышения безопасности клиентских RPC-подключений, разрешая только проверенные и зашифрованные запросы. Если состояние имеет значение «Включен», то службы	Enabled (Включено)

Политика	Описание	Значение
	удаленных рабочих столов принимают запросы только от RPC-клиентов, поддерживающих безопасные запросы, и не допускают небезопасные подключения недоверенных клиентов. Если состояние имеет значение «Отключен», то службы удаленных рабочих столов всегда запрашивают безопасную передачу всего RPC-трафика. Однако RPC-клиентам, не отвечающим на запрос, разрешается небезопасное подключение. Если состояние имеет значение «Не задан», допускаются небезопасные подключения. Примечание. Интерфейс RPC используется для администрирования и настройки служб удаленных рабочих столов.	
Set client connection encryption level (Установить уровень шифрования для клиентских подключений)	тот параметр политики определяет, требуется ли особый уровень шифрования для безопасного взаимодействия между клиентскими компьютерами и серверами узла сеансов удаленных рабочих столов во время удаленных подключений по протоколу RDP. Если вы включаете этот параметр политики, все взаимодействия между клиентами и серверами узлов сеансов удаленных рабочих столов во время удаленных подключений должны использовать метод шифрования, заданный в этом параметре. По умолчанию задано значение уровня шифрования «Высокий». Поддерживаются следующие методы шифрования. Высокий. Значение «Высокий» означает, что данные, которыми обмениваются клиент и сервер, шифруются на основе стойкого 128-битного шифрования. Используйте этот уровень в средах, которые содержат только 128-битные клиенты (например, клиенты, использующие службу «Подключение к удаленному рабочему столу»). Клиенты, которые не поддерживают этот уровень шифрования, не могут подключиться к серверам узла сеансов удаленных рабочих столов. Совместимый с клиентским. Значение «Совместимый с клиентским» означает, что данные, которыми обмениваются клиент и сервер, шифруются с	Enabled Encryption Level: High Level (Включено Уровень шифрования: Высокий уровень)

Политика	Описание	Значение
	использованием ключа максимальной стойкости, поддерживаемой клиентом. Используйте этот уровень шифрования в средах с не поддерживающими 128-битное шифрование клиентами. Низкий. При значении «Низкий» с помощью 56-битного шифрования шифруются только данные, пересылаемые от клиента к серверу. Если параметр отключен или не задан, групповая политика не регламентирует уровень шифрования, используемый для удаленных подключений к серверам узла сеансов удаленных рабочих столов. Важно! Соответствие стандарту FIPS можно настроить через «Системные средства шифрования». Используйте FIPS-совместимые алгоритмы для параметров шифрования, хэширования и цифровой подписи в групповой политике (Конфигурация компьютера\Параметры Windows\Параметры безопасности\Локальные политики\Параметры безопасности). Параметр «FIPS-совместимый» обеспечивает шифрование и расшифровку данных, отправляемых от клиента к серверу и обратно, с помощью алгоритмов шифрования FIPS 140-1 (Federal Information Processing Standard), используя модули шифрования корпорации Майкрософт. Используйте этот уровень шифрования при взаимодействии между клиентами и серверами узла сеансов удаленных рабочих столов, которое требует наивысшего уровня шифрования.	

Ограничение сеансов по времени

Путь: **Компоненты Windows → Службы удаленных рабочих столов → Узел сеансов удаленных рабочих столов → Ограничение сеансов по времени**

(англ. — *Windows Components → Remote Desktop Services → Remote Desktop Session Host → Session Time Limits*)

Описание политик

Политика	Описание	Значение
End session when time limits are reached (Завершать сеанс при достижении ограничения по времени)	Этот параметр политики определяет, завершается ли сеанс служб удаленных рабочих столов по тайм-ауту вместо отключения. Вы можете использовать этот параметр для принудительного завершения сеанса служб удаленных рабочих столов (в этом случае осуществляется принудительный выход пользователя, а сведения о сеансе удаляются с сервера) по достижении предела ограничения активного или бездействующего сеанса. По умолчанию службы удаленных рабочих столов отключают сеансы по истечении указанного для них времени сеанса. Ограничения по времени устанавливаются администратором сервера локально или с помощью групповой политики. См. параметры политики «Задать ограничение по времени для активных сеансов служб удаленных рабочих столов» и «Задать ограничение по времени для активных, но бездействующих сеансов служб удаленных рабочих столов». Если вы включаете этот параметр политики, службы удаленных рабочих столов завершают все сеансы с истекшим временем ожидания. Если вы отключаете этот параметр политики, службы удаленных рабочих столов всегда отключают сеансы, прекращенные по тайм-ауту, даже если администратором сервера определено иное поведение для этого параметра политики. Если вы не настраиваете этот параметр политики, службы удаленных рабочих столов отключают сеансы, прекращенные по тайм-ауту, если иное не определено в локальных параметрах. Примечание. Этот параметр политики применяется только к явно определенным администратором ограничениям по времени ожидания. Этот параметр политики не применяется к событиям времени ожидания, которые определяются условиями сетевых	Enabled (Включено)

Политика	Описание	Значение
	подключений. Этот параметр доступен в папках «Конфигурация компьютера» и «Конфигурация пользователя». Если настроены оба параметра, то приоритет имеет параметр в папке «Конфигурация компьютера».	
Set time limit for disconnected sessions (Задать ограничение по времени для отключенных сеансов)	Этот параметр политики позволяет настроить ограничение по времени для отключенных сеансов служб удаленных рабочих столов. С помощью этого параметра политики можно определить максимальный период времени, в течение которого отключенный сеанс остается активным на сервере. По умолчанию службы удаленных рабочих столов разрешают пользователям отключаться от сеанса служб удаленных рабочих столов без завершения этого сеанса и выхода из него. Когда сеанс находится в отключенном состоянии, выполнение запущенных программ продолжается, хотя пользователь не подключен. По умолчанию такие отключенные сеансы остаются открытыми на сервере неограниченное время. Если вы включаете этот параметр политики, отключенные сеансы удаляются с сервера по истечении указанного времени. Чтобы обеспечить поведение по умолчанию, согласно которому отключенные сеансы обслуживаются без ограничения времени, выберите «Никогда». Для консольного сеанса ограничения по времени к отключенным сеансам не применяются. Если вы отключаете или не настраиваете этот параметр политики, на уровне групповой политики он не определен. По умолчанию отключенные сеансы служб удаленных рабочих столов остаются незавершенными без ограничений по времени. Примечание. Этот параметр присутствует в папках «Конфигурация компьютера» и «Конфигурация пользователя». Если параметры политики заданы в обеих папках, то приоритет имеет параметр в папке «Конфигурация компьютера».	Enabled End a disconnected session: 1 minute (Включено Завершение отключенного сеанса: 1 минута)

Временные папки

Путь: **Компоненты Windows → Службы удаленных рабочих столов → Узел сеансов удаленных рабочих столов → Временные папки**

(англ. — *Windows Components → Remote Desktop Services → Remote Desktop Session Host → Temporary folders*)

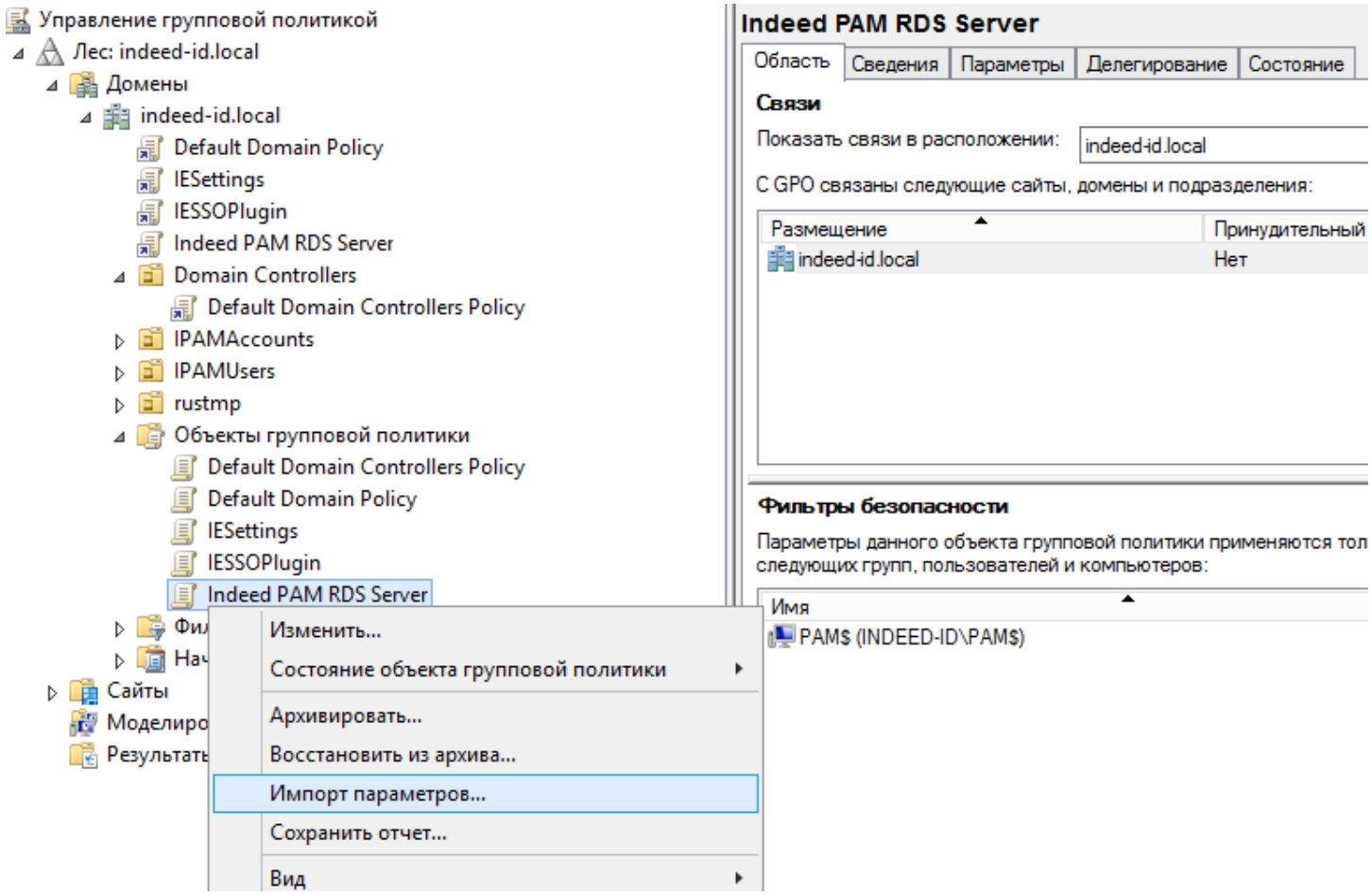
▼ Описание политик

Политика	Описание	Значение
Do not delete temp folders upon exit (Не удалять временные папки при выходе)	Этот параметр политики определяет, сохраняются ли временные папки служб удаленных рабочих столов после завершения сеансов. Этот параметр политики позволяет сохранять временные папки сеансов пользователей на удаленном компьютере даже после завершения сеанса. По умолчанию службы удаленных рабочих столов удаляют временные папки пользователей при выходе пользователя. Если вы включаете этот параметр политики, временные папки сеансов пользователей не удаляются после завершения сеансов. Если вы отключаете этот параметр политики, временные папки удаляются при завершении сеанса, даже если администратор сервера указал иначе. Если вы не настраиваете этот параметр политики, службы удаленных рабочих столов удаляют временные папки с удаленного компьютера при выходе из системы, если администратором сервера не определен другой режим. Примечание. Этот параметр имеет значение, только если на сервере используются временные папки сеансов. Если включен параметр политики «Не использовать временные папки для сеанса», то данный параметр ни на что не влияет.	Disabled (Отключено)

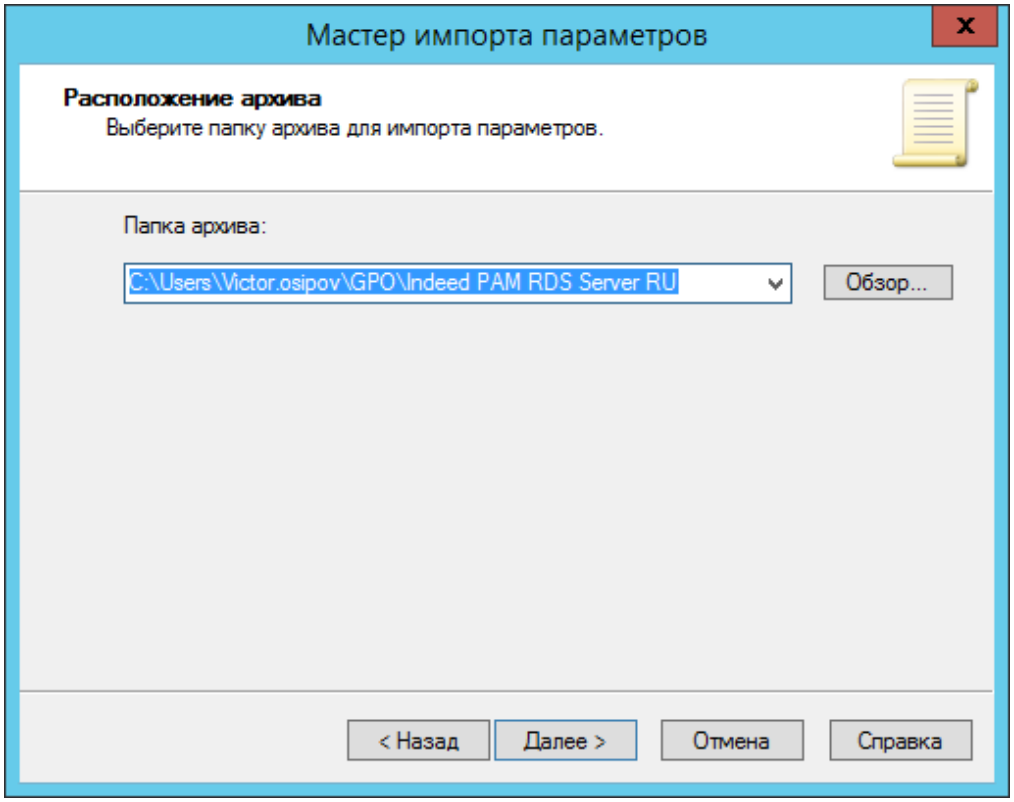
Политика	Описание	Значение
Do not use temporary folders per session (Не использовать временные папки для сеанса)	Данный параметр политики не позволяет службам удаленных рабочих столов создавать временные папки сеансов. С помощью этого параметра политики можно запретить создание на удаленном компьютере отдельных временных папок для каждого сеанса. По умолчанию службы удаленных рабочих столов создают отдельную временную папку для каждого активного сеанса пользователя на удаленном компьютере. Такие временные папки создаются на удаленном компьютере в папке Temp папки профиля пользователя и получают имя по коду сеанса. Если вы включаете этот параметр политики, временные папки сеансов не создаются. Вместо этого временные файлы пользователя для всех сеансов на удаленном компьютере хранятся в общей папке Temp папки профиля пользователя на удаленном компьютере. Если вы отключаете этот параметр политики, отдельные временные папки всегда создаются для каждого сеанса, даже если администратором сервера определен другой режим. Если вы не настраиваете этот параметр политики, отдельные временные папки для каждого сеанса создаются в том случае, если администратором сервера не определен другой режим.	Disabled (Отключено)

Порядок импорта политик

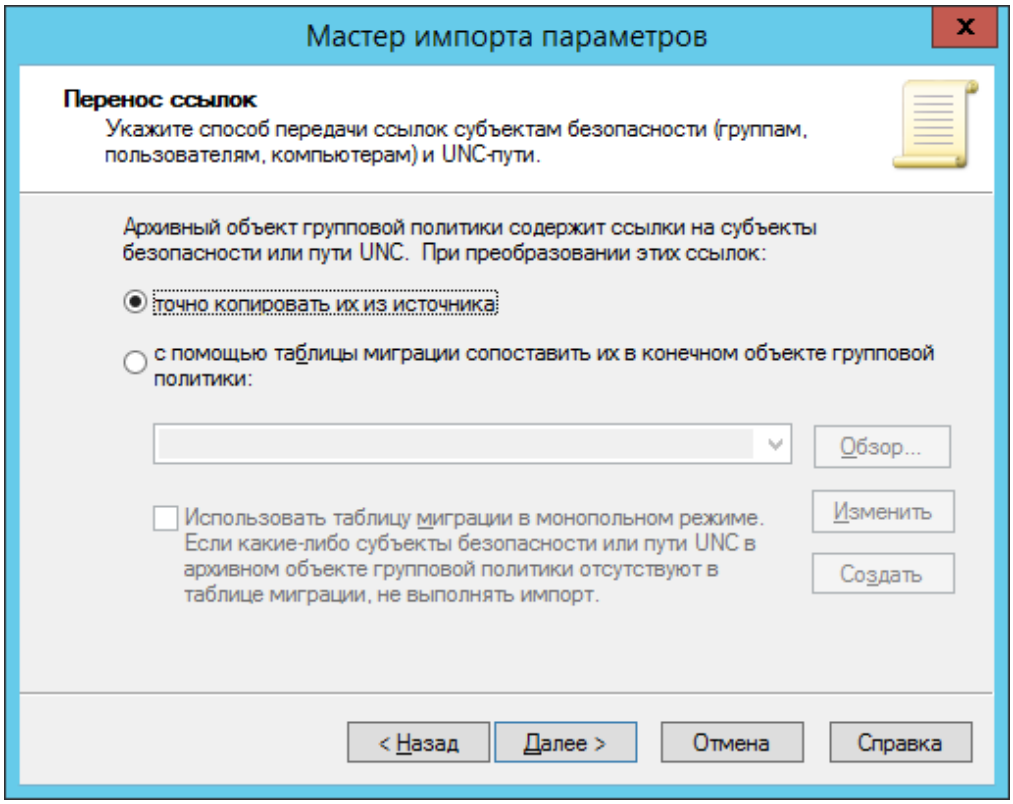
1. На контроллере домена создайте новый объект групповой политики, например "Indeed PAM RDS Server".
2. Настройте фильтры безопасности объекта групповой политики для применения только к объекту сервера Indeed PAM Gateway.
3. Скачайте архив с набором политик для русской или английской версии сервера и распакуйте во временную папку.
4. Нажмите правой кнопкой мыши по созданному объекту групповой политики и выберите в контекстном меню пункт "Импорт параметров...".



5. Укажите путь к папке с распакованным архивом.



6. В окне "Перенос ссылок" выберите флажок "точно копировать их из источника".



7. После успешного импорта откройте объект групповой политики и исправьте политику **Разрешать вход в систему через службы удаленных рабочих столов** (англ. — *Allow log on through Remote Desktop Services*), добавив в нее группу безопасности пользователей, которым необходим удаленный доступ.
8. Выполните привязку объекта групповой политики к организационному подразделению, которому принадлежит сервер Indeed PAM Gateway.
9. Примените политики, выполнив команду `gpupdate /force` на сервере Indeed PAM Gateway.

Настройки безопасности сервера доступа

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Обязательно выполните действия, которые перечислены на этой странице. Это требуется для корректной работы Indeed PAM.

Применение настроек с помощью утилиты

Чтобы применить необходимые настройки безопасности сервера доступа выполните следующие действия:

1. Перейдите в папку с дистрибутивом **IndeedPAM_3.0_RU\indeed-pam-tools\configuration-protector**.

2. Запустите командную строку от имени администратора.

3. Выполните команду:

   ```
   .\Pam.Tools.Configuration.Protector.exe apply-gateway-security
   ```

4. Установите параметр **Запретить доступ к панели управления и параметрам компьютера** групповой политики в значение **Включено**.

   Путь: Конфигурация пользователя → Административные шаблоны → Панель управления → Запретить доступ к панели управления и параметрам компьютера.

   (англ. — *User configuration → Administrative Templates → Control Panel → Prohibit access to Control Panel and PC settings*)

5. Перезагрузите машину с сервером доступа.

6. Убедитесь, что необходимые настройки безопасности сервера доступа применились.

7. Проверьте ваши целевые ресурсы — убедитесь, что параметр **Требовать использование специального уровня безопасности для удаленных подключений по протоколу RDP** групповой политики установлен в одно из значений:

   - **Не задано**
   - **Включено: Negotiate**
   - **Включено: SSL**

   Путь: Конфигурация компьютера → Административные шаблоны → Компоненты Windows → Службы удаленных рабочих столов → Узел сеансов удаленных рабочих столов → Безопасность → Требовать использование специального уровня безопасности для удаленных подключений по протоколу RDP

   (англ. — *Computer Configuration → Administrative Templates → Windows Components → Remote Desktop Services → Remote Desktop Session Hosts → Security → Require Use of Specific Security Layer for Remote (RDP) Connections*)

   > ⚠ **ПРЕДУПРЕЖДЕНИЕ**
   >
   > Значение **Включено: RDP** не поддерживается системой Indeed PAM.

Проверка успешного применения настроек безопасности сервера доступа

Чтобы убедиться, что необходимые настройки безопасности сервера доступа применились, выполните следующие действия:

1. Перейдите в папку с дистрибутивом **IndeedPAM_3.0_RU\indeed-pam-tools\configuration-protector**.
2. Запустите командную строку от имени администратора.
3. Выполните команду:

```
.\Pam.Tools.Configuration.Protector.exe validate-gateway-security
```

Применение настроек вручную

Если использование утилиты Pam.Tools.Configuration.Protector по каким-либо причинам невозможно, то примените необходимые настройки безопасности вручную, как описано ниже.

1. **Копирование файла библиотеки в директорию ProxyApp.**

   Перейдите в директорию `C:\Program Files\dotnet\shared\Microsoft.NETCore.App\3.1.24`, скопируйте файл `Microsoft.DiaSymReader.Native.amd64.dll` в директорию `C:\Program Files\Indeed\Indeed PAM\Gateway\ProxyApp`. Версия в исходном пути может отличаться, в зависимости от версии Dotnet Runtime, установленного на сервере. Используйте наибольшую версию, которая начинается с 3.1.

2. **Отключение пользовательского хранилища доверенных корневых сертификатов ЦС**

   Есть два способа:

   - Через групповую политику
   - Через настройку в реестре на RDS Gateway сервере, если не применена групповая политика

   Способ 1 — через групповую политику

   Измените настройку в групповой политике, действующей на RDS Gateway сервер:

   Путь: Конфигурация компьютера → Конфигурация Windows → Параметры безопасности → Политика открытого ключа → Параметры подтверждения пути сертификата

   (англ. — *Computer Configuration → Windows Settings → Security Settings → Public Key Policies → Certificate Path Validation Settings*)

   Во вкладке Хранилища (англ. — *Stores*):

   i. Включите опцию **Определить параметры политики** (англ. — *Define these policy settings*)

   ii. Отключите опцию **Разрешить использование корневых ЦС, которым доверяет пользователь, для проверки сертификатов** (англ. — *Allow user trusted root CAs to be used to validate certificates*)

   Способ 2 — через настройку в реестре

   В `HKLM\SOFTWARE\Policies\Microsoft\SystemCertificates\Root\ProtectedRoots` создайте ключ `Flags` с типом `DWORD` и установите значение `1`. Пользовательское хранилище доверенных корневых сертификатов ЦС отключено, если первый бит значения в `Flags` равен `1`.

3. **Отключение служб системы push-уведомлений Windows.**

   Отключите следующие службы:

   - **Служба системы push-уведомлений Windows** (англ. — *Windows Push Notifications*, *WpnService*)
   - **Пользовательская служба push-уведомлений Windows** (англ. — *Windows Push Notifications User*, *WpnUserService*)

4. **Отключение Панели Управления для пользователей в групповой политике.**

   Установите параметр **Запретить доступ к панели управления и параметрам компьютера** групповой политики в значение **Включено**.

   Путь: Конфигурация пользователя → Административные шаблоны → Панель управления → Запретить доступ к панели управления и параметрам компьютера.

   (англ. — *User configuration → Administrative Templates → Control Panel → Prohibit access to Control Panel and PC settings*)

5. **Проверка выбранного уровня безопасности для удаленных подключений по протоколу RDP в групповой политике целевых ресурсов.**

   Проверьте ваши целевые ресурсы — убедитесь, что параметр **Требовать использование специального уровня безопасности для удаленных подключений по протоколу RDP** групповой политики установлен в одно из значений:

   - **Не задано**
   - **Включено: Negotiate**
   - **Включено: SSL**

   Путь: Конфигурация компьютера → Административные шаблоны → Компоненты Windows → Службы удаленных рабочих столов → Узел сеансов удаленных рабочих столов → Безопасность → Требовать использование специального уровня безопасности для удаленных подключений по протоколу RDP

   (англ. — *Computer Configuration → Administrative Templates → Windows Components → Remote Desktop Services → Remote Desktop Session Hosts → Security → Require Use of Specific Security Layer for Remote (RDP) Connections*)

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Значение **Включено: RDP** не поддерживается системой Indeed PAM.

Смена ключа шифрования БД PAM

В случае компрометации ключа шифрования предусмотрена возможность ротации мастер ключа БД без остановки работы PAM.

Для этого используется утилита Key Rotator.

Windows	IndeedPAM_3.0_RU\indeed-pam-tools\key-rotator\Pam.Tools.KeyRotator.exe
Linux	/etc/indeed/indeed-pam/tools/key-rotator.sh

Перед запуском утилиты внесите изменения в конфигурационный файл компонента **Core**, в секцию **Encryption**.

По умолчанию в этой секции находится только подсекция **Primary**, в которой указан действующий ключ шифрования и другие действующие настройки БД.

Чтобы изменить ключ шифрования БД, выполните следующие шаги:

1. Создайте вторую подсекцию **Secondary** в секции **Encryption**.
2. Перенесите настройки из **Primary** в **Secondary**.
3. Внесите новый ключ шифрования в секцию **Primary**.
4. Сохраните изменения конфигурационного файла.
5. Запустите утилиту Key Rotator.
6. После завершения работы утилиты удалите из конфигурационного файла секцию **Secondary**.

Сервисные операции

Сервисные операции для ресурсов Windows

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Если компоненты сервера управления установлены на операционную систему Linux, то для выполнения сервисных операций на Windows ресурсе должна быть настроена служба WinRM по HTTPS

Сервисные операции для ресурсов Windows выполняются от имени доменной или локальной учетной записи:

- Проверка соединения с ресурсом
- Синхронизация локальных учетных записей
- Проверка пароля локальных учетных записей
- Изменение пароля локальных учетных записей
- Получение данных о ОС
- Получение списка групп безопасности

Настройка доменной учетной записи в качестве сервисной

1. Выполните вход на ресурс.
2. Запустите оснастку **Управление компьютером** (Computer management).
3. Перейдите в раздел **Служебные программы** (System tools) → **Локальные пользователи** (Local Users and Groups) → **Группы** (Groups).
4. Откройте контекстное меню группы **Администраторы** (Administrators).
5. Выберите пункт **Свойства** (Properties).
6. Нажмите **Добавить** (Add).
7. Выберите доменную учетную запись, которая будет использоваться в роли сервисной для ресурса и нажмите **Ок**.

Настройка локальной учетной записи в качестве сервисной

Если в качестве сервисной учетной записи будет использоваться локальный встроенный (built-in) администратор, то дополнительная настройка не требуется. Если в качестве сервисной учетной записи будет использоваться не встроенная локальная учетная запись администратора, то необходимо:

1. Выполните вход на ресурс.
2. Запустите оснастку **Управление компьютером** (Computer management).
3. Перейдите в раздел **Служебные программы** (System tools) → **Локальные пользователи** (Local Users and Groups) → **Группы** (Groups).
4. Откройте контекстное меню группы **Администраторы** (Administrators).
5. Выберите пункт **Свойства** (Properties).
6. Нажмите **Добавить** (Add).
7. Выберите локальную учетную запись, которая будет использоваться в роли сервисной для ресурса и нажмите **Ок**.
8. Запустите **Редактор реестра** (RegEdit).
9. Раскройте ветку **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System** .
10. Откройте контекстное меню раздела **System**.
11. Выберите пункт **Создать** (Create) → **Параметр DWORD 32** (DWORD (32-bit) Value).
12. Введите название параметра — **LocalAccountTokenFilterPolicy**.
13. Откройте контекстное меню параметра **LocalAccountTokenFilterPolicy**.
14. Выберите пункт **Изменить** (Modify) и установите **Значение:** (Value data:) равное **1**.

Настройка реестра необходима из-за ограничений удаленного управления WinRM для всех локальных учетных записей, кроме встроенного (built-in) администратора.

Настройка Indeed PAM Core для выполнения сервисных операций от имени локальных учетных записей ресурса

Сервисные операции выполняются при помощи WinRM, для использования локальных учетных записей ресурса в качестве сервисных необходимо добавить ресурс в список доверенных **TrustedHosts** на сервере Indeed PAM Core.

Настройка TrustedHosts

1. Выполните вход на сервер Indeed PAM Core.

2. Откройте **Командную строку** (CMD) от имени администратора.
3. Выполните команду:

```
C:\>winrm s winrm/config/client @{TrustedHosts="Resource1.domain.local,
Resource2.domain.local"}
```

Указанные ресурсы будут добавлены в список доверенных.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> При добавлении новых ресурсов в список доверенных необходимо указывать добавленные ранее ресурсы и новые, так как новое значение перезаписывает старое.
>
> ```
> @{TrustedHosts="Resource1.domain.local, Resource2.domain.local,
> Resource3.domain.local"}
> ```

Сервисные операции в Active Directory

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Если компоненты сервера управления установлены на операционную систему Linux, то для выполнения сервисных операций в домене должен быть настроен LDAPS (LDAP over SSL)

Настройка сервисной учетной записи

1. Запустите оснастку **Active Directory** → **пользователи и компьютеры** (Active Directory Users and Computers).
2. Откройте контекстное меню контейнера или подразделения.
3. Выберите пункт **Создать** (Create) → **Пользователь** (User).
4. Укажите имя, например, **IPAMADServiceOps**.
5. Заполните обязательные поля и завершите создание учетной записи.
6. Откройте контекстное меню контейнера, подразделения или корня домена.

7. Выберите пункт **Свойства** (Properties).
8. Перейдите на вкладку **Безопасность** (Security).

> ⓘ **ИНФОРМАЦИЯ**
>
> Если вкладки **Безопасность** нет, то в меню **Вид** (View) включите Advanced features.

9. Нажмите **Добавить** (Add).
10. Выберите учетную запись **IPAMADServiceOps** и нажмите **Ок**.
11. Нажмите **Дополнительно** (Advanced).
12. Выберите учетную запись **IPAMADServiceOps** и нажмите **Изменить** (Edit).
13. Установите для поля **Применяется к:** (Applies to:) значение **Дочерние объекты: Пользователь** (Descendant User objects).
14. В разделе **Разрешения:** (Permissions:) отметьте **Сброс пароля** (Reset password).
15. Сохраните внесенные изменения.

Сервисные операции для ресурсов *nix

Сервисные операции для ресурсов *nix выполняются от имени локальной сервисной учетной записи:

- Проверка соединения с ресурсом
- Поиск учетных локальных записей доступа
- Проверка пароля локальных учетных записей доступа
- Изменение пароля локальных учетных записей доступа
- Получение данных о ОС
- Получение списка групп безопасности

Создание и настройка сервисной учетной записи

1. Выполните вход на ресурс
2. Запустите **Терминал** (Terminal)

3. Создайте пользователя, например, **IPAMService**

```
adduser IPAMService
```

4. Добавьте пользователя в группу **SUDO**

```
usermod -aG sudo IPAMService
```

Настройка группы привилегированных учетных записей

Автоматический поиск и добавление учетных записей доступа в Indeed PAM выполняется на основании их права на выполнение команды SUDO. Для предоставления прав на выполнение команды SUDO необходимо внести изменения в файл **/etc/sudoers**.

Консоль администратора

Получите доступ к консоли администратора

Первый запуск

Лицензируйте продукт, укажите сетевые пути к хранилищам и добавьте все объекты

Настройка политик

Выберите разделы, которые будут управляться политиками

Справочник по разделам

Количество глав: 17

Выгрузка паролей

Ознакомьтесь с информацией о выгрузке паролей при нештатной ситуации

Работа с PostgreSQL Proxy

Ознакомьтесь с информацией о возможностях Indeed PAM PostgreSQL Proxy

Консоль администратора

Администрирование Indeed PAM выполняется при помощи **консоли администратора** — специальной оболочки для Indeed PAM Core. Доступна по следующему URL:

- **Windows:** https://pam.domain.local/mc
- **Linux:** https://pam.domain.local/mc

Аутентификация

Для получения доступа к консоли администратора необходим второй фактор аутентификации, для регистрации первого аутентификатора выполните следующие действия:

- запустите консоль администратора от имени пользователя, чей SID был указан в конфигурации IDP;
- ознакомьтесь с инструкцией по регистрации аутентификатора;
- установите приложение для генерации OTP и отсканируйте QR-код;
- введите полученное значение в поле **Код** на странице регистрации.

После успешной регистрации вы будете перенаправлены в консоль администратора. При повторном подключении к консоли администратора потребуется ввести новый код из приложения для генерации OTP.

> **ПОДСКАЗКА**
>
> После первого входа для включения функций управления необходимо добавить пользователя в состав административной роли.

Первый запуск

После первого входа перейдите в раздел **Роли** и добавьте текущего пользователя в роль Administrator, обновите страницу — в консоли отобразятся все разделы.

Откройте раздел **Пользователи**, нажмите значок поиска, убедитесь что все пользователи из указанного организационного подразделения корректно отобразились.

Перейдите в раздел **Конфигурация** → **Лицензии**. Скопируйте значение из поля **Идентификатор инсталляции** и передайте его в техническую поддержку для выпуска файла лицензии. При получении файла лицензии **PAM_гггг.мм.дд.lic** в этом же разделе нажмите **Добавить** и выберите указанный файл.

Перейдите в раздел **Конфигурация** → **Системные настройки**. В секции **Подключение к Gateway** укажите **Адрес RDCB**, **Имя коллекции RDCB**. В секции **RDP Proxy** укажите **Адрес RDP Proxy**. В секции **PostgreSQL Proxy** укажите **Адрес PostgreSQL Proxy**. В секции **Настройки SSH-подключений** укажите **Адрес SSH Proxy**. Сохраните изменения.

Перейдите в раздел **События** — там должно отобразиться событие изменения параметров конфигурации.

При отсутствии ошибок далее можно переходить к добавлению объектов.

Добавление текущего домена

1. Перейдите в раздел **Домены**, нажмите **Добавить**.
2. Введите имя домена (например, INDEED-ID) и его DNS (например, indeed-id.local), нажмите **Сохранить**.
3. Откройте страницу добавленного домена.
4. Нажмите **Добавить учетную запись** и введите имя сервисной учетной записи (например, **IPAMADServiceOps**).
5. Задайте пароль вручную и нажмите **Сохранить**.
6. Нажмите значок карандаша рядом с надписью **Сервисная учетная запись** и выберите сервисную учетную запись (**IPAMADServiceOps**).
7. Нажмите **Проверить соединение** и проверьте успешность установления соединения.

8. Здесь же, на странице домена, перейдите на вкладку **Контейнеры для ресурсов** и добавьте контейнер Active Directory, в котором находятся нужные доменные ресурсы (например, **Computers**).
9. Здесь же, на странице домена, перейдите на вкладку **Привилегированные группы** и укажите группы безопасности, в которых находятся учетные записи, с помощью которых пользователи будут получать доступ к доменным ресурсам (например, **IPAMPrivilegedAccounts**).
10. Здесь же, на странице домена, нажмите кнопки **Импортировать ресурсы** и **Синхронизировать учетные записи**. После этого все доступные ресурсы и учетные записи добавятся в соответствующие разделы консоли.
11. При необходимости перейдите на вкладку **События** для просмотра подробной информации о доменных событиях.

Добавление и взятие под контроль учетных записей

В разделе **Учетные записи** отметьте галочкой импортированные доменные учетные записи: они начинаются с имени домена, отмечены знаком вопроса и находятся в состоянии **Ожидает решения**. Вверху нажмите кнопку **Сделать управляемой**. После этого у выбранных учетных записей пароль будет сброшен на новый в соответствии с политикой.

Добавление не доменных ресурсов

1. Перейдите в раздел **Ресурсы**, нажмите **Добавить**.
2. Выберите **Подразделение**.
3. Укажите **Имя ресурса**, **DNS имя** и/или **IP-адрес**.
4. На шаге **Пользовательское подключение** выберите тип подключения, при необходимости укажите адрес подключения и порт.
5. На шаге **Сервисное подключение** снимите галочку **Использовать коннектор для сервисного подключения**, т.к. локальных учетных записей еще не добавлялось, завершите добавление ресурса. Новый ресурс отобразится в списке ресурсов.
6. Откройте страницу ресурса, нажмите Добавить учетную запись, задайте пароль вручную.

Ресурс готов к работе: для него можно выдавать разрешения.

Для выполнения сервисных операций (поиск и добавление учетных записей, автоматическая смена паролей, обновление информации о ресурсе) необходима настройка сервисного подключения.

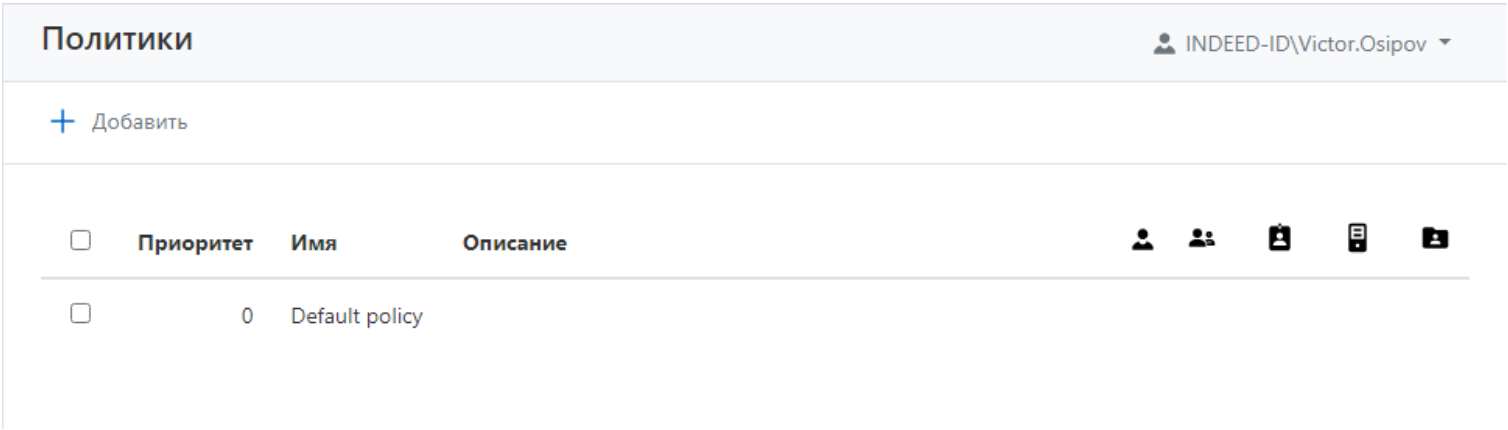
Настройка политик

Управление политиками

Раздел содержит список политик, расположенных по приоритету применения.

Для политик отображаются данные:

- **Приоритет** — число, указывающее порядок применения конкретной политики по отношению к остальным. Нулевой приоритет соответствует политике по умолчанию (Default policy) и применяется в самую последнюю очередь. Чем выше расположена политика, тем выше ее приоритет и наоборот.
- **Имя** — название политики.
- **Описание** — произвольный текст.
- — количество пользователей, на которых действует политика.
- — количество групп пользователей, на которые действует политика.
- — количество учетных записей, на которые действует политика.
- — количество ресурсов, на которые действует политика.
- — количество доменов, на которые действует политика.



Политика по умолчанию содержит набор параметров для всех доступных категорий и применяется ко всем новым объектам, поэтому целесообразно начать настройку с нее.

> **ПРИМЕЧАНИЕ**

> Политика по умолчанию применяется и к сессиям, открытым от имени пользовательских учетных записей, если к данным пользователям явно не применены другие политики.

Откройте страницу политики, задайте нужные параметры для категорий **Учетные записи**, **Сессии**, **RDP,** и сохраните настройки.

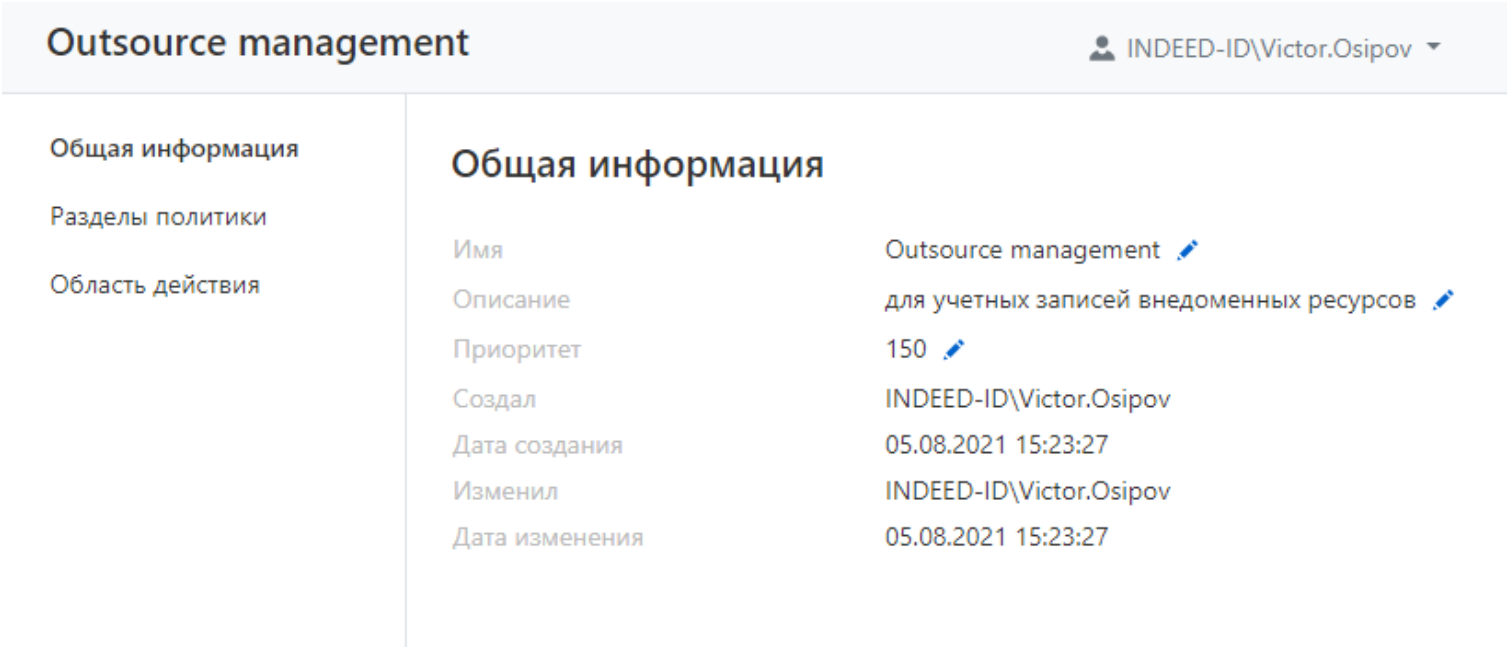
Добавление новой политики

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Для добавления, просмотра, редактирования и удаления политик необходимы соответствующие привилегии из раздела **Управление политиками** (Policy.Create, Policy.Read, Policy.Update, Policy.Delete).

Нажмите **Добавить** в разделе **Политики**,заполните поля **Имя политики**, **Описание** и **Приоритет**. Новая политика отобразится в списке.

Общая информация

Откройте страницу политики, ознакомьтесь с общей информацией, при необходимости внесите правки в **Имя**, **Описание** или **Приоритет**, нажав значок карандаша



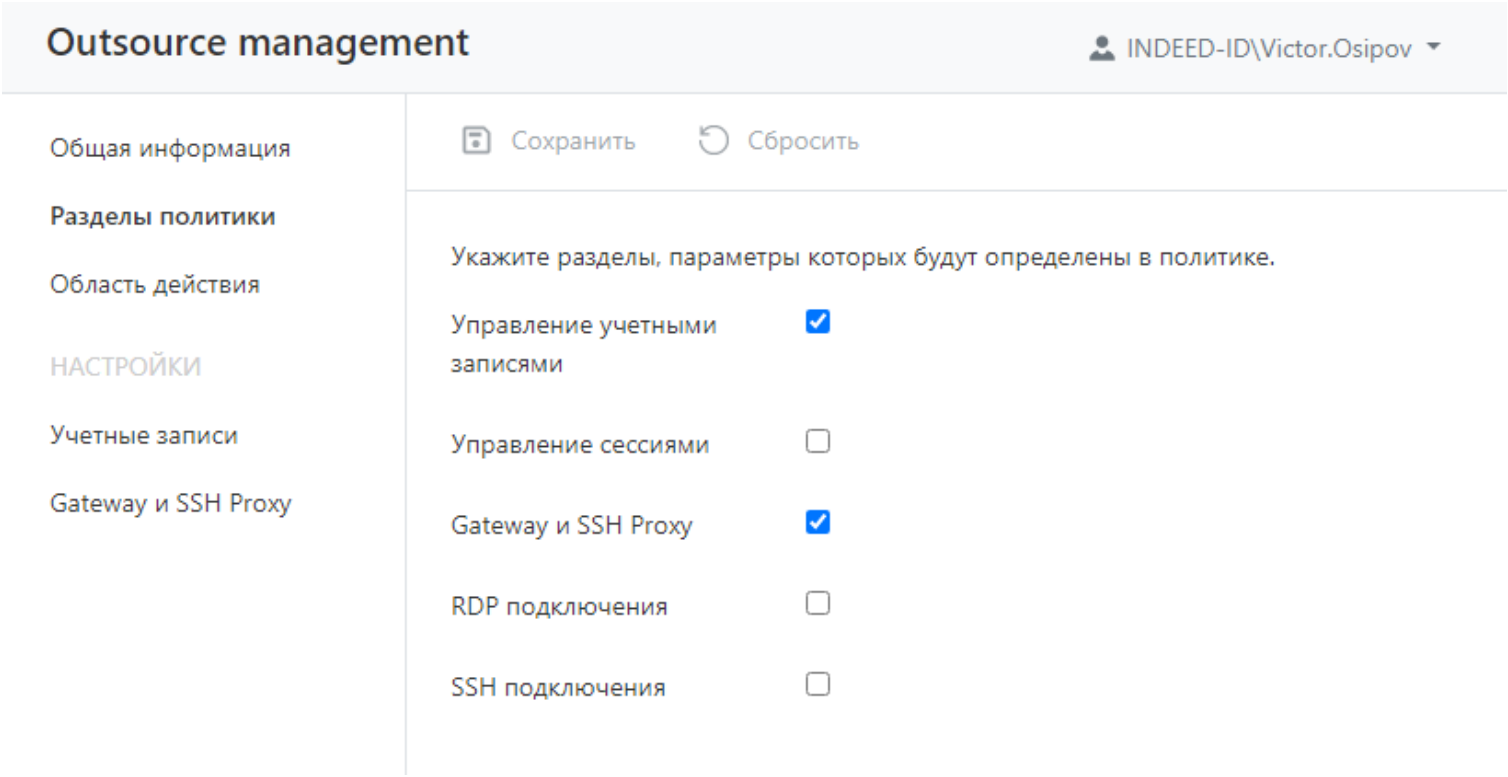
- **Имя** — название политики, устанавливается при создании новой политики, может быть изменено в любой момент эксплуатации.
- **Описание** — необязательное поле.

- **Приоритет** — числовое значение приоритета политики. Нулевой приоритет - минимальный, применяется к объектам в последнюю очередь.
- **Создал** — имя администратора Indeed PAM.
- **Дата создания** — дата и время создания политики.
- **Изменил** — имя администратора Indeed PAM, который сохранил настройки политики.
- **Дата изменения** — дата и время сохранения настроек политики.

Для редактирования **Имени**, **Описания** и **Приоритета** нажмите

Разделы политики

Перейдите в **Разделы политики** и отметьте разделы, параметры которых будут определены политикой, сохраните изменения. Соответствующие разделы станут доступными для настройки параметров.



> **ПРИМЕЧАНИЕ**
>
> Для неотмеченных разделов будут применяться другие политики по порядку их приоритета.

Область действия

> **ПРЕДУПРЕЖДЕНИЕ**

> Для назначения политик необходимы соответствующие привилегии (User.SetPolicy, UsersGroup.SetPolicy, Account.SetPolicy, Resource.SetPolicy, Domain.SetPolicy).

Содержит данные о том, к каким пользователям, группам пользователей, учетным записям, ресурсам или доменам применена политика.

Чтобы применить политику к объекту, нажмите **Добавить**, выберите тип объекта для установки политики и далее сами объекты.

Чтобы отменить действие политики для объектов, выберите нужные объекты и нажмите **Удалить**.

Создание копии политики

Отметьте одну политику в разделе **Политики** и нажмите **Создать копию**, заполните поля **Имя политики**, **Описание** и **Приоритет**.
Скопированная политика отобразится в списке.

Удаление политики

Перед удалением политики убедитесь, что она не применяется ни к каким объектам.

Отметьте нужные политики в разделе **Политики** и нажмите **Удалить**.

> **ПРИМЕЧАНИЕ**
>
> Политика **Default policy** недоступна для удаления.

Изменение приоритета политики

Отметьте галочкой одну политику в разделе **Политики**, нажмите **Задать приоритет** и введите число для значения приоритета политики.

Также изменить приоритет можно открыв нужную политику и в разделе **Общая информация** нажать значок карандаша рядом со значением приоритета.

Разделы политик

Учетные записи

Показ учетных данных

Опция	Описание
Сбрасывать пароль и SSH-ключ учетной записи после показа	Если опция включена, то пароль и SSH-ключ привилегированной учетной записи будет сбрасываться каждый раз после просмотра пользователем в своем личном кабинете (консоли пользователя).
Сбрасывать пароль и SSH-ключ через X мин.	После просмотра пароль и SSH-ключ будет сброшены на случайное значение через указанное количество минут.
Требовать указать причину просмотра пароля и SSH-ключа	Если опция включена, то пользователь каталога должен указать причину перед просмотром пароля или SSH-ключа учетной записи доступа.
Просмотр пароля и SSH-ключа требует подтверждения администратором PAM	Если опция включена, то перед каждым просмотром пользователем учетных данных администратор PAM должен подтвердить операцию.
Время ожидания подтверждения просмотра пароля и SSH-ключа, мин.	Таймаут ожидания подтверждения просмотра пароля и SSH-ключа, от 1 до 180 минут.
Шифровать SSH-ключ сгенерированным паролем перед показом пользователю	Если опция включена, то SSH-ключ будет показан в зашифрованном виде, а сгенерированный пароль шифрования - в скрытом. Ключ и пароль шифрования генерируется средствами PAM при просмотре данных каждый раз заново.

Задание учетных данных

Опция	Описание
Разрешить пользователям PAM задавать учетные данные для	Если опция включена, то когда пользователь попытается подключиться к ресурсу от имени учетной записи с

Опция	Описание
учетных записей, если они не заданы	незаданным паролем, то ему будет предложено задать пароль этой учетной записи в PAM системе.

Проверка и смена учетных данных

Опция	Описание
Синхронизировать ресурсы и УЗ по расписанию	Если опция включена, то будет выполняться автоматический поиск данных о ресурсах и учетных записей доступа.
Период синхронизации ресурсов и УЗ, сут.	Автоматический поиск данных о ресурсах и учетных записях доступа будет выполняться один раз в указанное количество дней, от 1 до 10000 дней
Периодически проверять пароль и SSH-ключ учетной записи	Если опция включена, то будет выполняться автоматическая проверка паролей и SSH-ключей для учетных записей доступа.
Период проверки пароля и SSH-ключа, сут.	Автоматическая проверка паролей и SSH-ключей учетных записей доступа будет выполняться один раз в указанное количество дней, от 1 до 10000 дней.
Сбрасывать пароль и SSH-ключ если обнаружено несовпадение	Если опция включена, то будет выполняться автоматический сброс паролей и ключей при расхождении в PAM и на ресурсах.
Удалять SSH-ключи, не управляемые PAM	Если в PAM нет SSH-ключа для добавленной учетной записи, а на ресурсе есть, то с ресурса все обнаруженные ключи будут удалены.
Проверять пароль и SSH-ключ при ручной установке	Если опция включена, то при установке или изменении пароля, или SSH-ключа будет выполняться их проверка.
Периодически изменять пароль и SSH-ключ учетной записи	Если опция включена, то для учетных записей доступа будет автоматически изменяться пароль или SSH-ключ на

Опция	Описание
	случайное значение.
Период изменения пароля и SSH-ключа, сут.	Автоматическое изменение пароля или SSH-ключа для учетных записей доступа будет выполняться один раз в указанное количество дней.

Требования к генератору паролей

Опция	Описание
Длина генерируемого пароля	Общее количество символов для автоматически генерируемых паролей.
Латинские строчные буквы	Если опция включена, то автоматически генерируемые пароли будут состоять из латинских строчных букв. При комбинации с другими настройками пароль будет содержать минимум одну латинскую строчную букву.
Латинские прописные буквы	Если опция включена, то автоматически генерируемые пароли будут состоять из латинских прописных букв. При комбинации с другими настройками пароль будет содержать минимум одну латинскую прописную букву.
Цифры	Если опция включена, то автоматически генерируемые пароли будут состоять из цифр. При комбинации с другими настройками пароль будет содержать минимум одну цифру.
Специальные символы	Если опция включена, то автоматически генерируемые пароли будут состоять из специальных символов. При комбинации с другими настройками пароль будет содержать минимум один специальный символ.
Запретить использование спецсимволов в начале пароля	Если опция включена, то пароль начнется с буквы или с цифры.

Опция	Описание
Максимальное число последовательных спецсимволов	Настройка определяет, сколько спецсимволов подряд разрешено. Например, при указании значения 1 пароль `password#!` не пройдет валидацию. При этом пароль `passwor#d!` пройдет валидацию, потому что спецсимволы идут не подряд, их разделяет латинская буква. Чтобы разрешить любое количество подряд идущих спецсимволов, укажите 0.
Запрещенные символы	Символы, которые генератор паролей не должен использовать при генерации паролей. Поле может быть пустым. В этом случае никаких ограничений не применяется.
Обязательные символы	Символы, из которых хотя бы один обязательно будет использован при генерации пароля. Поле может быть пустым. В этом случае никаких ограничений не применяется.
Количество паролей, которые не должны повторяться	Количество последних паролей учетной записи, с которыми новый пароль не будет повторяться.

Требования к паролю для ручного ввода

Опция	Описание
Минимальная длина пароля	Минимальное количество символов при ручном вводе пароля.
Ограничить символы для ручного ввода пароля	Если опция включена, то доступны для редактирования настройки, описанные в этой таблице. Если опция отключена, то в паролях разрешены любые символы.

Опция	Описание
Латинские строчные буквы	Если опция включена, то пароль должен содержать минимум одну латинскую строчную букву.
Латинские прописные буквы	Если опция включена, то пароль должен содержать минимум одну латинскую прописную букву.
Цифры	Если опция включена, то пароль должен содержать минимум одну цифру.
Специальные символы	Если опция включена, то пароль должен содержать минимум один спецсимвол.
Разрешить использование пробела	Если настройка включена, то пробелы допустимы в пароле, но не обязательны. Указать пробел в полях **Запрещенные символы** и **Обязательные символы** нельзя.
Запретить использование спецсимволов в начале пароля	Если опция включена, то пароль потребуется начинать с буквы или цифры.
Максимальное число последовательных спецсимволов	Настройка определяет, сколько спецсимволов подряд разрешено. Например, при указании значения 1 пароль `password#!` не пройдет валидацию. При этом пароль `passwor#d!` пройдет валидацию, потому что спецсимволы идут не подряд, их разделяет латинская буква. Чтобы разрешить любое количество подряд идущих спецсимволов, укажите 0.
Запрещенные символы	Символы, которые не должны использоваться в паролях. Указать в этом поле пробел нельзя. Поле может быть пустым. В этом случае никаких ограничений не применяется.

Опция	Описание
Обязательные символы	Символы, из которых хотя бы один обязательно требуется использовать при вводе пароля. Указать в этом поле пробел нельзя. Поле может быть пустым. В этом случае никаких ограничений не применяется.
Количество паролей, которые не должны повторяться	Количество последних паролей учетной записи, с которыми новый пароль не будет повторяться.

Сессии

Общее

Опция	Описание
Требовать указать причину подключения	Если опция включена, то при подключении к конечному ресурсу, пользователь обязан указать причину запуска сессии. **Внимание!** Если используете PostgreSQL Proxy, то предупредите пользователей, что потребуется вводить причину в то же поле, где имя учетной записи. Подробная информация в пункте Подключение к ресурсу через PostgreSQL Proxy.
Максимальная длительность сессии	Опция задействует предел длительности сессии в часах и минутах, после истечения которого сессия будет принудительно завершена.
Включить эксклюзивное использование учетной записи	Если опция включена, то учетная запись может быть использована только в одной активной сессии одновременно.
Открытие сессии требует подтверждения	Если опция включена, то для каждой открываемой сессии необходимо ручное подтверждение администратора PAM.

Опция	Описание
администратора PAM	**Внимание!** Оставьте опцию выключенной, если используете PostgreSQL Proxy, иначе открыть SQL-сессию будет невозможно.
Время ожидания подтверждения сессии, мин.	Таймаут для подтверждения администратором PAM, в интервале от 1 до 180 минут.
Прерывать сессию при отсутствии пользовательской активности	Если опция включена, то в случае отсутствия активности пользователя в течение заданного времени его сессия обрывается. Для уже существующих политик эта опция по умолчанию выключена, а для новых — включена. Под активностью пользователя понимается его взаимодействие с экраном или терминалом сессии, а также операции по передаче файлов. Эта опция политики применяется только для сессий, открытых через SSH Proxy и RDP Proxy.
Время отсутствия пользовательской активности, мин.	Минимальное значение: 1 минута Значение по умолчанию: 30 минут Максимальное значение: 720 минут
Сбрасывать пароль и SSH-ключ по завершении сессии	Сброс пароля и SSH-ключа после каждой сессии.

Артефакты

Опция	Описание
Сохранять текстовые логи сессии	Если опция включена, то после завершения сессии будет доступен для просмотра и скачивания текстовый лог. Поддерживается только в сессиях на Windows ресурсах при наличии PAM агента и в SSH-сессиях.

Опция	Описание
Продолжать RDP-сессию без логирования, если не удалось получить текстовый лог	Если опция включена, то при потере связи с PAM-агентом сессия не прерывается, пользователи могут продолжать работу в этой сессии. При этом в журнал однократно заносится событие "Потеряна связь с PAM-агентом", в текстовый лог сессии однократно записывается строка "WARNING: Lost connection with PAM Agent". При восстановлении связи с PAM-агентом в журнал однократно заносится событие "Восстановлена связь с PAM-агентом", в текстовый лог сессии однократно записывается строка "INFO: Connection with PAM Agent restored". Если опция выключена (по умолчанию), то при потере связи с PAM-агентом сессия прерывается.
Сохранять видео сессии	Если опция включена, то после завершения сессии будет доступна для просмотра и скачивания запись потокового видео. Поддерживается только при открытии сессий через PAM Gateway.
Количество кадров в секунду	Настройка определяет частоту кадров для записи потокового видео, от 1 до 10.
Разрешение видео	Настройка позволяет установить разрешение для записи потокового видео.
Ротация видео	Если опция включена, то записи потокового видео будут автоматически удаляться.
Удалять видео сессии старше X дней	Автоматическое удаление записи потокового видео старше указанного количества дней, от 1 до 10000.
Сохранять снимки экрана	Если опция включена, то снимки экрана сессии будут сохраняться. Поддерживается только при открытии сессий через PAM Gateway.

Опция	Описание
Интервал снимков, сек	Сохранение снимка экрана через указанной количество секунд, от 60 до 10000.
Разрешение изображения	Настройка позволяет установить разрешение снимка экрана.
Ротация снимков экрана	Если опция включена, то снимки экрана будут автоматически удаляться.
Удалять снимки экрана старше X дней	Автоматическое удаление снимков экрана старше указанного количества дней.
Сохранять переданные файлы	Если опция включена, то файлы при передаче с локальной машины на ресурс будут дублироваться в указанную сетевую папку. Поддерживается только для Windows ресурсов с включенным пробросом дисков (про раздел RDP - ниже).
Ротация переданных файлов	Если опция включена, то переданные файлы будут автоматически удаляться.
Удалять переданные файлы старше X дней	Автоматическое удаление файлов старше указанного количества дней, от 1 до 10000.

Отправка текстового лога по syslog

Опция	Описание
Ключевые слова	По syslog будут отправлены строки текстового лога, в которых будут найдены указанные ключевые слова. Ключевое слово может быть регулярным выражением.

Gateway и SSH Proxy

Опция	Описание
Переопределить настройки подключения к Gateway	Если опция включена, то следующие настройки будут использованы вместо указанных в разделе Конфигурация
Адрес RDCB	IP адрес/DNS имя Remote Desktop Connection Broker
Имя коллекции RDCB	Имя коллекции Remote Desktop Connection Broker для Indeed PAM Gateway
Использовать RDGW	Подключаться к Indeed PAM Gateway с использованием Remote Desktop Gateway
Адрес RDGW	Адрес Remote Desktop Gateway для Indeed PAM Gateway
Параметры Gateway RDP-файла	Параметры будут добавлены в настройки подключения по RDP к PAM Gateway и заменят старые настройки.
Переопределить настройки SSH Proxy	Если опция включена, то следующая настройка будет использована вместо указанной в разделе Конфигурация
Адрес SSH Proxy	IP адрес или DNS имя и порт (необязательно).

RDP

> **ПРИМЕЧАНИЕ**
>
> Настройки применяются только при подключении к серверам по протоколу RDP.

Опция	Описание
Принтеры	Если опция включена, то пользователь получит возможность пробросить принтер со своего рабочего места на конечный ресурс.
Буфер обмена	Если опция включена, то пользователь получит возможность использовать буфер обмена между своим рабочим местом и

Опция	Описание
	конечным ресурсом.
Смарт-карты	Если опция включена, то пользователь получит возможность пробросить смарт-карту со своего рабочего места на конечный ресурс.
Порты	Если опция включена, то пользователь получит возможность пробросить COM-порты со своего рабочего места на конечный ресурс.
Диски	Если опция включена, то пользователь получит возможность пробросить локальные диски со своего рабочего места на конечный ресурс.
Требовать доверенный сертификат ресурса для открытия RDP-сессии	Если опция включена и сертификат ресурса недействительный, то сессия не откроется. Если опция выключена и сертификат ресурса недействительный, то сессия откроется.
Параметры RDP-файла	Параметры, которые будут добавлены в настройки подключения RDP и заменят старые настройки.

SSH

Повышение привилегий

Опция	Описание
Разрешить выполнять pamsu	Поддержка выполнения команд с привилегиями root в SSH-сессиях на ресурсах с установленным компонентом PamSu.

ИНФОРМАЦИЯ

> Разрешение, выданное на выполнение pamsu при создании разрешения, приоритетнее, чем настройка в политике.

Разрешенные и запрещенные команды

Опция	Описание
Приглашение оболочки (prompt)	Регулярное выражение приглашения оболочки для корректного распознавания ввода команд. При вводе регулярного выражения обратите внимание, что экранировать символы `<` и `>` не требуется, так как они не входят в список специальных символов: `.[{}()*+?|^$`. Подробная информация о синтаксисе регулярных выражений Boost доступна по ссылке.
Реакция на запрещенную команду	Поведение терминала в ответ на запрещенную команду: CTRL+C (отмена выполнения) либо завершение сессии.
SSH-команды	Список разрешенных или запрещенных для выполнения команд в SSH-сессии.

Для составления списка контролируемых команд:

1. Справа от параметра **SSH-команды** нажмите **Добавить**.
2. Введите команду или регулярное выражение.

   При вводе регулярного выражения обратите внимание, что экранировать символы `<` и `>` не требуется, так как они не входят в список специальных символов: `.[{}()\*+?|^$`. Символ `]` также является специальным, но только когда введен после `[`.

   Подробная информация о синтаксисе регулярных выражений Boost доступна по ссылке.
3. Выберите состояние **Разрешена** либо **Запрещена**.

> **ИНФОРМАЦИЯ**
>
> Запрет на выполнение команд имеет приоритет над разрешением.
>
> Без явного разрешения команды будут считаться запрещенными, поэтому не рекомендуется удалять последнее правило, разрешающее выполнение команд.

Для разрешения либо запрета сразу нескольких команд отметьте их флажками и нажмите **Разрешить** или **Запретить**.

При работе со списком команд, а также при попытках выполнения запрещенной команды в журнале фиксируются соответствующие события.

Передача данных

Опция	Описание
SCP	Параметр передачи файлов по протоколу SCP
SFTP	Параметр передачи файлов по протоколу SFTP
Максимальный размер файла, МБ	Файл большего размера не удастся передать.

Пользователи

Пользователи

Группы пользователей

Группы пользователей

Ресурсы

Количество глав: 5

Службы

Службы

Группы ресурсов

Группы ресурсов

Учетные записи

Количество глав: 2

Домены

Количество глав: 4

Структура

Структура

Разрешения

Количество глав: 3

Запросы сессий

Запросы сессий

Активные сессии

Активные сессии

Все сессии

Количество глав: 1

События

События

Уведомления

Уведомления

Конфигурация

Количество глав: 2

Роли

Роли

Приложения

Приложения

Пользователи

Раздел предназначен для работы с каталогом пользователей Active Directory.

По умолчанию на странице отображается 15 пользователей.

> **ИНФОРМАЦИЯ**
>
> Отображаемое по умолчанию количество пользователей на странице можно изменить в конфигурационном файле.

Внизу страницы расположен пагинатор для просмотра остальных пользователей. Если пользователей меньше 15, т.е. они помещаются на одну страницу, то пагинатор не отображается.

Можно просмотреть максимум 1000 пользователей. На странице с тысячным пользователем отображается сообщение о невозможности загрузить больше пользователей.

Поиск

Поиск осуществляется в разделе **Пользователи**.

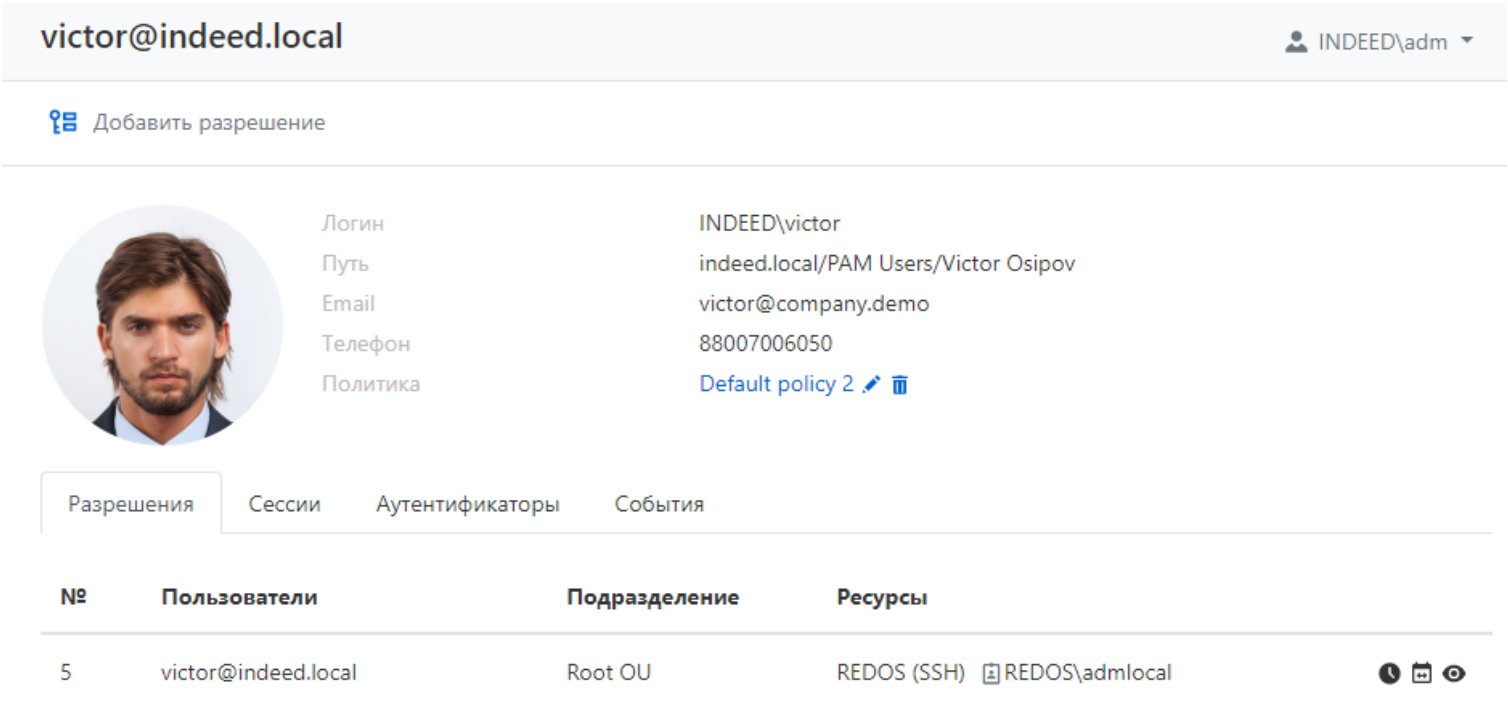
Быстрый поиск

Введите в строку поиска **Имя**, **Фамилию**, **Номер телефона** или **Email** полностью или частично.

Расширенный поиск

Нажмите **Расширенный поиск** и введите один или несколько критериев, **Имя**, **Фамилию**, **Номер телефона** или **Email** полностью или частично.

Профиль пользователя



Профиль отображает данные пользователя Active Directory:

- **Логин** — имя для входа.
- **Путь** — LDAP.
- **Email** — адрес электронной почты.
- **Телефон** — контактный телефон.
- **Политика** — политика сессий, привязанная к пользователю.
- **Фото** — фотография из Active Directory (атрибут thumbnailPhoto).

Разрешения

Все разрешения пользователя доступны на вкладке **Разрешения**.

Для каждого разрешения отображаются следующие данные:

- **№** — порядковый номер разрешения.
- **Пользователи** — пользователь каталога Active Directory, для которого выдано разрешение.
- **Ресурсы** — ресурсы, на которых может быть открыта RDP, SSH или web-сессия от имени учетной записи, указанной в разрешении. Рядом с именем ресурса указана привилегированная учетная запись, которая используется для доступа к ресурсу.
- **Значки статуса разрешения** — подсказка о статусе отобразится при наведении курсора мыши.

Сессии

Все активные и завершенные сессии пользователя доступны на вкладке **Сессии**.

Для каждой сессии отображаются следующие данные:

- **Пользователь** — пользователь каталога Active Directory, который инициировал сессию.
- **Учетная запись** — учетная запись, которая используется для открытия RDP, SSH или web-сессии.
- **Ресурс** — ресурс, на котором была открыта RDP, SSH или web-сессия от имени учетной записи.
- **Адрес подключения** — фактический адрес, используемый при открытии сессии.
- **Длительность** — длительность сессии.
- **Подключение** — тип удаленного подключения (RDP, SSH, пользовательские типы)
- **Подключение к PAM** — дата и время открытия сессии.
- **Завершение** — дата и время закрытия сессии.
- **Состояние** — отображает текущее состояние сессии (активная, завершенная или прерванная).

Для просмотра подробной информации о сессии необходимо нажать на нее. Чтобы вывести все сессии для данного пользователя, нажмите **Показать все**.

Аутентификаторы

Все зарегистрированные аутентификаторы пользователя, а также настройка требования доступны на вкладке **Аутентификаторы**.

События

События пользователя доступны на вкладке **События**, здесь отображаются последние 5 событий.

Для каждого события отображаются следующие данные:

- **Время создания** — дата и время создания события.
- **Код** — код события.
- **Событие** — описание события.
- **Компонент** — компонент Indeed PAM, который сгенерировал событие.
- **Инициатор** — учетная запись, которая инициировала генерацию события.

Для просмотра подробной информации о событии необходимо нажать на него. Чтобы вывести все события для данного пользователя, нажмите **Показать все**.

Сброс аутентификатора пользователя

1. Откройте профиль пользователя и перейдите на вкладку **Аутентификаторы**.
2. Нажмите ✕ справа от нужного аутентификатора.

Отключение аутентификатора пользователя

1. Откройте профиль пользователя и перейдите на вкладку **Аутентификаторы**.
2. Нажмите ✎ справа от **Требовать второй фактор** и выберите одну из опций.
   - **По умолчанию** — по умолчанию требуется ввод пользователем второго фактора для аутентификации в системе.
   - **Включено** — у пользователя будет запрашиваться второй фактор для аутентификации в системе.
   - **Отключено** — у пользователя не будет запрашиваться второй фактор для аутентификации в системе.

Блокировка пользователя

С помощью этой функции администратор PAM может быстро закрыть пользователю доступ к ресурсам. При этом менять ресурсы и учетные записи не нужно.

Заблокированный пользователь не может:

- открывать сессии
- просматривать, устанавливать и менять пароль учетной записи
- получать доступ к аутентификационным данным приложений AAPM

В момент блокировки пользователя закрываются все его активные сессии.

> ⚠ **РЕКОМЕНДАЦИЯ**
>
> Заблокируйте пользователя, если заметили от него подозрительные действия. Это позволит быстро закрыть пользователю доступ к ресурсам до выяснения обстоятельств. Если тревога

ложная, то вы сможете разблокировать пользователя. Это так же быстро, как заблокировать.

Чтобы заблокировать пользователя:

1. Зайдите в раздел **Пользователи**.
2. Откройте профиль пользователя.
3. Нажмите **Заблокировать**.
4. В окне подтверждения операции нажмите **Заблокировать**.

> ⚠ **ВНИМАНИЕ**
>
> Не используйте эту функцию, чтобы закрывать доступ уволенным сотрудникам. У них останется возможность аутентифицироваться в консоль пользователя и консоль администратора (если доступ был). При увольнении сотрудников удаляйте пользователей из каталога Active Directory.

Разблокировка пользователя

Чтобы разблокировать пользователя:

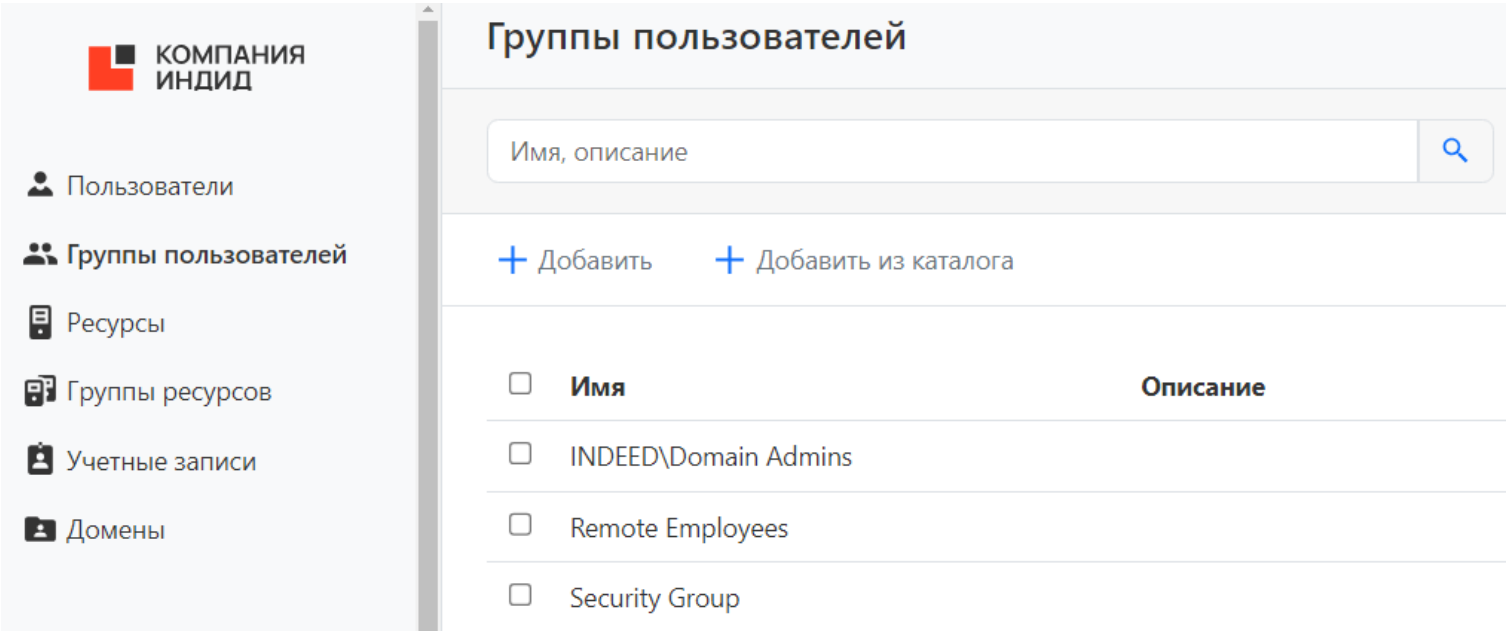
1. Зайдите в раздел **Пользователи**.
2. Откройте профиль заблокированного пользователя.
3. Нажмите **Разблокировать**.
4. В окне подтверждения операции нажмите **Разблокировать**.

Выбор политики для пользователя

1. Откройте профиль пользователя.
2. Нажмите , чтобы добавить или изменить политику.

Группы пользователей

Раздел предназначен для работы с разрешениями групп пользователей.



Создание группы пользователей PAM

Чтобы добавить группу пользователей, выполните следующие действия:

1. Перейдите в раздел **Группы пользователей**.
2. Нажмите **Добавить**, введите название группы и нажмите **Сохранить**.

Создание группы пользователей из каталога Active Directory

Чтобы добавить группу пользователей из каталога Active Directory, выполните следующие действия:

1. Перейдите в раздел **Группы пользователей**.
2. Нажмите **Добавить из каталога**, выберите группу и нажмите **Сохранить**.

Управление группой пользователей

Добавление пользователей в группу

> ⓘ **ПРИМЕЧАНИЕ**
>
> Только для групп, созданных через PAM.

1. Перейдите в созданную группу пользователей.
2. В разделе **Пользователи** нажмите **Добавить** и выберите нужных пользователей.

Добавление разрешения на группу пользователей

1. Перейдите в созданную группу пользователей.
2. Нажмите **Добавить разрешение** и выдайте его.

Просмотр созданных разрешений

1. Перейдите в раздел **Разрешения**.
2. Посмотрите выданные разрешения для выбранной группы пользователей.

Просмотр сведений о текущих сессиях в рамках группы пользователей и событиях системы PAM

- В разделе **Сессии** отображаются активные сессии.
- В разделе **События** отображаются события, произошедшие в PAM.

Синхронизация группы пользователей с каталогом

> ⓘ **ПРИМЕЧАНИЕ**
>
> Только для групп из Active Directory.

1. Перейдите в созданную группу пользователей.
2. Нажмите **Синхронизировать**.

Выбор политики для группы пользователей

1. Перейдите в созданную группу пользователей.

2. Нажмите , чтобы добавить или изменить политику.

Ресурсы

Раздел предназначен для работы с серверами, рабочими станциями, сетевым оборудованием и клиентскими приложениями.

Поиск ресурсов

Поиск осуществляется в разделе **Ресурсы**.

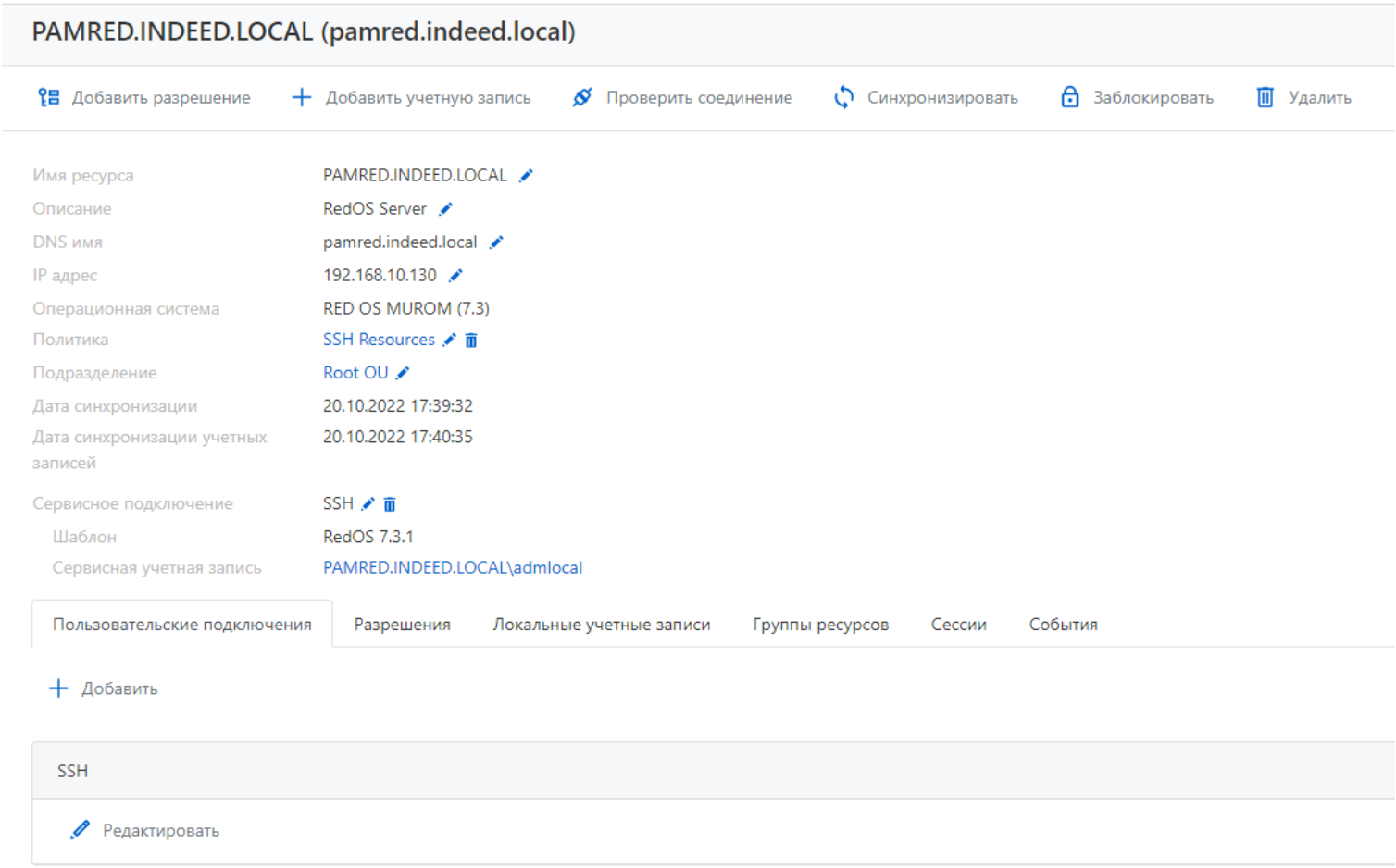
Быстрый поиск

Введите в строку поиска **Имя ресурса** или **Адрес (DNS имя/IP адрес)** полностью или частично.

Расширенный поиск

Нажмите **Расширенный поиск** и введите один или несколько критериев, **Имя ресурса**, **DNS-имя**, **IP-адрес** полностью или частично. Выберите **Состояние ресурса**, **Сервисное подключение**, **Пользовательское подключение**, **Отпечаток SSH-ключа**.

Профиль ресурса



Профиль отображает данные указанные при добавлении:

- **Имя ресурса** — имя компьютера (актуализируется после выполнения синхронизации).
- **Описание** — произвольный текст.
- **Операционная система** — название и версия операционной системы (заполняется после выполнения синхронизации).
- **Политика** — набор правил действующий на локальные учетные записи доступа, добавленные в Indeed PAM.
- **Подразделение** — имя подразделения в котором состоит ресурс.
- **Дата синхронизации** — дата и время последней синхронизации данных о ресурсе.
- **Дата синхронизации учетных записей** — дата и время последней синхронизации учетных записей ресурса.
- **Сервисное подключение** — тип подключения к ресурсу, которое будет использоваться локальной или доменной сервисной учетной записью.
- **Шаблон** — имя шаблона, используемого для выполнения сервисных операций (для SSH коннектора).
- **Сервисная учетная запись** — имя учетной записи, используемой для сервисного подключения.

Пользовательские подключения

Здесь отображаются и настраиваются подключения для открытия привилегированных сессий.

Для каждого ресурса можно создавать несколько пользовательских подключений, если на одном сервере установлены несколько приложений, к которым необходим привилегированный доступ.

Разрешения

Все разрешения, в которых используется ресурс отображаются на вкладке **Разрешения**.

Для каждого разрешения отображаются следующие данные:

- **№** — номер разрешения.
- **Пользователи** — пользователи каталога Active Directory, для которых выданы разрешения.
- **Ресурсы** — ресурсы, на которых может быть открыта RDP, SSH или web-сессия от имени учетной записи, указанной в разрешении.
- **Подразделение** — имя подразделения, в котором состоит ресурс с данным разрешением.
- **Значки статуса разрешения** — подсказка о статусе отобразится при наведении курсора мыши.

Локальные учетные записи

Все добавленные локальные учетные записи доступа отображаются на вкладке **Локальные учетные записи**.

Для каждой локальной учетной записи отображаются следующие данные:

- **Имя** — имя локальной учетной записи ресурса.
- **Размещение** — название ресурса, на котором размещена локальная учетная запись.
- **Состояние** — состояние в котором, находится локальная ученая запись.
- **Подразделение** — имя подразделения, в котором состоит ресурс с данной локальной учетной записью.
- **Описание** — произвольный текст.

Группы ресурсов

Группы ресурсов, в которых состоит данный ресурс, отображаются на вкладке **Группы ресурсов**.

Чтобы добавить группу ресурсов нажмите кнопку + Добавить .

После добавления группы ресурсов будут отображаться следующие данные:

- **Группа ресурсов** — название добавленной группы ресурсов.
- **Тип подключения** — тип подключения к ресурсу.
- **Адрес подключения** — адрес ресурса.
- **Учетная запись** — учетная запись, которая используется для подключения к ресурсу.

Сессии

Все активные и завершенные сессии на ресурсе отображаются на вкладке **Сессии**.

Для каждой сессии отображаются следующие данные:

- **Пользователь** — пользователь каталога Active Directory, который инициировал сессию.
- **Учетная запись** — учетная запись, которая используется для открытия RDP, SSH или web-сессии.
- **Ресурс** — ресурс, на котором была открыта RDP, SSH или web-сессия от имени учетной записи.
- **Адрес подключения** — фактический адрес подключения к конечному ресурсу
- **Длительность** — длительность сессии.
- **Подключение** — тип подключения.
- **Подключение к PAM** — дата и время открытия сессии
- **Завершение** — дата и время закрытия сессии.
- **Состояние** — отображает текущее состояние сессии (Активная или завершенная).

Чтобы вывести все сессии для данного ресурса, нажмите кнопку **Показать все**.

События

Все события на ресурсе отображаются на вкладке **События**, здесь отображаются последние 5 событий.

Для каждого события отображаются следующие данные:

- **Время создания** — дата и время создания события.
- **Код** — код события.

- **Событие** — описание события.
- **Компонент** — компонент Indeed PAM, который сгенерировал событие.
- **Инициатор** — учетная запись, которая инициировала генерацию события.

Для просмотра подробной информации о событии необходимо раскрыть его. Чтобы вывести все события для данного ресурса, нажмите кнопку **Показать все**.

Службы

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Эта вкладка отображается только если на выбранном ресурсе настроено сервисное подключение для Windows.

Все добавленные службы отображаются на вкладке **Службы**.

Для каждой службы отображаются следующие данные:

- **Имя службы** — значение, заданное при создании службы. Совпадает со значением поля Имя службы (Service name) оснастки Службы на ресурсе.
- **Учетная запись** — учетная запись, от имени которой запускается служба.
- **Описание** — произвольный текст.

Также на этой вкладке вы можете добавить службу для этого ресурса, для этого нажмите **Добавить**.

Выбор политики для ресурса

1. Откройте профиль ресурса.
2. Нажмите ✎, чтобы добавить или изменить политику.

Добавление ресурсов

Добавление ресурса вручную

Для предоставления доступа к ресурсу пользователям каталога необходимо добавить ресурс в Indeed PAM.

1. Нажмите **Добавить** в разделе **Ресурсы**.
2. Выберите **Подразделение**.
3. Введите **Имя ресурса**, **DNS** и/или **IP-адрес** и **Описание**.
   Для ресурсов на базе ОС Windows необходимо указывать реальное имя компьютера.
   При указании IP-адреса учитывайте, что он обязательно должен быть статическим.

Добавление ресурсов из файла

1. Подготовьте CSV-файл с ресурсами.
2. Нажмите **Добавить из файла** в разделе **Ресурсы**.
3. Выберите созданный CSV-файл.
4. Если для ресурсов необходимо определить политику поставьте галочку **Добавлять с политикой**.
5. Нажмите **Сохранить**.

Формат строки ресурса в CSV

```
Имя ресурса; Описание; DNS; IP-адрес; Тип пользовательского подключения; Адрес пользовательского подключения; Порт пользовательского подключения; URL страницы входа; URL страницы входа является регулярным выражением; Имя учетной записи для сервисного подключения; Тип сервисного подключения; Шаблон сервисного подключения SSH; Адрес сервисного подключения; Порт сервисного подключения; Пароль для привилегированного входа Cisco
```

Пример

```
Computer1;Typical Computer 1;res.test.com;;RDP;;;;;;;;;
```

```
Computer2;Typical Computer 2;;192.168.0.102;SSH;;;;;;;;;
```

Название	Приоритет	Описание
Имя ресурса	Обязательный	Имя ресурса в системе Indeed PAM.
Описание	Необязательный	Произвольный текст.
DNS или IP-адрес	Обязательный	DNS или IP-адрес ресурса. Необходимо указать один из параметров.
Тип пользовательского подключения	Обязательный	Указывается имя пользовательского подключения. Доступные пользовательские подключения и их имена можно посмотреть в разделе Конфигурации → Пользовательское подключение.
Адрес пользовательского подключения	Необязательный	Указывается IP-адрес или DNS для переопределения адреса подключения при подключении к ресурсу.
Порт пользовательского подключения	Необязательный	Указывается порт для его переопределения при подключении к ресурсу.
URL страницы входа	Необязательный	Указывается URL станицы входа web-приложения.
URL страницы входа является регулярным выражением	Необязательный	Указывается если задан URL страницы входа. Принимает значения TRUE/FALSE.
Имя учетной записи для сервисного подключения	Необязательный	Указывается имя сервисной учетной записи от имени которой будут выполняться сервисные операции. Учетная запись должна быть добавлена в систему.

Название	Приоритет	Описание
Тип сервисного подключения	Необязательный	Указывается имя сервисного подключения. Имена сервисных подключений можно посмотреть в разделе Конфигурации → Сервисное подключение.
Шаблон сервисного подключения SSH	Необязательный	Указывается имя SSH шаблона, если Тип сервисного подключения указан SSH. Имена SSH-шаблонов можно посмотреть в разделе Конфигурации → Сервисное подключение.
Адрес сервисного подключения	Необязательный	Указывается IP-адрес или DNS для переопределения адреса подключения при подключении к ресурсу.
Порт сервисного подключения	Необязательный	Указывается порт для его переопределения.
Пароль для привилегированного входа Cisco	Необязательный	Указывается для привилегированного входа Cisco, если Тип сервисного подключения указан Cisco IOS.

Настройка пользовательского подключения

Для каждого ресурса необходимо настроить пользовательское подключение, которое будет использовано для открытия сессии на ресурсе.

Настройка RDP-подключения

1. Выберите значение **RDP** в поле **Тип подключения**.
2. Если адрес подключения отличается от DNS или IP-адреса ресурса, то укажите его, нажав **Указать вручную**.
3. Введите **Порт**, если отличается от стандартного.
4. Включите опцию **Запускать как администратор**, если требуется открывать сессию с параметром **mstsc /admin**.

5. Завершите добавление ресурса.

> ⓘ **ИНФОРМАЦИЯ**
>
> При открытии сессии можно выбрать локальные диски для использования в удаленной сессии. Подключиться без перенаправления локальных дисков тоже можно.

Настройка SSH-подключения

1. Выберите значение **SSH** в поле **Тип подключения**.
2. Если адрес подключения отличается от DNS или IP-адреса ресурса, то укажите его, нажав **Указать вручную**.
3. Введите **Порт**, если отличается от стандартного.
4. Завершите добавление ресурса.

Настройка клиентского подключения

В Indeed PAM стандартными являются подключения RDP и SSH, остальные типы подключения, например, веб-сессия, или подключение к СУБД, настраиваются отдельно для каждого целевого приложения. Далее будут рассмотрены примеры настройки подключения к веб-консоли Citrix NetScaler и MS SQL Managemet Studio. После установки Indeed PAM эти типы подключения будут отсутствовать в списке подключений. Для создания нового типа подключения необходимо обратиться службу технической поддержки Indeed.

Настройка веб-сессии

1. Выберите значение **Citrix NetScaler** в поле **Тип подключения**.
2. Введите **URL** веб-приложения.
3. Введите **URL страницы входа** веб-приложения.
4. Завершите добавление ресурса.

> ⓘ **ИНФОРМАЦИЯ**
>
> Если **URL страницы входа** может не соответствовать указанному значению после обращения к нему, то включите опцию **Регулярное выражение**. Опция позволяет указывать выражение, которому будет соответствовать любое значение адреса.

Настройка подключения к СУБД

1. Выберите значение **MS SQL Management Studio** в поле **Тип подключения**.
2. Если адрес подключения экземпляра MS SQL Server отличается от DNS или IP-адреса ресурса, то укажите его, нажав **Указать вручную**.
3. Введите **Порт** при необходимости.
4. Переопределите произвольные поля из шаблона при необходимости.
5. Завершите добавление ресурса.

Настройка сервисного подключения для ресурсов

Для ресурсов на базе ОС Windows, ОС *nix и СУБД MS SQL Server, MySQL, OracleDB и PostgreSQL, а также Cisco IOS и Inspur BMC можно настроить сервисное подключение, которое позволит выполнять следующие операции:

- проверка соединения с ресурсом;
- синхронизация учетных записей;
- проверка пароля и ключа учетных записей;
- сброс пароля и ключа учетных записей;
- синхронизация групп безопасности учетных записей;
- синхронизация данных о версии ОС или СУБД.

Настройку сервисного подключения можно выполнить как во время добавления ресурса, так и после его добавления в Indeed PAM. В данной статье рассмотрены примеры настройки сервисного подключения для уже добавленных в систему ресурсов.

> **ИНФОРМАЦИЯ**
>
> Проверка паролей локальных учетных записей ресурсов под управлением ОС Linux может выполняться без настройки сервисного подключения к ресурсу.

Добавление учетных записей

Сервисные операции выполняются от имени сервисной учетной записи. В роли сервисной может быть назначена как локальная учетная запись ресурса, так и доменная учетная запись. Перед настройкой сервисного подключения требуется добавить в систему локальную или доменную учетную запись.

- Добавление ресурса
- Добавление локальных учетных записей
- Добавление домена
- Добавление доменных учетных записей

Настройка сервисного подключения для ОС Windows

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Перед настройкой сервисного подключения требуется добавить в Indeed PAM локальную или доменную учетную запись.

Чтобы настроить сервисное подключение для ОС Windows:

1. Откройте профиль ресурса и нажмите ✎ справа от параметра **Сервисное подключение**.
2. В поле **Коннектор** выберите значение **Windows**.
3. Если адрес сервисного подключения отличается от адреса ресурса, то для переключателя **Адрес подключения** выберите значение **Указать вручную** и введите другой адрес в поле **DNS-имя / IP-адрес**.
4. Нажмите **Вперед** для перехода к выбору учетной записи.
5. Выберите учетную запись.
6. Нажмите **Сохранить** для завершения настройки сервисного подключения.

Настройка сервисного подключения для ОС *nix

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Перед настройкой сервисного подключения требуется:
>
> - добавить в Indeed PAM локальную или доменную учетную запись;
> - загрузить шаблон SSH-коннектора.

Чтобы настроить сервисное подключение для ОС *nix:

1. Откройте профиль ресурса и нажмите ✎ справа от параметра **Сервисное подключение**.
2. В поле **Коннектор** выберите значение **SSH**.
3. Выберите **Шаблон** сервисного взаимодействия. В этом поле отображаются только загруженные в Indeed PAM шаблоны.

4. Если адрес сервисного подключения отличается от адреса ресурса, то для переключателя **Адрес подключения** выберите значение **Указать вручную** и введите другой адрес в поле **DNS-имя / IP-адрес**.
5. В поле **Порт** укажите значение, если отличается от стандартного.
6. Нажмите **Вперед** для перехода к выбору учетной записи.
7. Выберите учетную запись.
8. Нажмите **Сохранить** для завершения настройки сервисного подключения.

Настройка сервисного подключения для СУБД MS SQL Server

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Перед настройкой сервисного подключения требуется добавить в Indeed PAM локальную или доменную учетную запись.

Чтобы настроить сервисное подключение для СУБД MS SQL Server:

1. Откройте профиль ресурса и нажмите справа от параметра **Сервисное подключение**.
2. В поле **Коннектор** выберите значение **Microsoft SQL Server**.
3. Если адрес сервисного подключения отличается от адреса ресурса, то для переключателя **Адрес подключения** выберите значение **Указать вручную** и введите другой адрес в поле **DNS-имя / IP-адрес**.
4. В поле **Порт** укажите значение, если отличается от стандартного.
5. Нажмите **Вперед** для перехода к выбору учетной записи.
6. Выберите учетную запись.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Если экземпляр MS SQL Server не входит в состав домена Active Directory, то в качестве сервисной можно использовать только учетные записи СУБД.

> Если входит, то можно использовать как учетные записи СУБД, так и доменные учетные записи.

7. Нажмите **Сохранить** для завершения настройки сервисного подключения.

Настройка сервисного подключения для СУБД OracleDB

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Перед настройкой сервисного подключения требуется добавить в Indeed PAM локальную или доменную учетную запись.

Чтобы настроить сервисное подключение для СУБД OracleDB:

1. Откройте профиль ресурса и нажмите ✎ справа от параметра **Сервисное подключение**.
2. В поле **Коннектор** выберите значение **Oracle Database**.
3. Для переключателя **Адрес подключения** выберите значение **Указать вручную** и в поле **DNS-имя / IP-адрес** введите строку подключения к СУБД вида **host[:port][/service name]**.
4. Нажмите **Вперед** для перехода к выбору учетной записи.
5. Выберите учетную запись.
6. Нажмите **Сохранить** для завершения настройки сервисного подключения.

Настройка сервисного подключения для СУБД PostgreSQL или PostgreSQL Pro

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Перед настройкой сервисного подключения требуется добавить в Indeed PAM локальную или доменную учетную запись.

Чтобы настроить сервисное подключение для СУБД PostgreSQL или PostgreSQL Pro:

1. Откройте профиль ресурса и нажмите ✎ справа от параметра **Сервисное подключение**.
2. В поле **Коннектор** выберите значение **PostgreSQL**.

3. Если адрес сервисного подключения отличается от адреса ресурса, то для переключателя **Адрес подключения** выберите значение **Указать вручную** и введите другой адрес в поле **DNS-имя / IP-адрес**.
4. В поле **Порт** укажите значение, если отличается от стандартного.
5. Нажмите **Вперед** для перехода к выбору учетной записи.
6. Выберите учетную запись.
7. Нажмите **Сохранить** для завершения настройки сервисного подключения.

Настройка сервисного подключения для СУБД MySQL

Поддерживается для MySQL версии 8.4.5 и меньше. Для выполнения сервисных операций Indeed PAM использует тип аутентификации **mysql_native_password**. В версиях 8.4.0–8.4.5 этот тип по умолчанию отключен, потребуется его включить в соответствии с документацией MySQL. Остальные типы аутентификации не поддерживаются.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Перед настройкой сервисного подключения требуется добавить в Indeed PAM локальную или доменную учетную запись.

Чтобы настроить сервисное подключение для СУБД MySQL:

1. Откройте профиль ресурса и нажмите ✎ справа от параметра **Сервисное подключение**.
2. В поле **Коннектор** выберите значение **MySQL**.
3. Если адрес сервисного подключения отличается от адреса ресурса, то для переключателя **Адрес подключения** выберите значение **Указать вручную** и введите другой адрес в поле **DNS-имя / IP-адрес**.
4. В поле **Порт** укажите значение, если отличается от стандартного.
5. Нажмите **Вперед** для перехода к выбору учетной записи.
6. Выберите учетную запись.
7. Нажмите **Сохранить**.
8. Откройте профиль сервисной учетной записи MySQL и нажмите ✎ справа от параметра **Имя**.
9. Укажите значение хоста для учетной записи: `%/Имя хоста/IP-адрес`.

Настройка сервисного подключения для Cisco IOS

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Перед настройкой сервисного подключения требуется добавить в Indeed PAM локальную или доменную учетную запись.

Чтобы настроить сервисное подключение для Cisco IOS:

1. Откройте профиль ресурса и нажмите ✎ справа от параметра **Сервисное подключение**.
2. В поле **Коннектор** выберите значение **Cisco IOS**.
3. Если требуется задать пароль для привилегированного режима, то включите опцию **Привилегированный режим имеет пароль** и укажите пароль.
4. Если адрес сервисного подключения отличается от адреса ресурса, то для переключателя **Адрес подключения** выберите значение **Указать вручную** и введите другой адрес в поле **DNS-имя / IP-адрес**.
5. В поле **Порт** укажите значение, если отличается от стандартного.
6. Нажмите **Вперед** для перехода к выбору учетной записи.
7. Выберите учетную запись.
8. Нажмите **Сохранить** для завершения настройки сервисного подключения.

Настройка сервисного подключения для Inspur BMC

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Перед настройкой сервисного подключения требуется добавить в Indeed PAM локальную или доменную учетную запись.

Чтобы настроить сервисное подключение для Inspur BMC:

1. Откройте профиль ресурса и нажмите ✎ справа от параметра **Сервисное подключение**.
2. В поле **Коннектор** выберите значение **Inspur BMC**.

3. Если адрес сервисного подключения отличается от адреса ресурса, то для переключателя **Адрес подключения** выберите значение **Указать вручную** и введите другой адрес в поле **DNS-имя / IP-адрес**.
4. В поле **Порт** укажите значение, если отличается от стандартного.
5. Нажмите **Вперед** для перехода к выбору учетной записи.
6. Выберите учетную запись.
7. Нажмите **Сохранить** для завершения настройки сервисного подключения.

Операции над ресурсами

Редактирование ресурса

Для редактирования доступны следующие поля ресурса:

- **Имя ресурса**;
- **Описание**;
- **Подразделение**;
- **Политика**;
- **Пользовательское подключение**;
- **Сервисное подключение**.

Чтобы отредактировать ресурс, нажмите ✎ в профиле ресурса справа от нужного параметра.

Удаление связанных сущностей

Для удаления значений доступны следующие поля ресурса:

- **Политика**;
- **Сервисное подключение**.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> При удалении сервисного подключения с ресурса все связанные с ним службы также удаляются. Удаленные службы нельзя восстановить.
>
> Удаленные службы перестают отображаться в разделе **Службы**, но их можно просмотреть с помощью расширенного поиска.

Чтобы удалить **Политику** или **Сервисное подключение** с ресурса, нажмите иконку корзины в профиле ресурса справа от нужного параметра.

Добавление пользовательского подключения

Функция позволяет добавить одно или несколько пользовательских подключений, доступных для данного ресурса.

1. Нажмите **Добавить** на вкладке **Пользовательские подключения**.
2. Выберите тип подключения.
3. Укажите адрес, порт подключения и другие параметры пользовательского подключения.

Добавление учетной записи

Функция позволяет добавлять в Indeed PAM локальные учетные записи ресурса, которые могут использоваться для предоставления доступа на ресурс.

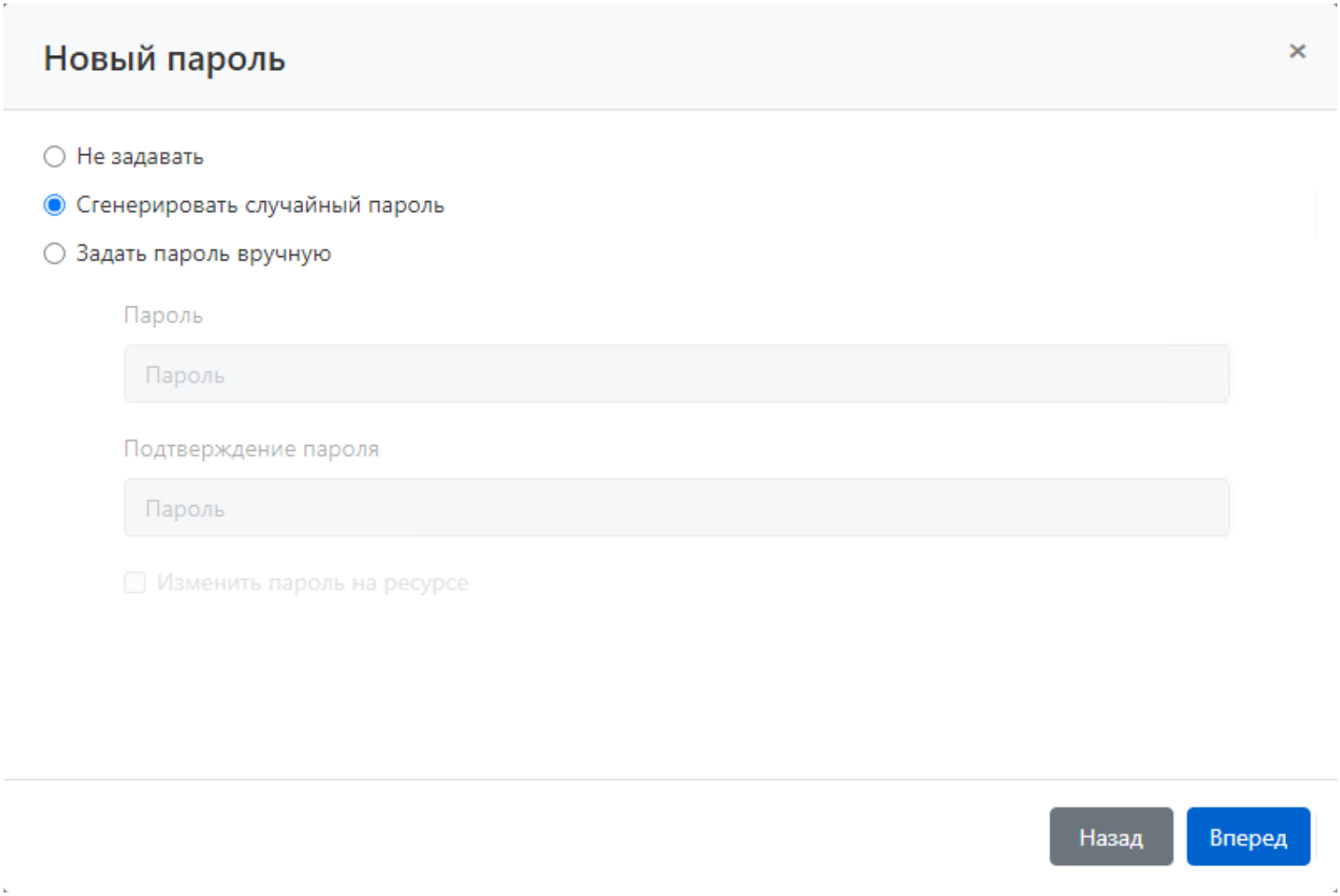
- Нажмите **Добавить учетную запись** в профиле ресурса.
- Введите **Имя учетной записи** и **Описание**.

Пароль и SSH-ключ

Если для ресурса сервисное подключение с типом SSH, то при добавлении учетной записи появится возможность генерации или ручного добавления не только пароля, но и SSH-ключа. Также, для таких учетных записей есть возможность не устанавливать пароль, мастер настройки отобразит дополнительный пункт при настройке пароля — **Не задавать**. Ниже будет рассмотрен пример добавления учетной записи ОС *nix. При добавлении учетных записей ОС Windows и СУБД будет отсутствовать пункт **Не задавать** при настройке пароля, и будет отсутствовать страница для генерации или ручной установки SSH-ключа.

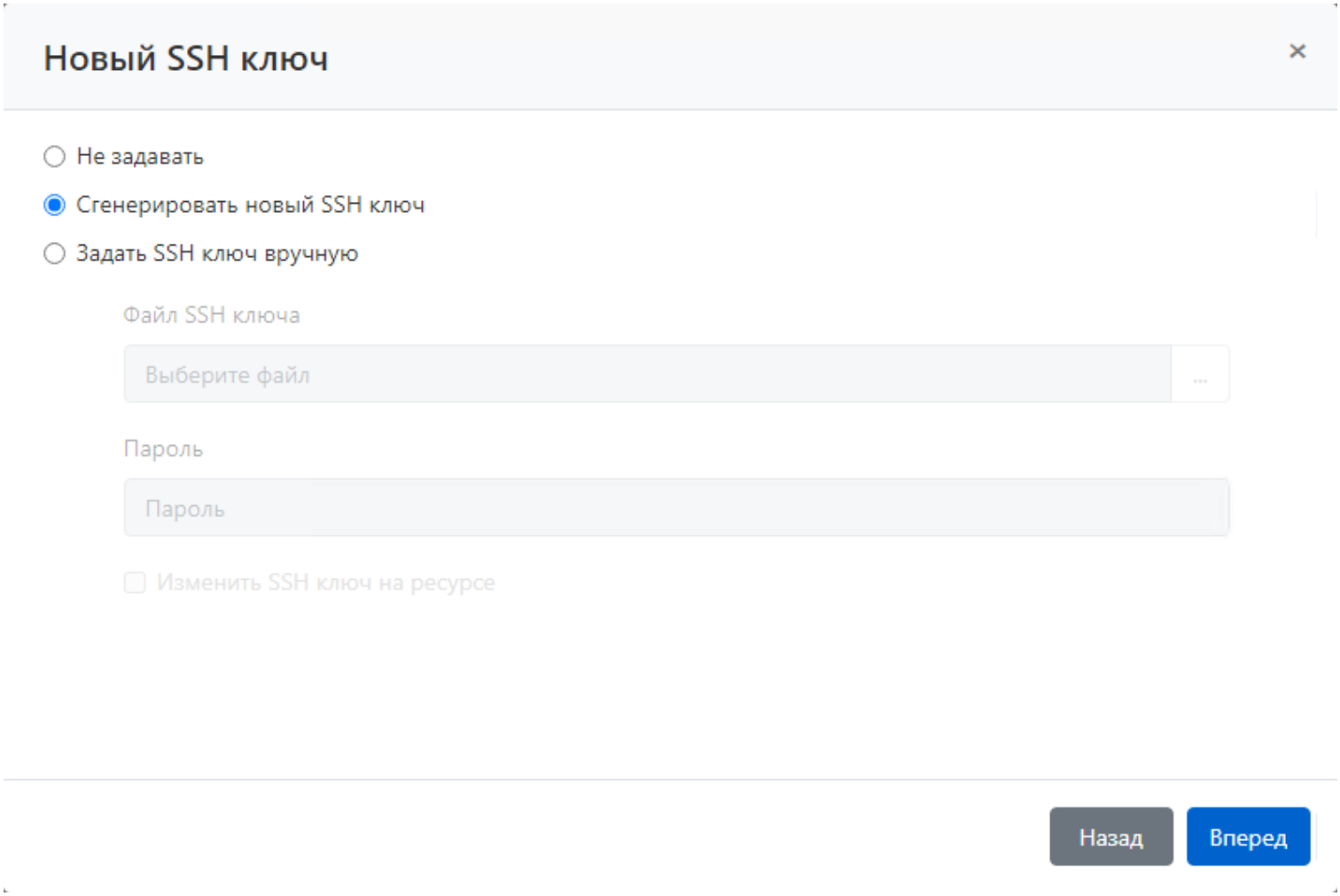
Настройка пароля

- Выберите пункт **Не задавать**, **Сгенерировать случайный пароль** или **Задать пароль вручную**.
- Введите пароль или продолжите выбрав пункт **Не задавать** или **Сгенерировать случайный пароль**.



Настройка SSH-ключа

- Выберите пункт **Не задавать**, **Сгенерировать новый SSH-ключ** или **Задать SSH-ключ вручную**.
- Выберите файл SSH-ключа и введите его пароль или продолжите выбрав пункт **Не задавать** или **Сгенерировать новый SSH-ключ**.
- Завершите добавление учетной записи.



Проверка соединения с ресурсом

Функция позволяет проверить сетевую доступность ресурса, корректность адреса, имени и пароля сервисной учетной записи.

- Нажмите **Проверить соединение** в профиле ресурса.

Синхронизация

Функция позволяет получить корректное имя ресурса, версию ОС или СУБД, локальные учетные записи ресурса и группы безопасности, в которых они состоят. **Синхронизация** доступна только для ресурсов с настроенным сервисным подключением, иначе функция **Синхронизация** будет отсутствовать в профиле ресурса.

- Нажмите **Синхронизировать** в профиле ресурса.

> **ПРИМЕЧАНИЕ**
>
> Учетные записи, которые были добавлены в Indeed PAM при помощи функции **Синхронизировать** будут отмечены символом , для продолжения работы с ними потребуется предоставить системе их пароль, или сбросить его на случайное значение. Подробное описание процесса подтверждения учетных записей описано в статье.

Блокировка

Функция позволяет приостановить действие всех разрешений, в которых используется ресурс.

- Нажмите **Заблокировать** в профиле ресурса.

> **ПРИМЕЧАНИЕ**
>
> Ресурс будет отмечен символом . Все разрешения, в которых ресурс является участником, будут отмечены символом .

Удаление/восстановление ресурса

Удаление ресурса

Перед удалением ресурса необходимо удалить все учетные записи, которые были добавлены из удаляемого ресурса.

> **ПРЕДУПРЕЖДЕНИЕ**
>
> При удалении ресурса все связанные с ним службы также удаляются. Удаленные службы нельзя восстановить.
>
> Удаленные службы перестают отображаться в разделе **Службы**, но их можно просмотреть с помощью расширенного поиска.

1. Откройте профиль ресурса.
2. Нажмите **Удалить**.

Восстановление ресурса

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> При восстановлении ресурса связанные с ним службы не восстанавливаются. Службы потребуется добавить заново. Информацию по удаленным службам можно просмотреть с помощью расширенного поиска в разделе Службы.

1. Нажмите **Расширенный поиск** в разделе **Ресурсы**.
2. Введите **Имя ресурса** или **Адрес (DNS адрес/IP адрес)** полностью или частично.
3. Выберите для поля **Состояние** значение **Удален** и нажмите **Найти**.
4. Откройте профиль ресурса и нажмите **Восстановить**.
5. Введите причину восстановления и нажмите **Восстановить**.

Массовые операции над ресурсами

Настройка сервисного подключения

- В разделе **Ресурсы** отметьте один или несколько ресурсов и нажмите **Настроить сервисное соединение**.

> ⓘ **ПРИМЕЧАНИЕ**
>
> Для выбранных ресурсов будут настроены одинаковые типы сервисных подключений и выбрана одна сервисная учетная запись. В качестве сервисной учетной записи рекомендуется использовать доменную учетную запись, которая имеет права локального администратора на всех выбранных ресурсах.

Проверка соединения с ресурсом

- В разделе **Ресурсы** отметьте один или несколько ресурсов и нажмите **Проверить соединение**.

Удаление ресурсов

- В разделе **Ресурсы** отметьте один или несколько ресурсов и нажмите **Удалить**.

> ⓘ **ПРИМЕЧАНИЕ**
>
> Перед удалением ресурсов необходимо удалить все учетные записи, которые были добавлены из удаляемых ресурсов.

Установить политику

- В разделе **Ресурсы** отметьте один или несколько ресурсов и нажмите **Установить политику**.
- Выберите новую политику для выбранных ресурсов и нажмите **Выбрать**.
- В окне подтверждения нажмите **Установить**.

Установить подразделение

- В разделе **Ресурсы** отметьте один или несколько ресурсов и нажмите **Установить подразделение**.
- Выберите новое подразделение для выбранных ресурсов и нажмите **Ок**.
- В окне подтверждения нажмите **Установить**.

Проверка отпечатков ключей SSH-сервера

Отпечатки ключей SSH-сервера используются для проверки подлинности ресурса в момент подключения к нему. Использование отпечатков помогает защититься от атак вида MITM (Man in the Middle).

Для отпечатков поддерживается только формат SHA256.

Поддерживаемые алгоритмы:

- Ed25519
- ECDSA
- RSA

> ⓘ **ИНФОРМАЦИЯ**
>
> Проверка всегда включена, ее нельзя выключить.
>
> Можно выбрать режим проверки в параметре **Аутентификация ресурсов по ключам SSH-сервера** в разделе **Конфигурация → Системные настройки → Настройки SSH-подключений**.

Предварительные требования

Для работы с отпечатками ключа SSH-сервера нужны привилегии **Управления ресурсами**.

Режимы заполнения отпечатков

Существует три режима заполнения отпечатков ключей SSH-сервера:

- **Автоматически заносить отпечатки ключей в PAM**

  В этом режиме значение отпечатка заносится в PAM без участия администратора. Отпечаток сохраняется в PAM только если он не был до этого задан. Отпечаток сохраняется в момент использования сервисного подключения (проверка соединения, проверка/ротация паролей,

проверка/ротация SSH-ключа, синхронизация) или в момент использования пользовательского подключения (при открытии сессии пользователем). Отпечаток заносится только один раз, после этого только проверяется, то есть он не перезаписывается. Проверка отпечатка происходит всегда.

- **Заносить отпечатки в PAM только вручную**

  В этом режиме сохранение отпечатка в PAM выполняется администратором PAM. Администратор PAM может вручную указать значение отпечатка, предварительно выбрав один из трех доступных алгоритмов или получить готовое значение отпечатка с удаленного хоста. Проверка отпечатка происходит всегда. Если отпечаток не указан, то подключение недоступно.

- **Заносить отпечатки в PAM только вручную и проверять, только если они указаны**

  В этом режиме сохранение отпечатка в PAM выполняется администратором PAM. Администратор PAM может вручную указать значение отпечатка, предварительно выбрав один из трех доступных алгоритмов или получить готовое значение отпечатка с удаленного хоста. Отличие этого режима от предыдущего в том, что если отпечаток не указан, проверка отпечатка выполняться не будет. То есть если отпечаток не указан, подключение к ресурсу все равно доступно.

  Не рекомендуется выбирать этот вариант, т.к. это снижает уровень информационной безопасности.

Выбор ресурсов для добавления отпечатков

1. Откройте раздел **Ресурсы**.
2. Откройте **Расширенный поиск**.
3. Выберите одно из значений в поле **Отпечаток SSH-ключа**:
   - **Не совпадает в СП/ПП**
     Для поиска ресурсов, у которых значение отпечатка в PAM и значение отпечатка на ресурсе не совпадают друг с другом.
   - **Не установлен в СП/ПП**
     Для поиска ресурсов, для которых отпечаток не занесен в PAM.

Добавление отпечатков

Добавлять отпечатки можно тремя способами:

- вручную
- автоматически
- групповой операцией

Добавление отпечатков вручную

Ввести значение отпечатка самостоятельно | **Получить значение отпечатка с ресурса**

Для добавления отпечатка для сервисного подключения выполните следующие действия:

1. Откройте профиль нужного ресурса.
2. Нажмите справа от поля **Сервисное подключение**.
3. В секции **Отпечаток SSH-ключа** выберите **Указать вручную**.
4. Выберите **Алгоритм**. Рекомендуется выбирать Ed25519, потому что это самый безопасный вариант.
5. Введите значение в поле **Отпечаток**.
6. Нажмите **Вперед**.
7. Выберите нужную сервисную учетную запись.
8. Нажмите **Сохранить**.

Для добавления отпечатка для пользовательского подключения выполните следующие действия:

1. Откройте профиль нужного ресурса.
2. Найдите нужное подключение с типом SSH и нажмите **Редактировать**.
3. В секции **Отпечаток SSH-ключа** выберите **Указать вручную**.
4. Выберите **Алгоритм**. Рекомендуется выбирать Ed25519, потому что это самый безопасный вариант.
5. Введите значение в поле **Отпечаток**.
6. Нажмите **Сохранить**.

Добавление отпечатков автоматически

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**

Этот способ работает только если в настройках SSH-подключений выбран режим **Автоматически заносить отпечатки ключей в PAM**.

Отпечатки для сервисного подключения задаются автоматически в момент использования сервисного подключения, например:

- проверка соединения
- проверка или смена пароля или SSH-ключа по расписанию
- синхронизация ресурса

Отпечатки для пользовательского подключения также задаются автоматически в момент использования пользовательского подключения, то есть при открытии сессии пользователем.

ИНФОРМАЦИЯ

В автоматическом режиме отпечатки только заносятся, но не перезаписываются.

Добавление отпечатков групповой операцией

С помощью этой операции можно задать отпечатки для нескольких ресурсов сразу. Для этого выполните следующие действия:

1. Откройте раздел **Ресурсы**.
2. Выберите один или несколько ресурсов, у которых есть сервисное и/или пользовательское подключение с типом SSH и не задан отпечаток ключа.
3. Нажмите **Получить отпечаток с ресурса** и подтвердите действие кнопкой **Вперед**.

ИНФОРМАЦИЯ

С помощью этой операции отпечатки заносятся только если до этого значение отпечатка было не задано, то есть имеющиеся отпечатки не перезаписываются.

Дополнительная информация о работе отпечатков SSH-ключей

- Атрибут **Отпечаток SSH-ключа** привязан не к ресурсу, а к подключению. Поэтому у обоих типов подключений (сервисное и пользовательское) есть свой атрибут для отпечатка SSH-ключа. Это сделано для случаев, когда на удаленном хосте установлено более одного SSH-сервера. Факт наличия или отсутствия отпечатка у одного из подключений не влияет на работу другого. Поэтому значения отпечатков для разных подключений одного и того же ресурса могут содержать разные значения.

- Проверка отпечатка SSH-ключа выполняется до аутентификации на ресурсе, т.е. до передачи учетных данных на ресурс.

- Если в настройках SSH-подключений выбран режим **Заносить отпечатки в PAM только вручную** и атрибут для отпечатка в PAM остался незаполненным, то подключение к ресурсу будет недоступно. В журнале появится событие о неуспешном подключении, на странице ресурса появится предупреждение красного цвета с описанием причины ошибки, перечислением несовпавших отпечатков и указанием типа подключения.

- Если в настройках SSH-подключений выбран режим **Заносить отпечатки в PAM только вручную**, атрибут для отпечатка в PAM заполнен, а на ресурсе отсутствует ключ для указанного алгоритма или отсутствуют любые ключи, то подключение к ресурсу будет недоступно. В журнале появится событие о неуспешном подключении, на странице ресурса появится предупреждение красного цвета с описанием причины ошибки, перечислением несовпавших отпечатков и указанием типа подключения.

- Для устранения ошибки о несовпадении отпечатка и восстановления корректной работы операций требуется заново получить отпечаток SSH-ключа с удаленного хоста, подробнее в пункте Добавление отпечатков.

Службы

Раздел предназначен для работы в PAM со службами Windows.

Службы Windows — это приложения, которые могут запускаться автоматически при запуске операционной системы.

Добавьте в PAM службы, которые запускаются от имени учетных записей, управляемых PAM. Эти службы будут автоматически получать актуальный пароль учетной записи при его смене через PAM.

<details>
<summary>А если не добавить?</summary>

В свойствах службы останется старый пароль учетной записи.

Запущенная служба продолжит работать до ближайшего перезапуска машины ресурса. А после этого служба не запустится, потому что пароль учетной записи, указанный в свойствах службы, не совпадает с реальным паролем учетной записи.

Чтобы запустить службу, понадобится подключиться к ресурсу и обновить пароль в свойствах службы вручную.
</details>

Предварительные требования

Для работы со службами нужны привилегии **Управления ресурсами**, а также требуется настроить сервисное подключение для Windows на ресурсе, на котором располагаются службы.

Добавление служб

1. Откройте раздел **Службы**.
2. Нажмите **Добавить**.
3. В открывшемся окне выберите ресурс. Ресурс должен быть в статусе **Доступен**. У службы будет такое же подразделение, как у выбранного ресурса.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Ресурс невозможно изменить после создания службы.

4. Заполните обязательное поле **Имя** службы.
   Введенное имя должно совпадать с названием службы, которое указано в поле Имя службы (Service name) оснастки Службы на ресурсе.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Не используйте имя, указанное в поле Отображаемое имя (Display name) оснастки Службы на ресурсе.
>
> Не пытайтесь создать вторую службу на том же ресурсе с тем же именем. Дубликаты не разрешены.

5. Введите **Описание** службы. Опционально.
   Введенное описание будет отображаться только в PAM, оно не поменяет описание, отображаемое в свойствах службы на ресурсе.

6. Включите или оставьте выключенной опцию **Перезапускать службу при смене пароля службы**.

> ⓘ **ИНФОРМАЦИЯ**
>
> Для служб с отложенным запуском рекомендуется оставить опцию выключенной. Новый пароль доставится в службу при перезапуске службы.

7. В следующем окне мастера выберите учетную запись.

8. В следующем окне мастера проверьте корректность введенных данных и нажмите **Добавить**.

Аналогично вы можете добавить службу из разделов **Ресурсы** и **Учетные записи**.

Редактирование служб

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Ресурс невозможно изменить, он задается только через мастер добавления службы.

Для редактирования доступны следующие поля службы:

- **Имя службы**
- **Описание**
- **Перезапуск службы**
- **Учетная запись**

Чтобы отредактировать службу, нажмите ✎ в профиле службы справа от нужного параметра.

> ⓘ **ИНФОРМАЦИЯ**
>
> Учитывайте, что на ресурсе не может существовать двух служб с одинаковым именем. Не вводите имя уже существующей на этом ресурсе службы.

Смена паролей служб

У служб нет собственных паролей, их пароли — это пароли связанных учетных записей.

Пароли учетных записей можно менять двумя способами:

- вручную
- по расписанию

Установка пароля в службе

Эта функция позволяет инициировать доставку актуального для связанной учетной записи пароля в службу на ресурсе. Это позволяет синхронизировать пароль в службе сразу, без необходимости ждать смены паролей по расписанию.

> ⓘ **ИНФОРМАЦИЯ**
>
> Если для службы включена опция **Перезапускать службу при смене пароля службы**, то при установке пароля служба перезапустится.

1. Откройте профиль службы.
2. Нажмите **Установить новый пароль в службе**.

Перезапуск служб

Перезапуск службы — это параметр, который задается при создании или редактировании службы с помощью опции **Перезапускать службу при смене пароля службы**. Если опция включена, то при смене или установке пароля служба перезапустится.

Для успешного перезапуска службы на ресурсе служба должна находиться в состоянии Выполняется (Running).

> **ИНФОРМАЦИЯ**
>
> В ситуации, когда служба на ресурсе изначально находилась в состоянии отличном от Выполняется (Running), перезапуска службы не будет. При этом создается событие с типом INFO *Перезапуск службы: Не требуется*. Такой сценарий считается успешным завершением перезапуска службы. Соответственно, он не вызывает новых ошибок и сбрасывает старые.

Если служба находилась в состоянии Выполняется (Running), но при этом возникла ошибка *Не удалось перезапустить службу*, то причина может быть в том, что истек таймаут ожидания нужного статуса. Подробнее в разделе Исправление ошибок в работе служб.

Поиск служб

Поиск позволяет отобразить только те службы, которые удовлетворяют заданному критерию. Есть два вида поиска:

- Быстрый — строка поиска. Можно искать только по одному критерию. Текстовый ввод.
- Расширенный — форма с несколькими полями. Можно искать по нескольким критериям сразу. Выпадающие списки.

Быстрый поиск

В поисковой строке можно искать по следующим полям:

- **Имя службы**;
- **Имя ресурса**;
- **Описание службы**;
- **Имя учетной записи**.

Расширенный поиск

Можно искать по одному или нескольким критериям. При выборе нескольких критериев отобразятся службы, которые удовлетворяют всем перечисленным критериям. Искать можно по следующим полям:

- **Имя службы**;
- **Учетная запись**;
- **Ресурс**;
- **Состояние**;
- Опция **Только службы с ошибками**.

Возможные состояния:

- **Управляется**;
- **Удалена**.

Поиск удаленных служб

1. Откройте раздел **Службы** и нажмите **Расширенный поиск**.
2. Выберите значение **Удалена** для параметра **Состояние**.
3. Нажмите **Поиск**.

Исправление ошибок в работе служб

Ошибки могут возникать:

- при установке пароля в службе;
- при перезапуске службы.

Ошибка при установке пароля в службе может появиться по разным причинам, вот несколько примеров:

- пропало интернет-соединение;
- завис хост, на котором установлен ресурс;
- сервисное подключение перестало работать.

Перезапуск службы заканчивается ошибкой, если истек таймаут ожидания нужного статуса. Например:

- служба слишком долго останавливалась;
- служба перезапустилась и тут же остановилась.

Узнать, какой статус ожидался и какой получили, можно в событиях этой службы. Эта информация поможет понять, как исправить ошибку.

Для исправления ошибки понадобится подключиться к ресурсу. Исправить ошибку из консоли управления не получится.

Удаление служб

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Службу невозможно восстановить после удаления.
>
> Создать новую с таким же именем на том же ресурсе можно.

Удаление из списка служб | **Удаление из профиля службы**

1. Откройте раздел **Службы**.
2. Выберите одну или несколько служб.
3. Нажмите **Удалить**.

Удаленные службы перестают отображаться в разделе **Службы**, но их можно просмотреть с помощью расширенного поиска.

Группы ресурсов

Раздел предназначен для группировки ресурсов с целью быстрой и удобной выдачи разрешений сразу на всю группу, а также просмотра сессий и событий в целом по группе.

Поиск групп ресурсов

Быстрый поиск

Введите в строку поиска **Имя** группы ресурса или **описание** полностью или частично.

Расширенный поиск

Нажмите **Расширенный поиск** и введите один или несколько критериев: **Имя** группы ресурса, **Состояние** или **Подразделение**. Выберите состояние:

- Доступна
- Удалена

Функции групп ресурсов

Редактирование группы

Функция позволяет изменить **Имя** и **Описание** группы

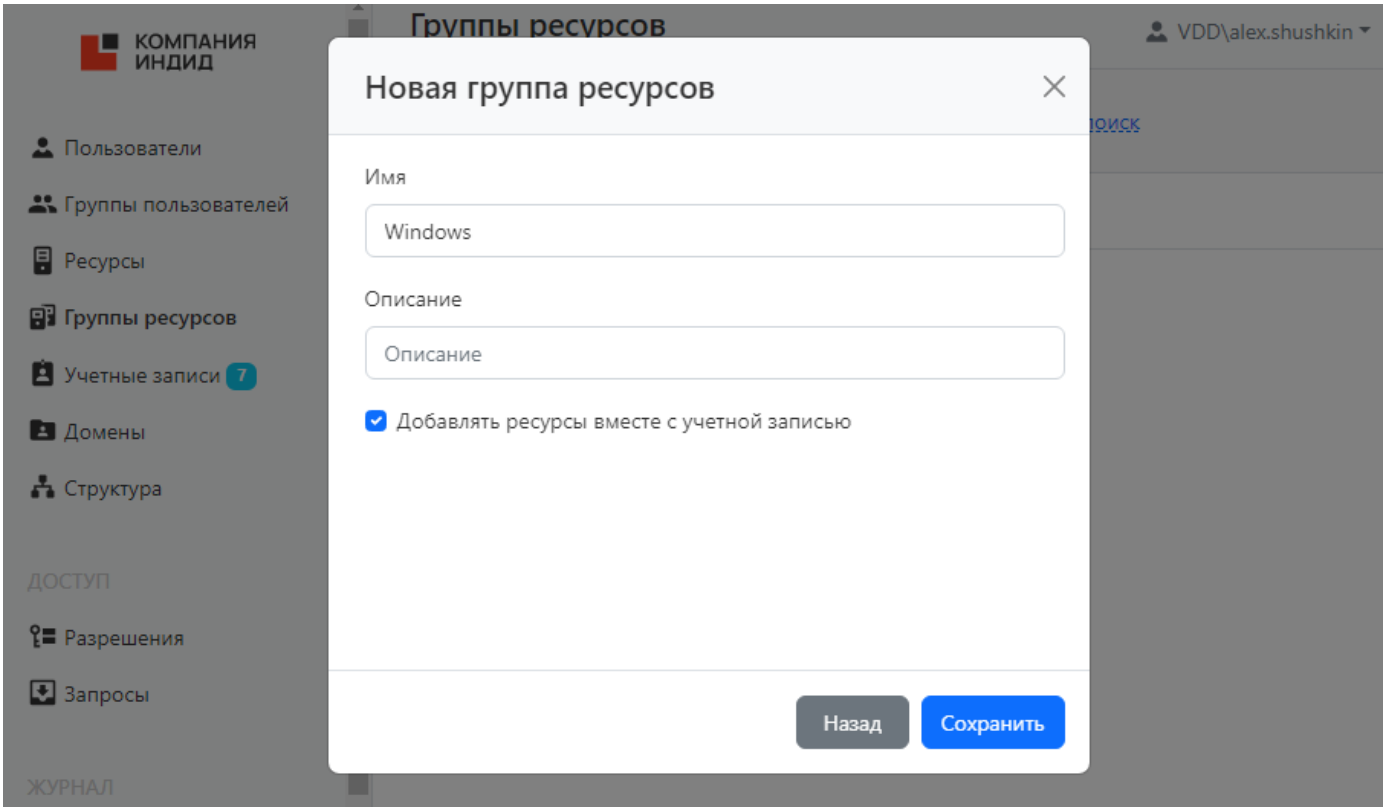
- Нажмите ✎ в профиле ресурса справа от нужного параметра.

Добавление ресурсов

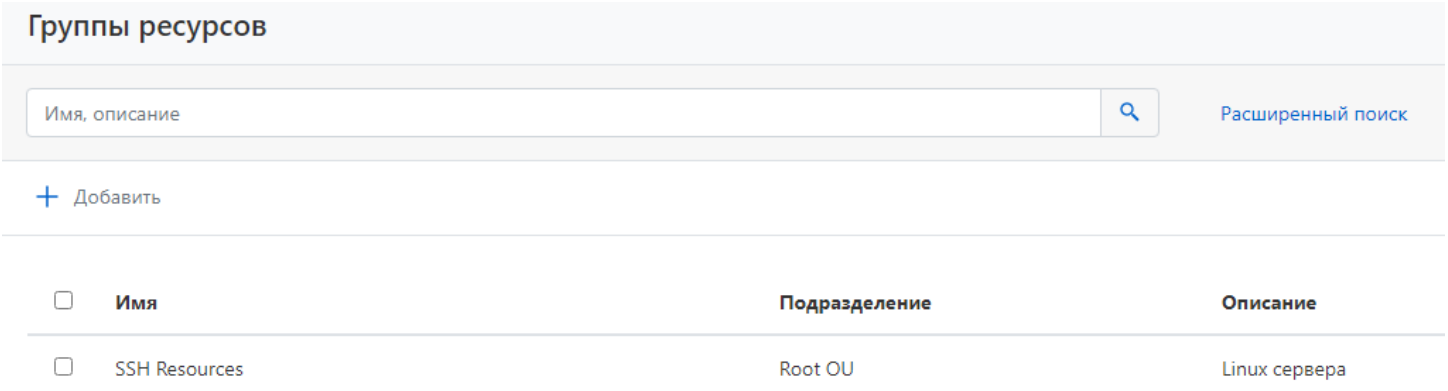
Для работы с группами ресурсов сначала необходимо создать группу и добавить в нее ресурсы.

1. Нажмите **Добавить** в разделе **Группы Ресурсов**.
2. Выберите **Подразделение**.
3. Введите **Имя группы ресурсов**, **Описание**.

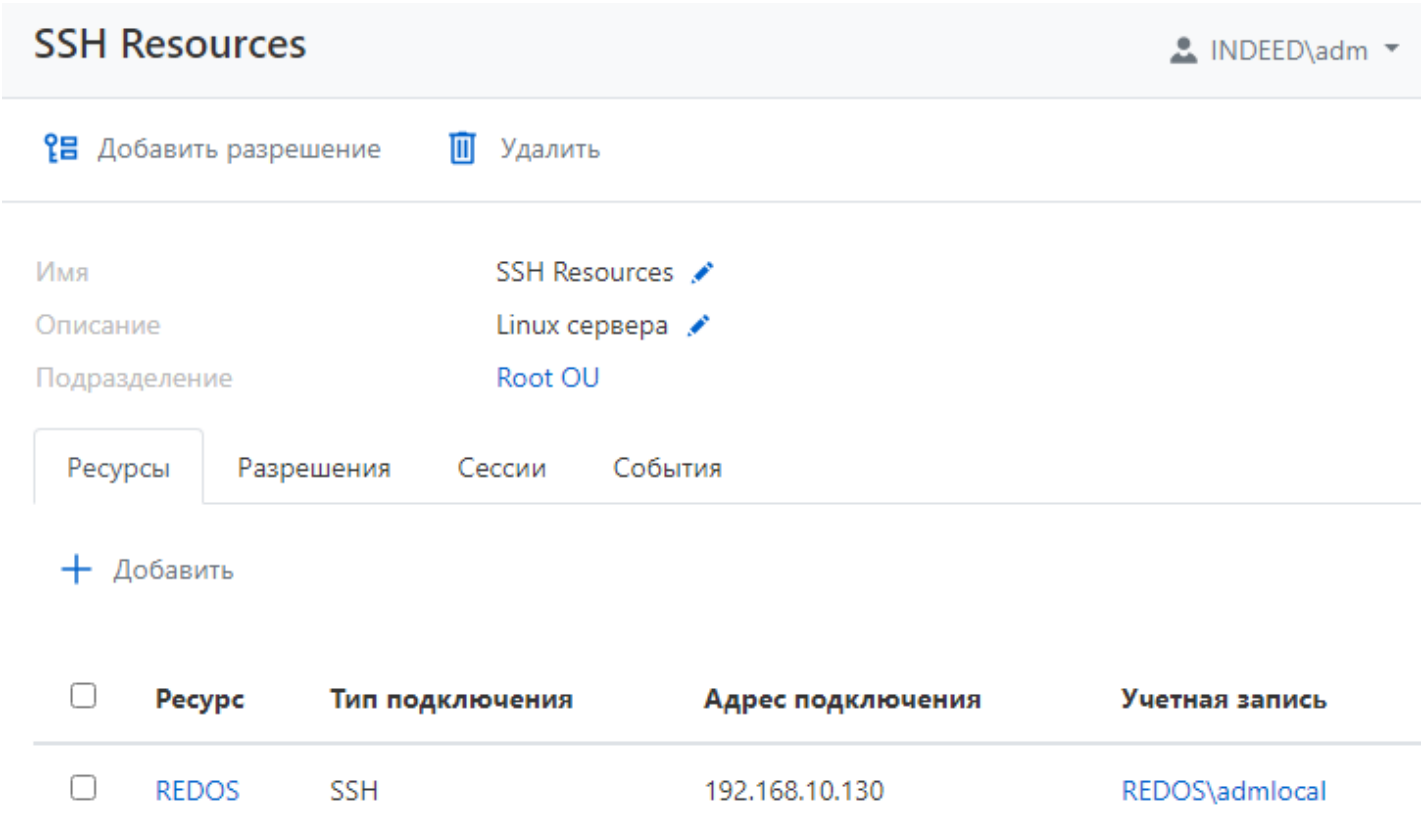
4. Во время добавления ресурса в группу есть параметр **Добавлять ресурсы вместе с учетной записью** от которого зависит способ работы группы ресурсов. Этот параметр влияет на то, как будет выдаваться разрешение на группу ресурсов.
    i. Если отметить этот параметр, то при добавлении каждого отдельного ресурса необходимо будет указать доменную учетную запись для доступа к ресурсам из группы.
    ii. Если не отмечать этот параметр, то при добавлении каждого отдельного ресурса указывать учетную запись будет не надо.



5. Сохраните изменения.



6. Откройте созданную группу ресурсов, во вкладке **Ресурсы** нажмите кнопку **Добавить** и добавьте в группу нужные ресурсы.



Добавление разрешений

Подробное описание работы с разрешениями описано далее, в разделе **Разрешения**.

Для создания нового разрешения нажмите **Добавить разрешение**, выберите пользователя из каталога AD, время действия разрешения, расписание доступа, возможность просмотра учетных данных, укажите источник подключения(если требуется) и повышение привилегий в SSH сессиях(опционально для SSH сессий) и нажмите **Создать**.

Если был отмечен параметр **Добавлять ресурсы вместе с учетной записью,** то разрешение на ресурсы будет выдаваться к каждому ресурсу под отдельно указанной учетной записью. Если этот параметр не был отмечен, то во время выдачи разрешения необходимо будет выбрать, от какой учетной записи будет выдано разрешение на всю группу.

Так как разрешение создается на всю группу, пользователю становятся доступны сразу все ресурсы группы. При изменении состава группы ресурсов у пользователя в рамках разрешения также изменится состав доступных для подключения ресурсов.

Список созданных разрешений можно посмотреть во вкладке **Разрешения**. При нажатии на разрешение откроется его профиль.

Просмотр сессий

Во вкладке **Сессии** отображается список последних сессий с каждым из ресурсов группы. При нажатии на ссылку **Показать все** откроется результат поиска всех сессий по данной группе ресурсов в разделе **Все сессии**.

Просмотр событий

Во вкладке **События** отображаются последние события о данной группе ресурсов. При нажатии на ссылку **Показать все** откроется результат поиска всех событий по данной группе ресурсов в разделе **События**.

Удаление групп ресурсов

В разделе **Группы ресурсов** отметьте одну или несколько групп и нажмите **Удалить**.

Учетные записи

Раздел предназначен для работы с локальными и доменными учетными записями.

Добавление учетной записи

Чтобы добавить учетную запись в PAM, выполните следующие действия:

1. Перейдите в раздел **Учетные записи** и нажмите **Добавить**.
2. Выберите ресурс или домен, в котором будет размещена учетная запись.
3. Введите имя учетной записи и, при необходимости, описание.
4. Задайте пароль. Максимальная длина пароля — 4096 символов.
5. Проверьте данные и сохраните учетную запись.

Поиск учетной записи

Поиск осуществляется в разделе **Учетные записи**.

Быстрый поиск

Введите в строку поиска **Имя учетной записи** полностью или частично.

Расширенный поиск

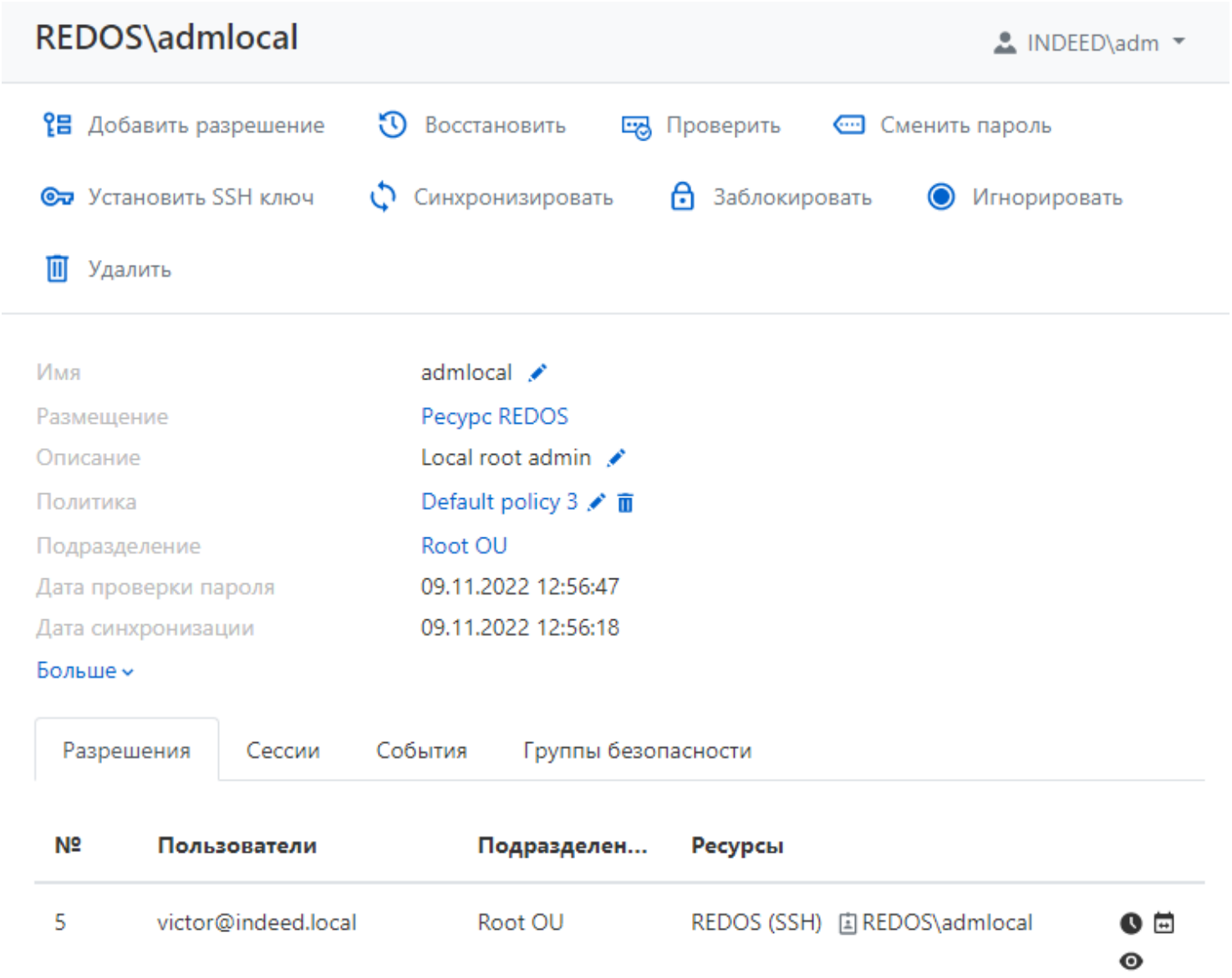
Нажмите **Расширенный поиск** и введите один или несколько критериев, **Имя учетной записи** полностью или частично. Выберите состояние учетной записи:

- Ожидает решения
- Игнорируется
- Управляется
- Заблокирована
- Удалена

Выберите размещение учетной записи:

- **Локальная учетная запись** Для поиска введите **Имя ресурса** или **Адрес (DNS адрес/IP адрес)** полностью или частично.
- **Доменная учетная запись** Для поиска введите **NetBIOS имя домена** или **DNS имя домена** полностью или частично.

Профиль учетной записи



Профиль отображает данные, указанные при добавлении учетной записи:

- **Имя** — имя ресурса, на котором размещена учетная запись доступа и имя учетной записи доступа.
- **Размещение** — имя ресурса или домена где расположена учетная запись доступа.
- **Описание** — произвольный текст.

- **Политика** — набор правил, действующих при открытии сессий от имени учетной записи доступа.
- **Подразделение** — имя подразделения, в котором состоит ресурс.
- **Дата проверки пароля** — дата и время последней проверки пароля учетной записи.
- **Дата проверки SSH ключа** — дата и время последней проверки SSH ключа учетной записи.
- **Дата синхронизации** — дата и время последней синхронизации данных.
- **Дата добавления** — дата и время добавления учетной записи доступа в Indeed PAM.
- **Последнее изменение** — дата и время последнего редактирования учетной записи доступа.
- **Время последней смены пароля** — дата и время изменения пароля в базе Indeed PAM.
- **Время последней смены пароля на ресурсе/в домене** — дата и время изменения пароля в базе Indeed PAM и на ресурсе.
- **Время последней смены SSH ключа** — дата и время изменения SSH ключа в базе Indeed PAM.
- **Время последней смены SSH ключа на ресурсе** — дата и время изменения SSH ключа в базе Indeed PAM и на ресурсе.

Разрешения

Все разрешения, в которых используется учетная запись отображаются на вкладке **Разрешения**. Для каждого разрешения отображаются следующие данные:

- **№** — номер разрешения.
- **Пользователи** — пользователи каталога Active Directory, для которых выдано разрешение.
- **Подразделение** — имя подразделения, в котором состоит ресурс.
- **Учетная запись** — учетная запись, которая используется для открытия RDP, SSH или web-сессии на ресурсах указанных в разрешении.
- **Ресурсы** — ресурсы, на которых может быть открыта RDP, SSH или web-сессия от имени указанной учетной записи.

Сессии

Все активные и завершенные сессии учетной записи отображаются на вкладке **Сессии**. Для каждой сессии отображаются следующие данные:

- **Пользователь** — пользователь каталога Active Directory, который инициировал сессию.
- **Учетная запись** — учетная запись, которая используется для открытия RDP, SSH или web-сессии.
- **Подразделение** — имя подразделения, в котором состоит ресурс.

- **Ресурс** — ресурс, на котором была открыта RDP, SSH или web-сессия от имени учетной записи.
- **Адрес подключения** — фактический адрес, используемый при открытии сессии.
- **Длительность** — длительность сессии.
- **Подключение** — тип удаленного подключения (RDP, SSH, пользовательские типы)
- **Подключение к PAM** — дата и время открытия сессии.
- **Завершение** — дата и время закрытия сессии.
- **Состояние** — отображает текущее состояние сессии (Активная или завершенная).

Для просмотра подробной информации о сессии необходимо нажать на нее. Чтобы вывести все сессии для данной учетной записи, нажмите **Показать все**.

События

Все события учетной записи отображаются на вкладке **События**. Для каждого события отображаются следующие данные:

- **Время создания** — дата и время создания события.
- **Код** — код события.
- **Событие** — описание события.
- **Компонент** — компонент Indeed PAM, который сгенерировал событие.
- **Инициатор** — учетная запись, которая инициировала генерацию события.

Для просмотра подробной информации о событии необходимо раскрыть его. Чтобы вывести все события для данной учетной записи, нажмите **Показать все**.

Группы безопасности

На вкладке **Группы безопасности** отображается перечень групп безопасности, в которых состоит учетная запись.

> ⓘ **ПРИМЕЧАНИЕ**
>
> Для доменных учетных записей не отображаются Built-in группы безопасности.

Службы

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Для локальных учетных записей эта вкладка отображается только если у связанного ресурса есть настроенное сервисное подключение для Windows.

Все добавленные службы отображаются на вкладке **Службы**.

Для каждой службы отображаются следующие данные:

- **Имя службы** — значение, заданное при создании службы. Совпадает со значением поля Имя службы (Service name) оснастки Службы на ресурсе.
- **Учетная запись** — учетная запись, от имени которой запускается служба.
- **Описание** — произвольный текст.

Также на этой вкладке вы можете добавить службу для этой учетной записи, для этого нажмите **Добавить**.

Выбор политики для учетной записи

1. Откройте профиль учетной записи.
2. Нажмите ✒, чтобы добавить или изменить политику.

Операции над учетными записями

Редактирование учетной записи

Чтобы изменить **Имя учетной записи**, **Описание** или **Политику**, нажмите ✎ в профиле учетной записи.

Подтверждение учетной записи

Функция ресурса или домена **Синхронизация** позволяет получать локальные или доменные учетные записи в автоматическом режиме, но для работы с полученными учетными записями требуется подтверждение, так как Indeed PAM не получает их пароли.

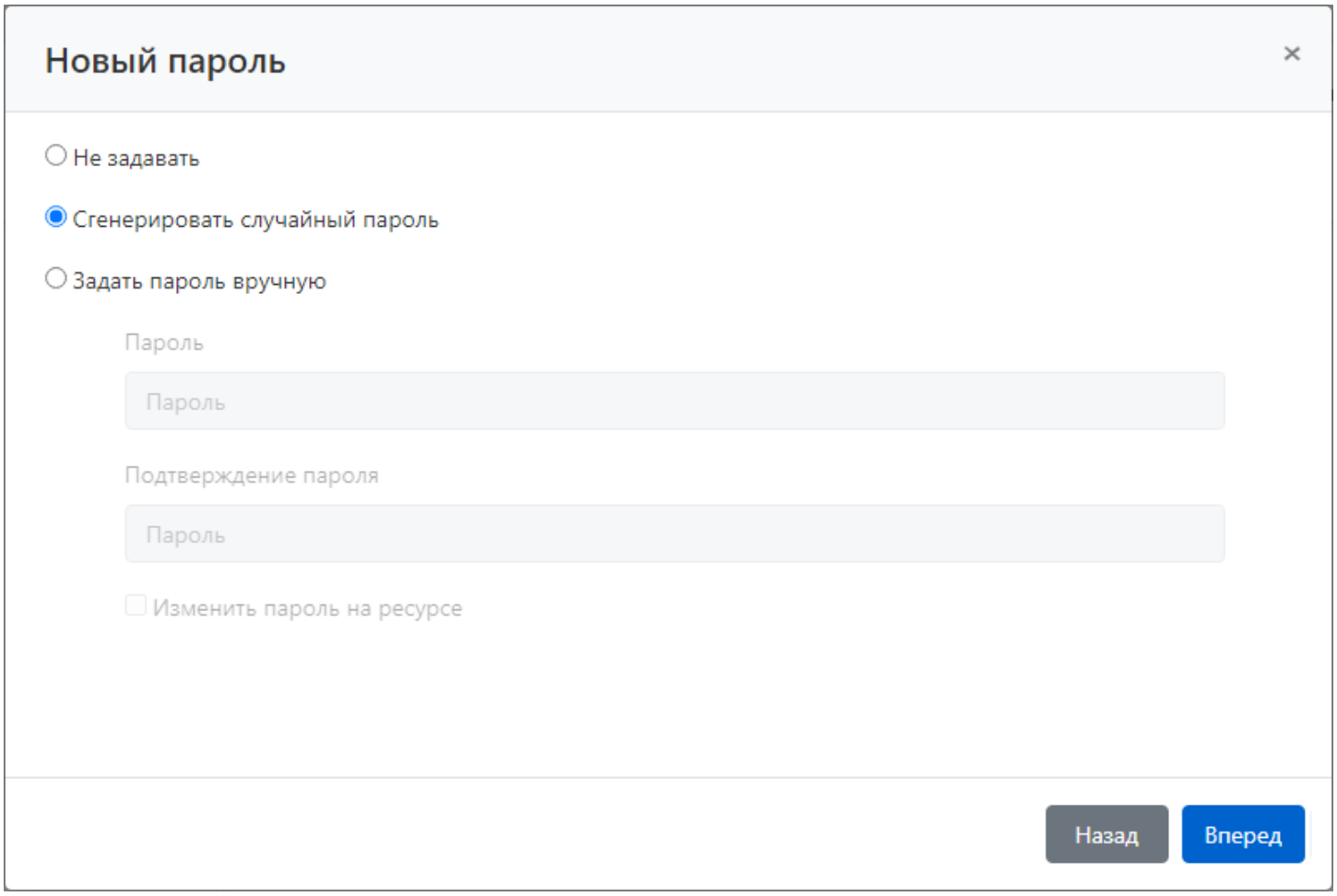
- Нажмите **Сделать управляемой** в профиле учетной записи.

Пароль и SSH-ключ

Если для ресурса, с которого добавлена учетная запись настроено сервисное подключение с типом SSH, то при подтверждении учетной записи появится возможность генерации или ручного добавления не только пароля, но и SSH-ключа. Ниже будет рассмотрен пример подтверждения учетной записи ОС *nix. При подтверждении учетных записей ОС Windows, СУБД или доменных учетных записей будет отсутствовать страница для генерации или ручной установки SSH-ключа.

Настройка пароля

- Выберите пункт **Не задавать**, **Сгенерировать случайный пароль** или **Задать пароль вручную**.
- Введите пароль или продолжите выбрав пункт **Не задавать** или **Сгенерировать случайный пароль**.



Настройка SSH-ключа

- Выберите пункт **Не задавать**, **Сгенерировать новый SSH-ключ** или **Задать SSH-ключ вручную**. Для указания SSH ключа вручную необходим файл с ключом в формате PEM. Если ключ уже был ранее создан, убедитесь что он начинается с указанной строки, иначе ключ необходимо преобразовать в формат RSA:

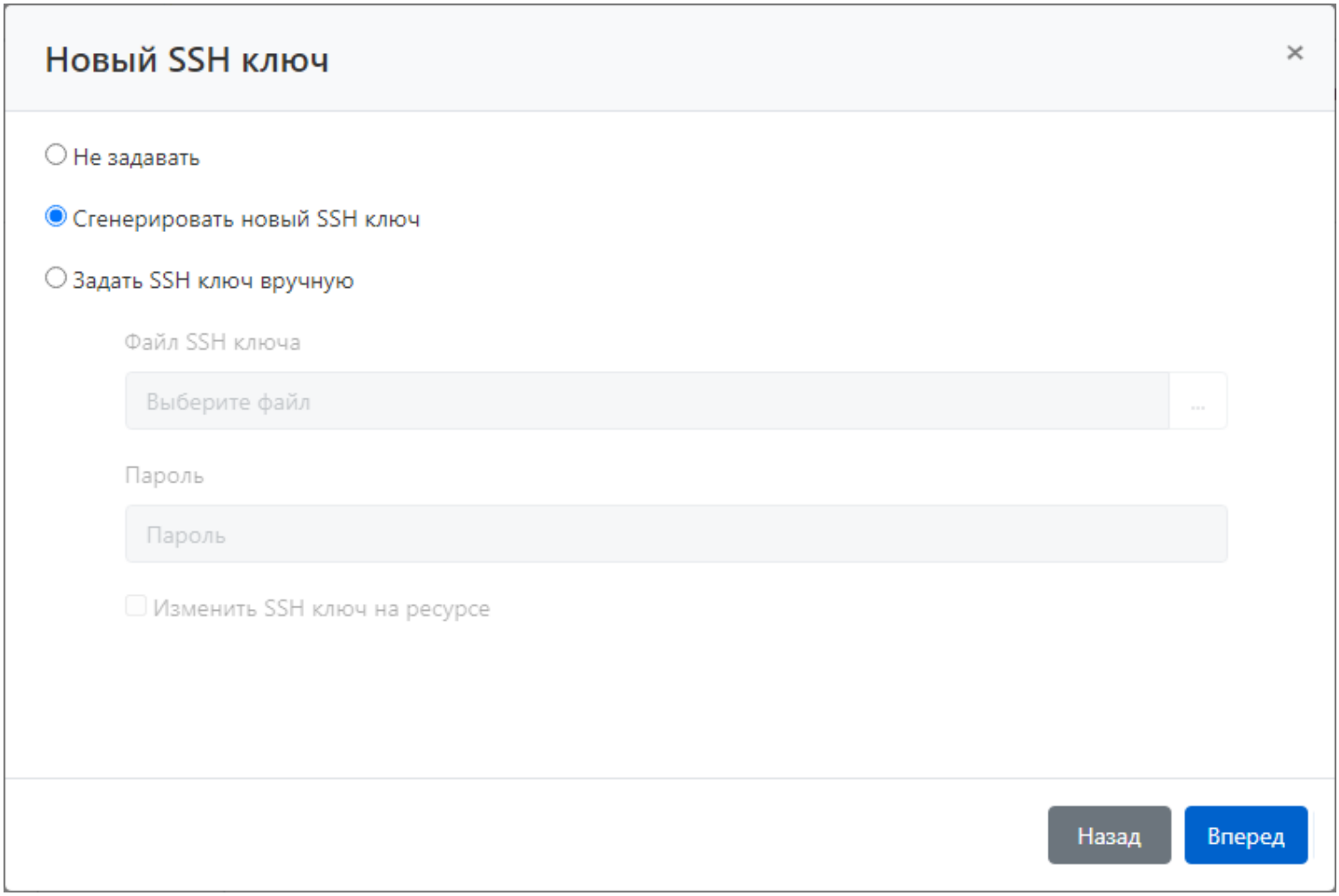
```
-----BEGIN RSA PRIVATE KEY-----
```

При необходимости, для создания нового ключа воспользуйтесь утилитой puttygen, либо одной из команд:

```
ssh-keygen -t rsa -m PEM
```

```
openssl genrsa -des3 -out privatekey.pem
```

- Выберите файл SSH-ключа и введите его пароль или продолжите выбрав пункт **Не задавать** или **Сгенерировать новый SSH-ключ**.

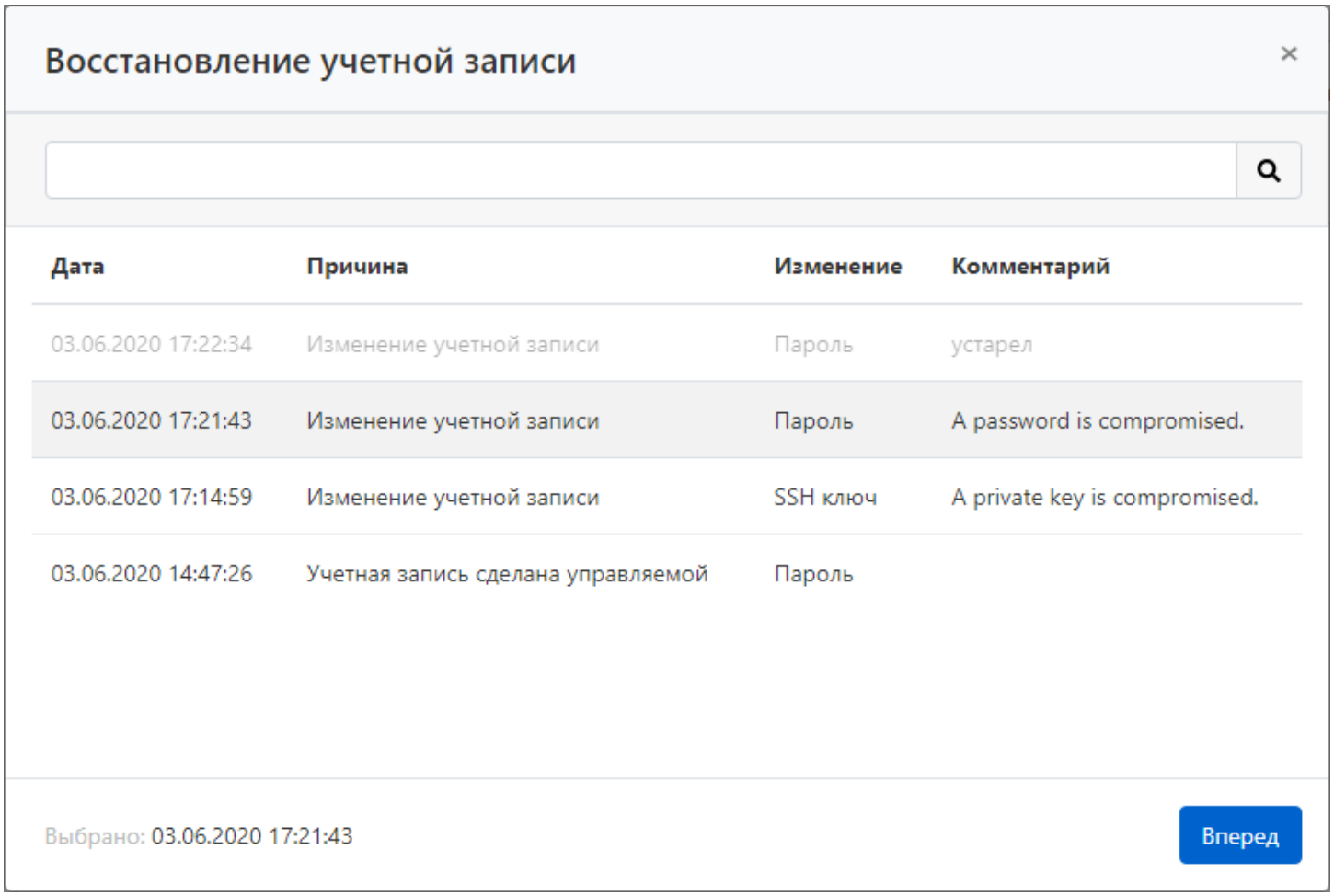


Восстановление пароля или SSH-ключа

Функция позволяет вернуть сохраненное состояние пароля или SSH-ключа для учетной записи.

- Нажмите **Восстановить** в профиле учетной записи.

- Выберите точку восстановления, укажите причину и завершите восстановление пароля.



Проверка пароля или SSH-ключа

Функция позволяет проверить соответствие пароля или SSH-ключа, а также наличие неуправляемых PAM SSH ключей.

- Нажмите **Проверить** в профиле учетной записи.

> **ПРИМЕЧАНИЕ**
>
> Проверка паролей доменных УЗ или локальных УЗ ресурсов под управлением ОС Linux может выполняться без настройки сервисного подключения к ресурсу или домену.

Смена пароля

> **ПРЕДУПРЕЖДЕНИЕ**

> При смене пароля учетной записи обращайте внимание, связаны ли с этой учетной записью службы. При смене пароля учетной записи, пароли связанных служб тоже поменяются.

Функция позволяет сбросить пароль, изменить пароль на случайное значение или ввести новый пароль в ручном режиме.

- Нажмите **Сменить пароль** в профиле учетной записи.
- Выберите пункт **Не задавать**, **Сгенерировать случайный пароль** или **Задать пароль вручную**.
- Введите пароль или продолжите выбрав пункт **Сгенерировать случайный пароль** или **Не задавать**.
- Введите причину смены пароля.
- Завершите смену пароля.

Смена пароля по расписанию

Смена паролей учетных записей по расписанию настраивается через политики.

1. Откройте раздел **Политики**.
2. Выберите политику, которая управляет нужной вам учетной записью.
3. Откройте раздел **Учетные записи**.
4. Включите опцию **Периодически изменять пароль и SSH-ключ учетной записи**.
5. Задайте количество дней в поле **Период изменения пароля и SSH-ключа**. Автоматическое изменение пароля или SSH-ключа будет выполняться один раз в указанное количество дней.

Смена SSH-ключа

Функция позволяет сбросить ключ, изменить ключ на случайное значение или загрузить новый ключ в ручном режиме.

- Нажмите **Сменить SSH-ключ** в профиле учетной записи.
- Выберите пункт **Не задавать**, **Сгенерировать новый SSH-ключ** или **Задать SSH-ключ вручную**.
- Выберите файл SSH-ключа и введите его пароль или продолжите выбрав пункт **Сгенерировать новый SSH-ключ** или **Не задавать**.
- Введите причину смены SSH-ключа.
- Завершите смену SSH-ключа.

Удаление неуправляемых SSH ключей

В случае наличия у УЗ ошибки "Обнаружены неуправляемые SSH ключи" в МС становится доступной кнопка "Удалить неуправляемые ключи". При нажатии удаляются только неуправляемые PAM SSH ключи. Созданные, либо добавленные в PAM SSH ключи остаются без изменений.

Синхронизация

Функция позволяет получить список групп безопасности, в которых состоит учетная запись.

- Нажмите **Синхронизировать** в профиле учетной записи.

Блокировка

Функция позволяет приостановить действие всех разрешений, в которых используется учетная запись.

- Нажмите **Заблокировать** в профиле учетной записи.

> **ПРИМЕЧАНИЕ**
>
> Учетная запись будет отмечена символом . Все разрешения, в которых учетная запись является участником, будут отмечены символом .

Игнорирование

Функция позволяет перевести учетную запись в состояние, в котором она хранится без пароля и не может становиться участником разрешений.

- Нажмите **Игнорировать** в профиле учетной записи.

> **ПРЕДУПРЕЖДЕНИЕ**
>
> Учетная запись будет отмечена символом . Все разрешения, в которых учетная запись является участником, перейдут в состояние *Неактивно*.

Удаление учетной записи

- Нажмите **Удалить** в профиле учетной записи.

> **ИНФОРМАЦИЯ**
>
> При удалении учетная запись пропадет из всех связанных с ней служб, то есть в карточке службы в поле **Учетная запись** будет стоять прочерк. Сами службы не удалятся.

Восстановление учетной записи

- Нажмите **Расширенный поиск** в разделе **Учетные записи**.
- Введите **Имя** учетной записи полностью или частично.
- Выберите для поля **Состояние** значение **Удалена**.
- Выберите ресурс или домен, с котором была добавлена учетная запись.
- Откройте профиль учетной записи и нажмите **Восстановить**.
- Выберите точку восстановления пароля учетной записи.
- Введите причину восстановления и нажмите **Восстановить**.

> **ИНФОРМАЦИЯ**
>
> При восстановлении учетной записи ранее существовавшие связи между учетной записью и службами не восстанавливаются.

Массовые операции над учетными записями

Подтверждение

- В раздел **Учетные записи** отметьте одну или несколько учетных записей и нажмите **Сделать управляемой**.
- Выберите политику сессий и завершите подтверждение.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> При массовом подтверждении всегда генерируются случайные пароли для учетных записей, генерация SSH-ключей не выполняется.

Проверка пароля или SSH-ключа

- В разделе **Учетные записи** отметьте одну или несколько учетных записей и нажмите **Проверить**.

Блокировка

- В раздел **Учетные записи** отметьте одну или несколько учетных записей и нажмите **Заблокировать**.

Игнорирование

- В разделе **Учетные записи** отметьте одну или несколько учетных записей и нажмите **Игнорировать**.

Удаление

- В разделе **Учетные записи** отметьте одну или несколько учетных записей и нажмите **Удалить**.

Домены

Раздел предназначен для работы с доменами Active Directory.

Поиск домена

Поиск осуществляется в разделе **Домены**.

Быстрый поиск

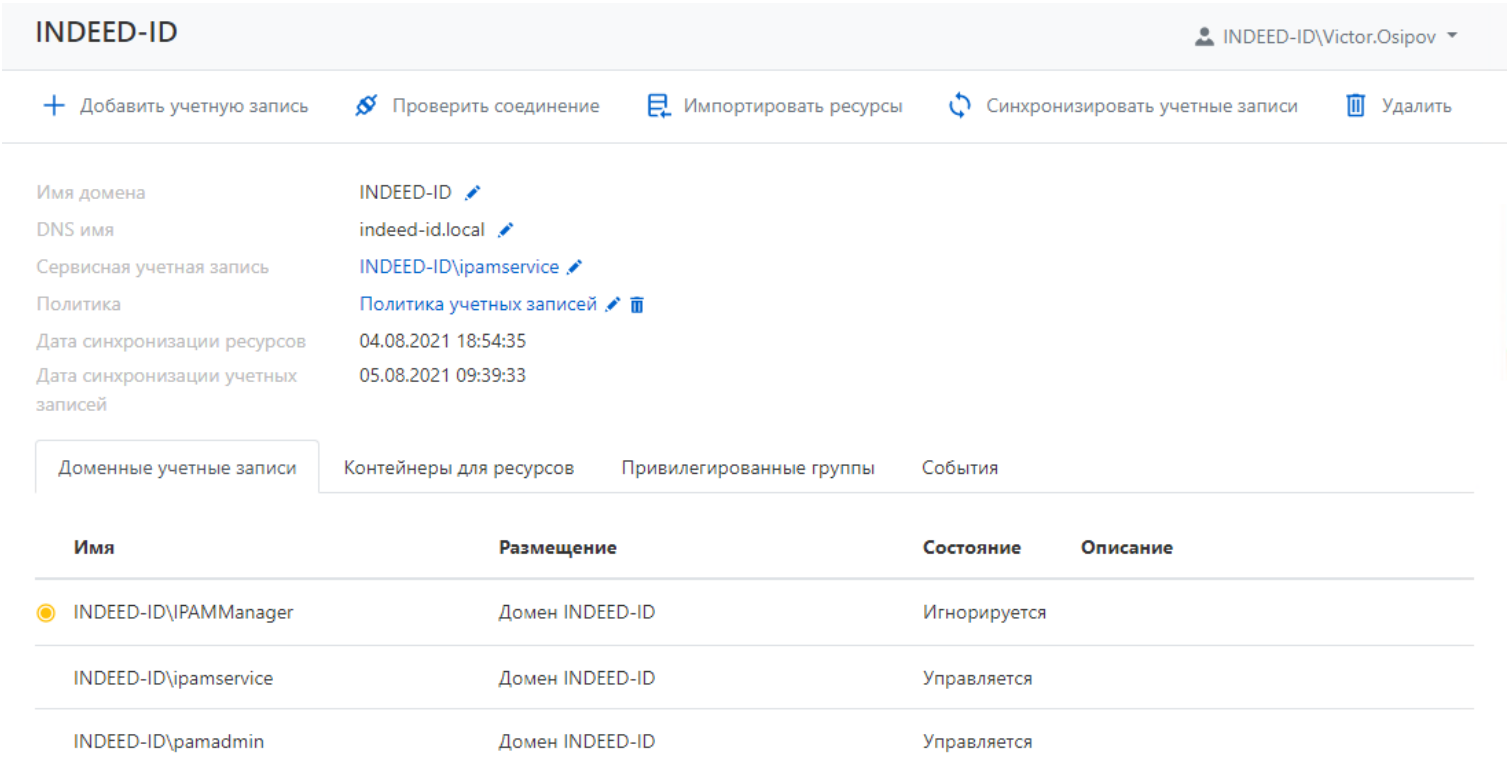
Введите в строку поиска **NetBIOS имя** или **DNS имя** полностью или частично.

Расширенный поиск

Нажмите **Расширенный поиск** и введите один или несколько критериев, **NetBIOS имя** или **DNS имя** полностью или частично. Выберите состояние домена:

- Доступен
- Удален

Профиль домена



Профиль отображает данные, указанные при добавлении:

- **NetBIOS имя**
- **DNS имя**
- **Сервисная учетная запись** — доменная учетная запись, от имени которой будут выполняться сервисные операции.
- **Политика** — набор правил, действующий на доменные учетные записи доступа, добавленные в Indeed PAM.
- **Дата синхронизации ресурсов** — дата и время последней синхронизации ресурсов.
- **Дата синхронизации учетных записей** — дата и время последней синхронизации учетных записей.

Доменные учетные записи

Все добавленные доменные учетные записи отображаются на вкладке **Доменные учетные записи**.

Контейнеры для ресурсов

Все выбранные для синхронизации доменных компьютеров контейнеры отображаются на вкладке **Контейнеры для ресурсов**.

Привилегированные группы

Все выбранные для синхронизации доменных учетных записей группы безопасности отображаются на вкладке **Привилегированные группы**.

События

Все события на ресурсе отображаются на вкладке **События**, здесь отображаются последние 5 событий. Для просмотра подробной информации о событии необходимо раскрыть его. Чтобы вывести все события для данного домена, нажмите кнопку **Показать все**.

Выбор политики для домена

1. Откройте профиль домена.
2. Нажмите , чтобы добавить или изменить политику.

Добавление доменов

Для управления доменными учетными записями доступа и получения доменных компьютеров необходимо добавить домен в Indeed PAM.

- Нажмите **Добавить** в раздел **Домены**.
- Введите **NetBIOS имя** и **DNS имя**.
- Сохраните данные.

Настройка сервисного подключения для доменов

Для доменов Active Directory можно настроить сервисное подключение, которое позволит выполнять операции:

- Проверка соединения с доменом
- Синхронизация доменных учетных записей
- Проверка пароля доменных учетных записей
- Сброс пароля доменных учетных записей
- Синхронизация групп безопасности доменных учетных записей
- Синхронизация доменных компьютеров

> **ПРИМЕЧАНИЕ**
>
> Проверка паролей доменных УЗ может выполняться без настройки сервисного подключения к домену.

Добавление учетных записей

Сервисные операции выполняются от имени сервисной учетной записи, в роли сервисной может быть назначена доменная учетная запись. Перед настройкой сервисного подключения необходимо добавить в систему доменную учетную запись.

- Добавление домена
- Добавление доменных учетных записей

Настройка сервисного подключения

- Откройте профиль домена и нажмите ✎ справа от параметра **Сервисная учетная запись**.
- Введите **Имя учетной записи** полностью или частично.
- Выберите учетную запись и завершите настройку сервисного подключения.

Операции над доменами

Редактирование домена

Функция позволяет изменить **NetBIOS имя**, **DNS имя**, **Сервисную учетную запись** или **Политику**.

- Нажмите справа от нужного параметра в профиле домена.

Добавление учетной записи

Функция позволяет добавлять в Indeed PAM доменные учетные записи ресурса, которые могут использоваться для предоставления доступа на ресурсы.

- Нажмите **Добавить учетную запись** в профиле домена.
- Введите **Имя учетной записи** и **Описание**.

Настройка пароля

- Выберите пункт **Сгенерировать случайный пароль** или **Задать пароль вручную**.
- Введите пароль или продолжите выбрав пункт **Сгенерировать случайный пароль**.

Проверка соединения с доменом

Функция позволяет проверить сетевую доступность домена, корректность NetBIOS имени, адреса, имени и пароля сервисной учетной записи.

- Нажмите **Проверить соединение** в профиле домена.

Импорт ресурсов

Функция позволяет автоматически добавлять в Indeed PAM доменные компьютеры.

Выбор контейнеров

- Перейдите на вкладку **Контейнеры для ресурсов в профиле домена** и нажмите **Добавить**.
- Введите полностью или частично имя контейнера и выберите один или несколько контейнеров.
- Завершите выбор контейнера.

Импорт

- Нажмите **Импортировать ресурсы** в профиле домена.

Синхронизация учетных записей

Функция позволяет автоматически добавлять в Indeed PAM доменные учетные записи, которые состоят в выбранных группах безопасности Active Directory.

Выбор групп привилегированных учетных записей

- Перейдите на вкладку **Привилегированные группы** и нажмите **Добавить**.
- Введите полностью или частично имя группы и выберите одну или несколько групп.
- Завершите выбор групп.

Синхронизация

- Нажмите **Синхронизировать учетные записи** в профиле домена.

Удаление/восстановление домена

Удаление домена

- Нажмите **Удалить** в профиле домена.

> ⓘ **ПРИМЕЧАНИЕ**
>
> Перед удалением домена необходимо удалить все учетные записи, которые были добавлены из удаляемого домена.

Восстановление домена

- Нажмите **Расширенный поиск** в разделе **Домены**.
- Введите **NetBIOS имя** или **DNS имя** полностью или частично.
- Выберите для поля **Состояние** значение **Удален** и нажмите **Найти**.
- Откройте профиль ресурса и нажмите **Восстановить**.
- Введите причину восстановления и нажмите **Восстановить**.

Массовые операции над доменами

Проверка соединения

- В разделе **Домены** отметьте один или несколько доменов и нажмите **Проверить соединение**.

Удаление доменов

- В разделе **Домены** отметьте один или несколько доменов и нажмите **Удалить**.

> ⓘ **ПРИМЕЧАНИЕ**
>
> Перед удалением доменов необходимо удалить все учетные записи, которые были добавлены из удаляемых доменов.

Структура

Раздел предназначен для создания подразделений (Organizational Unit, OU) организации. При создании подразделений можно разграничивать доступ администраторов PAM к отдельным ресурсам.

> **ПРИМЕЧАНИЕ**
>
> Подразделения PAM никак не связаны с подразделениями или контейнерами домена Active Directory.

Виды подразделений

Подразделение может быть глобальным или локальным. Так же и объекты PAM могут быть глобальными и локальными по принадлежности к подразделению.

Сразу после установки PAM в системе уже существует **Глобальное подразделение**. Ему принадлежат все объекты, у которых подразделение не указано явно. Соответственно, после обновления версии PAM на версию 2.7 или выше все ранее существующие объекты становятся **глобальными**.

Привязку администратора PAM к подразделению можно выполнить в настройках Роли. Пользователь может быть в ролях из одного подразделения. Нельзя добавлять пользователя в роль повторно, указывая другие подразделения.

Подразделение указывается при добавлении Ресурса, Домена, Группы ресурсов.

Система распознает является ли данный объект локальным по отношению к данному подразделению через связи объектов с ресурсами и доменами. Если объект связан с Ресурсом и Учетной записью, подразделение определяется по Ресурсу.

Локальный администратор

Локальный администратор ограничен в правах доступа и может работать только с набором объектов, которые принадлежат его подразделению. Ограничиваются только объекты доступа — Учетные записи и Ресурсы.

Исключения:

- может читать **Учетные записи глобальных доменов**
- может читать глобальные политики
- может читать **Домены**, но не их группы и контейнеры

Все создаваемые администратором объекты автоматически принадлежат его подразделению.

> ⓘ **ПРИМЕЧАНИЕ**
>
> Выбирать подразделения при создании объектов может только **Глобальный** администратор.

Локальному администратору недоступны:

- объекты, связанные с другими подразделениями
- разделы **Структура**, **Роли**, **Уведомления**

В разделах Управления доступны только для чтения:

- **Политики** и их настройки
- пользовательские подключения и сервисные подключения
- настройки **Конфигурации**

Остальные разделы недоступны.

Локальный администратор не может создавать разрешения с просмотром учетных данных для доменных **Учетных записей**, в том числе разрешение для **Приложения**.

Включение работы с подразделениями

Работа с подразделениями включается в конфигурационном файле Management Console.

Путь до конфигурационного файла:

Windows	C:\inetpub\wwwroot\mc\assets\config\
Linux	/etc/indeed/indeed-pam/mc/

Чтобы включить работу с подразделениями в PAM, введите значение `true` для параметра `enableOrganizationalUnits` в секции `view`:

```
"view": {
    "enableOrganizationalUnits": true
  }
```

Разрешения

Раздел предназначен для поиска, выдачи, отзыва и приостановки действия разрешений.

Поиск разрешений

Поиск позволяет отобразить только те разрешения, которые удовлетворяют заданному критерию. Есть два вида поиска:

- Быстрый — строка поиска. Можно искать только по одному критерию. Текстовый ввод.
- Расширенный — форма с несколькими полями. Можно искать по нескольким критериям сразу. Выпадающие списки.

Быстрый поиск

В поисковую строку можно вводить одно или несколько слов. Слова можно писать полностью или частично (3 и более букв).

Пример

Чтобы найти разрешение с описанием `Тестовое разрешение главного администратора`, нужно ввести любое из слов: `тест`, `разреш`, `глав`, `адм`.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> По концу слова поиск не работает. Если ввести `решение`, то разрешение не найдется.

Разрешение можно искать по двум словам, например: `тест разреш`, `разреш главн`, `главн адм`.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Слова в поисковом запросе должны идти в том же порядке, что в описании разрешения. Если ввести `разреш тест`, то разрешение не отобразится.
>
> Нельзя вводить слова, между которыми в описании разрешения есть другие слова. Если ввести `тест админ`, то разрешение не отобразится, потому что между `тест` и `админ` есть еще два слова.

Расширенный поиск

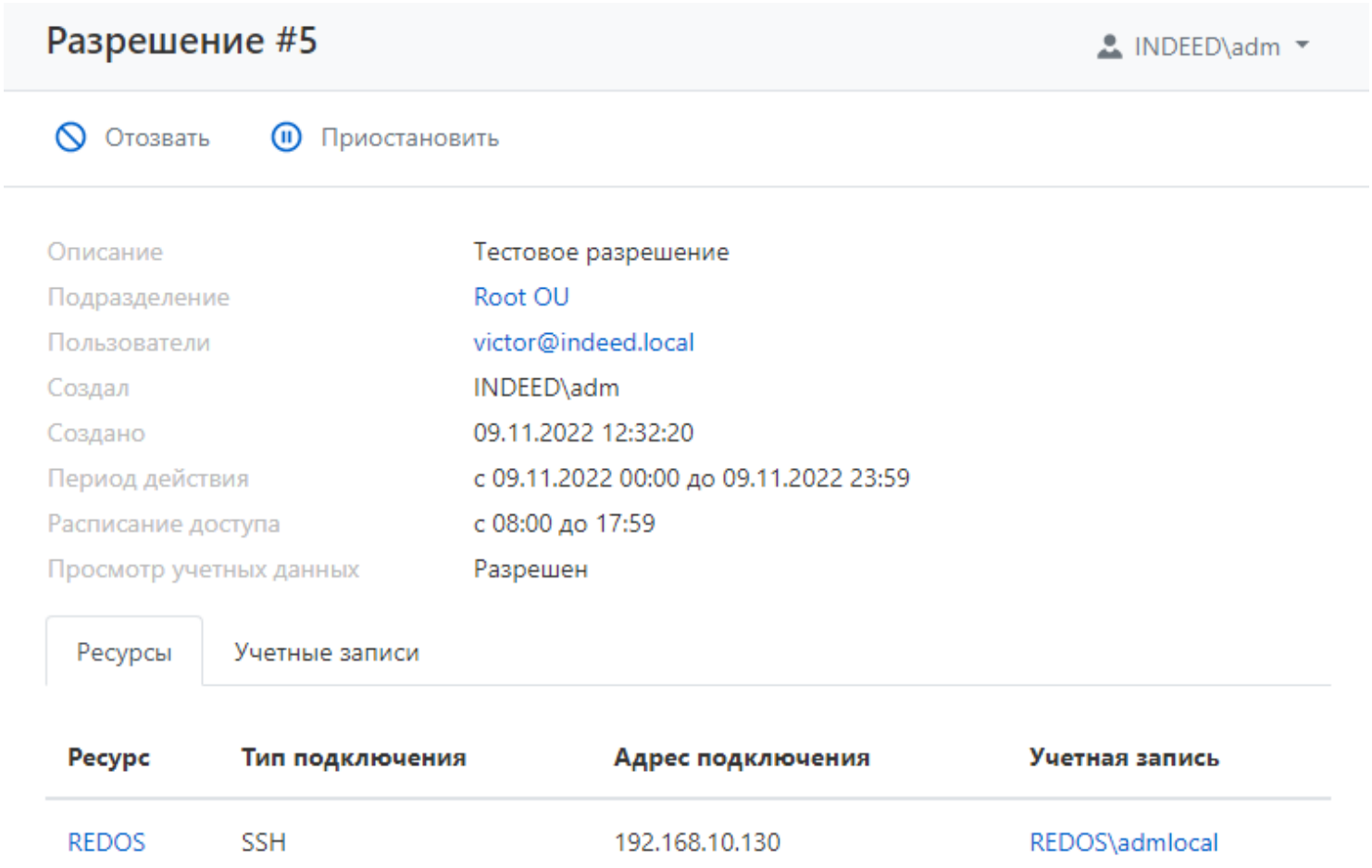
Можно искать по одному или нескольким критериям. При выборе нескольких критериев отобразятся сессии, которые удовлетворяют всем перечисленным критериям.

Пример

Если выбрать в поле **Пользователь** значение `ivan.ivanov@company.demo` и в поле **Состояние** значение `Отозвано`, то отобразятся только отозванные разрешения только этого пользователя.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> В каждом поле можно выбрать только одно значение. Вы не сможете в одном запросе расширенного поиска вывести разрешения пользователей `ivan.ivanov@company.demo` и `peter.ivanov@company.demo`. Вы сможете это сделать с помощью текстового поиска по запросу `ivanov`.

Профиль разрешения



Профиль разрешения отображает следующие данные:

- **Описание** — произвольный текст.
- **Подразделение** — имя подразделения, в котором состоит ресурс.
- **Пользователи** — пользователи каталога Active Directory, для которых выдано разрешение.
- **Создал** — учетная запись администратора Indeed PAM.
- **Создано** — дата и время создания разрешения.
- **Период действия** — даты, в период между которыми разрешение активно.
- **Расписание доступа** — время, в период между которым разрешение активно.
- **Просмотр учетных данных** — разрешение на просмотр пароля или SSH-ключа учетной записи доступа.
- **Ресурс** — имя ресурса, на котором может быть открыта RDP, SSH или web-сессия от имени учетной записи указанной в разрешении.
- **Тип подключения** — тип удаленного подключения (RDP, SSH, пользовательские типы).

- **Адрес подключения** — DNS имя или IP адрес конечного ресурса.
- **Учетная запись** — учетная запись, которая используется для открытия RDP, SSH или web-сессии на ресурсах указанных в разрешении.

Создание разрешений

Разрешения дают право на открытие сессий для пользователей каталога.

Чтобы выдать разрешение:

1. Зайдите в раздел **Разрешения**.
2. Нажмите **Создать**.
3. Выберите Подразделение, Пользователей, Ресурсы, Учетную запись, Ограничения времени и Параметры разрешения в открывшемся визарде.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Для работы с разрешениями необходимы привилегии **Управления разрешениями** (Permission.Create, Permission.Read, Permission.Revoke, Permission.Suspend).

Подразделение

Выберите, в каком подразделении находится ресурс.

> ⓘ **ПРИМЕЧАНИЕ**
>
> Этот раздел визарда не будет отображаться при создании разрешения локальным администратором этого подразделения.

Пользователь

Выберите пользователя или группу пользователей.

Чтобы выбрать пользователя:

1. На вкладке **Пользователи** введите в строке поиска **Имя**, **Фамилию**, **Номер телефона** или **E-mail** полностью или частично. Нажмите ENTER или .
2. Выберите одного или нескольких пользователей.

Чтобы выбрать группу пользователей:

1. На вкладке **Группы пользователей** введите в строке поиска **Имя** или **Описание** полностью или частично. Нажмите ENTER или  .
2. Выберите группу пользователей.

Ресурс

Разрешения можно выдавать на:

- Ресурсы, добавленные в Indeed PAM.
- Группу ресурсов.
- Произвольный ресурс.

Чтобы выбрать ресурс:

1. На вкладке **Ресурсы** введите в строке поиска **Имя ресурса**, **DNS-имя**, **IP-адрес** полностью или частично. Нажмите ENTER или  .
2. Выберите один или несколько ресурсов.

Чтобы выбрать группу ресурсов:

1. На вкладке **Группы ресурсов** введите в строке поиска **Имя** полностью или частично. Нажмите ENTER или  .
2. Выберите группу ресурсов.

Чтобы выбрать произвольный ресурс, на вкладке **Произвольные ресурсы** выберите типы подключений, по которым пользователь сможет подключаться к произвольныи ресурсам. Доступные типы подключений: RDP, SSH, Telnet.

Учетная запись

Для доступа к ресурсу можно использовать локальную, доменную или личную учетную запись пользователя.

> **ПРИМЕЧАНИЕ**

Если вы выбрали больше одного ресурса, то для каждого из них нужно последовательно выбрать учетную запись доступа.

Чтобы выбрать доменную или локальную учетную запись:

1. Введите в строке поиска **Имя учетной записи** полностью или частично. Нажмите ENTER или .
2. Выберите учетную запись.

Чтобы выбрать личную учетную запись, нажмите **Продолжить с пользовательской УЗ**.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Для произвольных ресурсов недоступен выбор локальной учетной записи.
>
> Для произвольных ресурсов учетная запись одна на все типы подключений.

Ограничения времени

Параметры этого раздела опциональные.

Для разрешения можно задать период действия — дату и время начала, дату и время окончания. Для этого:

1. Включите опции **Начало** и **Окончание**.
2. Выберите дату и время.

> ⓘ **ПРИМЕЧАНИЕ**
>
> Если опции **Начало** и **Окончание** не выбраны, то разрешение будет действовать бессрочно.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> По истечении периода действия разрешения сессия будет прервана.

Можно также задать расписание доступа к ресурсу по этому разрешению. В этом случае подключение будет доступно только в указанные часы. Например, только в рабочее время.

1. Включите опцию **Разрешить доступ только**.
2. Введите время **С** и **До**.

> ⓘ **ПРИМЕЧАНИЕ**
>
> Если опция **Разрешить доступ только** не выбрана, то разрешение будет действовать круглосуточно.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> По истечении времени, установленного в расписании доступа, сессия будет прервана.

Параметры разрешения

Параметры этого раздела опциональные.

Учетные данные

Indeed PAM позволяет задать, разрешено ли пользователю просматривать пароль привилегированных учетных записей, которые используются в его разрешениях. Чтобы разрешить, включите опцию **Разрешить просмотр учетных данных**.

Indeed PAM позволяет задать, разрешено ли пользователю изменять пароль привилегированных учетных записей, которые используются в его разрешениях. Чтобы разрешить, включите опцию **Разрешить изменение учетных данных**.

Источник подключения

Indeed PAM позволяет установить ограничение для подключений к ресурсам, а именно — установить конкретную сеть, из которой можно подключаться. Чтобы это сделать, выберите нужную сеть в поле **Сетевое расположение источников для разрешенных подключений**.

> ⓘ **ПРИМЕЧАНИЕ**
>
> Если не были добавлены никакие Сетевые расположения, то в выпадающем списке будет единственная настройка — Без ограничений. Это значит, что использовать данное разрешение можно с любого устройства в сети.

Повышение привилегий в SSH сессиях

Indeed PAM позволяет указать для каждого разрешения, будет ли в этом разрешении доступ к pamsu.

Возможные варианты:

- **Управляется политиками** — будет ли доступ к pamsu определяется политикой ресурса, на который выдается разрешение.
- **Разрешено** — будет доступ к pamsu независимо от настроек политики.
- **Запрещено** — не будет доступа к pamsu независимо от настроек политики.

Операции над разрешениями

Копирование

С помощью этой функции можно создать разрешение на основе ранее созданного разрешения. Состояние исходного разрешения может быть любым, в том числе отозванным и приостановленным.

Копирование схоже с процессом создания разрешения. При копировании открывается такой же мастер, в котором уже выбраны объекты из исходного разрешения. Этот выбор можно отредактировать — добавить недостающие объекты или убрать лишние.

> ⓘ **ИНФОРМАЦИЯ**
>
> Эта функция доступна только из профиля разрешения.

1. Откройте профиль разрешения.
2. Нажмите **Создать копию**.
3. Если требуется, внесите изменения в список выбранных объектов на страницах открывшегося мастера.

   Чтобы просмотреть список выбранных объектов, нажмите 🔍.

   > ⓘ **ИНФОРМАЦИЯ**
   >
   > Если какой-либо пользователь, ресурс или учетная запись, указанные в исходном разрешении, удалены или заблокированы, то они не будут выбраны.

4. Если требуется, внесите изменения в **Ограничения времени** и **Параметры разрешения**.
5. Выберите **Действие с исходным разрешением** — **Оставить**, **Приостановить** или **Отозвать**.

Отзыв

С помощью этой функции можно аннулировать разрешения, которые больше не требуются.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Отозванные разрешения нельзя восстановить.
>
> Если вам требуется временно запретить использовать разрешение, то приостановите его действие.

При отзыве разрешения учитывайте, что доступ у пользователей пропадет сразу, а не после того, как они сами отключились от ресурса.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> При отзыве разрешения сессия будет прервана.

Отзыв из списка разрешений | **Отзыв из профиля разрешения**

1. Откройте раздел **Разрешения**.
2. Отметьте нужное разрешение.
3. Нажмите **Отозвать**.

Отозванные разрешения перестают отображаться в разделе **Разрешения**, но их можно просмотреть с помощью поиска. Для этого откройте расширенный поиск в разделе **Разрешения** и выберите значение **Отозвано** для параметра **Состояние**.

Приостановка

С помощью этой функции можно временно запретить использовать разрешение.

Учитывайте, что доступ у пользователей пропадет сразу, а не после того, как они сами отключились от ресурса.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> При приостановке действия разрешения сессия будет прервана.

Приостановка из списка разрешений | **Приостановка из профиля разрешения**

1. Откройте раздел **Разрешения**.
2. Отметьте нужное разрешение.
3. Нажмите **Приостановить**.

Возобновление

С помощью этой функции можно активировать приостановленное разрешение, то есть вернуть его в состояние **Действительно**.

Возобновление из списка разрешений | **Возобновление из профиля разрешения**

1. Откройте раздел **Разрешения**.
2. Отметьте нужное разрешение.
3. Нажмите **Возобновить**.

Массовые операции над разрешениями

Отзыв

С помощью этой функции можно аннулировать разрешения, которые больше не требуются.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Отозванные разрешения нельзя восстановить.
>
> Если вам требуется временно запретить использовать разрешение, то приостановите его действие.

При отзыве разрешения учитывайте, что доступ у пользователей пропадет сразу, а не после того, как они сами отключились от ресурса.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> При отзыве разрешения сессия будет прервана.

Чтобы воспользоваться функцией, выполните следующие действия:

1. Откройте раздел **Разрешения**.
2. Отметьте одно или несколько разрешений.
3. Нажмите **Отозвать**.

Отозванные разрешения перестают отображаться в разделе **Разрешения**, но их можно просмотреть с помощью поиска. Для этого откройте расширенный поиск в разделе **Разрешения** и выберите значение **Отозвано** для параметра **Состояние**.

Приостановка

С помощью этой функции можно временно запретить использовать разрешение.

Учитывайте, что доступ у пользователей пропадет сразу, а не после того, как они сами отключились от ресурса.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> При приостановке действия разрешения сессия будет прервана.

Чтобы воспользоваться функцией, выполните следующие действия:

1. Откройте раздел **Разрешения**.
2. Отметьте одно или несколько разрешений.
3. Нажмите **Приостановить**.

Возобновление

С помощью этой функции можно активировать приостановленное разрешение, то есть вернуть его в состояние **Действительно**.

Чтобы воспользоваться функцией, выполните следующие действия:

1. Откройте раздел **Разрешения**.
2. Отметьте одно или несколько разрешений.
3. Нажмите **Возобновить**.

Запросы сессий

Раздел предназначен для работы с запросами на открытие сессий к соответствующим ресурсам. Данный механизм позволяет настроить дополнительное подтверждение вторым лицом (Администратором PAM) для подключения к конечному ресурсу.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Для работы необходима привилегия **Подтверждение сессий** (SessionRequest.Confirm).

> **ПОДСКАЗКА**
>
> Время ожидания запроса настраивается в Политике сессии. Время ожидания запроса на просмотр пароля и SSH-ключа настраивается в разделе Политика учетной записи.

В запросах сессий всегда отображаются исторические значения **Пользователя**, **Ресурса** и **Учетной записи** на момент создания запроса. Исторические имена в **Запросах** и **Сессиях** могут отличаться, т.к. при открытии сессии сохраняется актуальное значение **Пользователя**, **Ресурса**, **Учетной записи**.

Поиск запросов

> **ПРИМЕЧАНИЕ**
>
> Поиск **Запросов** по **Пользователю** находит **Запросы** пользователей, запрашивающих **Сессии**.
>
> По **Администратору**, который подтверждает **Запросы**, поиска нет.

Быстрый поиск

Введите в строку поиска **Пользователя**, **Учетную запись** или **Ресурс** полностью или частично.

Расширенный поиск

Нажмите **Расширенный поиск** и введите один или несколько критериев – **Номер запроса**, **промежуток времени создания**, **Учетную запись**, **Ресурс**, **Группу ресурсов**, **Пользователя** или **Подразделение**.

Выберите состояние запроса:

- Ожидает решения
- Подтвержден
- Отклонен
- Истек
- Отменен пользователем
- Использован
- Не использован

Выберите тип запроса:

- Сессия
- Учетные данные

Функции Запросов

Подтверждение запроса

Функция позволяет Администратору PAM подтвердить запрос Пользователя на подключение к конечному ресурсу.

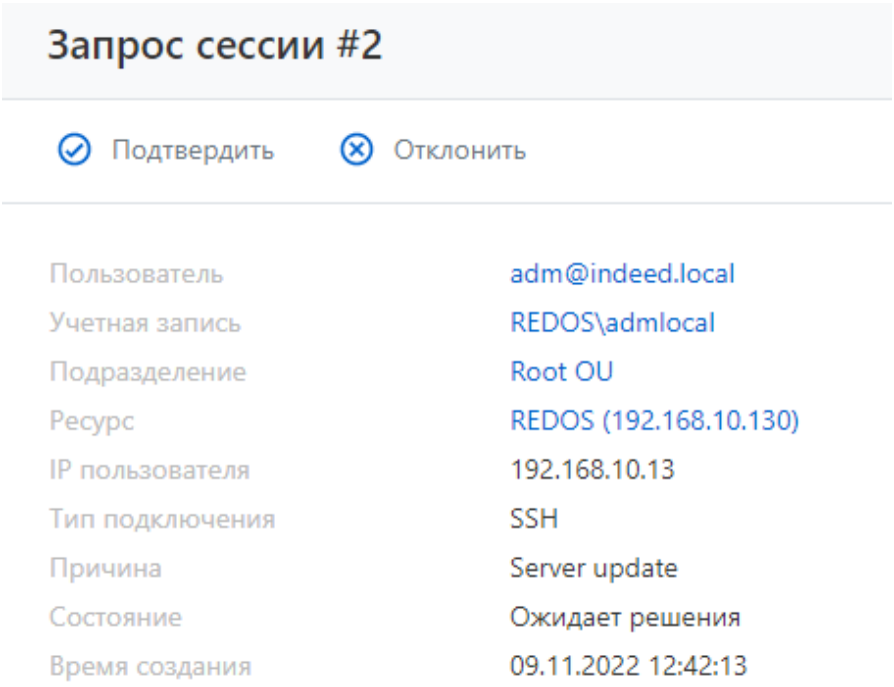
- Нажмите **Подтвердить** в профиле запроса, либо, выделив флажком ожидающие решения запросы.

Отклонение запроса

Функция позволяет Администратору PAM отклонить запрос Пользователя.

- Нажмите **Отклонить** в профиле запроса, либо, выделив флажком ожидающие решения запросы.

Профиль запроса



Профиль запроса отображает следующие данные:

- **Пользователь** — пользователь каталога Active Directory, создавший запрос на открытие сессии.
- **Учетная запись** — учетная запись, которая используется для открытия RDP, SSH или web-сессии на ресурсах указанных в разрешении.
- **Подразделение** — имя подразделения, в котором состоит ресурс.
- **Ресурс** — ресурсы, на которых может быть открыта RDP, SSH или web-сессия от имени учетной записи указанной в разрешении.
- **IP пользователя** — IP-адрес, с которого пользователь подключается к PAM Gateway, SSH proxy или RDP Proxy.
- **Тип подключения** — тип удаленного подключения (RDP, SSH, пользовательские типы).
- **Причина** — произвольный текст, введенный пользователем при создании запроса.
- **Состояние** — текущее состояние запроса (Ожидает решения, Подтвержден, Отклонен, Истек, Отменен пользователем, Использован, Не использован).
- **Время создания** — дата и время создания запроса пользователем.

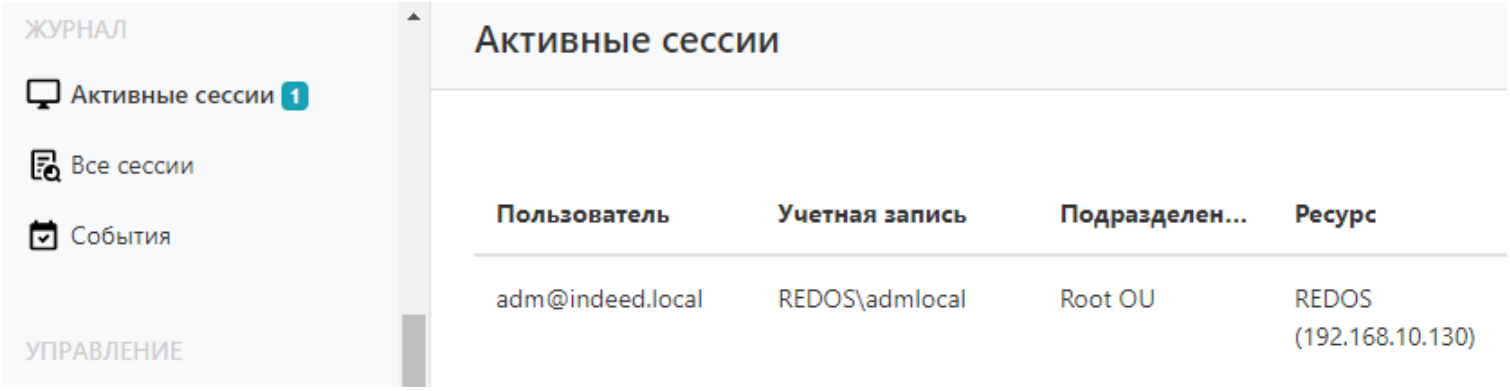
Активные сессии

Раздел предназначен для автоматической фильтрации и отображения активных сессий Indeed PAM.

Для каждой сессии отображаются следующие данные:

- **Пользователь** — пользователь каталога Active Directory, который инициировал сессию.
- **Учетная запись** — учетная запись, которая используется для открытия RDP, SSH или web-сессии.
- **Подразделение** — имя подразделения, в котором состоит ресурс.
- **Ресурс** — ресурс, на котором была открыта RDP, SSH или web-сессия от имени учетной записи.
- **Адрес подключения** — фактический адрес, используемый при открытии сессии.
- **Длительность** — длительность сессии.
- **Подключение** — тип удаленного подключения (RDP, SSH, пользовательские типы)
- **Подключение к PAM** — дата и время открытия сессии.

При наличии активных сессий на главном сайдбаре справа от заголовка раздела будет отображаться бейдж с количеством активных сессий:



Все сессии

Раздел предназначен для поиска и просмотра активных, завершенных и прерванных сессий.

По умолчанию на странице отображается 15 сессий.

> ⓘ **ИНФОРМАЦИЯ**
>
> Отображаемое по умолчанию количество сессий на странице можно изменить в конфигурационном файле.

Внизу страницы расположен пагинатор для просмотра остальных сессий.

Рядом с пагинатором находится переключатель **Показывать по: 15 30 60 100**, чтобы видеть больше строк на одной странице и не переключаться между страницами слишком часто.

Если элементов меньше 15, то они помещаются на одну страницу. В этом случае переключатель **Показывать по** (и сам пагинатор) не отображаются.

Поиск сессий

Поиск позволяет отобразить только те сессии, которые удовлетворяют заданному критерию. Есть два вида поиска:

- Быстрый — строка поиска. Можно искать только по одному критерию. Текстовый ввод.
- Расширенный — форма с несколькими полями. Можно искать по нескольким критериям сразу. Выпадающие списки.

Быстрый поиск

В поисковую строку можно вводить одно или несколько слов. Слова можно писать полностью или частично (3 и более букв).

Пример

Чтобы найти сессию с причиной открытия `Обновление программы, согласовано директором`, нужно ввести любое из слов: `обнов`, `прог`, `согл`, `дир`.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> По концу слова поиск не работает. Если ввести `новление`, то сессия не найдется.

Сессию можно искать по двум словам, например: `обнов прог`, `прогр согл`, `согл дир`.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Слова в поисковом запросе должны идти в том же порядке, что в причине открытия. Если ввести `прог обнов`, то сессия не отобразится.
>
> Нельзя вводить слова, между которыми в причине открытия есть другие слова. Если ввести `обнов дир`, то сессия не отобразится, потому что между `обнов` и `дир` есть еще два слова.

Расширенный поиск

Можно искать по одному или нескольким критериям. При выборе нескольких критериев отобразятся сессии, которые удовлетворяют всем перечисленным критериям.

Пример

Если выбрать в поле **Пользователь** значение `ivan.ivanov@company.demo` и в поле **Тип подключения** значение `SSH`, то отобразятся сессии только этого пользователя только с этим типом подключения.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> В каждом поле можно выбрать только одно значение. Вы не сможете в одном запросе расширенного поиска вывести сессии пользователей `ivan.ivanov@company.demo` и `peter.ivanov@company.demo`. Вы сможете это сделать с помощью текстового поиска по запросу `ivanov`.

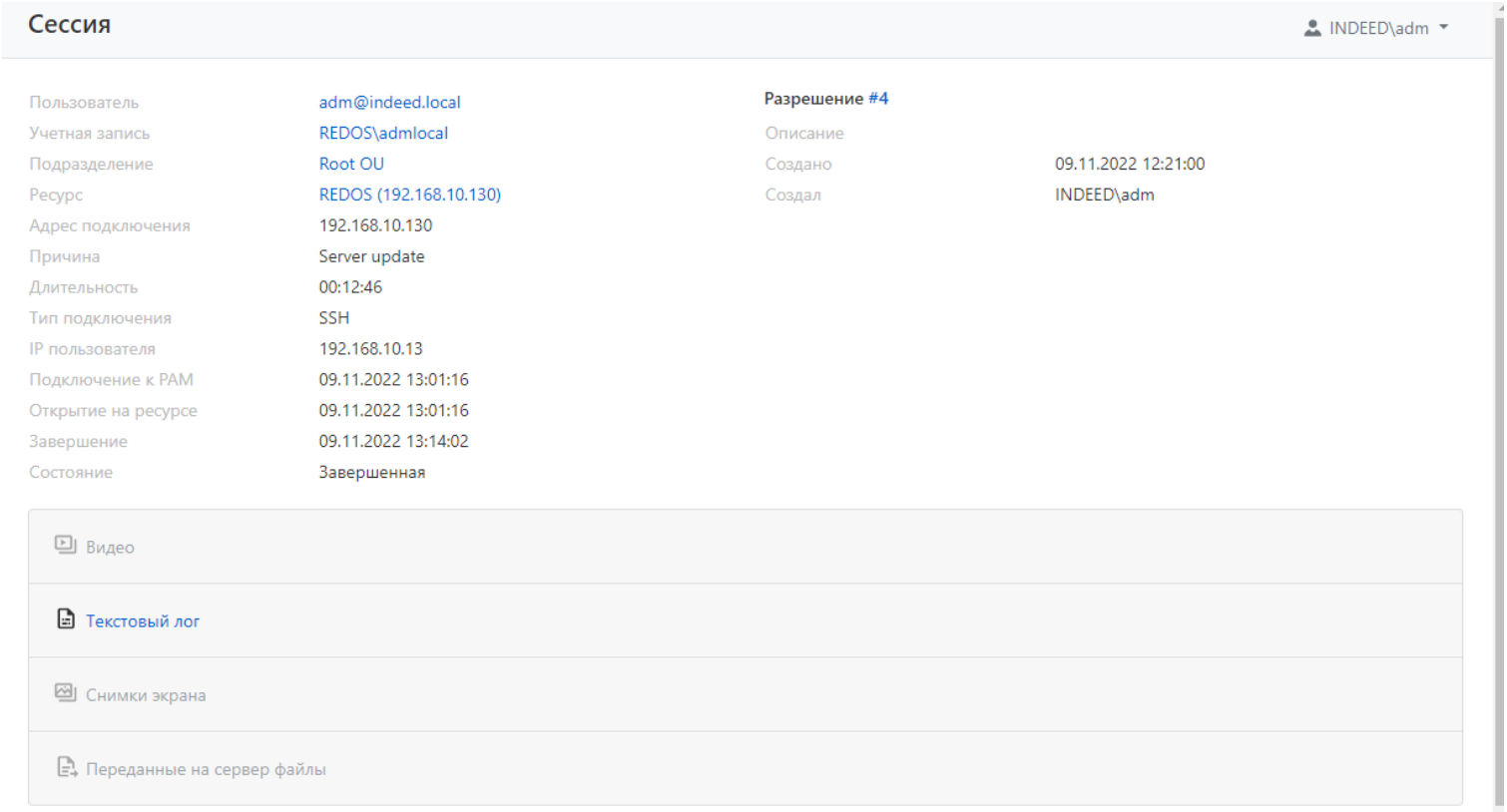
Выгрузка журнала сессий в файл

Выгрузка событий возможна в файлы двух типов: CSV и XSLX. Для выгрузки журнала нажмите на соответствующую кнопку.

Отчет формируется в виде таблицы со столбцами: "Пользователь","Учетная запись","Подразделение","Ресурс","Продолжительность","Тип подключения","Начало","Окончание","Состояние".

В выгрузку попадают только последние 10000 записей.

Профиль сессии



Для каждой сессии отображаются следующие данные:

- **Пользователь** — пользователь каталога Active Directory, который инициировал сессию.
- **Учетная запись** — учетная запись, которая используется для открытия RDP, SSH или WEB-сессии.
- **Подразделение** — имя подразделения, в котором состоит ресурс.
- **Ресурс** — ресурс, на котором была открыта RDP, SSH или WEB-сессия от имени учетной записи.
- **Адрес подключения** — IP-адрес ресурса.
- **Причина** — причина подключения к ресурсу.
- **Длительность** — длительность сессии в часах, минутах и секундах.
- **Тип подключения** — тип пользовательского подключения к ресурсу.

- **IP пользователя** — IP-адрес, с которого пользователь подключался к PAM Gateway, SSH proxy или RDP Proxy.
- **Подключение к PAM** — дата и время подключения пользователя к PAM.
- **Открытие на ресурсе** — дата и время открытия сессии на ресурсе.
- **Завершение** — дата и время закрытия сессии.
- **Состояние** — текущее состояние сессии.
- **Описание** — описание разрешения, указанное на этапе создания.
- **Создано** — дата и время создания разрешения.
- **Создал** — учетная запись администратора Indeed PAM.

Операции над сессиями

Прерывание сессии

Функция позволяет принудительно прервать сессию.

- Нажмите **Прервать** в профиле активной сессии.

Обновление сессии

Функция позволяет обновлять текстовый лог, снимки экрана и переданные на сервер файлы в ручном режиме.

- Нажмите **Обновить** в профиле активной сессии.

Видео

Для RDP-сессий, SSH-сессий, которые открыты через Indeed PAM Gateway и для сессий клиентских приложений доступны видеологирование.

Просмотр потокового видео

- Откройте секцию **Видео** в профиле активной сессии.

Просмотр/Скачивание итогового видео

- Откройте секцию **Видео** в профиле завершенной или прерванной сессии.
- Запустите видео или нажмите **Скачать все**.

Текстовый лог

Для RDP-сессий и SSH-сессий, которые открыты через Indeed PAM Gateway или Indeed PAM SSHPROXY доступен текстовый лог.

Просмотр/Поиск/Скачивание текстового лога

- Откройте секцию **Текстовый лог** в профиле завершенной или прерванной сессии.

> ⓘ **ПРИМЕЧАНИЕ**
>
> Текстовое логирование в RDP-сессиях поддерживается за счет компонента Indeed PAM Agent, агент регистрирует текстовый ввод, перехватывает названия активных окон и запускаемых процессов. Текстовое логирование в SSH-сессиях не требуется установки отдельных компонентов, в SSH-сессиях регистрируется полный ввод/вывод.

- Введите значение в поля для поиска или нажмите **Скачать**.

Снимки экрана

Для RDP-сессий, SSH-сессий, которые открыты через Indeed PAM Gateway и для сессий клиентских приложений.

Просмотр/Скачивание снимков экрана

- Откройте секцию **Снимки экрана** в профиле активной, завершенной или прерванной сессии.
- Откройте снимок экрана или нажмите **Скачать все**.

Переданные на сервер файлы

Для RDP-сессий доступен перехват и теневое копирование файлов, которые передаются с проброшенных дисков на ресурс.

Просмотр/Скачивание переданных файлов

- Откройте секцию **Переданные на сервер файлы** в профиле активной, завершенной или прерванной сессии.
- Перейдите по ссылке для скачивания переданных файлов.

События

В этом разделе отображается история событий, которые произошли в вашей инсталляции Indeed PAM.
Самые новые события — вверху таблицы.

Список всех существующих событий — скачать XLSX.

Поиск событий

Текстовый поиск **Расширенный поиск**

Введите в строку поиска **Код события**, **Компонент** или **Имя инициатора** полностью или частично.
Нажмите ENTER или .

Выгрузка событий в файл

Выгрузка событий возможна в файлы двух типов: CSV и XLSX. Для выгрузки журнала нажмите на соответствующую кнопку.

Отчет формируется в виде таблицы со столбцами: "Уровень", "Время создания", "Код", "Событие", "Описание", "Компонент", "Инициатор".

В выгрузку попадают только последние 10000 записей.

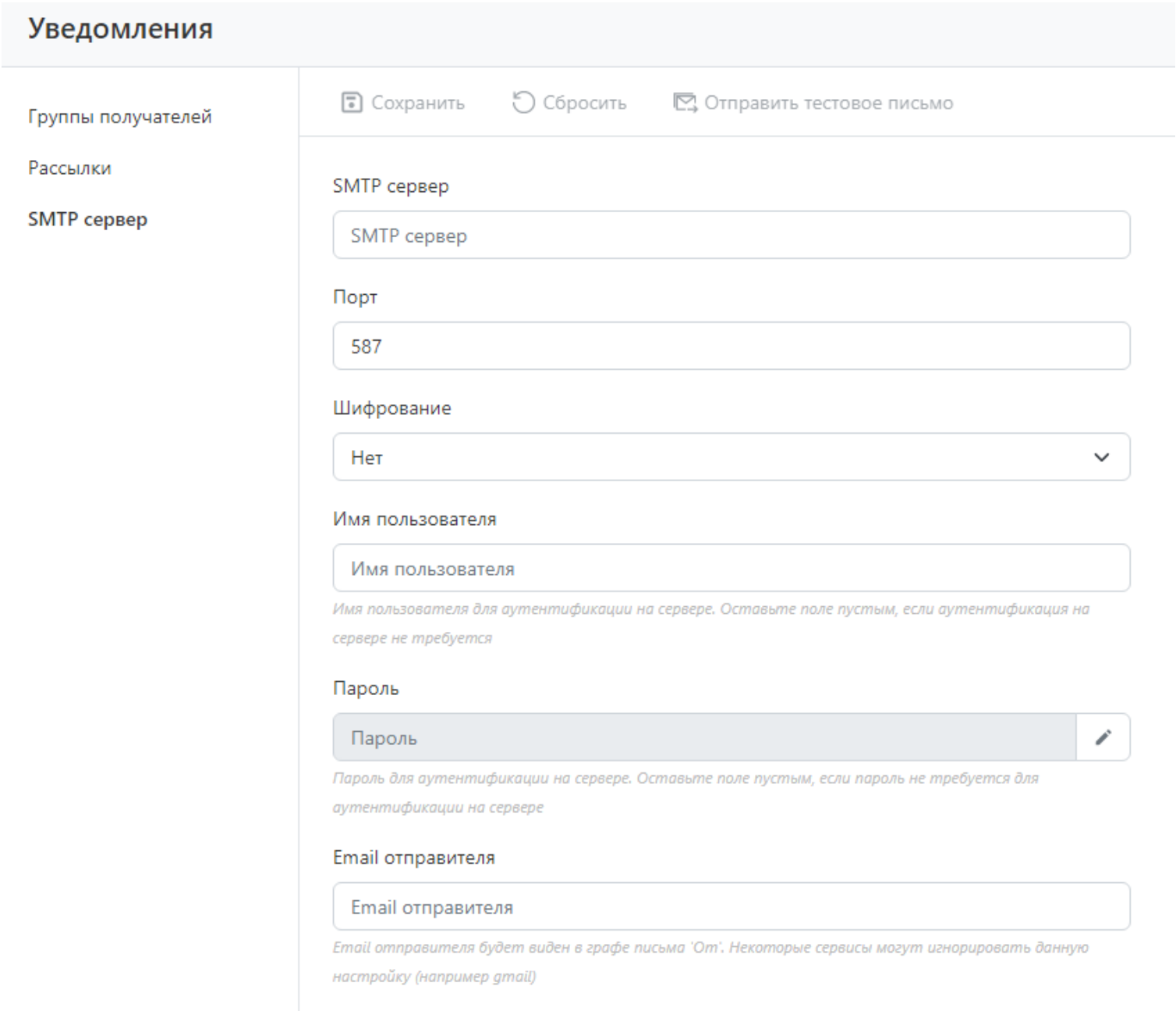
Уведомления

В данном разделе настраиваются почтовые уведомления на указанные события журнала.

Предварительная настройка

Для работы системы уведомлений укажите почтовые настройки: перейдите в раздел **SMTP сервер**, введите адрес почтового сервера, порт, данные для авторизации и сохраните изменения.

Для проверки настроек нажмите кнопку **Отправить тестовое письмо**.



Настройка уведомлений

Для настройки уведомлений выполните следующие шаги:

1. Создайте группы получателей — списки адресов для рассылки уведомлений о регистрации выбранных событий в журнале.
    i. Откройте раздел **Группы получателей**, нажмите кнопку **Добавить**, введите имя и описание группы получателей, нажмите **Сохранить**
    ii. Перейдите в созданную группу получателей, нажмите кнопку **Добавить email**, введите адрес электронной почты сотрудника.
2. В разделе **Рассылки** добавьте события, по которым необходима рассылка оповещений и соответствующие группы рассылки.

Удаление групп получателей или рассылок

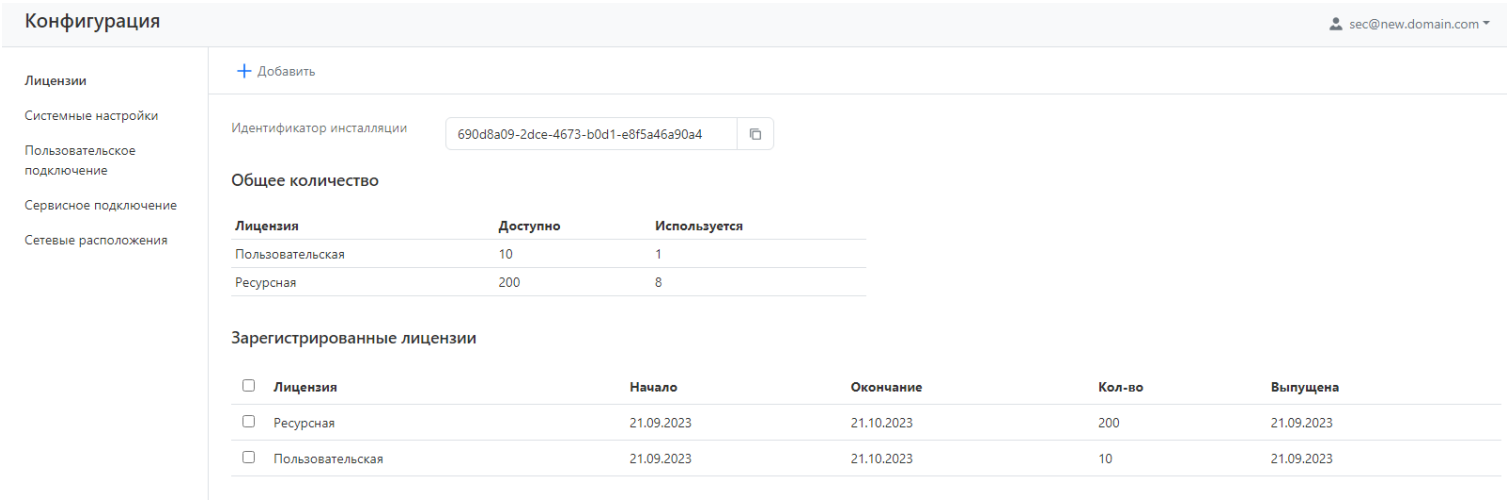
Для удаления элементов перейдите в соответствующий раздел, отметьте флажком нужные элементы и нажмите кнопку **Удалить**.

Конфигурация

Лицензии

Раздел содержит данные о лицензировании Indeed PAM.

Пользовательские лицензии



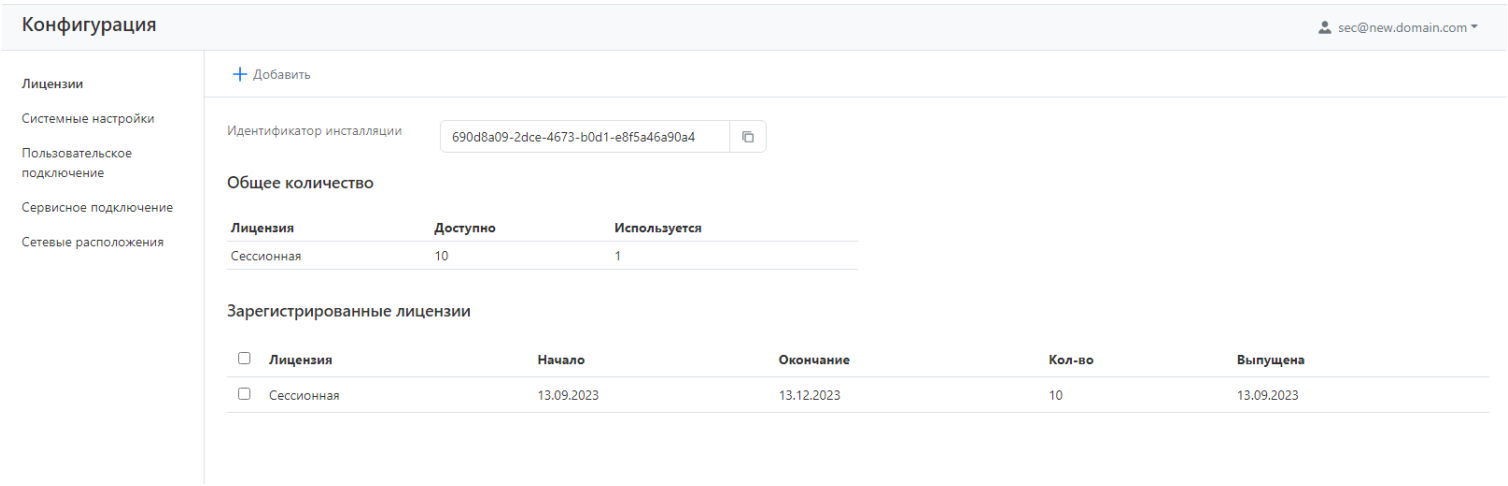
В разделе отображаются следующие данные:

- **Идентификатор инсталляции** — уникальный код инсталляции, необходим для формирования лицензии.
- **Доступно пользовательских лицензий** — общее количество пользовательских лицензий.
- **Использовано пользовательских лицензий** — количество использованных лицензий.
- **Доступно ресурсных лицензий** — общее количество ресурсных лицензий.
- **Использовано ресурсных лицензий** — количество использованных лицензий.

Для каждой лицензии отображаются следующие данные:

- **Дата начала** — дата начала действия лицензии.
- **Дата окончания** — дата окончания действия лицензии.
- **Дата выпуска** — дата формирования лицензии.
- **Количество** — количество лицензий.
- **Лицензия** — тип лицензии.

Сессионные лицензии



В разделе отображаются следующие данные:

- **Идентификатор инсталляции** — уникальный код инсталляции, необходим для формирования лицензии.
- **Доступно сессионных лицензий** — общее количество сессионных лицензий.
- **Использовано сессионных лицензий** — количество использованных лицензий.

Для каждой лицензии отображаются следующие данные:

- **Дата начала** — дата начала действия лицензии.
- **Дата окончания** — дата окончания действия лицензии.
- **Дата выпуска** — дата формирования лицензии.
- **Количество** — количество лицензий.
- **Лицензия** — тип лицензии.

Добавление лицензии

Нажмите **Добавить** и выберите файл лицензии.

Удаление лицензии

Отметьте нужную лицензию и нажмите **Удалить**.

Системные настройки

Настройка	Описание
Число неверных попыток ввода OTP	При превышении этого значения пользователь будет временно заблокирован, то есть не сможет вводить OTP. Минимальное значение: 0 Значение по умолчанию: 10 Максимальное значение: 99 0 означает, что блокировка не применяется, то есть количество попыток ввода не ограничено.
Период блокировки аутентификатора, мин	Определяет период времени, по истечении которого пользователь будет разблокирован и снова сможет вводить OTP. Минимальное значение: 1 Значение по умолчанию: 10 Максимальное значение: 9999

Пользовательское подключение

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Для работы с пользовательскими подключениями необходимы привилегии **Управления пользовательскими подключениями** (UserConnectionType.Create, UserConnectionType.Read, UserConnectionType.Update, UserConnectionType.Delete).

В Indeed PAM есть следующие встроенные типы пользовательских подключений:

- RDP

- SSH
- Telnet
- PostgreSQL

Встроенные типы не могут быть изменены или удалены.

Также доступно добавление собственных типов пользовательских подключений.

Добавление собственных типов пользовательских подключений

Для добавления нового типа подключения необходимо исследование клиентского приложения и разработка шаблона для Indeed ESSO Agent. Новый тип подключения уникален для каждого приложения, для разработки необходимо обратиться в службу технической поддержки Indeed.

Сервисное подключение

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Для работы с сервисными подключениями необходимы привилегии **Управления типами сервисных подключений** (ServiceConnectionType.Create, ServiceConnectionType.Read, ServiceConnectionType.Update, ServiceConnectionType.Delete).

В Indeed PAM есть следующие встроенные типы сервисных подключений:

- Windows
- SSH
- Microsoft SQL Server
- MySQL
- PostgreSQL
- Oracle Database
- Cisco IOS
- Inspur BMC

Встроенные типы не могут быть изменены или удалены.

Также доступно добавление собственных типов сервисных подключений.

Добавление собственных типов сервисных подключений

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Если сервер управления вашей инсталляции PAM установлен на хосте с ОС Windows, то можно добавлять только коннекторы с шаблоном powershell.
>
> Если сервер управления вашей инсталляции PAM установлен на хосте с ОС Linux, то можно добавлять только коннекторы с шаблоном bash.

1. Откройте раздел **Конфигурация** → **Сервисное подключение**.
2. Нажмите **Добавить тип сервисного подключения**.
3. В открывшемся окне загрузите ZIP-архив с файлом коннектора.
4. Задайте **Название** сервисного подключения или используйте значение, загруженное из метаданных.
5. Введите **Описание** сервисного подключения. Опционально.
6. Завершите добавление нажатием кнопки **Добавить**.

Подготовка файлов коннекторов

Для подготовки ZIP-архива с файлом коннектора используйте утилиту Connector Creation Tool.

Редактирование собственных типов сервисных подключений

Загрузить новый коннектор | **Отредактировать название или описание**

1. Откройте раздел **Конфигурация** → **Сервисное подключение**.
2. Нажмите **Редактировать** рядом с требуемым типом сервисного подключения.
3. Нажмите **Скачать архив** и выберите папку на компьютере для сохранения текущего ZIP-архива с файлом коннектора. Этот архив понадобится, чтобы восстановить предыдущее состояние сервисного подключения, если при загрузке нового архива возникнет ошибка.
4. Загрузите новый ZIP-архив с файлом коннектора.
5. Если требуется, отредактируйте **Название** и/или **Описание**.
6. Завершите редактирование нажатием **Сохранить**.

Просмотр кода скрипта коннектора

1. Откройте раздел **Конфигурация** → **Сервисное подключение**.
2. Нажмите **Показать код скрипта** рядом с требуемым типом сервисного подключения.

Удаление собственных типов сервисных подключений

1. Откройте раздел **Конфигурация** → **Сервисное подключение**.
2. Нажмите **Удалить** рядом с требуемым типом сервисного подключения.

> ⓘ **ИНФОРМАЦИЯ**
>
> Нельзя удалить тип сервисного подключения, если существует ресурс с таким типом.

Загрузка шаблона SSH-коннектора

Шаблон сервисных операций уникален для каждого дистрибутива *nix. В составе дистрибутива по пути **IndeedPAM_3.0_RU\indeed-pam-tools\ssh-templates** приложены шаблоны для следующих дистрибутивов *nix:

- Alt
- Astra
- CentOS
- Debian
- FreeBSD
- Gentoo
- Oracle
- RedOS
- RHEL
- Rocky
- SLES
- Ubuntu

Чтобы добавить шаблон в Indeed PAM:

1. Откройте раздел **Конфигурация** → **Сервисное подключение**.
2. Внутри блока SSH нажмите **Добавить**.

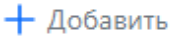
3. Выберите файл с нужным вам шаблоном SSH-коннектора из дистрибутива по пути **IndeedPAM_3.0_RU\indeed-pam-tools\ssh-templates**.

Для разработки другого шаблона обратитесь в службу технической поддержки Indeed.

Сетевые расположения

Раздел содержит данные о добавлении сетевых расположений, для ограничений использования ресурсов, выданных по адресам.

Добавление сетевого расположения

Нажмите кнопку 

.

Введите **Имя** и добавьте **Сетевые адреса** ресурсов, которым необходимо выдать ограниченное подключение.

Указание длительности сегмента видео при записи RDP-сессии

Во время RDP-сессии записывается видео с рабочего стола удаленного ресурса. Видеозапись RDP-сессии делится на сегменты. Чем длиннее сегмент видеозаписи, тем сильнее нагружается CPU в открытой сессии.

Чтобы снизить нагрузку на CPU, уменьшите значение следующего параметра: **Конфигурация** → **Системные настройки** → **Длительность сегмента записываемого видео** в консоли администратора PAM.

Работа с Connector Creation Tool

Connector Creation Tool (CCT) — это утилита командной строки для создания и отладки собственных типов сервисного подключения. Созданный с помощью этой утилиты архив загружается в PAM в разделе **Конфигурация → Сервисное подключение**.

Предварительные требования

Для запуска на Windows нет дополнительных требований.
Для запуска на Linux требуется наличие установленных Microsoft .NET Core 8 и Docker.

Подготовка коннектора

1. Для удобства работы с утилитой Connector Creation Tool (CCT) добавьте для нее псевдоним с помощью команды, указанной ниже. Перед выполнением команды замените `<путь до CCT>` на то расположение в файловой системе, по которому у вас находится Connector Creation Tool.

   После выполнения указанной команды закройте терминал и откройте заново.

   Windows | **Linux**

   Добавление пути до CCT в переменную окружения

   ```
   "New-Alias cct <путь до CCT>\Pam.Tools.ConnectorCreationTool.exe" | Add-Content $PROFILE
   ```

2. Создайте папку для коннектора и перейдите в нее:

   Создание папки для коннектора

   ```
   mkdir my_connector
   cd my_connector
   ```

3. Создайте шаблон коннектора с помощью команды `new`:

Создание шаблона коннектора

```
cct new
```

Тип коннектора выбирается в зависимости от ОС: на Windows — ps1, на Linux — sh. При необходимости можно поменять тип в опциях команды `new`, подробную информацию смотрите в справочнике команд.

После выполнения команды в директории появятся основные файлы коннектора. Подробную информацию смотрите в пункте структура коннектора.

4. В файле `connector.ps1/sh` по умолчанию есть методы, которые требуется реализовать. Изначально они возвращают ошибку и содержат закомментированные примеры с корректно возвращаемыми данными. Реализуйте эти методы.

> ⓘ **ИНФОРМАЦИЯ**
>
> Основной скрипт коннектора должен быть написан на языке bash или powershell, в зависимости от выбранного типа коннектора. При этом для реализации методов можно использовать любые языки и технологии, в зависимости от того, на чем удобнее делать обращения к ресурсу. В этом случае понадобится в основном скрипте `connector.ps1/sh` вызывать ваши скрипты или исполняемые файлы, созданные на других языках.

5. Переходите к отладке коннектора.

Отладка коннектора

После того, как методы в скрипте реализованы, можно проверить корректность их выполнения с помощью команды `run`. Подробную информацию о команде `run` смотрите в справочнике команд.

1. Проверьте соединение до коннектора.

Проверка соединения до коннектора

```
cct run test_connection -a <DNS или IP коннектора>
```

2. Проверьте команду установки пароля для пользователя.

Установка пароля для пользователя

```
cct run set_user_password -a <DNS или IP коннектора> --user <пользователь> --new-password <новый пароль>
```

3. Проверьте команду установки ключа для пользователя.

Установка ключа для пользователя

```
cct run set_user_key -a <DNS или IP коннектора> --user <пользователь> --old-key-path <старый ключ> --new-key-path <новый ключ>
```

4. Проверьте команду проверки пароля пользователя.

Проверка пароля пользователя

```
cct run test_password -a <DNS или IP коннектора> --user <пользователь> --password <пароль>
```

5. Проверьте команду проверки ключа пользователя.

Проверка ключа пользователя

```
cct run test_key -a <DNS или IP коннектора> --user <пользователь> --key-path <ключ>
```

6. Проверьте команду проверки наличия неуправляемых ключей.

Проверка наличия неуправляемых ключей

```
cct run test_unmanaged_keys -a <DNS или IP коннектора> --user <пользователь> --key-path <ключ>
```

7. Проверьте команду удаления неуправляемых ключей.

Удаление неуправляемых пользователем ключей

```
cct run remove_unmanaged_keys -a <DNS или IP коннектора> --key-path <ключ>
```

8. Проверьте команду получения информации о ресурсе.

Получение информации о ресурсе

```
cct run get_resource_info -a <DNS или IP коннектора>
```

9. Проверьте команду получения информации об аккаунте.

Получение информации об аккаунте

```
cct run get_account_info -a <DNS или IP коннектора> --user <пользователь>
```

10. Проверьте команду получения списка пользователей.

Получение списка пользователей

```
cct run get_users -a <DNS или IP коннектора>
```

11. После проверки всех сервисных операций переходите к упаковке коннектора.

Упаковка коннектора

Проверенные файлы коннектора требуется упаковать в ZIP-архив для его дальнейшей загрузки в PAM. Для этого выполните следующую команду в той же директории:

Упаковка коннектора

```
cct pack
```

Подробную информацию о команде `pack` смотрите в справочнике команд.

Готовый ZIP-архив будет записан в родительскую директорию. Далее переходите в PAM в раздел **Конфигурация → Сервисное подключение** для загрузки ZIP-архива коннектора.

Структура коннектора

В ZIP-архиве коннектора есть три основных файла:

- `info.json` — метаданные коннектора
- `info.schema.json` — JSON-схема файла info.json
- `connector.ps1/sh` — скрипт, выполняющий сервисные операции

Кроме основных файлов коннектор может содержать любые другие файлы, в том числе бинарные, кроме файлов с именем `wrapper.ps1` и `wrapper.sh` Эти имена файлов зарезервированы под PAM для вспомогательного скрипта для запуска коннектора.

Максимальный размер ZIP-архива коннектора — 100 МБ.

Пример файла info.json

```
{
  "$schema": "info.schema.json",
  "Id": "TestBashConnector",
  "Name": "Test Bash connector",
  "Description": "This is a test connector",
  "Version": "1.0",
  "CreatedAt": "2024-12-05 14:45:03Z",
  "ConnectorType": "sh",
  "ScriptTimeout": 30,
  "IsKeyServiceOperationSupported": false,
  "LinuxSandbox": {
    "Image": "my-test-connector:1.0",
    "CpuLimit": "0.5",
    "MemoryLimitMb": "512",
    "StorageLimitMb": "1024",
    "PidCountLimit": "8"
  }
}
```

- `$schema` — имя файла JSON-схемы.
- `Id` — идентификатор коннектора, должен быть уникальным в рамках PAM.
- `Name` — имя коннектора, которое будет отображаться в PAM, должно быть уникальным в рамках PAM.

- `Description` — описание коннектора, которое можно будет просмотреть в деталях коннектора в PAM. Опциональное поле.
- `Version` — версия коннектора.
- `CreatedAt` — время создания коннектора, указывается автоматически при упаковке коннектора.
- `ConnectorType` — тип коннектора (sh или ps1).
- `ScriptTimeout` — таймаут работы коннектора в секундах. Если при выполнении сервисной операции скрипт не завершится за указанное время, то операция завершится по таймауту.
- `IsKeyServiceOperationSupported` — флаг, показывающий, поддерживается ли коннектором работа с SSH-ключами. Если в скрипте реализованы операции с SSH-ключами, то укажите true.
- `LinuxSandbox` — опциональный раздел. Содержит настройки для переопределения настроек по умолчанию Docker-песочницы, указанных в Core/appsettings.json.
- `Image` — тег Docker-образа для выполнения песочницы.
- `CpuLimit` — ограничение работы CPU одного контейнера песочницы.
- `MemoryLimitMb` — ограничение работы по памяти одного контейнера песочницы.
- `StorageLimitMb` — ограничение временного хранилища одного контейнера песочницы.
- `PidCountLimit` — ограничение количества процессов одного контейнера песочницы.

> **ИНФОРМАЦИЯ**
>
> Для PowerShell-коннекторов песочницы нет.

Справочник команд

new

Создает шаблон для нового коннектора. Данная команда генерирует файлы `info.json`, `info.schema.json` и `connector.ps1/sh` в указанной директории.

Windows | **Linux**

Пример запуска команды

```
<путь до CCT>\Pam.Tools.ConnectorCreationTool.exe new -t ps1 -p
C:\Users\user\documents\folder1\
```

Параметры команды new

Имя	Обязательный	Описание
-v, --verbose	—	Включить показ дополнительных логов.
-p, --path `path`	—	Путь до каталога, в котором будут созданы файлы info.json и connector.ps1. Если не указан, то файлы будут созданы в текущей папке.
-t, --type `type`	—	Тип скрипта коннектора. Возможные значения: sh, ps1. • sh — выполняются только на Linux (bash) • ps1 — выполняются только на Windows (powershell)
-h, --help	—	Информация об использовании и помощь.

pack

Создает ZIP-архив коннектора для последующей загрузки в консоли администратора.

Windows **Linux**

Пример запуска команды

```
<путь до CCT>\Pam.Tools.ConnectorCreationTool.exe pack -p
C:\Users\user\documents\folder1\ -n b80d094b715aa08375b87e9.1.1
```

Параметры команды pack

Имя	Обязательный	Описание
-v, --verbose	—	Включить показ дополнительных логов.
-p, --path `path`	—	Путь до коннектора.

Имя	Обязательный	Описание
-n, --name `name`	—	Имя ZIP-файла без указания расширения .zip. По умолчанию имя состоит из значений полей ID и Version файла info.json.
-h, --help	—	Информация об использовании и помощь.

hash

Рассчитывает хеш SHA-256 файла. Используется для обеспечения целостности файлов.

Windows Linux

Пример запуска команды

```
<путь до CCT>\Pam.Tools.ConnectorCreationTool.exe hash -p
C:\Users\user\documents\folder1\
```

Параметры команды hash

Имя	Обязательный	Описание
-v, --verbose	—	Включить показ дополнительных логов.
-p, --path `path`	Да	Путь до коннектора (ZIP-архив).
-h, --help	—	Информация об использовании и помощь.

run

Запускает коннектор, выполняет скрипт коннектора в указанной директории.

Windows Linux

Пример запуска команды

```
<путь до CCT>\Pam.Tools.ConnectorCreationTool.exe run test_connection -p
C:\Users\user\documents\folder1\ -a 192.168.5.1
```

Параметры команды run

Имя	Обязательный	Описание
-v, --verbose	—	Включить показ дополнительных логов.
-p, --path	—	Путь до коннектора (ZIP-архив или директория).
-a, --address `address`	Да	Адрес коннектора в виде DNS или IP.
--port `port`	—	Порт коннектора.
-sa, --service-account `account`	—	Имя сервисного аккаунта.
-sp, --service-account-password `password`	—	Пароль сервисного аккаунта.
-skp, --service-account-key-path `key-path`	—	Ключ сервисного аккаунта.
-slt, --service-account-location-type `location-type`	—	Тип нахождения сервисного аккаунта. Возможные значения: Domain, Local.
--disable-sandbox	—	Отключить песочницу.
-h, --help	—	Информация об использовании и помощь.

Команды, которые можно запускать с помощью run

Имя	Описание
test_connection	Проверить соединение до коннектора.
set_user_password	Установить пароль для пользователя.
set_user_key	Установить ключ для пользователя.
test_password	Проверить пароль пользователя.
test_key	Проверить ключ пользователя.
test_unmanaged_keys	Проверить наличие неуправляемых ключей.
remove_unmanaged_keys	Удалить неуправляемые пользователем ключи.
get_resource_info	Получить информацию о ресурсе.
get_account_info	Получить информацию об аккаунте.
get_users	Получить список пользователей.

Роли

Раздел предназначен для настройки привилегий пользователей-администраторов PAM в консоли управления Indeed PAM.

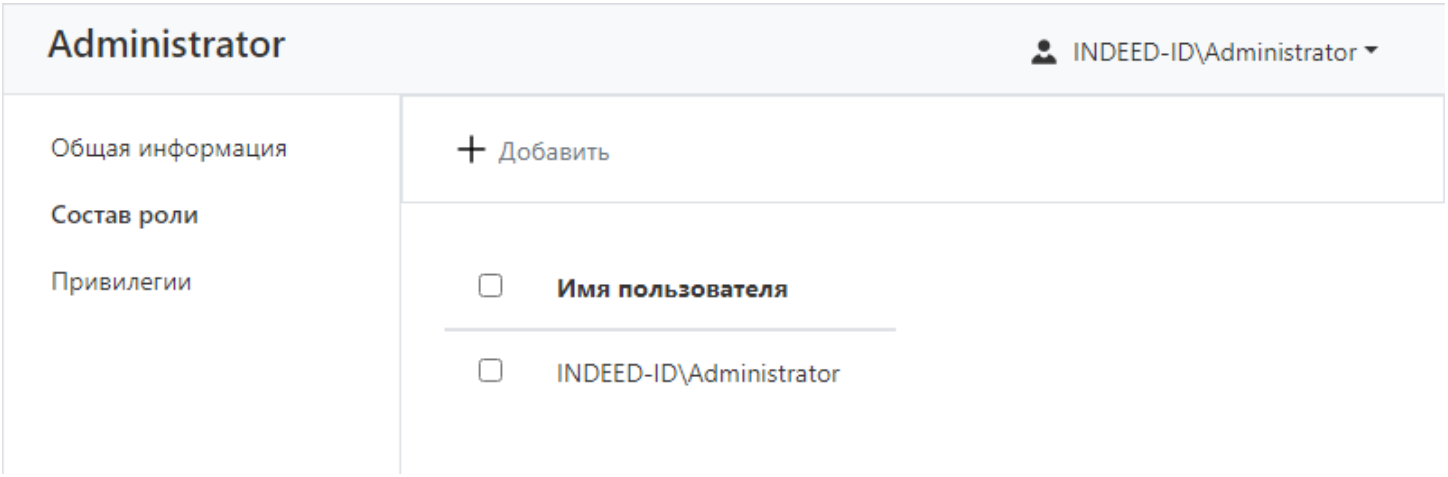
Предварительная настройка

После первого входа в консоль администратора потребуется добавить текущего пользователя в состав роли **Administrator**, для этого:

1. Перейдите в раздел **Роли**

2. Откройте роль **Administrator** и перейдите в подраздел **Состав роли**

3. Нажмите **Добавить**, выберите текущего пользователя и добавьте его в состав роли



4. Заново войдите в консоль управления и убедитесь что в консоли появились остальные разделы.

Предустановленные роли

После установки будут доступны роли **Administrator**, **Operator** и **Supervisor**.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Внимание! После перехода на новую версию необходимо проверить составы привилегии у всех используемых ролей.

Для роли **Administrator** включен полный набор привилегий.

Для роли **Operator** включены привилегии, позволяющие выдавать или отзывать разрешения (к примеру, обрабатывать заявки на доступ), а также выполнять проверку привилегированных Учетных записей и доступность конечных Ресурсов.

Роль **Supervisor** предназначена для поиска и просмотра значений, за исключением паролей Учетных записей. Привилегии на добавление и изменение значений отключены. Роль будет полезна для контроля за работой администраторов PAM.

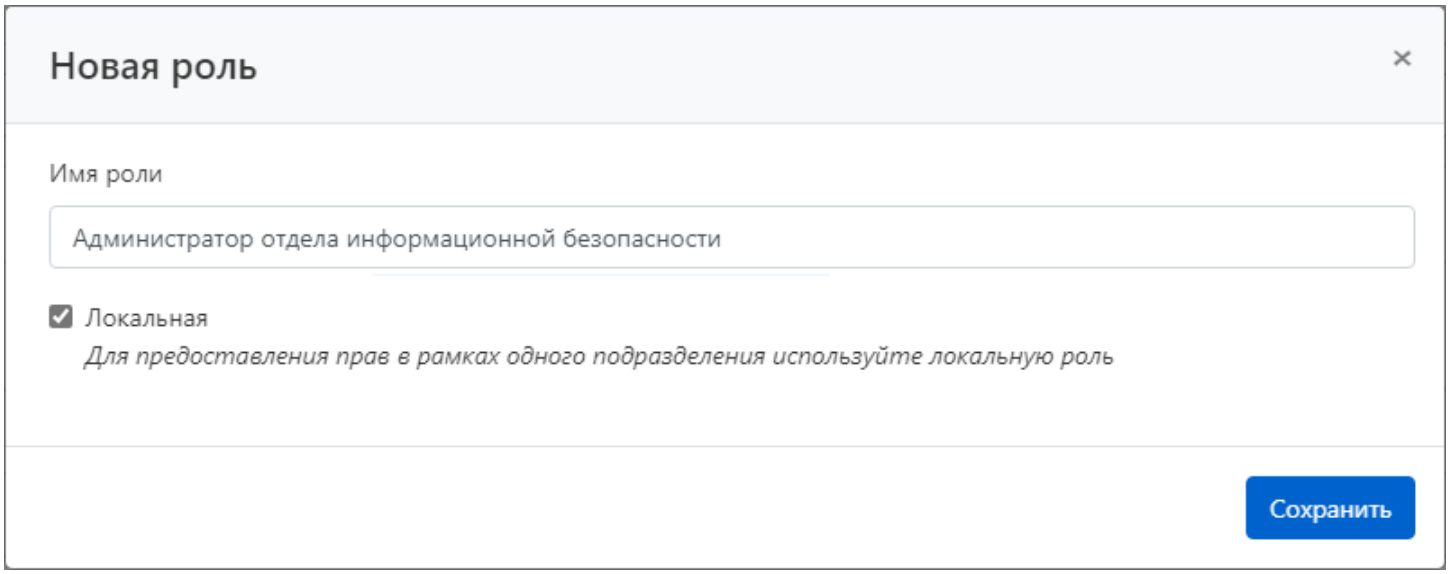
Данные роли являются Глобальными. Сделать роль Локальной можно только при создании новой роли.

Создание новых ролей

> **ПРИМЕЧАНИЕ**
>
> Для выполнения операций с ролями необходимы привилегии управления ролями доступа.

Выполните следующие шаги:

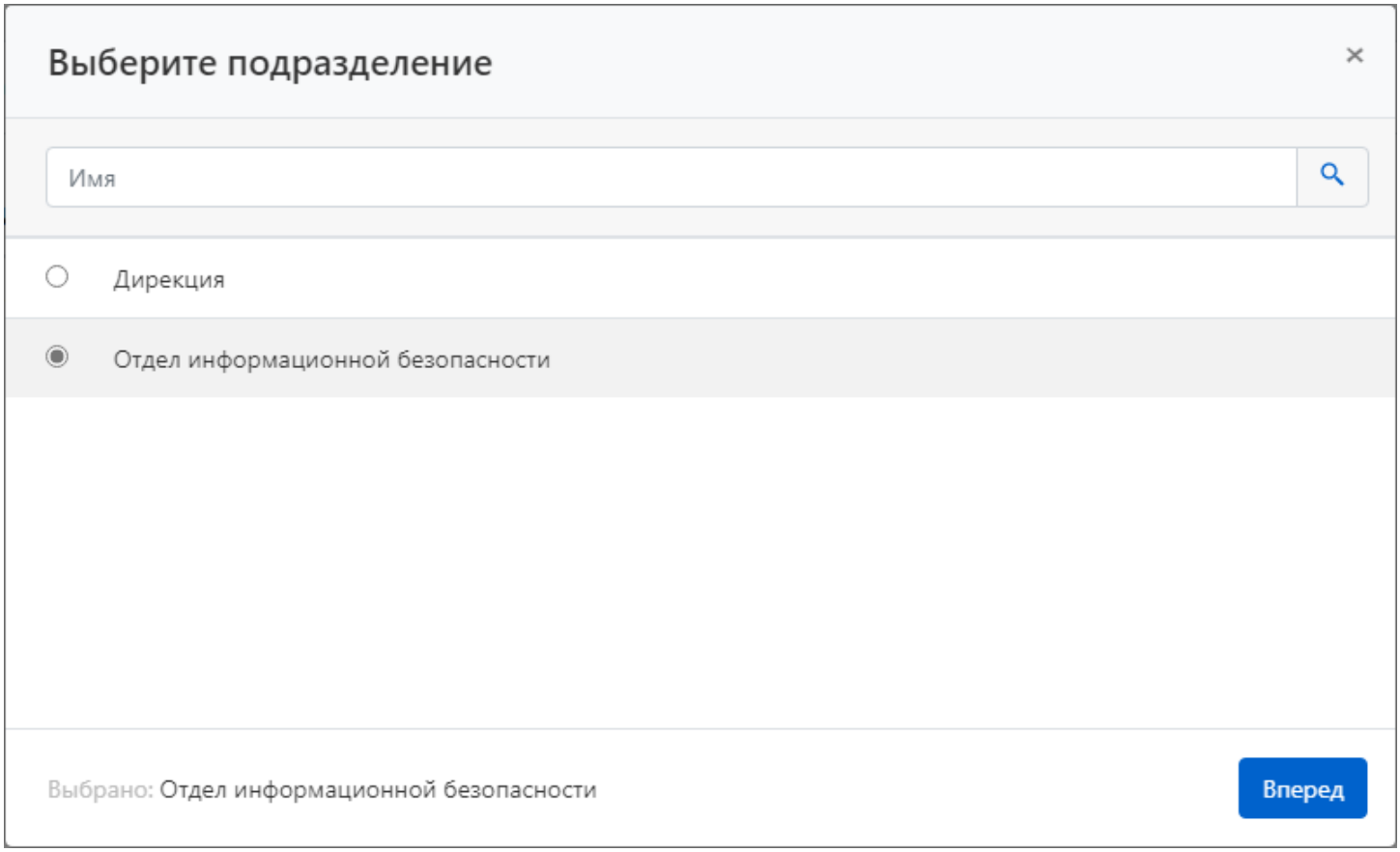
1. Перейдите в раздел **Роли**, нажмите кнопку **Добавить**, укажите имя для новой роли, для создания локальной роли включите флажок **Локальная**. Новая роль добавится в список ролей.
2. Откройте созданную роль, перейдите в раздел **Привилегии**, выберите необходимый набор привилегий и сохраните изменения.



Добавление пользователей в состав роли

Для назначений привилегий администраторам PAM выполните следующие действия:

1. Перейдите в раздел **Роли**, откройте необходимую роль.
2. Перейдите в раздел **Состав роли**, нажмите **Добавить**. Выберите подразделение, затем пользователя.



> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Если пользователь добавлен в состав нескольких ролей, то он получает сумму привилегий из всех своих ролей.

Удаление ролей

Перейдите в раздел **Роли**, отметьте флажком нужные роли, нажмите **Удалить**.

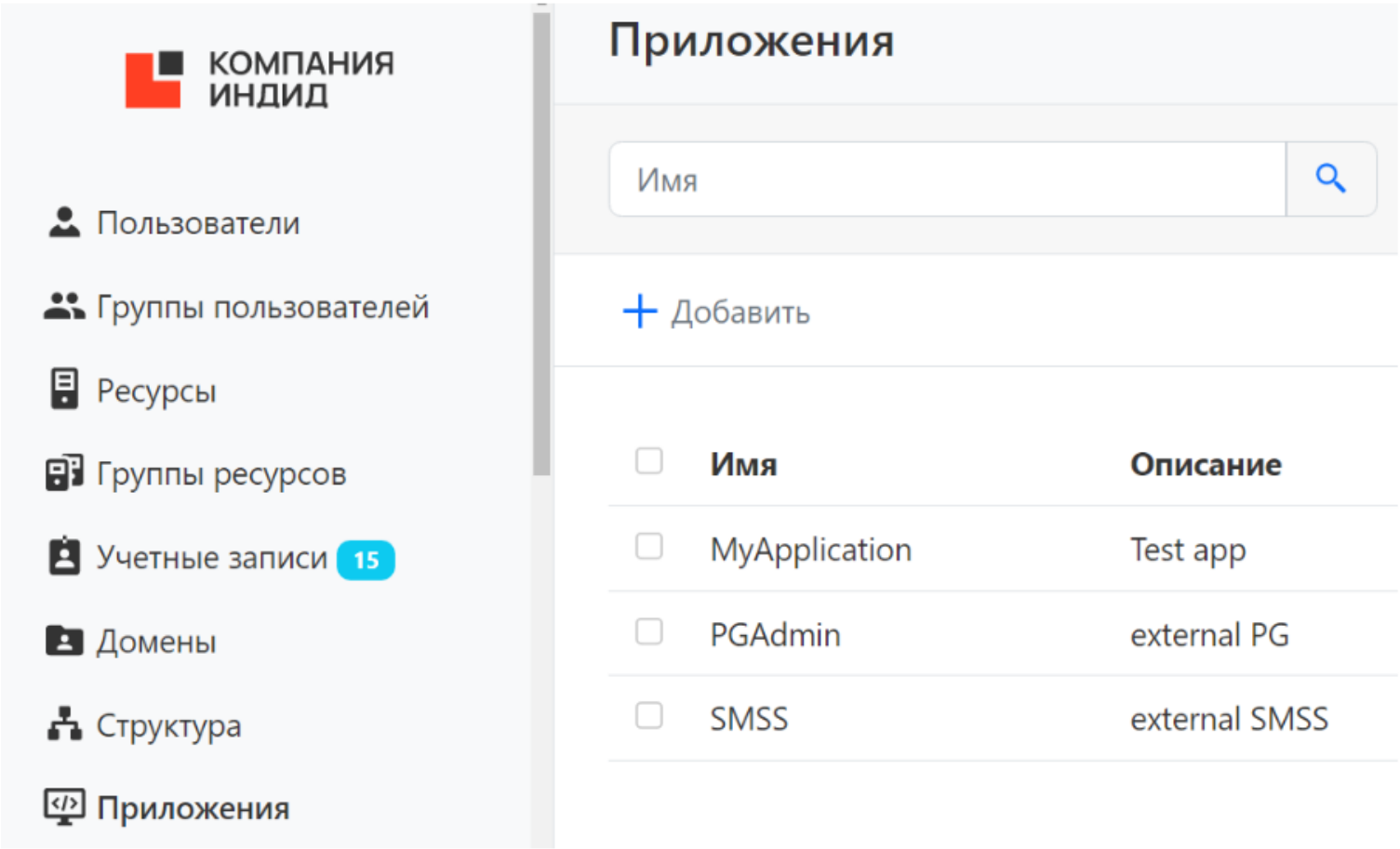
Приложения

AAPM — это набор методов и инструментов для автоматизации получения паролей и SSH ключей (учетных данных) УЗ приложениями.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Для использования Приложений необходимо иметь AAPM лицензии.

Чтобы добавить приложение в Indeed PAM необходимо:

1. Перейти в раздел Приложения в МС
2. Нажать кнопку Добавить

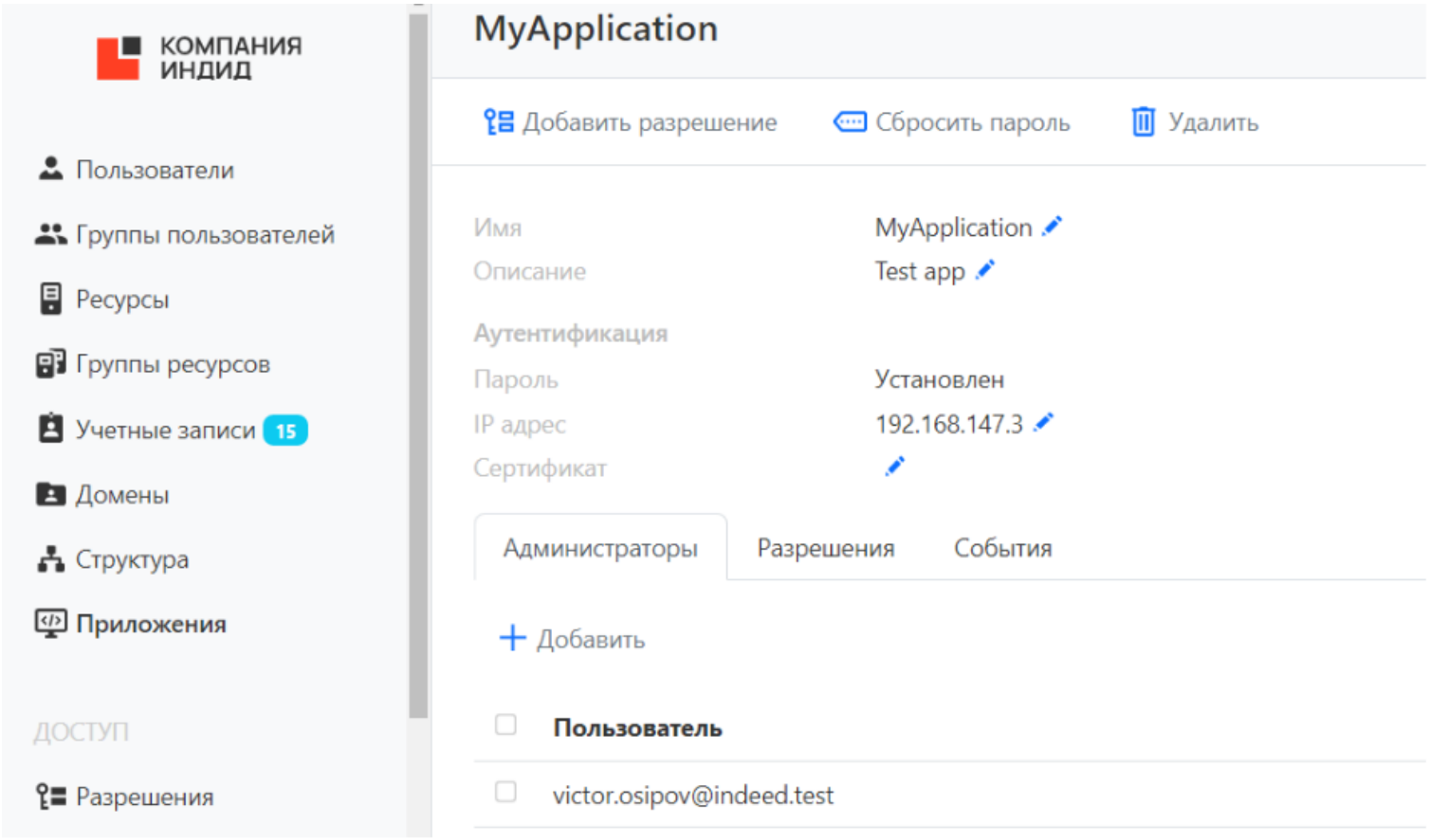


Настройка приложений:

В разделе приложения можно:

- Задавать имя приложения, описание, настроить тип аутентификации.

- Добавлять администраторов приложения. Это позволяет просматривать пароль от этого приложения в UC.
- Добавлять разрешения. Для этого необходимо:
  - Нажмите на кнопку **Добавить разрешение**.
  - Выберите подразделение.
  - Выберите учетную запись, от которой необходимо получать пароль.
  - Настройте время работы разрешения и описание.
  - Завершите создание разрешения кнопкой **Создать**.
- Сбрасывать пароль. Для этого необходимо нажать на кнопку **Сбросить пароль**.
- Удалить приложение. Для этого необходимо нажать на кнопку **Удалить**.
- Просмотреть выданные разрешения и события, которые произошли в системе PAM для этого приложения



Аутентификация приложений:

Приложения, как и пользователи, аутентифицируются на IDP и получают токен.

Возможны несколько способов аутентификации приложений:

1. Статичный пароль — задается автоматически при создании приложения. Администратор PAM может **сбросить** через MC, но не может посмотреть. Пользователь PAM, являющийся администратором конкретного приложения, может посмотреть пароль этого приложения в UC.
2. IP-адрес — опционально. IDP проверяет, что запрос на получение токена пришел с указанного IP-адреса. Задается администратором PAM в MC.

Выгрузка паролей

В случае нештатной ситуации, при отказе компонентов PAM предусмотрена возможность выгрузки паролей привилегированных учетных записей из базы PAM.

Выгрузка осуществляется с помощью утилиты **IndeedPAM_3.0_RU\indeed-pam-tools\dump\Pam.Tools.Dump.exe**

Перед использованием откройте конфигурационный файл утилиты **indeed-pam-windows\MISC\Dump\appsettings.json** и укажите параметры доступа к базе Core:

Секция `Database`.

- `Database` — провайдер для работы с СУБД
  - `mssql` — Microsoft SQL Server
  - `pgsql` — PostgreSQL, PostgreSQL Pro
- `ConnectionStrings`

<details>
<summary>Строка подключения к MicrosoftSQL</summary>

- `Data Source` — имя сервера СУБД или именованного экземпляра
- `Initial Catalog` — имя базы данных
- `User ID` — учетная запись для работы с БД
- `Password` — пароль учетной записи
- Другие параметры доступны в документации по строке подключения SqlClient 3.0 .NET Core

```
"ConnectionString": "Data Source=sql.domain.local; Initial Catalog=IPAMCore;
Integrated Security=False; User ID=IPAMSQLService; Password=password"
```

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> В случае использования именованного экземпляра Microsoft SQL Server значение параметра `Server` необходимо указывать в формате **имя сервера\\имя экземпляра**.
</details>

```
"PamCore": "Data Source=sql\\instance; ..."
```

▼ Строка подключения к PostgreSQL

- `Host` — имя сервера СУБД или именованного экземпляра
- `Database` — имя базы данных
- `Username` — учетная запись для работы с БД
- `Password` — пароль учетной записи
- Другие параметры доступны в документации по строке подключения Npgsql

```
"ConnectionString": "Host=sql.domain.local; Database=IPAMCore; Integrated
Security=False; Username=IPAMSQLService; Password=password"
```

Секция `Encryption`.

- `Algorithm` — алгоритм шифрования базы Core
- `Key` — ключ шифрования базы Core

Утилита запускается с аргументами:

- `decrypt-ssh-key` — расшифровка зашифрованного экспортированного ssh-ключа учетной записи.
- `decrypt-password` — расшифровка зашифрованного экспортированного пароля учетной записи.
- `decrypt-secrets` — расшифровка учетных данных учетных записей из указанной или выбранной папки.
- `ssh-key` — выгрузка SSH ключа привилегированной учетной записи, необходимо указать учетную запись, пример:
  `Pam.Tools.Dump.exe sshKey --name res2\administrator`.
- `password` — выгрузка пароля привилегированной учетной записи, необходимо указать учетную запись, пример:

`Pam.Tools.Dump.exe password --name res2\administrator`.

- `all-secrets` — выгрузка всех учетных данных в папку .\Results, либо в указанную. Пароли будут выгружены в файл **accounts.csv**, ключи будут выгружены в папку sshKeys в отдельные файлы. Пример команды:
  `Pam.Tools.Dump.exe secrets --output c:\temp`.
- `help` — вывод справки.
- `version` — вывод информации о версии.

Работа с PostgreSQL Proxy

Начиная с Indeed PAM 3.0 стало возможно открывать SQL-сессии через PostgreSQL Proxy. Это позволяет просматривать текстовый лог SQL-сессий, благодаря чему обеспечивается более полный контроль над сессиями и упрощается расследование инцидентов.

Настройка клиента СУБД

Часто у клиентов СУБД есть особенность работы: после подключения к серверу БД для выполнения SQL-запросов открывается отдельная сессия. В этом случае в PAM так же создается несколько сессий, что может доставлять неудобства при просмотре текстовых логов.

Чтобы SQL-запросы выполнялись в той же сессии, что и подключение к серверу БД, нужно настроить клиент СУБД. Ниже приведена информация, как это сделать на примере клиента DBeaver.

1. Откройте DBeaver.
2. В левой части экрана, в окне **Базы данных** (Database Navigator) найдите в списке доступных подключений нужный сервер, нажмите на него левой кнопкой мыши и нажмите на клавиатуре F4.
3. В открывшемся окне перейдите на вкладку **Метаданные** (Metadata), поставьте флаг **Настройки базы <имя сервера>** (Datasource <servername> settings).
4. Для параметра **Открывать отдельное соединение для чтения метаданных** (Open separate connection for metadata read) укажите опцию **Never** из выпадающего списка.
5. Перейдите на вкладку **Редактор SQL** (SQL Editor).
6. Для параметра **Открывать отдельное соединение для каждого редактора** (Open separate connection for each editor) укажите опцию **Never** из выпадающего списка.
7. Сохраните изменения нажатием кнопки **OK**.
8. Повторите все перечисленные действия для всех ваших серверов БД.

Указание адреса PostgreSQL Proxy в PAM

1. Откройте консоль управления Indeed PAM.
2. Перейдите в раздел **Конфигурация** → **Системные настройки**.
3. В секции **PostgreSQL Proxy** заполните поле **Адрес PostgreSQL Proxy**.

Открытие сессии через PostgreSQL Proxy

Описано в руководстве пользователя, в пункте Подключение к ресурсу через PostgreSQL Proxy.

Просмотр текстовых логов SQL-сессии

Чтобы просмотреть текстовые логи сессии, открытой через PostgreSQL Proxy:

1. Откройте консоль управления Indeed PAM.
2. Откройте раздел **Активные сессии**.
3. Выберите нужную сессию.
4. Нажмите **Текстовый лог**.

> **ИНФОРМАЦИЯ**
>
> Учитывайте, что разные SQL-клиенты могут по-разному сохранять текст SQL-запросов. Например, psql вырезает комментарии из SQL-запросов, а pgAdmin оставляет.

Текстовый лог, отображаемый в профиле сессии, не обновляется автоматически. Для получения актуального текстового лога, требуется периодически нажимать **Обновить**.

В текстовом логе не сохраняются результаты запросов.

В текстовый лог попадают только исходящие SQL-запросы (клиент → сервер). Исходящие запросы (сервер → клиент) не попадают.

Ограничения

- Двухфакторная аутентификация поддерживается только для инсталляций с аутентификацией через RADIUS, где вторым фактором является подтверждение запроса в приложении. Для инсталляций с аутентификацией через PAM параметр **Использовать двухфакторную аутентификацию** будет игнорироваться, то есть второй фактор запрашиваться не будет, подключение откроется без него.
- Подтверждение администратором открытия сессии не поддерживается. Отключите параметр **Открытие сессии требует подтверждения администратора PAM** в разделе **Политики** → **Сессии**, иначе открыть SQL-сессию будет невозможно.

- Указание причины открытия сессии поддерживается частично. Если включен параметр **Требовать указать причину подключения** в политике сессии, то пользователям потребуется вводить причину в то же поле, где имя учетной записи. Подробная информация в пункте Подключение к ресурсу через PostgreSQL Proxy.

Консоль пользователя

Получите доступ к консоли пользователя

Получение доступа к ресурсу

Ознакомьтесь со способами подключения к ресурсам

Подключение через SSH-клиенты

Ознакомьтесь со способами подключения к ресурсам через сторонние SSH-клиенты

SCP/SFTP подключение к ресурсу

Количество глав: 3

Личные папки ресурсов

Ознакомьтесь с возможностями группировки ресурсов

Выполнение команд с привилегией root

Прочитайте, как выполнить команду, если нужно sudo

Операции с учетными записями

Ознакомьтесь с информацией о поиске учетных записей, просмотре и смене паролей и SSH-ключей

Работа с AAPM Console Tool

Отредактируйте файл конфигурации appsettings.json для работы с AAPM Console Tool

Indeed PAM Desktop Console

Ознакомьтесь с описанием Indeed PAM Desktop Console

Консоль пользователя

Получение доступа к ресурсам выполняется при помощи **консоли пользователя** — специальной оболочки для Indeed PAM Core. Доступна по следующему URL:

- **Windows:** https://pam.domain.local/uc
- **Linux:** https://pam.domain.local/uc

Обучение аутентификатора

Для работы с консолью пользователя необходимо обучить аутентификатор. Выполните вход в консоль, если пользователь не имеет аутентификатора, то он будет перенаправлен на IDP для его регистрации.

После успешной регистрации вы будете перенаправлены в консоль пользователя.

> **ПРИМЕЧАНИЕ**
>
> При превышении числа неверных попыток ввода OTP пользователь будет временно заблокирован (по умолчанию на 10 минут).
>
> Число неверных попыток ввода OTP и период блокировки аутентификатора определяется администратором PAM в разделе системные настройки.
>
> Для срочного разблокирования Администратору PAM необходимо сбросить аутентификатор заблокированному пользователю.

Получение доступа к ресурсу

В консоли пользователя отображаются разрешения на доступ к ресурсам. Для каждого разрешения указан:

- **Ресурс**.
- **Тип подключения**.
- Адрес подключения (**IP** или **DNS**).
- **Учетная запись**, от имени которой будет открыта сессия.

По каждому столбцу доступна сортировка. При вводе символов в поле для поиска совпадения будут выводиться по всем столбцам.

Если пользователю доступны произвольные ресурсы, то они будут отображаться в верхней части списка.

Для доступа к ресурсу нужно скачать RDP-файл. Это потребуется сделать только при первом подключении к ресурсу по выбранному разрешению. Сохраните файл и используйте при дальнейших подключениях. Скачанный RDP-файл можно использовать пока активно разрешение.

RDP-файл шлюза доступа PAM можно использовать для подключения к ресурсам независимо от доступных разрешений, потому что каждый раз при подключении к шлюзу будет отображаться актуальный список ресурсов.

При нажатии на строку с разрешением отображается дополнительная информация:

- **Период действия**.
- **Расписание доступа**.
- **Разрешение** — идентификатор разрешения, то есть порядковый номер разрешения в разделе **Разрешения** в консоли администратора.

Прямое подключение к ресурсу

1. Нажмите **Загрузить RDP-файл для подключения** справа от нужного разрешения.

   Для ресурсов, для которых доступно подключение и по RDP, и по SSH, по умолчанию отображается кнопка **Скопировать SSH-команду**. В этом случае чтобы скачать RDP-файл,

нажмите , а затем **Загрузить RDP-файл для подключения**.

2. Запустите RDP-файл для доступа к ресурсу.
3. Пройдите аутентификацию и настройте подключение.

> **ИНФОРМАЦИЯ**
>
> При открытии сессии можно выбрать локальные диски для использования в удаленной сессии. Подключиться без перенаправления локальных дисков тоже можно.

Подключение к шлюзу доступа

1. Нажмите **Подключиться к шлюзу доступа**, начнется скачивание RDP-файла.
2. Запустите этот RDP-файл.
3. Пройдите аутентификацию и настройте подключение.

Подключение к SSH Proxy

Для подключения к шлюзу SSH Proxy можно воспользоваться любым SSH-клиентом.

1. Запустите SSH-клиент.
2. Укажите адрес SSH Proxy и откройте соединение.
3. Пройдите аутентификацию.
4. Выберите ресурс для подключения.

Подключение по SSH напрямую

Справа от нужного разрешения до SSH-ресурса нажмите кнопку **Скопировать SSH-команду**. В буфер обмена скопируется SSH-команда для подключения к этому ресурсу.

Также можете написать SSH-команду вручную по указанному ниже шаблону.

Шаблон SSH-команды

```
ssh [user-name]#[resource]#[account-name]#[reason]@[proxy-address]
```

- `user-name` — имя пользователя
- `resource` — IP-адрес или DNS-имя ресурса
- `account-name` — имя привилегированной учетной записи
- `reason` — текст причины подключения
- `proxy-address` — IP-адрес или DNS-имя сервера SSH Proxy

Можно опустить любой параметр, кроме адреса сервера SSH Proxy. В этом случае SSH Proxy запросит эти параметры отдельно.

Если причина содержит пробелы, то указывайте ее в кавычках.

После выполнения команды SSH Proxy запросит пароль пользователя и TOTP.

Пример SSH-команды

```
ssh ivan.ivanov#ubuntu#webmaster#"system configuration"@pam
```

Подключение к ресурсу через PostgreSQL Proxy

GUI-клиент СУБД | **Консольный клиент СУБД Psql**

1. Нажмите **Показать данные для подключения**.
2. Откройте клиент СУБД и введите в его форму подключения данные, которые вы получили на предыдущем шаге:
   - **Адрес подключения**
   - **Порт подключения**
   - **Имя учетной записи**
   - **База данных по умолчанию**

3. Если в политике сессии включена опция **Требовать указать причину подключения**, то добавьте к полю **Имя учетной записи** текст причины подключения.

   Пример: если значение поля **Имя учетной записи** было `admin@company.local#1.1.1.1#MYCOMPANY\test-admin`, то с добавлением причины оно станет: `admin@company.local#1.1.1.1#MYCOMPANY\test-admin#"my reason to connect"`.

   Если эта опция отключена, то пропустите этот шаг.

4. Введите в форме подключения пароль своей учетной записи PAM.

Подключение к произвольному ресурсу

Произвольные ресурсы — это те ресурсы, которые не зарегистрированы в системе Indeed PAM. Этот вид подключения дает возможность подключаться к любым ресурсам по заранее определенным администратором PAM типам подключений.

1. Нажмите **Указать адрес подключения** справа от нужного разрешения до произвольного ресурса.

2. Выберите **Тип подключения**.

   > ⓘ **ПРИМЕЧАНИЕ**
   >
   > Доступные типы подключения определяются администратором PAM при выдаче разрешений.

3. Введите **Адрес подключения**.

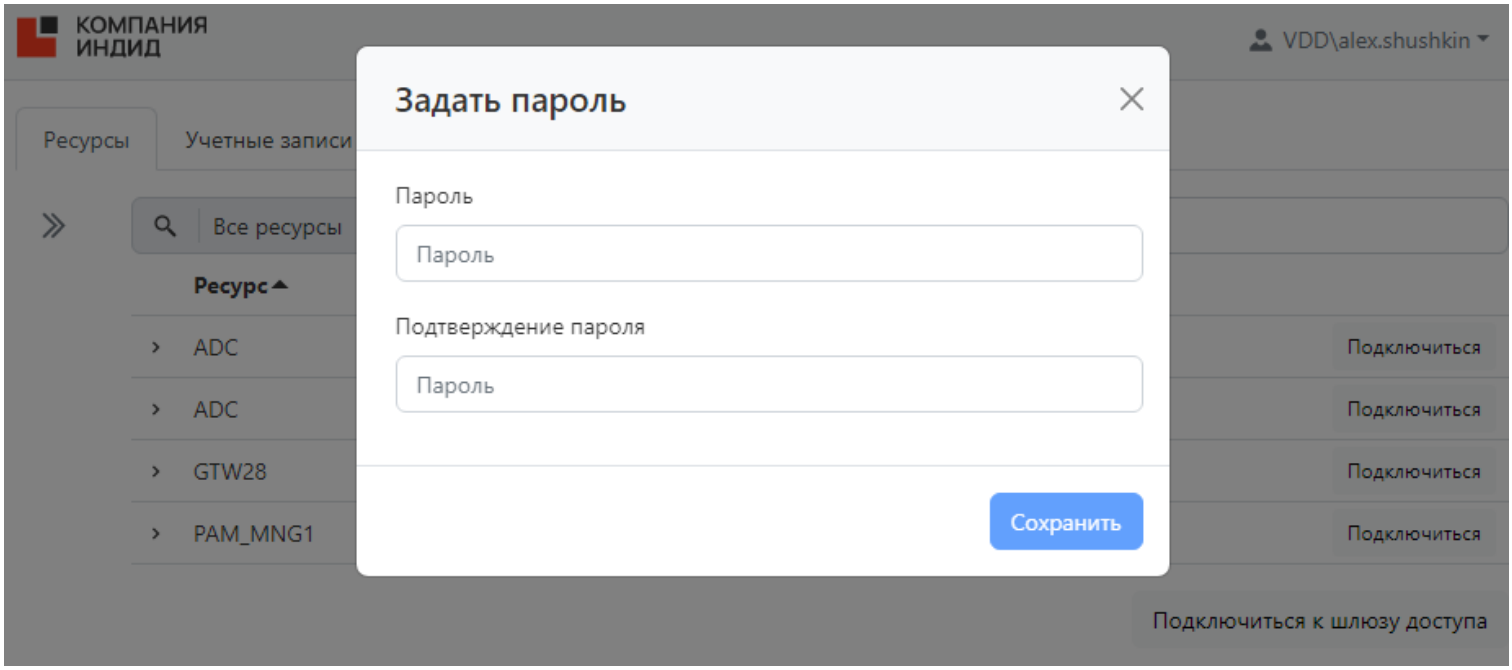
4. В зависимости от выбранного типа подключения нажмите одну из кнопок: **Скопировать SSH-команду** или **Загрузить RDP-файл для подключения**.

> ⓘ **ПРИМЕЧАНИЕ**
>
> Если у вас есть несколько разрешений (с разными типами) к произвольному ресурсу, а в окне **Подключение к произвольному ресурсу** в поле **Тип подключения** нет нужных вариантов, то проверьте **Расписание доступа** разрешений.

> Тип подключения не будет отображаться в поле **Тип подключения**, если пытаетесь подключиться по разрешению вне часов, указанных в **Расписании доступа**.

Задание пароля при подключении

При подключении к ресурсу у вас может быть запрошен пароль.



Это значит, что у учетной записи, от имени которой вам предоставлен доступ к ресурсу, отсутствует пароль. Подключиться к ресурсу с такой учетной записью нельзя. Обратитесь к вашему администратору PAM по вопросу подключения к этому ресурсу, так как только администратор может установить пароль учетной записи.

Завершение сессии

Для завершения сессии закройте окно удаленного подключения или выйдите из системы на ресурсе.

Подключение через SSH-клиенты

В этом разделе описаны способы SSH подключения через сторонние клиенты.

Подключение через шлюз доступа

Командная строка | **PuTTY** | **MobaXterm** | **SecureCRT**

1. Откройте консольную утилиту.
2. Введите строку подключения к SSH Proxy или Балансировщику. Можно использовать IP-адрес или DNS.

   ```
   ssh indeedproxy
   ```

   При необходимости укажите пользователя и порт.

   ```
   ssh user@indeedproxy -p 2222
   ```

3. Введите пароль и TOTP.
4. Выберите ресурс, к которому необходимо подключиться.

Подключение к конкретному ресурсу

Командная строка | **PuTTY** | **MobaXterm** | **SecureCRT**

1. Справа от нужного разрешения до SSH-ресурса нажмите кнопку **Скопировать SSH-команду**. В буфер обмена скопируется SSH-команда для подключения к этому ресурсу.
2. Вставьте скопированную строку в консольную утилиту.
3. Введите пароль и TOTP.

Командная строка

Подключение по SCP, SFTP, PSCP, PSFTP

WinSCP

WinSCP

FileZilla

FileZilla

Командная строка

SCP

> ⓘ **ПРИМЕЧАНИЕ**
>
> На устройствах под управлением ОС Windows Server 2019, Windows 10 1809 и старше команда SCP входит в состав предустановленных в клиенте OpenSSH.

Для передачи файлов по протоколу SCP можно использовать встроенную в ОС утилиту SCP. Используйте стандартную команду для копирования, но вместо адреса ресурса укажите адрес SSH Proxy:

Для ОС Windows:

```
scp -r C:\temp\configs\ ivan.ivanov@sshproxy.indeed-id.local:/tmp

scp -r C:\путь_до_локального_файла имя_пользователя@адрес_ssh_proxy:/
путь_куда_копировать_файл_на_ресурсе
```

Для ОС Linux:

```
scp -r /tmp ivan.ivanov@sshproxy.indeed-id.local:/tmp

scp -r /путь_до_локального_файла имя_пользователя@адрес_ssh_proxy:/
путь_куда_копировать_файл_на_ресурсе
```

Ключ -r означает рекурсивное копирование, то есть, если указать для копирования папку, то она она будет скопирована полностью со своим содержимым. Без этого ключа можно копировать только отдельные файлы.

Далее, после успешной аутентификации выберите номер ресурса для передачи файлов.

SFTP

На устройствах под управлением ОС Window для передачи файлов можно использовать утилиту sftp

Для передачи файлов:

1. Запустите командную строку
2. Подключитесь к серверу SSH Proxy

```
sftp ivan.ivanov@sshproxy.indeed-id.local
```

3. Выберите ресурс, к которому хотите подключиться
4. Передайте файлы с помощью команды:

```
put -r C:\temp\configs\ /tmp
put -r Путь_до_локальных_файлов Путь_до_файлов_на_ресурсе
```

   Ключ -r означает рекурсивное копирование, то есть, если указать для копирования папку, то она она будет скопирована полностью со своим содержимым. Без этого ключа можно копировать только отдельные файлы.

PSCP

> ⓘ **ПРИМЕЧАНИЕ**
>
> Для работы команд PSCP и PSFTP на устройстве должен быть установлен клиент PuTTY.

На устройствах под управлением ОС Window для передачи файлов можно использовать утилиту pscp

Команда для передачи файлов:

```
pscp -r C:\temp\configs\ ivan.ivanov@sshproxy.indeed-id.local:/tmp

pscp -r C:\путь_до_локального_файла имя_пользователя@адрес_ssh_proxy:/
путь_куда_копировать_файл_на_ресурсе
```

Ключ -r означает рекурсивное копирование, то есть, если указать для копирования папку, то она она будет скопирована полностью со своим содержимым. Без этого ключа можно копировать только отдельные файлы.

PSFTP

На устройствах под управлением ОС Window для передачи файлов можно использовать утилиту psftp

Для передачи файлов:

1. Запустите командную строку
2. Введите команду psft
3. Подключитесь к серверу SSH Proxy

```
open ivan.ivanov@sshproxy.indeed-id.local
```

4. Выберите ресурс, к которому хотите подключиться
5. Передайте файлы с помощью команды:

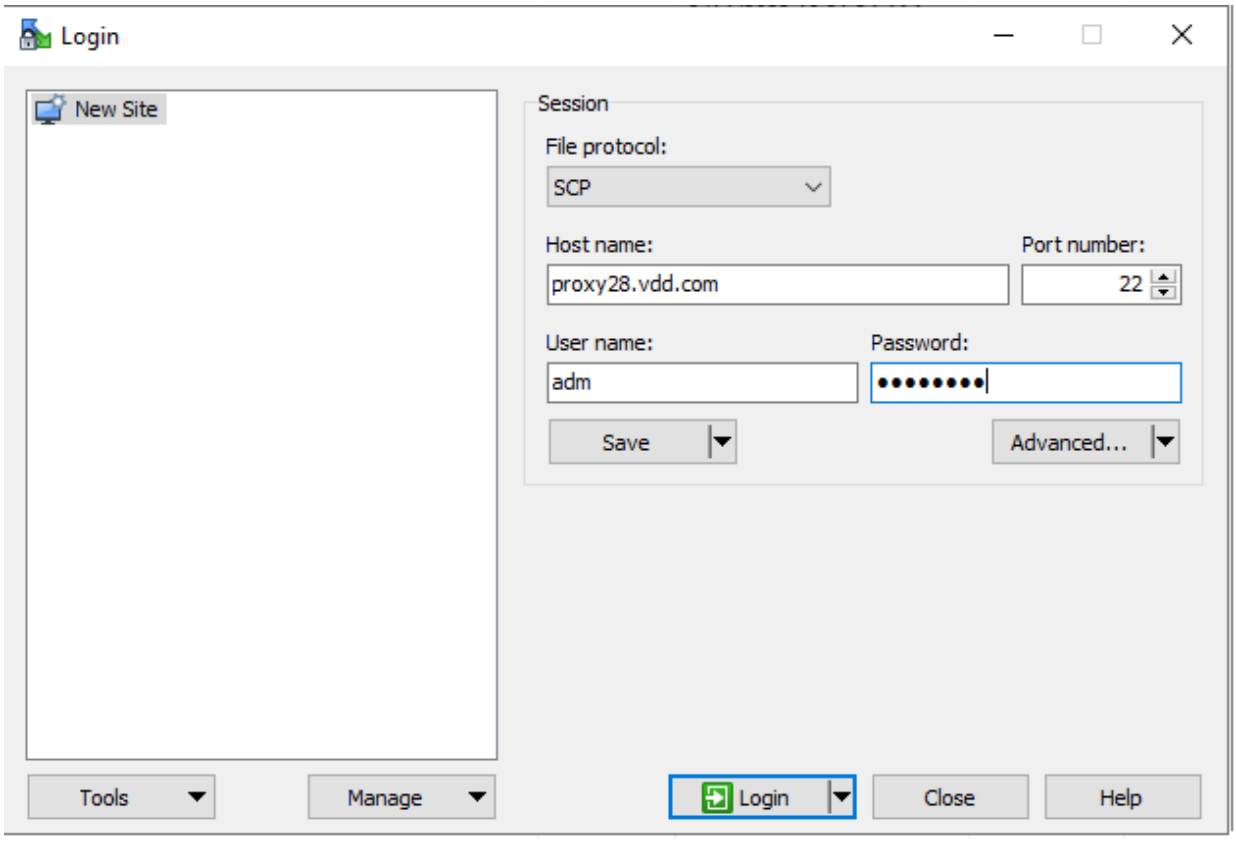
```
put -r C:\temp\configs\ /tmp/configs
put -r Путь_до_локальных_файлов Путь_до_файлов_на_ресурсе
```

   Ключ -r означает рекурсивное копирование, то есть, если указать для копирования папку, то она она будет скопирована полностью со своим содержимым. Без этого ключа можно копировать только отдельные файлы. Также обязательно нужно указать имя файла, которое будет сохранено на ресурсе.

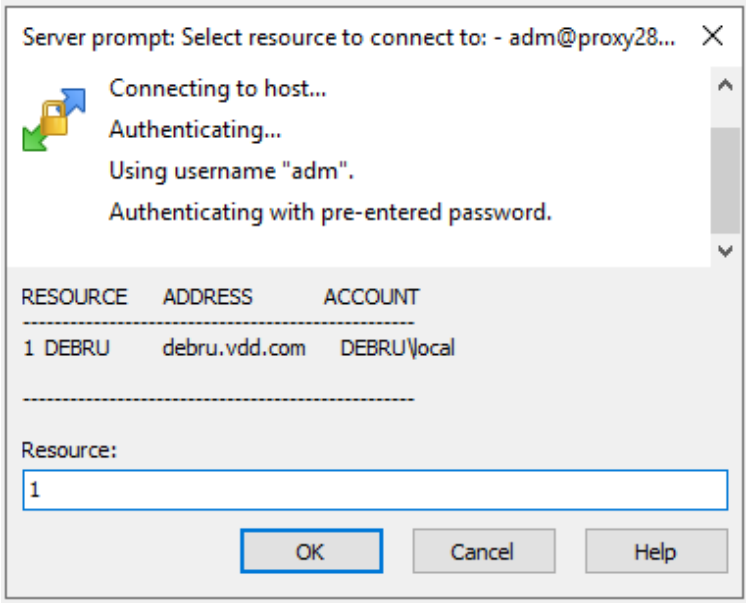
WinSCP

Подключение через шлюз доступа

1. Откройте клиент WinSCP
2. Выберите "File protocol" **SCP** или **SFTP**. Введите адрес и порт подключения сервера SSH Proxy в поля "Host Name" и "Port number". Введите логин и пароль в поля "User name" и "Password".

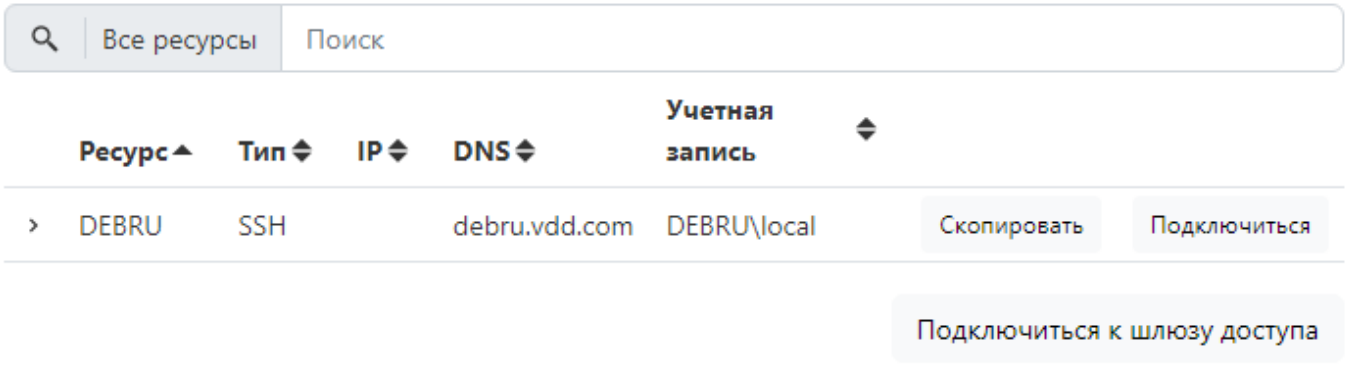


3. Нажмите кнопку "Login" и выберите ресурс, к которому хотите подключиться



Подключение напрямую к ресурсу

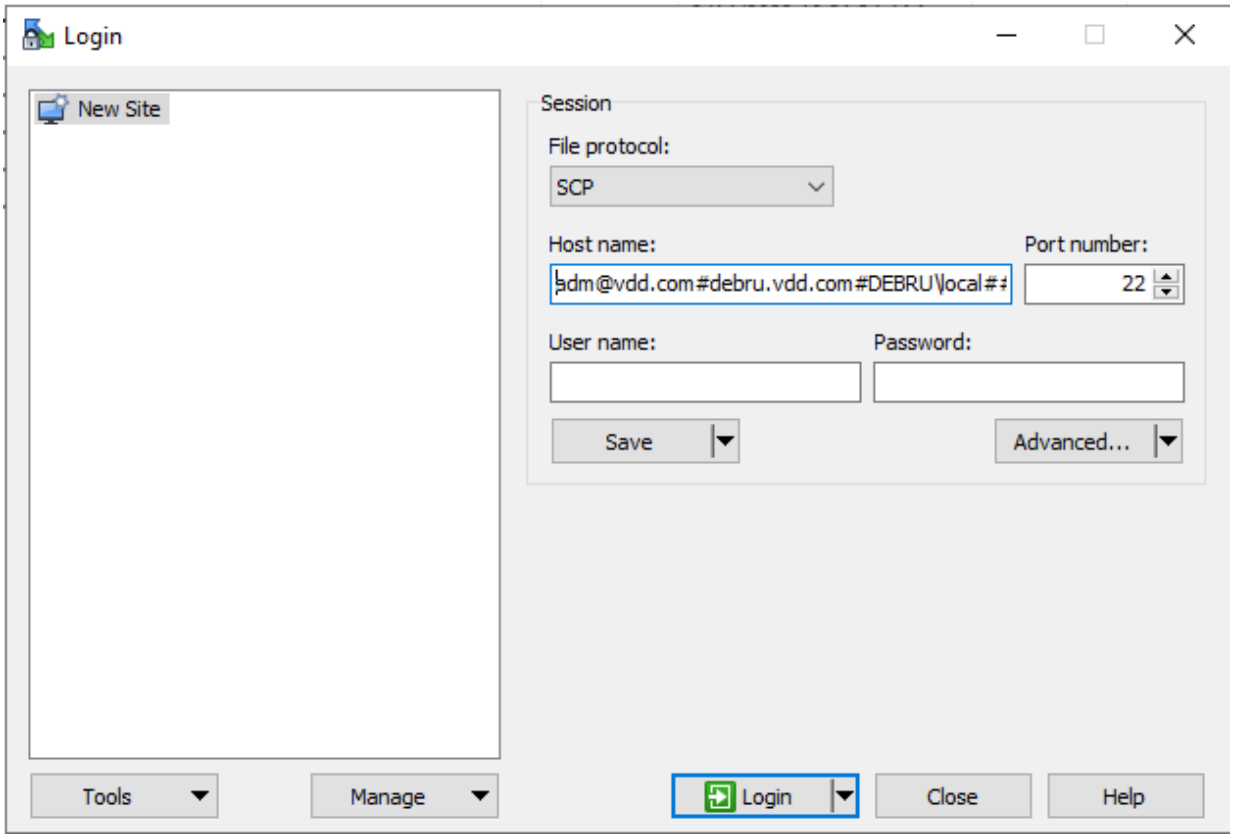
1. Перейдите в консоль пользователя и скопируйте строку подключения к ресурсу.



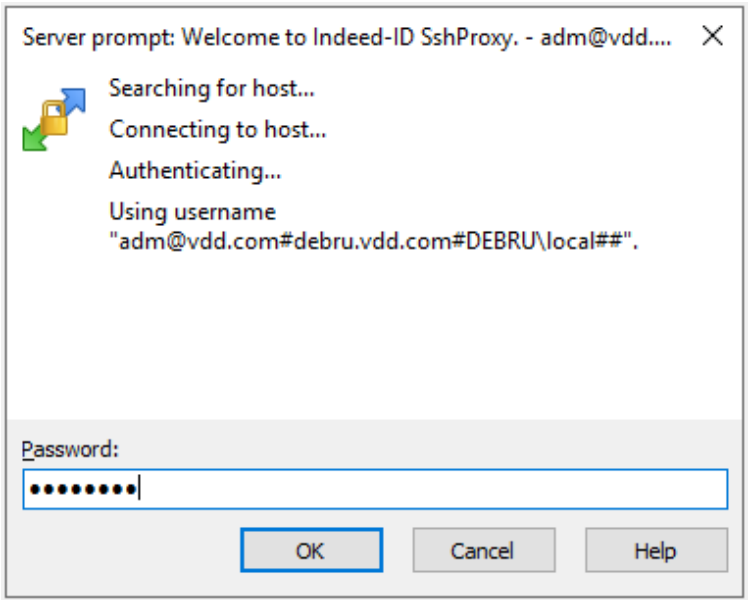
2. Откройте клиент WinSCP.

3. Выберите "File protocol" **SCP** или **SFTP**. Вставьте строку подключения в пункт "Host name", удалив из строки кавычки и ssh. Строка подключения должна выглядеть следующим образом:

```
adm@vdd.com#debru.vdd.com#DEBRU\local##@proxy28.vdd.com
```



4. Введите свой пароль.



FileZilla

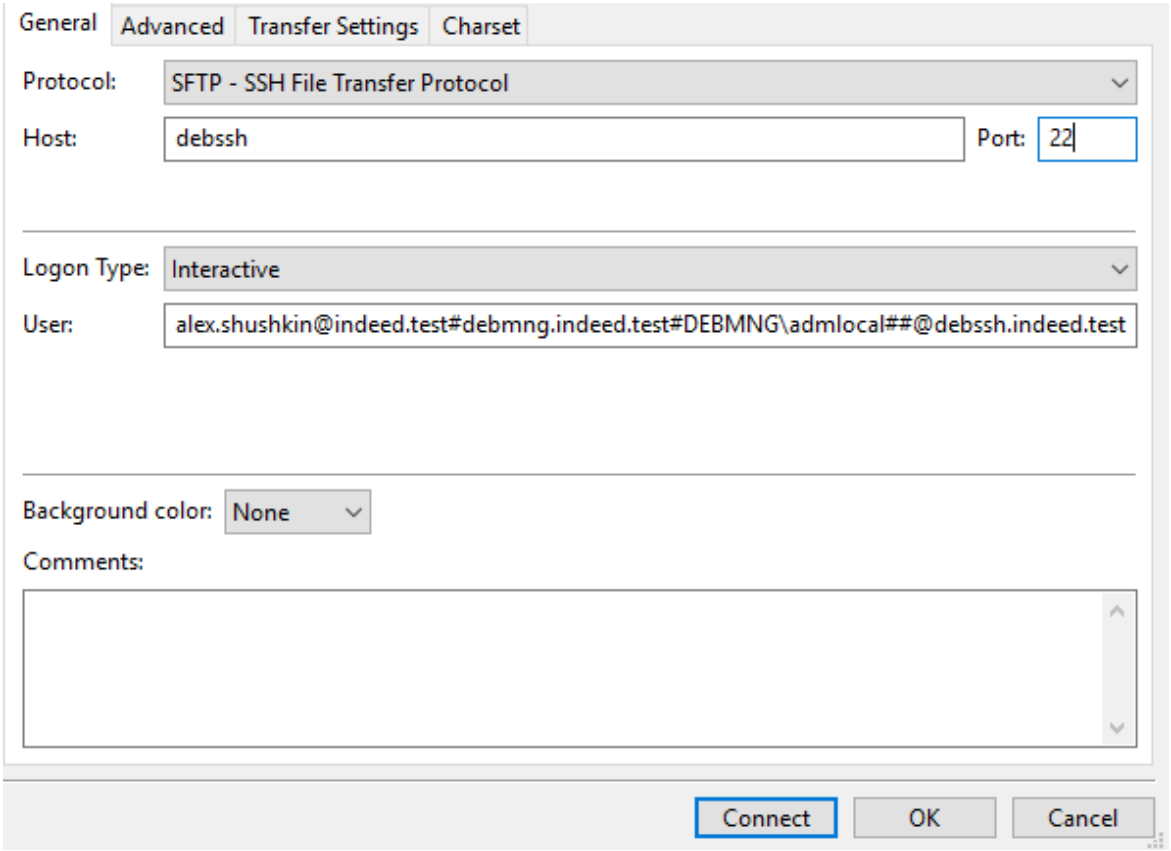
SFTP подключение к ресурсу

Для настройки SFTP подключения в клиенте FileZilla необходимо:

1. Перейдите в **File** → **Site Manager** → **New site**.

2. Заполните раздел **General**:

    - Protocol: SFTP — SSH File Transfer Protocol
    - Host: Адрес сервера SSH Proxy
    - Port: Порт сервера SSH Proxy
    - Logon Type: Interactive
    - User: строка подключения, скопированная из **UC** для подключения к ресурсу. Из строки необходимо удалить "SSH" и кавычки.



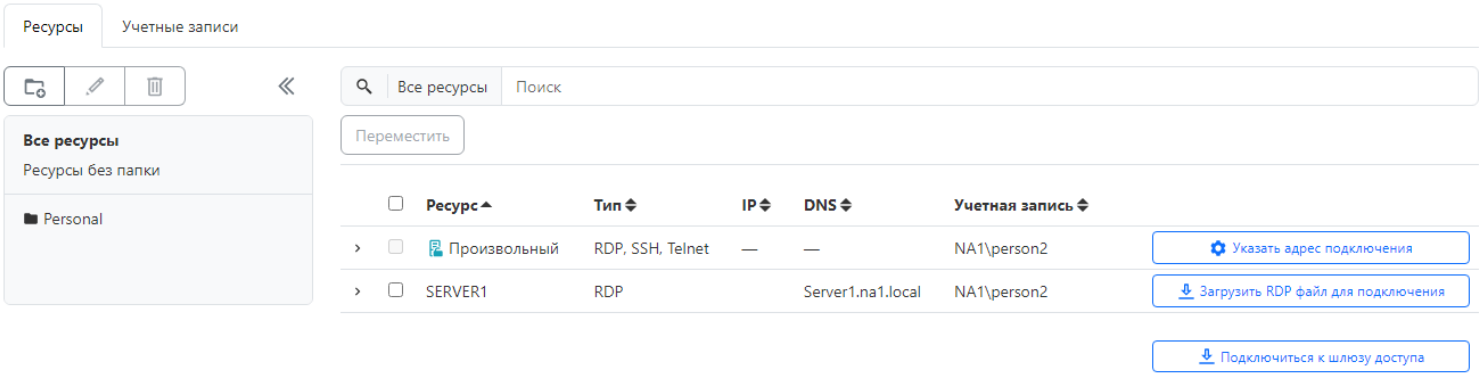
3. Перейдите в раздел **Transfer Settings** и включите настройку **Limit number of simultaneous connections**. Установите значение параметра **Maximum number of connections** равное 1.

4. Нажмите кнопку **Connect**.

> ⓘ **ПРИМЕЧАНИЕ**
>
> FileZilla не поддерживает SCP-соединение.

Личные папки ресурсов

Раздел предназначен для работы с личными папками ресурсов пользователей.



Для создания личной папки необходимо:

- Перейдите в раздел **Ресурсы**, нажмите значок папки .
- Введите новое имя папки и нажмите **Сохранить**.

Можно редактировать название папки:

- Перейдите в раздел **Ресурсы**.
- Выберите папку и нажмите значок карандаша .
- Введите новое имя папки и нажмите **Сохранить**.

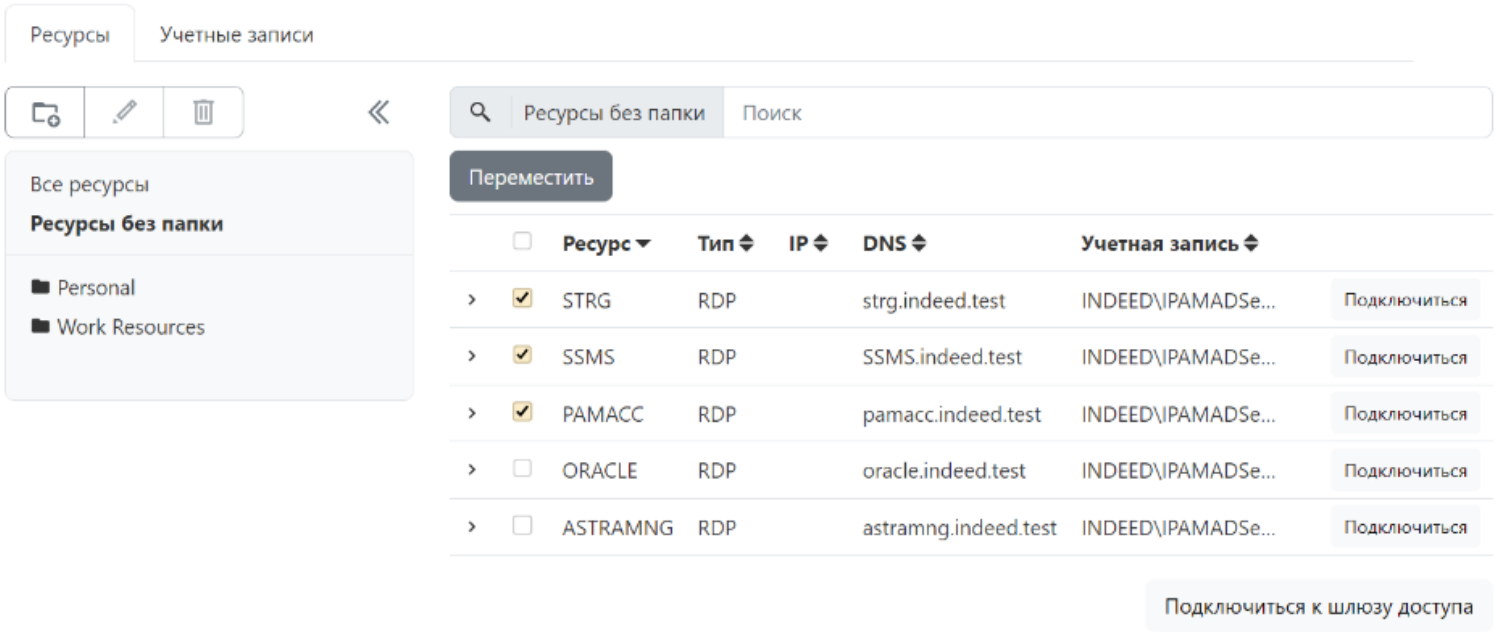
Можно удалить папку:

- Перейдите в раздел **Ресурсы**.
- Выберите папку и нажмите значок корзины .
- Подтвердите удаление папки.

Для добавления ресурсов в папку необходимо:

- Перейдите в раздел **Ресурсы** и нажмите **Все ресурсы** или **Ресурсы без папки**.
- Отметьте ресурсы, которые необходимо переместить в папку.
- Нажмите кнопку **Переместить**.
- Выберите нужную папку и нажмите **Сохранить**.

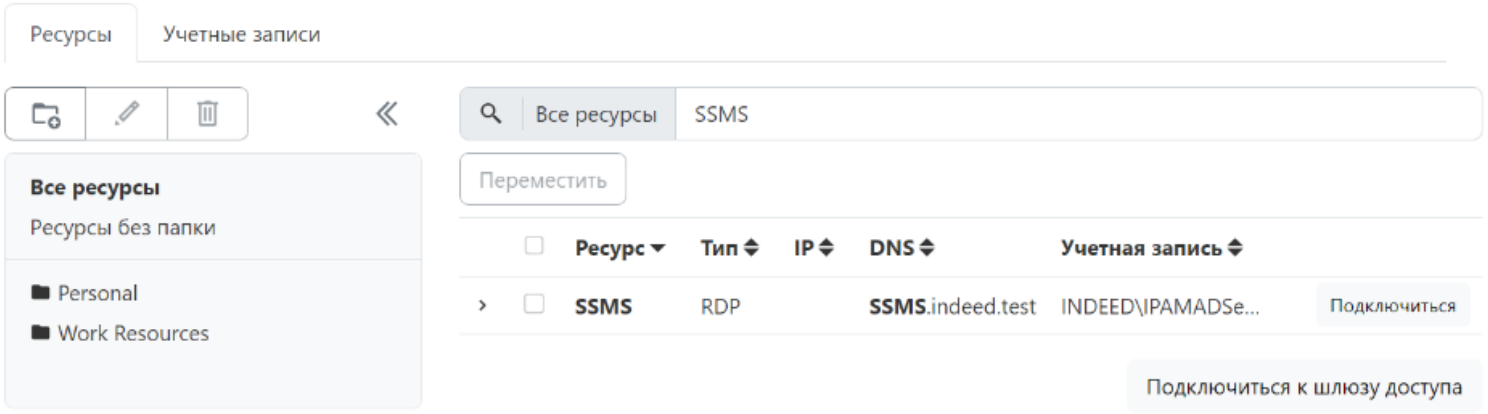
> **ПРИМЕЧАНИЕ**
>
> Добавление произвольных ресурсов в папки не поддерживается.



Можно выполнить поиск по ресурсам:

- Перейдите в раздел **Ресурсы**.
- Выберите папку, **Все ресурсы** или **Ресурсы без папки**.
- В поисковой строке введите имя ресурса.

> **ПРИМЕЧАНИЕ**
>
> Произвольные ресурсы можно найти по запросу "adhoc".



Выполнение команд с привилегией root

Для выполнения команд с привилегией root, аналогично sudo используется команда pamsu. Отличие заключается в том, что аутентификация будет запрашиваться у пользователя PAM, а не привилегированной УЗ от имени которой открыта сессия.

Пример:

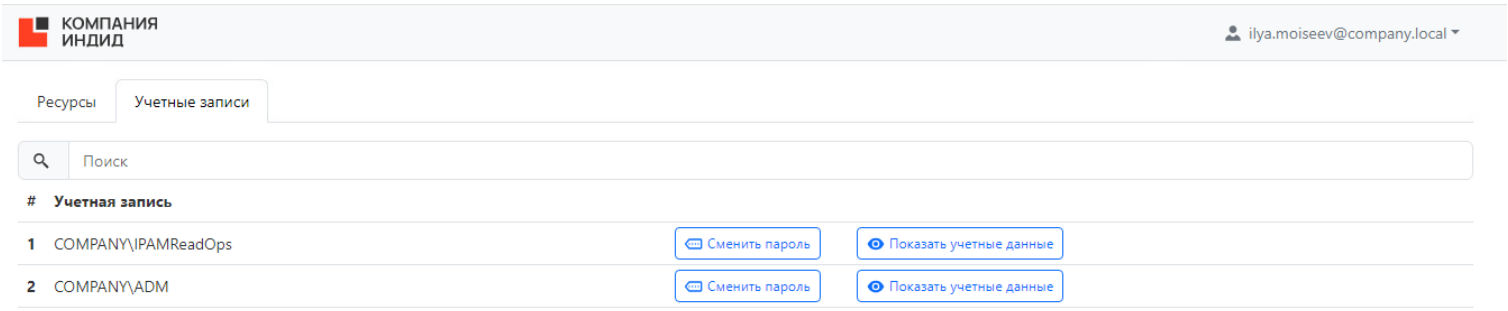
```
[administrator@centos7su ~]$ pamsu ls -la /etc/ssl
Password for indeed-id\ivan.ivanov:
total 12
drwxr-xr-x. 4 root root 68 Sep 22 19:20 .
drwxr-xr-x. 75 root root 8192 Sep 22 17:49 ..
drwxr-xr-x. 2 root root 123 Sep 22 19:30 CA
lrwxrwxrwx. 1 root root 21 Sep 22 15:51 cert.pem -> /etc/pki/tls/cert.pem
lrwxrwxrwx. 1 root root 16 Nov 23 2020 certs -> ../pki/tls/certs
[administrator@centos7su ~]$
```

Операции с учетными записями

Поиск учетных записей

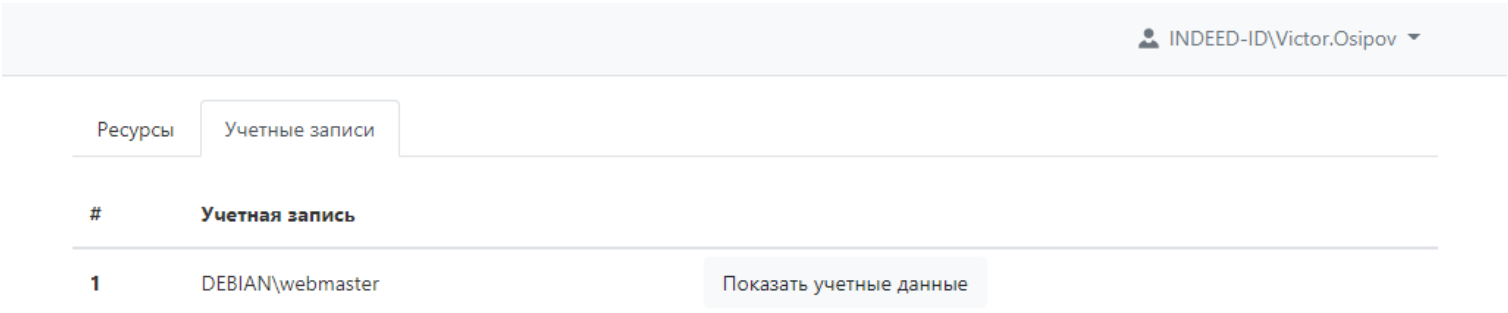
Поиск позволяет отобразить только те учетные записи, которые удовлетворяют заданному критерию.

Поиск учетных записей работает аналогично поиску ресурсов.



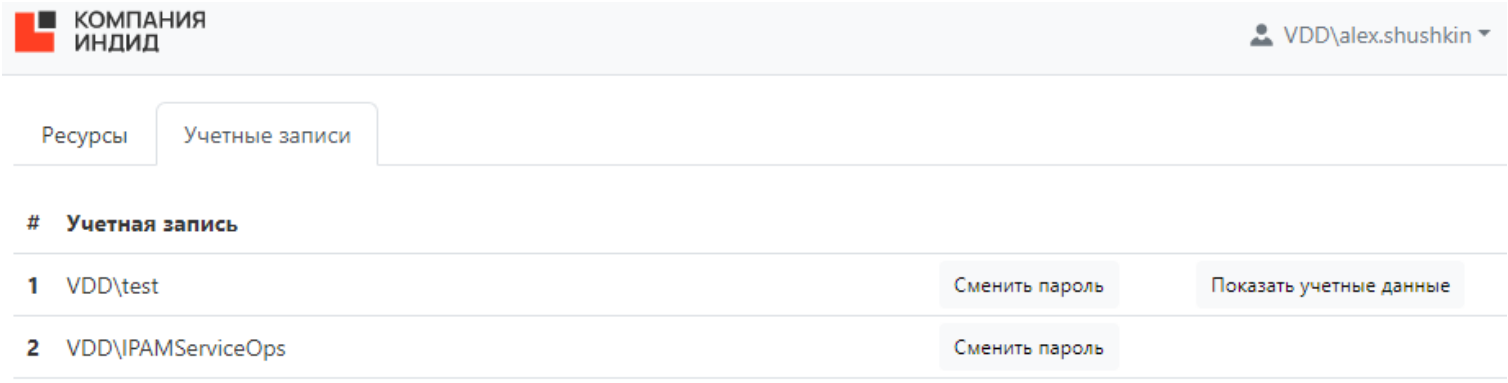
Просмотр пароля и SSH-ключа учетной записи

Если пользователь имеет разрешение, в котором включена опция **Разрешить просмотр учетных данных**, то в разделе **Учетные записи** будут доступны соответствующие данные. Для просмотра нажмите **Показать учетные данные**, введите причину просмотра и подтвердите свои действия.

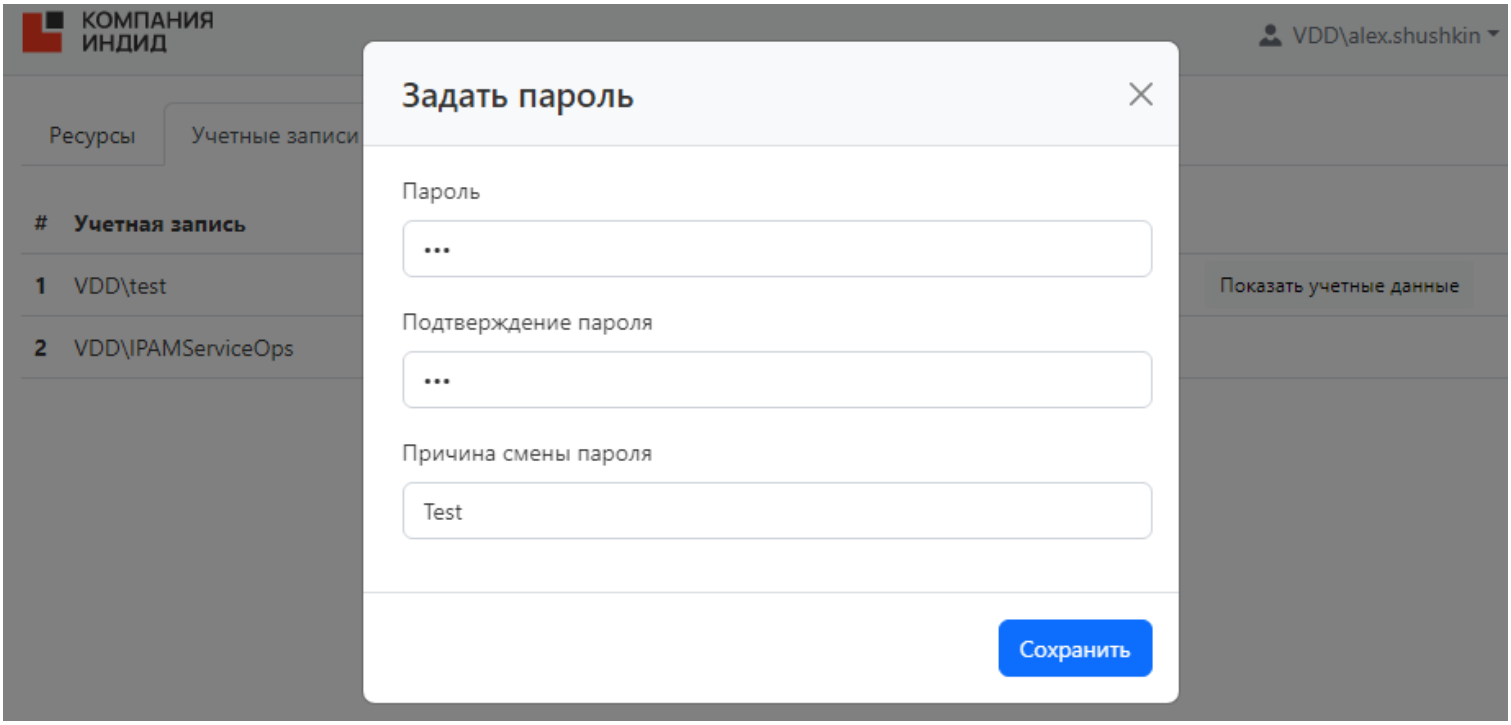


Смена пароля и SSH-ключа учетной записи

Если пользователь имеет разрешение, в котором включена опция **Разрешить изменение учетных данных**, то в разделе **Учетные записи** будет доступно редактирование пароля учетной записи.



Для смены пароля нажмите нажмите **Сменить пароль**, введите новый пароль, введите причину и подтвердите свои действия.



Работа с AAPM Console Tool

Pam.Tools.Aapm — консольная утилита для автоматизированного получения паролей или SSH ключей учетных записей Приложениями.

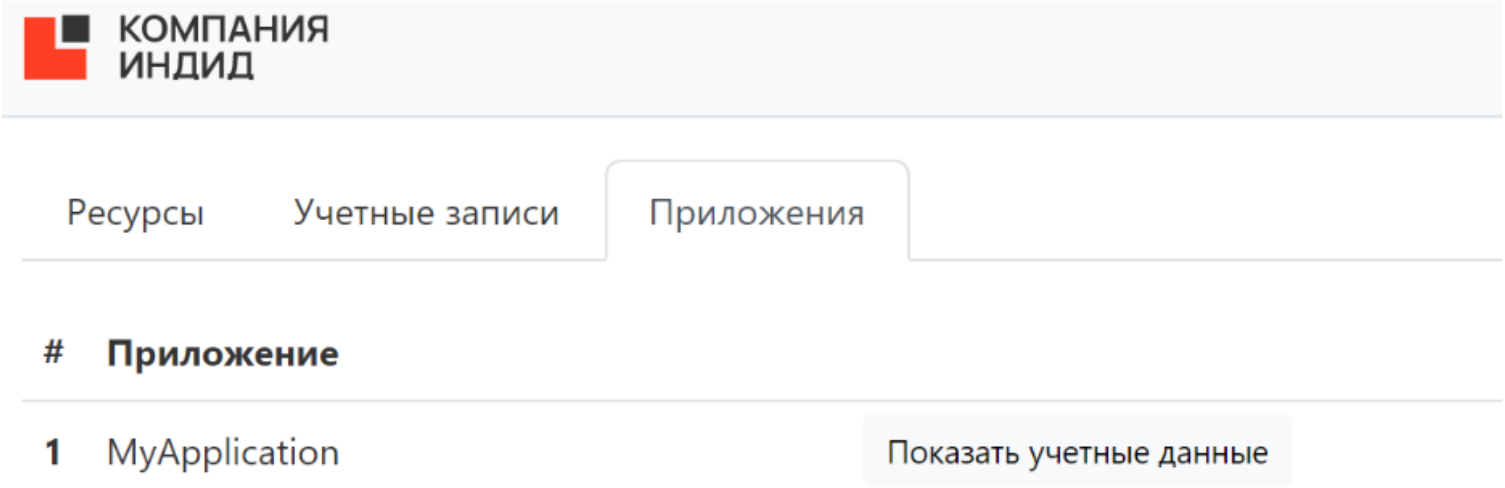
Путь: **IndeedPAM_3.0_RU\indeed-pam-tools\aapm**

Настройка консольной утилиты

Для настройки консольной утилиты необходимо отредактировать файл appsettings.json:

Секция `Auth`:

- `Auth.Username` — имя Приложения.
- `Auth.Password` — пароль Приложения. Чтобы получить пароль, перейдите в UC → Приложения → Показать учетный данные.



Секция `Endpoints`:

- `CoreUrl` — адрес Core
- `IdpUrl` — адрес Idp

Пример настройки:

```
{
  "Auth": {
    "Username": "MyApplication",
```

```
    "Password": "M3YTy;[j;q&*DrZQSl(?B1agm$7uS+",
  },
  "Endpoints": {
    "CoreUrl": "https://debmng.indeed.test/core",
    "IdpUrl": "https://debmng.indeed.test/idp"
  }
```

Использование консольной утилиты

Windows

Для запуска консольной утилиты откройте терминал, перейдите в папку с утилитой и выполните команду **.\Pam.Tools.Aapm.exe**.

Возможные параметры:

```
 get-accounts    Get accounts for which the application can view credentials.

 get-ssh-key     Gets SSH key for specified account. Passphrase for the key will be written in stdout
stream, the key will be saved in the output path

 get-password    Gets password for specified account

 help            Display more information on a specific command.

 version         Display version information.
```

Примеры использования:

1. Ввод: **./Pam.Tools.Aapm.exe get-password --name INDEED\IPAMADServiceOps**

```
PS C:\Users\adm\Desktop\IndeedPAM_2.8.0_RU_Linux\MISC\Aapm> ./Pam.Tools.Aapm.exe get-password --name INDEED\IPAMADServiceOps
Qwerty1!
```

2. Ввод: **./Pam.Tools.Aapm.exe get-accounts**

```
PS C:\Users\adm\Desktop\IndeedPAM_2.8.0_RU_Linux\MISC\Aapm> .\Pam.Tools.Aapm.exe get-accounts
3 accounts available:
    - INDEED\IPAMADServiceOps
    - DEBIAN\admlocal
    - CENTOS\admlocal
```

Linux

> ⚠ **ВАЖНО**
>
> Убедитесь, что dotnet-runtime-8.0 установлена.

Чтобы запустить консольную утилиту, откройте терминал, перейдите в папку с утилитой:

```
cd IndeedPAM_3.0_RU\indeed-pam-tools\aapm\
```

и вызовите команду `Pam.Tools.Aapm.dll` с нужным аргументом.

Пример использования:

Ввод
`dotnet Pam.Tools.Aapm.dll get-accounts`

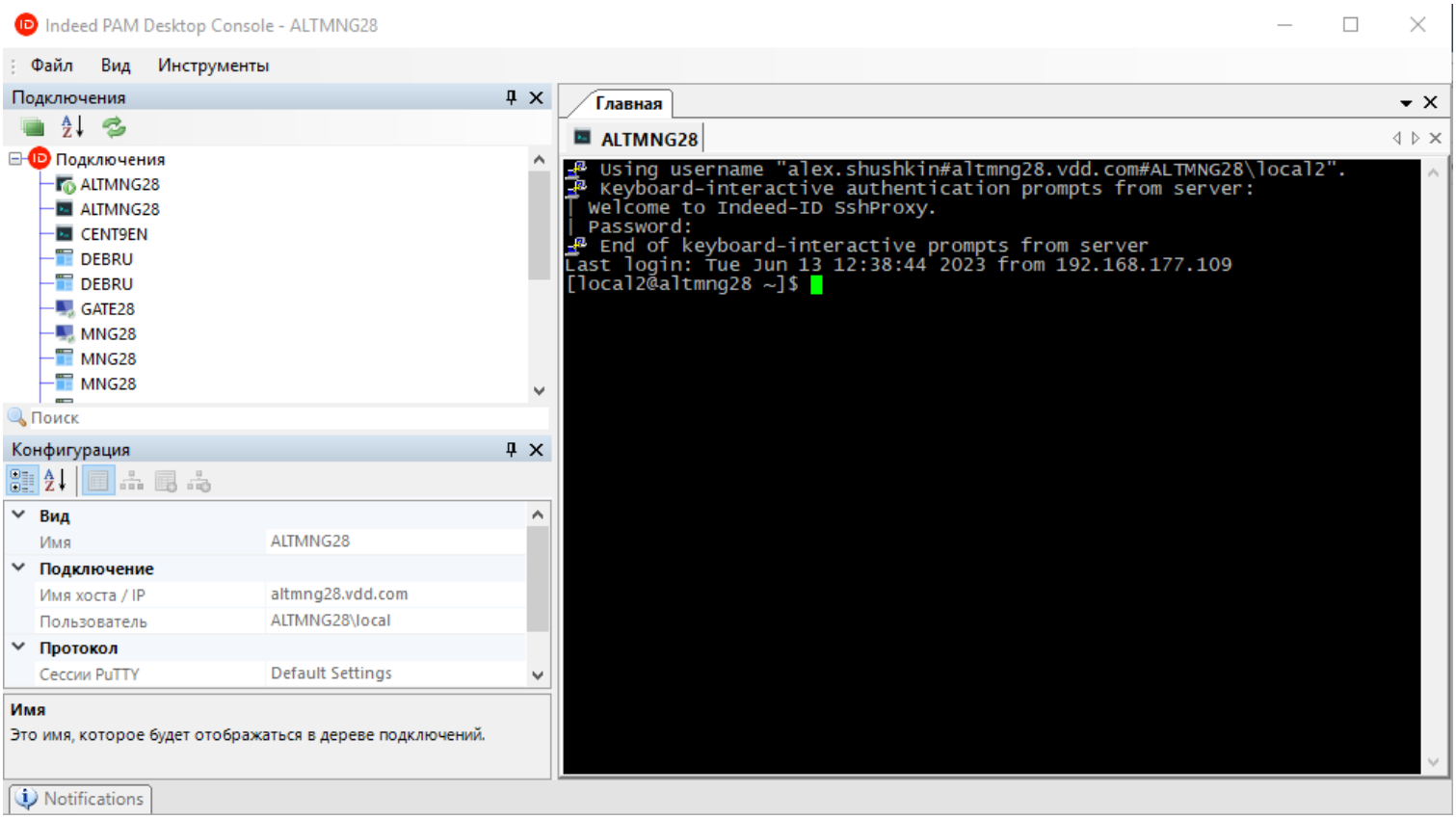
Indeed PAM Desktop Console

Установка и настройка приложения происходит в соответствии с документацией.

Desktop Console представляет собой Windows приложение, которое можно использовать вместо Web консоли пользователя.

Чтобы запустить утилиту Desktop Console, убедитесь, что вы вошли в систему с учетной записью Active Directory (в противном случае запустите утилиту Desktop Console от имени учетной записи пользователя Active Directory), дважды нажмите ярлык Indeed PAM Desktop Console, появится окно аутентификации PAM. Обучите или введите код TOTP. После успешной аутентификации вы увидите доступные ресурсы на панели **Подключения**.

Чтобы открыть соединение, дважды нажмите на нужный ресурс (также можно нажать правой кнопкой мыши и выбрать пункт меню **Подключиться**) и завершить аутентификацию. Вы можете открыть несколько подключений одновременно.



Настройка и сбор логов

Ознакомьтесь с информацией о логировании

Техническая поддержка

Как создать обращение в поддержку

Настройка и сбор логов

Расположение логов

Логи всех .Net компонентов и утилит пишутся в текстовые файлы, расположенные в папках `logs`:

- `/etc/indeed/indeed-pam/logs/Имя_Компонента/`
- `C:\inetpub\wwwroot\Имя_Компонента\logs\`
- `C:\Program Files\Indeed\Indeed PAM\Gateway\ProxyApp\logs\`
- `[indeed-pam-windows\MISC]\папки утилит\logs\`

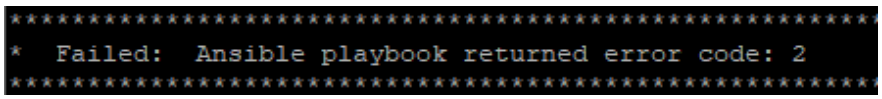
Описание логов компонентов Core, IDP, LS

Файл	core	idp	LS	Содержимое
commands.log	+	+		все логи команд
queries.log	+	+		все логи запросов
errors.log	+	+	+	все ошибки PAM/LS
jobs.log	+			все логи задач (job)
events.log	+			все логи, связанные с Событиями
connections.log	+			все логи сервисных подключений
db.log	+	+	+	логи, связанные с доступом к БД
hangfire.log	+	+	+	все логи от Hangfire
ils.log	+			все логи от LogServer client
full-yyyy-MM-dd.log	+	+	+	все логи PAM/LS с указанием имени логгера и traceId

Файл	core	idp	LS	Содержимое
stdout_yyyyMMddHHmmss_xxxx.log	+	+	+	логи с ошибками от IIS

Логирование скрипта установки

Скрипт установки run-deploy.sh может прерваться с ошибкой. В этом случае нужно отправить файл с логами в техническую поддержку.

Пример ошибки скрипта: 

Расположение файла с логами: *indeed-pam-linux/logs/deploy.log*.

По умолчанию в логи записывается краткая информация. Чтобы получить расширенный вывод логов нужно запустить скрипт с опцией `-vvv`:

```
run-deploy.sh -vvv
```

ProxyApp

Логи пишутся в папку `C:\Program Files\Indeed\Indeed PAM\Gateway\ProxyApp\logs\``shortDate\processId`, чтобы разделить логи от нескольких запусков в один день. В папке может быть 2 файла с логами:

- `ffmpeg.log` — отладочная информация от ffmpeg
- `Pam.Proxy.App.log` — все прочие логи

Утилиты

Все логи пишутся в один файл без даты в имени, с названием утилиты, например `Pam.Tools.Migrator.log`

Логирование нативных компонент

К нативным компонентам относятся:

- MstscAddin
- WindowsAgent
- Pam.Service
- Pam.Putty
- ProcessCreateHook

Для включения / получения логов можно использовать утилиту Indeed GetLog. Логи сохраняются в директорию `C:\\Windows\\System32\\LogFiles\\Indeed-ID`. Для каждого процесса создается своя отдельная директория.

Логирование в nix компонентах

SSH Proxy

Все логи пишутся в один файл, `${ISODate}.log`.
Файлы располагаются по пути `/etc/indeed/indeed-pam/logs/ssh``/`

PAMSU

Все логи, генерируемые нашим кодом, пишутся в один файл, `${ISODate}.log`.
Файлы располагаются по пути `/opt/Indeed-PAM/pamsu/logs/`.

Помимо этого существует возможность активировать логирование кода, предоставленного `sudo`.
Это делается через изменения в файле `/etc/pamsu.conf` . Правила настройки и управления такие же как у `sudo`. См.: `man sudo.conf`

Настройка логирования

Конфигурация логирования компонентов .Net находится в файлах appsettings.json.

Настройка appsettings.json

Файлы appsettings.json располагаются по пути:

- **C:\inetpub\wwwroot\Имя_Компонента\appsettings.json** — сервер управления Windows
- **C:\Program Files\Indeed\IndeedPAM\Gateway\ProxyApp\appsettings.json** — сервер доступа Windows

- **/etc/indeed/indeed-pam/Имя_Компонента/appsettings.json** — сервер управления или доступа Linux

Секция NLog

- Параметр **variables** — раздел, в котором можно задать переменные для дальнейшей настройки логирования. Количество переменных не ограничено. (не обязательный параметр).

```
"variables":  {
               "minLevel":  "Trace",
               "dbMinLevel":  "Info"
               }
```

> **ПРИМЕЧАНИЕ**
>
> Чтобы вызывать заданную переменную при дальнейшей настройке ее необходимо будет записывать в виде **${Имя_Переменной}**

Для каждого лога можно настроить свой уровень логирования.

Существуют следующие уровни логирования:

Уровень логирования	Порядковый номер	Строгость логирования
Trace	0	Самый подробный уровень. Используется для разработки и редко используется в производстве.
Debug	1	Отладка поведения приложения по интересующим внутренним событиям.
Info	2	Информация, отражающая ход выполнения или события жизненного цикла приложения.
Warn	3	Предупреждения о проблемах проверки или временных сбоях, которые можно устранить.
Error	4	Ошибки, при которых функциональность не удалась или было получено исключение.

Уровень логирования	Порядковый номер	Строгость логирования
Fatal	5	Самый критический уровень. Приложение будет прервано.

Обычная конфигурация заключается в указании минимального уровня, в который включены этот уровень и более высокие уровни. Например, если минимальный уровень равен Info, то Info, Warn, Error и Fatal регистрируются, но Debug и Trace игнорируются.

- Параметр **rules** — определяет правила маршрутизации логов.
  - У каждого типа лога есть свое **имя**, которое не рекомендуется редактировать.

```
"Rules": {
"03_Hangfire": {
        "logger": "Hangfire.*",
        "minLevel": "Info",
        "writeTo": "hangfireFile",
        "final": true
      },
"20_Errors":  {
        "logger":  "*",
        "minLevel":  "Error",
        "writeTo":  "errorsFile"
              },
"40_Commands": {
        "logger": "Idp.Application.*Command",
        "minLevel": "${minLevel}",
        "writeTo": "commandsFile",
        "Enabled": false
      },
}
```

Для каждого типа лога можно указать следующие теги:

logger — Имя логгера — обычно это имя ассоциированного со строчкой лога элемента в коде (имя класса). Может содержать подстановочные символы (* и ?) Таким образом имя правила '*' соответствует любому имени логгера, а 'Common*' соответствует всем логгерам, чьи имена начинаются с 'Common'. Не рекомендуется редактировать этот параметр.

LogLevel — уровни логирования, можно указать сразу несколько:

1. **minlevel** — минимальный уровень логирования
2. **maxlevel** — максимальный уровень логирования
3. **level** — один уровень для логирования
4. **levels** — уровни логирования, записанные через запятую

writeTo — разделенный запятыми список файлов для записи логов

final — Если текущее правило помечено как **final** и его имя соответствует имени логгера, то NLog завершает на нем построение цепочек для всех уровней логирования, включенных для данного правила. Или Логи, помеченные как final, перестают записываться в логи, находящиеся по цепочке ниже.

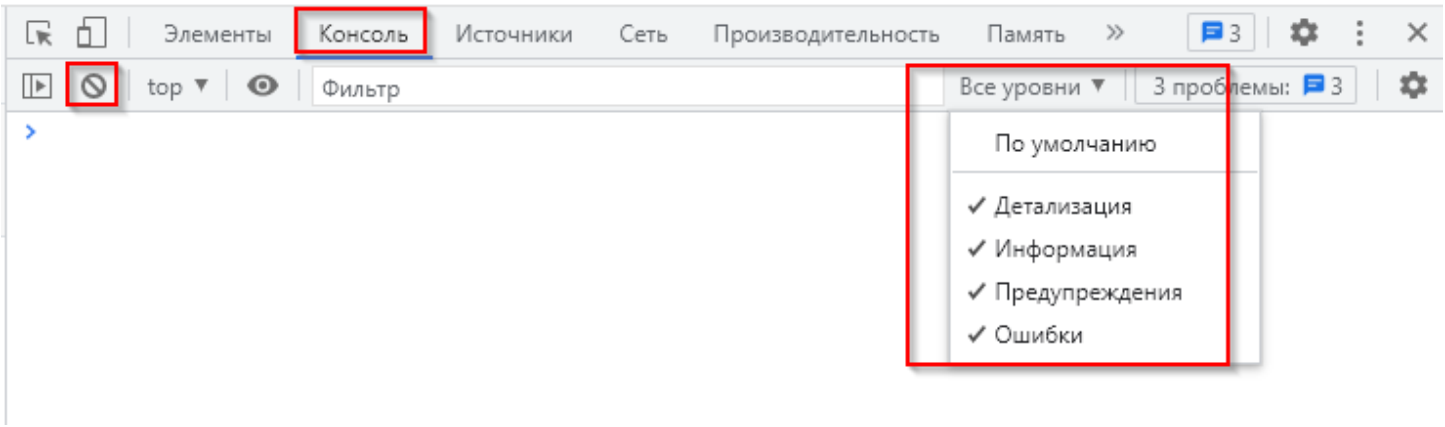
enabled — для отключения правила логирования без его удаления необходимо проставить флаг **false**

- Параметр **targets** – определяет log targets/outputs (необязательный параметр)
- Параметр **extensions** – загружает расширения NLog из файла *.dll (необязательный параметр)
- Параметр **include** – включает внешний конфигурационный файл (необязательный параметр)

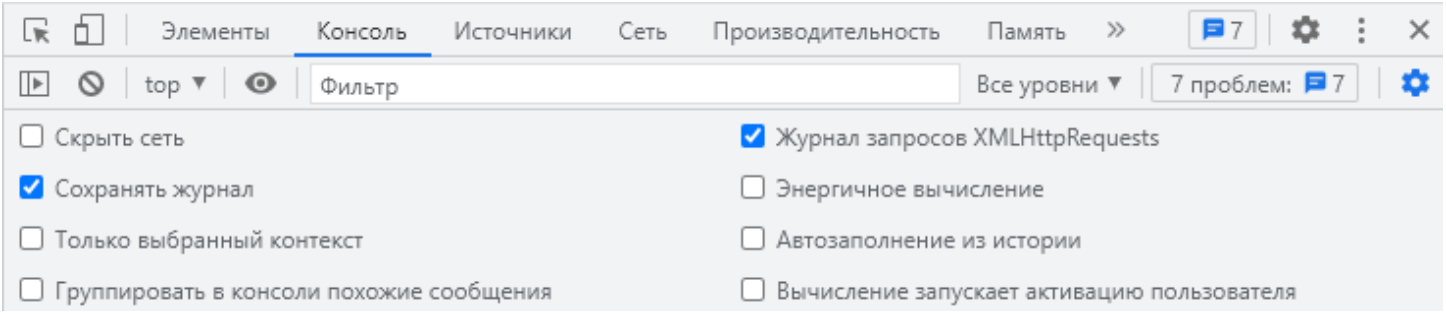
Сборка логов из браузера

Chrome, Edge, Yandex

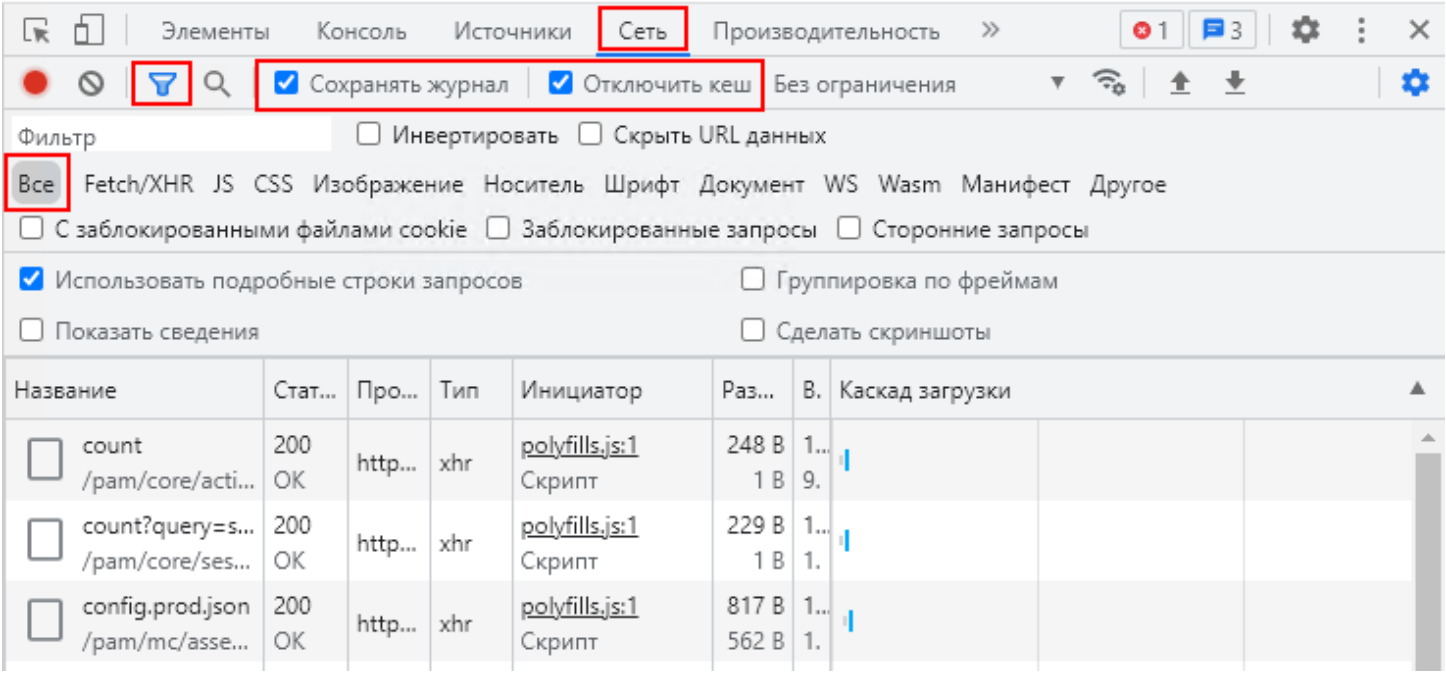
1. Запустите браузер, перейдите на страницу в которой выходит ошибка, запустите **Инструменты разработчика** (нажмите Ctrl+Shift+I или F12).
2. Во вкладке **Консоль** нажмите иконку для очистки консоли, включите опции **Детализация**, **Информация**, **Предупреждения**, **Ошибки**:



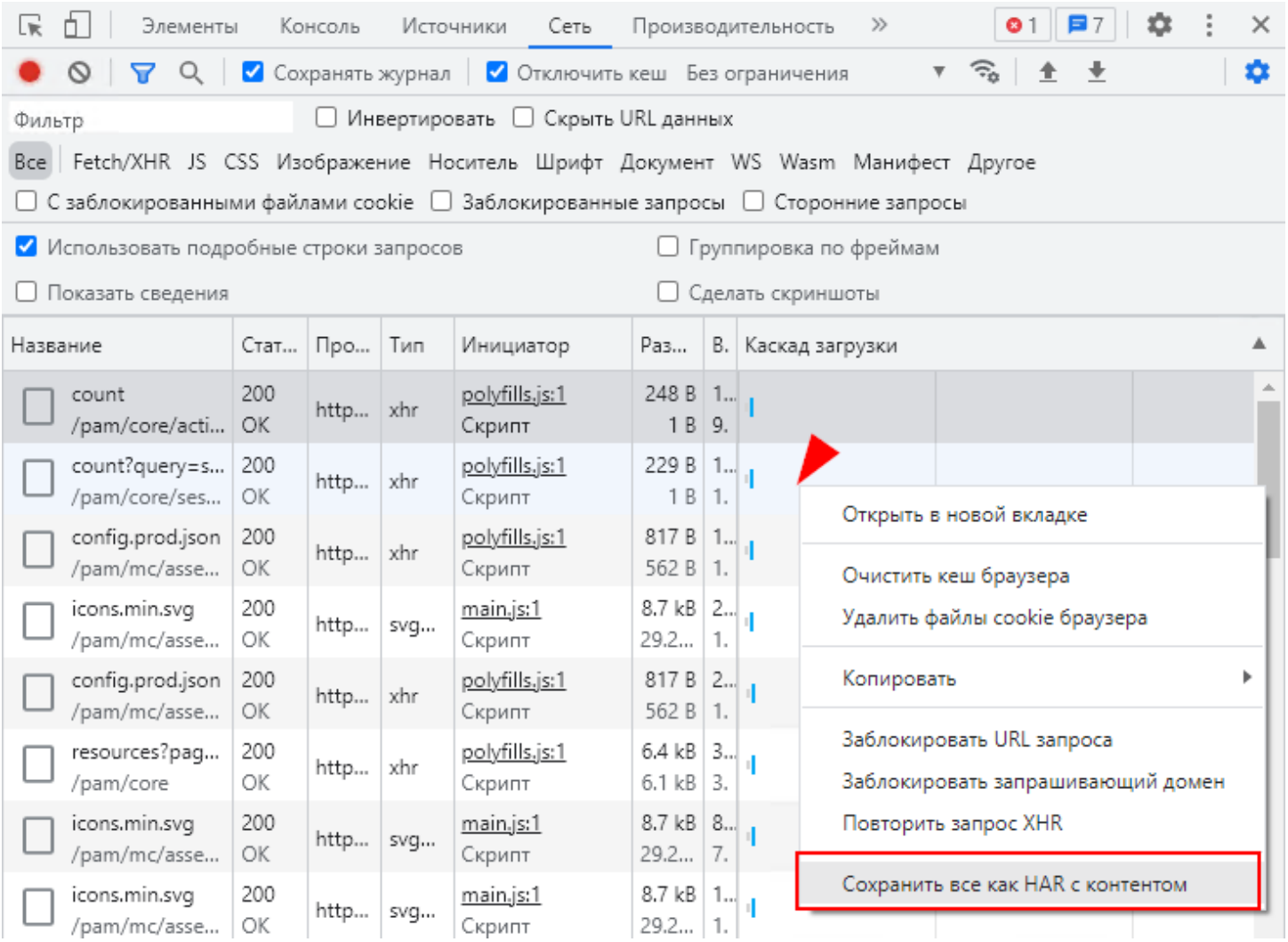
3. Нажмите значок шестеренки (Настройки консоли) и отметьте опции **Сохранять журнал**, **Журнал запросов XMLHttpRequests**:



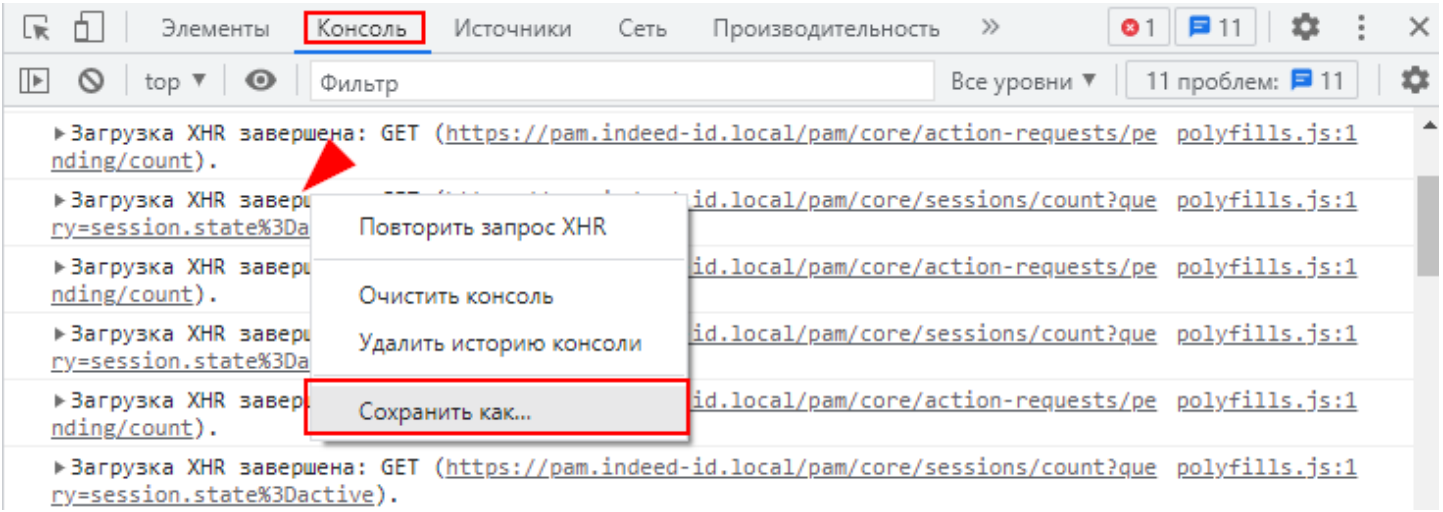
4. Во вкладке **Сеть** включите настройки **Сохранять журнал**, **Отключить кеш**, тип фильтра **Все**, как на скриншоте ниже:



5. Нажмите иконку для сброса списка запросов и не закрывая консоль разработчика выполните последовательность действий, приводящих к ошибке.
6. Нажмите по полю запросов правой кнопкой мыши, выберите пункт **Сохранить все как HAR с контентом** и сохраните файл:



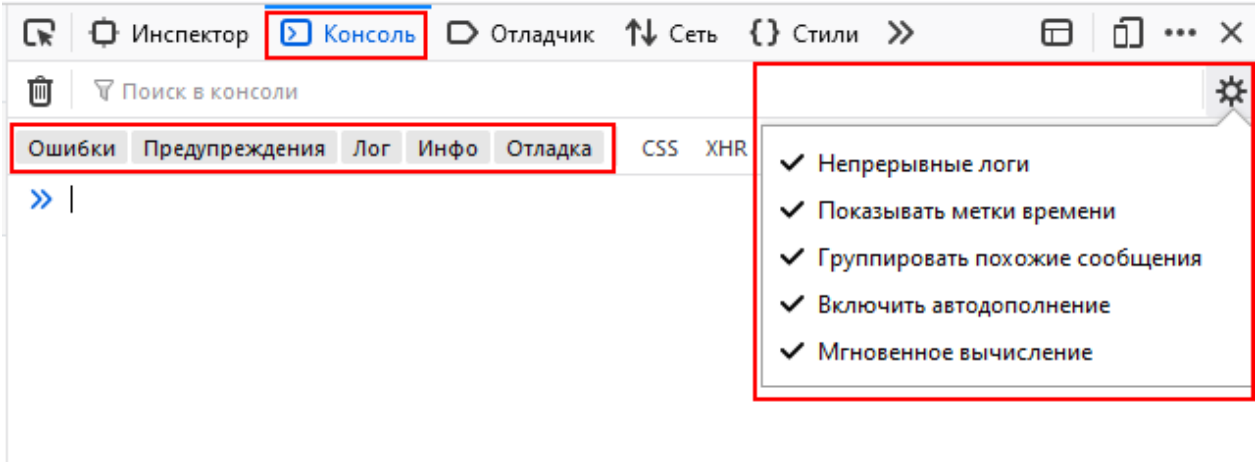
7. Перейдите во вкладку Консоль, нажмите правой кнопкой по сообщениям консоли, выберите пункт **Сохранить как** и сохраните файл:



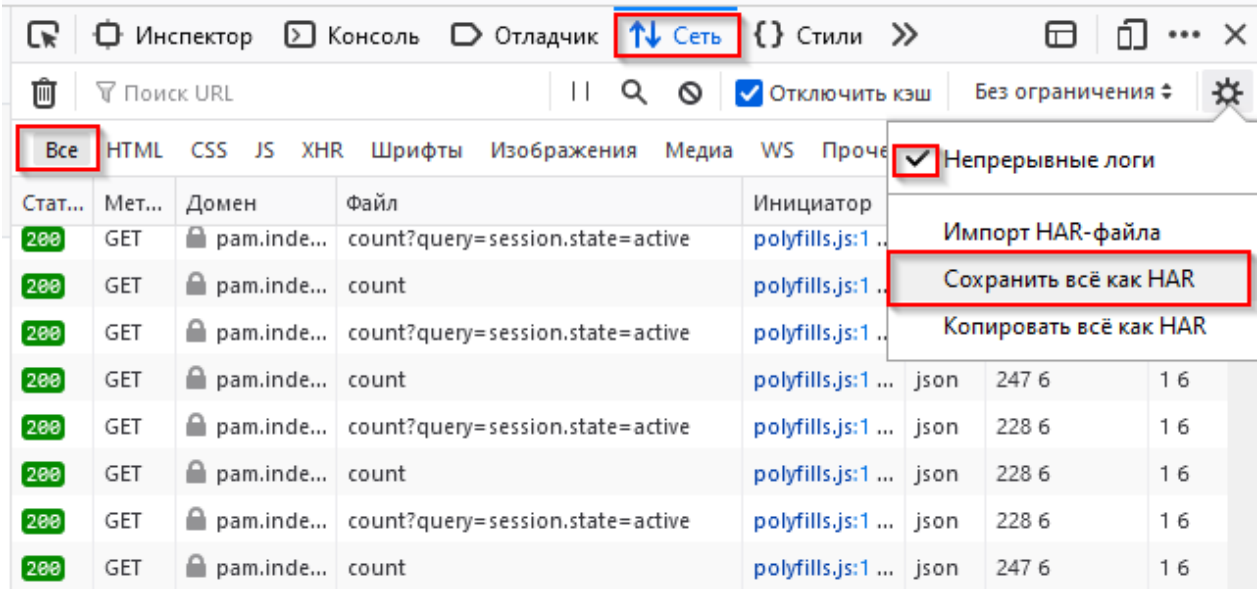
8. Сохраненные файлы перешлите в техническую поддержку.

Firefox

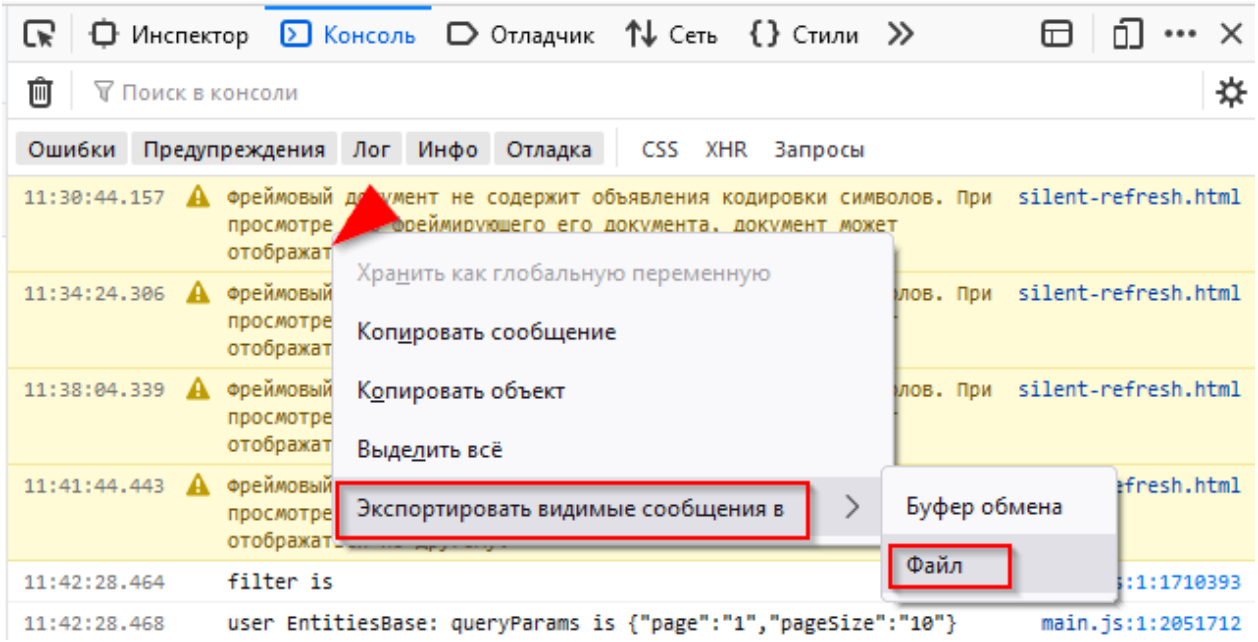
1. Запустите браузер, перейдите на страницу в которой выходит ошибка, запустите **Инструменты веб-разработчика** (нажмите Ctrl+Shift+I или F12).
2. Во вкладке **Консоль** нажмите иконку корзины для очистки, включите опции **Ошибки**, **Предупреждения**, **Лог**, **Инфо**, **Отладка**. В настройках консоли отметьте все опции, в т.ч. **Непрерывные логи**:



3. Во вкладке **Сеть** также нажмите иконку корзины для очистки, отключите фильтр, выбрав “**Все**”, нажмите значок шестеренки и отметьте опцию **Непрерывные логи**.
4. Не закрывая консоль разработчика выполните последовательность действий, приводящих к ошибке.
5. Далее в консоли разработчика во вкладке **Сеть** нажмите значок шестеренки, выберите пункт **Сохранить всё как HAR** и сохраните файл:



6. Перейдите во вкладку **Консоль**, нажмите правой кнопкой по сообщениям консоли, выберите пункт “**Экспортировать видимые сообщения в** > **Файл**” и сохраните файл.



7. Сохраненные файлы перешлите в техническую поддержку.

Техническая поддержка

Если вы не нашли ответ на ваш вопрос в документации или базе знаний, вы можете обратиться за помощью в службу поддержки.

Если вы обращаетесь в поддержку для решения проблемы, предоставьте как можно больше информации, включая файлы, скриншоты, логи. Это поможет решить проблему оперативно.

Чтобы отправить обращение в поддержку, выполните следующее:

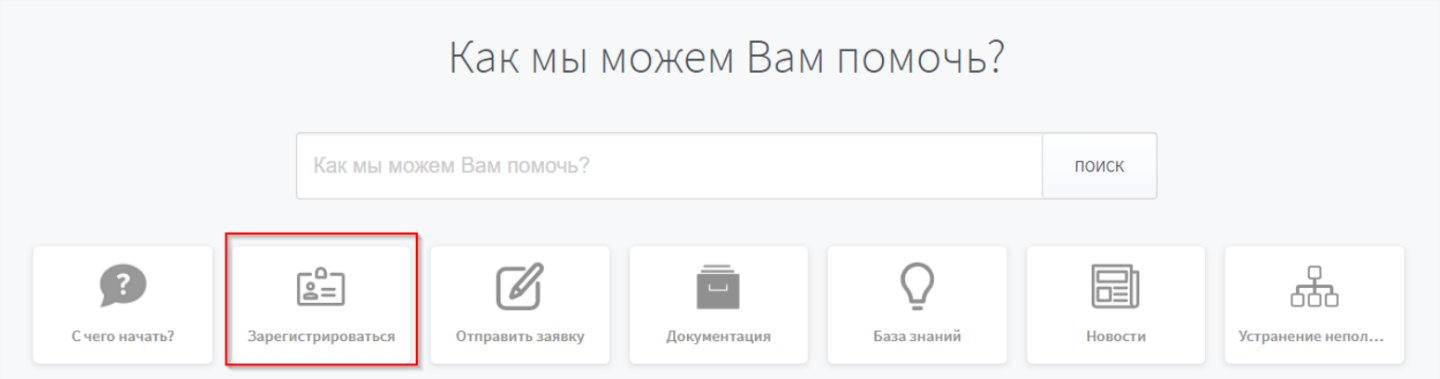
1. Откройте портал технической поддержки.
2. Введите ваш электронный адрес и пароль и нажмите **Вход**.

▼ Если у вас нет логина и пароля

Вы можете зарегистрироваться на портале поддержки самостоятельно или отправить заявку на регистрацию.

Чтобы зарегистрироваться самостоятельно:

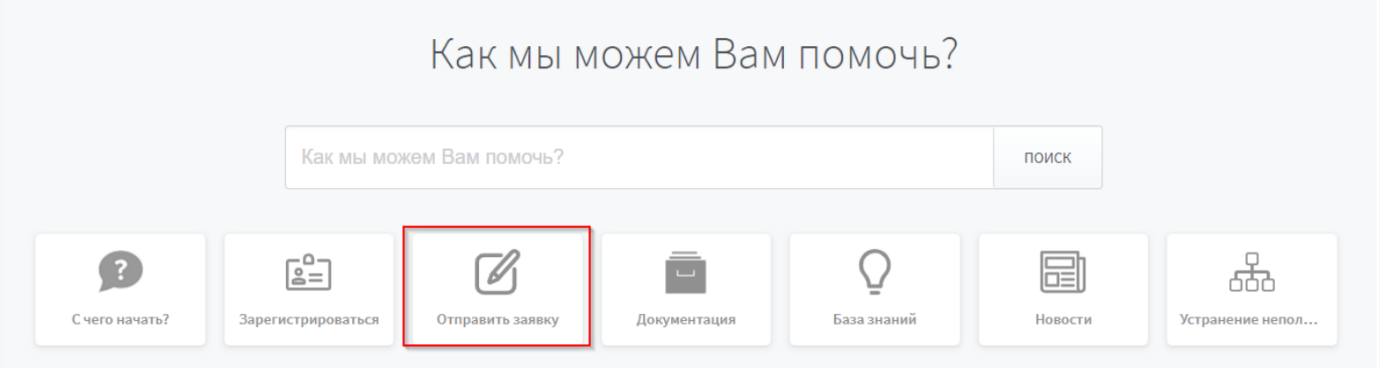
1. Нажмите **Зарегистрироваться**.



2. Откроется форма регистрации. Заполните поля и нажмите **Зарегистрироваться**.
3. На указанный электронный адрес вы получите письмо со ссылкой для активации аккаунта. Пройдите по ссылке.

Чтобы отправить заявку на регистрацию

1. Нажмите **Отправить заявку**.



2. Откроется форма заявки. Укажите, что это заявка на создание учетной записи.
3. На указанный электронный адрес вы получите письмо со ссылкой для активации аккаунта. Пройдите по ссылке.

3. Нажмите **Отправить заявку**.
4. Выберите департамент и нажмите **Вперед**.
5. Заполните форму заявки и нажмите **Отправить**.

Также вы можете связаться с командой поддержки по следующим телефонам:

- 8 800 333 09-06,
- +7 (495) 640 06-09,
- +7 (812) 640 06-09.

История версий

В этом разделе содержится краткое описание изменений и улучшений в продукте Indeed Privileged Access Manager по версиям.

3.0

- Добавлена функциональность по работе со службами Windows.
- Добавлена возможность копировать разрешения.
- Добавлен новый компонент PostgreSQL Proxy и новый тип пользовательского подключения — PostgreSQL.
- В политики сессий добавлена опция **Прерывать сессию при отсутствии пользовательской активности**.
- Подключили библиотеку Boost для работы с регулярными выражениями. В связи с этим есть небольшие изменения в синтаксисе регулярных выражений при задании списка разрешенных и запрещенных команд в SSH-сессиях.
- В политики добавлены параметры для управления ограничениями для генерируемых паролей, а также для паролей, вводимых вручную.
- Добавлена возможность открывать RDP-сессии без перенаправления локальных дисков.
- Добавлена проверка отпечатков ключей SSH-сервера.
- Добавлена возможность создавать и редактировать собственные типы сервисных подключений.
- Разработан новый мастер, который позволяет установить, обновить версию или изменить конфигурацию Indeed PAM.

2.10

- Добавлена поддержка служб каталогов OpenLDAP и ALD PRO.
- Добавлена возможность заблокировать пользователя.
- Добавлена возможность сменить ключ и/или алгоритм шифрования БД PAM без остановки работы PAM.
- Добавлена возможность указать несколько серверов RADIUS для аутентификации пользователей PAM.
- Добавлена возможность назначать политики на группы пользователей.

- Добавлена возможность подключаться к произвольным ресурсам.
- Добавлена нативная поддержка SIEM через CEF и LEEF формат логов.
- Увеличена максимальная длина пароля учетной записи до 4096 символов.
- Добавлены параметры для управления блокировкой пользователей при неверном вводе OTP.
- Добавлена поддержка хранилищ типа S3.
- Добавлена возможность включить перезапуск контейнеров сервисов прокси.

2.9

- Добавлена возможность установить Indeed PAM на любой дистрибутив Linux с поддержкой Docker.
- Появился новый компонент – RDP Proxy, который выполняет функции прокси-сервера для RDP-сессий.
- Добавлена поддержка службы каталогов FreeIPA.
- Добавлена возможность создавать группы пользователей на основе групп из внешних каталогов пользователей.
- Добавлена возможность настроить доступ к Indeed PAM из разных подсетей.
- Добавлена возможность отправки одноразовых паролей по электронной почте.

2.8

- Добавлена возможность подключаться к ресурсам по протоколам SFTP и SCP.
- Для SSH proxy добавлена возможность перенаправления портов с целевого ресурса на локальный хост.
- Добавлена возможность создавать группы ресурсов без привязки к конкретным привилегированным учетным записям. Привязка реализуется на этапе выдачи разрешения, что позволит разным пользователям открывать сессии от имени разных учетных записей на одних и тех же ресурсах, входящих в одну группу.
- Добавлена возможность создавать группы пользователей, чтобы быстро предоставлять доступ к ресурсам Indeed PAM на основе принадлежности к группам.
- Добавлена возможность фильтровать сессии в архиве сессий по группе пользователей.
- Добавлена возможность сортировать список политик по типу объектов в консоли удминистратора.
- Добавлена возможность задавать пароли учетных записей в консоли пользователя.
- Добавлена возможность группировать ресурсы по папкам в консоли пользователя.

- Добавлена возможность сортировать ресурсы по названию, типу подключения, IP-адресу, DNS и учетной записи в консоли пользователя.