

Indeed Privileged Access Manager

Техническая документация

Версия: 3.4

Дата: 23.04.2026

Содержание

О продукте 5

Компоненты 6

Лицензирование 15

Системные требования 21

- Серверные компоненты 22
- Рабочее место пользователя 40
- СУБД 41

Схемы развертывания компонентов 42

- Упрощенная на Windows 43
- Упрощенная на Linux 47
- Основная 51
- Отказоустойчивая 54

Общий план внедрения 57

Подготовка к установке 59

- Учетные записи каталога пользователей 60
- Сертификаты 67
- Базы данных 71
- Медиахранилище 76
  - SMB-хранилище 77
  - NFS-хранилище 78
  - S3-хранилище 86
- Серверы 88
- Учетные записи для установки PAM через мастер 91

Установка 92

- Основная на Windows 93
- Основная на Linux 111
- Отказоустойчивая на Windows 128
- Отказоустойчивая на Linux 147

Настройка 165

- Настройка IIS 166
- Установка и настройка клиентских компонентов 167
- Настройка подписи RDP-файла 174
- Приложение А. Конфигурационные файлы 178

Изменение конфигурации PAM 181

Безопасность 185

- Резервные учетные записи 187

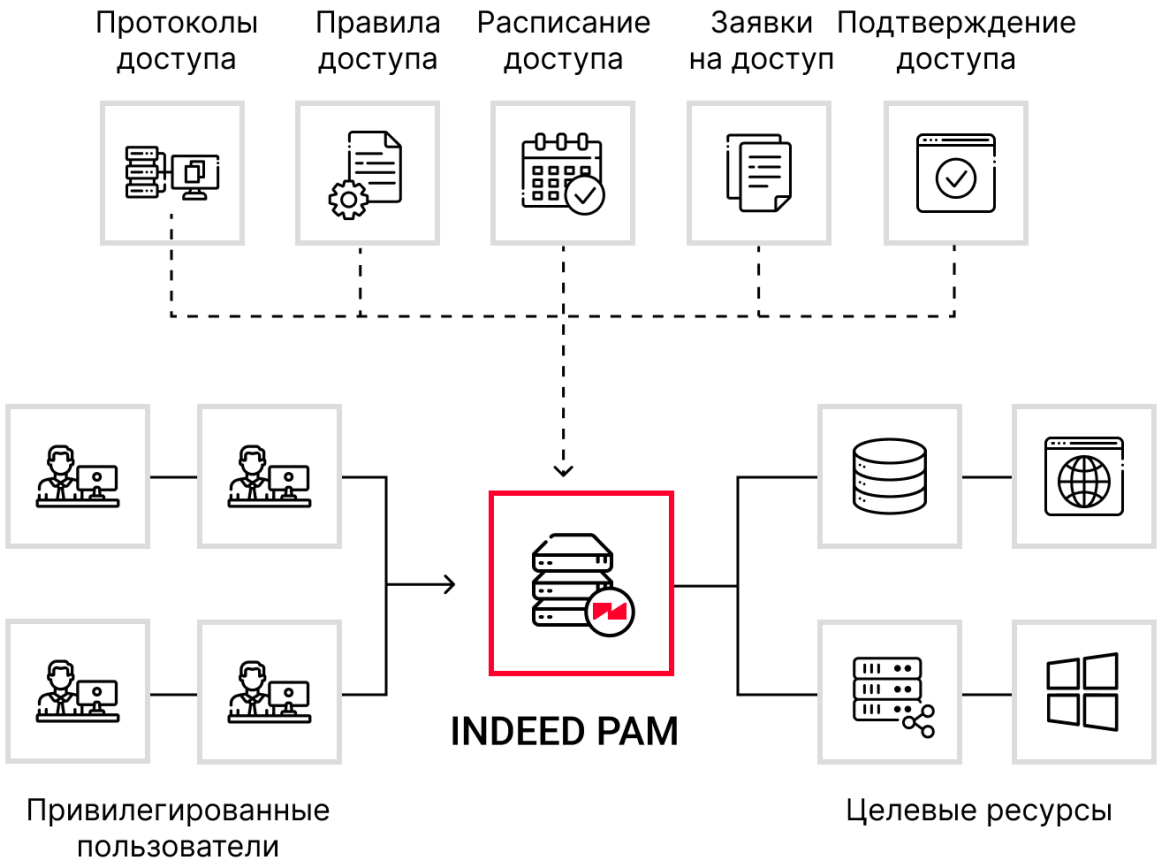
Шифрование паролей и секретов 188
Фильтрация процессов и ФС 193
Шифрование материалов сессии 199
Политики безопасности сервера доступа 200
Настройки безопасности сервера доступа 296
Смена ключа шифрования БД 300
Аутентификация 308
Протокол OpenID Connect 309
Настройка RADIUS 312
Сертификат X.509 315
Настройка одноразового пароля по Email 318
Сервисные операции 320
Руководство администратора 324
Консоль администратора 326
Пользователи 328
Группы пользователей 337
Ресурсы 340
Добавление ресурсов 342
Настройка сервисного подключения для ресурсов 348
Операции над ресурсами 354
Массовые операции над ресурсами 362
Проверка отпечатков ключей SSH-сервера 364
Службы 369
Группы ресурсов 375
Учетные записи 377
Домены 387
Структура 392
Разрешения 394
Запросы сессий 399
Активные сессии 402
Все сессии 403
События 405
История отчетов 406
Уведомления 410
Конфигурация 412
Указание длительности сегмента видео при записи RDP-сессии 431
Работа с Connector Creation Tool 432
Роли 442
Приложения 445
Первый запуск 448

Дашборд 452
Настройка политик 458
Настройка подключения пользователей по SSH-ключам 472
Выгрузка паролей 474
Работа с PostgreSQL и MSSQL Proxy 477
Работа с Web Proxy 481
Автоматизация через ConsoleApp 484
Руководство пользователя 512
Консоль пользователя 513
Подключение к ресурсу 518
RDP, Web, SSH и SQL подключение 519
SCP и SFTP подключение 534
Командная строка 535
WinSCP 538
FileZilla 541
Интеграция с Ansible 543
Ansible Lookup Plugin 544
Подключение через SSH Proxy 554
Работа с APPM 563
Python SDK 564
AAPM API 577
Консольная утилита 586
Аутентификация в SSH Proxy по SSH-ключу 590
Дополнительные утилиты 594
Использование PamSu 595
Indeed PAM Desktop Console 596
Решение проблем 597
Проблемы с сертификатом 598
Логи 605
Сбор логов серверных компонентов 606
Сбор логов клиентских компонентов 621
Сбор программных логов 625
Техническая поддержка 629
Справочник 631
События 632
Привилегии 650
Соответствие атрибутов каталога пользователей и PAM 658
История версий 662

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.



Компоненты

Сервер управления

Сервер управления — ядро и главный компонент Indeed PAM, который управляет работой всех компонентов и выполняет следующие задачи:

- Централизованное управление всеми данными в PAM.
- Шифрование критичных данных в базе данных, например, паролей привилегированных пользователей.
- Мониторинг всех действий и их фиксация в журнале.
- Задачи по расписанию, например, поиск новых учетных записей на ресурсе или ротация SSH-ключей.

Indeed PAM Core

Центральный компонент сервера управления, контролирующий все объекты Indeed PAM. Компонент выполняет следующие задачи:

- Управление учетными записями, ресурсами и доменами.
- Выдача разрешений и отзыв прав доступа.
- Запуск и контроль сессий.
- Применение политик.
- Аудит и запись событий PAM.
- Фоновые операции, например, синхронизация с доменом или проверка доступа к ресурсу.

Состав компонента и среда выполнения

Инфраструктура	Windows	Linux
Среда выполнения	Windows Server 2016–2022	Docker
Веб-сервер	Internet Information Services (IIS)	Nginx
Веб-приложение	core	core

Indeed PAM IdP

IdP (Identity Provider) — центр идентификации пользователей и компонентов Indeed PAM. Компонент выполняет следующие задачи:

- Аутентификация пользователей при доступе к PAM, в том числе двухфакторная.
- Проверка подлинности компонентов Indeed PAM.
- Аутентификация приложений, использующих API.

Состав компонента и среда выполнения

Инфраструктура	Windows	Linux
Среда выполнения	Windows Server 2016–2022	Docker
Веб-сервер	Internet Information Services (IIS)	Nginx
Веб-приложение	idp	idp

Indeed PAM Management Console

Веб-приложение для управления Indeed PAM. В консоли администратора можно настроить доступы к ресурсам, выдать разрешение на открытие сессий, выгрузить логи или просмотреть статистику. Подробнее о работе в консоли читайте в разделе **Руководство администратора**.

Состав компонента и среда выполнения

Инфраструктура	Windows	Linux
Среда выполнения	Windows Server 2016–2022	Docker
Веб-сервер	Internet Information Services (IIS)	Nginx
Веб-приложение	mc	mc

Indeed PAM User Console

Веб-приложение для доступа к защищаемым объектам Indeed PAM. Через консоль пользователя можно подключиться к ресурсу и открыть сессию в соответствии с полученным разрешением.

Подробнее о работе в консоли читайте в разделе **Руководство пользователя**.

Состав компонента и среда выполнения

Инфраструктура	Windows	Linux
Среда выполнения	Windows Server 2016–2022	Docker
Веб-сервер	Internet Information Services (IIS)	Nginx
Веб-приложение	uc	uc

Indeed Log Server

Компонент сервера управления, отвечающий за сбор, обработку и хранение событий.

Состав компонента и среда выполнения

Инфраструктура	Windows	Linux
Среда выполнения	Windows Server 2016–2022	Docker
Веб-сервер	Internet Information Services (IIS)	Nginx
Веб-приложение	ls	ls

Сервер доступа

Сервер доступа — связующее звено между пользователем и конечным ресурсом, к которому нужно предоставить доступ. В качестве ресурсов могут выступать сервера, СУБД, веб-сайты или приложения.

Когда пользователь открывает сессию, например, выполняет в терминале скопированную SSH-команду для подключения к ресурсу, происходит аутентификация в PAM. Далее сервер доступа SSH проверяет права пользователя и, при наличии разрешения, предоставляет доступ к конечному ресурсу.

Indeed PAM Gateway

Набор приложений и клиентов, предоставляющих доступ к ресурсам на ОС Windows по протоколам RDP/SSH/Telnet в режиме RemoteApp. Компонент ведет видеозапись сессии и сохраняет ее артефакты: текстовые логи, снимки экрана и передаваемые файлы.

Компонент автоматически развертывается на сервер доступа RDS во время установки PAM. Серверу нужно установить роль Remote Desktop Services.

Состав компонента и среда выполнения

Среда выполнения: 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
- Модуль контроля запуска процессов Pam.Proxy.ProcessCreateHook

Indeed PAM RDP Proxy

Прокси-сервер, предоставляющий доступ к ресурсам на ОС Linux по протоколу RDP без раскрытия данных привилегированной учетной записи. Компонент ведет видеозапись сессии и сохраняет ее артефакты: текстовые логи, снимки экрана и передаваемые файлы.

Компонент автоматически развертывается на сервере доступа RDP во время установки PAM и не нуждается в дополнительной настройке.

Состав компонента и среда выполнения

Среда выполнения: Linux

Состав: Docker-контейнер pam-rdp-proxy

Indeed PAM SSH Proxy

Прокси-сервер, предоставляющий доступ к ресурсам по протоколам SSH, SCP и SFTP. Компонент сохраняет текстовые логи сессии и передаваемые файлы.

Компонент автоматически развертывается на сервер доступа SSH во время установки PAM и поддерживает работу различных SSH-клиентов.

Состав компонента и среда выполнения

Среда выполнения: Linux

Состав: Docker-контейнер pam-ssh-proxy

Indeed PAM PostgreSQL Proxy

Прокси-сервер, контролирующий доступ к СУБД PostgreSQL. Компонент упрощает подключение к PostgreSQL, предоставляет пользователям доступ без раскрытия данных привилегированной учетной записи, а также ведет текстовое логирование SQL-сессий. Компонент поддерживает работу различных клиентов управления базами данных.

PostgreSQL Proxy автоматически развертывается на сервер доступа PostgreSQL во время установки PAM.
Как настроить компонент и открывать SQL-сессии, читайте в разделе **Работа с PostgreSQL и MSSQL Proxy**.

Состав компонента и среда выполнения

Среда выполнения: Linux

Состав: Docker-контейнер pam-sql-proxy

Indeed PAM MSSQL Proxy

Прокси-сервер, контролирующий доступ к СУБД Microsoft SQL Server (MSSQL). Компонент упрощает подключение к MSSQL, предоставляет пользователям доступ без раскрытия данных привилегированной учетной записи, а также ведет текстовое логирование SQL-сессий. Компонент поддерживает работу различных клиентов управления базами данных.

MSSQL Proxy автоматически развертывается на сервер доступа MSSQL во время установки PAM.
Как настроить компонент и открывать SQL-сессии, читайте в разделе **Работа с PostgreSQL и**

MSSQL Proxy.

Состав компонента и среда выполнения

Среда выполнения: Linux

Состав: Docker-контейнер pam-tsql-proxy

Indeed PAM Web Proxy

Прокси-сервер, предоставляющий безопасный доступ к веб-приложениям и сайтам через браузер без необходимости использования Microsoft RDS. Веб-сессия запускается прямо из консоли пользователя. Компонент поддерживает видеологирование сессий.

Web Proxy автоматически развертывается на сервер доступа Web во время установки PAM. Как настроить компонент и открывать веб-сессии, читайте в разделе **Работа с Web Proxy**.

Состав компонента и среда выполнения

Среда выполнения: Linux

Состав: Docker-контейнер pam-web-proxy

Indeed ESSO Agent и Indeed Admin Pack

Набор компонентов для автоматического заполнения форм аутентификации в веб-ресурсах и приложениях. Компоненты устанавливаются на сервер доступа RDS и самостоятельно заполняют учетные данные пользователя во время сессии, открытой в режиме RemoteApp.

Состав компонента и среда выполнения

Среда выполнения: 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, Microsoft EDGE

Клиенты

Indeed PAM Web Terminal

Клиент позволяет открывать сессии через консоль пользователя и подключаться к RDP- и SSH-ресурсам напрямую из браузера без использования сторонних программ. Клиент ведет видеозапись сессии и сохраняет ее артефакты: текстовые логи, снимки экрана и передаваемые файлы.

Компонент автоматически развертывается на сервере Web Terminal во время установки PAM и не нуждается в дополнительной настройке.

Состав компонента и среда выполнения

Среда выполнения: Linux

Состав: Docker-контейнер pam-web-terminal

Дополнительные компоненты

Indeed PAM Agent

Компонент для текстового логирования RDP-сессий. В лог попадают записи о смене активных окон, запуске приложений и процессов, а также данные клавиатурного ввода.

Как установить и настроить PAM Agent, читайте в разделе **Установка и настройка клиентских компонентов**.

Состав компонента и среда выполнения

Среда выполнения:

- Windows Server 2012R2–2022
- Windows XP SP3 x64
- Windows 7 x64 и выше

Состав:

- Служба Pam.Proxy.WindowsAgentService
- Приложение Pam.Proxy.WindowsAgent

Indeed PamSU

Компонент позволяет пользователям PAM запускать команды с правами администратора. При подключении к ресурсу запрашивается пароль учетной записи PAM, а не локального пользователя, от имени которого открыта сессия.
Вместо `sudo` используется команда `pamsu`.

Как установить и настроить PamSU, читайте в разделе **Установка и настройка клиентских компонентов**.

Состав компонента и дистрибутивы Linux, поддерживающие PamSU

Состав: Установочный пакет в формате .deb или .rpm

Дистрибутивы Linux:

- CentOS 7 и выше
- Oracle Linux 7.9 и выше
- Rocky Linux 8.8 и выше
- Debian 10 и выше
- Ubuntu 18 LTS и выше
- Astra Linux Special Edition 1.7 и выше
- Astra Linux Common Edition 2.12 и выше
- RedOS 7.3 и выше
- ALT Linux 8 и выше
- Red Hat Enterprise Linux (RHEL) 6 и выше

Indeed PAM Desktop Console

Клиентское приложение, позволяющее подключиться через Indeed PAM к целевым ресурсам по протоколам SSH и RDP. Компонент устанавливается на рабочее место пользователя.

Как настроить Desktop Console, читайте в разделе **Установка и настройка клиентских компонентов**.

Состав компонента

Многопротокольный менеджер удаленных подключений mRemoteNG.exe

Лицензирование

В Indeed PAM есть две схемы лицензирования:

- по пользователям и ресурсам;
- по сессиям (одновременным подключениям).

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

Отдельно, вне схем лицензирования, можно приобрести лицензии на отдельные функциональные модули. Такие лицензии не влияют на возможность пользователей установить сессию через PAM или на возможность администратора выдать разрешение. Лицензии на функциональные модули ограничивают возможность использования дополнительных функций. К таким лицензиям относятся:

- AAPM;
- произвольные ресурсы;
- SQL Proxy.

Лицензирование по пользователям и ресурсам

Количество пользователей и ресурсов в вашей инсталляции Indeed PAM ограничено количеством приобретенных лицензий следующих типов:

- Пользовательская — определяет количество пользователей, которые могут использовать Indeed PAM.
  Лицензии можно перераспределить: освободить лицензии у одних сотрудников и назначить другим.
- Ресурсная — определяет количество ресурсов, которые можно добавить в Indeed PAM.
  Ресурсные лицензии можно освободить и назначить на другие ресурсы.

Количество одновременно открытых сессий не ограничено.

> ⓘ **ПРИМЕЧАНИЕ**
> Любые лицензии можно докупить.

Назначение

Пользовательская лицензия

Чтобы занять пользовательскую лицензию, добавьте пользователю хотя бы одно активное разрешение. Если все пользовательские лицензии исчерпаны, добавить разрешение новому пользователю нельзя.

Ресурсная лицензия

Чтобы занять ресурсную лицензию, создайте или восстановите ресурс в Indeed PAM. Если все ресурсные лицензии исчерпаны, создать новый ресурс нельзя.

Освобождение

Пользовательская лицензия

Пользовательская лицензия освобождается в результате таких действий с разрешениями, как:

- отзыв;
- приостановка;
- истечение срока.

Ресурсная лицензия

Ресурсная лицензия освобождается при удалении ресурса.

Срок действия

По сроку действия лицензии бывают:

- не ограниченные по времени;
- ограниченные конкретной календарной датой:
  - пробный период;
  - подписка.

После истечения срока действия лицензии нельзя:

- добавить ресурс;
- добавить пользователя;
- открыть сессию.

Лицензирование по сессиям

Количество одновременно открытых сессий в Indeed PAM ограничено количеством приобретенных лицензий, количество пользователей и ресурсов — не ограничено.

Назначение и освобождение

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

Срок действия

По сроку действия лицензии бывают:

- не ограниченные по времени;
- ограниченные конкретной календарной датой:
  - пробный период;
  - подписка.

После истечения срока действия лицензии можно:

- редактировать разрешения;
- редактировать созданные ресурсы;
- редактировать учетные записи.

После истечения срока действия лицензии нельзя открывать сессии.

Лицензия на AAPM

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

Количество учетных записей, которым можно дать разрешения при помощи механизма AAPM, ограничено количеством приобретенных лицензий. Количество разрешений, приложений и их пользователей не ограничено.

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

Назначение и освобождение

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.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> Приостановка разрешений не освобождает лицензию на AAPM.

Срок действия

После истечения срока действия лицензии нельзя:

- добавить новые разрешения на приложения;
- использовать сценарии получения секретов учетных записей из Indeed PAM сторонними приложениями.

По сроку действия лицензии бывают:

- не ограниченные по времени;
- ограниченные конкретной календарной датой:
  - пробный период;
  - подписка.

После истечения срока действия лицензии нельзя:

- добавить новые разрешения на приложения;
- использовать сценарии получения секретов учетных записей из Indeed PAM сторонними приложениями.

Лицензия на произвольные ресурсы

Лицензия позволяет подключаться к произвольным ресурсам. Лицензия не ограничивает количество разрешений или одновременно открытых сессий на произвольные ресурсы.

> ⓘ **ПРИМЕЧАНИЕ**
> Лицензия на произвольные ресурсы не зависит от выбранной схемы лицензирования.
>
> Лицензию на произвольные ресурсы можно докупить или удалить в любой момент.

Срок действия

По сроку действия лицензии бывают:

- не ограниченные по времени;
- ограниченные конкретной календарной датой:
  - пробный период;
  - подписка.

Когда срок действия лицензии истечет, ранее созданные разрешения перейдут в состояние *Неактивно*, а также станут недоступны операции:

- добавить или возобновить разрешения на подключение к произвольным ресурсам;
- открыть сессию на произвольный ресурс.

Лицензия на SQL Proxy

Лицензия на SQL Proxy позволяет подключаться к ресурсам с типом MSSQL и PostgreSQL. Лицензия определяет количество активных разрешений на ресурсы с типом MSSQL и PostgreSQL.

> ⓘ **ПРИМЕЧАНИЕ**
> Лицензия на SQL Proxy не зависит от выбранной схемы лицензирования.
>
> Лицензию на SQL Proxy можно докупить или удалить в любой момент.

Назначение

Чтобы занять лицензию SQL Proxy, добавьте пользователю хотя бы одно активное разрешение на ресурс с типом MSSQL или PostgreSQL. Если все лицензии SQL Proxy исчерпаны, добавить разрешение новому пользователю на ресурс нельзя.

Освобождение

Лицензия SQL Proxy освобождается в результате таких действий с разрешениями на ресурс с типом PostgreSQL, как:

- отзыв;
- приостановка;
- истечение срока.

Срок действия

По сроку действия лицензии бывают:

- не ограниченные по времени;
- ограниченные конкретной календарной датой:
  - пробный период;
  - подписка.

После истечения срока действия лицензии нельзя:

- добавить или возобновить разрешения на подключение к ресурсам с типом MSSQL или PostgreSQL;
- добавить пользователей в группу, для которой есть активное разрешение на ресурс с типом MSSQL или PostgreSQL;
- добавить ресурсы в группу, для которой есть активное разрешение на ресурс с типом MSSQL или PostgreSQL;
- выбрать тип MSSQL или PostgreSQL при редактировании пользовательского подключения ресурса, для которого есть активное разрешение;
- открыть сессию на ресурс с типом MSSQL или PostgreSQL.

Системные требования

Серверные компоненты

Аппаратные и программные требования для серверных компонентов Indeed PAM

Рабочее место пользователя

Аппаратные и программные требования рабочего места пользователя

СУБД

Аппаратные требования к СУБД

Серверные компоненты

Для каждого компонента приведены рекомендуемые программные и аппаратные требования. Для расчета индивидуальной конфигурации PAM обратитесь в техническую поддержку.

Сервер управления

> **ПРИМЕЧАНИЕ**
> Системные требования определены в ходе испытаний в тестовой среде при типовом профиле нагрузки.

Windows

Аппаратные требования

Параметры	50 сессий	100 сессий	200 сессий
Процессор	8 ядер	16 ядер	32 ядра
Оперативная память	8 ГБ	16 ГБ	32 ГБ
Жесткий диск	120 ГБ	120 ГБ	120 ГБ
Скорость сетевого адаптера	1 Гбит/с	1 Гбит/с	1 Гбит/с
Операционная система	Windows Server 2016–2022		
Домен	Microsoft Active Directory		
Веб-сервер	Internet Information Services 8.5–10.0		

Модули веб-сервера	• Basic Authentication (Обычная проверка подлинности) • Windows Authentication (Проверка подлинности Windows) • Static Content (Статическое содержимое) • HTTP Redirection (Перенаправление HTTP) • ASP.NET Core Runtime • ISAPI Extensions (Расширения ISAPI) • .NET Extensibility (Расширяемость .NET) • ISAPI Filters (Фильтры ISAPI) • IIS Management Console (Консоль управления службами IIS)
Компоненты Microsoft	• Microsoft .NET Core 8 • URL Rewrite

Сетевое взаимодействие

Входящие

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

Исходящие

Протокол	Порт	Описание
TCP	389, 636	Чтение каталога пользователей
TCP	389, 636	Сервисные операции в каталогах пользователей
TCP	5985, 5986, 139, 445	Сервисные операции в ОС Windows
TCP	22	Сервисные операции в ОС Linux, Cisco IOS XE, Inspur BMC
TCP	1433	Сервисные операции или запись данных в СУБД Microsoft SQL Server
TCP	5432	Сервисные операции или запись данных в СУБД PostgreSQL

Протокол	Порт	Описание
TCP	1521	Сервисные операции в СУБД OracleDB
TCP	3306	Сервисные операции в СУБД MySQL
TCP	445	Запись снимков экрана в медиахранилище
TCP	5443	Чтение стрима сессии с сервера доступа Windows
TCP	8443	Чтение стрима сессии с сервера доступа Linux

Linux

Аппаратные требования

Параметры	50 сессий	100 сессий	200 сессий
Процессор	2 ядра	2 ядра	2 ядра
Оперативная память	4 ГБ	4 ГБ	4 ГБ
Жесткий диск	120 ГБ	120 ГБ	120 ГБ
Скорость сетевого адаптера	1 Гбит/с	1 Гбит/с	1 Гбит/с
Операционная система	Linux с поддержкой 64-битной архитектуры: • Debian 11 и выше • Ubuntu 22.04 и выше • Astra Linux 1.7 и выше • РЕД ОС 7.3 и выше • ALT Linux 9 и выше		
Пакеты	• Docker 18.09 и выше • Docker Compose 1.29.2 и выше **Примечание:** Docker должен быть установлен из репозитория дистрибутива ОС Linux.		

Дополнительные компоненты	• iptables 1.4 и выше • python 3.5 и выше • openssh-server (версия зависит от дистрибутива Linux) **Примечание:** Если на сервере установлена утилита nftables, то удалите ее и установите iptables.

Разметка диска	• Корневая файловая система (/) — раздел с файлами приложений и операционной системы. Рекомендуется выделить 10–20 ГБ в зависимости от установленного ПО. • */home* — раздел для хранения пользовательских данных. Также используется для хранения временных файлов и docker-образов во время установки PAM. Необходимо выделить не менее 10 ГБ свободного пространства. • */var* — раздел для хранения временных файлов, логов, баз данных, кешей. Рекомендуется выделить 20 ГБ и более. • */tmp* — раздел с временными файлами. Объем раздела должен быть достаточным для временных операций, например распаковки файлов или хранения кешей. Рекомендуется выделить 10 ГБ и более. • */boot* — раздел, содержащий загрузчик и ядро. Рекомендуется выделить 1 ГБ с учетом будущих расширений и обновлений. • *swap* — раздел используется как виртуальная память. Рекомендуется выделить объем, равный размеру оперативной памяти. • */var/lib/docker* — раздел для Docker root directory, содержащий docker-образы, тома и временные файлы. При возрастании количества пользовательских сессий требуется увеличить объем раздела. Рекомендуется выделить 100 ГБ и более. • */etc/indeed* — раздел для данных PAM: конфигураций, сертификатов, ключей, логов. В раздел сохраняются временные данные, ожидающие отправки в удаленное медиахранилище. Рекомендуется выделить 40 ГБ и более.

Пример разметки диска

Пример разметки для сервера с объемом диска 240 ГБ и 32 ГБ оперативной памяти.

Раздел	Объем, ГБ	% от общего объема диска
Корневая файловая система (/)	20	8,33
/home	10	4,17
/var	20	8,33
/tmp	10	4,17
/boot	1	0,42
swap	32	13,33
/var/lib/docker	100	41,67
/etc/indeed	47	19,58

Сетевое взаимодействие

Входящие

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

Исходящие

Протокол	Порт	Описание
TCP	389, 636	Чтение каталога пользователей
TCP	389, 636	Сервисные операции в каталогах пользователей

Протокол	Порт	Описание
TCP	5985, 5986, 139, 445	Сервисные операции в ОС Windows
TCP	22	Сервисные операции в ОС Linux, Cisco IOS XE, Inspur BMC
TCP	1433	Сервисные операции или запись данных в СУБД Microsoft SQL Server
TCP	5432	Сервисные операции или запись данных в СУБД PostgreSQL
TCP	1521	Сервисные операции в СУБД OracleDB
TCP	3306	Сервисные операции в СУБД MySQL
TCP	445	Запись снимков экрана в хранилище видео
TCP	5443	Чтение стрима сессии с сервера доступа Windows
TCP	8443	Чтение стрима сессии с сервера доступа Linux

Сервер доступа RDS

> ⓘ **ПРИМЕЧАНИЕ**
> Системные требования определены в ходе испытаний в тестовой среде при типовом профиле нагрузки.

Аппаратные требования			
Параметры	**10 RDP- или SSH-сессий**	**50 RDP- или SSH-сессий**	**100 RDP- или SSH-сессий**

Процессор	8 ядер	16 ядер	32 ядра
Оперативная память	12 ГБ	32 ГБ	64 ГБ
Жесткий диск	160 GB + 5 GB на каждого пользователя PAM	320 GB + 5 GB на каждого пользователя PAM	520 GB + 5 GB на каждого пользователя PAM
Скорость сетевого адаптера	1 Гбит/с	1 Гбит/с	1 Гбит/с
Операционная система	Windows Server 2016–2022		
Домен	Microsoft Active Directory		
Роли Remote Desktop Services	• Remote Desktop Services Broker (RDCB) • Remote Desktop Services Host (RDSH) • Remote Desktop Web Access (RDWA)		
Компоненты Microsoft	• Microsoft .NET Desktop Runtime x64 v8 • Microsoft C++ 2015–2019 Redistributable		
Браузер	• Google Chrome • Microsoft EDGE		
Дополнительные требования	• Поддержка Simultaneous multithreading (AMD) или Hyper-Threading (Intel) • Разрешение монитора по ширине не менее 1280 пикселей		

Сетевое взаимодействие

Входящие

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

Исходящие

Протокол	Порт	Описание
TCP	443	Взаимодействие с сервером управления
TCP	3389	Подключение к ресурсу по протоколу RDP
TCP	22	Подключение к ресурсу по протоколу SSH
TCP	23	Подключение к ресурсу по протоколу Telnet
TCP	445	Запись видео сессии в медиахранилище

Сервер доступа RDP

> **ПРИМЕЧАНИЕ**
> Системные требования определены в ходе испытаний в тестовой среде при типовом профиле нагрузки.

Аппаратные требования

Параметры	10 RDP-сессий	50 RDP-сессий	100 RDP-сессий
Процессор	2 ядра	8 ядер	8 ядер
Оперативная память	4 ГБ	12 ГБ	12 ГБ
Жесткий диск	120 ГБ	120 ГБ	120 ГБ
Скорость сетевого адаптера	1 Гбит/с	1 Гбит/с	1 Гбит/с

Операционная система	Linux с поддержкой 64-битной архитектуры: • Debian 11 и выше • Ubuntu 22.04 и выше • Astra Linux 1.7 и выше • РЕД ОС 7.3 и выше • ALT Linux 9 и выше
Пакеты	• Docker 18.09 и выше • Docker Compose 1.29.2 и выше **Примечание:** Docker должен быть установлен из репозитория дистрибутива ОС Linux.
Дополнительные компоненты	• iptables 1.4 и выше • python 3.5 и выше • openssh-server (версия зависит от дистрибутива Linux) **Примечание:** Если на сервере установлена утилита nftables, то удалите ее и установите iptables.
Дополнительные требования	Разрешение монитора по ширине не менее 1280 пикселей

Сетевое взаимодействие

Входящие

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

Исходящие

Протокол	Порт	Описание
TCP	443	Взаимодействие с сервером управления

Протокол	Порт	Описание
TCP	3389	Подключение к ресурсу по протоколу RDP
TCP	445	Запись видео сессии в медиахранилище

Сервер доступа SSH

> ⓘ **ПРИМЕЧАНИЕ**
> Системные требования определены в ходе испытаний в тестовой среде при типовом профиле нагрузки.

Аппаратные требования			
Параметры	**50 SSH-сессий**	**100 SSH-сессий**	**200 SSH-сессий**
Процессор	2 ядра	2 ядра	4 ядра
Оперативная память	2 ГБ	4 ГБ	4 ГБ
Жесткий диск	120 ГБ	120 ГБ	120 ГБ
Скорость сетевого адаптера	1 Гбит/с	1 Гбит/с	1 Гбит/с
Операционная система	Linux с поддержкой 64-битной архитектуры: • Debian 11 и выше • Ubuntu 22.04 и выше • Astra Linux 1.7 и выше • РЕД ОС 7.3 и выше • ALT Linux 9 и выше		
Пакеты	• Docker 18.09 и выше • Docker Compose 1.29.2 и выше **Примечание:** Docker должен быть установлен из репозитория дистрибутива ОС Linux.		

Дополнительные компоненты	• iptables 1.4 и выше • python 3.5 и выше • openssh-server (версия зависит от дистрибутива Linux) **Примечание:** Если на сервере установлена утилита nftables, то удалите ее и установите iptables.

Сетевое взаимодействие

Входящие

Протокол	Порт	Описание
TCP	2222	Подключение к серверу доступа

Исходящие

Протокол	Порт	Описание
TCP	443	Взаимодействие с сервером управления
TCP	22	Подключение к ресурсу по протоколу SSH/SCP/SFTP
TCP	445	Сохранение переданных файлов

Сервер доступа PostgreSQL

> ⓘ **ПРИМЕЧАНИЕ**
> Системные требования определены в ходе испытаний в тестовой среде при типовом профиле нагрузки.

Аппаратные требования

Параметры	50 SQL-сессий	100 SQL-сессий	200 SQL-сессий

Процессор Оперативная память Жесткий диск Скорость сетевого адаптера	2 ядра 4 ГБ 120 ГБ 1 Гбит/с	2 ядра 4 ГБ 120 ГБ 1 Гбит/с	2 ядра 4 ГБ 120 ГБ 1 Гбит/с
Операционная система	Linux с поддержкой 64-битной архитектуры: • Debian 11 и выше • Ubuntu 22.04 и выше • Astra Linux 1.7 и выше • РЕД ОС 7.3 и выше • ALT Linux 9 и выше		
Пакеты	• Docker 18.09 и выше • Docker Compose 1.29.2 и выше **Примечание:** Docker должен быть установлен из репозитория дистрибутива ОС Linux.		
Дополнительные компоненты	• iptables 1.4 и выше • python 3.5 и выше • openssh-server (версия зависит от дистрибутива Linux) **Примечание:** Если на сервере установлена утилита nftables, то удалите ее и установите iptables.		

Сетевое взаимодействие

Входящие

Протокол	Порт	Описание
TCP	5432	Подключение к серверу доступа

Исходящие

Протокол	Порт	Описание
TCP	5432	Запись данных в СУБД PostgreSQL

Сервер доступа MSSQL

Операционная система	Linux с поддержкой 64-битной архитектуры: • Debian 11 и выше • Ubuntu 22.04 и выше • Astra Linux 1.7 и выше • РЕД ОС 7.3 и выше • ALT Linux 9 и выше
Пакеты	• Docker 18.09 и выше • Docker Compose 1.29.2 и выше **Примечание:** Docker должен быть установлен из репозитория дистрибутива ОС Linux.
Дополнительные компоненты	• iptables 1.4 и выше • python 3.5 и выше • openssh-server (версия зависит от дистрибутива Linux) **Примечание:** Если на сервере установлена утилита nftables, то удалите ее и установите iptables.

Сетевое взаимодействие

Входящие

Протокол	Порт	Описание
TCP	1433	Подключение к серверу доступа

Исходящие

Протокол	Порт	Описание
TCP	1433	Запись данных в СУБД MSSQL

Сервер Web Terminal

> **ПРИМЕЧАНИЕ**
> Системные требования определены в ходе испытаний в тестовой среде при распределении нагрузки:
>
> - 40% на SSH-сессии;
> - 60% на RDP-сессии.

Аппаратные требования

Параметры	25 сессий	50 сессий	75 сессий	100 сессий
Процессор	1 ядро	2 ядра	3 ядра	4 ядра
Оперативная память	2 ГБ	4 ГБ	6 ГБ	8 ГБ
Жесткий диск	120 ГБ	120 ГБ	120 ГБ	120 ГБ
Скорость сетевого адаптера	1 Гбит/с	1 Гбит/с	1 Гбит/с	1 Гбит/с
Операционная система	Linux с поддержкой 64-битной архитектуры: • Debian 11 и выше • Ubuntu 22.04 и выше • Astra Linux 1.7 и выше • РЕД ОС 7.3 и выше • ALT Linux 9 и выше			

Пакеты	• Docker 18.09 и выше • Docker Compose 1.29.2 и выше **Примечание:** Docker должен быть установлен из репозитория дистрибутива ОС Linux.
Дополнительные компоненты	• iptables 1.4 и выше • python 3.5 и выше • openssh-server (версия зависит от дистрибутива Linux) **Примечание:** Если на сервере установлена утилита nftables, то удалите ее и установите iptables.

Сетевое взаимодействие

К Web Terminal

Протокол	Порт	Источник
HTTPS	443	Подключение к Web Terminal

От Web Terminal до SSH / RDP Proxy

Протокол	Порт	Источник
TCP	2222	Подключение к ресурсу по протоколу SSH Proxy
TCP	3389	Подключение к ресурсу по протоколу RDP Proxy

От SSH / RDP Proxy

Протокол	Порт	Описание
HTTPS	443	Взаимодействие с сервером управления
HTTPS	443	Взаимодействие с IDP
SSH	22	Подключение к серверу доступа SSH

Протокол	Порт	Описание
RDP	3389	Подключение к серверу доступа RDP
SMB/CIFS	445	Запись видео сессии в медиахранилище

Сервер доступа Web

> **ПРИМЕЧАНИЕ**
> Системные требования определены в ходе испытаний в тестовой среде при типовом профиле нагрузки и рекомендуемом разрешении видео. Задайте эту настройку перед открытием веб-сессии.

Аппаратные требования

Параметры	10 веб-сессий	50 веб-сессий	100 веб-сессий
Процессор	2 ядра	8 ядер	16 ядер
Оперативная память	6 ГБ	18 ГБ	32 ГБ
Жесткий диск	120 ГБ	120 ГБ	120 ГБ
Скорость сетевого адаптера	1 Гбит/с	1 Гбит/с	1 Гбит/с
Операционная система	Linux с поддержкой 64-битной архитектуры: • Debian 11 и выше • Ubuntu 22.04 и выше • Astra Linux 1.7 и выше • РЕД ОС 7.3 и выше • ALT Linux 9 и выше		
Пакеты	• Docker 18.09 и выше • Docker Compose 1.29.2 и выше **Примечание:** Docker должен быть установлен из репозитория дистрибутива ОС Linux.		

Дополнительные компоненты	• iptables 1.4 и выше • python 3.5 и выше • openssh-server (версия зависит от дистрибутива Linux) **Примечание:** Если на сервере установлена утилита nftables, то удалите ее и установите iptables.

Сетевое взаимодействие

Входящие

Протокол	Порт	Описание
TCP	5443	Подключение к серверу доступа
TCP	58080	Мониторинг состояния серверов

Исходящие

Протокол	Порт	Описание
TCP	443	Подключение к веб-ресурсу по протоколу HTTPS
TCP	80	Подключение к веб-ресурсу по протоколу HTTP

Настройки безопасности CIS Benchmark

На серверах PAM требуется применить настройки безопасности CIS Benchmark, описанные в PDF-файле.

- Скачать файл
- Перейти на официальный сайт cisecurity

Рабочее место пользователя

Перед установкой Indeed PAM убедитесь, что ваша инфраструктура соответствует системным требованиям.

Браузеры

Работа консолей Indeed PAM поддерживается в следующих браузерах:

- Google Chrome
- Microsoft Edge
- Яндекс Браузер

Desktop Console

Аппаратные требования	• Не менее 2 ГБ оперативной памяти • Не менее 500 МБ свободного дискового пространства
Операционная система	• Windows 7 и выше • Windows Server 2008 и выше
Дополнительные компоненты Microsoft	Microsoft .NET Framework 4.6.2 и выше

СУБД

Перед установкой и настройкой СУБД убедитесь, что ваша инфраструктура соответствует системным требованиям.

Аппаратные требования			
Параметры	**50 сессий**	**100 сессий**	**200 сессий**
Процессор	2 ядра	2 ядра	2 ядра
Оперативная память	2 ГБ	4 ГБ	4 ГБ
Жесткий диск	1 ТВ	1 ТВ	1 ТВ
Скорость сетевого адаптера	1 Гбит/с	1 Гбит/с	1 Гбит/с
Поддерживаемые СУБД	• Microsoft SQL Server 2016–2022 с поддержкой Full-Text and Semantic Extractions for Search • PostgreSQL 12–18 • Postgres Pro Standard 12–17 • Postgres Pro Enterprise 12–17 • Jatoba 4–6		

Схемы развертывания компонентов

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

Серверы управления и доступа (RDS) на ОС Windows

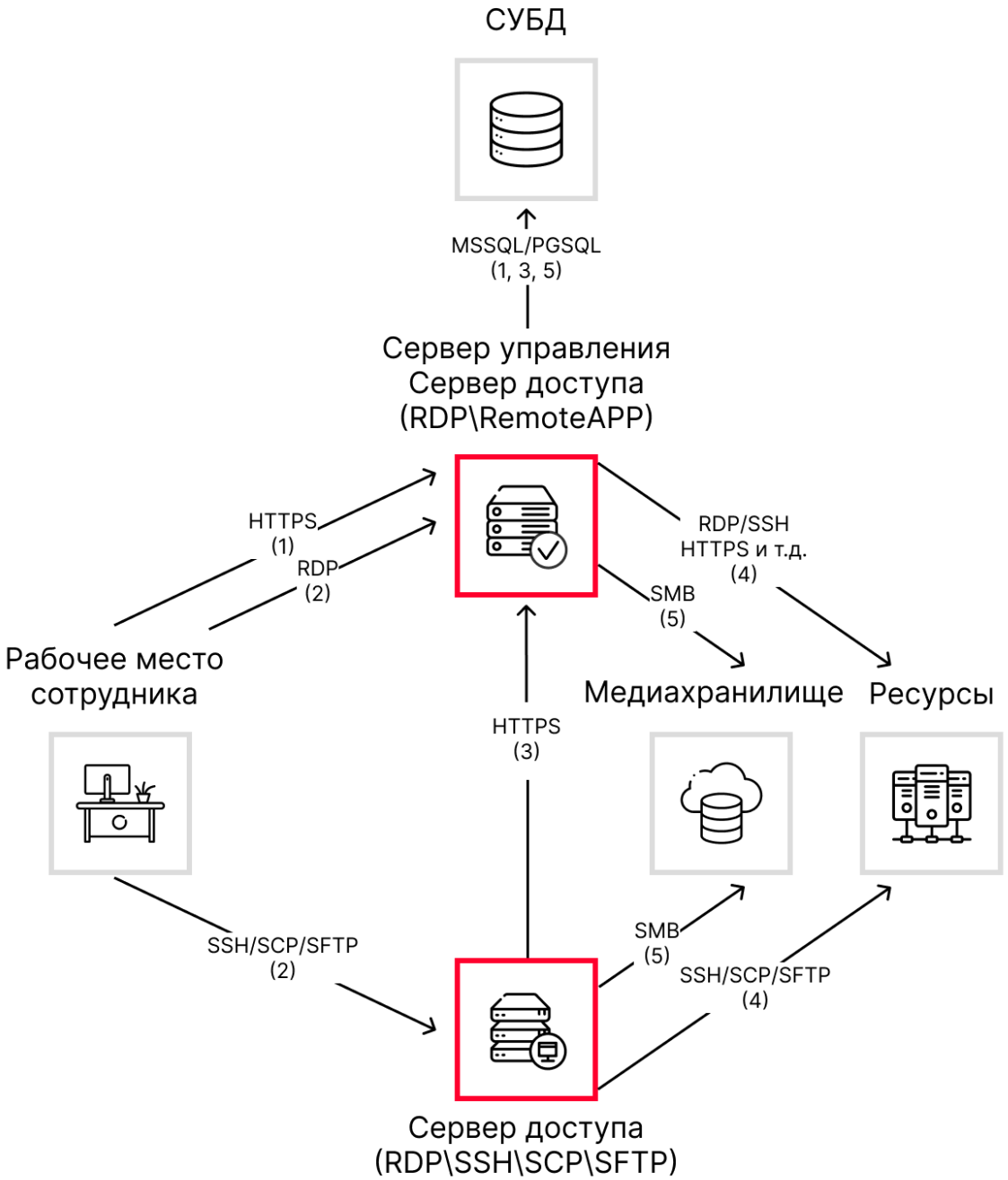
- Indeed PAM Core
- Indeed PAM IdP
- Indeed PAM Management Console
- Indeed PAM User Console
- Indeed Log Server
- Indeed PAM EventLog
- Indeed PAM Gateway
- Indeed ESSO Admin Pack
- Indeed ESSO Agent

Сервер доступа и Web Terminal на ОС Linux

- Indeed PAM SSH Proxy
- Indeed PAM RDP Proxy
- Indeed PAM PostgreSQL Proxy
- Indeed PAM MSSQL Proxy
- Indeed PAM Web Proxy
- Indeed PAM Web Terminal

Сценарии работы

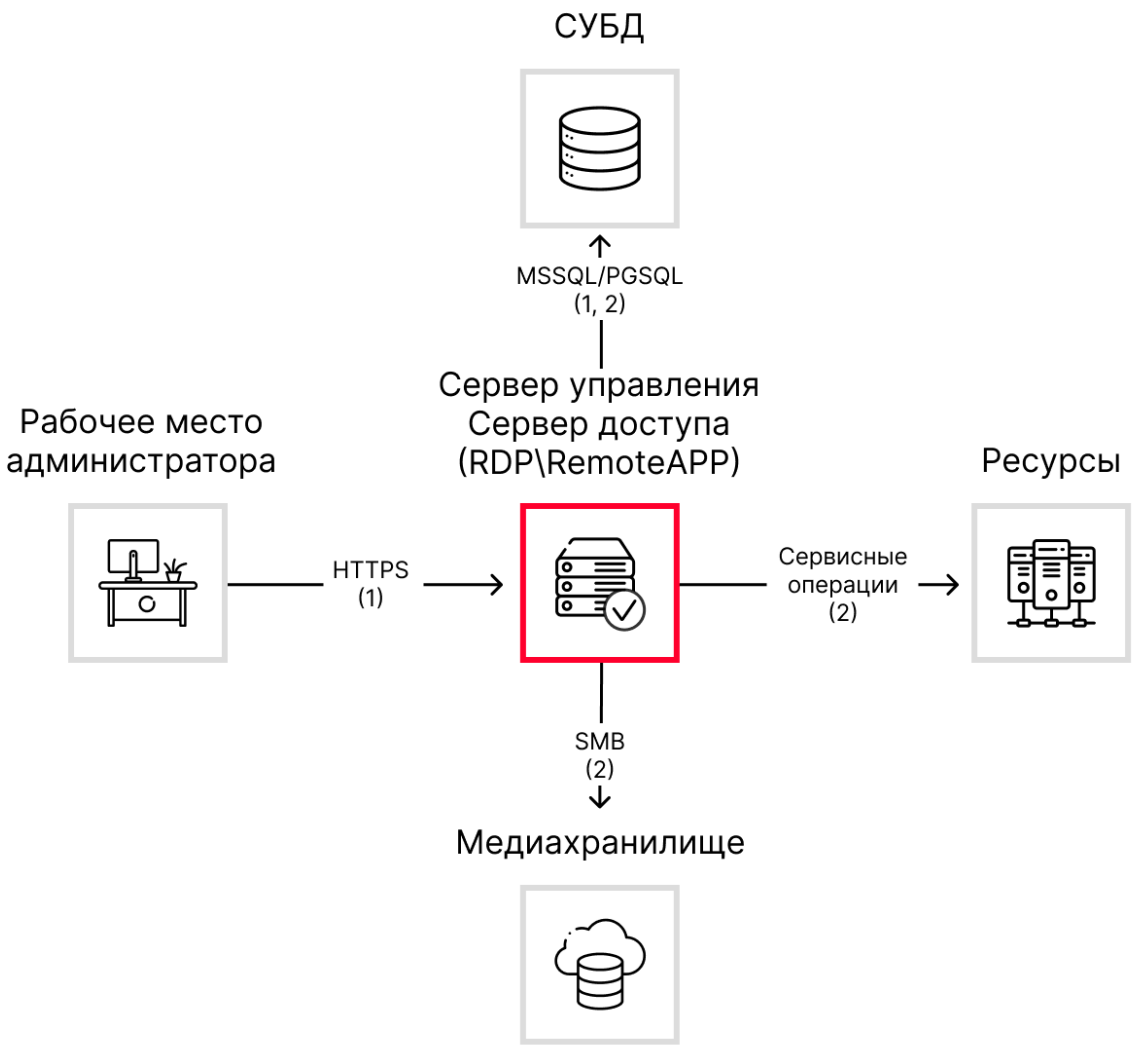
Пользовательский



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

Web Terminal, серверы управления и доступа на ОС Linux

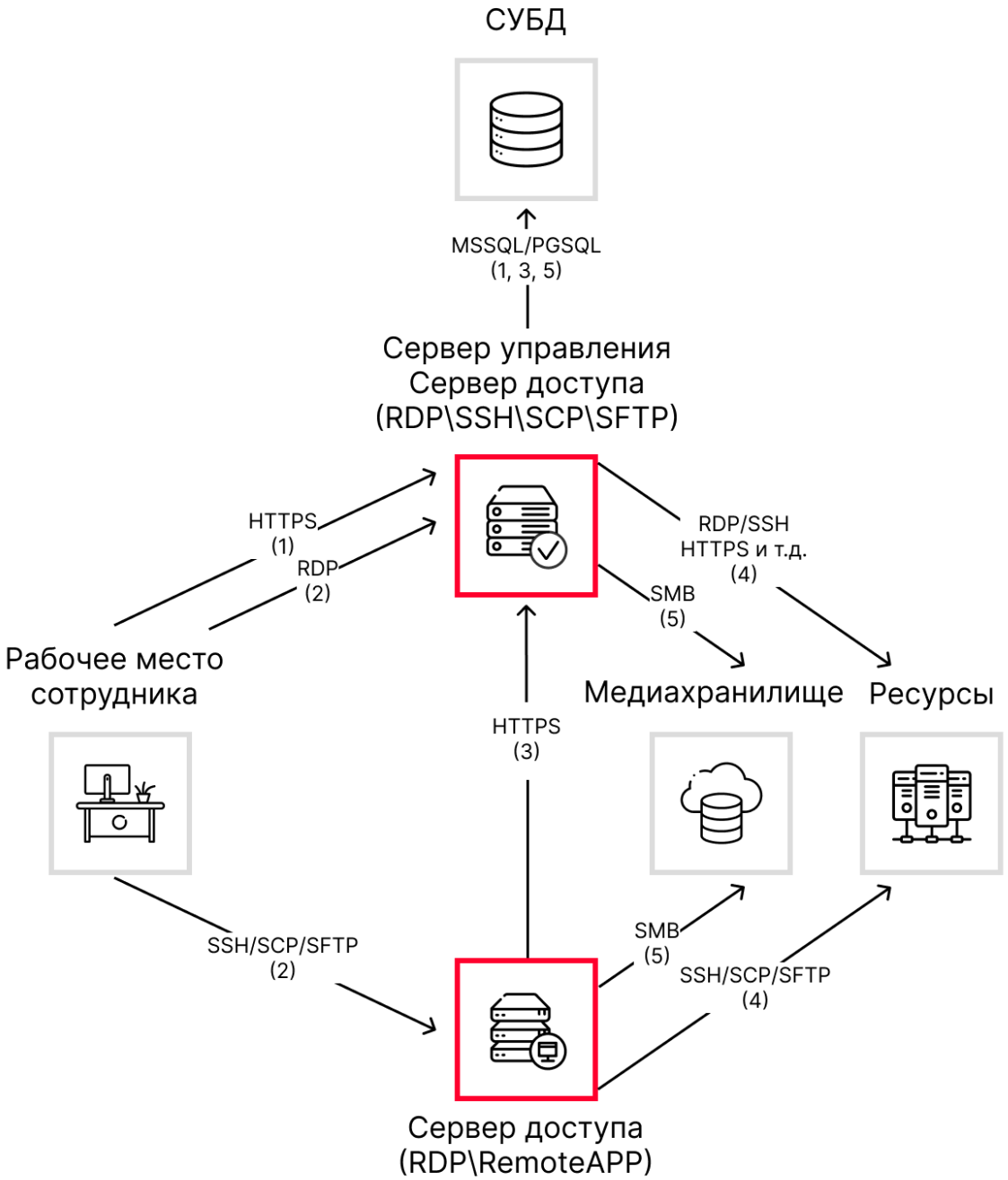
- Indeed PAM Core
- Indeed PAM IdP
- Indeed PAM Management Console
- Indeed PAM User Console
- Indeed Log Server
- Indeed PAM SSH Proxy
- Indeed PAM RDP Proxy
- Indeed PAM PostgreSQL Proxy
- Indeed PAM MSSQL Proxy
- Indeed PAM Web Proxy
- Indeed PAM Web Terminal

Сервер доступа (RDS) на ОС Windows

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

Сценарии работы

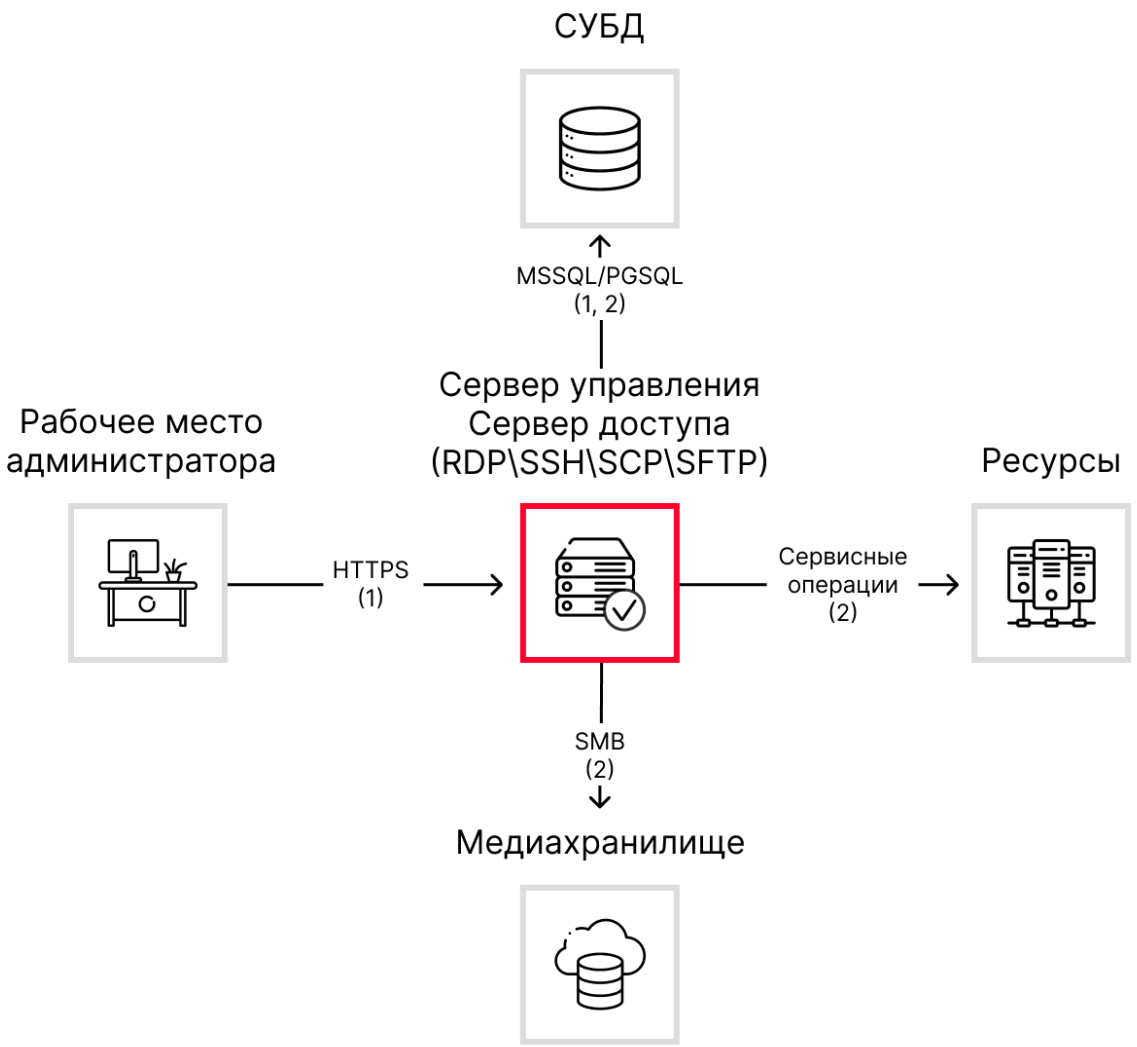
Пользовательский



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 на ОС Linux

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

Сервер доступа (RDS) на ОС Windows

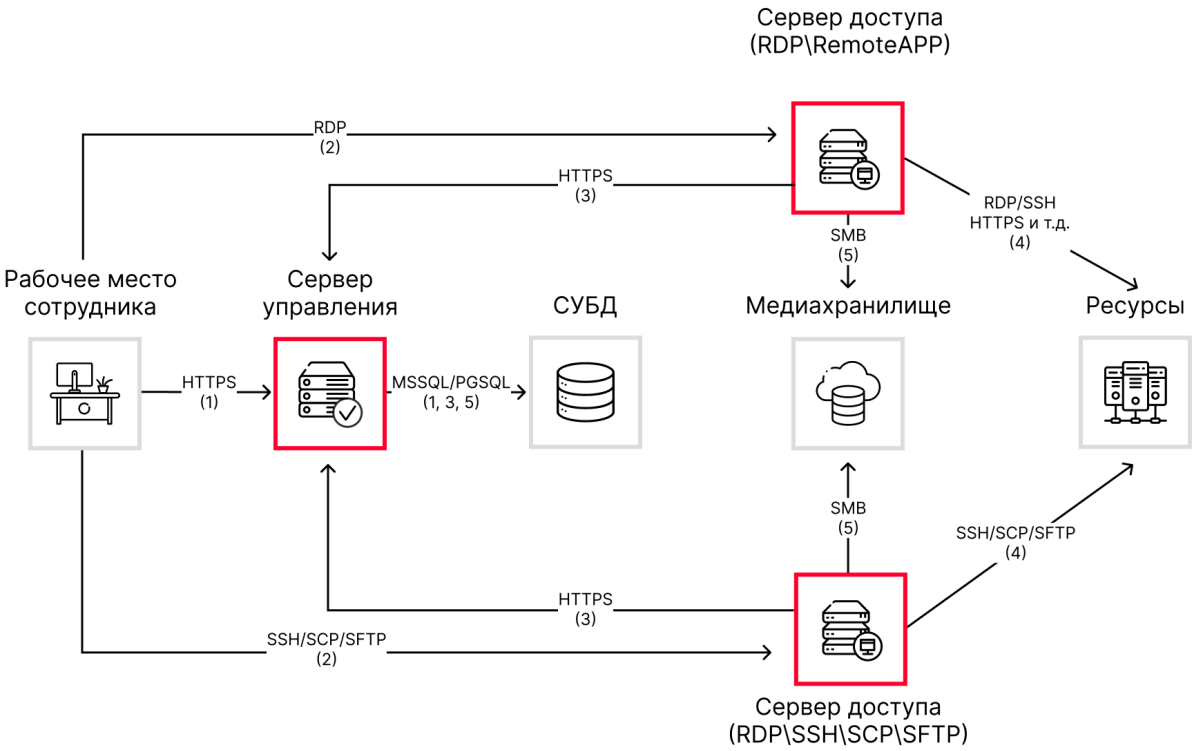
- Indeed PAM Gateway
- Indeed ESSO Admin Pack
- Indeed ESSO Agent

Сервер доступа и Web Terminal на ОС Linux

- Indeed PAM SSH Proxy
- Indeed PAM RDP Proxy
- Indeed PAM PostgreSQL Proxy
- Indeed PAM MSSQL Proxy
- Indeed PAM Web Proxy
- Indeed PAM Web Terminal

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 на ОС Linux

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

Сервер доступа (RDS) на ОС Windows

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

Сервер доступа и Web Terminal на ОС Linux

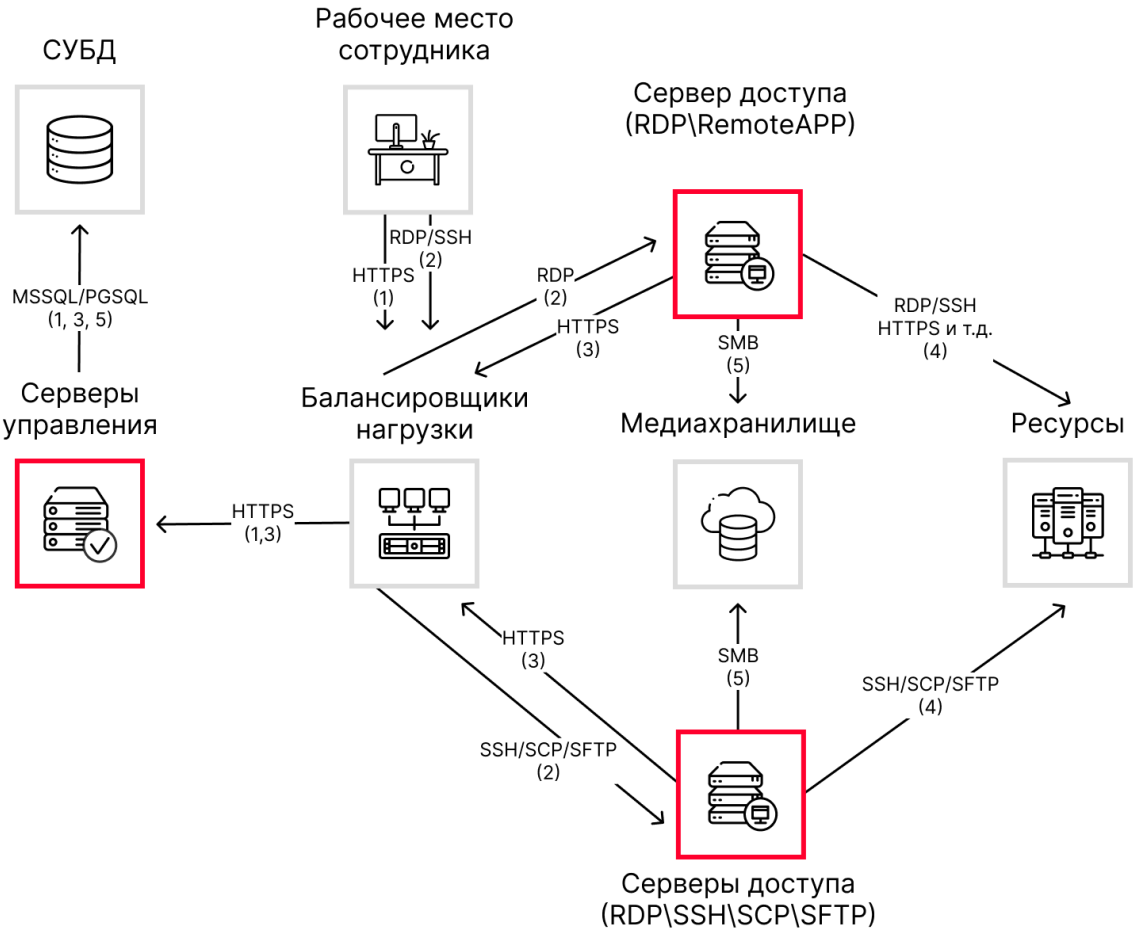
- Indeed PAM SSH Proxy
- Indeed PAM RDP Proxy
- Indeed PAM PostgreSQL Proxy
- Indeed PAM MSSQL Proxy
- Indeed PAM Web Proxy
- Indeed PAM Web Terminal

Балансировщик

- HAProxy на ОС Linux
- Настраиваемый балансировщик на ОС Windows

Сценарии работы

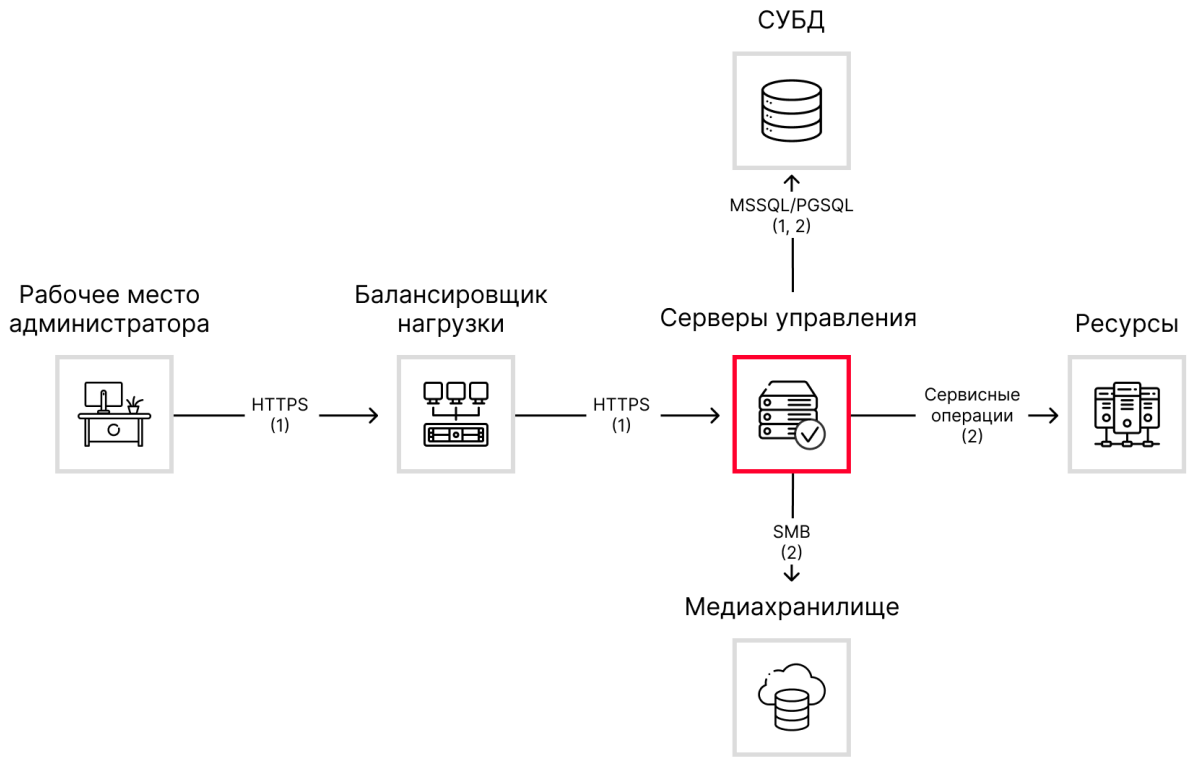
Пользовательский



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.

Общий план внедрения

Подготовка инфраструктуры

1. Предоставьте серверные и клиентские компоненты в соответствии с их системно-аппаратными требованиями.
2. Установите и настройте Службу удаленных рабочих столов (Remote Desktop Services).
3. Установите дополнительные компоненты Microsoft для корректной работы серверных компонентов Indeed PAM.
4. Настройте сетевое взаимодействие серверных и клиентских компонентов в соответствии с требованиями.
5. Настройте хранилище данных Indeed PAM:
    - Предоставьте доступ к экземпляру Microsoft SQL, PostgreSQL, PostgreSQL Pro или Jatoba.
    - Создайте базу данных.
    - Настройте сервисную учетную запись или предоставьте доступ к имеющейся учетной записи.
    - Создайте и настройте медиахранилище для хранения видеозаписей, снимков экрана и файлов.
6. Определите LDAP-пути контейнеров и подразделений, в которых будет расположен каталог пользователей Indeed PAM в иерархии службы каталогов.
7. Создайте и настройте сервисную учетную запись для работы с каталогом пользователей Indeed PAM или предоставьте доступ к имеющейся учетной записи.
8. Создайте и настройте сервисную учетную запись для сервисных операций в службе каталогов или предоставьте доступ к имеющейся учетной записи.

Установка и настройка серверных компонентов Indeed PAM

Windows

1. Сервер управления на ОС Windows
2. Сервер доступа RDS

Linux

1. Сервер управления на ОС Linux

2. Сервер доступа RDP
3. Сервер доступа SSH
4. Сервер доступа PostgreSQL
5. Сервер доступа MSSQL
6. Сервер доступа Web
7. Сервер Web Terminal

Установка и настройка клиентских компонентов Indeed PAM

1. Установите и настройте PamSu.
2. Установите и настройте Indeed PAM Agent.
3. Установите и настройте Indeed PAM Desktop Console.

Тестовый запуск Indeed PAM

1. Проверьте работу серверных и клиентских компонентов.
2. Устраните ошибки.
3. Проверьте сценарии заказчика:
    - Настройте сервисные операции для ресурсов с ОС Windows.
    - Настройте сервисные операции для ресурсов с ОС Linux.
    - Настройте сервисные операции в службе каталогов.
    - Настройте пользовательские типы сервисных подключений.

Завершающий этап

1. Продемонстрируйте функционал.
2. Обучите работе с PAM.
3. Введите PAM в эксплуатацию.

Подготовка к установке

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

Количество глав: 3

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.

Поддерживаются следующие службы каталогов:

- Active Directory;
- FreeIPA 4.12.1 и ниже;
- OpenLDAP 2.6 и ниже;
- ALD Pro 3.0 и ниже;
- RED ADM 2.0.1 и ниже;
- Samba DC 4.23 и ниже.

> ⓘ **ПРИМЕЧАНИЕ**
> В Indeed PAM версии 3.2 и выше доступна работа с внутренними пользователями без подключения службы каталогов.

Учетная запись для работы с каталогом пользователей

Active Directory

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.

FreeIPA

1. Запустите оснастку FreeIPA под пользователем с правами администратора.
2. Создайте пользователя, например, **IPAMADReadOps**.
3. Откройте вкладку **IPA Server**.

4. В выпадающем меню **Role-Based Access Control** выберите пункт **Permissions**.
5. Создайте разрешение со следующими значениями:
   - **Permission name**: `pam_attr_read`.
   - **Granted Rights**: `read`, `search`.
   - **Effective attributes**: `entryDn`, `entryUUID`, `ipaUniqueID`, `ipaNTSecurityIdentifier`, `memberOf`, `uid`, `givenName`, `krbPrincipalName`, `cn`, `sn`, `photo` (или `jpegPhoto`), `member`, `nsOsVersion`, `fqdn`, `initials`, `krbPasswordExpiration`.
6. В выпадающем меню **Role-Based Access Control** выберите пункт **Privileges**.
7. Создайте новую привилегию (например, `pam_privilege_read`) и добавьте в нее только что созданное разрешение `pam_attr_read`.
8. В выпадающем меню **Role-Based Access Control** выберите пункт **Roles**.
9. Создайте новую роль (например, `IPAMADReadOps_role`) и добавьте в нее созданную привилегию `pam_privilege`.
10. Назначьте созданную роль на пользователя **IPAMADServiceOps** одним из способов:
    - назначьте роль на пользователя;
    - назначьте роль на группу пользователей и добавьте пользователя в эту группу.

ALD Pro

1. Запустите оснастку ALD Pro **Пользователи и компьютеры**, в выпадающем меню выберите пункт **Пользователи**.
2. Нажмите **Новый пользователь**.
3. В поле **Имя учетной записи** укажите **IPAMADReadOps** или другое удобное для вас имя учетной записи для работы с каталогом пользователей.
4. Заполните обязательные поля и завершите создание учетной записи.
5. Добавьте созданного пользователя в группу admins.

OpenLDAP

1. Создайте пользователя, например, **IPAMADReadOps**.
2. Выдайте пользователю права на чтение следующих атрибутов:
   - `entryUUID`
   - `entryDn`
   - `uid`
   - `cn`
   - `osVersion`
   - `groupOfUniqueNames`

- `uniqueMember`

RED ADM

Создайте учетную запись одним из описанных ниже способов.

Чтобы создать учетную запись с помощью оснастки **Active Directory — пользователи и компьютеры** (Active Directory Users and Computers), выполните следующие шаги:

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.

Чтобы создать учетную запись с помощью веб-интерфейса RED ADM, выполните следующие шаги:

1. Откройте веб-интерфейс RED ADM.
2. В левой части экрана выберите пункт **Пользователи**.
3. Нажмите **Создать**.
4. Укажите имя, например, **IPAMADReadOps**.
5. Заполните обязательные поля и завершите создание учетной записи.

Samba DC

Создайте учетную запись одним из описанных ниже способов.

Чтобы создать учетную запись с помощью оснастки **Active Directory — пользователи и компьютеры** (Active Directory Users and Computers), выполните следующие шаги:

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.

Чтобы создать учетную запись с помощью командной строки, введите следующую команду:

```
samba-tool user create IPAMADReadOps
```

Учетная запись для сервисных операций

Active Directory

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.

FreeIPA

1. Запустите оснастку FreeIPA под пользователем с правами администратора.
2. Создайте пользователя, например, **IPAMADServiceOps**.
3. Откройте вкладку **IPA Server**.
4. В выпадающем меню **Role-Based Access Control** выберите пункт **Permissions**.
5. Создайте разрешение со следующими значениями:
   - **Permission name**: `pam_attr_read`.
   - **Granted Rights**: `read`, `search`.
   - **Effective attributes**: `entryDn`, `entryUUID`, `ipaUniqueID`, `ipaNTSecurityIdentifier`, `memberOf`, `uid`, `givenName`, `krbPrincipalName`, `cn`, `sn`, `photo` (или `jpegPhoto`), `member`,

`nsOsVersion`, `fqdn`, `initials`, `krbPasswordExpiration`.

6. Создайте еще одно разрешение со следующими значениями:
   - **Permission name**: `pam_attr_write`.
   - **Granted Rights**: `write`.
   - **Effective attributes**: `userPassword`, `krbPasswordExpiration`.
7. В выпадающем меню **Role-Based Access Control** выберите пункт **Privileges**.
8. Создайте новую привилегию (например, `pam_privilege_change_pswd`) и добавьте в нее только что созданные два разрешения `pam_attr_read` и `pam_attr_write`.
9. В выпадающем меню **Role-Based Access Control** выберите пункт **Roles**.
10. Создайте новую роль (например, `IPAMADServiceOps_role`) и добавьте в нее созданную привилегию `pam_privilege_change_pswd`.
11. Назначьте созданную роль на пользователя **IPAMADServiceOps** одним из способов:
    - назначьте роль на пользователя;
    - назначьте роль на группу пользователей и добавьте пользователя в эту группу.

ALD Pro

1. Запустите оснастку ALD Pro **Пользователи и компьютеры**, в выпадающем меню выберите пункт **Пользователи**.
2. Нажмите **Новый пользователь**.
3. В поле **Имя учетной записи** укажите **IPAMADServiceOps** или другое удобное для вас имя учетной записи для работы с каталогом пользователей.
4. Заполните обязательные поля и завершите создание учетной записи.
5. Добавьте созданного пользователя в группу admins.

OpenLDAP

1. Создайте пользователя, например, **IPAMADServiceOps**.
2. Выдайте пользователю права на чтение следующих атрибутов:
   - `entryUUID`
   - `entryDn`
   - `uid`
   - `cn`
   - `osVersion`
   - `groupOfUniqueNames`
   - `uniqueMember`

3. Выдайте пользователю права на запись для атрибута `userPassword`.

RED ADM

Создайте учетную запись одним из описанных ниже способов.

Чтобы создать учетную запись с помощью оснастки **Active Directory — пользователи и компьютеры** (Active Directory Users and Computers), выполните следующие шаги:

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.

Чтобы создать учетную запись с помощью веб-интерфейса RED ADM, выполните следующие шаги:

1. Откройте веб-интерфейс RED ADM.
2. В левой части экрана выберите пункт **Пользователи**.
3. Нажмите **Создать**.
4. Укажите имя, например, **IPAMADServiceOps**.
5. Заполните обязательные поля и завершите создание учетной записи.
6. Добавьте созданного пользователя в группу Account Operators.

Samba DC

Создайте учетную запись одним из описанных ниже способов.

Чтобы создать учетную запись с помощью оснастки **Active Directory — пользователи и компьютеры** (Active Directory Users and Computers), выполните следующие шаги:

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.

Чтобы создать учетную запись с помощью командной строки, выполните следующие шаги:

1. Создайте пользователя **IPAMADServiceOps** командой:

```
samba-tool user create IPAMADServiceOps
```

2. Добавьте созданного пользователя в группу Account Operators командой:

```
samba-tool group addmembers "Account Operators" IPAMADServiceOps
```

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.

Требования к сертификатам

- Сертификаты должны быть действующими.
- Минимальная длина RSA-ключа: 2048.
- Заданы настройки:
  - Для расширения *Enhanced Key Usage (EKU)* указано *Server Authentication*.
    Настройка позволяет использовать сертификат для аутентификации сервера.
  - Для расширения *Key Usage* указано *Digital Signature* и *Key Encipherment*.
    Настройка определяет криптографические операции: позволяет ключу создавать цифровые подписи и разрешает шифровать симметричные ключи сессии.
- В сертификате указаны Common Name (CN) и Subject Alternative Names (SAN).
  Поля содержат доменные имена хоста в формате FQDN.

Схема заполнения CN и SAN

При формировании сертификата поля CN и SAN заполняются в зависимости от роли и принадлежности хоста отказоустойчивому кластеру (Keepalived), а также от наличия балансировщика.

Наличие балансировщика	Хост — балансировщик в кластере Keepalived	Хост совмещает сервер доступа	Конфигурация сертификата
Нет	Нет	Нет	Поле Subject: `CN` — имя хоста Поле SAN: `DNS` — имя хоста
Да	Да	Нет	Поле Subject: `CN` — имя хоста Поле SAN: `DNS` — имя хоста `DNS` — FQDN PAM
Да	Нет	Да	Поле Subject: `CN` — имя хоста Поле SAN: `DNS` — имя хоста `DNS` — FQDN PAM
Да	Нет	Нет	Поле Subject: `CN` — имя хоста Поле SAN: `DNS` — имя хоста

Перечень сертификатов

Инсталляция без балансировки

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.

Отказоустойчивая инсталляция с HAProxy

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 управления с приватным ключом в формате .pfx.
- Сертификаты на все серверы доступа RDP, RDS и PostgreSQL с альтернативными именами всех балансировщиков и FQDN PAM с приватным ключом в формате .pfx. Кроме случая, когда сервер доступа установлен на одном хосте с сервером управления.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> Если на одном хосте планируется расположить балансировщик и сервер управления, то потребуется сертификат с альтернативным именем FQDN PAM.
>
> При использовании vIP в каждом сертификате балансировщика нужно альтернативное имя FQDN PAM.
>
> Если есть серверы доступа на Windows, то их сертификаты должны содержать FQDN PAM или быть такими же, как для FQDN PAM, иначе проверка сертификатов в мастере приведет к ошибке.

Отказоустойчивая инсталляция со сторонним балансировщиком

Вам понадобятся следующие сертификаты:

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

⚠ **ПРЕДУПРЕЖДЕНИЕ**

Если на одном хосте планируется расположить балансировщик и сервер управления, то потребуется сертификат с альтернативным именем FQDN PAM.

При использовании vIP в каждом сертификате балансировщика нужно альтернативное имя FQDN PAM.

ⓘ **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 сертификат удостоверяющего центра в *IndeedPAM_3.4_RU\indeed-pam\state\target\ca-certificates* перед запуском мастера.

Базы данных

Для хранения данных Indeed PAM использует:

- **Core** — БД компонента Indeed PAM Core, используется для хранения данных привилегированных учетных записей, ресурсов, разрешений и других 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 событий Indeed PAM.

Создание баз данных

MSSQL

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**.

PostgreSQL

Клиент pgAdmin

1. Запустите **pgAdmin** и выполните подключение к экземпляру PostgreSQL.
2. Откройте контекстное меню пункта **Базы данных** (Databases).
3. Выберите пункт **Создать** (Create) и **База данных** (Database).
4. Укажите имя базы данных, например: **Core**, **CoreJobs**, **Idp**, **IdpJobs**, **ILS**.
5. Нажмите **Сохранить** (Save).

Консольный клиент psql

1. Запустите командную строку от имени администратора.
2. Выполните подключение к экземпляру PostgreSQL от имени суперпользователя `postgres`:

```
psql -U postgres -h <host> -p <port>
```

- `host` — IP-адрес или DNS-имя сервера.
- `port` — порт, по умолчанию `5432`.

После успешного подключения приглашение командной строки изменится на `postgres=#`.

3. Создайте базы данных **Core**, **CoreJobs**, **Idp**, **IdpJobs**, **ILS** командой:

```
CREATE DATABASE Core;
CREATE DATABASE CoreJobs;
CREATE DATABASE Idp;
CREATE DATABASE IdpJobs;
CREATE DATABASE ILS;
```

4. Убедитесь, что базы данных созданы:

```
\l
```

Jatoba

> ⓘ **ИНФОРМАЦИЯ**
> Jatoba поддерживает работу консольного клиента psql.

1. Запустите командную строку от имени администратора.

2. Выполните подключение к экземпляру Jatoba от имени суперпользователя `postgres`:

```
psql -U postgres -h <host> -p <port>
```

- `host` — IP-адрес или DNS-имя сервера.
- `port` — порт, по умолчанию `5432`.

После успешного подключения приглашение командной строки изменится на `postgres=#`.

3. Создайте базы данных **Core**, **CoreJobs**, **Idp**, **IdpJobs**, **ILS** командой:

```
CREATE DATABASE Core;
CREATE DATABASE CoreJobs;
CREATE DATABASE Idp;
CREATE DATABASE IdpJobs;
CREATE DATABASE ILS;
```

4. Убедитесь, что базы данных созданы:

```
\l
```

Создание и назначение учетной записи для работы с хранилищем данных

MSSQL

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.
>
> Для работы PAM требуется выполнить установку сертификата для инстанса MSSQL.

PostgreSQL

Клиент pgAdmin

1. Запустите **pgAdmin** и выполните подключение к экземпляру PostgreSQL.
2. Откройте контекстное меню пункта **Роли входа/группы** (Login/Group Roles).
3. Выберите пункт **Создать** (Create) и **Роль входа/группы** (Login/Group Role).
4. Укажите **Имя** (Name) учетной записи, например, **IPAMSQLServiceOps**.
5. Перейдите на вкладку **Определения** (Definition) и введите пароль для учетной записи.
6. Перейдите на вкладку **Права** (Privileges), выберите **Да** (Yes) для пунктов **Вход разрешен?** (Can login?) и **Суперпользователь?** (Superuser?).
7. Нажмите **Сохранить** (Save).

Консольный клиент psql

1. Запустите командную строку от имени администратора.
2. Выполните подключение к экземпляру PostgreSQL от имени суперпользователя `postgres`:

   ```
   psql -U postgres -h <host> -p <port>
   ```

   - `host` — IP-адрес или DNS-имя сервера.
   - `port` — порт, по умолчанию `5432`.

   После успешного подключения приглашение командной строки изменится на `postgres=#`.
3. Создайте роль с указанием имени и пароля:

   ```
   CREATE ROLE <username> WITH LOGIN PASSWORD 'your_password_here' SUPERUSER;
   ```

   - `username` — содержит имя учетной записи, например, `IPAMSQLServiceOps`.
   - `LOGIN` — разрешает роли подключаться к серверу БД.
   - `PASSWORD` — задает пароль, например, `'DB_Prod_Password789!'`.
   - `SUPERUSER` — задает права суперпользователя.
4. Убедитесь, что создана роль с атрибутами `Can login` и `Superuser`:

   ```
   \du <username>
   ```

> ⓘ **ПРИМЕЧАНИЕ**
>
> Права **Superuser** для PostgreSQL требуются только для первого обращения к БД.

Jatoba

> **ИНФОРМАЦИЯ**
> Jatoba поддерживает работу консольного клиента psql.

1. Запустите командную строку от имени администратора.

2. Выполните подключение к экземпляру Jatoba от имени суперпользователя `postgres`:

```
psql -U postgres -h <host> -p <port>
```

   - `host` — IP-адрес или DNS-имя сервера.
   - `port` — порт, по умолчанию `5432`.

   После успешного подключения приглашение командной строки изменится на `postgres=#`.

3. Создайте роль с указанием имени и пароля:

```
CREATE ROLE <username> WITH LOGIN PASSWORD 'your_password_here' SUPERUSER;
```

   - `username` — содержит имя учетной записи, например, `IPAMSQLServiceOps`.
   - `LOGIN` — разрешает роли подключаться к серверу БД.
   - `PASSWORD` — задает пароль, например, `'DB_Prod_Password789!'`.
   - `SUPERUSER` — задает права суперпользователя.

4. Убедитесь, что создана роль с атрибутами `Can login` и `Superuser`:

```
\du <username>
```

Медиахранилище

SMB-хранилище

Создайте и настройте SMB-хранилище

NFS-хранилище

Создайте и настройте NFS-хранилище

S3-хранилище

Настройте S3-хранилище на базе MinIO

SMB-хранилище

Indeed PAM поддерживает работу файлового хранилища на основе сетевого протокола доступа SMB (Server Message Block). SMB-хранилище является стандартным сетевым хранилищем для ОС Windows.

Чтобы создать и настроить хранилище:

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

Системные требования

> **ИНФОРМАЦИЯ**
> Системные требования к хранилищу рассчитаны на примере инсталляции PAM с 700 одновременными сессиями с видеологированием.

Рекомендуемые системные требования:

- Количество ядер процессора: 6 ядер.
- Тактовая частота процессора: 2.8 ГГц и более.
- Поддержка технологии гиперпоточности, например, Hyper-threading.
- Объем оперативной памяти: 16 ГБ.
- Пропускная способность канала: 1 Гбит/с.
- Дисковая система: RAID-массив с чередованием (например, RAID 0) или SSD-накопитель в качестве кеша для массива дисков.

NFS-хранилище

Indeed PAM поддерживает работу файлового хранилища на основе сетевого протокола доступа NFS (Network File System).

Подготовка хранилища на Linux

RPM

1. Установите 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
   ```

DEB

1. Установите пакеты:

   ```
   sudo apt update
   sudo apt install nfs-kernel-server
   ```

2. Запустите службы NFS-сервера:

   ```
   sudo systemctl start nfs-kernel-server.service
   sudo systemctl enable nfs-kernel-server.service
   sudo systemctl status nfs-kernel-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 DEB (например, Ubuntu, Debian) также может потребоваться настройка firewall, чтобы разрешить доступ к NFS.

   - Чтобы проверить статус firewall и при необходимости открыть порты для NFS:

     ```
     sudo ufw status
     sudo ufw allow from <IP-адрес_клиента> to any port nfs
     sudo ufw allow 2049/tcp
     sudo ufw allow 111/tcp
     sudo ufw allow 111/udp
     ```

   - Если используется AppArmor, убедитесь, что профили для NFS настроены должным образом. В некоторых случаях может потребоваться их корректировка или временное отключение.

```
sudo aa-status
```

Если AppArmor мешает работе NFS, его можно временно отключить для тестирования:

```
sudo systemctl stop apparmor
sudo systemctl disable apparmor
```

Настройка PAM для работы с NFS

Настройка хранилища выполняется после установки Indeed PAM.

Linux

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

   ```
   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/медиахранилища /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/медиахранилища /путь/до/папки/монтирования nfs defaults 0 0
   ```

   Пример команды

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

   Для проверки монтирования выполните:

   ```
   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` требуется добавить путь к монтированному хранилищу:

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

   Пример для Core

```yaml
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 требуется указать путь до монтированного хранилища:

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

7. Перезагрузите контейнеры:

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

Windows

1. Установите клиент для монтирования NFS:
    1. Нажмите в левом нижнем углу **Start** → **Server Manager**.
    2. Нажмите **Add Roles and Features**.
    3. На странице **Features** активируйте чекбокс **Client for NFS** и нажмите **Next**.
    4. Нажмите **Install**.
2. Выполните монтирование хранилища и добавьте в автозапуск:

   Используйте PowerShell без повышения прав.

   Шаблон команды

   ```
   New-PSDrive -PSProvider FileSystem -Name <буква диска> -Root \\
   <fqdn_or_ip_nfs_server>\путь\до\медиахранилища -Persist
   ```

   Пример команды

   ```
   New-PSDrive -PSProvider FileSystem -Name Z -Root
   \\192.168.131.200\mnt\data_storage\ -Persist
   ```

3. Внесите изменения в секцию `Storage` конфигурационных файлов Core и Gateway-Service:
    - Core — путь до конфигурационного файла на сервере управления: *C:\inetpub\wwwroot\core\appsettings.json*
    - Gateway-Service — путь до конфигурационного файла на сервере доступа: *C:\Program Files\Indeed\Indeed PAM\Gateway\Pam.Gateway.Service\appsettings.json*

   Измените секцию `Storage` на:

   Шаблон секции

```
"Storage": {
  "Type": "FileSystem",
  "Settings": {
    "Root": "\\\\<fqdn_or_ip_nfs_server>\\путь\\до\\медиахранилища"
  }
},
```

Пример секции

```
"Storage": {
  "Type": "FileSystem",
  "Settings": {
    "Root": "\\\\192.168.131.200\\mnt\\data_storage\\"
  }
},
```

4. Перезагрузите IIS и службу Gateway-Service:

   - Перезагрузите IIS на сервере управления:

     Откройте **IIS Manager** и выполните команду **Restart** на нужном сервере.

   - Перезагрузите Gateway-Service:

     Откройте **Task Manager**, найдите сервис PAM.Gateway.Service и перезапустите его.

S3-хранилище

Объектные хранилища на основе протокола S3 (Simple Storage Service) позволяют хранить файлы любых типов. Для группировки и хранения файлов используются специальные контейнеры — бакеты (bucket).
Indeed PAM поддерживает работу S3-хранилища MinIO.

Чтобы создать и настроить хранилище:

1. Выполните вход на сервер, который будет выступать в роли файлового хранилища.
2. Перейдите в раздел **Buckets** на левой панели.
3. Нажмите **Create bucket**.
4. Заполните поле **Bucket Name**.
5. Нажмите **Create bucket**.
6. Убедитесь, что в разделе **Buckets** появилось созданное хранилище.
7. Перейдите в раздел **Access Keys** на левой панели.
8. Нажмите **Create Access Key**.
9. Заполните поля **Access Key** и **Secret Key**.

   > ⓘ **ИНФОРМАЦИЯ**
   > Ключи нужны Indeed PAM Gateway Service для доступа к хранилищу. Укажите Access Key и Secret Key в мастере при настройке хранилища данных.

10. Откройте командную строку от имени администратора и проверьте доступность хранилища:

```
rclone lsjson \
--s3-endpoint <hostname> \
--s3-provider Other \
--s3-access-key-id <access-key-id> \
--s3-secret-access-key <secret-access-key> \
--s3-acl public-read-write \
:s3:<bucket_name>
```

    - `hostname` — IP-адрес или DNS-имя сервера с хранилищем.
      Пример: `"http://127.0.0.1:9000"`

- `access-key-id` — Access key (Ключ доступа).
- `secret-access-key` — Secret key (Секретный ключ доступа).
- `bucket_name` — название хранилища.

Если медиахранилище доступно и не содержит файлов, команда вернет пустой список: `[]`.

Серверы

Windows

Для установки компонентов PAM серверы на ОС Windows должны:

- обращаться к одному DNS-серверу;
- находиться в одном домене и сети;
- иметь запущенную службу WinRM;
- иметь имя хоста, совпадающее с DNS-именем сервера, в нижнем регистре и формате FQDN.
  Пример: pam.my-company.local.

Аппаратные и программные требования, а также сетевое взаимодействие для серверов смотрите в разделе Системные требования.

Запуск службы WinRM

Для выполнения сервисных операций на серверах управления и доступа запустите службу WinRM.

Чтобы запустить службу:

1. Запустите PowerShell от имени администратора.
2. Выполните команду:

```
Enable-PSRemoting -Force
```

Команда задает стандартные настройки WinRM, меняет тип запуска службы на автоматический и разрешает входящие сетевые подключения через брандмауэр Windows к портам 5985 и 5986.

Настройка сервера доступа RDS

Пользователи PAM могут открывать Web/Desktop-сессии через сервер доступа RDS. Подключение реализовано с помощью Remote Desktop Services Microsoft (Службы удаленных рабочих столов). Когда пользователь подключается к серверу доступа RDS, запускается приложение Indeed PAM. Приложение проверяет права пользователя, аутентифицирует его и ведет логирование сессии. Запуск приложений осуществляется в режиме RemoteApp.

Чтобы подготовить сервер к работе, включите службу WinRM, разверните роль RDS и настройте брандмауэр.

Перед тем как развернуть сервер с ролью RDS убедитесь, что:

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

Развертывание роли Remote Desktop Services

1. Откройте **Server Manager** (Диспетчер серверов) и в меню **Manage** (Управление) выберите **Add Roles and Features** (Добавить роли и компоненты).
2. Выберите тип установки **Remote Desktop Services Installation** (Установка служб удаленных рабочих столов) и нажмите **Next**.
3. Выберите тип развертывания **Standard deployment** (Стандартное развертывание) и нажмите **Next**.
4. Выберите сценарий развертывания **Session-based desktop deployment** (Развертывание рабочих столов на основе сеансов) и нажмите **Next**.
5. Пропустите шаг **Role Services** (Роли серверов) и нажмите **Next**.
6. Выберите имя текущего сервера на шагах **RD Connection Broker** (Посредник подключений к удаленным рабочим столам), **RD Web Access** (Веб-доступ к удаленным рабочим столам), **RD Session Host** (Узел сеансов удаленных рабочих столов) и нажмите **Next**.
7. Включите опцию **Restart the destination server automatically if required** (Автоматически перезапускать конечный сервер, если это потребуется) и нажмите **Deploy** (Развернуть).
8. После перезагрузки откройте **Server Manager** (Диспетчер серверов) и дождитесь завершения процесса.

Настройка правила брандмауэра

1. Перейдите на вкладку **Local server** (Локальный сервер) и нажмите на значение параметра **Windows Defender Firewall** (Брандмауэр Microsoft Defender).
2. Перейдите в окно **Firewall & network protection** (Брандмауэр и безопасность сети) и нажмите **Advanced settings** (Дополнительные параметры).
3. Перейдите в окно **Windows Defender Firewall with Advanced Security** (Мониторинг брандмауэра Защитника Windows) и откройте вкладку **Inbound Rules** (Правила для входящих подключений).
4. Нажмите **New Rule** (Создать правило) и задайте настройки:
    1. Выберите тип правила **Port** (Для порта) и нажмите **Next**.
    2. Укажите порт в поле **Specific local ports** (Определенные локальные порты):
        - 5985 — для подключений по протоколу HTTP
        - 5986 — для подключений по протоколу HTTPS
    3. Выберите **Allow the connection** (Разрешить подключение) и нажмите **Next**.
    4. Выберите все профили и нажмите **Next**.

5. Введите название правила в поле **Name** (Имя) и нажмите **Finish** (Готово).

Linux

Для установки компонентов PAM серверы на ОС Linux должны:

- обращаться к одному DNS-серверу;
- находиться в одном домене и сети;
- иметь имя хоста, совпадающее с DNS-именем сервера, в нижнем регистре и формате FQDN.
  Пример: pam.my-company.local.

Аппаратные и программные требования, а также сетевое взаимодействие для серверов смотрите в разделе Системные требования.

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).

  Подробнее

  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.

- 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.

Установка

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.

1. Загрузите и распакуйте дистрибутив PAM на Linux-машину.
2. Поместите сертификат удостоверяющего центра в *IndeedPAM_3.3_RU\indeed-pam\state\target\ca-certificates*. Это требуется для корректной работы LDAPS. Пропуск этого шага приведет к ошибке работы мастера.
3. Запустите мастер командой:

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

4. Дождитесь выполнения скрипта.
5. После выполнения скрипта перейдите по URL, указанному в консоли.
6. 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.

7. 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 и необходимые сервера доступа. Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом. Сервер доступа RDS используется для подключения в режиме RemoteApp.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> Разверните PAM по отказоустойчивой схеме, если планируете установить сервер Web Terminal и разместить серверы доступа Web, RDP, SSH, MSSQL или PostgreSQL на двух и более хостах.

Сервер управления

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

Сервер доступа RDS

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> При добавлении сервера доступа RDS учитывайте, что на последующем шаге **Каталоги пользователей** обязательно добавить каталог. Продолжить только с внутренними пользователями нельзя.

1. Нажмите **Добавить хост**.
2. Для переключателя **Операционная система хоста** выберите **Windows**.
3. Включите опцию **Сервер доступа RDS**.
4. Введите IP-адрес или DNS-имя в поле **Адрес хоста**.
   Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.
5. Заполните поле **Порт**.
6. Выберите тип учетной записи для хоста: **Общая доменная УЗ** или **Отдельная УЗ для этого хоста**.
7. Заполните поля **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-имя в поле **Адрес хоста**.
   Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.
5. Заполните поле **Порт**.
6. Выберите способ аутентификации учетной записи на хосте:
   - При выборе **По паролю** заполните поля **Логин** и **Пароль**.
   - При выборе **По SSH-ключу** заполните поля **Логин**, **Пароль sudo**, **Парольная фраза** и загрузите **SSH-ключ**.
7. 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-имя в поле **Адрес хоста**.
   Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.
5. Заполните поле **Порт**.
6. Выберите способ аутентификации учетной записи на хосте:
   - При выборе **По паролю** заполните поля **Логин** и **Пароль**.
   - При выборе **По SSH-ключу** заполните поля **Логин**, **Пароль sudo**, **Парольная фраза** и загрузите **SSH-ключ**.
7. Нажмите **Добавить**.

Сервер доступа MSSQL

1. Нажмите **Добавить хост**.
2. Для переключателя **Операционная система хоста** выберите **Linux**.
3. Включите опцию **Сервер доступа MSSQL**.
4. Введите IP-адрес или DNS-имя в поле **Адрес хоста**.
   Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.
5. Заполните поле **Порт**.
6. Выберите способ аутентификации учетной записи на хосте:
   - При выборе **По паролю** заполните поля **Логин** и **Пароль**.
   - При выборе **По SSH-ключу** заполните поля **Логин**, **Пароль sudo**, **Парольная фраза** и загрузите **SSH-ключ**.
7. Нажмите **Добавить**.

Сервер доступа Web

1. Нажмите **Добавить хост**.
2. Для переключателя **Операционная система хоста** выберите **Linux**.
3. Включите опцию **Сервер доступа Web**.
4. Введите IP-адрес или DNS-имя в поле **Адрес хоста**.
   Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.
5. Заполните поле **Порт**.
6. Выберите тип учетной записи для хоста: **Общая доменная УЗ** или **Отдельная УЗ для этого хоста**.
7. Заполните поля **Логин** в формате UPN или SAM и **Пароль** для указанной учетной записи.
8. Нажмите **Добавить**.

Сервер Web Terminal

1. Нажмите **Добавить хост**.
2. Для переключателя **Операционная система хоста** выберите **Linux**.
3. Включите опцию **Сервер Web Terminal**.
4. Введите IP-адрес или DNS-имя в поле **Адрес хоста**.
   Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.
5. Заполните поле **Порт**.
6. Выберите тип учетной записи для хоста: **Общая доменная УЗ** или **Отдельная УЗ для этого хоста**.
7. Заполните поля **Логин** в формате UPN или SAM и **Пароль** для указанной учетной записи.
8. Нажмите **Добавить**.

> **ИНФОРМАЦИЯ**
> Сервер управления и сервер доступа RDS могут располагаться на одном хосте.
> Сервер Web Terminal и серверы доступа RDP, Web, SSH, MSSQL, 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 **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

> **ПРИМЕЧАНИЕ**
> 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

Компонент	Порт по умолчанию
RDP Proxy	3390
PostgreSQL Proxy	5432
MSSQL Proxy	1433
Web Proxy	5443
MC/UC HTTP	80
MC/UC HTTPS	443
Gateway Service Web Terminal	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.

Выбор базы данных PostgreSQL

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.

ИНФОРМАЦИЯ

База данных Jatoba поддерживается в PAM. Для настройки обратитесь в техническую поддержку.

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.

ПРИМЕЧАНИЕ

После установки PAM настройте файловое хранилище (NFS).

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

Добавьте один или несколько каталогов пользователей, или нажмите **Далее**, чтобы использовать PAM только с внутренними пользователями.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> Если на шаге **Схема хостов** добавлен сервер доступа RDS, то обязательно добавьте каталог. Продолжить только с внутренними пользователями нельзя.

Выбор каталога Active Directory

1. Нажмите **Добавить каталог**.
2. В поле **Служба каталогов** выберите **Active Directory**.
3. В поле **ID каталога** введите идентификатор каталога в PAM.
   Значение может состоять из латинских букв и цифр, максимальная длина — 32 символа.
   Если планируете использовать несколько каталогов, то их ID должны быть разными.
4. Заполните поле **DNS-имя домена**.
5. (Опционально) В поле **Контроллеры домена** укажите адрес контроллера домена в формате FQDN.
   Можно указать несколько адресов через запятую.
   Если не указать адрес, PAM подключится по DNS-имени домена.
6. В поле **DN контейнера пользователей** укажите контейнер или подразделение, в котором располагаются пользователи системы.
7. Введите имя пользователя в формате UPN и его пароль.
   Пример: `pamadmin@my.company`.
8. (Опционально) Включите опцию **Использовать LDAPS**.
9. (Опционально) Измените соответствие атрибутов пользователей и/или атрибутов групп пользователей.
10. Нажмите **Добавить**.
11. Нажмите **Далее** для перехода к следующему шагу мастера.

Выбор каталога ALD PRO, FreeIPA, OpenLDAP

1. Нажмите **Добавить каталог**.
2. В поле **Служба каталогов** выберите **ALD PRO**, **FreeIPA** или **OpenLDAP**.
3. В поле **ID каталога** введите идентификатор каталога в PAM.
   Значение может состоять из латинских букв и цифр, максимальная длина — 32 символа.
   Если планируете использовать несколько каталогов, то их ID должны быть разными.
4. Заполните поле **DNS-имя домена**.
5. (Опционально) В поле **Контроллеры домена** укажите адрес контроллера домена в формате FQDN.
   Можно указать несколько адресов через запятую.
   Если не указать адрес, PAM подключится по DNS-имени домена.
6. В поле **DN контейнера пользователей** укажите контейнер или подразделение, в котором располагаются пользователи системы.
7. Введите имя пользователя в формате DN и его пароль.
   Пример: `'uid=pamadmin,cn=users,cn=accounts,dc=my,dc=company'`.
8. (Опционально) Включите опцию **Использовать LDAPS**.
9. Если выбрали ALD PRO или FreeIPA, то укажите **Формат идентификатора пользователей и групп** — SID или GUID.
10. (Опционально) Измените соответствие атрибутов пользователей и/или атрибутов групп пользователей.
11. Нажмите **Добавить**.
12. Нажмите **Далее** для перехода к следующему шагу мастера.

Выбор каталога RED ADM, Samba DC

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> При выборе каталогов RED ADM или Samba DC версии 4.20.8 и ниже добавьте в конфигурационный файл в секцию `[global]` строку: `ldap server require strong auth = allow_sasl_over_tls`
>
> Конфигурационный файл нужно отредактировать на всех контроллерах домена или на контроллере, который будет использоваться PAM для получения доступа к службе каталогов.
>
> Конфигурационные файлы находятся по пути:
>
> - Samba DC: */etc/samba/smb.conf*
> - RED ADM: */opt/reddc/etc/smb.conf*

1. Нажмите **Добавить каталог**.
2. В поле **Служба каталогов** выберите **RED ADM** или **Samba DC**.
3. В поле **ID каталога** введите идентификатор каталога в PAM.
   Значение может состоять из латинских букв и цифр, максимальная длина — 32 символа.
   Если планируете использовать несколько каталогов, то их ID должны быть разными.
4. Заполните поле **DNS-имя домена**.
5. (Опционально) В поле **Контроллеры домена** укажите адрес контроллера домена в формате FQDN.
   Можно указать несколько адресов через запятую.
   Если не указать адрес, PAM подключится по DNS-имени домена.
6. В поле **DN контейнера пользователей** укажите контейнер или подразделение, в котором располагаются пользователи системы.
7. Введите имя пользователя в формате UPN и его пароль.
   Пример: `pamadmin@my.company`.
8. (Опционально) Включите опцию **Использовать LDAPS**.
9. (Опционально) Измените соответствие атрибутов пользователей и/или атрибутов групп пользователей.
10. Нажмите **Добавить**.
11. Нажмите **Далее** для перехода к следующему шагу мастера.

Администраторы ролей

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

В качестве администратора ролей можно выбрать как пользователя из каталога, так и внутреннего. Выбранному пользователю будут выданы права на управление ролями PAM. Этот пользователь сможет выдать права на доступ к консоли управления PAM другим пользователям.

Из каталога

1. Выберите из каталога учетную запись.
2. Нажмите **Далее** для перехода к следующему шагу мастера.

Внутренний

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> При выборе внутреннего пользователя в качестве первого администратора ролей учитывайте, что на следующем шаге **Аутентификация пользователей** механизм аутентификации Windows недоступен. Такая комбинация настроек является некорректной конфигурацией PAM, т.к. администратор не может аутентифицироваться в системе.

1. Задайте логин.

   > ⚠ **ПРЕДУПРЕЖДЕНИЕ**
   > Логин нельзя изменять после установки PAM.

2. Задайте или сгенерируйте пароль. Пароль потребуется только для первого входа. После входа система автоматически запросит его смену.
3. Введите Email.
4. Нажмите **Далее** для перехода к следующему шагу мастера.

Аутентификация пользователей

На этом шаге требуется задать механизм аутентификации и настройки двухфакторной аутентификации.

Механизм аутентификации

1. Выберите подходящий вариант: LDAP, RADIUS или Windows.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Если на предыдущем шаге **Администраторы ролей** выбран внутренний пользователь, то выбор механизма Windows недоступен. Такая комбинация настроек является некорректной конфигурацией PAM, т.к. администратор не может аутентифицироваться в системе.
>
> Если в качестве первого администратора выбран пользователь из каталога, то выбрать механизм Windows можно. При такой конфигурации работа с внутренними пользователями не поддерживается.

2. При выборе RADIUS добавьте сервер RADIUS и введите необходимые данные.

Аутентификация по RADIUS

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> Для внутренних пользователей недоступна аутентификация через RADIUS. Заданные здесь настройки действуют только на пользователей из каталога.

При выборе RADIUS в качестве механизма аутентификации требуется 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.

Настройка 2FA

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> При выборе механизма аутентификации RADIUS пользователи из каталога аутентифицируются через RADIUS, а указанные ниже настройки действуют только на внутренних пользователей.

1. Включите опцию **Включить двухфакторную аутентификацию для всех пользователей по умолчанию**.
2. Для переключателя **Тип второго фактора** выберите подходящее значение: TOTP или Email.
3. Отметьте компоненты, для которых требуется включить кеширование второго фактора:
   - Management Console
   - User Console

- Desktop Console
- SSH Proxy
- RDP Proxy
- RDS Proxy

4. Если требуется, отредактируйте значение в поле **Время кеширования**.
5. 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 отправляется письмо
- Порт
- Имя пользователя — логин для авторизации на сервере
- Пароль

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

Syslog-сервер используется для интеграции с SIEM-системой и выполняет роль единого хранилища для записей событий PAM и текстовых логов сессий. Данные обновляются в режиме реального времени. Это позволяет быстро выявлять инциденты и аномалии, связанные с действиями привилегированных пользователей.

1. Заполните данные для подключения Syslog-сервера.
   Можно пропустить этот шаг и при необходимости добавить Syslog-сервер после установки PAM.

   Syslog-сервер

   При добавлении Syslog-сервера заполните поля:

   - Адрес сервера;
   - Сетевой протокол: TCP или UDP;
   - 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.

> **ПРИМЕЧАНИЕ**
>
> Файлы с логами установки находятся по следующему пути: *IndeedPAM_3.4_RU/indeed-pam/logs/*.
>
> В случае возникновения ошибки установки просмотрите эти файлы и при необходимости обратитесь за помощью по исправлению ошибки в техническую поддержку.

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
```

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.

1. Загрузите и распакуйте дистрибутив PAM на Linux-машину.
2. Поместите сертификат удостоверяющего центра в *IndeedPAM_3.3_RU\indeed-pam\state\target\ca-certificates*. Это требуется для корректной работы LDAPS. Пропуск этого шага приведет к ошибке работы мастера.
3. Запустите мастер командой:

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

4. Дождитесь выполнения скрипта.
5. После выполнения скрипта перейдите по URL, указанному в консоли.
6. 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.

7. 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 и необходимые сервера доступа. Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом. Сервер доступа RDS используется для подключения в режиме RemoteApp.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> Разверните PAM по отказоустойчивой схеме, если планируете установить сервер Web Terminal и разместить серверы доступа Web, RDP, SSH, MSSQL или PostgreSQL на двух и более хостах.

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-имя в поле **Адрес хоста**.
   Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.
5. Заполните поле **Порт**.
6. Выберите способ аутентификации учетной записи на хосте:
   - При выборе **По паролю** заполните поля **Логин** и **Пароль**.
   - При выборе **По SSH-ключу** заполните поля **Логин**, **Пароль sudo**, **Парольная фраза** и загрузите **SSH-ключ**.
7. 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-имя в поле **Адрес хоста**.
   Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.
5. Заполните поле **Порт**.
6. Выберите способ аутентификации учетной записи на хосте:
   - При выборе **По паролю** заполните поля **Логин** и **Пароль**.
   - При выборе **По SSH-ключу** заполните поля **Логин**, **Пароль sudo**, **Парольная фраза** и загрузите **SSH-ключ**.
7. 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-имя в поле **Адрес хоста**.
   Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.
5. Заполните поле **Порт**.
6. Выберите способ аутентификации учетной записи на хосте:
   - При выборе **По паролю** заполните поля **Логин** и **Пароль**.
   - При выборе **По SSH-ключу** заполните поля **Логин**, **Пароль sudo**, **Парольная фраза** и загрузите **SSH-ключ**.
7. 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-имя в поле **Адрес хоста**.
   Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.
5. Заполните поле **Порт**.
6. Выберите способ аутентификации учетной записи на хосте:
   - При выборе **По паролю** заполните поля **Логин** и **Пароль**.
   - При выборе **По SSH-ключу** заполните поля **Логин**, **Пароль sudo**, **Парольная фраза** и загрузите **SSH-ключ**.
7. Нажмите **Добавить**.

Сервер доступа MSSQL

1. Нажмите **Добавить хост**.
2. Для переключателя **Операционная система хоста** выберите **Linux**.
3. Включите опцию **Сервер доступа MSSQL**.
4. Введите IP-адрес или DNS-имя в поле **Адрес хоста**.
   Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.
5. Заполните поле **Порт**.
6. Выберите способ аутентификации учетной записи на хосте:
   - При выборе **По паролю** заполните поля **Логин** и **Пароль**.
   - При выборе **По SSH-ключу** заполните поля **Логин**, **Пароль sudo**, **Парольная фраза** и загрузите **SSH-ключ**.
7. 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-имя в поле **Адрес хоста**.
   Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.
5. Заполните поле **Порт**.
6. Выберите тип учетной записи для хоста: **Общая доменная УЗ** или **Отдельная УЗ для этого хоста**.
7. Заполните поля **Логин** в формате UPN или SAM и **Пароль** для указанной учетной записи.
8. Нажмите **Добавить**.

Сервер доступа Web

1. Нажмите **Добавить хост**.
2. Для переключателя **Операционная система хоста** выберите **Linux**.
3. Включите опцию **Сервер доступа Web**.
4. Введите IP-адрес или DNS-имя в поле **Адрес хоста**.
   Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.
5. Заполните поле **Порт**.
6. Выберите тип учетной записи для хоста: **Общая доменная УЗ** или **Отдельная УЗ для этого хоста**.
7. Заполните поля **Логин** в формате UPN или SAM и **Пароль** для указанной учетной записи.
8. Нажмите **Добавить**.

Сервер Web Terminal

1. Нажмите **Добавить хост**.
2. Для переключателя **Операционная система хоста** выберите **Linux**.
3. Включите опцию **Сервер Web Terminal**.
4. Введите IP-адрес или DNS-имя в поле **Адрес хоста**.
   Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.
5. Заполните поле **Порт**.
6. Выберите тип учетной записи для хоста: **Общая доменная УЗ** или **Отдельная УЗ для этого хоста**.
7. Заполните поля **Логин** в формате UPN или SAM и **Пароль** для указанной учетной записи.
8. Нажмите **Добавить**.

> **ИНФОРМАЦИЯ**
> Сервер управления, Web Terminal, а также серверы доступа RDP, Web, SSH, MSSQL и 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 **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

> ⓘ **ПРИМЕЧАНИЕ**
> Порты компонентов PAM должны быть уникальными.

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
MSSQL Proxy	1433
Web Proxy	5443
MC/UC HTTP	80
MC/UC HTTPS	443
Gateway Service Web Terminal	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.

Выбор базы данных Microsoft SQL

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.

ИНФОРМАЦИЯ

База данных Jatoba поддерживается в PAM. Для настройки обратитесь в техническую поддержку.

Хранилище данных

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

> **ПРИМЕЧАНИЕ**
> После установки PAM настройте файловое хранилище (NFS).

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

Добавьте один или несколько каталогов пользователей, или нажмите **Далее**, чтобы использовать PAM только с внутренними пользователями.

Выбор каталога ALD PRO, FreeIPA, OpenLDAP

1. Нажмите **Добавить каталог**.
2. В поле **Служба каталогов** выберите **ALD PRO**, **FreeIPA** или **OpenLDAP**.
3. В поле **ID каталога** введите идентификатор каталога в PAM.
   Значение может состоять из латинских букв и цифр, максимальная длина — 32 символа.
   Если планируете использовать несколько каталогов, то их ID должны быть разными.
4. Заполните поле **DNS-имя домена**.
5. (Опционально) В поле **Контроллеры домена** укажите адрес контроллера домена в формате FQDN.
   Можно указать несколько адресов через запятую.
   Если не указать адрес, PAM подключится по DNS-имени домена.
6. В поле **DN контейнера пользователей** укажите контейнер или подразделение, в котором располагаются пользователи системы.
7. Введите имя пользователя в формате DN и его пароль.
   Пример: `'uid=pamadmin,cn=users,cn=accounts,dc=my,dc=company'`.
8. (Опционально) Включите опцию **Использовать LDAPS**.
9. Если выбрали ALD PRO или FreeIPA, то укажите **Формат идентификатора пользователей и групп** — SID или GUID.
10. (Опционально) Измените соответствие атрибутов пользователей и/или атрибутов групп пользователей.
11. Нажмите **Добавить**.
12. Нажмите **Далее** для перехода к следующему шагу мастера.

Выбор каталога RED ADM, Samba DC

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> При выборе каталогов RED ADM или Samba DC версии 4.20.8 и ниже добавьте в конфигурационный файл в секцию `[global]` строку: `ldap server require strong auth = allow_sasl_over_tls`
>
> Конфигурационный файл нужно отредактировать на всех контроллерах домена или на контроллере, который будет использоваться PAM для получения доступа к службе каталогов.
>
> Конфигурационные файлы находятся по пути:
>
> - Samba DC: */etc/samba/smb.conf*
> - RED ADM: */opt/reddc/etc/smb.conf*

1. Нажмите **Добавить каталог**.
2. В поле **Служба каталогов** выберите **RED ADM** или **Samba DC**.
3. В поле **ID каталога** введите идентификатор каталога в PAM.
   Значение может состоять из латинских букв и цифр, максимальная длина — 32 символа.
   Если планируете использовать несколько каталогов, то их ID должны быть разными.
4. Заполните поле **DNS-имя домена**.
5. (Опционально) В поле **Контроллеры домена** укажите адрес контроллера домена в формате FQDN.
   Можно указать несколько адресов через запятую.
   Если не указать адрес, PAM подключится по DNS-имени домена.
6. В поле **DN контейнера пользователей** укажите контейнер или подразделение, в котором располагаются пользователи системы.
7. Введите имя пользователя в формате UPN и его пароль.
   Пример: `pamadmin@my.company`.
8. (Опционально) Включите опцию **Использовать LDAPS**.
9. (Опционально) Измените соответствие атрибутов пользователей и/или атрибутов групп пользователей.
10. Нажмите **Добавить**.
11. Нажмите **Далее** для перехода к следующему шагу мастера.

Выбор каталога Active Directory

1. Нажмите **Добавить каталог**.
2. В поле **Служба каталогов** выберите **Active Directory**.
3. В поле **ID каталога** введите идентификатор каталога в PAM.
   Значение может состоять из латинских букв и цифр, максимальная длина — 32 символа.
   Если планируете использовать несколько каталогов, то их ID должны быть разными.
4. Заполните поле **DNS-имя домена**.
5. (Опционально) В поле **Контроллеры домена** укажите адрес контроллера домена в формате FQDN.
   Можно указать несколько адресов через запятую.
   Если не указать адрес, PAM подключится по DNS-имени домена.
6. В поле **DN контейнера пользователей** укажите контейнер или подразделение, в котором располагаются пользователи системы.
7. Введите имя пользователя в формате UPN и его пароль.
   Пример: `pamadmin@my.company`.
8. (Опционально) Включите опцию **Использовать LDAPS**.
9. (Опционально) Измените соответствие атрибутов пользователей и/или атрибутов групп пользователей.
10. Нажмите **Добавить**.
11. Нажмите **Далее** для перехода к следующему шагу мастера.

Администраторы ролей

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

В качестве администратора ролей можно выбрать как пользователя из каталога, так и внутреннего. Выбранному пользователю будут выданы права на управление ролями PAM. Этот пользователь сможет выдать права на доступ к консоли управления PAM другим пользователям.

Из каталога

1. Выберите из каталога учетную запись.
2. Нажмите **Далее** для перехода к следующему шагу мастера.

Внутренний

1. Задайте логин.

   > ⚠ **ПРЕДУПРЕЖДЕНИЕ**
   > Логин нельзя изменять после установки PAM.

2. Задайте или сгенерируйте пароль. Пароль потребуется только для первого входа. После входа система автоматически запросит его смену.

3. Введите Email.

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

Аутентификация пользователей

На этом шаге требуется задать механизм аутентификации и настройки двухфакторной аутентификации.

Механизм аутентификации

1. Выберите подходящий вариант: LDAP или RADIUS.
2. При выборе RADIUS добавьте сервер RADIUS и введите необходимые данные.

Аутентификация по RADIUS

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> Для внутренних пользователей недоступна аутентификация через RADIUS. Заданные здесь настройки действуют только на пользователей из каталога.

При выборе RADIUS в качестве механизма аутентификации требуется 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.

Настройка 2FA

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> При выборе механизма аутентификации RADIUS пользователи из каталога аутентифицируются через RADIUS, а указанные ниже настройки действуют только на внутренних пользователей.

1. Включите опцию **Включить двухфакторную аутентификацию для всех пользователей по умолчанию**.
2. Для переключателя **Тип второго фактора** выберите подходящее значение: TOTP или Email.
3. Отметьте компоненты, для которых требуется включить кеширование второго фактора:
   - Management Console
   - User Console

- Desktop Console
- SSH Proxy
- RDP Proxy
- RDS Proxy

4. Если требуется, отредактируйте значение в поле **Время кеширования**.
5. 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 отправляется письмо
- Порт
- Имя пользователя — логин для авторизации на сервере
- Пароль

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

Syslog-сервер используется для интеграции с SIEM-системой и выполняет роль единого хранилища для записей событий PAM и текстовых логов сессий. Данные обновляются в режиме реального времени. Это позволяет быстро выявлять инциденты и аномалии, связанные с действиями привилегированных пользователей.

1. Заполните данные для подключения Syslog-сервера.
   Можно пропустить этот шаг и при необходимости добавить Syslog-сервер после установки PAM.

   Syslog-сервер

   При добавлении Syslog-сервера заполните поля:

   - Адрес сервера;
   - Сетевой протокол: TCP или UDP;
   - 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.

> **ПРИМЕЧАНИЕ**
> Файлы с логами установки находятся по следующему пути: *IndeedPAM_3.4_RU/indeed-pam/logs/*.
>
> В случае возникновения ошибки установки просмотрите эти файлы и при необходимости обратитесь за помощью по исправлению ошибки в техническую поддержку.

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
```

Отказоустойчивая на Windows

Компоненты Indeed PAM устанавливаются на четыре сервера без учета балансировщиков нагрузки. Серверы управления и доступа дублируются для обеспечения отказоустойчивости. Схема развертывания с балансировкой подходит для внедрения и эксплуатации в промышленной среде.

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.

1. Загрузите и распакуйте дистрибутив PAM на Linux-машину.
2. Поместите сертификат удостоверяющего центра в *IndeedPAM_3.3_RU\indeed-pam\state\target\ca-certificates*. Это требуется для корректной работы LDAPS. Пропуск этого шага приведет к ошибке работы мастера.
3. Запустите мастер командой:

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

4. Дождитесь выполнения скрипта.
5. После выполнения скрипта перейдите по URL, указанному в консоли.
6. 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.

7. 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** в поле **FQDN PAM** укажите общее полное доменное имя (FQDN), которое направлено на IP-адрес балансировщиков нагрузки.
   Пример: pam.my-company.local.

2. Добавьте сервер управления и необходимые сервера доступа. Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом. Сервер доступа RDS используется для подключения в режиме RemoteApp.

Сервер управления

1. Нажмите **Добавить хост**.
2. Для переключателя **Операционная система хоста** выберите **Windows**.
3. Включите опцию **Сервер управления**.
4. Введите IP-адрес или DNS-имя 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 УЗ** или **Отдельная УЗ для этого хоста**.
7. Заполните поля **Логин** в формате UPN или SAM и **Пароль** для указанной учетной записи.
8. Нажмите **Добавить**.

Сервер доступа RDS

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> При добавлении сервера доступа RDS учитывайте, что на последующем шаге **Каталоги пользователей** обязательно добавить каталог. Продолжить только с внутренними пользователями нельзя.

1. Нажмите **Добавить хост**.
2. Для переключателя **Операционная система хоста** выберите **Windows**.
3. Включите опцию **Сервер доступа RDS**.
4. Введите IP-адрес или DNS-имя в поле **Адрес хоста**.
   Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.
5. Заполните поле **Порт**.
6. Выберите тип учетной записи для хоста: **Общая доменная УЗ** или **Отдельная УЗ для этого хоста**.
7. Заполните поля **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-имя в поле **Адрес хоста**.
   Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.
5. Заполните поле **Порт**.
6. Выберите способ аутентификации учетной записи на хосте:
   - При выборе **По паролю** заполните поля **Логин** и **Пароль**.
   - При выборе **По SSH-ключу** заполните поля **Логин**, **Пароль sudo**, **Парольная фраза** и загрузите **SSH-ключ**.
7. 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-имя в поле **Адрес хоста**.
   Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.
5. Заполните поле **Порт**.
6. Выберите способ аутентификации учетной записи на хосте:
   - При выборе **По паролю** заполните поля **Логин** и **Пароль**.
   - При выборе **По SSH-ключу** заполните поля **Логин**, **Пароль sudo**, **Парольная фраза** и загрузите **SSH-ключ**.
7. Нажмите **Добавить**.

Сервер доступа MSSQL

1. Нажмите **Добавить хост**.
2. Для переключателя **Операционная система хоста** выберите **Linux**.
3. Включите опцию **Сервер доступа MSSQL**.
4. Введите IP-адрес или DNS-имя в поле **Адрес хоста**.
   Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.
5. Заполните поле **Порт**.
6. Выберите способ аутентификации учетной записи на хосте:
   - При выборе **По паролю** заполните поля **Логин** и **Пароль**.
   - При выборе **По SSH-ключу** заполните поля **Логин**, **Пароль sudo**, **Парольная фраза** и загрузите **SSH-ключ**.
7. Нажмите **Добавить**.

Сервер доступа Web

1. Нажмите **Добавить хост**.
2. Для переключателя **Операционная система хоста** выберите **Linux**.
3. Включите опцию **Сервер доступа Web**.
4. Введите IP-адрес или DNS-имя в поле **Адрес хоста**.
   Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.
5. Заполните поле **Порт**.
6. Выберите тип учетной записи для хоста: **Общая доменная УЗ** или **Отдельная УЗ для этого хоста**.
7. Заполните поля **Логин** в формате UPN или SAM и **Пароль** для указанной учетной записи.
8. Нажмите **Добавить**.

Сервер Web Terminal

1. Нажмите **Добавить хост**.
2. Для переключателя **Операционная система хоста** выберите **Linux**.
3. Включите опцию **Сервер Web Terminal**.
4. Введите IP-адрес или DNS-имя в поле **Адрес хоста**.
   Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.
5. Заполните поле **Порт**.
6. Выберите тип учетной записи для хоста: **Общая доменная УЗ** или **Отдельная УЗ для этого хоста**.
7. Заполните поля **Логин** в формате UPN или SAM и **Пароль** для указанной учетной записи.
8. Нажмите **Добавить**.

> **ИНФОРМАЦИЯ**
> Сервер управления и сервер доступа RDS могут располагаться на одном хосте.
> Сервер Web Terminal и серверы доступа Web, SSH, MSSQL и 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 **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.

> **ПРИМЕЧАНИЕ**
> 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. Для переключателя **Балансировщик** выберите **HAProxy**.
2. Нажмите **Добавить балансировщик**.
3. Введите IP-адрес или DNS-имя в поле **Адрес балансировщика**.
4. Заполните поле **Порт**.
5. Выберите способ аутентификации учетной записи на хосте:
   - При выборе **По паролю** заполните поля **Логин** и **Пароль**.
   - При выборе **По SSH-ключу** заполните поля **Логин**, **Пароль sudo**, **Парольная фраза** и загрузите **SSH-ключ**.
6. Нажмите **Добавить**.

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

Порты

> **ПРИМЕЧАНИЕ**
> 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
PostgreSQL Proxy	5432
MSSQL Proxy	1433
Web Proxy	5443
MC/UC HTTP	80
MC/UC HTTPS	443

Компонент	Порт по умолчанию
Gateway Service Web Terminal	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.

Выбор базы данных PostgreSQL

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.

> **ИНФОРМАЦИЯ**
>
> База данных Jatoba поддерживается в PAM. Для настройки обратитесь в техническую поддержку.

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.

> **ПРИМЕЧАНИЕ**
>
> После установки PAM настройте файловое хранилище (NFS).

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

Добавьте один или несколько каталогов пользователей, или нажмите **Далее**, чтобы использовать PAM только с внутренними пользователями.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> Если на шаге **Схема хостов** добавлен сервер доступа RDS, то обязательно добавьте каталог. Продолжить только с внутренними пользователями нельзя.

Выбор каталога Active Directory

1. Нажмите **Добавить каталог**.
2. В поле **Служба каталогов** выберите **Active Directory**.
3. В поле **ID каталога** введите идентификатор каталога в PAM.
   Значение может состоять из латинских букв и цифр, максимальная длина — 32 символа.
   Если планируете использовать несколько каталогов, то их ID должны быть разными.
4. Заполните поле **DNS-имя домена**.
5. (Опционально) В поле **Контроллеры домена** укажите адрес контроллера домена в формате FQDN.
   Можно указать несколько адресов через запятую.
   Если не указать адрес, PAM подключится по DNS-имени домена.
6. В поле **DN контейнера пользователей** укажите контейнер или подразделение, в котором располагаются пользователи системы.
7. Введите имя пользователя в формате UPN и его пароль.
   Пример: `pamadmin@my.company`.
8. (Опционально) Включите опцию **Использовать LDAPS**.
9. (Опционально) Измените соответствие атрибутов пользователей и/или атрибутов групп пользователей.
10. Нажмите **Добавить**.
11. Нажмите **Далее** для перехода к следующему шагу мастера.

Выбор каталога ALD PRO, FreeIPA, OpenLDAP

1. Нажмите **Добавить каталог**.
2. В поле **Служба каталогов** выберите **ALD PRO**, **FreeIPA** или **OpenLDAP**.
3. В поле **ID каталога** введите идентификатор каталога в PAM.
   Значение может состоять из латинских букв и цифр, максимальная длина — 32 символа.
   Если планируете использовать несколько каталогов, то их ID должны быть разными.
4. Заполните поле **DNS-имя домена**.
5. (Опционально) В поле **Контроллеры домена** укажите адрес контроллера домена в формате FQDN.
   Можно указать несколько адресов через запятую.
   Если не указать адрес, PAM подключится по DNS-имени домена.
6. В поле **DN контейнера пользователей** укажите контейнер или подразделение, в котором располагаются пользователи системы.
7. Введите имя пользователя в формате DN и его пароль.
   Пример: `'uid=pamadmin,cn=users,cn=accounts,dc=my,dc=company'`.
8. (Опционально) Включите опцию **Использовать LDAPS**.
9. Если выбрали ALD PRO или FreeIPA, то укажите **Формат идентификатора пользователей и групп** — SID или GUID.
10. (Опционально) Измените соответствие атрибутов пользователей и/или атрибутов групп пользователей.
11. Нажмите **Добавить**.
12. Нажмите **Далее** для перехода к следующему шагу мастера.

Выбор каталога RED ADM, Samba DC

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> При выборе каталогов RED ADM или Samba DC версии 4.20.8 и ниже добавьте в конфигурационный файл в секцию `[global]` строку: `ldap server require strong auth = allow_sasl_over_tls`
>
> Конфигурационный файл нужно отредактировать на всех контроллерах домена или на контроллере, который будет использоваться PAM для получения доступа к службе каталогов.
>
> Конфигурационные файлы находятся по пути:
>
> - Samba DC: */etc/samba/smb.conf*
> - RED ADM: */opt/reddc/etc/smb.conf*

1. Нажмите **Добавить каталог**.
2. В поле **Служба каталогов** выберите **RED ADM** или **Samba DC**.
3. В поле **ID каталога** введите идентификатор каталога в PAM.
   Значение может состоять из латинских букв и цифр, максимальная длина — 32 символа.
   Если планируете использовать несколько каталогов, то их ID должны быть разными.
4. Заполните поле **DNS-имя домена**.
5. (Опционально) В поле **Контроллеры домена** укажите адрес контроллера домена в формате FQDN.
   Можно указать несколько адресов через запятую.
   Если не указать адрес, PAM подключится по DNS-имени домена.
6. В поле **DN контейнера пользователей** укажите контейнер или подразделение, в котором располагаются пользователи системы.
7. Введите имя пользователя в формате UPN и его пароль.
   Пример: `pamadmin@my.company`.
8. (Опционально) Включите опцию **Использовать LDAPS**.
9. (Опционально) Измените соответствие атрибутов пользователей и/или атрибутов групп пользователей.
10. Нажмите **Добавить**.
11. Нажмите **Далее** для перехода к следующему шагу мастера.

Администраторы ролей

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

В качестве администратора ролей можно выбрать как пользователя из каталога, так и внутреннего. Выбранному пользователю будут выданы права на управление ролями PAM. Этот пользователь сможет выдать права на доступ к консоли управления PAM другим пользователям.

Из каталога

1. Выберите из каталога учетную запись.
2. Нажмите **Далее** для перехода к следующему шагу мастера.

Внутренний

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> При выборе внутреннего пользователя в качестве первого администратора ролей учитывайте, что на следующем шаге **Аутентификация пользователей** механизм аутентификации Windows недоступен. Такая комбинация настроек является некорректной конфигурацией PAM, т.к. администратор не может аутентифицироваться в системе.

1. Задайте логин.

   > ⚠ **ПРЕДУПРЕЖДЕНИЕ**
   > Логин нельзя изменять после установки PAM.

2. Задайте или сгенерируйте пароль. Пароль потребуется только для первого входа. После входа система автоматически запросит его смену.
3. Введите Email.
4. Нажмите **Далее** для перехода к следующему шагу мастера.

Аутентификация пользователей

На этом шаге требуется задать механизм аутентификации и настройки двухфакторной аутентификации.

Механизм аутентификации

1. Выберите подходящий вариант: LDAP, RADIUS или Windows.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Если на предыдущем шаге **Администраторы ролей** выбран внутренний пользователь, то выбор механизма Windows недоступен. Такая комбинация настроек является некорректной конфигурацией PAM, т.к. администратор не может аутентифицироваться в системе.
>
> Если в качестве первого администратора выбран пользователь из каталога, то выбрать механизм Windows можно. При такой конфигурации работа с внутренними пользователями не поддерживается.

2. При выборе RADIUS добавьте сервер RADIUS и введите необходимые данные.

Аутентификация по RADIUS

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> Для внутренних пользователей недоступна аутентификация через RADIUS. Заданные здесь настройки действуют только на пользователей из каталога.

При выборе RADIUS в качестве механизма аутентификации требуется 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.

Настройка 2FA

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> При выборе механизма аутентификации RADIUS пользователи из каталога аутентифицируются через RADIUS, а указанные ниже настройки действуют только на внутренних пользователей.

1. Включите опцию **Включить двухфакторную аутентификацию для всех пользователей по умолчанию**.
2. Для переключателя **Тип второго фактора** выберите подходящее значение: TOTP или Email.
3. Отметьте компоненты, для которых требуется включить кеширование второго фактора:
   - Management Console
   - User Console

- Desktop Console
- SSH Proxy
- RDP Proxy
- RDS Proxy

4. Если требуется, отредактируйте значение в поле **Время кеширования**.
5. 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 отправляется письмо
- Порт
- Имя пользователя — логин для авторизации на сервере
- Пароль

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

Syslog-сервер используется для интеграции с SIEM-системой и выполняет роль единого хранилища для записей событий PAM и текстовых логов сессий. Данные обновляются в режиме реального времени. Это позволяет быстро выявлять инциденты и аномалии, связанные с действиями привилегированных пользователей.

1. Заполните данные для подключения Syslog-сервера.
   Можно пропустить этот шаг и при необходимости добавить Syslog-сервер после установки PAM.

   Syslog-сервер

   При добавлении Syslog-сервера заполните поля:

   - Адрес сервера;
   - Сетевой протокол: TCP или UDP;
   - 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.

> ⓘ **ПРИМЕЧАНИЕ**
>
> Файлы с логами установки находятся по следующему пути: *IndeedPAM_3.4_RU/indeed-pam/logs/*.
>
> В случае возникновения ошибки установки просмотрите эти файлы и при необходимости обратитесь за помощью по исправлению ошибки в техническую поддержку.

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
```

Отказоустойчивая на Linux

Компоненты Indeed PAM устанавливаются на четыре сервера без учета балансировщиков нагрузки. Серверы управления и доступа дублируются для обеспечения отказоустойчивости. Схема развертывания с балансировкой подходит для внедрения и эксплуатации в промышленной среде.

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.

1. Загрузите и распакуйте дистрибутив PAM на Linux-машину.
2. Поместите сертификат удостоверяющего центра в *IndeedPAM_3.3_RU\indeed-pam\state\target\ca-certificates*. Это требуется для корректной работы LDAPS. Пропуск этого шага приведет к ошибке работы мастера.
3. Запустите мастер командой:

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

4. Дождитесь выполнения скрипта.
5. После выполнения скрипта перейдите по URL, указанному в консоли.
6. 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.

7. 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** в поле **FQDN PAM** укажите общее полное доменное имя (FQDN), которое направлено на IP-адрес балансировщиков нагрузки.
   Пример: pam.my-company.local.

2. Добавьте сервер управления и необходимые сервера доступа. Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом. Сервер доступа RDS используется для подключения в режиме RemoteApp.

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-имя в поле **Адрес хоста**.
   Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.
5. Заполните поле **Порт**.
6. Выберите способ аутентификации учетной записи на хосте:
   - При выборе **По паролю** заполните поля **Логин** и **Пароль**.
   - При выборе **По SSH-ключу** заполните поля **Логин**, **Пароль sudo**, **Парольная фраза** и загрузите **SSH-ключ**.
7. 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-имя в поле **Адрес хоста**.
   Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.
5. Заполните поле **Порт**.
6. Выберите способ аутентификации учетной записи на хосте:
   - При выборе **По паролю** заполните поля **Логин** и **Пароль**.
   - При выборе **По SSH-ключу** заполните поля **Логин**, **Пароль sudo**, **Парольная фраза** и загрузите **SSH-ключ**.
7. 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-имя в поле **Адрес хоста**.
   Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.
5. Заполните поле **Порт**.
6. Выберите способ аутентификации учетной записи на хосте:
   - При выборе **По паролю** заполните поля **Логин** и **Пароль**.
   - При выборе **По SSH-ключу** заполните поля **Логин**, **Пароль sudo**, **Парольная фраза** и загрузите **SSH-ключ**.
7. 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-имя в поле **Адрес хоста**.
   Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.
5. Заполните поле **Порт**.
6. Выберите способ аутентификации учетной записи на хосте:
   - При выборе **По паролю** заполните поля **Логин** и **Пароль**.
   - При выборе **По SSH-ключу** заполните поля **Логин**, **Пароль sudo**, **Парольная фраза** и загрузите **SSH-ключ**.
7. Нажмите **Добавить**.

Сервер доступа MSSQL

1. Нажмите **Добавить хост**.
2. Для переключателя **Операционная система хоста** выберите **Linux**.
3. Включите опцию **Сервер доступа MSSQL**.
4. Введите IP-адрес или DNS-имя в поле **Адрес хоста**.
   Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.
5. Заполните поле **Порт**.
6. Выберите способ аутентификации учетной записи на хосте:
   - При выборе **По паролю** заполните поля **Логин** и **Пароль**.
   - При выборе **По SSH-ключу** заполните поля **Логин**, **Пароль sudo**, **Парольная фраза** и загрузите **SSH-ключ**.
7. 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-имя в поле **Адрес хоста**.
   Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.
5. Заполните поле **Порт**.
6. Выберите тип учетной записи для хоста: **Общая доменная УЗ** или **Отдельная УЗ для этого хоста**.
7. Заполните поля **Логин** в формате UPN или SAM и **Пароль** для указанной учетной записи.
8. Нажмите **Добавить**.

Сервер доступа Web

1. Нажмите **Добавить хост**.
2. Для переключателя **Операционная система хоста** выберите **Linux**.
3. Включите опцию **Сервер доступа Web**.
4. Введите IP-адрес или DNS-имя в поле **Адрес хоста**.
   Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.
5. Заполните поле **Порт**.
6. Выберите тип учетной записи для хоста: **Общая доменная УЗ** или **Отдельная УЗ для этого хоста**.
7. Заполните поля **Логин** в формате UPN или SAM и **Пароль** для указанной учетной записи.
8. Нажмите **Добавить**.

Сервер Web Terminal

1. Нажмите **Добавить хост**.
2. Для переключателя **Операционная система хоста** выберите **Linux**.
3. Включите опцию **Сервер Web Terminal**.
4. Введите IP-адрес или DNS-имя в поле **Адрес хоста**.
   Учитывайте, что нельзя добавить несколько хостов с одинаковым адресом.
5. Заполните поле **Порт**.
6. Выберите тип учетной записи для хоста: **Общая доменная УЗ** или **Отдельная УЗ для этого хоста**.
7. Заполните поля **Логин** в формате UPN или SAM и **Пароль** для указанной учетной записи.
8. Нажмите **Добавить**.

ИНФОРМАЦИЯ

Сервер управления, сервер Web Terminal, а также серверы доступа RDP, Web, SSH, MSSQL и 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 **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.

> **ПРИМЕЧАНИЕ**
> 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. Для переключателя **Балансировщик** выберите **HAProxy**.
2. Нажмите **Добавить балансировщик**.
3. Введите IP-адрес или DNS-имя в поле **Адрес балансировщика**.
4. Заполните поле **Порт**.
5. Выберите способ аутентификации учетной записи на хосте:
   - При выборе **По паролю** заполните поля **Логин** и **Пароль**.
   - При выборе **По SSH-ключу** заполните поля **Логин**, **Пароль sudo**, **Парольная фраза** и загрузите **SSH-ключ**.
6. Нажмите **Добавить**.

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

Порты

> **ПРИМЕЧАНИЕ**
> 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

Компонент	Порт по умолчанию
RDP Proxy	3390
PostgreSQL Proxy	5432
MSSQL Proxy	1433
Web Proxy	5443
MC/UC HTTP	80
MC/UC HTTPS	443
Gateway Service Web Terminal	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.

Выбор базы данных Microsoft SQL

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.

ИНФОРМАЦИЯ

База данных Jatoba поддерживается в PAM. Для настройки обратитесь в техническую поддержку.

Хранилище данных

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

ПРИМЕЧАНИЕ

После установки PAM настройте файловое хранилище (NFS).

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

Добавьте один или несколько каталогов пользователей, или нажмите **Далее**, чтобы использовать PAM только с внутренними пользователями.

Выбор каталога ALD PRO, FreeIPA, OpenLDAP

1. Нажмите **Добавить каталог**.
2. В поле **Служба каталогов** выберите **ALD PRO**, **FreeIPA** или **OpenLDAP**.
3. В поле **ID каталога** введите идентификатор каталога в PAM.
   Значение может состоять из латинских букв и цифр, максимальная длина — 32 символа.
   Если планируете использовать несколько каталогов, то их ID должны быть разными.
4. Заполните поле **DNS-имя домена**.
5. (Опционально) В поле **Контроллеры домена** укажите адрес контроллера домена в формате FQDN.
   Можно указать несколько адресов через запятую.
   Если не указать адрес, PAM подключится по DNS-имени домена.
6. В поле **DN контейнера пользователей** укажите контейнер или подразделение, в котором располагаются пользователи системы.
7. Введите имя пользователя в формате DN и его пароль.
   Пример: `'uid=pamadmin,cn=users,cn=accounts,dc=my,dc=company'`.
8. (Опционально) Включите опцию **Использовать LDAPS**.
9. Если выбрали ALD PRO или FreeIPA, то укажите **Формат идентификатора пользователей и групп** — SID или GUID.
10. (Опционально) Измените соответствие атрибутов пользователей и/или атрибутов групп пользователей.
11. Нажмите **Добавить**.
12. Нажмите **Далее** для перехода к следующему шагу мастера.

Выбор каталога RED ADM, Samba DC

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> При выборе каталогов RED ADM или Samba DC версии 4.20.8 и ниже добавьте в конфигурационный файл в секцию `[global]` строку: `ldap server require strong auth = allow_sasl_over_tls`
>
> Конфигурационный файл нужно отредактировать на всех контроллерах домена или на контроллере, который будет использоваться PAM для получения доступа к службе каталогов.
>
> Конфигурационные файлы находятся по пути:
>
> - Samba DC: */etc/samba/smb.conf*
> - RED ADM: */opt/reddc/etc/smb.conf*

1. Нажмите **Добавить каталог**.
2. В поле **Служба каталогов** выберите **RED ADM** или **Samba DC**.
3. В поле **ID каталога** введите идентификатор каталога в PAM.
   Значение может состоять из латинских букв и цифр, максимальная длина — 32 символа.
   Если планируете использовать несколько каталогов, то их ID должны быть разными.
4. Заполните поле **DNS-имя домена**.
5. (Опционально) В поле **Контроллеры домена** укажите адрес контроллера домена в формате FQDN.
   Можно указать несколько адресов через запятую.
   Если не указать адрес, PAM подключится по DNS-имени домена.
6. В поле **DN контейнера пользователей** укажите контейнер или подразделение, в котором располагаются пользователи системы.
7. Введите имя пользователя в формате UPN и его пароль.
   Пример: `pamadmin@my.company`.
8. (Опционально) Включите опцию **Использовать LDAPS**.
9. (Опционально) Измените соответствие атрибутов пользователей и/или атрибутов групп пользователей.
10. Нажмите **Добавить**.
11. Нажмите **Далее** для перехода к следующему шагу мастера.

Выбор каталога Active Directory

1. Нажмите **Добавить каталог**.
2. В поле **Служба каталогов** выберите **Active Directory**.
3. В поле **ID каталога** введите идентификатор каталога в PAM.
   Значение может состоять из латинских букв и цифр, максимальная длина — 32 символа.
   Если планируете использовать несколько каталогов, то их ID должны быть разными.
4. Заполните поле **DNS-имя домена**.
5. (Опционально) В поле **Контроллеры домена** укажите адрес контроллера домена в формате FQDN.
   Можно указать несколько адресов через запятую.
   Если не указать адрес, PAM подключится по DNS-имени домена.
6. В поле **DN контейнера пользователей** укажите контейнер или подразделение, в котором располагаются пользователи системы.
7. Введите имя пользователя в формате UPN и его пароль.
   Пример: `pamadmin@my.company`.
8. (Опционально) Включите опцию **Использовать LDAPS**.
9. (Опционально) Измените соответствие атрибутов пользователей и/или атрибутов групп пользователей.
10. Нажмите **Добавить**.
11. Нажмите **Далее** для перехода к следующему шагу мастера.

Администраторы ролей

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

В качестве администратора ролей можно выбрать как пользователя из каталога, так и внутреннего. Выбранному пользователю будут выданы права на управление ролями PAM. Этот пользователь сможет выдать права на доступ к консоли управления PAM другим пользователям.

Из каталога

1. Выберите из каталога учетную запись.
2. Нажмите **Далее** для перехода к следующему шагу мастера.

Внутренний

1. Задайте логин.

   > ⚠ **ПРЕДУПРЕЖДЕНИЕ**
   > Логин нельзя изменять после установки PAM.

2. Задайте или сгенерируйте пароль. Пароль потребуется только для первого входа. После входа система автоматически запросит его смену.

3. Введите Email.

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

Аутентификация пользователей

На этом шаге требуется задать механизм аутентификации и настройки двухфакторной аутентификации.

Механизм аутентификации

1. Выберите подходящий вариант: LDAP или RADIUS.
2. При выборе RADIUS добавьте сервер RADIUS и введите необходимые данные.

Аутентификация по RADIUS

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> Для внутренних пользователей недоступна аутентификация через RADIUS. Заданные здесь настройки действуют только на пользователей из каталога.

При выборе RADIUS в качестве механизма аутентификации требуется 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.

Настройка 2FA

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> При выборе механизма аутентификации RADIUS пользователи из каталога аутентифицируются через RADIUS, а указанные ниже настройки действуют только на внутренних пользователей.

1. Включите опцию **Включить двухфакторную аутентификацию для всех пользователей по умолчанию**.
2. Для переключателя **Тип второго фактора** выберите подходящее значение: TOTP или Email.
3. Отметьте компоненты, для которых требуется включить кеширование второго фактора:
   - Management Console
   - User Console

- Desktop Console
- SSH Proxy
- RDP Proxy
- RDS Proxy

4. Если требуется, отредактируйте значение в поле **Время кеширования**.
5. 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 отправляется письмо
- Порт
- Имя пользователя — логин для авторизации на сервере
- Пароль

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

Syslog-сервер используется для интеграции с SIEM-системой и выполняет роль единого хранилища для записей событий PAM и текстовых логов сессий. Данные обновляются в режиме реального времени. Это позволяет быстро выявлять инциденты и аномалии, связанные с действиями привилегированных пользователей.

1. Заполните данные для подключения Syslog-сервера.
   Можно пропустить этот шаг и при необходимости добавить Syslog-сервер после установки PAM.

   Syslog-сервер

   При добавлении Syslog-сервера заполните поля:

   - Адрес сервера;
   - Сетевой протокол: TCP или UDP;
   - 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.

> **ПРИМЕЧАНИЕ**
>
> Файлы с логами установки находятся по следующему пути: *IndeedPAM_3.4_RU/indeed-pam/logs/*.
>
> В случае возникновения ошибки установки просмотрите эти файлы и при необходимости обратитесь за помощью по исправлению ошибки в техническую поддержку.

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
```

Настройка

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 подписи RDP-файла

Отредактируйте файл конфигурации appsettings.json

Приложение А. Конфигурационные файлы

Ознакомьтесь с расположением конфигурационных файлов PAM

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.
3. Перейдите в раздел **Default Web Site\core**.
4. В разделе **Управление** (англ. — *Manage*) откройте **Редактор конфигурации** (англ. — *Configuration Editor*).
5. Раскройте выпадающий список **Раздел:** (англ. — *Section:*) и выберите **system.webServer\serverRuntime**.
6. Установите для параметра **uploadReadAheadSize** значение **1048576**.
7. В разделе **Действия** (англ. — *Actions*) нажмите **Применить** (англ. — *Apply*).
8. 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 службы каталогов. Установка выполняется вручную на Linux-ресурсах, где требуется запускать команды с правами root.

> ⓘ **ПРИМЕЧАНИЕ**
> Чтобы разрешить выполнять команду `pamsu`, в настройке политики включите опцию **Разрешить выполнять pamsu**.

Установка PamSu

В зависимости от дистрибутива Linux, выберите нужный формат установочного пакета:

- Формат .deb предназначен для дистрибутивов на базе Debian: к ним относятся Debian, Ubuntu и Astra Linux.
- Формат .rpm предназначен для дистрибутивов на базе RHEL: к ним относятся CentOS, Oracle Linux, Rocky Linux, RedOS и RHEL.

DEB

Чтобы установить PamSu:

1. Перейдите в папку с дистрибутивом */IndeedPAM_3.4_RU/indeed-pam-tools/pamsu/*
2. Установите утилиту PamSu последней OSSL версии:

```
sudo dpkg -i "indeed-pam.pamsu-ossl(3.1.8)-v3.4.0-master.276206.x64.deb"
```

Если во время установки возникли ошибки или PamSu не работает:

1. Удалите утилиту:

```
sudo dpkg -P pamsu
```

2. Установите:

   - более раннюю OSSL версию, например:

     ```
     sudo dpkg -i "indeed-pam.pamsu-ossl(1.1.1s)-v3.4.0-master.276206.x64.deb"
     ```

   - NO-SSL версию, если уже установлены дополнительные криптографические модули для OpenSSL:

     ```
     sudo dpkg -i "indeed-pam.pamsu-no-ossl(3.1.8)-v3.4.0-master.276206.x64.deb"
     ```

RPM

Чтобы установить PamSu:

1. Перейдите в папку с дистрибутивом */IndeedPAM_3.4_RU/indeed-pam-tools/pamsu/*

2. Установите утилиту PamSu последней OSSL версии:

   ```
   sudo rpm -i "indeed-pam.pamsu-ossl(3.1.8)-v3.4.0-master.276206.x64.rpm"
   ```

Если во время установки возникли ошибки или PamSu не работает:

1. Удалите утилиту:

   ```
   sudo rpm -e pamsu
   ```

2. Установите:

   - более раннюю OSSL версию, например:

     ```
     sudo rpm -i "indeed-pam.pamsu-ossl(1.1.1s)-v3.4.0-master.276206.x64.rpm"
     ```

   - NO-SSL версию, если уже установлены дополнительные криптографические модули для OpenSSL:

     ```
     sudo rpm -i "indeed-pam.pamsu-no-ossl(3.1.8)-v3.4.0-master.276206.x64.rpm"
     ```

Если установить PamSu не получилось, обратитесь в техническую поддержку.

Настройка PamSu

На ресурсе нужно настроить доверие к сертификатам компонентов Core и IdP.

Чтобы проверить корректность работы с сертификатами, выполните команду:

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

Откройте с правами администратора конфигурационный файл */etc/pamsu.conf* и укажите настройки для `idp_url`, `api_url`, `log_path` и `log_level`:

- `idp_url` — адрес компонента IdP;
- `core_url` — адрес компонента Core;
- `log_path` — путь к каталогу с файлами логов;
- `log_level` — уровень логирования, может принимать значения *INFO*, *WARN*, *ERROR*, *FATAL*.

Пример

```
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_*`.

Indeed PAM Agent

Установите Indeed PAM Agent на ресурс, чтобы включить текстовое логирование RDP-сессий.

Если на ресурсе одновременно открыто несколько RDP-сессий, дополнительно установите службу Pam.Proxy.WindowsAgentService. Служба включается автоматически при подключении к ресурсу и предотвращает повышенную нагрузку на процессор.

Чтобы установить агент и службу:

1. Перейдите в папку *[Дистрибутив PAM]\indeed-pam-tools\agent*

2. Скопируйте установочные пакеты агента Pam.Proxy.WindowsAgent и службы Pam.Proxy.WindowsAgentService на ресурс.
3. Установите агент и службу на ресурс.
4. Перезагрузите ресурс.

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

Indeed PAM Desktop Console

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> Для работы Indeed PAM Desktop Console на клиентском компьютере должен быть установлен Microsoft .NET Framework версии 4.6.2 и выше.
> С информацией по установке можно ознакомиться в документации Microsoft.

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 настройте **PAM connection settings** (Настройки подключения с PAM). Укажите следующие URL: https://<ваш_FQDN>/core и https://<ваш_FQDN>/idp.
5. Обновите групповые политики на клиентском компьютере.

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 настройте **PAM connection settings** (Настройки подключения с PAM). Укажите следующие URL: https://<ваш_FQDN>/core и https://<ваш_FQDN>/idp.

Настройка записи событий в Syslog

Syslog-сервер используется для интеграции с SIEM-системой и выполняет роль единого хранилища для записей событий PAM и/или текстовых логов сессий. Данные обновляются в режиме реального времени: в процессе активного удаленного подключения, а не после его завершения.

Чтобы отправлять записи журнала **События** на Syslog-сервер, настройте конфигурационные файлы по инструкции ниже.
Отправка на Syslog-сервер текстовых логов сессий настраивается в разделе **Конфигурация**.

Windows

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

```
<Application Id="pam" SchemaId="Pam.Schema">
  <ReadTargetId>Pam.TargetDb</ReadTargetId>
  <WriteTargets>
    <TargetId>Pam.TargetDb</TargetId>
    <TargetId>Pam.Syslog</TargetId>
  </WriteTargets>
  <AccessControl>
    <!--<CertificateAccessControl CertificateThumbprint="001122...AA11"
Rights="Read" />-->
  </AccessControl>
</Application>
```

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

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

```
<Targets>
  ...
  <Target Id="Pam.TargetDb" Type="mssql"/>
  <Target Id="Pam.Syslog" Type="syslog"/>
</Targets>
```

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

Linux

1. Перейдите в каталог */etc/indeed/indeed-pam/ls/targets*, отредактируйте `<Settings> … </Settings>` в файле *Pam.Syslog.config* 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

/etc/indeed/indeed-pam/ls/targets

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

2. В файле */etc/indeed/indeed-pam/ls/clientApps.config* отредактируйте секцию `pam` для работы с файлом *Pam.Syslog.config* — добавьте новый `TargetId` для `WriteTarget`:

/etc/indeed/indeed-pam/ls/clientApps.config

```
<Application Id="pam" SchemaId="Pam.Schema">
  <ReadTargetId>Pam.DbTarget</ReadTargetId>
  <WriteTargets>
    <TargetId>Pam.DbTarget</TargetId>
    <TargetId>Pam.Syslog</TargetId>
  </WriteTargets>
  <AccessControl>
    <!--<CertificateAccessControl CertificateThumbprint="001122...AA11" Rights="Read"/>-->
  </AccessControl>
</Application>
```

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

/etc/indeed/indeed-pam/ls/clientApps.config

```
<Targets>
  ...
  <Target Id="Pam.DbTarget" Type="mssql"/>
  <Target Id="Pam.Syslog" Type="syslog"/>
</Targets>
```

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

Настройка подписи RDP-файла

Настройка подписи RDP-файла происходит на сервере управления с установленным компонентом Core.

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

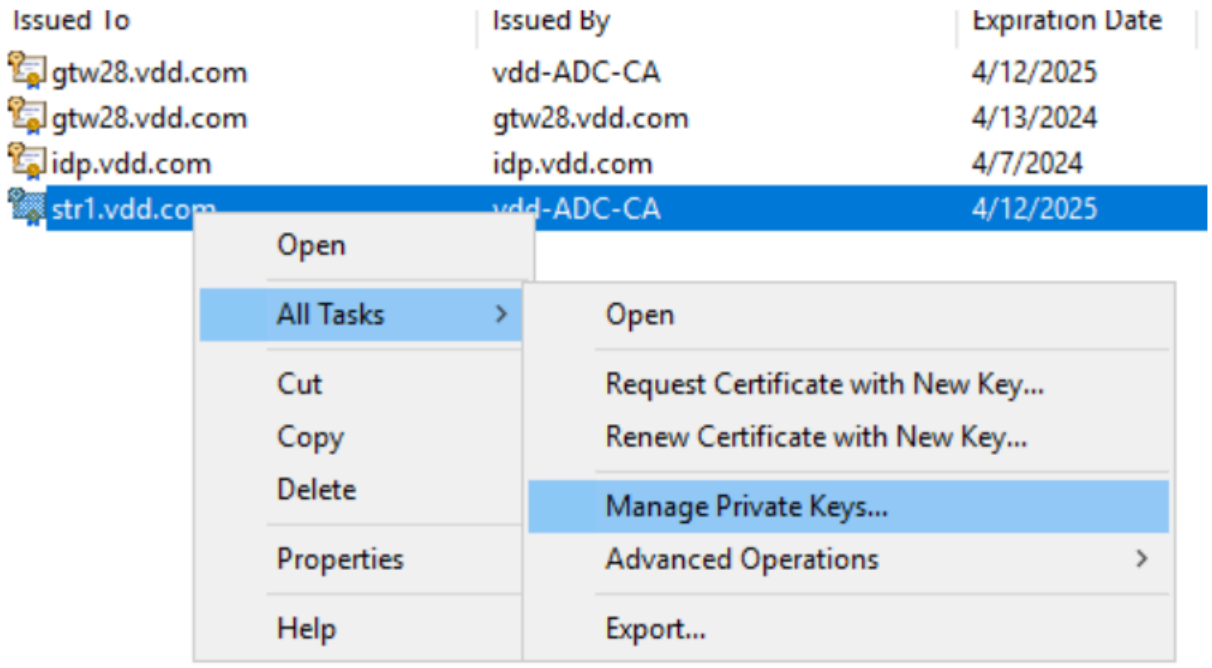
Windows

Настройка сертификата с отпечатком

1. Запустите PowerShell от имени администратора.
2. Откройте оснастку Certificates с помощью команды:

```
certlm.msc
```

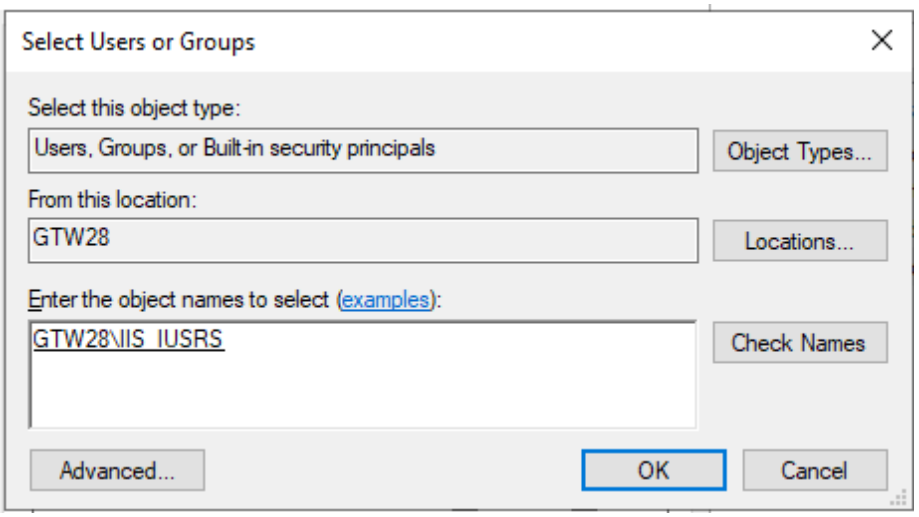
3. Добавьте сертификат в личное хранилище компьютера.
4. Нажмите правой кнопкой мыши на сертификат и выберите **All Tasks** (Все задачи) → **Manage Private Keys** (Управление закрытыми ключами*).



5. Нажмите **Add** (Добавить).

6. В открывшемся окне нажмите **Locations** (Размещение), выберите локальный компьютер и нажмите **OK**.

7. В текстовом поле введите имя `IIS_IUSRS`, нажмите **OK** и далее **Apply**.



8. Дважды нажмите на сертификат и перейдите на вкладку **Details** (Подробно).

9. В списке найдите поле **Thumbprint** (Отпечаток) и нажмите на него.

10. Скопируйте значение отпечатка сертификата без пробелов.

Редактирование конфигурационного файла

1. Откройте в редакторе конфигурационный файл *appsettings.json* компонента Core, который находится по пути:

C:\inetpub\wwwroot\core\appsettings.json

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

2. Отредактируйте секцию `RDP`:

   - Для ключа `SignRdpFile` задайте значение `true` (включение подписи RDP-файла).
   - Для ключа `Certificate` укажите отпечаток сертификата.

3. Сохраните измененные значения.

Перезапуск компонента Core

После редактирования файла конфигурации требуется перезапустить компонент Indeed PAM Core.

1. Запустите PowerShell от имени администратора.
2. Перезапустите группу приложения Core:

```
C:\Windows\System32\inetsrv\appcmd.exe recycle apppool Indeed.PAM.Core
```

Linux

Настройка сертификата с импортированием ключа

1. Скопируйте сертификат в папку */etc/indeed/indeed-pam/keys/core/*
2. Откройте в редакторе конфигурационный файл *appsettings.json* компонента Core, который находится по пути:

/etc/indeed/indeed-pam/core/appsettings.json

```
{
   "Rdp": {
     "UseRemoteApp": false,
     "SignRdpFile": true,
     "Certificate": "/etc/indeed/indeed-pam/keys/core/rdp-sign.pfx",
     "Password": "1234"
   }
}
```

3. Отредактируйте секцию `RDP`:
   - Для ключа `SignRdpFile` задайте значение `true` (включение подписи RDP-файла).
   - Для ключа `Certificate` укажите путь до сертификата.
   - Для ключа `Password` укажите пароль, который был задан при выгрузке сертификата.
4. Сохраните измененные значения.
5. Перейдите в папку */etc/indeed/indeed-pam/scripts/* с повышением привилегий:

```
sudo -i
```

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

6. Сбросьте права на файлы скриптом:

```
bash set-permissions.sh
```

Перезапуск компонента Core

После редактирования файла конфигурации требуется перезапустить компонент Indeed PAM Core.

1. Перейдите в папку */etc/indeed/indeed-pam/scripts/* с повышением привилегий:

```
sudo -i
```

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

2. Перезапустите компонент Core скриптом:

```
bash run-pam.sh
```

Приложение A. Конфигурационные файлы

Раздел содержит информацию о расположении конфигурационных файлов PAM.

После редактирования конфигурационного файла обязательно перезапустите компонент.

Windows

Чтобы перезапустить компонент:

1. Запустите PowerShell от имени администратора.
2. Запустите IIS Manager:

```
start inetmgr
```

3. Нажмите на нужный сервер на левой панели.
4. Нажмите **Restart** (Перезапустить) на правой панели.

Компонент	Путь к конфигурационному файлу
IDP	*C:\inetpub\wwwroot\idp\appsettings.json*
Core	*C:\inetpub\wwwroot\core\appsettings.json*
Management Console (mc)	*C:\inetpub\wwwroot\mc\assets\config\config.prod.json*
User Console (uc)	*C:\inetpub\wwwroot\uc\assets\config\config.prod.json*
ProxyApp	*C:\Program Files\Indeed\Indeed PAM\Gateway\ProxyApp\appsettings.json*
Gateway Service	*C:\Program Files\Indeed\Indeed PAM\Gateway\Pam.Gateway.Service\appsettings.json*
Log Server (ls)	*C:\inetpub\wwwroot\ls\appsettings.json* *C:\inetpub\wwwroot\ls\clientApps.config*

Linux

Чтобы перезапустить компонент:

1. Перейдите в папку */etc/indeed/indeed-pam/scripts/*

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

2. Выполните команду из таблицы.

Компонент	Путь к конфигурационному файлу	Команда для перезапуска
IDP	*/etc/indeed/indeed-pam/idp/appsettings.json*	`bash restart-pam.sh idp`
Core	*/etc/indeed/indeed-pam/core/appsettings.json*	`bash restart-pam.sh core`
Management Console (mc)	*/etc/indeed/indeed-pam/mc/config.prod.json*	`bash restart-pam.sh mc`
User Console (uc)	*/etc/indeed/indeed-pam/uc/config.prod.json*	`bash restart-pam.sh uc`
SSH Proxy	*/etc/indeed/indeed-pam/ssh-proxy/appsettings.json*	`bash restart-pam.sh ssh-proxy`
RDP Proxy	*/etc/indeed/indeed-pam/rdp-proxy/appsettings.json*	`bash restart-pam.sh rdp-proxy`
PostgreSQL Proxy	*/etc/indeed/indeed-pam/sql-proxy/appsettings.json*	`bash restart-pam.sh sql-proxy`

Компонент	Путь к конфигурационному файлу	Команда для перезапуска
MSSQL Proxy	*/etc/indeed/indeed-pam/tsql-proxy/appsettings.json*	`bash restart-pam.sh tsql-proxy`
Web Proxy	*/etc/indeed/indeed-pam/web-proxy/appsettings.json*	`bash restart-pam.sh web-proxy`
Gateway Service	*/etc/indeed/indeed-pam/gateway-service/appsettings.json*	`bash restart-pam.sh gateway-service`
Log Server (ls)	*/etc/indeed/indeed-pam/ls/clientApps.config* */etc/indeed/indeed-pam/ls/targets/Pam.DbTarget.config* */etc/indeed/indeed-pam/ls/appsettings.json*	`bash restart-pam.sh ls`
Файл .env	*/etc/indeed/indeed-pam/.env*	`bash restart-pam.sh`
Web Terminal	*/etc/indeed/indeed-pam/web-terminal-proxy/appsettings.json* */etc/indeed/indeed-pam/web-terminal-tunnel/appsettings.yml*	`bash restart-pam.sh web-terminal-proxy`

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.

1. Загрузите и распакуйте дистрибутив PAM на Linux-машину.
2. Поместите сертификат удостоверяющего центра в *IndeedPAM_3.3_RU\indeed-pam\state\target\ca-certificates*. Это требуется для корректной работы LDAPS. Пропуск этого шага приведет к ошибке работы мастера.
3. Запустите мастер командой:

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

4. Дождитесь выполнения скрипта.
5. После выполнения скрипта перейдите по URL, указанному в консоли.
6. 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.

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

Сценарий

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

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.

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.
- При добавлении каталога пользователей может потребоваться сертификат удостоверяющего центра.

Подробнее

Проверьте, каким удостоверяющим центром выпущен LDAPS-сертификат для этого каталога.

Windows

Если сертификат этого УЦ отсутствует в хранилище доверенных центров сертификации на серверах управления PAM, то добавьте этот сертификат УЦ в список доверенных корневых центров сертификации и перезапустите компоненты сервера управления в IIS.

Linux

Если сертификат этого УЦ отсутствует в */etc/indeed/indeed-pam/ca-certificates/* на серверах управления PAM, то выполните следующие действия:

i. Добавьте сертификат этого УЦ в */etc/indeed/indeed-pam/ca-certificates/*.

ii. Перейдите в папку PAM:

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

iii. Установите права на сертификат:

```
sudo bash scripts/set-permissions.sh
```

iv. Перезапустите компоненты сервера управления:

```
sudo bash scripts/restart-pam.sh
```

- 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 параметра **Способ изменения конфигурации** выберите значение **Из мастера**.

2. Нажмите **Применить изменения**.
   Отслеживайте процесс с помощью прогресс-бара.

   > ⓘ **ИНФОРМАЦИЯ**
   >
   > Если во время применения изменений возникли ошибки, нажмите **Скачать полный лог**.
   > Просмотрите скачанные логи и при необходимости обратитесь за помощью в техническую поддержку.
   > Файлы с логами находятся по пути: *IndeedPAM_3.4_RU/indeed-pam/logs/*.

3. После завершения применения изменений нажмите **Завершить работу мастера** или выполните команду в терминале:

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

Безопасность



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

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

Шифрованию подлежат конфигурационные файлы компонентов:

- Core
- IdP
- Log Server
- ProxyApp
- RDP Proxy
- SSH Proxy
- PostgreSQL Proxy
- MSSQL Proxy
- Web Proxy
- Web Terminal
- Gateway Service

Расположение ключа:

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

Право на использование директории предоставляется только приложениям Indeed PAM.

Во время работы с системой может потребоваться редактирование файлов конфигурации. Редактировать можно только расшифрованные файлы. После внесения всех необходимых правок требуется снова зашифровать файлы конфигурации. Это можно сделать с помощью утилиты на Windows или скрипта на Linux.

Утилита на Windows

Снятие шифрования

1. Перейдите в каталог с дистрибутивом PAM по пути *%PAM_HOME%\indeed-pam-tools\configuration-protector*.

2. Запустите PowerShell от имени администратора.

3. Выполните одну из команд для снятия шифрования.

   - Снятие шифрования со всех файлов конфигурации, расположенных в стандартных директориях:

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

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

   - Снятие шифрования с файлов конфигурации отдельных компонентов:

     ```
     .\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"
     ```

> **ИНФОРМАЦИЯ**
>
> Допускается указать путь без кавычек, если он не содержит пробелов.

Шифрование

1. Перейдите в каталог с дистрибутивом PAM по пути *IndeedPAM_3.4_RU\indeed-pam-tools\configuration-protector*.
2. Запустите PowerShell от имени администратора.
3. Выполните одну из команд для шифрования.
   - Шифрование всех файлов конфигурации, расположенных в стандартных директориях:

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

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

   - Шифрование файлов конфигурации отдельных компонентов:

     ```
     .\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"
     ```

> **ИНФОРМАЦИЯ**
> Допускается указать путь без кавычек, если он не содержит пробелов.

Скрипт на Linux

Снятие шифрования

1. Перейдите в директорию с файлом протектора:

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

2. Выполните одну из команд для снятия шифрования.

   - Снятие шифрования со всех файлов конфигурации, расположенных в стандартных директориях:

     ```
     bash protector.sh unprotect
     ```

   - Снятие шифрования с файлов конфигурации отдельных компонентов:

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

     Например:

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

Шифрование

1. Перейдите в директорию с файлом протектора:

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

2. Выполните одну из команд для шифрования.

   - Шифрование всех файлов конфигурации, расположенных в стандартных директориях:

     ```
     bash protector.sh protect
     ```

- Шифрование файлов конфигурации отдельных компонентов:

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

Например:

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

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\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\\Indeed\\Indeed PAM\\Gateway\\ProxyApp\\Pam.Proxy.App.exe"
      ],
      "ApplicationPaths": [
        "C:\\Program Files\\Indeed\\Indeed PAM\\Gateway\\ProxyApp\\ffmpeg.exe",
        "C:\\Program Files\\Indeed\\Indeed PAM\\Gateway\\ProxyApp\\ffprobe.exe"
      ]
    },
    {
      "Comment": "Common, UserInit process",
      "ParentProcessPaths": [
        "C:\\Windows\\System32\\userinit.exe"
      ],
      "ApplicationPaths": [
        "C:\\Windows\\system32\\rdpinit.exe",
        "C:\\Program Files\\Indeed\\Indeed PAM\\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\\Indeed\\Indeed PAM\\Gateway\\ProxyApp\\Pam.Proxy.App.exe"
      ]
    },
    {
      "Comment": "Common, start WebView for authentication on IDP",
```

```
      "ParentProcessPaths": [
        "C:\\Program Files\\Indeed\\Indeed PAM\\Gateway\\ProxyApp\\Pam.Proxy.App.exe",
        "C:\\Program Files\\Indeed\\Indeed PAM\\Gateway\\ProxyApp\\Microsoft.WebView2.FixedVersionRuntime\\msedgewebview2.exe"
      ],
      "ApplicationPaths": [
        "C:\\Program Files\\Indeed\\Indeed PAM\\Gateway\\ProxyApp\\Microsoft.WebView2.FixedVersionRuntime\\msedgewebview2.exe"
      ]
    },
    {
      "Comment": "RDP",
      "ParentProcessPaths": [
        "C:\\Program Files\\Indeed\\Indeed PAM\\Gateway\\ProxyApp\\Pam.Proxy.App.exe"
      ],
      "ApplicationPaths": [
        "C:\\Windows\\system32\\mstsc.exe",
        "C:\\Windows\\SysWOW64\\mstsc.exe"
      ]
    },
    {
      "Comment": "SSH",
      "ParentProcessPaths": [
        "C:\\Program Files\\Indeed\\Indeed PAM\\Gateway\\ProxyApp\\Pam.Proxy.App.exe"
      ],
      "ApplicationPaths": [
        "C:\\Program Files\\Indeed\\Indeed PAM\\Gateway\\SshClient\\Pam.Putty.exe"
      ]
    }
  ]
}
```

- `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\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\\Indeed PAM\\Gateway\\ProxyApp\\appsettings.json",
      "AllowedProcesses": [
        "C:\\Program Files\\Indeed\\Indeed PAM\\Gateway\\ProxyApp\\Pam.Proxy.App.exe"
      ]
    },
    {
      "Path": "C:\\ProgramData\\Indeed\\Indeed PAM\\SessionTemp\\RDP",
      "AllowedProcesses": [
        "C:\\Program Files\\Indeed\\Indeed PAM\\Gateway\\ProxyApp\\Pam.Proxy.App.exe",
        "C:\\Windows\\System32\\mstsc.exe",
        "C:\\Windows\\SysWOW64\\mstsc.exe"
      ]
    },
    {
      "Path": "C:\\ProgramData\\Indeed\\Indeed PAM\\SessionTemp\\SSH",
      "AllowedProcesses": [
        "C:\\Program Files\\Indeed\\Indeed PAM\\Gateway\\ProxyApp\\Pam.Proxy.App.exe",
        "C:\\Program Files\\Indeed\\Indeed PAM\\Gateway\\SshClient\\Pam.Putty.exe"
      ]
    },
    {
      "Path": "C:\\ProgramData\\Indeed\\Indeed PAM\\SessionTemp\\Video",
      "AllowedProcesses": [
        "C:\\Program Files\\Indeed\\Indeed PAM\\Gateway\\ProxyApp\\Pam.Proxy.App.exe",
        "C:\\Program Files\\Indeed\\Indeed PAM\\Gateway\\ProxyApp\\ffmpeg.exe",
        "C:\\Program Files\\Indeed\\Indeed PAM\\Gateway\\ProxyApp\\ffprobe.exe"
      ]
    },
    {
      "Path": "C:\\ProgramData\\Indeed\\Indeed PAM\\PamStorage",
      "AllowedProcesses": [
        "C:\\Program Files\\Indeed\\Indeed PAM\\Gateway\\ProxyApp\\Pam.Proxy.App.exe",
        "C:\\Program Files\\Indeed\\Indeed PAM\\Gateway\\ProxyApp\\ffmpeg.exe",
        "C:\\Program Files\\Indeed\\Indeed PAM\\Gateway\\ProxyApp\\ffprobe.exe",
        "C:\\Program Files\\Indeed\\Indeed PAM\\Gateway\\SshClient\\Pam.Putty.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.

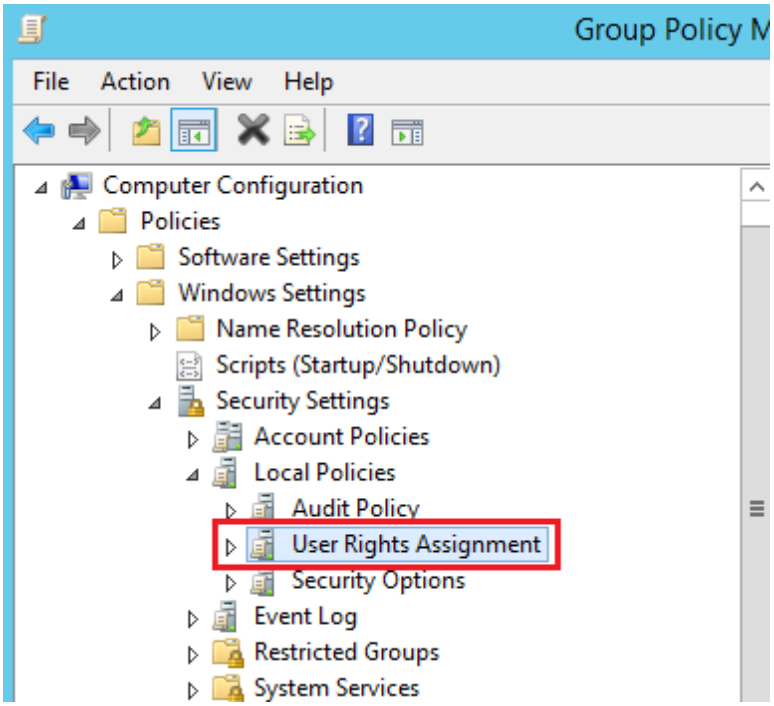
Политики безопасности сервера доступа

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 caller (Доступ к диспетчеру учетных данных от имени доверенного вызывающего)	Этот параметр используется диспетчером учетных данных в ходе 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.	Не определено
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! Назначение этого права пользователю может представлять угрозу безопасности. Назначайте такие права только доверенным пользователям.	Не определено

Политика	Описание	Значения
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 ее 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 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.	BUILTIN\Administrators

Политика	Описание	Значения
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 время, а не действительное время совершения событий.	BUILTIN\Administrators, NT AUTHORITY\LOCAL SERVICE
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

Политика	Описание	Значения
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 процессу, которым нежелательно позволять управлять системой.	Не определено
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

Политика	Описание	Значения
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 символических ссылок)	Эта привилегия определяет для пользователя возможность создавать 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.	BUILTIN\Administrators
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

Политика	Описание	Значения
Deny log on as a batch job (Отказать во входе в качестве пакетного задания)	Этот параметр безопасности определяет, каким учетным записям 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.	BUILTIN\Guests
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 обе 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 систему через службу удаленных рабочих столов)	Этот параметр безопасности определяет, каким пользователям и группам будет запрещено входить в систему как клиенту служб удаленных рабочих столов.	BUILTIN\Guests

Политика	Описание	Значения
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 «Троянский конь», которые имитируют входящих клиентов и используют их учетные данные для получения доступа к сетевым ресурсам.	BUILTIN\Administrators
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

Политика	Описание	Значения
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 сведения см. в разделе «Аудит: немедленно завершить работу системы при невозможности протоколирования аудита безопасности»	NT AUTHORITY\LOCAL SERVICE, NT AUTHORITY\NETWORK SERVICE

Политика	Описание	Значения
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 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.	BUILTIN\Administrators, NT AUTHORITY\SERVICE

Политика	Описание	Значения
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
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

Политика	Описание	Значения
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 помощи планировщика заданий, последний регистрирует этого пользователя в системе как пользователя с пакетным входом, а не как интерактивного пользователя.	BUILTIN\Administrators
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. Процессы, выполняющиеся под учетной записью пользователя, без этой привилегии могут понижать уровень метки объекта, владельцем которого является данный пользователь.	Не определено

Политика	Описание	Значения
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. 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».	BUILTIN\Administrators

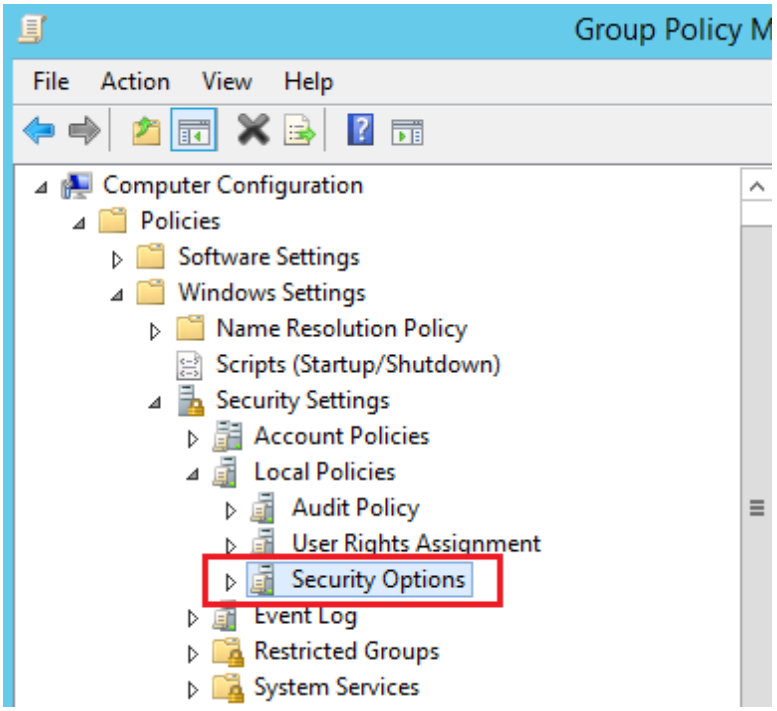
Политика	Описание	Значения
Perform volume maintenance tasks (Выполнение задач по обслуживанию томов)	Этот параметр безопасности определяет пользователей и группы, которые могут выполнять задачи по обслуживанию томов, например, удаленную дефрагментацию. При назначении этого права пользователя следует 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 (Профилирование производительности системы)	Этот параметр безопасности определяет пользователей, которые могут использовать средства мониторинга производительности для отслеживания производительности системных процессов.	BUILTIN\Administrators
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

Политика	Описание	Значения
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 перезаписывать параметры реестра, скрывать данные и получать во владение системные объекты, назначать его следует только доверенным пользователям.	BUILTIN\Administrators
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 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.	Enabled (Включен)
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)

Политика	Описание	Значение
Accounts: Limit local account use of blank passwords to console logon only (Учетные записи: разрешить использование пустых паролей только при консольном 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 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.	Enabled (Включен)

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

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 влияет на возможность добавления локального принтера. Параметр не затрагивает администраторов.	Enabled (Включен)
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)

Политика	Описание	Значение
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)

Политика	Описание	Значение
Interactive logon: Number of previous logons to cache (in case domain controller is not available) (Интерактивный вход в систему: количество предыдущих подключений к кэшу (в случае отсутствия доступа к контроллеру домена))	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 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.	0 logons (0 входов в систему)
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 требуется предоставить данные входа. Для учетных записей доменов этот параметр безопасности определяет, требуется 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. 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.	Disabled (Отключен)
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)

Политика	Описание	Значение
Network access: Do not allow anonymous enumeration of SAM accounts and shares (Сетевой доступ: не разрешать перечисление учетных записей SAM и общих ресурсов анонимными пользователями)	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 пользователям в доверенном домене, не поддерживающем взаимное доверие. Чтобы запретить перечисление учетных записей SAM и общих ресурсов анонимными пользователями, включите этот параметр.	Enabled (Включен)
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)

Политика	Описание	Значение
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, 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».	Disabled (Отключен)
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

Политика	Описание	Значение
Network access: Remotely accessible registry paths and sub-paths (Сетевой доступ: удаленно доступные пути и вложенные пути реестра.)	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
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

Политика	Описание	Значение
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 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 требуется 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.	Classic - local users authenticate as themselves (Обычная - локальные пользователи удостоверяются как они сами)

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)

Политика	Описание	Значение
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 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.	Enabled (Включен)

Политика	Описание	Значение
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: 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).	Send NTLMv2 response only. Refuse LM & NTLM (Отправлять только NTLMv2-ответ. Отказывать LM и NTLM)

Политика	Описание	Значение
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 security for NTLM SSP based (including secure RPC) servers (Сетевая безопасность: минимальная сеансовая безопасность для серверов на базе NTLM SSP (включая безопасный RPC).)	Этот параметр безопасности позволяет серверу 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 целостность сообщений не согласована, подключение не будет установлено. Требовать 128-битное 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)

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 требуется успешно выполнить вход в систему и он должен иметь право на завершение работы системы.	Disabled (Отключен)
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, требуется 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, требуется 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 выбор с пунктов «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 рабочего стола или путем отключения параметра политики «Контроль учетных записей: переключение к безопасному рабочему столу при выполнении запроса на повышение прав».	Disabled (Отключен)

Политика	Описание	Значение
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. 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.	Prompt for consent for non-Windows binaries (Запрос согласия для исполняемых файлов, отличных от Windows)

Политика	Описание	Значение
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 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.	Prompt for credentials on the secure desktop (Запрос учетных данных на безопасном рабочем столе)

Политика	Описание	Значение
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 учетных записей: все администраторы работают в режиме одобрения администратором)	Этот параметр политики определяет характеристики всех политик контроля учетных записей для компьютера. При изменении этого параметра политики требуется перезагрузить 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.	Enabled (Включен)

Политика	Описание	Значение
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 (Контроль учетных записей: при сбоях записи в файл или реестр виртуализация в размещение пользователя)	Этот параметр политики управляет перенаправлением сбоев записи приложений в определенные расположения в реестре и файловой системе. Этот параметр политики 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.	Enabled (Включен)

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 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.	Users can't add Microsoft accounts (Пользователи не могут добавлять учетные записи Майкрософт)
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)

Политика	Описание	Значение
Domain member: Disable machine account password changes (Член домена: отключить изменение пароля учетных записей компьютера)	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 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.	Disabled (Отключен)
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

Политика	Описание	Значение
Domain member: Require strong (Windows 2000 or later) session key (Член домена: требовать стойкий сеансовый ключ (Windows 2000 или выше))	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. 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.	Enabled (Включен)

Политика	Описание	Значение
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 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	User display name only (Только имя пользователя)

Политика	Описание	Значение
	при выборе значения «Только имя пользователя». 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 требуется применить KB4013429. Пользователи не смогут скрыть дополнительные сведения. Рекомендации Возможности применения этой политики зависят от ваших требований безопасности 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».	

Политика	Описание	Значение
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 требуется 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 session (Сервер сети Microsoft: время бездействия до приостановки сеанса)	Этот параметр безопасности определяет продолжительность отрезка времени SMB-сеанса до его приостановки по причине неактивности. Администраторы могут использовать этот параметр 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.	15 минут

Политика	Описание	Значение
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 требуется 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 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.	Disabled (Отключено)

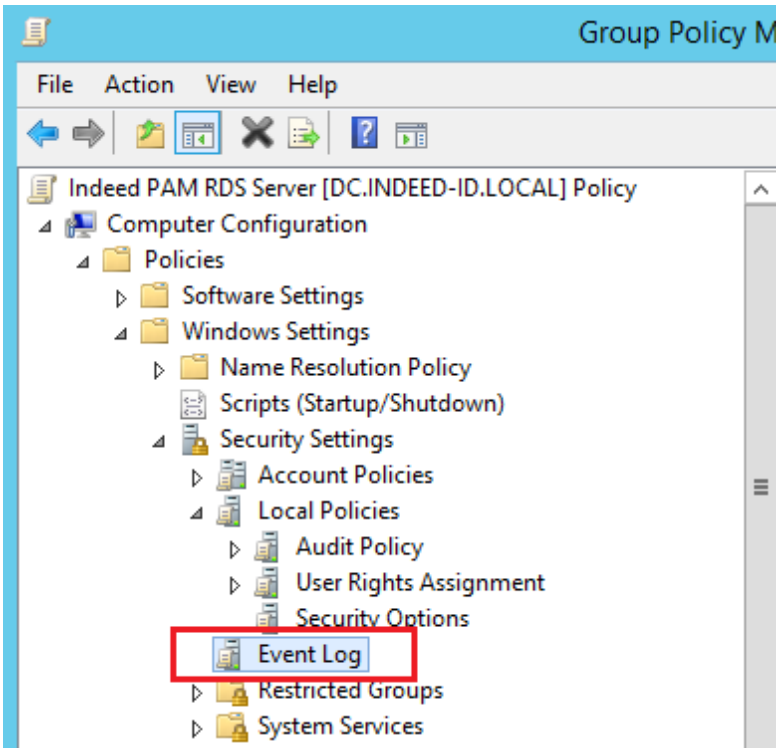
Политика	Описание	Значение
Microsoft network server: Disconnect clients when logon hours expire (Сервер сети Microsoft: отключать клиентов по истечении разрешенных часов входа)	Этот параметр безопасности определяет, будут ли отключаться пользователи, подключенные к локальному компьютеру, по истечении 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): уровень проверки сервером имени участника-службы конечного объекта)	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 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.	Off (Откл.)

Политика	Описание	Значение
Recovery console: Allow automatic administrative logon (Консоль восстановления: разрешить автоматический вход администратора)	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)
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*)


Group Policy M
File
Action
View
Help
Indeed PAM RDS Server [DC.INDEED-ID.LOCAL] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services

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 требуется 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 подразделения, чтобы использовать преимущества параметров групповой политики.	100032 КБ
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)

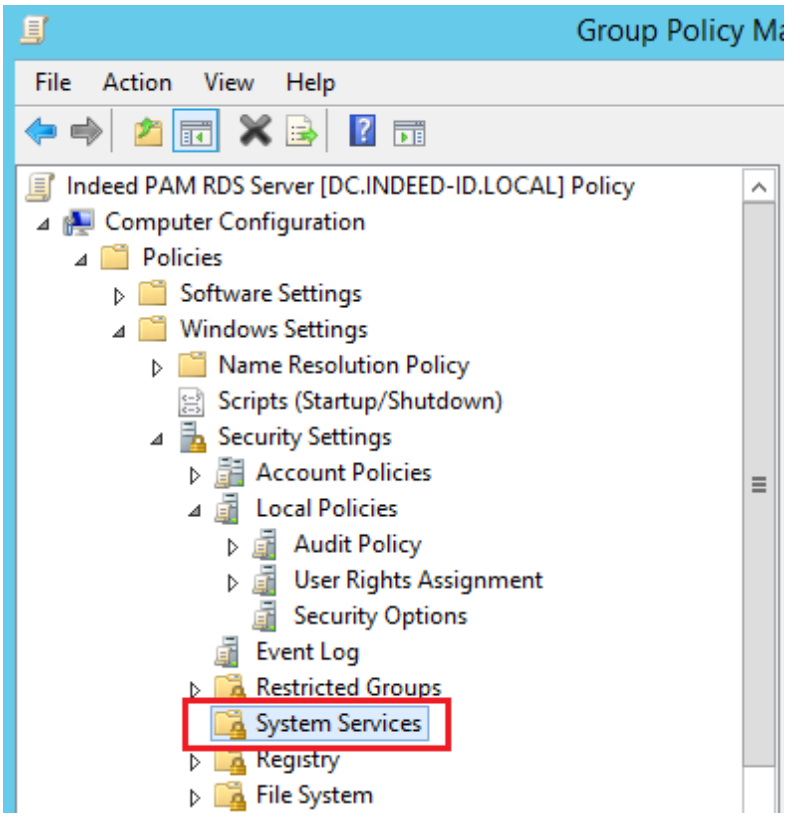
Политика	Описание	Значение
Prevent local guests group from accessing security log (Запретить доступ локальной группы гостей к журналу безопасности)	Этот параметр безопасности определяет, запрещен ли гостям доступ к журналу событий безопасности. Примечания Этот параметр отсутствует в объекте локальной политики компьютера.	Enabled (Включен)
Prevent local guests group from accessing system log (Запретить доступ локальной группы гостей к журналу системы)	Этот параметр безопасности определяет, запрещен ли гостям доступ к журналу событий системы. Примечания Этот параметр отсутствует в объекте локальной политики компьютера.	Enabled (Включен)
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, включите в диалоговом окне «Свойства» этой политики опцию «Определить этот параметр политики», а затем выберите значение «Переписывать события при необходимости». Если архивирование журнала выполняется через заданные промежутки времени, включите в диалоговом окне «Свойства» этой политики опцию «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 требуется сохранять в журнале все события, включите в диалоговом окне «Свойства» этой политики опцию «Определить этот параметр политики», а затем выберите значение «Не переписывать события (очистить журнал вручную)». При выборе этого варианта журнал требуется 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*)


Group Policy Ma
File
Action
View
Help
Indeed PAM RDS Server [DC.INDEED-ID.LOCAL] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System

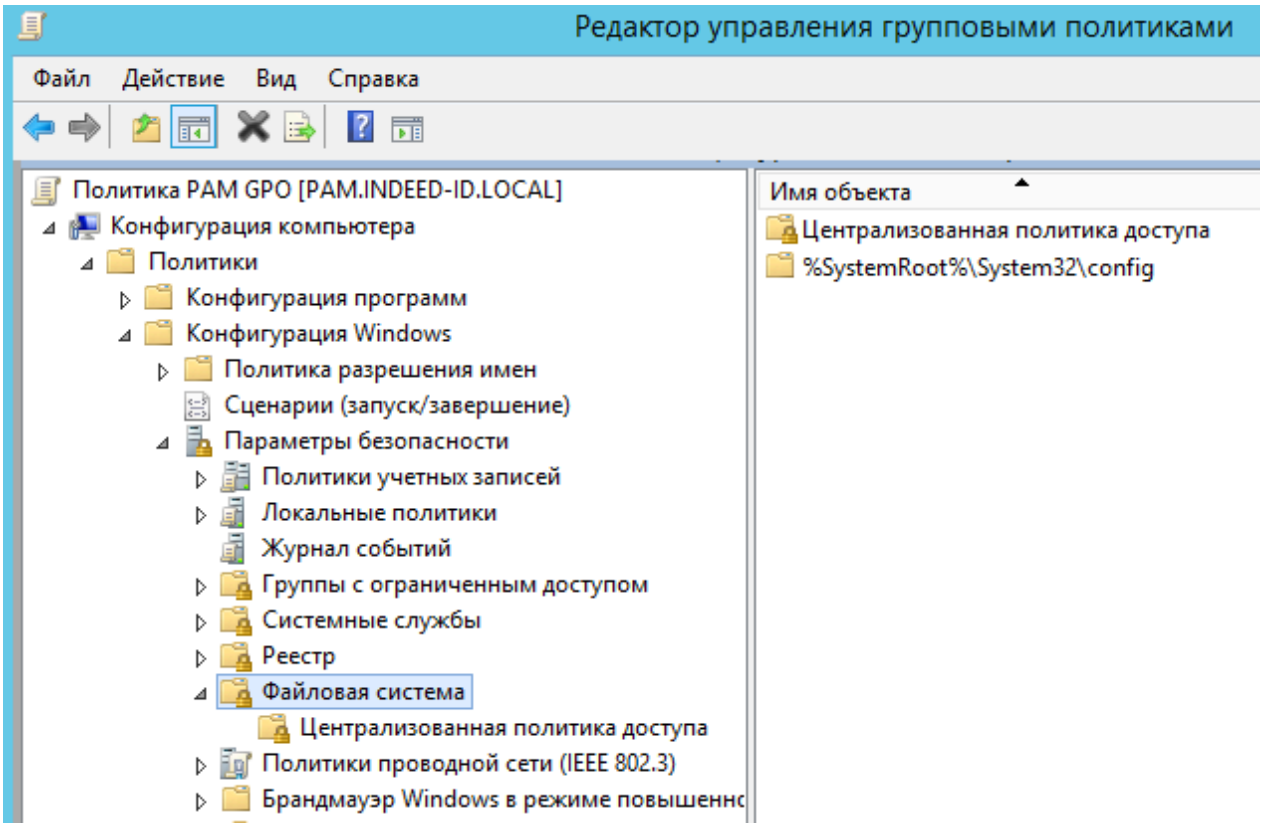
Описание политик

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: запрещен)	Не определены	Не определен
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 (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)

Type (Тип)	Principal (Субъект)	Access (Доступ)	Applies To (Применяется к)
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 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)

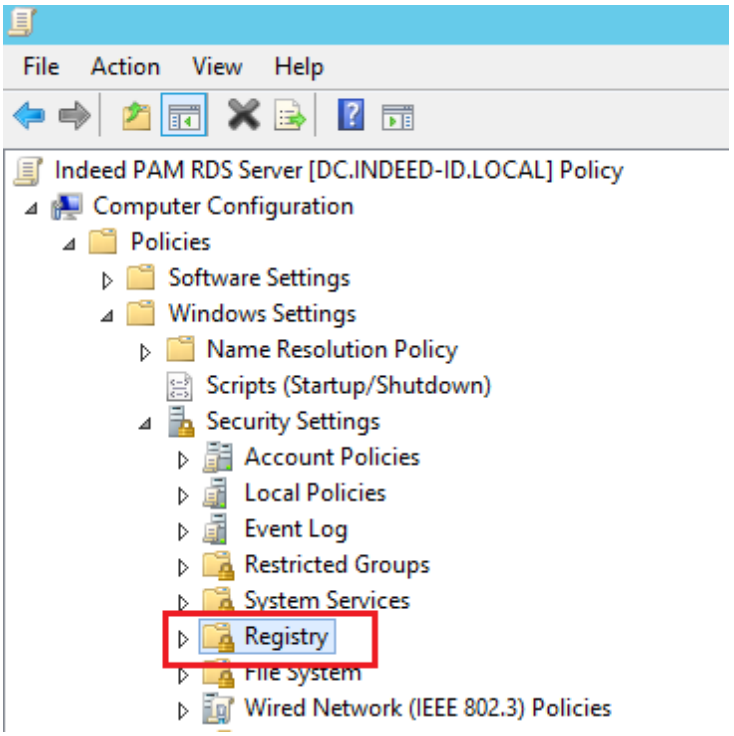
Type (Тип)	Principal (Субъект)	Access (Доступ)	Applies To (Применяется к)
All (Все)	Everyone (Все)	Create files / Write data, Create folders / Append data, Write attributes, Write extended attributes, Delete subfolders and files, Delete, Change permissions, Take ownership (Создание файлов / Запись данных, 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)

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 (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

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 (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)

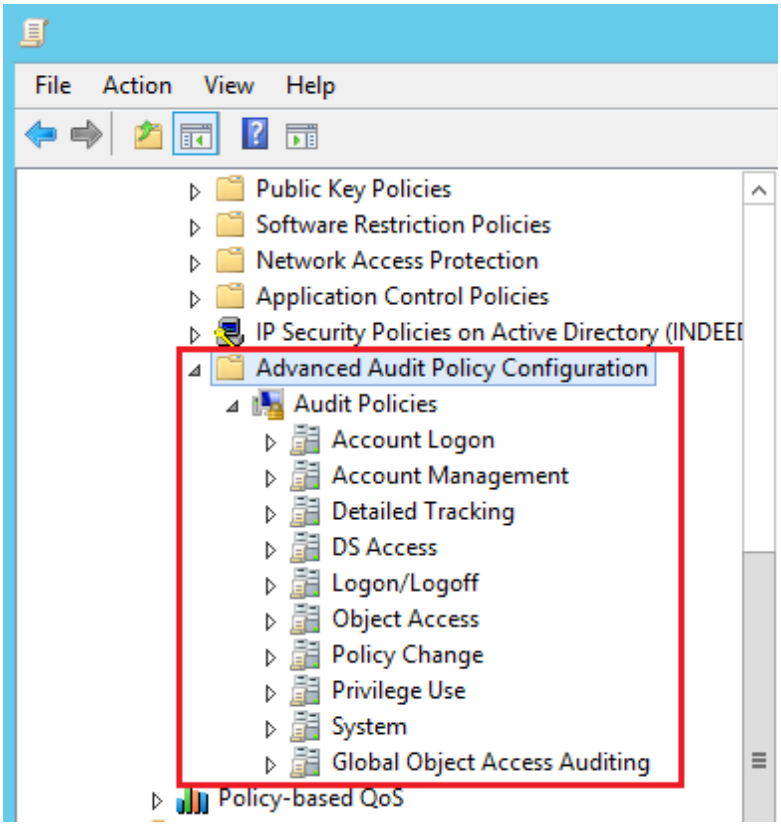
Auditing (Аудит)

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)
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. Примечание. События этой подкатегории регистрируются только на контроллерах домена.	Success, Failure (Успех, Отказ)
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)

Политика	Описание	Значение
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 учетными записями пользователей)	Этот параметр политики позволяет вести аудит изменений, вносимых в учетные записи пользователей. Отслеживаются следующие события: Создание, 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.	Success, Failure (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 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.	Success, Failure (Успех, Отказ)
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)

Политика	Описание	Значение
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 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.	Success, Failure (Успех, Отказ)
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 соответствует параметрам, установленным в списке SACL. Примечание. Чтобы задать список SACL для объекта файловой системы, воспользуйтесь вкладкой «Безопасность» диалогового окна «Свойства» объекта.	Success, Failure (Успех, Отказ)

Политика	Описание	Значение
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. 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.	Success, Failure (Успех, Отказ)

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)
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)

Политика	Описание	Значение
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 изменения политики платформы фильтрации)	Этот параметр политики позволяет вести аудит событий, возникающих при выполнении изменений платформы фильтрации Windows (WFP), таких как следующие: Состояние служб IPsec. Изменения параметров политики IPsec. Изменения параметров политики брандмауэра Windows. Изменения поставщиков и модуля WFP.	Success, Failure (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 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.	Success, Failure (Успех, Отказ)

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

Система

(англ. — *System*)

Описание политик

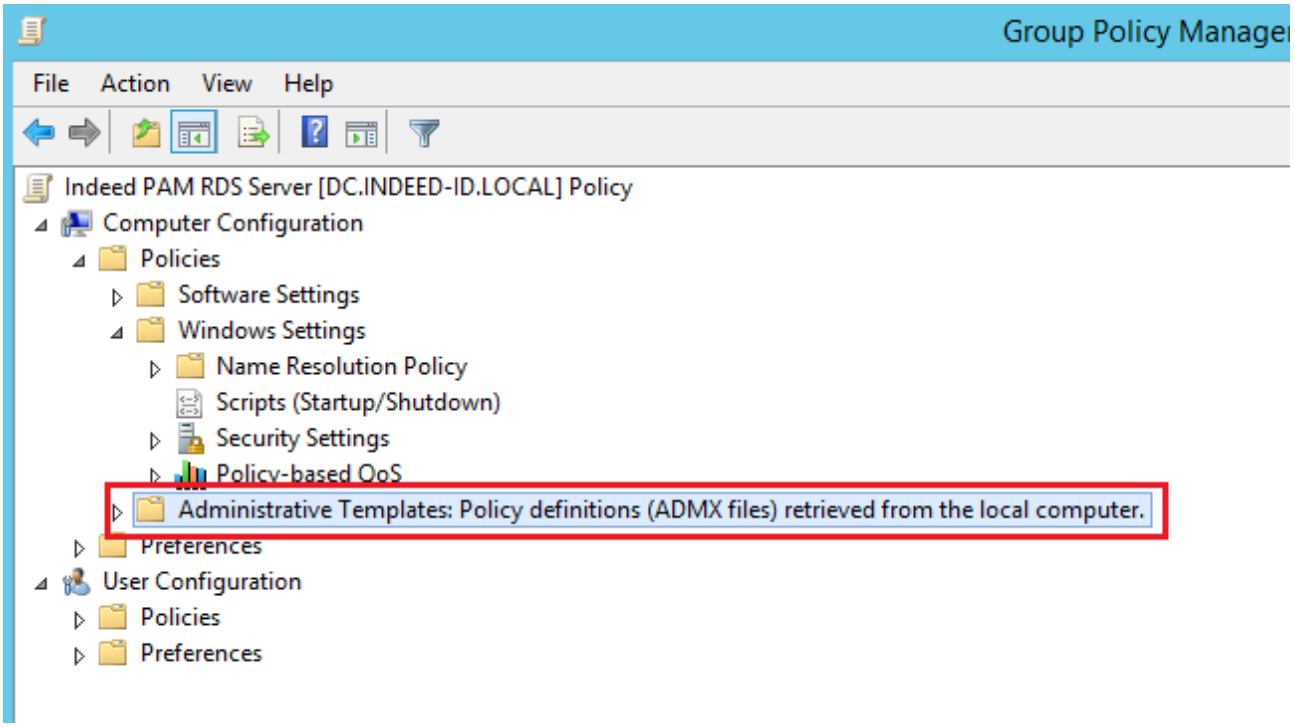
Политика	Описание	Значение
Audit Other System Events (Аудит других системных событий)	Этот параметр политики позволяет вести аудит следующих событий: Запуск и завершение работы службы и драйвера брандмауэра Windows. Обработка политики безопасности службой брандмауэра Windows. Операции с файлами ключей 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 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.	Success, Failure (Успех, Отказ)

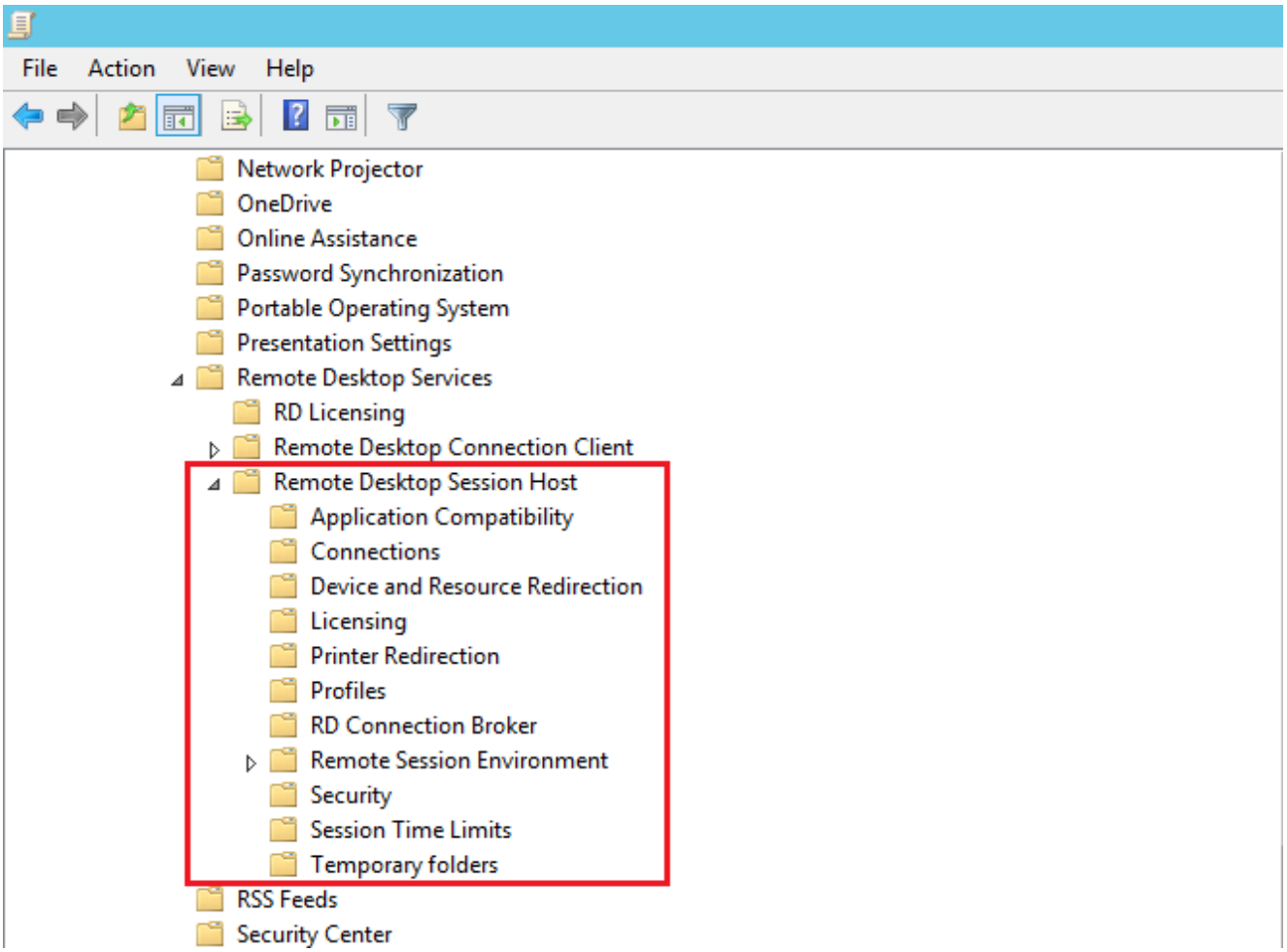
Политика	Описание	Значение
Audit System Integrity (Аудит целостности системы)	Этот параметр политики позволяет вести аудит событий, связанных с нарушениями целостности подсистемы безопасности, такими как следующие: События, которые не удается записать в журнал событий из-за ошибок системы аудита. Процессы, 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, включив опцию «Восстановить подключение при разрыве» на вкладке «Взаимодействие» в диалоговом окне «Подключение к удаленному рабочему столу».	Disabled (Отключено) Чтобы избежать разрыва сессии при использовании Desktop Console, установите состояние Enabled (Включено) или Not Configured (Не задано)

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)

Политика	Описание	Значение
Set rules for remote control of Remote Desktop Services user sessions (Устанавливает правила удаленного управления для пользовательских сеансов служб удаленных рабочих столов)	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: 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.	Enabled Options: Full Control without user's permission (Включено Параметры: 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-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.	Enabled (Включено)

Политика	Описание	Значение
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)
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 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.	Enabled (Включено)

Политика	Описание	Значение
Set client connection encryption level (Установить уровень шифрования для клиентских подключений)	Этот 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 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.	Enabled Encryption Level: High Level (Включено Уровень шифрования: Высокий уровень)

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 подключений. Этот параметр доступен в папках «Конфигурация компьютера» и «Конфигурация пользователя». Если настроены оба параметра, то приоритет имеет параметр в папке «Конфигурация компьютера».	Enabled (Включено)

Политика	Описание	Значение
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*)

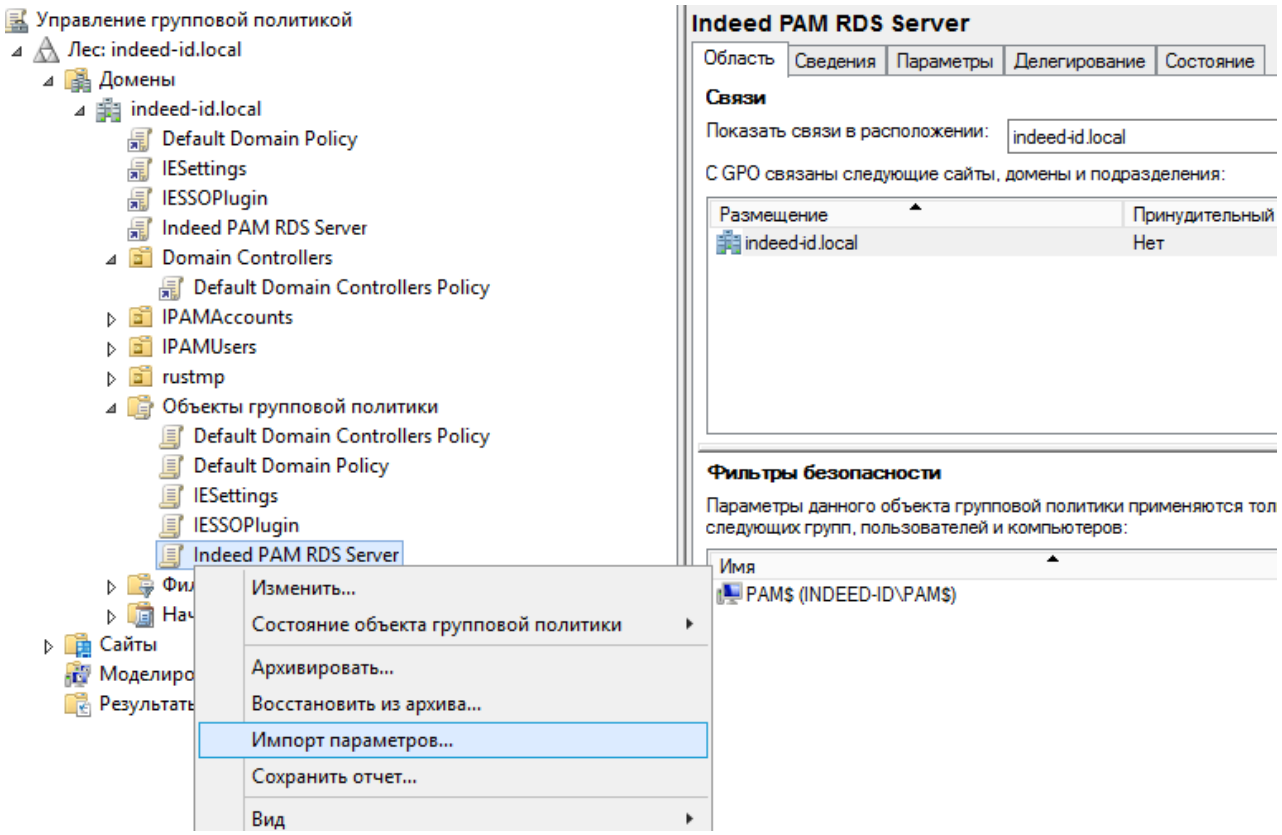
Описание политик

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)

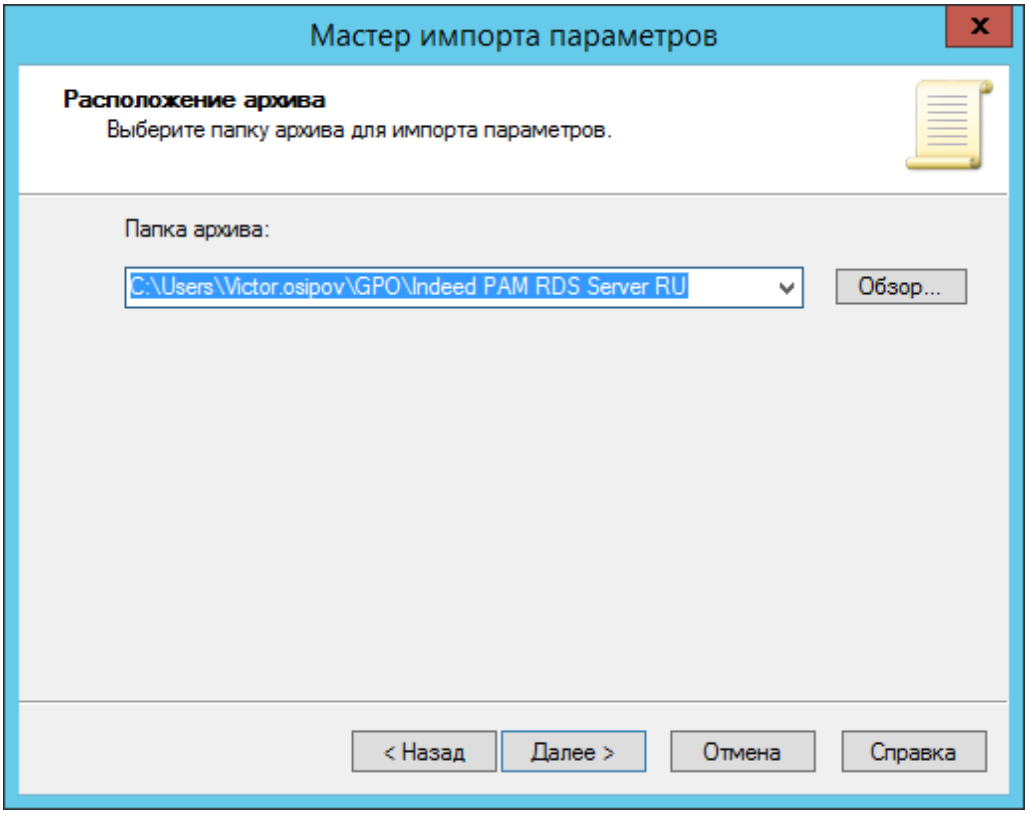
Политика	Описание	Значение
Do not use temporary folders per session (Не использовать временные папки для сеанса)	Данный параметр политики не позволяет службам удаленных рабочих столов создавать временные папки сеансов. С помощью этого параметра политики можно запретить создание на удаленном компьютере 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

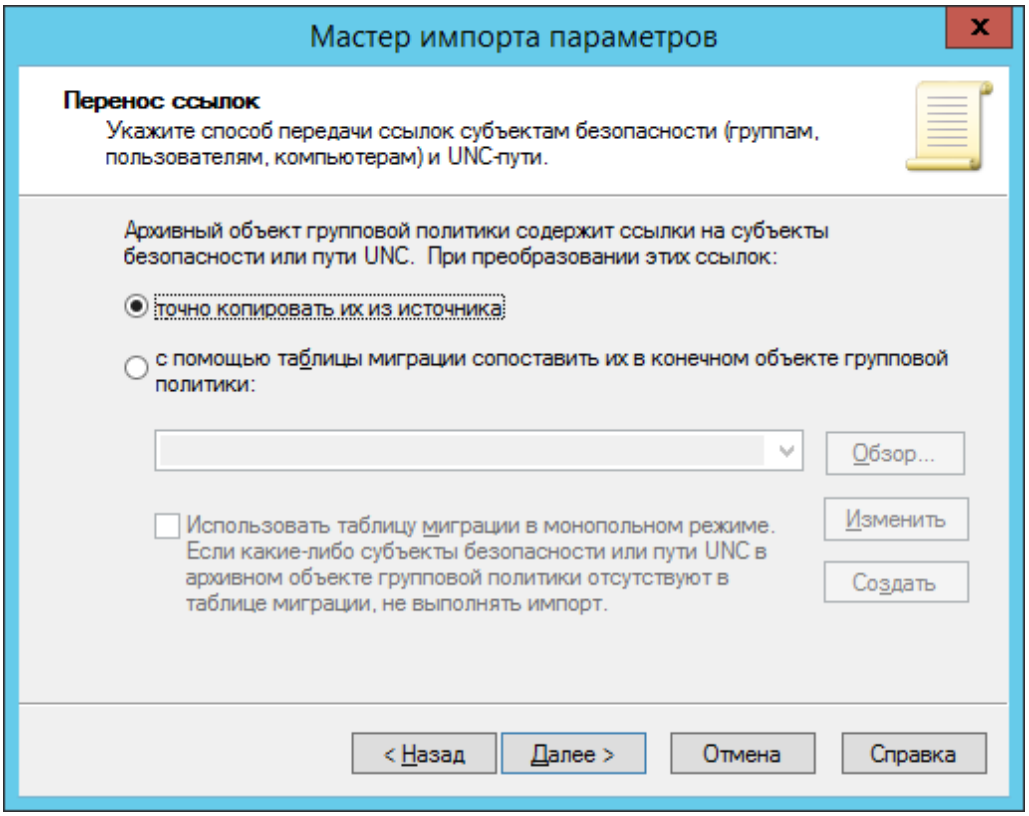
1. На контроллере домена создайте новый объект групповой политики, например «Indeed PAM RDS Server».
2. Настройте фильтры безопасности объекта групповой политики для применения только к объекту сервера Indeed PAM Gateway.
3. Скачайте архив с набором политик для русской или английской версии сервера и 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» включите опцию «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_3.4_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_3.4_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*):

1. Включите опцию **Определить параметры политики** (англ. — *Define these policy settings*)
2. 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

Компрометация ключа — ситуация, когда ключ становится известен и может быть использован третьими лицами. Если произошла компрометация ключей шифрования баз данных PAM, смените ключи путем обновления конфигурации PAM. Для ротации ключей используется утилита KeyRotator.

Пути к конфигурационным файлам компонентов приведены в таблице.

Компонент	Windows	Linux
KeyRotator	*IndeedPAM_3.4_RU\indeed-pam-tools\key-rotator\appsettings.json*	*/etc/indeed/indeed-pam/tools/key-rotator/appsettings.json*
Core	*C:\inetpub\wwwroot\core\appsettings.json*	*/etc/indeed/indeed-pam/core/appsettings.json*
IdP	*C:\inetpub\wwwroot\idp\appsettings.json*	*/etc/indeed/indeed-pam/idp/appsettings.json*

Настройка конфигурации KeyRotator

1. Расшифруйте конфигурационные файлы PAM в зависимости от схемы установки.

2. Откройте конфигурационный файл KeyRotator.

3. В секции `Database` для параметра `Provider` укажите тип сервера СУБД: `PgSql` или `MsSql`.
   Не закрывайте файл.

   Конфигурационный файл KeyRotator

   ```
   "Database": {
     "Provider": "MsSql", // Укажите СУБД
     "PamCore": "PAM_CORE_DB_CONNECTION_STRING",
     "PamIdp": "PAM_IDP_DB_CONNECTION_STRING"
   }
   ```

4. Откройте конфигурационный файл Core.

5. В секции `ConnectionStrings` скопируйте значение параметра `PamCore`.
   Укажите это значение в конфигурационном файле KeyRotator в секции `Database` для параметра

`PamCore`.

Конфигурационный файл Core

```
  "$schema": "appsettings.schema.json",
  "ConnectionStrings": {
    "PamCore": "a4a1b2e2910371e15b353", // Скопируйте это значение
    "JobsQueue": "ecda23a59b856554561ce"
  }
```

Конфигурационный файл KeyRotator

```
"Database": {
  "Provider": "MsSql",
  "PamCore": "a4a1b2e2910371e15b353", // Вставьте значение из файла компонента Core
  "PamIdp": "PAM_IDP_DB_CONNECTION_STRING"
 }
```

6. Откройте конфигурационный файл Idp.

7. В секции `ConnectionStrings` скопируйте значение параметра `DefaultConnection`. Укажите это значение в конфигурационном файле KeyRotator в секции `Database` для параметра `PamIdp`.

Конфигурационный файл Idp

```
"ConnectionStrings": {
     "DefaultConnection": "77f6951e7881ed232cd2d", // Скопируйте это значение
     "JobsQueue": "0786670f99283fcceee86"
  }
```

Конфигурационный файл KeyRotator

```
"Database": {
   "Provider": "MsSql",
   "PamCore": "ENCRYPTED_CfDJ8DpxpXA-mxxMpMmnxTrA",
   "PamIdp": "77f6951e7881ed232cd2d" // Вставьте значение из файла компонента IdP
 }
```

8. Сохраните изменения в конфигурационном файле KeyRotator.

Смена ключа шифрования

Смените ключи шифрования баз данных компонентов Core или Idp. Если нужны изменения для обоих компонентов, меняйте ключи поочередно, так как конфигурационный файл KeyRotator хранит только один набор ключей.

База данных компонента Core

1. Сгенерируйте новый ключ шифрования.

Windows

Чтобы сгенерировать ключ с помощью утилиты KeyGen:

1. Перейдите в дистрибутив PAM по пути *IndeedPAM_3.4_RU\indeed-pam-tools\key-gen*
2. Запустите утилиту IndeedPAM.KeyGen.exe.
3. Для параметра **Algorithm** выберите **Aes** и нажмите **Generate**.
   В результате сгенерируется ключ, например, `e16155e21c73e86c4792c`.
4. Сохраните или скопируйте ключ.

Linux

Чтобы сгенерировать ключ с помощью утилиты OpenSSL, выполните команду:

```
openssl rand -hex 32
```

- `rand` — команда для генерации случайных данных.
- `-hex` — вывод ключа в шестнадцатеричном формате.

- `32` — размер ключа в байтах.

В консоли появится ключ, например, `e16155e21c73e86c4792c`. Сохраните или скопируйте его.

2. Откройте конфигурационный файл Core. В секции `Encryption` у параметра `Key` скопируйте старый ключ и сохраните его, затем укажите новый ключ шифрования.

Конфигурационный файл Core

```
"Encryption": {
  "Primary": {
    "Algorithm": "AES",
    "HashAlgorithm": "SHA512",
    "Key": "1c697af0512e1a20ce099", // Скопируйте старый ключ, а затем вставьте новый ключ
    "MediaFiles": {
      "Algorithm": "AES"
    }
  }
}
```

3. Откройте конфигурационный файл KeyRotator.

4. В секции `Encryption` для параметра `Key` укажите новый ключ шифрования.
   В секции `Secondary` для параметра `Key` укажите значение старого ключа из конфигурационного файла Core.

Конфигурационный файл KeyRotator

```
"Encryption": {
// new encryption settings
  "Primary": {
    "Algorithm": "AES",
    "HashAlgorithm": "SHA512",
    "Key": "e16155e21c73e86c4792c" // Вставьте новый ключ
  },
// old encryption settings
  "Secondary": {
    "Algorithm": "AES",
    "HashAlgorithm": "SHA512",
    "Key": "1c697af0512e1a20ce099" // Вставьте старый ключ из файла компонента Core
    }
  }
```

5. Сохраните изменения в конфигурационных файлах KeyRotator и Core.

6. Выполните ротацию ключа с помощью утилиты KeyRotator.

Windows

1. Перейдите в дистрибутив PAM по пути *IndeedPAM_3.4_RU\indeed-pam-tools\key-rotator*
2. Запустите утилиту Pam.Tools.KeyRotator.exe.

Linux

Выполните команду в терминале:

```
sudo bash /etc/indeed/indeed-pam/tools/key-rotator.sh rotate --component Core
```

7. Зашифруйте конфигурационный файл и перезапустите сервер управления.

База данных компонента Idp

1. Сгенерируйте новый ключ шифрования.

Windows

Чтобы сгенерировать ключ с помощью утилиты KeyGen:

1. Перейдите в дистрибутив PAM по пути *IndeedPAM_3.4_RU\indeed-pam-tools\key-gen*
2. Запустите утилиту IndeedPAM.KeyGen.exe.
3. Для параметра **Algorithm** выберите **Aes** и нажмите **Generate**.
   В результате сгенерируется ключ, например, `594d73ab13ead58463da6`.
4. Сохраните или скопируйте ключ.

Linux

Чтобы сгенерировать ключ с помощью утилиты OpenSSL, выполните команду:

```
openssl rand -hex 32
```

- `rand` — команда для генерации случайных данных.
- `-hex` — вывод ключа в шестнадцатеричном формате.
- `32` — размер ключа в байтах.

В консоли появится ключ, например, `594d73ab13ead58463da6`. Сохраните или скопируйте его.

2. Откройте конфигурационный файл IdP. В секции `Encryption` у параметра `Key` скопируйте старый ключ и сохраните его, затем укажите новый ключ шифрования.

Конфигурационный файл IdP

```
"Encryption": {
  "Primary": {
    "Algorithm": "AES",
    "HashAlgorithm": "SHA512",
    "Key": "ceaaa7f6ac059e0140051", // Скопируйте старый ключ, а затем вставьте новый ключ
    }
  }
```

3. Откройте конфигурационный файл KeyRotator.

4. В секции `Encryption` для параметра `Key` укажите новый ключ шифрования.
   В секции `Secondary` для параметра `Key` укажите значение старого ключа из конфигурационного

файла IdP.

Конфигурационный файл KeyRotator

```
"Encryption": {
// new encryption settings
  "Primary": {
    "Algorithm": "AES",
    "HashAlgorithm": "SHA512",
    "Key": "594d73ab13ead58463da6" // Вставьте новый ключ
  },
// old encryption settings
  "Secondary": {
    "Algorithm": "AES",
    "HashAlgorithm": "SHA512",
    "Key": "ceaaa7f6ac059e0140051" // Вставьте старый ключ из файла компонента Idp
    }
  }
```

5. Сохраните изменения в конфигурационных файлах KeyRotator и IdP.

6. Выполните ротацию ключа с помощью утилиты KeyRotator.

Windows

1. Перейдите в дистрибутив PAM по пути *IndeedPAM_3.4_RU\indeed-pam-tools\key-rotator*
2. Запустите утилиту Pam.Tools.KeyRotator.exe.

Linux

Выполните команду в терминале:

```
sudo bash /etc/indeed/indeed-pam/tools/key-rotator.sh rotate --component Core
```

7. Зашифруйте конфигурационный файл и перезапустите сервер управления.

Шифрование и перезапуск сервера управления

После изменения конфигурационных файлов KeyRotator, Core или IdP выполните шифрование файлов и перезагрузите контейнеры сервера управления PAM.

Windows

1. Выполните шифрование конфигурационных файлов PAM.
2. Запустите PowerShell от имени администратора.
3. Запустите IIS Manager:

```
start inetmgr
```

4. Нажмите на нужный сервер на левой панели.
5. На правой панели нажмите **Restart** (Перезапустить).

Linux

1. Выполните шифрование конфигурационных файлов PAM.
2. Перейдите в папку со скриптами PAM и перезапустите компонент:

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

Аутентификация



Протокол OpenID Connect

Настройте аутентификацию через внешний Identity Provider



Настройка RADIUS

Отредактируйте файл конфигурации appsettings.json



Сертификат X.509

Настройте аутентификацию по сертификату X.509



Настройка одноразового пароля по Email

Отредактируйте файл конфигурации appsettings.json

Протокол OpenID Connect

OpenID Connect (OIDC) — протокол аутентификации, разработанный на основе OAuth 2.0. Протокол позволяет приложениям проверять идентичность пользователя и получать информацию о нем от провайдера идентификации (Identity Provider).

При первой аутентификации по протоколу OIDC сравнивается адрес электронной почты пользователя PAM с адресом почты (`email`) в Identity Provider. Если адреса совпадают, пользователь входит в консоль Indeed PAM. Для каждого пользователя сохраняется уникальный идентификатор (`sub`), который используется при повторной аутентификации для сопоставления пользователя PAM с учетной записью Identity Provider.

Чтобы добавить вход в консоль Indeed PAM через Identity Provider:

1. Укажите адреса электронной почты для пользователей в Indeed PAM.
   Убедитесь, что адреса электронной почты в PAM и Identity Provider совпадают.
2. Настройте конфигурацию для входа через Identity Provider.

> ⓘ **ПРИМЕЧАНИЕ**
>
> Прокси-компоненты не поддерживают аутентификацию по протоколу OpenID Connect. Чтобы получить доступ к ресурсам, включите опции **Открытие сессий без повторной аутентификации** и/или **Аутентификация по SSH-ключам**.

Настройка конфигурации

Чтобы добавить аутентификацию через внешний Identity Provider:

1. В консоли администратора перейдите в раздел **Конфигурация** → **Аутентификация пользователей**.
2. Включите опцию **Включить аутентификацию через OIDC Identity Provider**.
3. В поле **Название кнопки входа** введите название кнопки аутентификации через Identity Provider.
   Кнопка отображается на странице входа в консоли Indeed PAM.
4. В поле **Redirect URI** укажите DNS-имя сервера Indeed PAM.
   Пример: `pam.my-company.local`.
5. Скопируйте значение **Redirect URI** и укажите его при регистрации PAM в настройках Identity Provider.
   На указанный адрес Identity Provider перенаправляет пользователя после аутентификации.
6. В поле **OIDC Provider URL** укажите адрес OIDC-сервера из настроек Identity Provider.
   Пример: `https://idp.company.ru`.

7. Выберите сценарий OIDC-аутентификации:
    - **Authorization Code Flow** — пользователь перенаправляется на сервер авторизации и получает код, который обменивается на токен доступа.
    - **Authorization Code Flow + PKCE (по умолчанию)** — рекомендуемый сценарий, в котором используется расширение Proof Key for Code Exchange (PKCE). Для каждого запроса авторизации генерируется дополнительный секрет, который проверяется при обмене кода на токен доступа.
    - **Implicit Flow** — сервер авторизации возвращает токен доступа в URL-адресе после аутентификации пользователя. Не рекомендуется использовать этот сценарий из-за риска перехвата токенов.
8. В поле **Client ID** укажите идентификатор клиента, созданного при регистрации PAM в Identity Provider.
9. Напротив поля **Client Secret** нажмите  и введите секрет клиента, выданный при регистрации PAM в Identity Provider. Обязательно заполните поле, если выбран сценарий **Authorization Code Flow**.
10. (Опционально) Раскройте дополнительные настройки и заполните поля:
    - **Claim** — имя OIDC-атрибута, из которого PAM получает адрес электронной почты пользователя для сопоставления с учетной записью Identity Provider. По умолчанию используется `email`.
    - **Scope** — имя OIDC-области, используемой в запросе к OIDC-провайдеру для получения значения `claim` с адресом электронной почты пользователя. По умолчанию используется `email`.
11. Нажмите **Сохранить**.

После настройки конфигурации на странице входа в консоль Indeed PAM доступна аутентификация через внешний Identity Provider.

Вход в консоль

> ⓘ **ПРИМЕЧАНИЕ**
> Аутентификация через внешний Identity Provider — дополнительный способ входа.
> Вход по логину и паролю сохраняется.

1. Откройте консоль пользователя или администратора.
2. Перейдите к аутентификации через внешний Identity Provider.
   При неудачной попытке входа свяжитесь с администратором PAM.

Обновление данных пользователя

Если у пользователя в Identity Provider изменился адрес электронной почты (`email`) или идентификатор (`sub`), обновите данные пользователя PAM.

Чтобы обновить данные:

1. В консоли администратора перейдите в раздел **Пользователи**
2. Откройте профиль пользователя.
3. Напротив поля **Email** нажмите  и укажите новый адрес электронной почты.
   Если пользователь из службы каталога, измените адрес электронной почты в каталоге.
4. Нажмите **Сохранить**.
5. Перейдите на вкладку **Аутентификаторы**.
6. Напротив поля **Идентификатор (sub)** нажмите  .
7. В окне подтверждения нажмите **Удалить**.

При повторной аутентификации через OIDC новое значение идентификатора автоматически сохранится в PAM.

Настройка RADIUS

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

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> После внесения изменений в файл конфигурации требуется 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

```
1   "IdentitySettings": {
2   ...
3   "DirectoryMechanism": "Radius",
4   "Authentication": "Local",
5   ...
6   }
```

Секция Radius

- `Timeout` — время ожидания ответа от сервера RADIUS.

`RemoteEndpoints`:

- `Address` — адрес сервера RADIUS для подключения.
- `Port` — адрес сервера RADIUS для подключения (по умолчанию 1812).
- `Secret` — секрет для дополнительной аутентификации компонента.
- `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.
- `CheckMessageAuthenticator` — параметр включает или выключает проверку атрибута `Message-Authenticator` в IDP. Отключать не рекомендуется, так как это понижает безопасность.

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

```
"Radius": {
    "Timeout": 60,
    "RemoteEndpoints": [
      {
        "Address": "PAM_RADIUS_SERVER_ADDRESS",
        "Port": 1812,
        "Secret": "PAM_RADIUS_SERVER_SECRET",
        "AuthenticationScheme": "MSCHAPV2",
        "AuthenticationUserName": "PrincipalName",
        "CheckMessageAuthenticator": true
      }
    ]
  },
```

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

Сертификат X.509

Сертификат X.509 — цифровой документ для проверки пользователей, серверов, устройств или веб-сайтов. Сертификат используется в инфраструктуре открытых ключей (PKI) и содержит информацию о владельце, открытый ключ и цифровую подпись УЦ, подтверждающую подлинность сертификата.

При аутентификации Indeed PAM проверяет сертификат и сравнивает значение `Distinguished Name` (`DN`), извлеченное из поля `Subject` (`Субъект`) в сертификате, со значением `Subject` (`Субъект`) пользователя в PAM. Если значения совпадают, пользователь входит в консоль Indeed PAM.

Чтобы настроить аутентификацию по сертификату X.509:

1. Подготовьте сертификаты X.509 в соответствии с требованиями и разместите их в хранилище сертификатов хоста.
2. Выберите режим аутентификации по сертификату.
3. Добавьте значение `Subject` сертификата для пользователей в Indeed PAM.
   У каждого пользователя должен быть уникальный `Subject`.
4. Откройте консоль пользователя или администратора и аутентифицируйтесь с помощью сертификата X.509.

> ⓘ **ПРИМЕЧАНИЕ**
> Прокси-компоненты не поддерживают аутентификацию по сертификатам.
> Чтобы получить доступ к ресурсам, включите опции **Открытие сессий без повторной аутентификации** и/или **Аутентификация по SSH-ключам**.

Требования к сертификату

- Действующий сертификат в формате .cer, .crt, .pem и .der.
- Сертификат подписан корневым сертификатом или выпускающим сертификатом УЦ.
- В поле `Subject` (`Субъект`) указан `DN` в формате RFC 4514.
  Пример: `CN=Иван Иванов,OU=Разработка,O=Компания,C=RU`.

Настройка конфигурации

Чтобы включить аутентификацию по сертификату X.509:

1. В консоли администратора перейдите в раздел **Конфигурация** → **Аутентификация пользователей**.

2. Для параметра **Аутентификация по сертификату** выберите режим:

   - **Включена (опционально)** — пользователи могут входить в консоль по сертификату или по логину и паролю.
   - **Обязательна для пользователей с указанным Subject сертификата** — пользователи с указанным `Subject` аутентифицируются только по сертификату. Остальные пользователи входят по логину и паролю.
   - **Обязательна для всех пользователей** — вход в консоль возможен только по сертификату.

     > ⚠ **ПРЕДУПРЕЖДЕНИЕ**
     > При выборе режима **Обязательна для всех пользователей** убедитесь, что у пользователей верно заполнено поле **Subject (Субъект)**, иначе войти в консоль не получится.

3. Нажмите **Сохранить**.

Добавление Subject сертификата

> ⓘ **ПРИМЕЧАНИЕ**
> Чтобы добавить для пользователя значение `Subject`, у администратора должна быть привилегия *Управление Subject X.509 сертификатами пользователей*.

Укажите значение `Subject` для всех пользователей с включенной аутентификацией по сертификату X.509. Если `Subject` не задан или введен неверно, пользователь не сможет войти в консоль.

Чтобы добавить `Subject` сертификата:

1. В консоли администратора перейдите в раздел **Пользователи**.
2. Откройте профиль пользователя и перейдите на вкладку **Аутентификаторы**.
3. Напротив поля **Subject (Субъект)** нажмите ✎ и выберите одну из опций:

   - **Вставить вручную** — введите значение `Subject` сертификата.

Пример заполнения

В одну строку

```
CN=Иван Иванов,OU=Отдел разработки,O=Компания
```

Построчно

```
CN=Иван Иванов
OU=Отдел разработки
O=Компания
```

- **Загрузить сертификат** — выберите и загрузите сертификат в формате .cer, .crt, .pem или .der.
  Если сертификат корректный, отобразится распознанное значение `Subject`.

4. Нажмите **Добавить**.

Вход в консоль

> ⓘ **ПРИМЕЧАНИЕ**
> Если сертификат некорректен или просрочен, перезапустите браузер и выберите другой сертификат.

1. Откройте консоль пользователя или администратора.
2. В появившемся окне выберите корректный сертификат X.509 и нажмите **ОК**.

Настройка одноразового пароля по Email

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

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.

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 об 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:

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 требуется 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 требуется 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 службе каталогов

> ⚠ **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 Linux

Сервисные операции для ресурсов Linux выполняются от имени локальной сервисной учетной записи:

- Проверка соединения с ресурсом
- Поиск локальных учетных записей доступа
- Проверка пароля локальных учетных записей доступа
- Изменение пароля локальных учетных записей доступа
- Получение данных об 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. Чтобы предоставить права на выполнение команды SUDO, требуется внести изменения в файл */etc/sudoers*.

Руководство администратора

Консоль администратора

Количество глав: 18

Первый запуск

Лицензируйте продукт, укажите сетевые пути к хранилищам и добавьте все объекты

Дашборд

В режиме реального времени анализируйте активность пользователей и состояние системы.

Настройка политик

Выберите разделы, которые будут управляться политиками

Настройка подключения пользователей по SSH-ключам

Настройка подключения пользователей по SSH-ключам

Выгрузка паролей

Ознакомьтесь с информацией о выгрузке паролей при нештатной ситуации

Работа с PostgreSQL и MSSQL Proxy

Ознакомьтесь с информацией о возможностях PostgreSQL Proxy и MSSQL Proxy.

Работа с Web Proxy

Ознакомьтесь с информацией о возможностях Indeed PAM Web Proxy

Автоматизация через ConsoleApp

Утилита для управления ресурсами, учетными записями и правами доступа в PAM

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

> **ПРИМЕЧАНИЕ**
> Разрешение монитора по ширине должно быть не менее 1280 пикселей, иначе элементы интерфейса консоли администратора будут отображаться некорректно.

Регистрация аутентификатора

Чтобы зарегистрировать аутентификатор, выполните следующие действия:

1. Запустите консоль администратора от имени пользователя, чей SID был указан в конфигурации IDP.
2. Ознакомьтесь с инструкцией по регистрации аутентификатора.
3. Установите приложение для генерации OTP и отсканируйте QR-код.
4. 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 требуется добавить пользователя в состав административной роли.

Вход

1. Откройте консоль администратора.
2. Введите логин. Примеры формата логина:
    - john.smith@space.local — в формате UPN
    - SPACE\john.smith — в формате домен\пользователь

- john.smith — без доменной части

> **ПРИМЕЧАНИЕ**
> Если в инфраструктуре есть пользователь из каталога, у которого совпадает логин с внутренним пользователем, то для входа под пользователем из каталога вводите логин с указанием домена.

3. Введите пароль.
4. Нажмите **Войти**.
5. Введите второй фактор аутентификации.

Смена пароля

> **ПРЕДУПРЕЖДЕНИЕ**
> Эта операция применима только для внутренних пользователей Indeed PAM.

Внутренний пользователь может самостоятельно сменить свой пароль. Для этого выполните следующие действия:

1. Пройдите аутентификацию в консоли администратора.
2. В правом верхнем углу нажмите на логин.
3. В выпадающем списке выберите **Сменить пароль**.
4. В открывшемся окне введите текущий пароль и новый пароль.
5. Если требуется, отключите опцию **Завершить все активные сессии**.
6. Нажмите **Сменить пароль**.

Выход

1. Убедитесь, что вы аутентифицированы в консоли администратора.
2. В правом верхнем углу нажмите на логин.
3. В выпадающем списке нажмите **Выйти** и подтвердите действие.

Пользователи

Раздел предназначен для работы со следующими видами пользователей Indeed PAM:

- Пользователи из службы каталога.
  Для таких пользователей в поле **Источник** указано *Каталог*.
- Внутренние пользователи.
  Для таких пользователей в поле **Источник** указано *PAM*.

По умолчанию на странице отображается 15 пользователей. Для просмотра доступно только 1000 пользователей.
Изменить количество отображаемых пользователей на странице можно в конфигурационном файле:

- Windows: *C:\inetpub\wwwroot\mc\assets\config\config.prod.json*
- Linux: */etc/indeed/indeed-pam/mc/config.prod.json*

Найти пользователя

Введите в поисковую строку имя, фамилию, номер телефона или Email и нажмите .

Нажмите **Расширенный поиск,** введите один или несколько запросов и нажмите **Найти**.

> ⓘ **ПРИМЕЧАНИЕ**
> Поиск по логину не поддерживается.

Чтобы найти удаленных пользователей:

1. Откройте раздел **Пользователи** и нажмите **Расширенный поиск**.
2. Выберите значение **Удален** для параметра **Состояние**.
3. Нажмите **Найти**.

Создать внутреннего пользователя

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> Не закрывайте окно, пока не передадите пароль пользователю.
>
> Для внутренних пользователей недоступно подключение через RDS.

1. Откройте раздел **Пользователи**.

2. Нажмите **Создать**.
3. Заполните поле **Логин**.
   По логину происходит вход в консоли пользователя и администратора.
4. Выберите одну из опций:
   - **Задать пароль вручную** — пароль задается в ручном режиме.
   - **Сгенерировать** — пароль генерируется PAM.
5. Скопируйте пароль и передайте его пользователю.
6. Задайте опцию **Требовать смену пароля при первом входе**.
7. Введите Email пользователя.
8. Нажмите **Дополнительно** и заполните поля: **Имя**, **Фамилия**, **Телефон**, **Описание**.
9. Завершите добавление пользователя:
   - Нажмите **Создать**, чтобы остаться в разделе **Пользователи**.
   - Нажмите **Создать и открыть**, чтобы перейти в профиль нового пользователя.

Профиль пользователя

Для каждого пользователя отображаются:

- **Разрешения** — список выданных разрешений для пользователя на подключение к ресурсу.
- **Группы пользователей** — список групп, в которых состоит пользователь.
- **Сессии** — список активных, завершенных и прерванных сессий.
- **Аутентификаторы** — информация о настроенных аутентификаторах пользователя.
- **События** — записи об операциях, связанных с пользователем.

Выбрать политику

1. Откройте профиль пользователя.
2. Нажмите ✎ напротив параметра **Политика**.
3. Выберите политику из списка и нажмите **Выбрать**.

Настроить аутентификатор

На вкладке **Аутентификаторы** отображается информация о пароле, втором факторе и SSH-ключах, которые позволяют подключаться к SSH Proxy без пароля.

Для всех пользователей отображается состояние аутентификатора. Значение *Не обучена* указывает на незарегистрированный аутентификатор. При первом входе пользователя в консоль

администратора или консоль пользователя откроется страница с инструкцией по регистрации аутентификатора. После регистрации отображается значение *Обучена*.

SSH-ключи

SSH-ключи позволяют подключаться к SSH Proxy без пароля. Одному пользователю можно добавить максимум 10 SSH-ключей. Ключи должны быть уникальными в рамках одного пользователя, но могут повторяться у разных пользователей.

Поддерживаемые алгоритмы шифрования ключей

Поддерживаемые алгоритмы шифрования ключей:

- rsa-sha2-256
- rsa-sha2-512
- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384
- ecdsa-sha2-nistp521
- ssh-ed25519

Включить или отключить использование ключей можно в разделе **Конфигурация**.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> Чтобы добавить ключ пользователю, у администратора должна быть привилегия *User.ManageSshAuthorizedKeys*.

Чтобы добавить SSH-ключ:

- вставьте скопированную строку, содержащую алгоритм шифрования и ключ;
- прикрепите файл сертификата X.509.

Ключ в текстовом формате

1. Откройте профиль пользователя.
2. Перейдите на вкладку **Аутентификаторы**.
3. Нажмите **Добавить**.
4. Вставьте ключ в формате OpenSSH в поле **Открытый ключ**. Строка с ключом должна содержать алгоритм шифрования и ключ. Опционально строка может содержать комментарий, например имя пользователя и хост.
   Пример: `ssh-ed25519 AAAAC3... user@host`

5. Заполните поле **Описание**.
6. Нажмите **Добавить**.

Сертификат X.509

1. Откройте профиль пользователя.
2. Перейдите на вкладку **Аутентификаторы**.
3. Нажмите **Добавить**.
4. Нажмите **Загрузить сертификат**.
5. Проверьте срок действия сертификата. Для этого запустите одну из команд в зависимости от используемой ОС:

   Команда для Windows

   ```
   certutil -verify -urlfetch "Название файла сертификата.crt"
   ```

   Команда для Linux

   ```
   openssl x509 -in "Название файла сертификата.crt" -text -noout
   ```

   Убедитесь, что срок, в который планируется подключение по ключу, входит в промежуток дат между `NotBefore` и `NotAfter`.

6. Загрузите файл в поле **Сертификат X.509**.

   > ⚠ **ПРЕДУПРЕЖДЕНИЕ**
   > Загрузка сертификата, который содержит цепочку сертификатов, не поддерживается.
   >
   > Автоматической проверки на срок действия сертификата нет.

7. Отредактируйте поле **Описание**.
8. Нажмите **Добавить**.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> Ключ невозможно восстановить после удаления.

Чтобы удалить SSH-ключ:

1. Откройте профиль пользователя.
2. Перейдите на вкладку **Аутентификаторы**.
3. Выберите один или несколько ключей.
4. Нажмите **Удалить**.

При удалении SSH-ключа открытая с помощью этого ключа сессия не разрывается.

> ⓘ **ПРИМЕЧАНИЕ**
> Если один и тот же ключ добавлен нескольким пользователям, то удаление ключа у одного пользователя не приведет к удалению такого же ключа у других пользователей.

Второй фактор

1. Откройте профиль пользователя и перейдите на вкладку **Аутентификаторы**.
2. Нажмите ✎ напротив параметра **Требовать второй фактор** и выберите одну из опций:
   - **По умолчанию** — по умолчанию требуется ввод пользователем второго фактора для аутентификации в системе.
   - **Включено** — у пользователя запрашивается второй фактор для аутентификации в системе.
   - **Отключено** — у пользователя не запрашивается второй фактор для аутентификации в системе.
3. Нажмите **Изменить**.

Чтобы сбросить аутентификатор, нажмите ✕ напротив нужного аутентификатора.

Сертификат X.509

Укажите значение `Subject` для всех пользователей с включенной аутентификацией по сертификату X.509. Если `Subject` не задан или введен неверно, пользователь не сможет войти в консоль.

Чтобы добавить `Subject` сертификата:

1. Откройте профиль пользователя и перейдите на вкладку **Аутентификаторы**.
2. Напротив поля **Subject (Субъект)** нажмите ✎ и выберите одну из опций:
   - **Вставить вручную** — введите значение `Subject` сертификата.

Пример заполнения

В одну строку

```
CN=Иван Иванов,OU=Отдел разработки,O=Компания
```

Построчно

```
CN=Иван Иванов
OU=Отдел разработки
O=Компания
```

- **Загрузить сертификат** — выберите и загрузите сертификат в формате .cer, .crt, .pem или .der.
  Если сертификат корректный, отобразится распознанное значение `Subject`.

3. Нажмите **Добавить**.

OIDC Identity Provider

Идентификатор используется при входе в консоль Indeed PAM для сопоставления пользователя PAM с учетной записью Identity Provider. Если у пользователя в Identity Provider изменился адрес электронной почты (`email`) или идентификатор (`sub`), обновите данные пользователя PAM.

Чтобы обновить данные:

1. Откройте профиль пользователя.
2. Напротив поля **Email** нажмите и укажите новый адрес электронной почты.
   Если пользователь из службы каталога, измените адрес электронной почты в каталоге.
3. Нажмите **Сохранить**.
4. Перейдите на вкладку **Аутентификаторы**.
5. Напротив поля **Идентификатор (sub)** нажмите .
6. В окне подтверждения нажмите **Удалить**.

При повторной аутентификации через OIDC новое значение идентификатора автоматически сохранится в PAM.

Добавить разрешение

1. Откройте профиль пользователя.
2. Нажмите **Добавить разрешение**.
3. Выберите параметр разрешения:
   - **Ресурсы** — разрешение выдается на один или несколько выбранных ресурсов.
   - **Группы ресурсов** — разрешение выдается на выбранную группу ресурсов.
   - **Произвольные подключения** — разрешение выдается на любые ресурсы с выбранным типом подключения, в том числе на ресурсы, не зарегистрированные в PAM.
4. Выберите учетную запись:
   - **Выбрать УЗ в PAM** — учетная запись, от имени которой пользователь открывает сессию на ресурсе.
   - **Пользовательская УЗ** — в разрешении не указывается учетная запись. Пользователь вводит логин и пароль учетной записи на ресурсе. В RDP- и SSH-сессиях можно войти с текущими учетными данными пользователя Indeed PAM.
5. Настройте **Ограничения времени** и нажмите **Вперед**.
6. Настройте **Параметры разрешения** и нажмите **Вперед**.
7. Заполните поле **Описание** и нажмите **Вперед**.
8. Проверьте данные и нажмите **Создать**.

Добавить и удалить из группы

Чтобы добавить пользователя в группу:

1. Откройте профиль пользователя и перейдите на вкладку **Группы пользователей**.
2. Нажмите **Добавить группы пользователей**.
3. Выберите одну или несколько групп и нажмите **ОК**.

Чтобы удалить пользователя из группы:

1. Откройте профиль пользователя и перейдите на вкладку **Группы пользователей**.
2. Выберите одну или несколько групп.
3. Нажмите **Удалить**.
4. Подтвердите действие нажатием **Удалить** во всплывающем окне.

Чтобы добавить в группу нескольких пользователей, в разделе **Пользователи** выберите нужных пользователей и нажмите **Добавить в группу**. Выберите одну или несколько групп и нажмите **ОК**.

Задать, сбросить или запросить пароль

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> Доступно только для внутренних пользователей Indeed PAM.

1. Откройте профиль внутреннего пользователя.
2. Нажмите **Сбросить пароль**.
3. Выберите одну из опций:
   - **Сгенерировать** — пароль создается автоматически.
   - **Задать пароль вручную** — пароль задается в ручном режиме.
   - **Запросить смену пароля** — пароль запрашивается PAM при входе в систему.
4. Передайте пароль пользователю. После закрытия формы узнать пароль будет невозможно.
5. Задайте опцию **Требовать смену пароля при первом входе**.
6. Задайте опцию **Прервать все активные сессии и выйти из системы**.
7. Нажмите **Сохранить**.

Чтобы сбросить пароль для нескольких пользователей, в разделе **Пользователи** выберите нужных пользователей и нажмите **Запросить смену пароля**. Можно прервать все активные сессии выбранных пользователей.

Заблокировать и разблокировать

Заблокируйте пользователя, если нужно ограничить доступ к PAM. При блокировке доступ в систему полностью прекращается: аутентификация в консолях пользователя и администратора недоступна, а все активные сессии завершаются. В любой момент пользователя можно разблокировать.

Чтобы заблокировать пользователя:

1. Зайдите в раздел **Пользователи**.
2. Откройте профиль пользователя.
3. Нажмите **Заблокировать**.
4. В окне подтверждения операции нажмите **Заблокировать**.

Чтобы заблокировать нескольких пользователей, в разделе **Пользователи** выберите нужных пользователей и нажмите **Заблокировать**.

Чтобы разблокировать пользователя:

1. Зайдите в раздел **Пользователи**.
2. Откройте профиль заблокированного пользователя.

3. Нажмите **Разблокировать**.
4. В окне подтверждения операции нажмите **Разблокировать**.

Чтобы разблокировать нескольких пользователей, в разделе **Пользователи** выберите заблокированных пользователей и нажмите **Разблокировать**.

Удалить пользователя

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> Эта операция применима только для внутренних пользователей Indeed PAM.
> Удаленного пользователя нельзя восстановить. Невозможно удалить самого себя и первого администратора ролей.

Чтобы удалить пользователя:

1. Откройте профиль внутреннего пользователя.
2. Нажмите **Удалить**.
3. Прочитайте информацию во всплывающем окне и подтвердите действие нажатием **Удалить**.

Чтобы удалить нескольких пользователей PAM, в разделе **Пользователи** выберите нужных пользователей и нажмите **Удалить**.

После удаления пользователя:

- все активные сессии завершаются;
- выданные разрешения отзываются;
- пользователю недоступен вход в PAM и аутентификация;
- пользователь исключается из всех групп пользователей и области действия политики, в которых он состоит;
- логин удаленного пользователя меняется: к нему добавляется суффикс `_deleted` и случайно сгенерированная строка.

Удаленные пользователи перестают отображаться в разделе **Пользователи**, но их можно просмотреть с помощью расширенного поиска.

Группы пользователей

Раздел предназначен для работы с группами пользователей.

Создать группу пользователей PAM

1. Перейдите в раздел **Группы пользователей** и нажмите **Добавить**.
2. Заполните поля **Имя** и **Описание**.
3. Нажмите **Сохранить**.

Создать группу пользователей из службы каталогов

1. Перейдите в раздел **Группы пользователей** и нажмите **Добавить из каталога**.
2. Введите имя каталога и нажмите  .
3. Выберите группу и нажмите **Сохранить**.

Профиль группы

Для каждой группы пользователей отображаются:

- Пользователи — список пользователей, которые состоят в группе.
- Разрешения — список выданных разрешений для группы на подключение к ресурсу.
- Сессии — список активных, завершенных и прерванных сессий.
- События — записи об операциях, связанных с группой.

Добавить пользователей в группу

> **ПРИМЕЧАНИЕ**
> Только для групп, созданных через PAM.

Чтобы добавить пользователей в группу:

1. Откройте профиль группы пользователей.
2. Перейдите на вкладку **Пользователи** и нажмите **Добавить пользователей**.

3. Выберите одного или несколько пользователей и нажмите **ОК**.
4. Подтвердите выбор и нажмите **Добавить**.

Добавить разрешение

1. Откройте профиль группы пользователей.
2. Нажмите **Добавить разрешение**.
3. Выберите параметр разрешения:
   - **Ресурсы** — разрешение выдается на один или несколько выбранных ресурсов.
   - **Группы ресурсов** — разрешение выдается на выбранную группу ресурсов.
   - **Произвольные подключения** — разрешение выдается на любые ресурсы с выбранным типом подключения, в том числе на ресурсы, незарегистрированные в PAM.
4. Выберите учетную запись:
   - **Выбрать УЗ в PAM** — учетная запись, от имени которой пользователь открывает сессию на ресурсе.
   - **Пользовательская УЗ** — в разрешении не указывается учетная запись. Пользователь вводит логин и пароль учетной записи на ресурсе. В RDP- и SSH-сессиях можно войти с текущими учетными данными пользователя Indeed PAM.
5. Настройте **Ограничения времени** и нажмите **Вперед**.
6. Настройте **Параметры разрешения** и нажмите **Вперед**.
7. Введите **Описание** и нажмите **Вперед**.
8. Проверьте данные и нажмите **Создать**.

Синхронизировать группы пользователей с каталогом

> ⓘ **ПРИМЕЧАНИЕ**
> Только для групп из службы каталогов.

1. Откройте профиль группы пользователей.
2. Нажмите **Синхронизировать** и подтвердите действие.

Выбрать политику

1. Откройте профиль группы пользователей.
2. Нажмите ✎ напротив параметра **Политика**.

3. Выберите политику из списка и нажмите **Выбрать**.

Удалить

1. Откройте профиль группы пользователей.
2. Нажмите **Удалить**.
3. Подтвердите действие нажатием **Удалить**.

Чтобы удалить несколько групп, в разделе **Группы пользователей** выберите нужные группы и нажмите **Удалить**.

Ресурсы

Раздел предназначен для работы с серверами, рабочими станциями, сетевым оборудованием и клиентскими приложениями.

Поиск

Поиск осуществляется в разделе **Ресурсы**.

Быстрый поиск

Введите в поисковую строку имя ресурса, DNS-имя, IP-адрес, пользовательское подключение или тег и нажмите  .

Расширенный поиск

Нажмите **Расширенный поиск**, введите один или несколько запросов и нажмите **Найти**.

Профиль ресурса

Пользователи могут подключаться к ресурсам и открывать сессии по протоколам RDP, SSH, Telnet, PostgreSQL, а также Web/Desktop-сессии. Для запуска сессии нужно получить разрешение на подключение учетной записи к ресурсу.

Для каждого ресурса отображаются:

- Пользовательские подключения — список подключений для установки соединения с ресурсом. Для каждого ресурса можно создать несколько пользовательских подключений. Это необходимо при наличии на сервере нескольких приложений, требующих привилегированного доступа.
- Разрешения — список выданных разрешений для подключения к ресурсу.
- Локальные учетные записи — список локальных учетных записей, которые используются для открытия сессии на ресурсе.
- Группы ресурсов — список групп, в которые добавлен ресурс.
- Сессии — список активных, завершенных и прерванных сессий на ресурсе.
- События — записи об операциях, связанных с ресурсом.
- Службы — список приложений, которые могут запускаться автоматически при запуске операционной системы.

Вкладка отображается, если у связанного ресурса есть настроенное сервисное подключение для Windows.

Добавить ресурс в группу

1. Откройте профиль ресурса и перейдите на вкладку **Группы ресурсов**.
2. Нажмите **Добавить группу ресурсов**.
3. Выберите группу и нажмите **Вперед**.
4. Выберите одно или несколько пользовательских подключений и нажмите **Вперед**.
5. Проверьте данные и нажмите **Добавить**.

Добавить службу

1. Откройте профиль ресурса и перейдите на вкладку **Службы**.
2. Заполните поля **Имя** и **Описание**.
3. Задайте опцию **Перезапускать службу при смене пароля службы** и нажмите **Вперед**.
4. Выберите учетную запись для службы.
5. Проверьте данные и нажмите **Добавить**.

Выбрать политику

1. Откройте профиль ресурса.
2. Нажмите напротив параметра **Политика**.
3. Выберите политику и нажмите **Выбрать**.

Добавление ресурсов

Чтобы пользователи могли подключаться к ресурсам, добавьте ресурсы в Indeed PAM.

Добавить ресурс вручную

1. Перейдите в раздел **Ресурсы** и нажмите **Добавить**.
2. Заполните поле **Имя ресурса**.
   Для ресурсов с ОС Windows укажите имя компьютера.
3. Заполните поле **DNS-имя** и/или **IP-адрес**.
4. Введите описание и нажмите **Вперед**.
5. Выберите тип пользовательского подключения.
6. Выберите **Адрес подключения**:
   - **Наследовать из ресурса** — адрес подключения дублирует DNS-имя, URL- или IP-адрес ресурса.
   - **Указать вручную** — адрес подключения задается вручную в формате `https://app.local:port` или `https://app.local`.
7. Заполните поле **Порт**.
8. Укажите дополнительные параметры в зависимости от выбранного типа подключения:

   PostgreSQL или MSSQL

   Заполните поле **База данных по умолчанию**.
   Выбор базы по умолчанию не ограничивает доступ пользователя к другим базам данных на этом ресурсе. Доступные базы определяются правами учетной записи СУБД, указанной в разрешении.

SSH

1. Задайте **Отпечаток SSH-ключа**:

   - **Получить с ресурса** — используйте отпечаток SSH-ключа с ресурса.
   - **Указать вручную** — выберите алгоритм и введите отпечаток в формате SHA256.

2. Укажите форматы логинов для локальной и доменной учетных записей:

   - **По умолчанию** — формат, заданный в конфигурации подключения.
   - **Указать вручную** — форматы логинов задаются вручную.
     Используйте обязательную переменную `%username%` и дополнительные `%location%`, `%location-dns%`.

     #### Примеры

     Формат логина john.smith@pam.local

     ```
     %username%@%location-dns%
     ```

     Формат логина SPACE\john.smith

     ```
     %location%\%username%
     ```

     Формат логина john.smith

     ```
     %username%
     ```

RDP

(Опционально) Включите опцию **Запустить как администратор**.
RDP-сессия откроется с параметром `/admin`. Пользователь получит доступ к административной консоли и сможет выполнять команды, требующие повышенных привилегий.

Собственный тип пользовательского подключения

> **ПРИМЕЧАНИЕ**
> Добавить собственный тип пользовательского подключения можно в разделе **Конфигурация → Пользовательское подключение**.

1. (Опционально) В поле **URL страницы входа** укажите URL-адрес, на который нужно перейти при запуске веб-сессии.

2. (Опционально) Включите опцию **Регулярное выражение**, если при переходе на указанную страницу в URL-адрес динамически добавляются параметры запроса. В поле **URL страницы входа** укажите регулярное выражение, соответствующее адресу страницы.

   Пример

   Сессия открывается по адресу `https://app.org/mainpage`.

   При переходе по ссылке к URL динамически добавляются параметры `theme` и `page`.
   Адрес страницы принимает вид `https://app.org/mainpage/?theme=dark&page=dashboard`.

   Чтобы перейти по нужному адресу, включите опцию **Регулярное выражение** и в поле **URL страницы входа** укажите регулярное выражение, соответствующее адресу страницы.
   Например: `https://app.org/mainpage*`, где символ `*` заменяет дополнительные параметры в строке запроса.

9. (Опционально) Включите опцию **Использовать коннектор для сервисного подключения** и настройте сервисное подключение. На следующем шаге выберите сервисную учетную запись.

10. Нажмите **Вперед**.

11. Проверьте введенные данные и нажмите **Сохранить**.

Добавить ресурс из файла

1. Подготовьте CSV-файл с ресурсами.

2. Откройте раздел **Ресурсы**.
3. Нажмите **Добавить из файла**.
4. Выберите созданный CSV-файл.
5. Если для ресурсов требуется определить политику, включите опцию **Добавлять с политикой**.
6. Нажмите **Вперед** для перехода к следующему окну мастера.
7. Выберите политику.
8. 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;;;;;;;;;
```

Список параметров

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. Требуется 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 страницы 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.
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.

Название	Приоритет	Описание
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 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

Редактировать ресурс

Для редактирования доступны следующие поля ресурса:

- Имя ресурса;
- Описание;
- DNS-имя;
- IP-адрес;
- Политика;
- Сервисное подключение.

Чтобы отредактировать ресурс, нажмите ✎ напротив нужного параметра.

Добавить и удалить тег

> **ИНФОРМАЦИЯ**
> Если у вас еще нет тегов, создайте их в разделе Конфигурация.

Чтобы добавить теги ресурсу:

1. Откройте профиль ресурса.
2. Нажмите + рядом с полем **Теги**.
3. Выберите теги и нажмите **Вперед**.
4. Проверьте выбранные теги и нажмите **Добавить** для завершения операции.

> **ИНФОРМАЦИЯ**
> У каждого ресурса может быть максимум 50 тегов.

Чтобы удалить тег у ресурса:

1. Откройте профиль ресурса.
2. Нажмите ✕ рядом с тегом, который требуется удалить.
3. В окне подтверждения нажмите **Удалить**.

Удалить связанные сущности

Для удаления значений доступны следующие поля ресурса:

- **Политика**;
- **Сервисное подключение**.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> При удалении сервисного подключения с ресурса все связанные с ним службы удалятся без возможности восстановления.
>
> Удаленные службы перестают отображаться в разделе **Службы**, но их можно просмотреть с помощью расширенного поиска.

Чтобы удалить **Политику** или **Сервисное подключение** с ресурса, нажмите 🗑 напротив нужного параметра.

Добавить пользовательское подключение

1. Откройте профиль ресурса.
2. На вкладке **Пользовательские подключения** нажмите **Добавить пользовательское подключение**.
3. Выберите тип подключения.
4. Выберите адрес подключения:
   - **Наследовать из ресурса** — адрес подключения дублирует DNS-имя, URL- или IP-адрес ресурса.
   - **Указать вручную** — адрес подключения задается вручную в формате `https://app.local:port` или `https://app.local`.
5. (Опционально) Укажите порт, если он отличается от порта по умолчанию.
6. Укажите дополнительные параметры в зависимости от выбранного типа подключения:

PostgreSQL или MSSQL

Заполните поле **База данных по умолчанию**.
Выбор базы по умолчанию не ограничивает доступ пользователя к другим базам данных на этом ресурсе. Доступные базы определяются правами учетной записи СУБД, указанной в разрешении.

SSH

1. Задайте **Отпечаток SSH-ключа**:
   - **Получить с ресурса** — используйте отпечаток SSH-ключа с ресурса.
   - **Указать вручную** — выберите алгоритм и введите отпечаток в формате SHA256.
2. Укажите форматы логинов для локальной и доменной учетных записей:
   - **По умолчанию** — формат, заданный в конфигурации подключения.
   - **Указать вручную** — форматы логинов задаются вручную.
     Используйте обязательную переменную `%username%` и дополнительные `%location%`, `%location-dns%`.

Примеры

Формат логина john.smith@pam.local

```
%username%@%location-dns%
```

Формат логина SPACE\john.smith

```
%location%\%username%
```

Формат логина john.smith

```
%username%
```

RDP

(Опционально) Включите опцию **Запустить как администратор**.
RDP-сессия откроется с параметром `/admin`. Пользователь получит доступ к административной консоли и сможет выполнять команды, требующие повышенных привилегий.

Собственный тип пользовательского подключения

> **ПРИМЕЧАНИЕ**
> Добавить собственный тип пользовательского подключения можно в разделе **Конфигурация → Пользовательское подключение**.

1. (Опционально) В поле **URL страницы входа** укажите URL-адрес, на который нужно перейти при запуске веб-сессии.

2. (Опционально) Включите опцию **Регулярное выражение**, если при переходе на указанную страницу в URL-адрес динамически добавляются параметры запроса. В поле **URL страницы входа** укажите регулярное выражение, соответствующее адресу страницы.

   #### Пример

   Сессия открывается по адресу `https://app.org/mainpage`.

   При переходе по ссылке к URL динамически добавляются параметры `theme` и `page`.
   Адрес страницы принимает вид `https://app.org/mainpage/?theme=dark&page=dashboard`.

   Чтобы перейти по нужному адресу, включите опцию **Регулярное выражение** и в поле **URL страницы входа** укажите регулярное выражение, соответствующее адресу страницы.
   Например: `https://app.org/mainpage*`, где символ `*` заменяет дополнительные параметры в строке запроса.

7. Нажмите **Сохранить**.

Добавить разрешение

1. Откройте профиль ресурса.
2. Нажмите **Добавить разрешение**.
3. Выберите пользователей или группу пользователей и нажмите **Вперед**.
4. Выберите одно или несколько подключений и нажмите **Вперед**.
5. Выберите учетную запись:
   - **Выбрать УЗ в PAM** — учетная запись, от имени которой пользователь открывает сессию на ресурсе.
   - **Пользовательская УЗ** — в разрешении не указывается учетная запись.
     Пользователь вводит логин и пароль учетной записи на ресурсе. В RDP- и SSH-сессиях можно войти с текущими учетными данными пользователя Indeed PAM.
6. Настройте **Ограничения времени** и нажмите **Вперед**.
7. Настройте **Параметры разрешения** и нажмите **Вперед**.
8. Заполните поле **Описание** и нажмите **Вперед**.
9. Проверьте данные и нажмите **Создать**.

Добавить учетную запись

Функция позволяет добавлять в Indeed PAM локальные учетные записи ресурса, которые могут использоваться для предоставления доступа на ресурс.

1. Перейдите на вкладку **Локальные учетные записи** и нажмите **Добавить локальную учетную запись**.
2. Введите **Имя учетной записи** и **Описание**.
3. Нажмите **Вперед**.

Пароль и SSH-ключ

> ⓘ **ИНФОРМАЦИЯ**
> При добавлении учетной записи для ресурса с настроенным сервисным подключением SSH можно настроить не только пароль, но и SSH-ключ.
>
> При добавлении учетных записей ОС Windows и СУБД необходимо задать пароль. Настройка SSH-ключа для данных типов недоступна.

Настройка пароля

1. Выберите одну из опций:

- **Сгенерировать случайный пароль** — пароль создается автоматически и синхронизируется с ресурсом или доменом.
- **Задать пароль вручную** — пароль задается в ручном режиме.
  Введите пароль и подтвердите его.
  Чтобы пароль учетной записи сменился не только в PAM, но и на ресурсе или домене, включите опцию **Изменить пароль на ресурсе** или **Изменить пароль в домене**.
- **Не задавать** — учетная запись создается без пароля, его можно задать позже при редактировании.

2. Нажмите **Вперед**.

Настройка SSH-ключа

1. Выберите одну из опций:

   - **Сгенерировать новый SSH-ключ** — ключ создается автоматически и синхронизируется с ресурсом или доменом. Выберите криптографический алгоритм для генерации ключа: **Ed25519** или **RSA**.

   - **Задать SSH-ключ вручную** — ключ задается в ручном режиме. Выберите файл SSH-ключа и введите его пароль. Поддерживаются ключи RSA в форматах OpenSSH и PEM, а также Ed25519 в формате OpenSSH.

     Как сгенерировать SSH-ключ?

     Чтобы создать SSH-ключ и записать его в файл, воспользуйтесь программой PuTTYgen или одной из команд:

     Ключ RSA в формате OpenSSH

     ```
     ssh-keygen -t rsa -b 4096 -f id_rsa_openssh -C "RSA OpenSSH key"
     ```

     Ключ RSA в формате PEM

     ```
     ssh-keygen -t rsa -b 4096 -f id_rsa_pem -C "RSA PEM key" -m PEM
     ```

     Ключ Ed25519 в формате OpenSSH

     ```
     ssh-keygen -t ed25519 -f id_ed25519_openssh -C "Ed25519 OpenSSH key"
     ```

Чтобы SSH-ключ учетной записи сменился не только в PAM, но и на ресурсе или домене, включите опцию **Изменить SSH-ключ на ресурсе** или **Изменить SSH-ключ в домене**.

- **Не задавать** — учетная запись создается без SSH-ключа, его можно установить позже при редактировании.

2. Нажмите **Вперед**.

3. Проверьте данные и нажмите **Сохранить**

Проверить соединение

Функция позволяет проверить сетевую доступность ресурса, корректность адреса, имени и пароля сервисной учетной записи.

Операция выполняется с помощью кнопки **Проверить соединение** в профиле ресурса.

Синхронизировать

Функция позволяет получить корректное имя ресурса, версию ОС или СУБД, локальные учетные записи и группы безопасности, в которых они состоят. Синхронизация доступна только для ресурсов с настроенным сервисным подключением.

Операция выполняется с помощью кнопки **Синхронизировать** в профиле ресурса.

> **ПРИМЕЧАНИЕ**
>
> Синхронизированные учетные записи будут отмечены символом ⚠. Для продолжения работы с учетными записями потребуется предоставить системе их пароль или сбросить его на случайное значение.
>
> Как подтвердить учетную запись читайте в разделе **Учетные записи**.

Заблокировать

Функция позволяет приостановить действие всех разрешений, в которых используется ресурс.

Операция выполняется с помощью кнопки **Заблокировать** в профиле ресурса.

> ⓘ **ПРИМЕЧАНИЕ**
>
> Заблокированный ресурс будет отмечен символом  .
>
> Все разрешения, в которых ресурс является участником, будут отмечены символом  .

Удалить и восстановить ресурс

Удалить ресурс

Перед удалением ресурса требуется удалить все учетные записи, которые были добавлены из удаляемого ресурса.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> При удалении ресурса все связанные с ним службы также удалятся без возможности восстановления.
>
> Удаленные службы перестают отображаться в разделе **Службы**, но их можно просмотреть с помощью расширенного поиска.

1. Откройте профиль ресурса.
2. Нажмите **Удалить**.

Восстановить ресурс

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> При восстановлении ресурса связанные с ним службы не восстанавливаются. Информацию по удаленным службам можно просмотреть с помощью расширенного поиска в разделе Службы.

1. В разделе **Ресурсы** нажмите **Расширенный поиск**.
2. Введите **Имя ресурса** или **Адрес (DNS-имя или IP-адрес)**.
3. В поле **Состояние** выберите 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

1. В разделе **Ресурсы** отметьте один или несколько ресурсов.
2. 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

1. В разделе **Ресурсы** отметьте один или несколько ресурсов.
2. Нажмите **Проверить соединение**.

Удаление ресурсов

1. В разделе **Ресурсы** отметьте один или несколько ресурсов.
2. Нажмите **Удалить**.

> ⓘ **ПРИМЕЧАНИЕ**
> Перед удалением ресурсов требуется удалить все учетные записи, которые были добавлены из удаляемых ресурсов.

Установка политики

1. В разделе **Ресурсы** отметьте один или несколько ресурсов и нажмите **Установить политику**.
2. Выберите новую политику для выбранных ресурсов и нажмите **Выбрать**.
3. В окне подтверждения нажмите **Установить**.

Установка подразделения

1. В разделе **Ресурсы** отметьте один или несколько ресурсов и нажмите **Установить подразделение**.
2. Выберите новое подразделение для выбранных ресурсов и нажмите **Ок**.
3. В окне подтверждения нажмите **Установить**.

Добавление тегов

> **ИНФОРМАЦИЯ**
>
> Если у вас еще нет тегов, создайте их в разделе Конфигурация.

1. В разделе **Ресурсы** отметьте один или несколько ресурсов и нажмите **Добавить теги**.
2. Выберите один или несколько тегов.
3. Нажмите **Вперед**.
4. Проверьте выбранные ресурсы и выбранные теги.
5. Нажмите **Добавить** для завершения операции.

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

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**.

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 **Получить с ресурса**.
4. Нажмите **Использовать значение отпечатка с ресурса**.
5. Нажмите **Вперед**.
6. Выберите нужную сервисную учетную запись.
7. 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 **Получить с ресурса**.
4. Нажмите **Использовать значение отпечатка с ресурса**.
5. 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 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.

А если не добавить?

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.

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.
   >
   > Нельзя создать вторую службу на том же ресурсе с тем же именем. Дубликаты не разрешены.

5. Если требуется, введите **Описание** службы.
   Введенное здесь описание будет отображаться только в PAM. Обратите внимание, что описание, отображаемое в свойствах службы на ресурсе, не поменяется.

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 в разделах **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 службы, которая уже существует на этом ресурсе.

Смена паролей служб

У служб нет собственных паролей, их пароли — это пароли связанных учетных записей.

Пароли учетных записей можно изменить вручную или 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.

Чтобы перезапуск службы на ресурсе произошел успешно, служба должна находиться в состоянии Выполняется (Running).

> ⓘ **ИНФОРМАЦИЯ**
> Если служба на ресурсе изначально находилась в состоянии, отличном от Выполняется (Running), служба не перезапустится. При этом создается событие с типом INFO *Перезапуск службы: Не требуется*. Такой сценарий считается успешным завершением перезапуска службы, поэтому 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 **Найти**.

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;
- не отвечает 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 получен, можно в событиях этой службы. Эта информация поможет понять, как исправить ошибку.

Для исправления ошибки понадобится подключиться к ресурсу. Исправить ошибку из консоли управления нельзя.

Удаление служб

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> Службу невозможно восстановить после удаления.
>
> Вы можете создать новую службу с таким же именем на том же ресурсе.

Удаление из списка служб

1. Откройте раздел **Службы**.
2. Выберите одну или несколько служб.
3. Нажмите **Удалить**.

Удаление из профиля службы

1. Откройте профиль службы.
2. Нажмите **Удалить**.

Удаленные службы перестают отображаться в разделе **Службы**, но их можно просмотреть с помощью расширенного поиска.

Группы ресурсов

Раздел предназначен для просмотра данных по группе ресурсов и быстрой выдачи разрешений.

Найти группу

Введите в поисковую строку название группы и нажмите  .

Нажмите **Расширенный поиск**, введите один или несколько запросов и нажмите **Найти**.

Добавить группу

Для начала работы требуется создать группу и добавить в нее ресурсы.

1. Нажмите **Добавить** в разделе **Группы Ресурсов**.
2. Введите **Имя группы ресурсов** и **Описание**.
3. Задайте опцию **Добавлять ресурсы вместе с учетной записью**:
    - Если опция включена, то при добавлении ресурсов в группу потребуется выбрать учетную запись для каждого ресурса отдельно.
      При выдаче разрешения на такую группу выбирать учетные записи не требуется.
    - Если опция выключена, то при добавлении ресурсов в группу выбирать учетные записи не требуется.
      При выдаче разрешения на такую группу потребуется выбрать одну учетную запись, которая будет использоваться для доступа ко всем ресурсам группы.
4. Сохраните изменения.
5. Откройте созданную группу ресурсов.
6. Нажмите **Добавить ресурсы** во вкладке **Ресурсы**.
7. Выберите один или несколько ресурсов и нажмите **Вперед**.
8. Проверьте данные и нажмите **Добавить**.

Профиль группы

Для каждой группы ресурсов отображаются:

- Ресурсы — список ресурсов в группе.
- Разрешения — список выданных группе разрешений.
- Сессии — список активных, завершенных и прерванных сессий.

- События — записи об операциях, связанных с группой.

Добавить разрешение

1. Нажмите **Добавить разрешение**.
2. Выберите пользователей или группу и нажмите **Вперед**.
3. Настройте **Ограничения времени** и нажмите **Вперед**.
4. Настройте **Параметры разрешения** и нажмите **Вперед**.
5. Введите **Описание** и нажмите **Вперед**.
6. Проверьте данные и нажмите **Создать**.

Разрешение создается на всю группу, поэтому пользователю станут доступны все ресурсы группы. При изменении состава группы ресурсов у пользователя в рамках разрешения также изменится состав доступных для подключения ресурсов.

Удалить группу

1. Откройте профиль группы ресурсов.
2. Нажмите **Удалить**.
3. Подтвердите действие нажатием **Удалить**.

Чтобы удалить несколько групп, в разделе **Группы ресурсов** выберите нужные группы и нажмите **Удалить**.

Учетные записи

Учетные записи — локальные и доменные учетные записи различных систем или служб каталогов, от которых Indeed PAM получил пароль. Пользователи от имени выбранной учетной записи могут подключаться к ресурсам и открывать SSH-, SQL- и Web/Desktop-сессии. Для запуска сессии нужно получить разрешение на подключение учетной записи к ресурсу.

Профиль учетной записи

Для каждой учетной записи отображаются:

- Разрешения — список выданных разрешений для учетной записи на подключение к ресурсу.
- Сессии — список активных, завершенных и прерванных сессий.
- События — записи об операциях, связанных с учетной записью.
- Группы безопасности — список групп безопасности, в которых состоит учетная запись.
  Для доменных учетных записей не отображаются встроенные (Built-in) группы безопасности.
- Службы — список приложений, которые могут запускаться автоматически при запуске операционной системы.
  Для локальных учетных записей вкладка отображается, если у связанного ресурса есть настроенное сервисное подключение для Windows.

Найти учетную запись

Введите в поисковую строку имя учетной записи и нажмите .

Нажмите **Расширенный поиск**, задайте один или несколько параметров и нажмите **Найти**.

Добавить учетную запись

Чтобы добавить учетную запись в PAM:

1. Перейдите в раздел **Учетные записи** и нажмите **Добавить**.
2. Выберите ресурс или домен, в котором будет размещена учетная запись, и нажмите **Вперед**.
3. Введите **Имя** учетной записи и **Описание**.
4. Нажмите **Вперед**

> ⓘ **ПРИМЕЧАНИЕ**
>
> При добавлении учетной записи для ресурса с типом подключения SSH можно настроить не только пароль, но и SSH-ключ.
> При добавлении учетных записей ОС Windows и СУБД необходимо задать пароль. Настройка SSH-ключа для данных типов недоступна.

5. Настройте пароль и выберите одну из опций:

   - **Сгенерировать случайный пароль** — пароль создается автоматически и синхронизируется с ресурсом или доменом.
   - **Задать пароль вручную** — пароль задается в ручном режиме.
     Введите пароль и подтвердите его.
     Если требуется, чтобы пароль учетной записи сменился не только в PAM, но и на ресурсе или домене, включите опцию **Изменить пароль на ресурсе** или **Изменить пароль в домене**.
   - **Не задавать** — учетная запись создается без пароля, его можно задать позже при редактировании.

6. Нажмите **Вперед**.

7. Настройте SSH-ключ и выберите одну из опций:

   - **Сгенерировать новый SSH-ключ** — ключ создается автоматически и синхронизируется с ресурсом или доменом. Выберите криптографический алгоритм для генерации ключа: **Ed25519** или **RSA**.

   - **Задать SSH-ключ вручную** — ключ задается в ручном режиме. Выберите файл SSH-ключа и введите его пароль. Поддерживаются ключи RSA в форматах OpenSSH и PEM, а также Ed25519 в формате OpenSSH.

Как сгенерировать SSH-ключ?

Чтобы создать SSH-ключ и записать его в файл, воспользуйтесь программой PuTTYgen или одной из команд:

Ключ RSA в формате OpenSSH

```
ssh-keygen -t rsa -b 4096 -f id_rsa_openssh -C "RSA OpenSSH key"
```

Ключ RSA в формате PEM

```
ssh-keygen -t rsa -b 4096 -f id_rsa_pem -C "RSA PEM key" -m PEM
```

Ключ Ed25519 в формате OpenSSH

```
ssh-keygen -t ed25519 -f id_ed25519_openssh -C "Ed25519 OpenSSH key"
```

Чтобы SSH-ключ учетной записи сменился не только в PAM, но и на ресурсе или домене, включите опцию **Изменить SSH-ключ на ресурсе** или **Изменить SSH-ключ в домене**.

- **Не задавать** — учетная запись создается без SSH-ключа, его можно установить позже при редактировании.

8. Нажмите **Вперед**.

9. Проверьте данные и нажмите **Сохранить**

Сделать управляемой

Учетные записи, добавленные в PAM после синхронизации с ресурсом, находятся в состоянии *Ожидает решения*.
PAM знает о существовании такой записи, но не управляет ей. Такие записи могут использоваться вне системы и обходить контроль доступа

Чтобы подтвердить учетную запись, нажмите **Сделать управляемой** в профиле учетной записи. Задайте пароль и/или SSH-ключ.

Чтобы подтвердить несколько учетных записей:

1. Перейдите в раздел **Учетные записи**
2. Выберите одну или несколько учетных записей.
3. Нажмите **Сделать управляемой**.
4. Выберите политику сессий и завершите подтверждение.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> При массовом подтверждении всегда генерируются случайные пароли для учетных записей, генерация SSH-ключей не выполняется.

Добавить разрешение

1. Откройте профиль учетной записи.
2. Нажмите **Добавить разрешение**.
3. Выберите пользователей или задайте группу пользователей.
4. Выберите параметр разрешения:
   - **Ресурсы** — разрешение выдается на один или несколько выбранных ресурсов.
   - **Группы ресурсов** — разрешение выдается на выбранную группу ресурсов.
   - **Произвольные подключения** — разрешение выдается на любые ресурсы с выбранным типом подключения, в том числе на ресурсы, незарегистрированные в PAM.
5. Настройте **Ограничения времени** и нажмите **Вперед**.
6. Настройте **Параметры разрешения** и нажмите **Вперед**.
7. Введите **Описание** и нажмите **Вперед**.
8. Проверьте данные и нажмите **Создать**.

Восстановить пароль или SSH-ключ

Функция позволяет вернуть сохраненное состояние пароля или SSH-ключа для учетной записи.

Чтобы выбрать точку восстановления:

1. Откройте профиль учетной записи.
2. Нажмите **Откатить** в профиле учетной записи.
3. Выберите точку восстановления, укажите причину и завершите восстановление пароля.

Проверить пароль или SSH-ключ

Чтобы проверить соответствие пароля, SSH-ключа и наличие неуправляемых SSH-ключей, в профиле учетной записи нажмите **Проверить**.

> ⓘ **ПРИМЕЧАНИЕ**
> Проверка паролей доменных или локальных учетных записей ресурсов под управлением ОС Linux может выполняться без настройки сервисного подключения к ресурсу или домену.

Чтобы проверить соответствие пароля или SSH-ключа для нескольких учетных записей, в разделе **Учетные записи** выберите нужные записи и нажмите **Проверить**.

Сменить или установить пароль

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> При смене пароля учетной записи обратите внимание, связаны ли с этой учетной записью службы. При смене пароля учетной записи пароли связанных служб тоже поменяются.

Вручную

Чтобы изменить или сбросить пароль вручную:

1. Нажмите **Сменить пароль** в профиле учетной записи.
2. Выберите одну из опций:
   - **Сгенерировать случайный пароль** — пароль создается автоматически и синхронизируется с ресурсом или доменом.
   - **Задать пароль вручную** — пароль задается в ручном режиме.
     Введите пароль и подтвердите его.
     Если требуется, чтобы пароль учетной записи сменился не только в PAM, но и на ресурсе или домене, включите опцию **Изменить пароль на ресурсе** или **Изменить пароль в домене**.
   - **Не задавать** — учетная запись создается без пароля, его можно задать позже при редактировании.
3. Введите причину смены пароля.
4. Нажмите **Сохранить**.

По расписанию

Смена паролей учетных записей по расписанию настраивается через политики.

1. Перейдите в раздел **Политики**.
2. Выберите политику, которая управляет нужной вам учетной записью.
3. Откройте раздел **Учетные записи**.
4. Включите опцию **Периодически ротировать пароль и SSH-ключ учетной записи**.
5. Задайте количество дней в поле **Период ротации пароля и SSH-ключа**.
   Автоматическое изменение пароля или SSH-ключа будет выполняться один раз в указанное количество дней.

Сменить или установить SSH-ключ

Чтобы сбросить, загрузить или сгенерировать SSH-ключ:

1. Нажмите **Сменить SSH-ключ** или **Установить SSH-ключ** в профиле учетной записи.

2. Выберите одну из опций:

   - **Сгенерировать новый SSH-ключ** — ключ создается автоматически и синхронизируется с ресурсом или доменом. Выберите криптографический алгоритм для генерации ключа: **Ed25519** или **RSA**.

   - **Задать SSH-ключ вручную** — ключ задается в ручном режиме. Выберите файл SSH-ключа и введите его пароль. Поддерживаются ключи RSA в форматах OpenSSH и PEM, а также Ed25519 в формате OpenSSH.

Как сгенерировать SSH-ключ?

Чтобы создать SSH-ключ и записать его в файл, воспользуйтесь программой PuTTYgen или одной из команд:

Ключ RSA в формате OpenSSH

```
ssh-keygen -t rsa -b 4096 -f id_rsa_openssh -C "RSA OpenSSH key"
```

Ключ RSA в формате PEM

```
ssh-keygen -t rsa -b 4096 -f id_rsa_pem -C "RSA PEM key" -m PEM
```

Ключ Ed25519 в формате OpenSSH

```
ssh-keygen -t ed25519 -f id_ed25519_openssh -C "Ed25519 OpenSSH key"
```

Чтобы SSH-ключ учетной записи сменился не только в PAM, но и на ресурсе или домене, включите опцию **Изменить SSH-ключ на ресурсе** или **Изменить SSH-ключ в домене**.

- **Не задавать** — учетная запись создается без SSH-ключа, его можно установить позже при редактировании.

3. Введите причину смены SSH-ключа.

4. Нажмите **Сохранить**.

Удалить неуправляемые SSH-ключи

Функция позволяет удалить неуправляемые SSH-ключи, при этом созданные или добавленные в PAM управляемые ключи останутся без изменений. Если в профиле учетной записи отображается ошибка **Обнаружены неуправляемые SSH-ключи**, нажмите **Удалить неуправляемые ключи**.

Синхронизировать

Синхронизация обновляет список групп безопасности, в которых состоит учетная запись. Функция доступна только при настроенном сервисном подключении к ресурсу или домену. При синхронизации не меняется пароль, SSH-ключ, описание или логин учетной записи.

Чтобы обновить данные о группах безопасности, в профиле учетной записи нажмите **Синхронизировать**. Если пользователя на ресурсе добавили или удалили из группы, PAM обновит данные во вкладке **Группы безопасности**.

Заблокировать

Блокировка учетной записи приостанавливает действие всех разрешений, в которых она используется.
Заблокированная учетная запись отмечена символом . Разрешения для этой учетной записи отмечены символом .

Чтобы заблокировать учетную запись:

1. Зайдите в раздел **Учетные записи**.
2. Откройте профиль учетной записи.
3. Нажмите **Заблокировать**.
4. В окне подтверждения операции нажмите **Заблокировать**.

Чтобы заблокировать несколько учетных записей, в разделе **Учетные записи** выберите нужные записи и нажмите **Заблокировать**.

Игнорировать

Игнорируемая учетная запись не участвует в операциях и синхронизации. PAM знает о существовании учетной записи, но не хранит и не управляет ее данными. Игнорируемые учетные записи отмечены символом .

Для таких учетных записей нельзя настроить новое разрешение, а существующие разрешения находятся в состоянии *Неактивно*.

Чтобы перевести учетную запись в состояние *Игнорируется*:

1. Зайдите в раздел **Учетные записи**.
2. Откройте профиль учетной записи.
3. Нажмите **Игнорировать**.
4. В окне подтверждения операции нажмите **Игнорировать**.

Чтобы игнорировать несколько учетных записей, в разделе **Учетные записи** выберите нужные записи и нажмите **Игнорировать**.

Удалить учетную запись

> ⓘ **ИНФОРМАЦИЯ**
> Удаленная учетная запись пропадет из всех связанных с ней служб: в карточке службы в поле **Учетная запись** будет стоять прочерк. Сами службы не удалятся.

Чтобы удалить учетную запись:

1. Зайдите в раздел **Учетные записи**.
2. Откройте профиль учетной записи.
3. Нажмите **Удалить**.
4. В окне подтверждения операции нажмите **Удалить**.

Чтобы удалить несколько учетных записей, в разделе **Учетные записи** выберите нужные записи и нажмите **Удалить**.

Восстановить учетную запись

> ⓘ **ИНФОРМАЦИЯ**
> При восстановлении учетной записи ранее существовавшие связи между учетной записью и службами не восстанавливаются.

Чтобы восстановить учетную запись:

1. Нажмите **Расширенный поиск** в разделе **Учетные записи**.
2. Введите **Имя** учетной записи.
3. Выберите для поля **Состояние** значение **Удалена** и нажмите **Найти**.
4. Откройте профиль учетной записи и нажмите **Восстановить**.
5. Выберите точку восстановления пароля учетной записи.
6. Введите причину восстановления и нажмите **Восстановить**.

Выбрать политику

1. Откройте профиль ресурса.
2. Нажмите напротив параметра **Политика**.
3. Выберите политику и нажмите **Выбрать**.

Добавить службу

1. Откройте профиль учетной записи и перейдите на вкладку **Службы**.
2. Выберите ресурс и нажмите **Вперед**.
3. Заполните поля **Имя** и **Описание**.
4. Задайте опцию **Перезапускать службу при смене пароля службы** и нажмите **Вперед**.
5. Проверьте данные и нажмите **Добавить**.

Домены

Раздел предназначен для работы с доменами службы каталогов.

Найти домен

Введите в поисковую строку имя домена или DNS-имя и нажмите  .

Нажмите **Расширенный поиск,** введите один или несколько запросов и нажмите **Найти**.

Добавить домен

Для управления доменными учетными записями и получения доменных компьютеров требуется добавить домен в Indeed PAM.

Чтобы добавить домен:

1. Перейдите в раздел **Домены**.
2. Нажмите **Добавить**.
3. Заполните поля **Имя домена** и **DNS-имя**.
4. Выберите службу каталогов.
5. Укажите порт.
6. Включите опцию **Использовать LDAPS**, если требуется подключение по протоколу LDAPS.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> Смена пароля возможна только при использовании LDAPS.

7. Нажмите **Сохранить**.

Профиль домена

Для каждого домена отображаются:

- Доменные учетные записи — список доменных учетных записей.
- Контейнеры для ресурсов — список контейнеров для синхронизации доменных компьютеров.

- Привилегированные группы — список групп безопасности для синхронизации доменных учетных записей.
- События — записи об операциях, связанных с ресурсами в домене.

Настроить сервисное подключения для доменов

Доменную учетную запись можно назначить сервисной учетной записью для выполнения следующих операций:

- 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 учетных записей может выполняться без настройки сервисного подключения к домену.

Чтобы настроить сервисное подключение:

1. Откройте профиль домена.
2. Нажмите ✎ напротив параметра **Сервисная учетная запись**.
3. Выберите учетную запись и нажмите **ОК**.

Добавить учетную запись

Добавьте в Indeed PAM доменные учетные записи ресурса, которые могут использоваться для предоставления доступа на ресурсы.

1. Откройте профиль домена.
2. Перейдите на вкладку **Доменные учетные записи** и нажмите **Добавить доменную учетную запись** .
3. Введите **Имя учетной записи** и **Описание**.
4. Нажмите **Вперед**.
5. Выберите одну из опций:

- **Сгенерировать случайный пароль** — пароль будет создан автоматически и синхронизирован с ресурсом или доменом.
- **Задать пароль вручную** — пароль будет задан в ручном режиме.
  Введите пароль и подтвердите его.
  Если требуется, чтобы пароль учетной записи сменился не только в PAM, но и в домене, включите опцию **Изменить пароль в домене**.
- **Не задавать** — учетная запись будет создана без пароля, его можно задать позже при редактировании.

6. Нажмите **Вперед**.
7. Проверьте данные и нажмите **Сохранить**.

Проверить соединение с доменом

Нажмите **Проверить соединение** в профиле домена, чтобы проверить:

- сетевую доступность домена;
- корректность DNS-имени и IP-адреса;
- корректность имени и пароля сервисной учетной записи.

Чтобы проверить соединение нескольких доменов, перейдите в раздел **Домены**, выберите нужные домены и нажмите **Проверить соединение**.

Добавить контейнер для ресурсов

1. Перейдите в профиль домена.
2. Перейдите на вкладку **Контейнеры для ресурсов** и нажмите **Добавить контейнер для ресурсов**.
3. Введите имя контейнера и нажмите .
4. Выберите один или несколько контейнеров и нажмите **ОК**.

Добавить группу безопасности

1. Откройте профиль домена.
2. Перейдите на вкладку **Привилегированные группы** и нажмите **Добавить привилегированную группу**.
3. Введите имя группы и выберите одну или несколько групп.
4. Завершите выбор групп.

Синхронизировать

Нажмите **Синхронизировать учетные записи** в профиле домена, чтобы обновить или добавить в Indeed PAM доменные учетные записи, которые состоят в добавленных привилегированных группах.

Импортировать ресурсы

Нажмите **Импортировать ресурсы** в профиле домена, чтобы автоматически добавить в Indeed PAM доменные компьютеры.

Выбрать политику

1. Откройте профиль домена.
2. Нажмите напротив параметра **Политика**.
3. Выберите политику из списка и нажмите **Выбрать**.

Чтобы задать политику для нескольких доменов, перейдите в раздел **Домены**, выберите нужные домены и нажмите **Установить политику**.

Удалить домен

1. Откройте профиль домена.
2. Нажмите **Удалить**.
3. Подтвердите действие.

Чтобы удалить несколько доменов, в разделе **Домены** выберите нужные домены и нажмите **Удалить**.

> ⓘ **ПРИМЕЧАНИЕ**
> Перед удалением домена требуется удалить все учетные записи, которые были добавлены из удаляемого домена.

Восстановить домен

1. Перейдите в раздел **Домены**.
2. Нажмите **Расширенный поиск** в разделе **Домены**.
3. Заполните поля **IP-адрес** и **DNS-имя**.

4. Выберите для поля **Состояние** значение **Удален** и нажмите **Найти**.
5. Откройте профиль ресурса и нажмите **Восстановить**.
6. Введите причину восстановления и нажмите **Восстановить**.

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 службы каталогов.

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

> ⓘ **НЕОБХОДИМЫ ПРИВИЛЕГИИ**
>
> Для работы с разрешениями необходимы привилегии **Управления разрешениями** (Permission.Create, Permission.Read, Permission.Revoke, Permission.Suspend).

Разрешения позволяют пользователям подключаться к ресурсам.

Найти разрешение

Введите в поисковую строку имя пользователя, учетную запись, ресурс или описание и нажмите  .

Нажмите **Расширенный поиск,** введите один или несколько запросов и нажмите **Найти**.

Создать разрешение

1. Перейдите в раздел **Разрешения**.
2. Нажмите **Создать**.
3. Выберите пользователей или группу пользователей.
4. Выберите параметр разрешения:
    - **Ресурсы** — разрешение выдается на один или несколько выбранных ресурсов.
    - **Группы ресурсов** — разрешение выдается на выбранную группу ресурсов.
    - **Произвольные ресурсы** — разрешение выдается на любые ресурсы с выбранным типом подключения, в том числе на ресурсы, не зарегистрированные в PAM. Требуется отдельная лицензия.

      > ⚠ **ПРЕДУПРЕЖДЕНИЕ**
      >
      > Для выдачи разрешения на ресурсы PostgreSQL и MSSQL или на группы, содержащие такие ресурсы, требуется отдельная лицензия. Перед созданием разрешения добавьте в PAM учетную запись из PostgreSQL Server. При создании разрешения укажите именно эту учетную запись.
      >
      > Для произвольных ресурсов учетная запись одна на все типы подключений. Выбор локальной учетной записи недоступен.

5. Выберите учетную запись:

    - **Выбрать УЗ в PAM** — учетная запись, от имени которой пользователь открывает сессию на ресурсе.
    - **Пользовательская УЗ** — в разрешении не указывается учетная запись.
      Пользователь вводит логин и пароль учетной записи на ресурсе. В RDP- и SSH-сессиях можно войти с текущими учетными данными пользователя Indeed PAM.

6. Настройте **Ограничения времени** и нажмите **Вперед**.

7. Настройте **Параметры разрешения** и нажмите **Вперед**.

8. Заполните поле **Описание** и нажмите **Вперед**.

9. Проверьте данные и нажмите **Создать**.

Ограничения времени

Задайте расписание доступа, согласно которому пользователи могут открывать сессии, смотреть и изменять учетные данные. Например, можно выдать разрешение на работу только по будним дням с 8:00 до 17:00.

Настройте параметры:

- **Период действия** — период времени, в течение которого действует разрешение. Например, можно выдать разрешение на один день или месяц.

    - **Начало** — задайте дату и время, когда разрешение станет активно.
      Если задать только **Начало**, разрешение начнет действовать в выбранную дату, а его период действия будет неограничен.

    - **Окончание** — задайте дату и время, когда разрешение станет неактивно.
      Если задать только **Окончание**, разрешение станет активным в момент создания, но приостановится в указанную дату.

      > ⓘ **ИНФОРМАЦИЯ**
      > Если параметры **Начало** и **Окончание** не заданы, то разрешение будет действовать бессрочно.

- **Расписание доступа** — ограничения по дням недели с учетом заданного расписания.

    - **Разрешить доступ только в выбранные дни** — выберите дни недели, когда разрешение будет активно.

- **Разрешить доступ только в выбранное время** — выберите время, когда разрешение будет активно.

> ⓘ **ИНФОРМАЦИЯ**
> Доступ по дням недели предоставляется по часовому поясу сервера управления.

По истечении периода действия разрешение перейдет в состояние *Ограничено/Неактивно*, а пользовательская сессия будет прервана.

Параметры разрешения

Задайте параметры доступа:

- **Учетные данные** — определяет действия с учетными данными.
  - **Разрешить просмотр учетных данных** — разрешает пользователю просматривать пароль привилегированных учетных записей, которые используются в разрешении.
  - **Разрешить изменение учетных данных** — разрешает пользователю менять пароль привилегированных учетных записей, которые используются в разрешении.
- **Источник подключения** — позволяет задать конкретную сеть, с которой разрешено устанавливать соединение.
  Выберите сеть в поле **Сетевое расположение источников для разрешенных подключений**.

> ⓘ **ПРИМЕЧАНИЕ**
> Если сетевые расположения не добавлены в PAM, будет задано *Без ограничений*. Это значит, что использовать данное разрешение можно с любого устройства в сети.

- **Повышение привилегий в SSH-сессиях** — определяет доступ к PamSu:
  - Управляется политиками — доступ определяется политикой ресурса, на который выдается разрешение.
  - Разрешено — право использовать `pamsu` независимо от настроек политики.
  - Запрещено — запрет на использование `pamsu` независимо от настроек политики.

Копировать разрешение

Можно создать копию любого разрешения, при этом исходное разрешение может быть отозвано или приостановлено. При копировании открывается окно создания, в котором заданы параметры исходного разрешения. Этот выбор можно отредактировать: изменить ресурс, убрать пользователей или задать ограничения.

> ⓘ **ИНФОРМАЦИЯ**
> Копирование доступно только из профиля разрешения.
>
> Если пользователь, ресурс или учетная запись в исходном разрешении удалены или заблокированы, то они не будут заданы.

Чтобы копировать разрешение:

1. Перейдите в раздел **Разрешения**.
2. Откройте профиль нужного разрешения.
3. Нажмите **Создать копию**.
4. Внесите изменения или оставьте исходный выбор.
5. Нажмите **Создать**.
6. Выберите действие с исходным разрешением:
   - Оставить исходное разрешение;
   - Приостановить исходное разрешение;
   - Отозвать исходное разрешение.
7. Нажмите **Завершить**.

Отозвать

Нажмите **Отозвать** и аннулируйте разрешение, которое больше не требуется. Доступ у пользователей пропадает сразу, а не после завершения сессии.

Чтобы аннулировать несколько разрешений, в разделе **Разрешения** выберите нужные разрешения и нажмите **Отозвать**.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> Отозванные разрешения нельзя восстановить.
>
> Если вам требуется временно запретить использовать разрешение, то приостановите его действие.

Отозванные разрешения перестают отображаться в разделе **Разрешения**, но их можно найти с помощью поиска:

1. Перейдите в раздел **Разрешения**.
2. Откройте **Расширенный поиск**.
3. Выберите состояние *Отозвано* и нажмите **Найти**.

Приостановить

Нажмите **Приостановить** в профиле разрешения, чтобы временно запретить использовать разрешение. Доступ у пользователей пропадает сразу, а не после завершения сессии.

Чтобы приостановить несколько разрешений, в разделе **Разрешения** выберите нужные разрешения и нажмите **Приостановить**.

Возобновить

Нажмите **Возобновить** в профиле разрешения, чтобы активировать приостановленное разрешение. Разрешение перейдет в состояние **Действительно**.

Чтобы активировать несколько разрешений, в разделе **Разрешения** выберите нужные разрешения и нажмите **Возобновить**.

Сформировать отчет

Отчет — выгрузка разрешений по заданным фильтрам. Например, можно сформировать отчет по отозванным разрешениям или выгрузить список всех разрешений определенного пользователя. По умолчанию в отчет попадают до 50 000 записей, но данный лимит можно увеличить.

Чтобы сформировать отчет:

1. Перейдите в раздел **Разрешения**.
2. (Опционально) Введите запрос в поисковой строке или примените фильтры расширенного поиска.
3. Нажмите **Сформировать отчет**.
4. В появившемся окне выберите формат CSV или XLSX.

Отчет формируется в фоновом режиме. Скачайте готовый отчет в разделе **История отчетов**.

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.

Чтобы подтвердить запрос, нажмите **Подтвердить** в профиле запроса.

Чтобы подтвердить несколько запросов, отметьте их в списке и нажмите **Подтвердить**.

Отклонение запроса

Функция позволяет Администратору PAM отклонить запрос Пользователя.

Чтобы отклонить запрос, нажмите **Отклонить** в профиле запроса.

Чтобы отклонить несколько запросов, отметьте их в списке и нажмите **Отклонить**.

Профиль запроса

Профиль запроса отображает следующие данные:

- **Пользователь** — пользователь, создавший запрос на открытие сессии.
- **Учетная запись** — учетная запись, которая используется для открытия RDP, SSH или WEB-сессии на ресурсах.
- **Подразделение** — имя подразделения, в котором состоит ресурс.
- **Ресурс** — ресурс, на котором была открыта RDP, SSH или WEB-сессия от имени учетной записи.

- **IP-адрес пользователя** — IP-адрес, с которого пользователь подключался к PAM Gateway, SSH Proxy или RDP Proxy.
- **Тип подключения** — тип пользовательского подключения к ресурсу.
- **Причина подключения** — текст, введенный пользователем при подключении к ресурсу.
- **Состояние** — текущее состояние запроса. Существуют следующие состояния: Ожидает решения, Подтвержден, Отклонен, Истек, Отменен пользователем, Использован, Не использован.
- **Время создания** — дата и время создания запроса пользователем.
- **Время подтверждения** — дата и время подтверждения сессии администратором.
- **Подтвердил** — учетная запись администратора Indeed PAM, который подтвердил открытие сессии.
- **Сессия** — ID сессии с указанием текущего статуса этой сессии.

Активные сессии

Раздел предназначен для автоматической фильтрации и отображения активных сессий Indeed PAM.

При наличии активных сессий на главном сайдбаре справа от заголовка раздела отображается бейдж с количеством активных сессий.

Для каждой сессии отображаются следующие данные:

- **Иконка состояния** — текущее состояние сессии. При наведении курсора на иконку состояния всплывает подсказка с названием состояния.
- **Пользователь** — пользователь, 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 или DNS ресурса.
- **Причина подключения** — текст, введенный пользователем при подключении к ресурсу.
- **Длительность** — длительность сессии в часах, минутах и секундах.
- **Подключение** — тип пользовательского подключения к ресурсу.
- **Подключение к PAM** — дата и время открытия сессии.

Все сессии

Раздел предназначен для поиска и просмотра активных, завершенных и прерванных сессий. По умолчанию на странице отображается 15 сессий. При превышении этого числа внизу страницы появится переключатель.

Отображаемое количество сессий на странице можно изменить в конфигурационном файле по пути:

- Windows: *C:\inetpub\wwwroot\mc\assets\config\config.prod.json*
- Linux: */etc/indeed/indeed-pam/mc/config.prod.json*

Найти сессию

Введите в поисковую строку имя пользователя, ресурс, учетную запись, тип подключения или причину и нажмите .

Нажмите **Расширенный поиск,** введите один или несколько запросов и нажмите **Найти**.

Сформировать отчет

Отчет — выгрузка сессий по заданным фильтрам. Например, можно выгрузить сессии пользователя на ресурсе за указанный период времени. По умолчанию в отчет попадают до 50 000 записей, но данный лимит можно увеличить.

Чтобы сформировать отчет:

1. Перейдите в раздел **Все сессии**.
2. (Опционально) Введите запрос в поисковой строке или примените фильтры расширенного поиска.
3. Нажмите **Сформировать отчет**.
4. В появившемся окне выберите формат CSV или XLSX.

Отчет формируется в фоновом режиме. Скачайте готовый отчет в разделе **История отчетов**.

Прервать сессию

Чтобы принудительно прервать сессию, перейдите в профиль активной сессии и нажмите **Прервать**.

Обновить сессию

Чтобы обновить текстовый лог, снимки экрана и переданные на сервер файлы, перейдите в профиль активной сессии и нажмите **Обновить**.

Просмотреть и скачать логи сессии

Для сессий, открытых через PAM, доступны виды логирования:

- Видео — для RDP- и SSH-сессий, открытых через Indeed PAM Gateway, и для сессий клиентских приложений.
- Текстовый лог — для RDP- и SSH-сессий, открытых через Indeed PAM Gateway и Indeed PAM SSH Proxy.

  > ⓘ **ИНФОРМАЦИЯ**
  > 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 требует установки отдельных компонентов. В SSH-сессиях регистрируется полный ввод/вывод.

- Снимки экрана — для RDP- и SSH-сессий, открытых через Indeed PAM Gateway, и для сессий клиентских приложений.
- Переданные на сервер файлы — для RDP-сессий. Перехватываются и копируются файлы, которые передаются с перенаправленных дисков на ресурс.

Чтобы скачать логи сессии, разверните секцию **Видео**, **Текстовый лог** или **Снимки экрана** и нажмите **Скачать** / **Скачать все**.

Чтобы скачать переданные файлы, разверните секцию **Переданные на сервер файлы** и перейдите по ссылке для скачивания файлов.

События

В разделе отображается история событий, которые произошли в Indeed PAM.

> ⓘ **ПРИМЕЧАНИЕ**
>
> Все события Indeed PAM перечислены в справочнике.

Найти событие

Введите в поисковую строку код события, компонент, имя инициатора или пользователя и нажмите  .

Нажмите **Расширенный поиск,** введите один или несколько запросов и нажмите **Найти**.

Сформировать отчет

Отчет — выгрузка событий по заданным фильтрам. Например, можно выгрузить события, которые произошли на ресурсе за выбранный период времени. По умолчанию в отчет попадают до 50 000 записей, но данный лимит можно увеличить.

Чтобы сформировать отчет:

1. Перейдите в раздел **События**.
2. (Опционально) Введите запрос в поисковой строке или примените фильтры расширенного поиска.
3. Нажмите **Сформировать отчет**.
4. В появившемся окне выберите формат CSV, XLSX или PDF.

Отчет формируется в фоновом режиме. Скачайте готовый отчет в разделе **История отчетов**.

История отчетов

> **НЕОБХОДИМЫ ПРИВИЛЕГИИ**
>
> Для работы в разделе администратору нужны привилегии *Просмотр и поиск разрешений*, *Просмотр и поиск сессий* или *Просмотр и поиск событий в журнале*.

Раздел содержит отчеты по разрешениям, сессиям и событиям. Для каждого отчета отображается статус:

- — сформирован и готов к скачиванию.
- — формируется.
- — не сформирован, возникла ошибка.
  Увеличьте время ожидания ответа от сервера или сформируйте отчет меньшего размера.
- — сформирован и готов к скачиванию, но выгружены не все записи.
  По умолчанию выгружается 50 000 записей. Лимит можно увеличить в конфигурационном файле.

Сформировать и скачать отчет

1. В консоли администратора перейдите в раздел **Разрешения**, **Все сессии** или **События**.
2. (Опционально) Введите запрос в поисковой строке или примените фильтры расширенного поиска.
3. Нажмите **Сформировать отчет**.
4. В появившемся окне выберите формат отчета.
   Отчет с заданными фильтрами формируется в фоновом режиме.
5. Перейдите в раздел **История отчетов** и напротив готового отчета нажмите **Скачать**.

Настройка конфигурации

В конфигурационном файле можно изменить:

- количество записей, выгружаемых в отчет;
- время ожидания ответа от сервера, если при формировании отчета возникает ошибка.

> **ПРИМЕЧАНИЕ**
>
> По умолчанию в каждый отчет выгружается 50 000 записей.
> Максимальный размер отчета: 1 000 000 записей.

Windows

Чтобы изменить лимит выгрузки или время ожидания ответа от сервера:

1. Откройте конфигурационный файл компонента Core по пути *C:\inetpub\wwwroot\idp\appsettings.json*
2. В секции `MaxTotalRecords` укажите количество записей для каждого вида отчета:
   - `Events` — отчет по событиям;
   - `Permissions` — отчет по разрешениям;
   - `Sessions` — отчет по сессиям.
3. Для параметра `CommandTimeout` укажите время ожидания ответа от сервера. Измените параметр только в том случае, если при формировании отчета возникает ошибка.

   Пример конфигурационного файла

   ```
   "Performance": {
     "SessionArtifactsRotation": {
       "MaxDegreeOfParallelism": 4
     },
     "Reports": {
       "CommandTimeout": "00:00:30",  // Время ожидания ответа от сервера
       "MaxTotalRecords": {
         "Events": 50000,             // Количество записей в отчете по событиям
         "Permissions": 50000,        // Количество записей в отчете по разрешениям
         "Sessions": 50000            // Количество записей в отчете по сессиям
       }
     }
   ```

4. Сохраните файл.

После редактирования конфигурационного файла перезапустите сервер IIS:

1. Запустите PowerShell от имени администратора.
2. Запустите IIS Manager:

   ```
   start inetmgr
   ```

3. На левой панели нажмите на нужный сервер.

4. На правой панели нажмите **Перезапустить** (Restart).

Linux

Чтобы изменить лимит выгрузки или время ожидания ответа от сервера:

1. Откройте конфигурационный файл компонента Core по пути */etc/indeed/indeed-pam/core/appsettings.json*

2. В секции `MaxTotalRecords` укажите количество записей для каждого вида отчета:

   - `Events` — отчет по событиям;
   - `Permissions` — отчет по разрешениям;
   - `Sessions` — отчет по сессиям.

3. Для параметра `CommandTimeout` укажите время ожидания ответа от сервера.
   Измените параметр только в том случае, если при формировании отчета возникает ошибка.

   Пример конфигурационного файла

```
"Performance": {
  "SessionArtifactsRotation": {
    "MaxDegreeOfParallelism": 4
  },
  "Reports": {
     "CommandTimeout": "00:00:30",  // Укажите время ожидания ответа от сервера
    "MaxTotalRecords": {
       "Events": 50000,             // Укажите количество записей в отчете по событиям
       "Permissions": 50000,        // Укажите количество в отчете по разрешениям
       "Sessions": 50000            // Укажите количество в отчете по сессиям
    }
  }
```

4. Сохраните файл.

5. Перейдите в папку со скриптами PAM и перезапустите компонент:

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

```
bash restart-pam.sh core
```

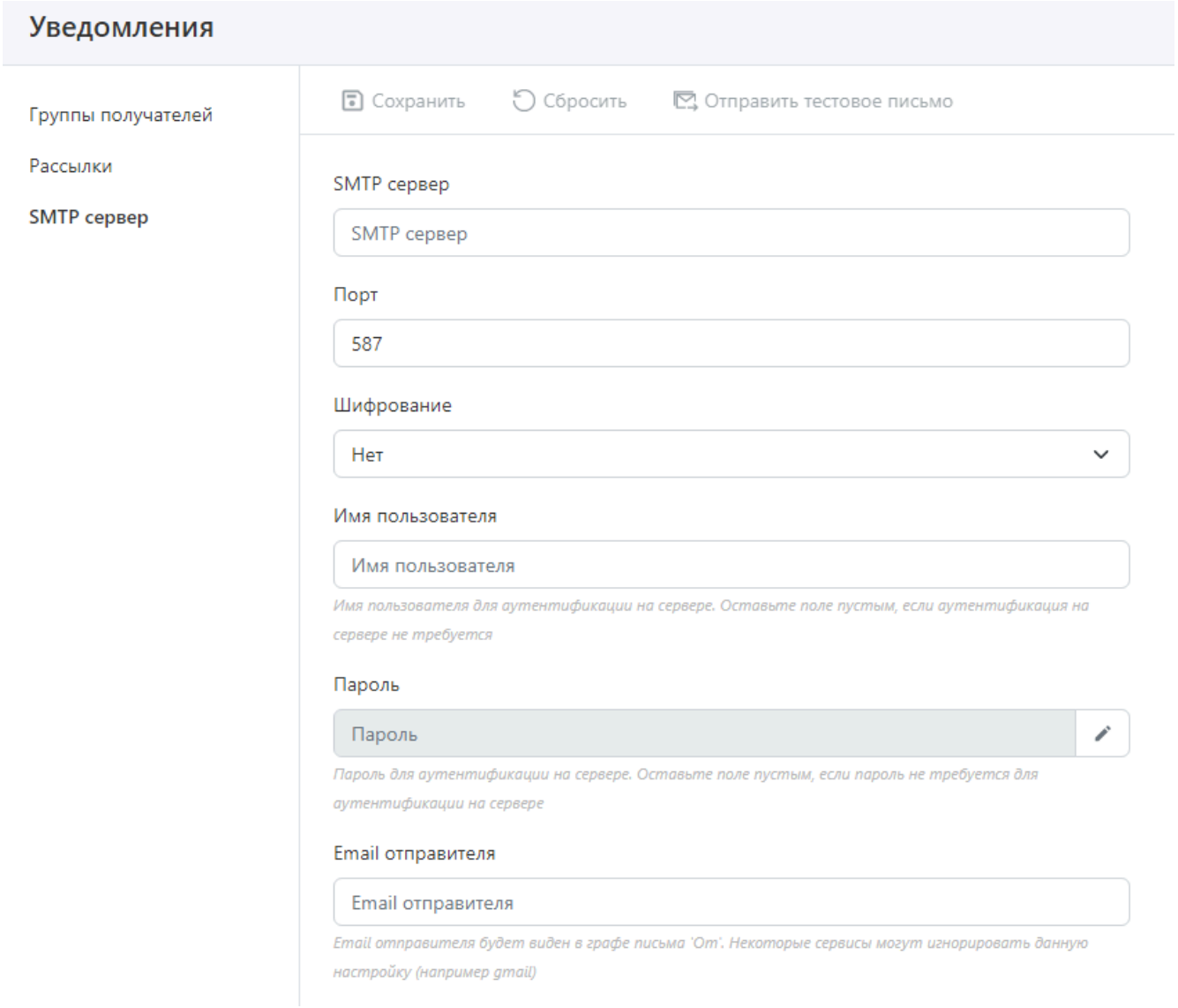
Уведомления

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.

Чтобы проверить настройки, нажмите **Отправить тестовое письмо**.



Настройка уведомлений

Чтобы настроить уведомления, выполните следующие действия:

1. Создайте группы получателей — списки адресов для рассылки уведомлений о регистрации выбранных событий в журнале.
    1. Откройте раздел **Группы получателей**, нажмите **Добавить**, введите имя и описание группы получателей, нажмите **Сохранить**.
    2. Перейдите в созданную группу получателей, нажмите **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

Чтобы удалить одну или несколько групп получателей или рассылок, перейдите в соответствующий раздел, отметьте один или несколько элементов и нажмите **Удалить**.

Конфигурация

Раздел предназначен для настройки Indeed PAM.

Системные настройки

В этом разделе указываются глобальные системные настройки. Точечная настройка выполняется в разделе **Политики**.

Задачи по расписанию

Настройка	Описание
Время старта проверки учетных записей	В это время начнется проверка паролей и SSH-ключей всех учетных записей в состоянии Управляемая.
Время старта синхронизации ресурсов и учетных записей	В это время начнется синхронизация данных о ресурсах и учетных записей на ресурсах и в доменах.
Время старта сброса паролей учетных записей	В это время начнется сброс всех паролей и SSH-ключей учетных записей.
Время старта проверки сервисного подключения	В это время начнется проверка сервисного подключения ресурсов и доменов.
Время старта ротации логов сессий	В это время начнется ротация логов сессий.
Интервал синхронизации пользовательских групп из каталога	Система PAM с заданным интервалом обновляет состав групп пользователей из каталога.

Видео

Настройка	Описание
Параметры кодека для записи видео	По умолчанию используется libx264 кодек: libx264 -preset medium -tune zerolatency
Параметры кодека потокового видео	По умолчанию используется libvpx кодек: libx264 -g 10 -tune zerolatency

Настройка	Описание
Длительность сегмента записываемого видео	По умолчанию 3600 секунд (1 час).

Сессии

Настройка	Описание
Таймаут соединения со шлюзом (сек.)	Время, после которого соединение будет закрыто, если шлюз не отвечает (сек.). Задайте нулевое значение, если не хотите, чтобы соединение прерывалось.
Время на подключение, мин.	Закрывать сессию на Gateway, если пользователь за указанное время не выполнил подключение к ресурсу.
Уведомление перед открытием сессии	Этот текст будет показан пользователю перед началом сессии. Оставьте пустым, если уведомление не требуется.
Максимальное число сессий на пользователя	Ограничение количества одновременных открытых сессий на одного пользователя, по умолчанию 0, без ограничений.
Уведомлять пользователя перед разрывом сессии, интервалы показа уведомлений	Перед разрывом сессии пользователю будут показаны предупреждения. Чтобы настроить время и интервал показа, заполните соответствующие поля.

Подключения к Gateway

Настройка	Описание
Адрес RDCB	IP-адрес или DNS 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	Эти параметры будут добавлены в настройки подключения RDP к PAM Gateway и заменят старые настройки.

RDP Proxy

В поле **Адрес RDP Proxy** введите IP-адрес или DNS-имя сервера с RDP Proxy. Укажите порт, иначе PAM использует порт по умолчанию.

Web Proxy

В поле **Адрес Web Proxy** введите IP-адрес или DNS-имя сервера с Web Proxy. Укажите порт, иначе PAM использует порт по умолчанию.

PostgreSQLProxy

В поле **Адрес PostgreSQL Proxy** введите IP-адрес или DNS-имя сервера с PostgreSQL Proxy. Укажите порт, иначе PAM использует порт по умолчанию.

MSSQL Proxy

В поле **Адрес MSSQL Proxy** введите IP-адрес или DNS-имя сервера с MSSQL Proxy. Укажите порт, иначе PAM использует порт по умолчанию.

Настройки SSH-подключений

Настройка	Описание
Адрес SSH Proxy	IP-адрес или DNS-имя сервера с SSH Proxy. Укажите порт, иначе будет использоваться порт по умолчанию. Порт по умолчанию: 2222
Аутентификация ресурсов по ключам SSH-сервера	Режим заполнения отпечатков ключей SSH-сервера. Подробную информацию можно прочитать в разделе режимы заполнения отпечатков.

Web-терминал

Активируйте Web-терминал с помощью опции **Включить Web-терминал**.
Web-терминал позволяет открывать SSH- и RDP-сессии в браузере без установки сторонних клиентов. Открыть сессию можно через консоль пользователя.

Syslog

Syslog-сервер используется для интеграции с SIEM-системой и выполняет роль единого хранилища для записей событий PAM и/или текстовых логов сессий. Данные обновляются в режиме реального

времени: в процессе активного удаленного подключения, а не после его завершения.

Чтобы отправлять текстовые логи сессий, заполните данные Syslog-сервера.
Отправка на Syslog-сервер записей журнала **События** настраивается через конфигурационные файлы.

Настройка	Описание
Syslog-сервер	IP-адрес или DNS-имя Syslog-сервера.
Порт	Порт Syslog-сервера.
Протокол	Сетевой протокол подключения к Syslog-серверу.
Формат	Формат событий, используемый Syslog-сервером.
Версия Syslog	IETF стандарт протокола Syslog.

После заполнения данных нажмите **Проверить подключение к Syslog-серверу**.
Убедитесь, что на Syslog-сервер пришло тестовое сообщение.

Аутентификация пользователей

В этом разделе указываются глобальные настройки аутентификации. Точечная настройка аутентификации выполняется в разделе **Политики**.

Блокировка пользователей

Если пользователь несколько раз подряд введет неверный пароль или OTP, его учетная запись будет заблокирована на указанное время.

Настройка	Описание
Число попыток	При превышении числа попыток пользователь временно блокируется. Значение 0 — блокировка не применяется.
Время блокировки	Определяет период времени, по истечении которого пользователь будет разблокирован и снова сможет вводить пароль или OTP.

Автоматический выход при бездействии

Параметр **Период бездействия в интерфейсе MC/UC** задает время, по истечении которого происходит автоматический выход из консолей пользователя и администратора. Настройка не влияет на пользовательские сессии к ресурсам.

Автоматический выход происходит, если пользователь:

- аутентифицирован в консоли пользователя и/или администратора через IDP;
- не совершал действий в любой вкладке браузера в течение заданного периода бездействия.

Задайте период бездействия от 0 до 480 минут, где 0 — отключение автоматического выхода. Фоновые операции браузера, такие как обновление данных или проверка состояния системы, не считаются действиями пользователя.

Аутентификация по SSH-ключам

Включите опцию **Разрешить пользователям подключаться к SSH Proxy с использованием SSH-ключей**, чтобы пользователи могли подключаться к SSH Proxy без паролей, с помощью добавленных в Indeed PAM SSH-ключей. Необходимость вводить OTP сохраняется.
Если опция отключена, то пользователи могут аутентифицироваться только с помощью пароля.

Открытие сессий без повторной аутентификации

Настройка позволяет отключить повторную аутентификацию при запуске RDP-, SSH- и SQL-сессий. В строку подключения или RDP-файл добавляется код, использующийся для аутентификации пользователя без запроса пароля и второго фактора. Код действует один раз и ограниченное время.

Для сессий, открытых через Web Proxy, код аутентификации используется всегда.

Как задать количество кодов аутентификации

Количество кодов задается в конфигурационном файле компонента Indeed PAM IdP по пути:

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

Задайте значение от 1 до 100 для параметра `MaxAuthCodesPerUser`:

```
"DirectoryMechanism": "Ldap",
"Authentication": "Local",
"UseDeveloperSigningCredential": false,
 "MaxAuthCodesPerUser": 100,
"QaToolClientSecret": "secret"
```

Настройка	Описание
Разрешить открытие сессий без повторной аутентификации	Если опция включена, в строку подключения или RDP-файл добавляется одноразовый код аутентификации.
Срок действия кода аутентификации	Определяет время действия кода аутентификации. Если запустить сессию с истекшим кодом, пользователю потребуется ввести пароль и второй фактор. Значение по умолчанию: 60 секунд. Минимальное значение: 5 секунд. Максимальное значение: 300 секунд.

Аутентификация по сертификатам X.509

Настройка **Аутентификация по сертификату** позволяет пользователям входить в консоль Indeed PAM с помощью клиентских сертификатов X.509, выданных доверенными удостоверяющими центрами.
О добавлении данного способа входа читайте в разделе **Сертификат X.509**.

Режимы аутентификации

- **Включена (опционально)** — пользователи могут входить в консоль по сертификату или по логину и паролю.
- **Обязательна для пользователей с указанным Subject сертификата** — пользователи с указанным `Subject` аутентифицируются только по сертификату. Остальные пользователи входят по логину и паролю.
- **Обязательна для всех пользователей** — вход в консоль возможен только по сертификату.

  > ⚠ **ПРЕДУПРЕЖДЕНИЕ**
  > При выборе режима **Обязательна для всех пользователей** убедитесь, что у пользователей верно заполнено поле **Subject (Субъект)**, иначе войти в консоль не получится.

- **Отключена** — аутентификация по сертификатам не используется.

Аутентификация через OIDC Identity Provider

Настройка позволяет включить аутентификацию через внешний Identity Provider по протоколу OpenID Connect.
О добавлении данного способа входа читайте в разделе **Протокол OpenID Connect**.

Настройка	Описание
Включить аутентификацию через внешний Identity Provider	Опция включает аутентификацию по протоколу OpenID Connect через внешний Identity Provider. Вход по логину и паролю остается доступен.
Название кнопки входа	Название кнопки аутентификации через Identity Provider. Кнопка отображается на странице входа в консоль Indeed PAM.
Redirect URI	Адрес, на который Identity Provider перенаправляет пользователя после аутентификации. Укажите DNS-имя сервера Indeed PAM. Пример: `pam.my-company.local`.
OIDC Provider URL	Адрес OIDC-сервера из настроек Identity Provider. Пример: `https://idp.company.ru`.

Настройка	Описание
Сценарий аутентификации	**Сценарии OIDC-аутентификации** • **Authorization Code Flow** — пользователь перенаправляется на сервер авторизации и получает код, который обменивается на токен доступа. • **Authorization Code Flow + PKCE (по умолчанию)** — рекомендуемый сценарий, в котором используется расширение Proof Key for Code Exchange (PKCE). Для каждого запроса авторизации генерируется дополнительный секрет, который проверяется при обмене кода на токен доступа. • **Implicit Flow** — сервер авторизации возвращает токен доступа в URL-адресе после аутентификации пользователя. Не рекомендуется использовать этот сценарий из-за риска перехвата токенов.
Client ID	Идентификатор клиента, созданный при регистрации PAM в Identity Provider
Client Secret	Секрет клиента, выданный при регистрации PAM в Identity Provider
Claim	Имя OIDC-атрибута, из которого PAM получает адрес электронной почты пользователя для сопоставления с учетной записью Identity Provider. Значение по умолчанию: `email`.
Scope	Имя OIDC-области, используемой в запросе к OIDC-провайдеру для получения значения `claim` с адресом электронной почты пользователя. Значение по умолчанию: `email`.

Требования к паролям внутренних пользователей

Настройка	Описание
Срок действия пароля	Минимальное значение: 0 — без ограничений. Значение по умолчанию: 45 дней. Максимальное значение: 999 дней.

Настройка	Описание
Минимальная длина пароля	Минимальное значение: 4 символа. Значение по умолчанию: 8 символов. Максимальное значение: 255 символов.
Строчные буквы	Если опция включена, то пароль должен содержать минимум одну латинскую строчную букву.
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 0–9.
Специальные символы	Если опция включена, то пароль должен содержать минимум один спецсимвол из списка: ~!@#$%^&*()_-+={}|[] \:;"'<>,.?/

Пользовательское подключение

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> Для работы с пользовательскими подключениями необходимы привилегии **Управление пользовательскими подключениями**: *UserConnectionType.Create*, *UserConnectionType.Read*, *UserConnectionType.Update*, *UserConnectionType.Delete*.

Пользовательское подключение — функциональная возможность ресурса, позволяющая открывать сессии по различным протоколам. С помощью пользовательского подключения можно удаленно совершать действия на ресурсе.

Ресурс может поддерживать один или несколько типов таких подключений, включая собственные типы пользовательских подключений.

Встроенные типы подключений Indeed PAM 3.4

- RDP
- SSH
- Telnet
- PostgreSQL
- MSSQL
- Web Proxy

Встроенные типы не могут быть изменены или удалены.

Добавление собственных типов пользовательских подключений

Добавьте собственный тип пользовательского подключения и открывайте сессии в браузере без использования сторонних приложений.

Web-приложение

1. Перейдите в раздел **Конфигурация** → **Пользовательское подключение**.
2. Нажмите **Добавить**
3. Введите название пользовательского подключения.
4. Задайте формат логина или оставьте значение по умолчанию.
5. Выберите тип приложения **Web-приложение** и нажмите **Вперед**.
6. Выберите способ открытия сессии:
   - **В браузере** — сессия откроется в новой вкладке браузера.
     Доступ реализован через сервер доступа Web.
   - **Через RDP** — сессия откроется через скачанный RDP-файл.
     Выберите браузер и задайте опцию **Запускать браузер в режиме киоска**. Доступ реализован через публикацию выбранного браузера на сервере доступа RDS.
7. Нажмите **Вперед**.
8. Задайте опцию **Автоматически заполнять формы входа учетными данными (SSO)**. Опция позволяет автоматически заполнить логин и пароль на целевом ресурсе с использованием данных привилегированной учетной записи. После включения опции загрузите SSO-шаблон в формате JSON для подключения через браузер, в формате XML — для RDP-файла.
9. Нажмите **Создать**.

Windows-приложение

> **ИНФОРМАЦИЯ**
> Перед добавлением нового подключения требуется исследовать клиентское приложение и разработать шаблон для Indeed ESSO Agent. При возникновении трудностей обратитесь в службу поддержки Indeed.

1. Перейдите в раздел **Конфигурация** → **Пользовательское подключение**.
2. Нажмите **Добавить**
3. Введите название пользовательского подключения.
4. Задайте формат логина или оставьте значение по умолчанию.
5. Выберите тип приложения **Windows-приложение** и нажмите **Вперед**.
6. В поле **Путь к исполняемому файлу** укажите путь к Windows-приложению.
7. Заполните поле **Аргументы командной строки** и нажмите **Вперед**.
8. Задайте опцию **Автоматически заполнять формы входа учетными данными (SSO)**. Опция позволяет автоматически заполнить логин и пароль на целевом ресурсе с использованием данных привилегированной учетной записи. После включения опции загрузите SSO-шаблон в формате XML.
9. Нажмите **Создать**.

Автоматическое заполнение учетных данных (SSO)

SSO (Single Sign-On) — метод, позволяющий пользователям аутентифицироваться на нескольких веб-ресурсах с одним набором учетных данных. Чтобы учетные данные заполнились автоматически, создайте SSO-шаблон — файл с данными формы входа.

Для пользовательского подключения со способом открытия сессии **В браузере** загрузите SSO-шаблон в формате JSON, для подключения **Через RDP** — в формате XML. Для настройки SSO-шаблона в формате XML обратитесь в техническую поддержку.

Пример SSO-шаблона находится в дистрибутиве PAM в папке *\indeed-pam-tools\sso-templates*

> **ПРЕДУПРЕЖДЕНИЕ**
> Учетные данные для аутентификации на веб-ресурсе должны совпадать с данными привилегированной учетной записи.

Структура SSO-шаблона в формате JSON

```
{
  "username-field": "input[id='login']",
  "password-field": "input[id='password']",
  "submit": "button[type='submit']",
  "cannot-submit": "div[class='v-messages__message']"
}
```

Чтобы автоматически аутентифицироваться на веб-ресурсе, измените значения CSS-селекторов:

- `username-field` — логин учетной записи, например: `"input[data-marker='login-form/login/input']"`
- `password-field` — пароль учетной записи, например: `"input[type='password']"`
- `submit` — кнопка входа, например: `"button[data-marker='login-form/login-button']"`
- `cannot-submit` — ошибка аутентификации, например: `"div[data-marker='login-form/error']"`

> **КАК УЗНАТЬ НАЗВАНИЕ CSS-СЕЛЕКТОРА**
> Откройте веб-ресурс в браузере и перейдите к форме аутентификации. Откройте **Инструменты разработчика** (DevTools) и перейдите на вкладку **Элементы** (Elements). Найдите нужный CSS-селектор и подставьте значение в SSO-шаблон.

Формат логина для SSH-подключений

Измените формат логина доменной или локальной учетной записи, если при подключении к ресурсу по протоколу SSH используется логин в формате UPN или DOMAIN\user.

Чтобы задать формат логина по умолчанию:

1. Перейдите в раздел **Конфигурация** → **Пользовательское подключение**.
2. В настройках подключения **SSH** нажмите **Редактировать**.
3. Укажите форматы логинов для локальной и доменной учетных записей.
   Используйте обязательную переменную `%username%` и дополнительные `%location%`, `%location-dns%`.

Примеры

Формат логина john.smith@pam.local

```
%username%@%location-dns%
```

Формат логина SPACE\john.smith

```
%location%\%username%
```

Формат логина john.smith

```
%username%
```

4. Нажмите **Сохранить**.

Сервисное подключение

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> Для работы с сервисными подключениями необходимы привилегии **Управление типами сервисных подключений**: *ServiceConnectionType.Create*, *ServiceConnectionType.Read*, *ServiceConnectionType.Update*, *ServiceConnectionType.Delete*.

Встроенные типы сервисных подключений Indeed PAM 3.4

- Windows
- SSH
- Microsoft SQL Server
- MySQL
- PostgreSQL
- Oracle Database
- Cisco IOS
- Inspur BMC

Встроенные типы нельзя изменить или удалить.

Вы можете добавить собственные типы 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. Если требуется, введите **Описание** сервисного подключения.
6. Нажмите **Добавить**, чтобы завершить добавление.

Подготовка файлов коннекторов

Чтобы подготовить ZIP-архив с файлом коннектора, используйте утилиту Connector Creation Tool.

Редактирование собственных типов сервисных подключений

Загрузить новый коннектор

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. Нажмите **Сохранить**, чтобы завершить редактирование.

Отредактировать название или описание

1. Откройте раздел **Конфигурация** → **Сервисное подключение**.

2. Нажмите **Редактировать** рядом с требуемым типом сервисного подключения.
3. Отредактируйте **Название** и/или **Описание**.
4. Нажмите **Сохранить**, чтобы завершить редактирование.

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.

> ⓘ **ПРИМЕЧАНИЕ**
>
> 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_3.4_RU\indeed-pam-tools\ssh-templates* приложены шаблоны для перечисленных ниже дистрибутивов *nix.

Шаблоны SSH-коннекторов в составе дистрибутива Indeed PAM

- 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_3.4_RU\indeed-pam-tools\ssh-templates*.

Для разработки другого шаблона обратитесь в службу технической поддержки.

Сетевые расположения

В разделе можно добавить сетевые расположения, чтобы разрешить подключение к ресурсам только с заданных сетевых адресов.

Чтобы добавить сетевое расположение:

1. Нажмите **Добавить**.
2. Введите **Имя**.
3. Добавьте **Сетевые адреса** ресурсов, которым требуется выдать ограниченное подключение.

Теги

В этом разделе отображаются все созданные теги. По умолчанию теги отсортированы по алфавиту в прямом порядке. Чтобы отсортировать их в обратном порядке, нажмите на заголовок таблицы, столбец **Теги**.

Чтобы создать тег:

1. Нажмите **Создать**.
2. Введите **Имя** тега. Оно может содержать от 2 до 50 символов и может состоять только из латиницы, кириллицы, цифр и спецсимволов. Имя тега должно быть уникально вне зависимости от регистра. Например, если у вас уже есть тег «Важно», то создать тег «важно» не удастся.
3. Выберите цвет.
4. Оставьте опцию **Отображать тег в консоли пользователя (UC)** включенной. Если выключить опцию, то тегом смогут пользоваться только администраторы PAM в MC.
5. Завершите добавление нажатием **Сохранить**.

Чтобы найти тег:

1. Введите имя тега в поисковой строке полностью или частично.
   В инсталляциях PAM на PostgreSQL поиск регистрозависимый. Например, если у вас есть тег «Важно», то он не отобразится при вводе в поисковой строке «важно» с маленькой буквы. В инсталляциях PAM на Microsoft SQL поиск регистронезависимый, то есть тег отобразится при вводе его названия и с прописной, и со строчной буквы.
2. Нажмите ENTER или  .

Чтобы отредактировать тег:

1. Выберите тег в списке.
2. Нажмите **Редактировать**.
3. Внесите изменения. Есть возможность изменить имя тега, цвет и видимость тега в консоли пользователя.
4. Завершите редактирование нажатием **Сохранить**.

Чтобы удалить один или несколько тегов:

1. Выберите один или несколько тегов в списке.
2. Нажмите **Удалить**.
3. Подтвердите удаление нажатием **Удалить** во всплывающем окне.

> **ПРИМЕЧАНИЕ**
> При удалении тег снимется со всех ресурсов, к которым был применен.

Мониторинг

Indeed PAM автоматически определяет неиспользуемые разрешения. Администратор может отозвать такие разрешения, чтобы минимизировать избыточные привилегии.

Настройка	Описание
Считать разрешение неиспользуемым, если им не пользовались более	Задает количество дней отсутствия активности по разрешению, при превышении которого разрешение считается неиспользуемым. Разрешение используется, если выполняются: • успешный запуск сессии; • просмотр или изменение учетных данных; • проверка разрешения на использование pamsu.
Считать пользователя неактивным, если он не пользовался своими разрешениями более	Определяет период времени, по истечении которого пользователь считается неактивным.

Лицензии

В этом разделе отображаются данные по зарегистрированным, доступным и занятым лицензиям. Подробнее о лицензиях читайте в разделе **Лицензирование**.

Получить

1. Перейдите в раздел **Конфигурация** → **Лицензии**.
2. Скопируйте значение из поля **ID инсталляции**.
3. Передайте этот идентификатор инсталляции в техническую поддержку для выпуска файла лицензии.
4. Дождитесь от технической поддержки ответ с файлом лицензии вида *PAM_гггг.мм.дд.lic*.

Добавить

1. Перейдите в раздел **Конфигурация** → **Лицензии**.
2. Нажмите **Добавить**.
3. Выберите файл лицензии и нажмите **Загрузить**.

Удалить

1. Перейдите в раздел **Конфигурация** → **Лицензии**.
2. Выберите одну или несколько лицензий и нажмите **Загрузить**.

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

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 находится Connector Creation Tool.

   Выполните указанную команду, затем закройте терминал и откройте заново.

   Windows

   Добавление пути до CCT в переменную окружения

   ```
   "New-Alias cct <путь до CCT>\Pam.Tools.ConnectorCreationTool.exe" | Add-Content $PROFILE
   ```

   Linux

   Добавление пути до CCT в переменную окружения

   ```
   echo 'alias cct="<путь до CCT>/run-cct.sh"' >> ~/.bashrc
   ```

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

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-адрес коннектора>
   ```

2. Проверьте команду установки пароля для пользователя.

Установка пароля для пользователя

```
cct run set_user_password -a <DNS или IP-адрес 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-адрес 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-адрес коннектора> --user <пользователь> --password <пароль>
```

5. Проверьте команду проверки ключа пользователя.

Проверка ключа пользователя

```
cct run test_key -a <DNS или IP-адрес 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-адрес 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-адрес коннектора> --key-path <ключ>
```

8. Проверьте команду получения информации о ресурсе.

Получение информации о ресурсе

```
cct run get_resource_info -a <DNS или IP-адрес коннектора>
```

9. Проверьте команду получения информации об аккаунте.

Получение информации об аккаунте

```
cct run get_account_info -a <DNS или IP-адрес коннектора> --user <пользователь>
```

10. Проверьте команду получения списка пользователей.

Получение списка пользователей

```
cct run get_users -a <DNS или IP-адрес коннектора>
```

11. После проверки всех сервисных операций переходите к упаковке коннектора.

Упаковка

Упакуйте файлы коннектора в ZIP-архив, чтобы в дальнейшем загрузить его 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**, чтобы загрузить ZIP-архив коннектора.

Структура

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` — параметр, показывающий, поддерживает ли коннектор работу 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

Пример запуска команды

```
<путь до CCT>\Pam.Tools.ConnectorCreationTool.exe new -t ps1 -p
C:\Users\user\documents\folder1\
```

Linux

Пример запуска команды

```
bash <путь до CCT>/run-cct.sh new -t ps1 -p /home/user/documents/folder1/
```

Параметры команды new

Имя	Обязательный	Описание
-v, --verbose	—	Включить показ дополнительных логов.

Имя	Обязательный	Описание
-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

Пример запуска команды

```
<путь до CCT>\Pam.Tools.ConnectorCreationTool.exe pack -p
C:\Users\user\documents\folder1\ -n b80d094b715aa08375b87e9.1.1
```

Linux

Пример запуска команды

```
bash <путь до CCT>/run-cct.sh pack -p /home/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

Пример запуска команды

```
<путь до CCT>\Pam.Tools.ConnectorCreationTool.exe hash -p
C:\Users\user\documents\folder1\
```

Linux

Пример запуска команды

```
bash <путь до CCT>/run-cct.sh hash -p /home/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

Пример запуска команды

```
<путь до CCT>\Pam.Tools.ConnectorCreationTool.exe run test_connection -p
C:\Users\user\documents\folder1\ -a 192.168.5.1
```

Linux

Пример запуска команды

```
bash <путь до CCT>/run-cct.sh run test_connection -p /home/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.

Имя	Обязательный	Описание
-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.

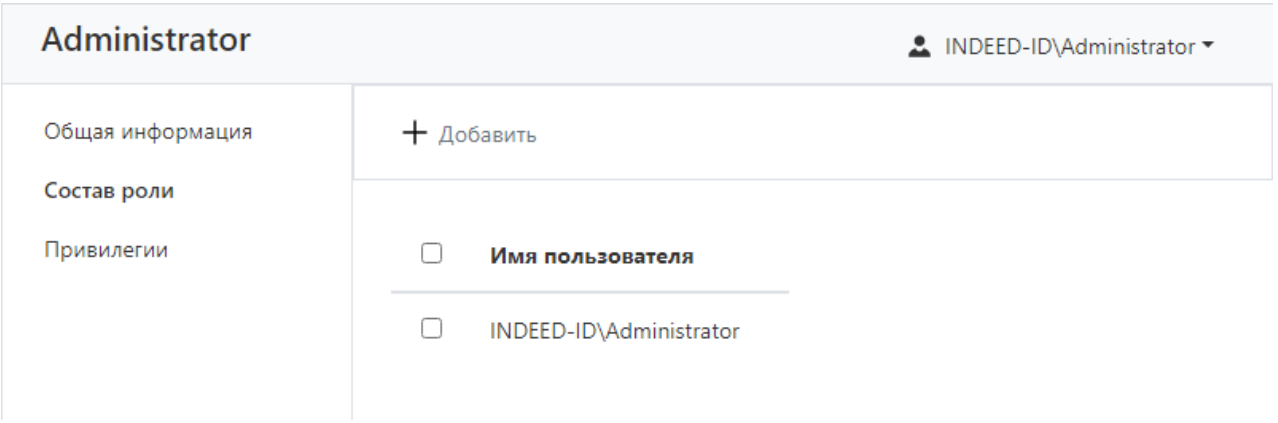
Роли

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 требуется проверить составы привилегий 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.

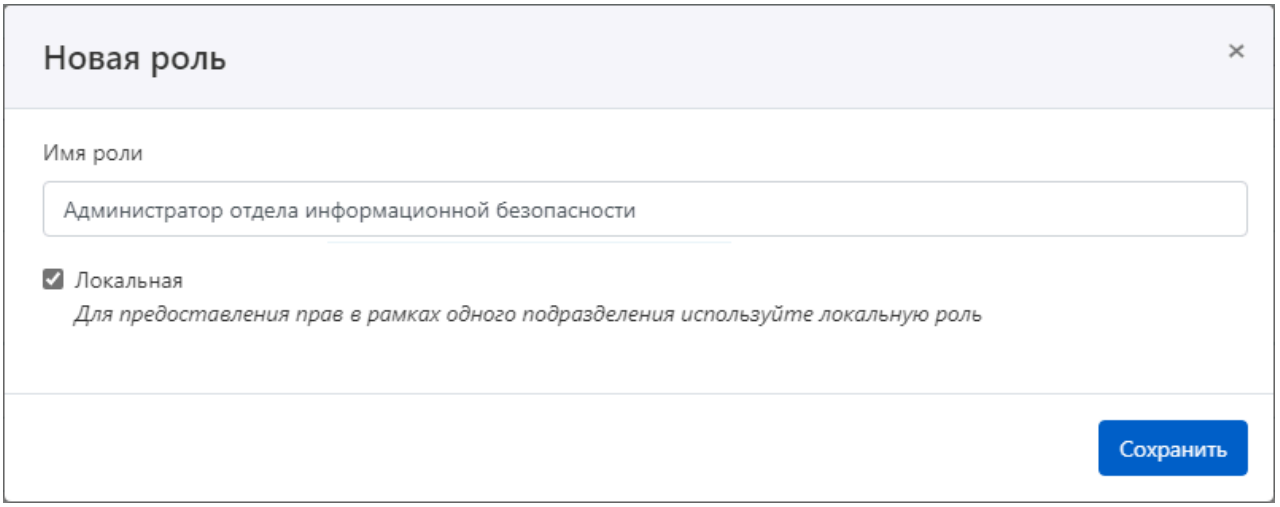
Данные роли являются Глобальными. Сделать роль Локальной можно только при создании новой роли.

Создание новых ролей

> **ПРИМЕЧАНИЕ**
> Для выполнения операций с ролями необходимы привилегии управления ролями доступа.

Выполните следующие шаги:

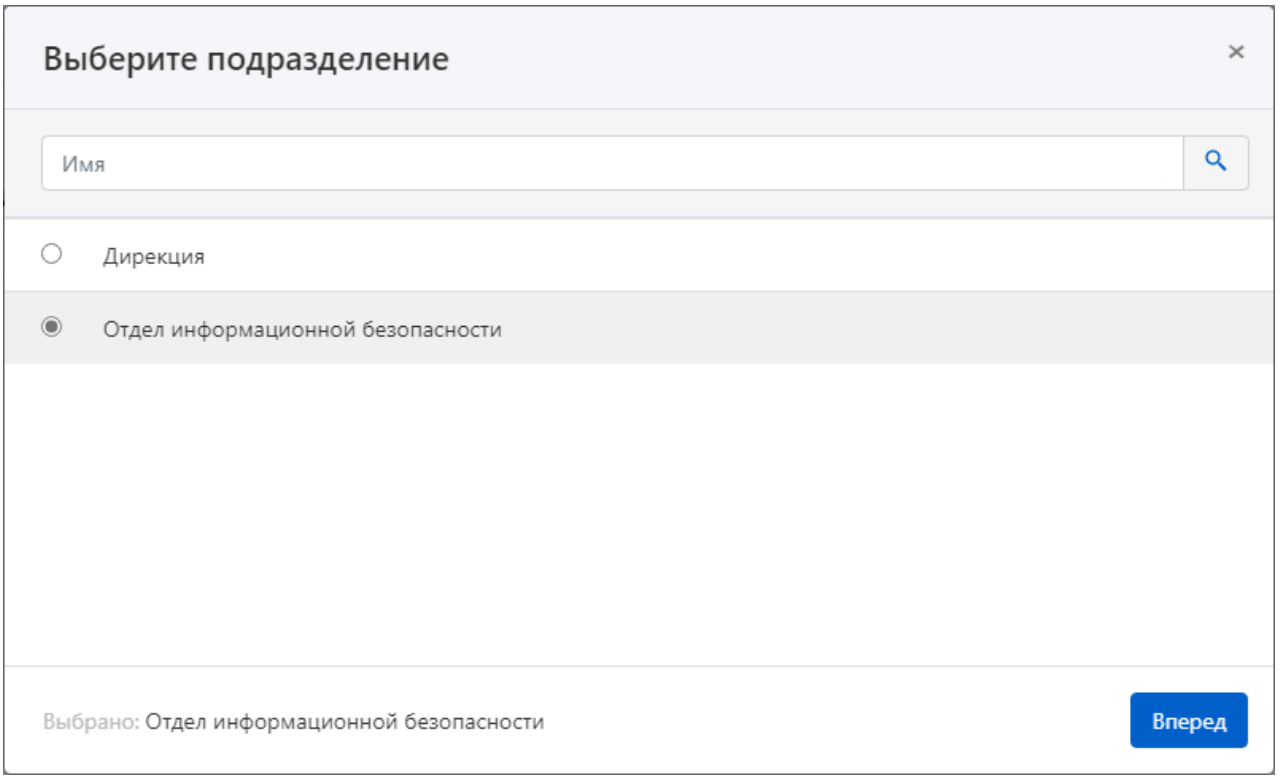
1. Перейдите в раздел **Роли**, нажмите **Добавить**, укажите имя для новой роли, для создания локальной роли включите опцию **Локальная**. Новая роль добавится в список ролей.
2. Откройте созданную роль, перейдите в раздел **Привилегии**, выберите необходимый набор привилегий и сохраните изменения.



Добавление пользователей в состав роли

Чтобы назначить привилегии 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 одну или несколько ролей, нажмите **Удалить**.

Приложения

Приложение (Application) — стороннее программное обеспечение для автоматизации и выполнения задач. При запуске приложение запрашивает аутентификацию с использованием данных учетных записей. Как правило, эти данные хранятся в открытом виде в скриптах или конфигурационных файлах, что увеличивает риск их перехвата третьими лицами.

Чтобы повысить безопасность, используйте метод автоматического получения учетных данных — Application to Application Password Management (AAPM). В таком случае пароли и SSH-ключи учетных записей хранятся в Indeed PAM и запрашиваются приложением только в момент выполнения задачи. Это позволяет контролировать доступ к учетным данным, не хранить их в открытом виде, а также автоматически обновлять.

Чтобы настроить работу с AAPM:

1. Добавьте приложение в Indeed PAM и настройте аутентификацию.
2. Выдайте разрешение и выберите те учетные записи, чьи пароли и/или SSH-ключи нужны для работы AAPM.
3. Выберите и настройте удобный способ получения учетных данных.

> ⓘ **ПРИМЕЧАНИЕ**
> Для работы с приложениями требуется AAPM-лицензия.

Профиль приложения

Для каждого приложения отображаются:

- Администраторы — перечень пользователей, которые могут просматривать учетные данные приложения.
- Разрешения — список выданных разрешений на использование данных учетных записей.
- События — записи об операциях, связанных с приложением.

Добавить приложение

> ⚠ **ОГРАНИЧЬТЕ ДОСТУП**
> Для повышения безопасности рекомендуется создавать приложение под конкретную задачу и ограничить количество выдаваемых разрешений.

1. Перейдите в раздел **Приложения** в консоли администратора.
2. Нажмите **Добавить**.
3. Заполните поля **Имя** и **Описание** и нажмите **Сохранить**.

Аутентификация

Перед началом работы в Indeed PAM приложения и пользователи проходят аутентификацию в IdP.
Для приложений поддерживаются следующие способы аутентификации:

- Пароль — обязателен и задается автоматически при добавлении приложения в PAM. В консоли администратора нельзя просмотреть пароль, но можно сбросить. Пароль может просмотреть администратор приложения в консоли пользователя.
- IP-адрес — задается дополнительно, если нужна проверка на соответствие IP-адреса, с которого приходит запрос на получение токена доступа.
- Сертификат — задается дополнительно, если нужна проверка отпечатков клиентского сертификата.

Добавить разрешение

Разрешения позволяют приложению использовать пароли и/или SSH-ключи учетных записей Indeed PAM.
Чтобы выдать разрешение:

1. Откройте профиль приложения.
2. Нажмите **Добавить разрешение**.
3. Выберите подразделение и нажмите **Вперед**.
4. Выберите одну или несколько учетных записей, чьи учетные данные нужны, и нажмите **Вперед**.
5. Настройте **Ограничения времени** и нажмите **Вперед**.
6. Настройте **Параметры разрешения** и нажмите **Вперед**.
7. Заполните поле **Описание** и нажмите **Вперед**.
8. Проверьте данные и нажмите **Создать**.

Сбросить пароль

При добавлении приложения Indeed PAM задает ему случайный пароль. В консоли администратора нельзя просмотреть этот пароль, но можно сбросить и задать новый. Для этого:

1. Перейдите в профиль приложения и нажмите **Сбросить пароль**.

2. В появившемся окне введите причину смены пароля и нажмите **Сбросить**.

После сброса старого пароля Indeed PAM сгенерирует новый.

Добавить или удалить администратора

Администраторы могут просматривать пароль приложения в консоли пользователя.
Чтобы добавить администратора:

1. Откройте профиль приложения и перейдите на вкладку **Администраторы**.
2. Нажмите **Добавить администратора**.
3. Выберите одного или нескольких пользователей и нажмите **ОК**.
4. Подтвердите действие и нажмите **Добавить**.

Чтобы удалить администратора:

1. Откройте профиль приложения и перейдите на вкладку **Администраторы**.
2. Выберите одного или нескольких пользователей и нажмите **Удалить**.
3. Подтвердите действие и нажмите **Удалить**.

Удалить приложение

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> После удаления приложения AAPM не сможет получить пароли и/или SSH-ключи учетных записей Indeed PAM.

Чтобы удалить приложение:

1. Перейдите в профиль приложения.
2. Нажмите **Удалить** и подтвердите действие.

Чтобы удалить несколько приложений, в разделе **Приложения** выберите нужные приложения и нажмите **Удалить**.

Первый запуск

После первого входа в консоль перейдите в раздел **Роли** и добавьте текущего пользователя в роль *Administrator*, обновите страницу и убедитесь, что в консоли отобразились все разделы.

Проверьте наличие пользователей

1. Перейдите в раздел **Пользователи**.
2. Нажмите  .
3. Убедитесь, что все пользователи из указанного организационного подразделения корректно отобразились.

Лицензируйте инсталляцию

1. Перейдите в раздел **Конфигурация** → **Лицензии**.
2. Скопируйте значение из поля **ID инсталляции**.
3. Передайте этот идентификатор инсталляции в техническую поддержку для выпуска файла лицензии.
4. Дождитесь от технической поддержки ответ с файлом лицензии вида *PAM_гггг.мм.дд.lic*.
5. В разделе **Конфигурация** → **Лицензии** нажмите **Добавить** и прикрепите полученный файл лицензии.

Заполните адреса компонентов

1. Перейдите в раздел **Конфигурация** → **Системные настройки**.
2. В секции **Подключение к Gateway** укажите **Адрес RDCB** и **Имя коллекции RDCB**.
3. В секции **RDP Proxy** укажите **Адрес RDP Proxy**.
4. В секции **PostgreSQL Proxy** укажите **Адрес PostgreSQL Proxy**.
5. В секции **Настройки SSH-подключений** укажите **Адрес SSH Proxy**.
6. Сохраните изменения.

Проверьте события

1. Перейдите в раздел **События**.
2. Убедитесь, что отобразилось событие изменения параметров конфигурации.

Определите работу текстового логирования

Если вы отказались от установки компонента Indeed PAM Agent, перейдите в раздел **Политики** → **Сессии** → **Артефакты** и выполните одно из действий:

- отключите опцию **Сохранять текстовые логи сессии**;
- включите опцию **Продолжать RDP-сессию без логирования, если не удалось получить текстовый лог**.

При отсутствии ошибок переходите к добавлению объектов.

Добавление текущего домена

1. Перейдите в раздел **Домены** и нажмите **Добавить**.
2. Введите **Имя домена** и **DNS-имя**.
3. Выберите службу из списка **Служба каталогов**.
4. Задайте **Порт** или оставьте значение по умолчанию.
5. Включите опцию **Использовать LDAPS**, если требуется подключение по этому протоколу. По умолчанию используется протокол LDAP.
6. Нажмите **Сохранить**.

Добавленный домен отображается в разделе **Домены**.

Настройка текущего домена

1. Откройте профиль добавленного домена.
2. Перейдите на вкладку **Доменные учетные записи** и нажмите **Добавить доменную учетную запись**.
3. Введите **Имя** сервисной учетной записи и **Описание**.
4. При задании пароля выберите одну из опций:

- **Сгенерировать случайный пароль** — пароль будет создан автоматически и синхронизирован с ресурсом или доменом.
- **Задать пароль вручную** — пароль будет задан в ручном режиме.
  Введите пароль и подтвердите его.
  Если требуется, чтобы пароль учетной записи сменился не только в PAM, но и в домене, включите опцию **Изменить пароль в домене**.
- **Не задавать** — учетная запись будет создана без пароля, его можно задать позже при редактировании.

5. Нажмите **Вперед**.
6. Проверьте данные и нажмите **Сохранить**.
7. Нажмите ✎ напротив параметра **Сервисная учетная запись**.
8. Выберите сервисную учетную запись и нажмите **ОК**.
9. Нажмите **Проверить соединение** и убедитесь в наличии соединения до домена.
10. Перейдите на вкладку **Контейнеры для ресурсов**:
    1. Нажмите **Добавить контейнер для ресурсов**.
    2. Выберите контейнер службы каталогов, в котором находятся доменные ресурсы, и нажмите **ОК**.
11. Перейдите на вкладку **Привилегированные группы**:
    1. Нажмите **Добавить привилегированную группу**.
    2. Выберите группы безопасности и нажмите **ОК**.
       В группах безопасности находятся учетные записи, с помощью которых пользователи будут получать доступ к доменным ресурсам.
12. Нажмите **Импортировать ресурсы** и **Синхронизировать учетные записи**.
    Все доступные ресурсы и учетные записи добавятся в PAM.

Для домена добавлены учетные записи и импортированы ресурсы. Теперь нужно подтвердить учетные данные.

Добавление и взятие под контроль учетных записей

В разделе **Учетные записи** отметьте импортированные доменные учетные записи: они начинаются с имени домена, отмечены символом ⚠ и находятся в состоянии **Ожидает решения**.

Для сброса старого пароля и установки нового в соответствии с политикой откройте профиль учетной записи и нажмите **Сделать управляемой**.

Добавление не доменных ресурсов

1. Перейдите в раздел **Ресурсы** и нажмите **Добавить**.
2. Введите **Имя ресурса**, **DNS-имя**, **IP-адрес**, **Описание** и нажмите **Вперед**.
3. Выберите **Тип подключения**, **DNS-имя / IP-адрес**, **Порт** и нажмите **Вперед**.
4. Отключите опцию **Использовать коннектор для сервисного подключения**, так как локальных учетных записей не было добавлено.
5. Нажмите **Сохранить**.
6. Откройте профиль ресурса и перейдите на вкладку **Локальные учетные записи**.
7. Нажмите **Добавить локальную учетную запись**.
8. Введите **Имя** и **Описание** и нажмите **Вперед**.
9. При задании пароля выберите одну из опций:
   - **Сгенерировать случайный пароль** — пароль будет создан автоматически и синхронизирован с ресурсом или доменом.
   - **Задать пароль вручную** — пароль будет задан в ручном режиме.
     Введите пароль и подтвердите его.
     Если требуется, чтобы пароль учетной записи сменился не только в PAM, но и в домене, включите опцию **Изменить пароль в домене**.
   - **Не задавать** — учетная запись будет создана без пароля, его можно задать позже при редактировании.
10. Нажмите **Вперед**.
11. Проверьте данные и нажмите **Сохранить**.

Для корректной работы сервисных операций требуется настройка сервисного подключения.

Дашборд

Дашборд позволяет анализировать активность пользователей в режиме реального времени. На дашборде расположены виджеты, отображающие сводные данные PAM. Виджеты позволяют переходить в другие разделы консоли администратора для более детального анализа.

Список виджетов

В Indeed PAM 3.4 доступны следующие виджеты:

- Сессии
- Серверы PAM
- Разрешения
- Учетные записи
- Использование лицензий
- Контроль активности

> **ПРИМЕЧАНИЕ**
> Дашборд находится в консоли администратора в разделе **Главная**.
>
> Для управления дашбордом включите привилегии *Просмотр страницы* и *Изменение конфигурации страницы*.

Сессии

Виджет показывает изменение количества сессий, ошибок аутентификации и просмотра учетных данных. Анализируйте сессии и действия пользователей, чтобы выявить потенциальные инциденты, например, активность в нерабочие часы или повторяющиеся ошибки в сессиях.

На график можно вывести данные за час, сутки или неделю и отобразить количество:

- Всех сессий — общее количество сессий.
- Сессий с ошибкой — количество сессий, завершенных из-за ошибки.
- Ошибок аутентификации — количество ошибок аутентификации в консолях пользователя и администратора.
- Просмотров учетных данных — количество просмотров учетных данных в консоли пользователя.

Чтобы перейти к списку всех сессий или сессий, завершенных из-за ошибки, нажмите **В сессии**.

Чтобы перейти к списку неудачных попыток аутентификации или просмотров учетных данных, нажмите **В события**.

Серверы PAM

Виджет показывает количество серверов с установленными компонентами Indeed PAM и их состояние. Важно следить за состоянием компонентов PAM — в случае сбоя получится своевременно обнаружить проблему и решить ее.

Для каждого компонента Indeed PAM отображается статус:

- *Работает* — все компоненты сервера работают корректно.
- *Сбой* — в работе одного или нескольких компонентов возник сбой.
- *Идет проверка* — проверка работы добавленного или измененного сервера.

Чтобы детально изучить состояния компонентов, перейдите в виджет **Серверы** и в левом меню выберите нужный сервер. Если в работе компонента возник сбой, раскройте ошибку и устраните ее.

Добавить сервер в виджет

Если появился новый сервер с установленными компонентами PAM, добавьте сервер в виджет для мониторинга за его состоянием.

Чтобы отображать состояние сервера в виджете:

1. Перейдите в виджет **Серверы PAM**.
2. В левом меню нажмите **Добавить сервер PAM**.
3. В поле **Адрес сервера** укажите DNS-имя или IP-адрес сервера.
4. Выберите операционную систему сервера.
5. В зависимости от операционной системы задайте одну или несколько ролей для сервера.
6. (Опционально) Раскройте настройку **Изменить порты** и укажите порты для каждой выбранной роли.

   > ⚠ **ПРЕДУПРЕЖДЕНИЕ**
   > Порты используются для проверки доступности сервера методом Healthcheck. Измените порты только в том случае, если в конфигурационных файлах компонентов PAM указаны порты не по умолчанию.

7. Нажмите **Проверить соединение**.
   Если возникла ошибка, убедитесь, что на сервере установлены компоненты PAM и верно выбраны роли.
8. Нажмите **Добавить**.

Добавленный сервер отображается со статусом *Идет проверка*. В течение минуты в виджете отобразится состояние сервера и его компонентов.

Редактировать данные сервера

Внесите новые данные в виджет при изменении конфигурации сервера, например, если добавлена новая роль или обновлено DNS-имя.

Чтобы изменить данные сервера:

1. Перейдите в виджет **Серверы PAM**.
2. Перейдите на вкладку с нужным сервером и нажмите **Редактировать**.
3. Внесите необходимые изменения.

   > ⚠ **ПРЕДУПРЕЖДЕНИЕ**
   > Порты используются для проверки доступности сервера методом Healthcheck. Измените порты только в том случае, если в конфигурационных файлах компонентов PAM указаны порты не по умолчанию.

4. Нажмите **Проверить соединение**.
   Если возникла ошибка, убедитесь, что на сервере установлены компоненты PAM и верно выбраны роли.
5. Нажмите **Сохранить**.

После редактирования сервер отображается со статусом *Идет проверка*. В течение минуты в виджете отобразится состояние сервера и его компонентов.

Удалить сервер из виджета

Удаление сервера влияет только на отображение виджета — статус удаленного сервера не отслеживается.

Чтобы не отображать сервер в виджете:

1. Перейдите в виджет **Серверы PAM**.
2. Перейдите на вкладку с нужным сервером и нажмите **Удалить**.
3. В окне подтверждения нажмите **Удалить**.

Разрешения

Виджет показывает количество проблемных или неиспользуемых разрешений. Поддерживайте актуальность разрешений: это обеспечивает контроль за привилегированным доступом и снижает риски несанкционированных действий.

Что отслеживается:

- Разрешения с ограничениями — количество разрешений с ошибками. Пользователи не могут открыть сессии по таким разрешениям. Ограничения возникают по нескольким причинам: нет лицензии, не задан SSH-отпечаток, пользователь или учетная запись недоступны. Исправьте ошибки, отзовите или пересоздайте разрешения.
- Неиспользуемые разрешения — количество разрешений, которыми не воспользовались в течение заданного периода времени. Отзовите такие разрешения. Период, по истечении которого разрешения считаются неиспользуемыми, можно настроить в разделе **Мониторинг**.

Чтобы перейти к подробному списку разрешений, нажмите ↗.

Учетные записи

Виджет показывает количество и состояния учетных записей. Убедитесь, что нужные учетные записи находятся под управлением PAM, а их пароли и SSH-ключи своевременно обновляются. Это защитит учетные записи от неправомерного использования в обход PAM.

Что отслеживается:

- Ожидает решения — учетные записи в состоянии *Ожидает решения*. PAM не управляет такими учетными записями. Они могут использоваться вне системы и обходить контроль доступа. Перейдите в профиль учетной записи и переведите ее в состояние *Управляется* или *Игнорируется*.
- Учетные записи с ошибками — учетные записи, у которых возникли ошибки при работе с PAM. Это может быть сбой при смене пароля или ошибки с SSH-ключами. Такие учетные записи не обновляются и могут не работать как ожидается. Проверьте детали и устраните проблему.
- Ротация пароля и SSH-ключа не включена в политике — учетные записи, у которых не ротируются учетные данные. Такие учетные записи уязвимы. Включите опцию **Периодически ротировать пароль и SSH-ключ учетной записи**.

Чтобы перейти к подробному списку учетных записей, нажмите ↗.

Другие состояния учетных записей

Состояния учетных записей:

- Управляется — управляемая учетная запись. PAM может хранить пароль и SSH-ключ от этой записи, выдавать разрешения и запускать сессии. При наличии сервисного подключения проверяются и меняются данные для этой учетной записи.
- Игнорируется — учетная запись не участвует в операциях и синхронизации. PAM знает о существовании учетной записи, но не хранит и не управляет ее данными.
- Заблокирована — учетная запись недоступна для использования.

Лицензии

Виджет показывает количество используемых и доступных лицензий. Следите за остатком и сроком действия лицензий: без них пользователи не могут открывать сессии, а администраторы — выдавать разрешения.
Подробнее о лицензиях читайте в разделе **Лицензирование**.

Отслеживаются лицензии:

- Пользовательская — определяет количество пользователей, которые могут использовать Indeed PAM.
- Ресурсная — определяет количество ресурсов, которые можно добавить в Indeed PAM.
- AAPM — количество учетных записей, которым можно дать разрешения при помощи механизма AAPM.
- SQL Proxy — определяет количество активных разрешений на ресурсы с типом PostgreSQL или MSSQL.
- Произвольные ресурсы — определяет количество произвольных ресурсов для подключения.

Чтобы перейти к списку лицензий, нажмите **Подробнее** в правом верхнем углу виджета.

Контроль активности

Виджет показывает количество неактивных пользователей. Пользователь считается неактивным, если не использовал свои разрешения в течение установленного администратором срока.

Чтобы перейти к подробному списку пользователей, нажмите ↗.

Настройка политик

Управление политиками

Политика — набор опций и ограничений, применяемых к различным объектам: пользователям, учетным записям, ресурсам или доменам. Например, с помощью настроенных политик можно задать для пользователя запрещенные SSH-команды, запрашивать причины для открытия сессии или ограничить работу буфера обмена между рабочим местом и ресурсом. Для каждого объекта можно назначить только одну политику.

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 в настройках **Учетные записи**, **Сессии**, **Gateway и SSH Proxy**, **RDP**, **SSH** и сохраните их.

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

- **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.

Чтобы отредактировать **Имя**, **Описание** или **Приоритет**, 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

Из списка политик

1. Откройте раздел **Политики**.
2. Отметьте одну политику.
3. Нажмите **Задать приоритет**.
4. Введите значение.
5. Нажмите **Сохранить**.

Из профиля политики

1. Откройте профиль политики.
2. В разделе **Общая информация** нажмите рядом со значением приоритета.
3. Введите значение.
4. Нажмите **Сохранить**.

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 будут сброшены на случайное значение через указанное количество минут.
Требовать указать причину просмотра пароля и SSH-ключа	Если опция включена, то пользователь 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.

Опция	Описание
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 генерируются средствами PAM при просмотре данных каждый раз заново.

Задание учетных данных

Опция	Описание
Разрешить пользователям PAM задавать учетные данные для учетных записей, если они не заданы	Если опция включена, то когда пользователь попытается подключиться к ресурсу от имени учетной записи с 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.

Опция	Описание
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 ротировать пароль и SSH-ключ учетной записи	Если опция включена, то для учетных записей доступа будет автоматически изменяться пароль или SSH-ключ на случайное значение.
Период ротации 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.
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.

Опция	Описание
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.
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 пользователю нужно 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.
Сообщение, которое пользователь увидит при запросе причины	Если опция **Требовать указать причину подключения** включена, то сообщение обязательно к заполнению. Значение по умолчанию: «Укажите причину подключения:». Можно поменять текст сообщения, чтобы подсказать пользователю, что именно требуется вводить при подключении. Например, если для подключения нужно указывать номер задачи в тикет-системе, то введите: «Укажите номер заявки для выполнения задачи на данном ресурсе:». Максимально допустимая длина сообщения: 100 символов.
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 администратора PAM	Если опция включена, то для каждой открываемой сессии требуется ручное подтверждение 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.

Опция	Описание
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.
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.

Опция	Описание
Сохранять видео сессии	Если опция включена, то после завершения сессии запись потокового видео будет доступна для просмотра и скачивания. Поддерживается при открытии сессий через PAM Gateway и RDP Proxy.
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. Рекомендуемая настройка для сессий через Web Proxy: Уменьшить в два раза.
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 при открытии сессий через PAM Gateway и RDP Proxy.
Интервал снимков, сек	Сохранение снимка экрана через указанное 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, в указанную сетевую папку сохраняются переданные на ресурс и полученные с ресурса файлы. Поддерживается в сессиях: • открытых через RDP Proxy в зависимости от настроек политики RDP; • открытых по протоколам SCP/SFTP в зависимости от настроек передачи данных политики SSH. В сессиях, открытых через PAM Gateway, сохраняются только переданные на ресурс файлы.

Опция	Описание
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 или DNS 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 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 перенаправить 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 конечным ресурсом.
Смарт-карты	Если опция включена, то пользователь получит возможность перенаправить смарт-карту со своего рабочего места на конечный ресурс.
Порты	Если опция включена, то пользователь получит возможность перенаправить COM-порты со своего рабочего места на конечный ресурс.
Диски	Если опция включена, то пользователь получит возможность перенаправить 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

Параметры сессии

Опция	Описание
Использовать PTY	Выделяет для SSH-сессии псевдотерминал (PTY). При отключении опции в сессии можно использовать только неинтерактивные команды.

Повышение привилегий

> **ПРИМЕЧАНИЕ**
> Разрешение, выданное на выполнение pamsu при создании разрешения, приоритетнее, чем настройка в политике.

Опция	Описание
Разрешить выполнять pamsu	Поддержка выполнения команд с привилегиями root в SSH-сессиях на ресурсах с установленным компонентом PamSu.

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.

Чтобы составить список контролируемых команд, выполните следующие действия:

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.

Чтобы разрешить или запретить сразу нескольких команд, отметьте их 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

Web-приложения

Настройки применяются только к ресурсам с типом Web-приложение со способом открытия сессии **В браузере**.
Если для веб-приложения выбран способ **Через RDP**, применяются настройки из раздела RDP.

Опция	Описание
Разрешить использование буфера обмена	Пользователь может копировать и вставлять текст между веб-приложением и локальным устройством.

Настройка подключения пользователей по SSH-ключам

Пользователи могут подключаться к SSH Proxy по SSH-ключам. Это обеспечивает безопасный и быстрый вход в SSH Proxy без необходимости использовать пароли.

Предварительные требования

В разделе Конфигурация → Аутентификация пользователей → Аутентификация по SSH-ключам включите опцию **Разрешить пользователям подключаться к SSH Proxy с использованием SSH-ключей**.

Добавьте администратору, который будет добавлять пользователям ключи, привилегию *User.ManageSshAuthorizedKeys* в роль.

Получение и добавление ключей

Ключ в текстовом формате

1. Попросите пользователя сгенерировать SSH-ключ.

   Поддерживаемые алгоритмы шифрования ключей:

   - rsa-sha2-256
   - rsa-sha2-512
   - ecdsa-sha2-nistp256
   - ecdsa-sha2-nistp384
   - ecdsa-sha2-nistp521
   - ssh-ed25519
2. Запросите у пользователя открытый ключ. Строка с ключом должна содержать алгоритм шифрования и ключ. Опционально строка может содержать комментарий, например имя пользователя и хост. Пример: ssh-ed25519 AAAAC3... user@host.
3. Добавьте полученный ключ этому пользователю в консоли управления Indeed PAM.

Сертификат X.509

1. Попросите пользователя сгенерировать сертификат X.509, в котором отсутствует цепочка сертификатов.

   Поддерживаемые алгоритмы шифрования ключей:

   - rsa-sha2-256
   - rsa-sha2-512
   - ecdsa-sha2-nistp256
   - ecdsa-sha2-nistp384
   - ecdsa-sha2-nistp521
   - ssh-ed25519
2. Запросите у пользователя файл с сертификатом. Поддерживаемые расширения файла: PEM, DER, CRT.
3. Добавьте полученный файл этому пользователю в консоли управления Indeed PAM.

Выгрузка паролей

В случае нештатной ситуации, при отказе компонентов PAM предусмотрена возможность выгрузки паролей привилегированных учетных записей из базы PAM.

Выгрузка выполняется с помощью утилиты *IndeedPAM_3.4_RU\indeed-pam-tools\dump\Pam.Tools.Dump.exe*.

Редактирование конфигурационного файла

Перед использованием утилиты откройте конфигурационный файл *IndeedPAM_3.4_RU\indeed-pam-tools\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
- `PamCore` — строка подключения к СУБД

Строка подключения к MicrosoftSQL

- `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

```
"PamCore": "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` требуется указывать в формате **имя сервера\\имя экземпляра**.
>
> ```
> "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

```
"PamCore": "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

Запуск утилиты

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, требуется указать учетную запись, пример:
  `Pam.Tools.Dump.exe ssh-key --name res2\administrator`.
- `password` — выгрузка пароля привилегированной учетной записи, требуется 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 all-secrets --output c:\temp`.
- `help` — вывод справки.
- `version` — вывод информации о версии.

Работа с PostgreSQL и MSSQL Proxy

Компоненты MSSQL Proxy и PostgreSQL Proxy позволяют открывать SQL-сессии через консольные и графические клиенты. Поддерживается текстовое логирование SQL-сессии, благодаря чему упрощается расследование инцидентов.

> ⓘ **ПРИМЕЧАНИЕ**
> Для подключения к ресурсам MSSQL и PostgreSQL требуется отдельная лицензия.

Настройка клиента СУБД

При подключении к серверу и работе с ним через SQL-клиент может создаваться несколько сессий. В этом случае в PAM тоже создается несколько сессий, что доставляет неудобства при просмотре логов.

Чтобы в рамках одного подключения к серверу была одна сессия, необходимо настроить SQL-клиент. Настройка на примере клиента DBeaver:

1. Установите клиент DBeaver. По умолчанию установлен английский язык.
2. В левой части экрана в окне **Database Navigator** найдите в списке доступных подключений нужный сервер.
   Нажмите на него левой кнопкой мыши и в контекстном меню выберите **Edit Connection**.
3. В открывшемся окне перейдите на вкладку **Metadata** и включите опцию **Datasource <servername> settings**.
4. Для параметра **Open separate connection for metadata read** выберите **Never** из выпадающего списка.
5. Перейдите на вкладку **SQL Editor** и включите опцию **Datasource <servername> settings**.
6. Для параметра **Open separate connection for each editor** выберите опцию **Never** из выпадающего списка.
7. Нажмите **OK**.
8. Повторите перечисленные действия для всех серверов БД.

Настройка SSL-шифрования

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> Для корректной работы необходимо настроить SSL как для прокси, так и на сервере.

PostgreSQL Proxy

Чтобы настроить работу PostgreSQL Proxy через SSL, включите использование SSL в PostgreSQL Proxy и на сервере PostgreSQL Server. Для этого:

1. Откройте файл конфигурации PostgreSQL Proxy по пути */etc/indeed/indeed-pam/sql-proxy/appsettings.json*.
2. Для параметра `SslIsRequired` установите значение `true` и сохраните изменения.
3. Откройте файл конфигурации PostgreSQL Server *postgresql.conf*.
4. Для параметра `ssl` установите значение `on`.
5. Для параметра `ssl_cert_file =` укажите путь до SSL-сертификата.
6. Сохраните изменения.

MSSQL Proxy

Чтобы настроить работу MSSQL Proxy через SSL, включите использование SSL в MSSQL Proxy и на сервере Microsoft SQL Server. Для этого:

1. Откройте файл конфигурации MSSQL Proxy по пути */etc/indeed/indeed-pam/tsql-proxy/appsettings.json*.
2. Для параметра `SslIsRequired` установите значение `true` и сохраните изменения.
3. Откройте клиент SQL Server Configuration Manager.
4. Раскройте вкладку **SQL Server Network Configuration** и выберите протокол для вашего экземпляра SQL Server.
5. Для параметра **Force Encryption** установите значение **Yes**.
6. Перейдите на вкладку **Certificate** и загрузите SSL-сертификат.
7. Нажмите **Apply** и **ОК**.

Возможно взаимодействие без SSL?

Да, для этого отключите использование SSL в прокси и на сервере.

Настройка конфигурации в PAM

Чтобы настроить подключение через прокси-сервер:

1. Перейдите в раздел **Конфигурация** → **Системные настройки**.

2. В поле **Адрес PostgreSQL Proxy** или **Адрес MSSQL Proxy** укажите IP-адрес или DNS-имя и порт компонента.

Запуск SQL-сессии

Чтобы открыть SQL-сессию, перейдите в консоль пользователя и подключитесь к ресурсу через MSSQL Proxy или PostgreSQL Proxy.

Логи

> ⓘ **ИНФОРМАЦИЯ**
>
> SQL-клиенты могут по-разному сохранять текст SQL-запросов. Например, psql вырезает комментарии из SQL-запросов, а pgAdmin оставляет.
>
> В текстовый лог попадают только исходящие SQL-запросы (клиент → сервер), и не сохраняются их результаты.

Чтобы просмотреть текстовые логи сессии, открытой через MSSQL Proxy или PostgreSQL Proxy:

1. Откройте консоль администратора и перейдите в раздел **Активные сессии**.
2. Выберите нужную сессию.
3. Нажмите **Текстовый лог**.

Чтобы получить актуальный текстовый лог, нажмите **Обновить**.

Если при работе возникают проблемы или ошибки, соберите логи PostgreSQL Proxy или MSSQL Proxy и обратитесь в техническую поддержку.

Ограничения

- Пользователь может открывать сессии через MSSQL Proxy и PostgreSQL Proxy только от имени учетной записи, добавленной в PAM с паролем. Подключение не будет установлено, если в разрешении выбрана:
  - учетная запись, добавленная в PAM без пароля;
  - пользовательская учетная запись, для которой запрашиваются учетные данные при открытии сессии.
- 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** игнорируется, то есть при подключении второй фактор не запрашивается.
- Пользователю не нужно подтверждение от администратора, чтобы открыть сессию. Отключите параметр **Открытие сессии требует подтверждения администратора PAM** в политике сессии, иначе открыть SQL-сессию невозможно.
- При открытии сессии пользователям требуется ввести причину подключения, если в политике сессий включена опция **Требовать указать причину подключения**.

Работа с Web Proxy

Компонент Web Proxy предоставляет безопасный доступ к веб-приложениям и сайтам через браузер без необходимости использования Microsoft RDS. Администратор может загрузить SSO-шаблон для автоматического заполнения формы входа на веб-ресурсе. Это обеспечивает удобный доступ и не раскрывает пользователю пароль.

Для работы с Web Proxy не требуются отдельные лицензии.

Предварительные действия

1. Перейдите в раздел **Конфигурация** → **Системные настройки** и заполните поле **Адрес Web Proxy**.
2. Перейдите в подраздел **Пользовательское подключение** и добавьте пользовательское подключение с типом **Web-приложение** и способом открытия сессии **В браузере**.
3. В разделе **Ресурсы** откройте профиль ресурса и добавьте созданное пользовательское подключение. Можно добавить несколько подключений с разными URL-адресами. Добавьте новый ресурс, если в PAM нет подходящего.
4. Примените к ресурсу политику с заданной опцией **Разрешить использование буфера обмена**.
5. В профиле ресурса откройте вкладку **Разрешения** и убедитесь, что для ресурса выдано разрешение. Если разрешение не выдано или нужно изменить состав пользователей или учетную запись для подключения, создайте новое разрешение.

Настройка HTTPS-соединения

Для работы с Web Proxy требуется защищенное HTTPS-подключение. Если у веб-ресурса самоподписанный сертификат, то этот сертификат не является доверенным. При попытке доступа к такому ресурсу Web Proxy блокирует соединение, так как считает его небезопасным.

> ⓘ **ПРИМЕЧАНИЕ**
> Сертификат веб-ресурса должен быть выдан доверенным удостоверяющим центром.

Чтобы настроить защищенное соединение:

1. Добавьте сертификат удостоверяющего центра веб-ресурса в папку */etc/indeed/indeed-pam/ca-certificates*

2. Перейдите в папку со скриптами PAM и перезапустите сервер доступа Web:

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

```
sudo bash restart-pam.sh web-proxy
```

3. Откройте сессию через консоль пользователя и подключитесь к веб-ресурсу.
   Убедитесь, что установлено HTTPS-соединение и веб-ресурс открывается.

Запуск веб-сессии

Чтобы открыть веб-сессию в новой вкладке браузера или через RDP-файл, перейдите в консоль пользователя и подключитесь к ресурсу через Web Proxy.

Логи

> **ИНФОРМАЦИЯ**
> Поддерживается только видеологирование сессии.

Чтобы просмотреть видео веб-сессии:

1. Откройте консоль администратора и перейдите в раздел **Активные сессии**.
2. Выберите нужную сессию.
3. Разверните секцию **Видео**.

Если при работе с Web Proxy возникают проблемы или ошибки, соберите логи компонента и обратитесь в техническую поддержку.

Ограничения

- Пользователю не нужно подтверждение от администратора, чтобы открыть сессию.
- Буфер обмена поддерживает работу только с текстовыми данными. Настройте работу буфера в политике.
- В веб-сессиях не поддерживается работа с pdf-файлами. Файл нельзя открыть или отправить на печать.
- Настройки **Прерывать сессию при отсутствии пользовательской активности** и **Открытие сессий без повторной аутентификации** не применяются к веб-сессиям.
- Адресная строка в веб-сессии недоступна для редактирования. Перейти на произвольный URL-адрес не получится.

- Нет ограничения на переход по ссылкам внутри веб-сессии.
- Для подключений нельзя настроить механизм HTTP Strict Transport Security (HSTS).
- Сессии, открытые через Web Proxy, не адаптированы для сенсорных экранов и мобильных браузеров.

Автоматизация через ConsoleApp

Утилита ConsoleApp позволяет автоматически управлять объектами Indeed PAM и настраивать права доступа. Например, с помощью утилиты можно одновременно создать несколько ресурсов или учетных записей, а также отозвать все неиспользуемые разрешения.

> **ПРИМЕЧАНИЕ**
> Все операции, выполненные утилитой, записываются в журнал **События**.

Аутентификация

Перед началом работы с утилитой настройте аутентификацию, чтобы получить доступ к Indeed PAM. ConsoleApp поддерживает следующие режимы аутентификации по протоколу OAuth 2.0:

- Resource Owner Password Flow (ROPC) — утилита получает токен доступа от имени пользователя PAM и передает его учетные данные компоненту Indeed PAM IDP. Все действия, совершаемые через утилиту, выполняются от имени пользователя PAM, а доступные операции ограничены привилегиями указанного пользователя.
- Client Credentials Flow — утилита аутентифицируется в PAM от своего имени в режиме Machine-to-Machine (M2M). Все действия, совершаемые через утилиту, выполняются от имени сервисного клиента `Console Application`, а доступные операции ограничены привилегиями этого клиента.

Resource Owner Password Flow

> **ПРИМЕЧАНИЕ**
> Для ROPC-аутентификации не заполняйте параметр `clientSecret` — оставьте значение пустым.

Чтобы настроить аутентификацию:

1. Перейдите в папку с утилитой и откройте конфигурационный файл *appsettings.json*.
2. Для параметра `coreUrl` укажите адрес компонента Core.
3. Для параметра `idpUrl` укажите адрес компонента IdP.
4. Для параметра `authUsername` укажите логин пользователя PAM.
   Если не заполнить параметр, логин потребуется ввести при запуске утилиты.
5. Для параметра `authPassword` укажите пароль пользователя PAM.
   Если не заполнить параметр, пароль потребуется ввести при запуске утилиты.

При запуске утилиты аутентификация выполняется от имени указанного пользователя PAM. Если для пользователя настроена двухфакторная аутентификация, утилита запросит OTP-код.

Client Credentials Flow

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> Не рекомендуется использовать данную аутентификацию — все пользователи, которые работают с утилитой, выполняют операции от имени сервисного клиента и имеют одинаковый набор привилегий. Чтобы разграничить права и повысить безопасность, используйте ROPC-аутентификацию.

Чтобы настроить аутентификацию:

1. Перейдите в папку с утилитой и откройте конфигурационный файл *appsettings.json*.
2. Для параметра `clientSecret` укажите секрет клиента `Console Application`.

При запуске утилиты аутентификация выполняется от имени сервисного клиента, при этом OTP-код не запрашивается.

> 💡 **ГДЕ НАЙТИ СЕКРЕТ КЛИЕНТА?**
> Перейдите в конфигурационный файл компонента IdP по пути:
>
> - Windows: *C:\inetpub\wwwroot\idp\appsettings.json*
> - Linux: */etc/indeed/indeed-pam/idp/appsettings.json*
>
> В секции `IdentitySettings` в параметре `ConsoleAppClientSecret` указан секрет клиента.

Пример конфигурационного файла

Resource Owner Password Flow

```
{
  "coreUrl": "https://pam.example.local/core",
  "idpUrl": "https://pam.example.local/idp",
  "clientSecret": "",
  "authUsername": "ConsoleAppUser",
  "authPassword": "#123QwerTy!",
  "skipErrorsInBulkProcessing": true,
  "NLog": {
    "variables": {
      "minLevel": "Trace",
      "dbMinLevel": "Info",
      "maxArchiveFilesPerCategory": 23
    },
    "rules": {
      "1": {
        "logger": "*",
        "minLevel": "Trace",
        "writeTo": "processFile"
      }
    }
  }
}
```

Client Credentials Flow

```
{
  "coreUrl": "https://pam.example.local/core",
  "idpUrl": "https://pam.example.local/idp",
  "clientSecret": "NPW8dALzsjzpSGDlTGIEMt5o6sjM8x3sz",
  "authUsername": "",
  "authPassword": "",
  "skipErrorsInBulkProcessing": true,
  "NLog": {
    "variables": {
      "minLevel": "Trace",
      "dbMinLevel": "Info",
      "maxArchiveFilesPerCategory": 23
    },
    "rules": {
      "1": {
        "logger": "*",
        "minLevel": "Trace",
        "writeTo": "processFile"
      }
    }
  }
}
```

Операции с учетными записями

Создать учетную запись

Одна учетная запись

Чтобы создать учетную запись в Indeed PAM:

1. Перейдите в папку с утилитой.

2. Запустите утилиту с параметрами из таблицы:

Windows

```
.\Pam.ConsoleApp.exe create-account <параметр> <значение>
```

Linux

```
dotnet ./Pam.ConsoleApp.dll create-account <параметр> <значение>
```

Параметры

Параметр	Требование	Описание
`--username`	Обязательный	Имя учетной записи
`--resource` или `--domain`	Обязательный	Размещение учетной записи: • `--resource` — имя ресурса; • `--domain` — имя домена. Укажите один из параметров.
`--password`	Необязательный	Пароль учетной записи
`--description`	Необязательный	Описание
`--policy`	Необязательный	Политика, которую требуется применить к учетной записи
`--key-file`	Необязательный	Путь к файлу SSH-ключа, например: `.\id_rsa`
`--key-passphrase`	Необязательный	Пароль к файлу SSH-ключа

Примеры команд

Windows

Создать учетную запись

```
.\Pam.ConsoleApp.exe create-account `
--username Administrator `
--resource app01.local `
--password "Pass123$" `
--description "Local admin" `
--policy Default
```

Создать доменную учетную запись

```
 .\Pam.ConsoleApp.exe create-account --username Administrator --domain
dev.local
```

Создать учетную запись с SSH-ключом

```
 .\Pam.ConsoleApp.exe create-account `
 --username root `
 --resource linux01.local `
 --password "Pass123$" `
 --key-file .\id_rsa `
 --key-passphrase "Passphrase"
```

Linux

Создать учетную запись

```
 dotnet ./Pam.ConsoleApp.dll create-account `
--username Administrator `
--resource app01.local `
--password "Pass123$" `
--description "Local admin" `
--policy Default
```

Создать доменную учетную запись

```
dotnet ./Pam.ConsoleApp.dll create-account --username Administrator --
domain dev.local
```

Создать учетную запись с SSH-ключом

```
dotnet ./Pam.ConsoleApp.dll create-account `
--username root `
--resource linux01.local `
--password "Pass123$" `
--key-file .\id_rsa `
--key-passphrase "Passphrase"
```

Несколько учетных записей

Чтобы создать несколько учетных записей в Indeed PAM:

1. Создайте файл в формате CSV по следующему шаблону:

```
Location type;Location Name;Username;Set password;Password;Description;SSH key
file path;SSH key passphrase
```

Параметры

Параметр	Требование	Описание
`Location type`	Обязательный	Тип учетной записи: • `Local` — ресурсная; • `Domain` — доменная.
`Location Name`	Обязательный	Имя ресурса или домена
`Username`	Обязательный	Имя учетной записи
`Set password`	Обязательный	Задать для учетной записи пароль: • `true` — задать пароль; • `false` — создать учетную запись без пароля.
`Password`	Необязательный	Пароль учетной записи. Укажите, если для `Set password` указано `true`.
`Description`	Необязательный	Описание
`SSH key file path`	Необязательный	Путь к файлу SSH-ключа, например: `.\id_rsa`
`SSH key passphrase`	Необязательный	Пароль к файлу SSH-ключа

Пример CSV-файла

```
Local;dc.dev.local;root;true;root;Local account;;
Local;raspberrypi;root;true;root;SSH key example;id_rsa;passphrase
Domain;dev.local;Administrator;false;;Domain admin;;
```

2. Перейдите в папку с утилитой и выполните команду:

Windows

```
.\Pam.ConsoleApp.exe create-accounts-from-file --file <путь к файлу>
```

Linux

```
dotnet ./Pam.ConsoleApp.dll create-accounts-from-file --file <путь к файлу>
```

Удалить учетную запись

Чтобы удалить учетную запись из Indeed PAM:

1. Перейдите в папку с утилитой.
2. Выполните команду, указав имя учетной записи или ее идентификатор:

Windows

```
.\Pam.ConsoleApp.exe delete-account --name <имя учетной записи>
```

```
.\Pam.ConsoleApp.exe delete-account --id <идентификатор учетной записи>
```

Linux

```
dotnet ./Pam.ConsoleApp.dll delete-account --name <размещение\имя учетной
записи>
```

```
dotnet ./Pam.ConsoleApp.dll delete-account --id <идентификатор учетной записи>
```

Идентификатор отображается в URL-адресе в профиле учетной записи.

Примеры команд

Windows

Удалить учетную запись по имени

```
.\Pam.ConsoleApp.exe delete-account --name app01.local\User
```

Удалить учетную запись по идентификатору

```
.\Pam.ConsoleApp.exe delete-account --id a988f1b0-b871-43fa-a40c-6f4ac75f904c
```

Linux

Удалить учетную запись по имени

```
dotnet ./Pam.ConsoleApp.dll delete-account --name app01.local\Administrator
```

Удалить учетную запись по идентификатору

```
dotnet ./Pam.ConsoleApp.dll delete-account --id a988f1b0-b871-43fa-a40c-6f4ac75f904c
```

Операции с ресурсами

Создать ресурс

Один ресурс

Чтобы создать ресурс в Indeed PAM:

1. Перейдите в папку с утилитой.

2. Запустите утилиту с параметрами из таблицы:

Windows

```
.\Pam.ConsoleApp.exe create-resource <параметр> <значение>
```

Linux

```
dotnet ./Pam.ConsoleApp.dll create-resource <параметр> <значение>
```

Параметры

Параметр	Требование	Описание
`--name`	Обязательный	Имя ресурса
`--description`	Необязательный	Описание
`--dns-name` или `--ip-address`	Обязательный	Адрес ресурса: - `--dns-name` — DNS-имя; - `--ip-address` — IP-адрес. Можно указать один из параметров.
`--user-connection-type`	Обязательный	Тип пользовательского подключения. Подробнее о типах читайте в разделе **Пользовательское подключение**.
`--user-connection-address`	Необязательный	IP-адрес или DNS-имя пользовательского подключения
`--user-connection-port`	Необязательный	Порт пользовательского подключения
`--user-connection-matching-url`	Необязательный	URL-адрес страницы входа для веб-ресурса

Параметр	Требование	Описание
`--user-connection-matching-url-is-regex`	Необязательный	URL-адрес страницы входа является регулярным выражением: • `true` — является; • `false` — не является. Укажите, если задан параметр `UC matching url`.
`--service-account`	Необязательный	Имя сервисной учетной записи
`--service-connection-type`	Необязательный	Тип сервисного подключения. Подробнее о типах читайте в разделе **Сервисное подключение**.
`--service-connection-port`	Необязательный	Порт для сервисного подключения
`--service-ssh-template`	Необязательный	Имя шаблона SSH-коннектора. Укажите, если выбран тип сервисного подключения `SSH`.
`--cisco-privilege-mode-password`	Необязательный	Пароль для привилегированного входа Cisco. Укажите, если задан тип сервисного подключения `Cisco IOS`.
`--policy`	Необязательный	Политика, которую требуется применить к ресурсу

Примеры команд

Windows

Создать один ресурс

```
.\Pam.ConsoleApp.exe create-resource `
--name APP01 `
--description "Application server" `
--dns-name app01.local `
--user-connection-type RDP `
--user-connection-port 3389 `
--service-account DOMAIN\svc_app `
--service-connection-type Windows
```

Linux

Создать один ресурс

```
dotnet ./Pam.ConsoleApp.dll create-resource `
--name APP01 `
--description "Application server" `
--dns-name app01.local `
--user-connection-type RDP `
--user-connection-port 3389 `
--service-account DOMAIN\svc_app `
--service-connection-type Windows
```

Несколько ресурсов

Чтобы создать несколько ресурсов в Indeed PAM:

1. Создайте файл в формате CSV по следующему шаблону:

```
Name;Description;DNS name;IP address;UC type;UC address;UC port;UC matching
url;UC matching url is regex;SC account name;SC type;SC SSH template;SC
address;SC port;Cisco privilege mode password
```

Параметры

Параметр	Требование	Описание
`Name`	Обязательный	Имя ресурса
`Description`	Необязательный	Описание
`DNS name` или `IP address`	Обязательный	DNS-имя или IP-адрес ресурса. Можно указать один из параметров.
`UC type`	Обязательный	Тип пользовательского подключения. Подробнее о типах читайте в разделе **Пользовательское подключение**.
`UC address`	Необязательный	IP-адрес или DNS-имя пользовательского подключения
`UC port`	Необязательный	Порт пользовательского подключения
`UC matching url`	Необязательный	URL-адрес страницы входа для веб-ресурса
`UC matching url is regex`	Необязательный	URL-адрес страницы входа является регулярным выражением: - `true` — является; - `false` — не является. Укажите, если задан параметр `UC matching url`.
`SC account name`	Необязательный	Имя сервисной учетной записи
`SC type`	Необязательный	Тип сервисного подключения. Подробнее о типах читайте в разделе **Сервисное подключение**.
`SC SSH template`	Необязательный	Имя шаблона SSH-коннектора. Укажите, если выбран тип сервисного подключения `SSH`.

Параметр	Требование	Описание
`SC address`	Необязательный	IP-адрес или DNS-имя сервисного подключения
`SC port`	Необязательный	Порт для сервисного подключения
`Cisco privilege mode password`	Необязательный	Пароль для привилегированного входа Cisco. Укажите, если задан тип сервисного подключения `Cisco IOS`.

Пример CSV-файла

```
APP01;Application server;app01.local;;RDP;;;;;DOMAIN\svc_app;Windows;;;;
WEB01;Corporate
website;portal.local;;WebTemplate;https://portal.local/;;https://portal.local
SSH01;Linux server;;192.168.0.50;SSH;;;;;;;;;
```

2. Перейдите в папку с утилитой и выполните команду:

```
.\Pam.ConsoleApp.exe create-resources-from-file --file <путь к файлу>
```

Удалить ресурс

Чтобы удалить ресурс из Indeed PAM:

1. Перейдите в папку с утилитой.

2. Выполните команду, указав имя ресурса или его идентификатор:

Windows

```
.\Pam.ConsoleApp.exe delete-resource --name <имя ресурса>
```

```
.\Pam.ConsoleApp.exe delete-resource --id <идентификатор ресурса>
```

Linux

```
dotnet ./Pam.ConsoleApp.dll delete-resource --name <имя ресурса>
```

```
dotnet ./Pam.ConsoleApp.dll delete-resource --id <идентификатор ресурса>
```

Идентификатор отображается в URL-адресе в профиле ресурса.

Примеры команд

Windows

Удалить ресурс по имени

```
.\Pam.ConsoleApp.exe delete-resource --name app01.local
```

Удалить ресурс по идентификатору

```
.\Pam.ConsoleApp.exe delete-resource --id a988f1b0-b871-43fa-a40c-
6f4ac75f904c
```

Linux

Удалить ресурс по имени

```
dotnet ./Pam.ConsoleApp.dll delete-resource --name app01.local
```

Удалить ресурс по идентификатору

```
dotnet ./Pam.ConsoleApp.dll delete-resource --id a988f1b0-b871-43fa-a40c-
6f4ac75f904c
```

Операции с разрешениями

Создать разрешение

Одно разрешение

Чтобы создать разрешение в Indeed PAM:

1. Перейдите в папку с утилитой.
2. Запустите утилиту с параметрами из таблицы:

Windows

```
.\Pam.ConsoleApp.exe create-permission <параметр> <значение>
```

Linux

```
dotnet ./Pam.ConsoleApp.dll create-permission <параметр> <значение>
```

Параметры

Параметр	Требование	Описание
`--user`	Обязательный	Имя пользователя PAM в формате UPN
`--account`	Необязательный	Имя учетной записи PAM для подключения к ресурсу. Если не указать значение, при запуске сессии потребуется указать логин пароль учетной записи.
`--resources` или `--resources-group`	Обязательный	Имя ресурса или группы ресурсов Укажите в формате: • `<имя ресурса>:<тип подключения>` — для одного или нескольких ресурсов; • `<имя группы>` — для группы ресурсов.
`--active-from`	Необязательный	Период времени, когда разрешени станет активным. Укажите в формате `ДД.ММ.ГГГГ ЧЧ:ММ` или `ДД.ММ.ГГГГ`.
`--active-to`	Необязательный	Период времени, когда разрешени приостановит свое действие. Укажите в формате `ДД.ММ.ГГГГ ЧЧ:ММ` или `ДД.ММ.ГГГ`
`--schedule-time-from`	Необязательный	Время, когда разрешение можно использовать. Укажите в формате `ЧЧ:ММ`.
`--schedule-time-end`	Необязательный	Время, когда разрешение нельзя использовать. Укажите в формате `ЧЧ:ММ`.

Параметр	Требование	Описание
`--schedule-time-utc`	Необязательный	Преобразовывать заданное время доступа из текущего часового пояс в UTC: • `true` — использовать текущи часовой пояс; • `false` — преобразовать в UTC.
`--allow-to-view-creds`	Необязательный	Разрешить пользователю просматривать данные учетных записей, добавленных в разрешение: • `true` — разрешить; • `false` — не разрешать.
`--allow-to-change-creds`	Необязательный	Разрешить пользователю менять данные учетных записей, добавленных в разрешение: • `true` — разрешить; • `false` — не разрешать.

Примеры команд

Windows

Создать разрешение для нескольких ресурсов

```
.\Pam.ConsoleApp.exe create-permission `
  --user ivanov@domain.local `
  --account DOMAIN\Administrator `
  --resources srv01.local:RDP,srv02.local:SSH
```

Создать разрешение для группы ресурсов

```
.\Pam.ConsoleApp.exe create-permission `
  --user ivanov@domain.local `
  --account DOMAIN\Administrator `
  --resources-group PROD-SERVERS
```

Создать разрешение с временным ограничением

```
.\Pam.ConsoleApp.exe create-permission `
  --user ivanov@domain.local `
  --resources srv01.local:SSH `
  --active-from "01.08.2026 09:00" `
  --active-to "31.08.2026 18:00" `
  --schedule-time-from 08:00 `
  --schedule-time-end 21:59 `
  --schedule-time-utc true `
  --allow-to-view-creds true `
  --allow-to-change-creds true
```

Linux

Создать разрешение для нескольких ресурсов

```
dotnet ./Pam.ConsoleApp.dll create-permission `
  --user ivanov@domain.local `
  --account DOMAIN\Administrator `
  --resources srv01.local:RDP,srv02.local:SSH
```

Создать разрешение для группы ресурсов

```
dotnet ./Pam.ConsoleApp.dll create-permission `
  --user ivanov@domain.local `
  --account DOMAIN\Administrator `
  --resources-group PROD-SERVERS
```

Создать разрешение с временным ограничением

```
dotnet ./Pam.ConsoleApp.dll create-permission `
  --user ivanov@domain.local `
  --account resource\Administrator `
  --resources srv01.local:SSH `
  --active-from "01.08.2026 09:00" `
  --active-to "31.08.2026 18:00" `
  --schedule-time-from 08:00 `
  --schedule-time-end 21:59 `
  --schedule-time-utc true `
  --allow-to-view-creds true `
  --allow-to-change-creds true
```

Несколько разрешений

Чтобы создать несколько разрешений в Indeed PAM:

1. Создайте файл в формате CSV по следующему шаблону:

```
UserPrincipalName;AccountName;Resource1[:ConnectionType];Resource2[:ConnectionType
```

Параметры

Параметр	Требование	Описание
`UserPrincipalName`	Обязательный	Имя пользователя PAM в формате UPN
`AccountName`	Обязательный	Имя учетной записи в формате DOMAIN\user. Если не указать значение, при запуске сессии потребуется указать логин и пароль учетной записи.
`Resource[:ConnectionType]`	Обязательный	Имя ресурса и пользовательского подключения. Можно указать несколько ресурсов. Пример: `srv01.local:RDP;srv02.local:SSH`. Если у ресурса одно пользовательское подключение, тип подключения можно не указывать.

Пример CSV-файла

```
ivanov@domain.local;DOMAIN\Administrator;srv01.local:RDP;srv02.local:SSH
petrov@domain.local;;linux01.local:SSH
```

2. Перейдите в папку с утилитой и выполните команду:

Windows

```
.\Pam.ConsoleApp.exe create-permissions-from-file --file <путь к файлу>
```

Linux

```
dotnet ./Pam.ConsoleApp.dll create-permissions-from-file --file <путь к файлу>
```

Отозвать разрешение

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> Отозванные разрешения нельзя восстановить. Если требуется временно запретить использовать разрешение, то приостановите его действие.

Одно разрешение

Чтобы отозвать разрешение:

1. Перейдите в папку с утилитой.
2. Выполните следующую команду:

Windows

Отозвать разрешение по номеру

```
.\Pam.ConsoleApp.exe revoke-permissions --permissions <номера разрешений>
```

Отозвать разрешение пользователя

```
.\Pam.ConsoleApp.exe revoke-permissions-by-user <параметр> <значение>
```

Linux

Отозвать разрешение по номеру

```
dotnet ./Pam.ConsoleApp.dll revoke-permissions --permissions <номера
разрешений>
```

Отозвать разрешение пользователя

```
dotnet ./Pam.ConsoleApp.dll revoke-permissions-by-user <параметр> <значение>
```

Параметры

Параметр	Требование	Описание
`--user`	Обязательный	Имя пользователя PAM в формате UPN
`--account`	Необязательный	Имя учетной записи
`--resources` или `--resources-group`	Обязательный	Имя ресурса или группы ресурсов. Укажите один из параметров.

Примеры команд

Windows

Отозвать разрешения пользователя по ресурсам

```
.\Pam.ConsoleApp.exe revoke-permissions-by-user `
  --user ivanov@domain.local `
  --account DOMAIN\Administrator `
  --resources srv01.local:RDP,srv02.local:SSH
```

Отозвать разрешения пользователя по группе ресурсов

```
.\Pam.ConsoleApp.exe revoke-permissions-by-user `
  --user ivanov@domain.local `
  --account DOMAIN\Administrator `
  --resources-group PROD-SERVERS
```

Linux

Отозвать разрешения на ресурс

```
dotnet ./Pam.ConsoleApp.dll revoke-permissions-by-user `
  --user ivanov@domain.local `
  --account DOMAIN\Administrator `
  --resources srv01.local:RDP,srv02.local:SSH
```

Отозвать разрешения пользователя на группу ресурсов

```
dotnet ./Pam.ConsoleApp.dll revoke-permissions-by-user `
  --user ivanov@domain.local `
  --account DOMAIN\Administrator `
  --resources-group PROD-SERVERS
```

Несколько разрешений

Чтобы отозвать несколько разрешений в Indeed PAM:

1. Создайте файл в формате CSV по следующему шаблону:

```
UserPrincipalName;AccountName;Resource1[:ConnectionType];Resource2[:ConnectionType
```

Параметры

Параметр	Требование	Описание
`UserPrincipalName`	Обязательный	Имя пользователя PAM в формате UPN
`AccountName`	Обязательный	Имя учетной записи в формате DOMAIN\user. Если не указать значение, при запуске сессии потребуется указать логин и пароль учетной записи.
`Resource[:ConnectionType]`	Обязательный	Имя ресурса и пользовательского подключения. Можно указать несколько ресурсов. Пример: `srv01.local:RDP;srv02.local:SSH`

Пример CSV-файла

```
ivanov@domain.local;DOMAIN\Administrator;srv01.local:RDP;srv02.local:SSH
petrov@domain.local;;linux01.local:SSH
```

2. Перейдите в папку с утилитой и выполните команду:

```
.\Pam.ConsoleApp.exe revoke-permissions-from-file --file <путь к файлу>
```

После выполнения команды указанные разрешения переходят в состояние *Отозвано*.

Приостановить разрешение

Неиспользуемое разрешение — разрешение, которым не воспользовались в течение периода, заданного в настройках **Контроль использования PAM**. Рекомендуется отозвать или приостановить такое разрешение.

Чтобы приостановить неиспользуемые разрешения:

1. Перейдите в папку с утилитой.
2. Выполните следующую команду:

Windows

```
.\Pam.ConsoleApp.exe suspend-unused-permissions
```

Linux

```
dotnet ./Pam.ConsoleApp.dll suspend-unused-permissions
```

После выполнения команды все неиспользуемые разрешения переходят в состояние *Приостановлено*.
В любой момент разрешение можно возобновить.

Руководство пользователя

Консоль пользователя

Получите доступ к консоли пользователя

Подключение к ресурсу

Количество глав: 2

Интеграция с Ansible

Количество глав: 2

Работа с APPM

Количество глав: 3

Аутентификация в SSH Proxy по SSH-ключу

Аутентификация в SSH Proxy по SSH-ключу

Дополнительные утилиты

Количество глав: 2

Консоль пользователя

Консоль пользователя — веб-приложение для доступа к защищаемым объектам Indeed PAM. Через консоль можно подключиться к ресурсу и открыть сессию с учетом действующих разрешений. URL-адрес консоли формируется из доменного имени Indeed PAM.
Пример адреса: `https://pam.domain.local/uc`.

Консоль пользователя содержит несколько разделов:

- **Ресурсы** — основной раздел, в котором отображаются разрешения на подключение к ресурсам.
- **Учетные записи** — список учетных записей с возможностью просмотра и редактирования пароля и SSH-ключа.
  В разделе отображаются только те учетные записи, в разрешении которых включены опции **Разрешить просмотр учетных данных** и/или **Разрешить изменение учетных данных**.
- **Приложения** — список приложений, добавленных в Indeed PAM, с возможностью просмотра учетных данных.
  Просматривать пароли могут только администраторы приложений.

Аутентификация и второй фактор

1. Откройте консоль пользователя.

2. Введите логин в одном из форматов:

   - john.smith@space.local — формат UPN;
   - SPACE\john.smith — формат домен\пользователь;
   - john.smith — без доменной части.

   Если логин пользователя из внешнего каталога совпадает с логином внутреннего пользователя, для входа под учетной записью из каталога укажите логин вместе с доменом.

3. Введите пароль и нажмите **Войти**.

4. Введите второй фактор аутентификации и нажмите **Войти**.

Как настроить второй фактор

При первом входе в консоль настройте двухфакторную аутентификацию.
Чтобы зарегистрировать аутентификатор:

1. Установите приложение для генерации OTP.
2. Отсканируйте QR-код или введите ключ доступа.
3. В консоли пользователя введите одноразовый код аутентификации.
4. Нажмите **Зарегистрировать**.

После регистрации появится форма входа в консоль. Введите новый код из приложения для генерации OTP.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> При превышении числа неверных попыток ввода OTP пользователь блокируется по умолчанию на 10 минут. Число попыток и время блокировки задает администратор в разделе **Конфигурация → Аутентификация пользователей**.

Чтобы выйти из консоли, в правом верхнем углу нажмите на логин и выберите **Выйти**.

Сменить пароль пользователя PAM

Внутренний пользователь Indeed PAM может самостоятельно сменить свой пароль.
Чтобы сменить пароль:

1. Пройдите аутентификацию в консоли пользователя.
2. В правом верхнем углу нажмите на логин.
3. В выпадающем списке выберите **Сменить пароль**.
4. В открывшемся окне введите текущий и новый пароль.
5. (Опционально) Задайте опцию **Завершить все активные сессии**.
6. Нажмите **Сменить пароль**.

Работа с папками

Папки помогают организовать работу в консоли. Сгруппируйте ресурсы по нужному признаку, например по отделу или типу подключения. Чтобы отобразить меню с папками, в разделе **Ресурсы** нажмите » и выберите нужное действие:

- — создать новую папку;
- — редактировать название выбранной папки;
- — удалить выбранную папку.

Чтобы добавить ресурс в папку:

1. Перейдите в раздел **Ресурсы** и нажмите **Все ресурсы** или **Ресурсы без папки**.
2. Выберите один или несколько ресурсов и нажмите **Переместить**.

> **ПРИМЕЧАНИЕ**
> Произвольные ресурсы нельзя добавить в папку.

3. Выберите нужную папку и нажмите **Сохранить**.

Найти ресурс, учетную запись или приложение

Чтобы найти ресурс:

1. Перейдите в раздел **Ресурсы**.
2. Нажмите » и в раскрывшемся меню выберите, где искать ресурс.
3. В поисковой строке введите название ресурса, имя учетной записи, тип, адрес подключения или тег.

> **ПРИМЕЧАНИЕ**
> Произвольные ресурсы можно найти по запросу «adhoc».

Чтобы найти учетную запись или приложение:

1. Перейдите в раздел **Учетные записи** или **Приложения**.
2. В поисковой строке введите имя учетной записи или приложения.

Показать учетные данные

В консоли пользователя доступен просмотр паролей и SSH-ключей учетных записей, у которых в разрешении включена опция **Разрешить просмотр учетных данных**.
Чтобы просмотреть учетные данные:

1. Перейдите в раздел **Учетные записи**.

2. Нажмите **Показать учетные данные** напротив нужной учетной записи.
3. Введите причину просмотра и нажмите **Показать учетные данные**.

Просматривать учетные данные приложений могут только их администраторы.
Чтобы просмотреть пароль приложения:

1. Перейдите в раздел **Приложения**.
2. Нажмите **Показать учетные данные** напротив нужного приложения.
3. Введите причину просмотра и нажмите **Показать учетные данные**.

Сменить пароль или SSH-ключ

В консоли пользователя доступно редактирование пароля и SSH-ключа для учетных записей, у которых в разрешении включена опция **Разрешить изменение учетных данных**.
Чтобы сменить учетные данные:

1. Перейдите в раздел **Учетные записи**.
2. Нажмите ▼ и выберите нужное действие:
   - **Сменить пароль** — введите пароль и подтвердите его.
   - **Сменить SSH-ключ** — выберите файл SSH-ключа и введите его пароль. Поддерживаются ключи RSA в форматах OpenSSH и PEM, а также Ed25519 в формате OpenSSH.

Как сгенерировать SSH-ключ

Чтобы создать SSH-ключ и записать его в файл, воспользуйтесь программой PuTTYgen или одной из команд:

Ключ RSA в формате OpenSSH

```
ssh-keygen -t rsa -b 4096 -f id_rsa_openssh -C "RSA OpenSSH key"
```

Ключ RSA в формате PEM

```
ssh-keygen -t rsa -b 4096 -f id_rsa_pem -C "RSA PEM key" -m PEM
```

Ключ Ed25519 в формате OpenSSH

```
ssh-keygen -t ed25519 -f id_ed25519_openssh -C "Ed25519 OpenSSH key"
```

3. Укажите причину смены пароля или SSH-ключа и нажмите **Сохранить**.

Подключение к ресурсу



RDP, Web, SSH и SQL подключение

Ознакомьтесь со способами подключения к ресурсам



SCP и SFTP подключение

Количество глав: 3

RDP, Web, SSH и SQL подключение

В консоли пользователя Indeed PAM отображаются разрешения на доступ к ресурсам. По каждому столбцу, кроме столбца **Теги**, доступна сортировка. При поиске совпадения будут выводиться по всем столбцам.

Если пользователю доступны произвольные ресурсы, они будут отображаться в верхней части списка.

Подключение к ресурсу по RDP

Подключитесь к ресурсу с помощью RDP-файла или откройте сессию в новой вкладке браузера через Web-терминал.

По RDP-файлу

1. Нажмите ▼ напротив разрешения и выберите **Загрузить RDP-файл для подключения**.
2. Откройте скачанный файл и пройдите аутентификацию от имени пользователя Indeed PAM.
   Если администратор включил код аутентификации, учетные данные вводить не нужно.
3. (Опционально) Укажите причину для подключения, если это задано в политике.
4. Пройдите аутентификацию на ресурсе:
   - Если в разрешении указана учетная запись, произойдет вход от имени этой учетной записи.
   - Если разрешение выдано на пользовательскую учетную запись и аутентификация в Indeed PAM пройдена от имени пользователя PAM, его логин и пароль подставляются в форму входа на ресурсе.

> ⓘ **ПРИМЕЧАНИЕ**
> Если включены коды аутентификации, то при повторном использовании RDP-файла введите пароль пользователя.

Через Web-терминал

1. Нажмите ▼ напротив разрешения и выберите **Открыть через Web-терминал**.
2. Пройдите аутентификацию от имени пользователя Indeed PAM и укажите причину для подключения.
   Если администратор включил код аутентификации, учетные данные вводить не нужно.
3. (Опционально) Укажите причину для подключения, если это задано в политике.

4. Пройдите аутентификацию на ресурсе:
   - Если в разрешении указана учетная запись, произойдет вход от имени этой учетной записи.
   - Если разрешение выдано на пользовательскую учетную запись и аутентификация в Indeed PAM пройдена от имени пользователя PAM, его логин и пароль подставляются в форму входа на ресурсе.

Сессия откроется в новой вкладке браузера. Чтобы прервать сессию, закройте вкладку.

> ⓘ **ОГРАНИЧЕНИЯ БУФЕРА ОБМЕНА**
> Буфер обмена поддерживает работу только с текстовыми данными.

Подключение к шлюзу доступа

Шлюз доступа принимает подключение пользователя и отображает список ресурсов, доступных для запуска сессии.

Шлюз RDS

1. Нажмите **Подключиться к шлюзу доступа**.
2. Запустите скачанный RDP-файл.
3. Пройдите аутентификацию и настройте подключение.

Шлюз SSH

Подключитесь к шлюзу SSH из командной строки или с помощью SSH-клиента.

Командная строка

1. Откройте терминал.

2. Введите IP-адрес или DNS-имя для подключения к серверу доступа SSH или балансировщику.
   Чтобы узнать адрес, перейдите в консоль пользователя и скопируйте SSH-команду к любому ресурсу. Используйте значение, указанное после символа `@`. Если требуется, укажите путь до закрытого ключа.

   Шаблон команды подключения к SSH Proxy

```
ssh <логин пользователя>@<IP-адрес или DNS-имя> -p <номер порта> -i <путь до закрытого ключа>
```

Пример команды для подключения к SSH Proxy

```
ssh user@indeedproxy -p 2222 -i "C:\Users\user\.ssh\id_ed25519"
```

3. Пройдите аутентификацию. Если настроена аутентификация по SSH-ключу, пропустите этот шаг.
4. Выберите ресурс и подключитесь.

PuTTY

Аутентификация по паролю

1. Откройте приложение PuTTY.
2. В поле **Host Name (or IP address)** введите адрес SSH Proxy или балансировщика. Можно использовать IP-адрес или DNS-имя. Чтобы узнать адрес SSH Proxy, скопируйте SSH-команду к любому ресурсу в консоли пользователя и используйте значение, указанное после символа @.
3. Если требуется, укажите порт в поле **Port**.
4. В поле **Connection type** выберите *SSH*.
5. Нажмите **Open**.
6. Введите логин пользователя.
7. Введите пароль.
8. Введите OTP.
9. Выберите ресурс и подключитесь.

Аутентификация по SSH-ключу

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> Этот способ возможен только если настроена аутентификация по SSH-ключу и ключ сгенерирован утилитой PuTTYgen.

1. Откройте приложение PuTTY.
2. В поле **Host Name (or IP address)** введите адрес SSH Proxy или балансировщика. Можно использовать IP-адрес или DNS-имя. Чтобы узнать адрес SSH Proxy, скопируйте SSH-

команду к любому ресурсу в консоли пользователя и используйте значение, указанное после символа @.

3. Если требуется, укажите порт в поле **Port**.
4. В поле **Connection type** выберите *SSH*.
5. Откройте **Connection** → **Data**. Введите логин пользователя в поле **Auto-login-username**.
6. Откройте **Connection** → **SSH** → **Auth** → **Credentials**. Укажите закрытый ключ в поле **Private key file for authentication**.
7. Нажмите **Open**.
8. Введите OTP.
9. Выберите ресурс и подключитесь.

Аутентификация по сертификату

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> Этот способ возможен только если настроена аутентификация по SSH-ключу и установлен PuTTY CAC.

1. Откройте приложение PuTTY.
2. В поле **Host Name (or IP address)** введите адрес SSH Proxy или балансировщика. Можно использовать IP-адрес или DNS-имя. Чтобы узнать адрес SSH Proxy, скопируйте SSH-команду к любому ресурсу в консоли пользователя и используйте значение, указанное после символа @.
3. Если требуется, укажите порт в поле **Port**.
4. В поле **Connection type** выберите *SSH*.
5. Откройте **Connection** → **Data**. Введите логин пользователя в поле **Auto-login-username**.
6. Откройте **Connection** → **SSH** → **Certificate**. Нажмите **Set CAPI Cert**.
7. Нажмите **Open**.
8. Введите OTP.
9. Выберите ресурс и подключитесь.

MobaXterm

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> В версиях MobaXterm ниже 23.0 требуется отключить опцию **Fix connection issues** в разделе **Settings** → **Configuration** → **SSH**.

Аутентификация по паролю

1. Откройте приложение MobaXterm.

2. Нажмите **Sessions** → **New Session**.
3. Выберите **SSH**.
4. В **Remote host** укажите адрес SSH Proxy или балансировщика. Можно использовать IP-адрес или DNS-имя. Чтобы узнать адрес SSH Proxy, скопируйте SSH-команду к любому ресурсу в консоли пользователя и используйте значение, указанное после символа @.
5. Включите опцию **Specify username** и введите имя пользователя.
6. Если требуется, укажите порт в поле **Port**.
7. Нажмите **ОК**.
8. Введите пароль.
9. Введите OTP.
10. Выберите ресурс и подключитесь.

Аутентификация по SSH-ключу

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> Этот способ возможен только если настроена аутентификация по SSH-ключу.

1. Откройте приложение MobaXterm.
2. Нажмите **Sessions** → **New Session**.
3. Выберите **SSH**.
4. В **Remote host** укажите адрес SSH Proxy или балансировщика. Можно использовать IP-адрес или DNS-имя. Чтобы узнать адрес SSH Proxy, скопируйте SSH-команду к любому ресурсу в консоли пользователя и используйте значение, указанное после символа @.
5. Включите опцию **Specify username** и введите имя пользователя.
6. Если требуется, укажите порт в поле **Port**.
7. Откройте вкладку **Advanced SSH Settings**.
8. Включите опцию **Use private key** и укажите в этом поле закрытый ключ.
9. Нажмите **Expert SSH settings**.
10. В поле **SSH protocol version** укажите *SSHv2*.
11. Нажмите **ОК**.
12. Введите OTP.
13. Выберите ресурс и подключитесь.

SecureCRT

Аутентификация по паролю

1. Откройте приложение SecureCRT.
2. Нажмите **File** → **Quick Connect**.

3. В поле **Protocol** выберите *SSH2*.
4. В поле **Hostname** укажите адрес SSH Proxy или балансировщика. Можно использовать IP-адрес или DNS-имя. Чтобы узнать адрес SSH Proxy, скопируйте SSH-команду к любому ресурсу в консоли пользователя и используйте значение, указанное после символа @.
5. Если требуется, укажите порт в поле **Port**.
6. В поле **Username** введите имя пользователя.
7. Нажмите **Connect**.
8. Введите пароль.
9. Введите OTP.
10. Выберите ресурс и подключитесь.

Аутентификация по SSH-ключу

1. Откройте приложение SecureCRT.
2. Нажмите **File** → **Quick Connect**.
3. В поле **Protocol** выберите *SSH2*.
4. В поле **Hostname** укажите адрес SSH Proxy или балансировщика. Можно использовать IP-адрес или DNS-имя. Чтобы узнать адрес SSH Proxy, скопируйте SSH-команду к любому ресурсу в консоли пользователя и используйте значение, указанное после символа @.
5. Если требуется, укажите порт в поле **Port**.
6. В поле **Username** введите имя пользователя.
7. В группе **Authentication** включите опцию **PublicKey** и выключите все остальные.
8. Выделите **PublicKey** и нажмите ⚙.
9. Выберите опцию **Use session public key setting**.
10. Укажите закрытый ключ в поле **Use identity or certificate file**.
11. Нажмите **OK**.
12. Нажмите **Connect**.
13. Введите OTP.
14. Выберите ресурс и подключитесь.

Подключение к ресурсу по SSH

Подключитесь к ресурсу с помощью командной строки, SSH-клиента или запустите SSH-сессию в новой вкладке браузера через Web-терминал.

Командная строка
Подключение по команде из консоли пользователя

1. Нажмите ▼ напротив разрешения и выберите **Скопировать SSH-команду**.

2. Запустите скопированную команду в терминале.
   Если требуется указать причину для подключения, введите ее в команду после имени пользователя.

   Пример команды с указанием причины

   ```
   ssh "pamadmin@pam.local#10.10.1.191#LINUX-PAM.LOCAL\pam-admin#reason-for-connection#@pam.indeed-id.hq" -p 2222
   ```

3. Пройдите аутентификацию от имени пользователя Indeed PAM.
   Если администратор включил код аутентификации, учетные данные вводить не нужно.

   Пример команды с указанием причины и кодом аутентификации

   ```
   ssh "pamadmin@pam.local#10.10.1.191#LINUX-PAM.LOCAL\pam-admin#reason-for-connection#ZO3nNVdBFMKIGEs@pam.indeed-id.hq" -p 2222
   ```

4. Пройдите аутентификацию на ресурсе:

   - Если в разрешении указана учетная запись, произойдет вход от имени этой учетной записи.
   - Если разрешение выдано на пользовательскую учетную запись и аутентификация в Indeed PAM пройдена от имени пользователя PAM, его логин и пароль подставляются в строку подключения.
     Чтобы войти на ресурс, дважды нажмите **Enter**.

> ⓘ **ПРИМЕЧАНИЕ**
> Если включены коды аутентификации, то при повторном использовании команды введите пароль пользователя.

Подключение по команде с дополнительными параметрами

Вы можете написать SSH-команду вручную по указанному ниже шаблону.

1. Напишите SSH-команду по указанному 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; если причина содержит пробелы, укажите ее в кавычках.
- `proxy-address` — IP-адрес или DNS-имя сервера SSH Proxy.

Можно опустить любой параметр, кроме `proxy-address`. В этом случае SSH Proxy запросит эти параметры отдельно.

2. Запустите команду в терминале.

3. Пройдите аутентификацию.

Через Web-терминал

Чтобы открыть SSH-сессию в новой вкладке браузера:

1. Нажмите ▼ напротив разрешения и выберите **Открыть через Web-терминал**.
2. Пройдите аутентификацию от имени пользователя Indeed PAM.
   Если администратор настроил код аутентификации, учетные данные вводить не нужно.
3. (Опционально) Укажите причину для подключения, если это задано в политике.
4. Пройдите аутентификацию на ресурсе:
   - Если в разрешении указана учетная запись, произойдет вход от имени этой учетной записи.
   - Если разрешение выдано на пользовательскую учетную запись и аутентификация в Indeed PAM пройдена от имени пользователя PAM, его логин и пароль подставляются в строку подключения.
     Чтобы войти на ресурс, дважды нажмите **Enter**.

Сессия откроется в новой вкладке браузера. Чтобы прервать сессию, закройте вкладку.

> ⓘ **ОГРАНИЧЕНИЯ БУФЕРА ОБМЕНА**
> Буфер обмена поддерживает работу только с текстовыми данными.

PuTTY

1. Нажмите ▼ напротив разрешения и выберите **Скопировать SSH-команду**.
2. Откройте приложение PuTTY.

3. Вставьте скопированную строку в поле **Host Name (or IP address)**. Удалите из этой строки ssh, кавычки и указание порта.
4. Укажите порт в поле **Port**.
5. Нажмите **Open**.
6. Введите пароль и OTP.

MobaXterm

1. Откройте приложение MobaXterm.
2. Нажмите **Sessions** → **New Session**.
3. Выберите **SSH**.
4. В **Remote host** укажите адрес SSH Proxy или балансировщика. Можно использовать IP-адрес или DNS-имя. Чтобы узнать адрес SSH Proxy, скопируйте SSH-команду к любому ресурсу в консоли пользователя и используйте значение, указанное после символа @.
5. Включите опцию **Specify username**.
6. Введите имя пользователя. Указать можно в формате:
   `[user-name]#[resource]#[account-name]#[reason]`

   Пример указания дополнительных параметров в имени пользователя

   ```
   VDD\alex.shushkin#cent9en.vdd.com#CENT9EN\local##
   ```

7. Если требуется, укажите порт в поле **Port**.
8. Нажмите **OK**.
9. Введите пароль и OTP.

SecureCRT

1. Откройте приложение SecureCRT.
2. Нажмите **File** → **Quick Connect**.
3. В пункте **Protocol** выберите *SSH2*.
4. В поле **Hostname** укажите адрес SSH Proxy или балансировщика. Можно использовать IP-адрес или DNS-имя. Чтобы узнать адрес SSH Proxy, скопируйте SSH-команду к любому ресурсу в консоли пользователя и используйте значение, указанное после символа @.
5. Если требуется, укажите порт в поле **Port**.
6. В поле **Username** укажите имя пользователя.
   Указать можно в формате: `[user-name]#[resource]#[account-name]#[reason]`

Пример указания дополнительных параметров в имени пользователя

```
VDD\alex.shushkin#cent9en.vdd.com#CENT9EN\local##
```

7. Нажмите **Connect**.
8. Введите пароль и OTP.

Подключение к ресурсу через PostgreSQL Proxy

⚠ **ПРЕДУПРЕЖДЕНИЕ**

Для подключения к ресурсу PostgreSQL требуется отдельная лицензия.

Консольный клиент psql

1. Нажмите ▼ напротив разрешения и выберите **Скопировать команду для Psql**.
2. Запустите скопированную команду в терминале.
   Если требуется указать причину для подключения, введите ее в команду после имени пользователя.

   Пример команды без указания причины

   ```
    psql
   "postgresql://pamadmin%40pam.local%2310.10.1.105%23POSTGRESQL%5CAdmin@pam.indeed-id.hq:5432/postgres"
   ```

   Пример команды с указанием причины

   ```
    psql
   "postgresql://pamadmin%40pam.local%2310.10.1.105%23POSTGRESQL%5CAdmin%23reason-for-connection@pam.indeed-id.hq:5432/postgres"
   ```

3. Пройдите аутентификацию. Если администратор настроил запуск сессии без повторной аутентификации, учетные данные вводить не нужно.

Пример команды с указанием причины и кодом аутентификации

```
psql "postgresql://pamadmin%40pam.local%2310.10.1.105%23POSTGRESQL%23reason-for-connection%230C6XI9IrGx:nopassword@pam.indeed.hq:5432/postgres"
```

> ⓘ **ПРИМЕЧАНИЕ**
> Если включены коды аутентификации, то при повторном использовании команды введите пароль от учетной записи.

GUI-клиент СУБД

1. Откройте консоль пользователя Indeed PAM.
2. Нажмите **Показать данные для подключения**.
3. 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**
4. 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.
5. Введите в форме подключения пароль своей учетной записи PAM.

Подключение к ресурсу через MSSQL Proxy

> ⓘ **ПРИМЕЧАНИЕ**
> Для подключения к ресурсу MSSQL требуется отдельная лицензия.

Консольный клиент sqlcmd

1. Нажмите ▼ напротив разрешения и выберите **Скопировать команду для sqlcmd**.
2. Запустите скопированную команду в терминале.
   Если требуется указать причину для подключения, введите ее в команду после имени пользователя.

   Пример команды без указания причины

   ```
   sqlcmd -S pam.local,8081 -U ivan.ivanov#SQL -d master
   ```

   Пример команды с указанием причины

   ```
   sqlcmd -S pam.local,8081 -U ivan.ivanov#SQL#MSSQLuser#reason-for-connection -d master
   ```

3. Пройдите аутентификацию. Если администратор настроил запуск сессии без повторной аутентификации, учетные данные вводить не нужно.

   Пример команды с указанием причины и кодом аутентификации

   ```
   sqlcmd -S pam.local,8081 -U ivan.ivanov#SQL#MSSQLuser#reason-for-connection#C6XI9IrGx:nopassword -d master
   ```

   > ⓘ **ПРИМЕЧАНИЕ**
   > При повторном использовании команды требуется ввести пароль от учетной записи.

GUI-клиент СУБД

1. Откройте консоль пользователя Indeed PAM.
2. Нажмите **Показать данные для подключения**.
3. 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**

4. 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.

5. Введите в форме подключения пароль своей учетной записи PAM.

Подключение к ресурсу через Web Proxy

Подключитесь к веб-приложению или сайту через Web Proxy из консоли пользователя.

Открыть в новой вкладке

Чтобы открыть веб-ресурс в новой вкладке браузера:

1. Нажмите **Открыть в новой вкладке** напротив нужного разрешения.
2. Укажите причину для подключения и нажмите **Подтвердить**.

Сессия откроется в новой вкладке браузера. Чтобы прервать сессию, закройте вкладку.

> ⓘ **ОГРАНИЧЕНИЯ БУФЕРА ОБМЕНА**
> Буфер обмена поддерживает работу только с текстовыми данными.

По RDP-файлу

1. Нажмите ▼ напротив разрешения и выберите **Загрузить RDP-файл для подключения**.
2. Откройте скачанный файл и пройдите аутентификацию от имени пользователя Indeed PAM. Если администратор включил код аутентификации, учетные данные вводить не нужно.
3. (Опционально) Укажите причину для подключения, если это задано в политике.
4. Пройдите аутентификацию на ресурсе:
   - Если в разрешении указана учетная запись, произойдет вход от имени этой учетной записи.

- Если разрешение выдано на пользовательскую учетную запись и аутентификация в Indeed PAM пройдена от имени пользователя PAM, его логин и пароль подставляются в форму входа на ресурсе.

> ⓘ **ПРИМЕЧАНИЕ**
> Если включены коды аутентификации, то при повторном использовании RDP-файла введите пароль пользователя.

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.

> ⓘ **ПРИМЕЧАНИЕ**
> Для подключения к произвольному ресурсу требуется отдельная лицензия.

1. Нажмите **Указать адрес подключения** справа от 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 к произвольному ресурсу с разными типами подключений, а в окне **Подключение к произвольному ресурсу** в поле **Тип подключения** нет нужных вариантов, то проверьте **Расписание доступа** разрешений.
>
> Тип подключения не отображается 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.

SCP и SFTP подключение



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 выше 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 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 Windows или Linux для передачи файлов можно использовать утилиту sftp.

Чтобы передать файлы:

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 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 Windows 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 будет скопирована полностью со своим содержимым. Без этого ключа можно копировать только отдельные файлы.

PSFTP

На устройствах под управлением ОС Windows для передачи файлов можно использовать утилиту psftp.

Чтобы передать файлы:

1. Запустите командную строку.
2. Введите команду psftp.
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:

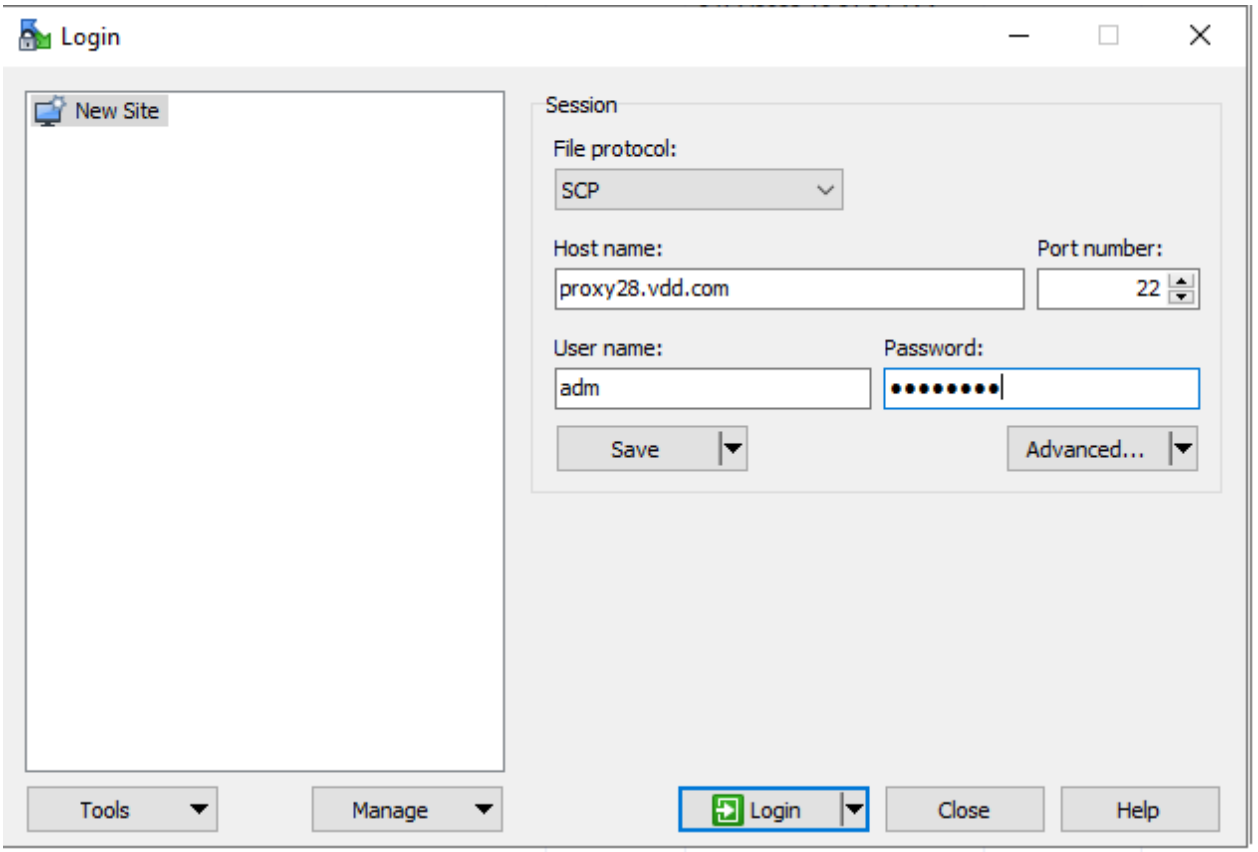
   ```
   put -r C:\temp\configs\ /tmp/configs
   put -r Путь_до_локальных_файлов Путь_до_файлов_на_ресурсе
   ```

   Ключ `-r` означает рекурсивное копирование, то есть, если указать для копирования папку, то она 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.

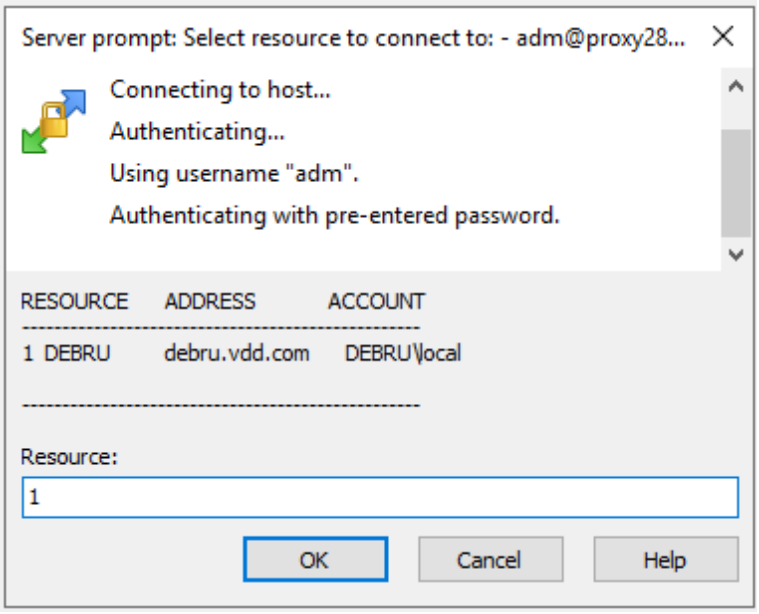
WinSCP

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".

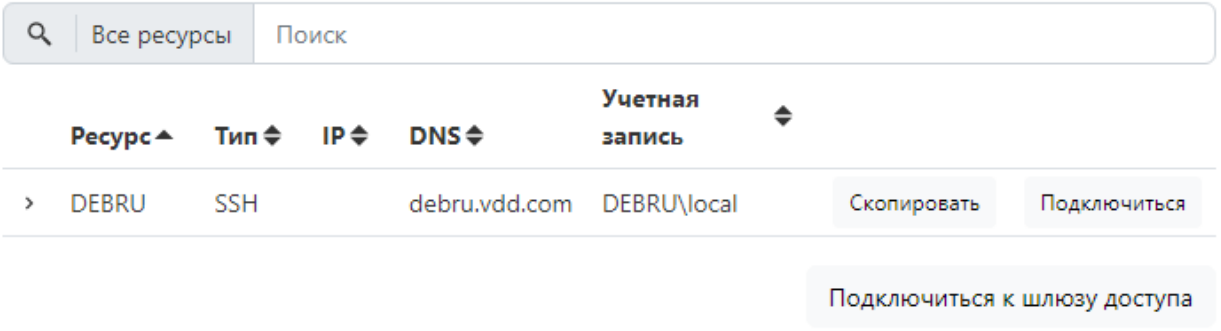


3. Нажмите "Login" и выберите ресурс, к которому хотите подключиться



Подключение напрямую к ресурсу

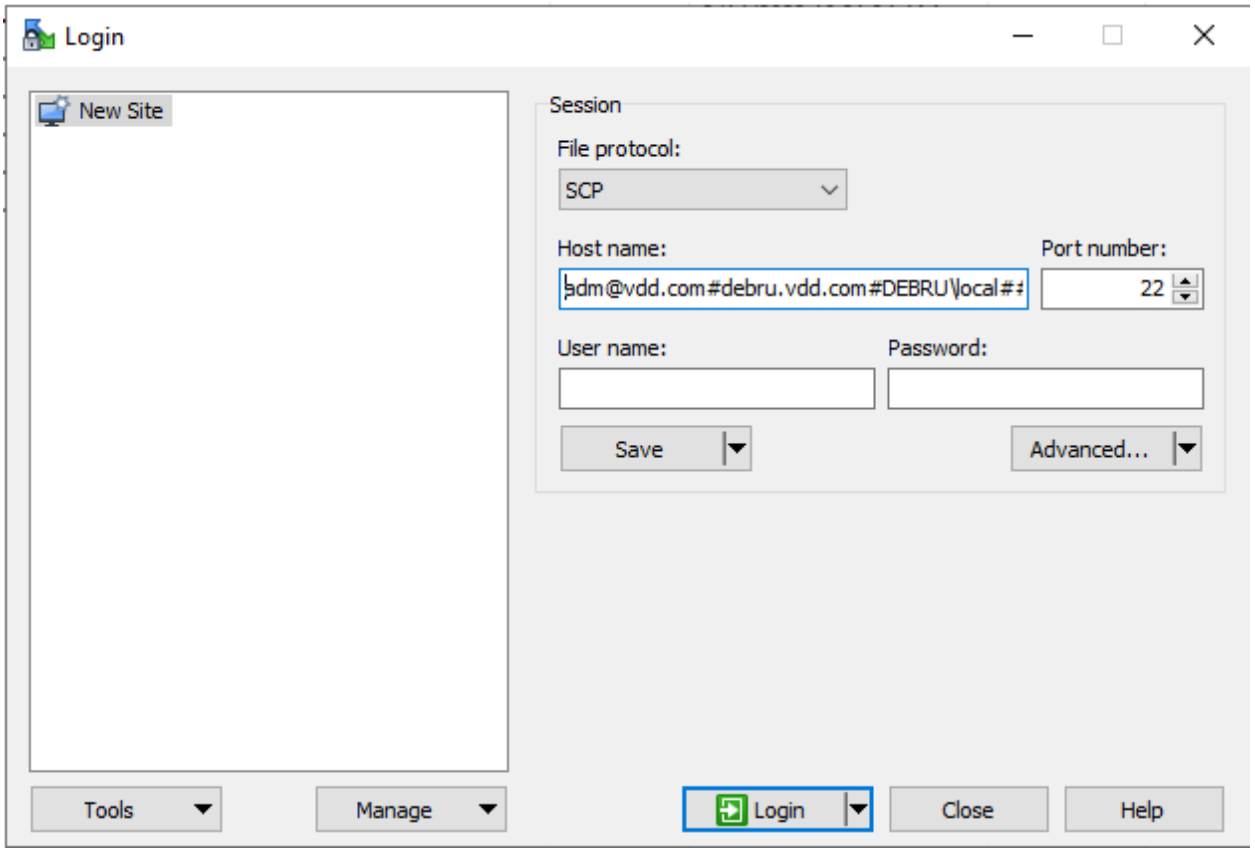
1. Перейдите в консоль пользователя и скопируйте строку подключения к ресурсу.



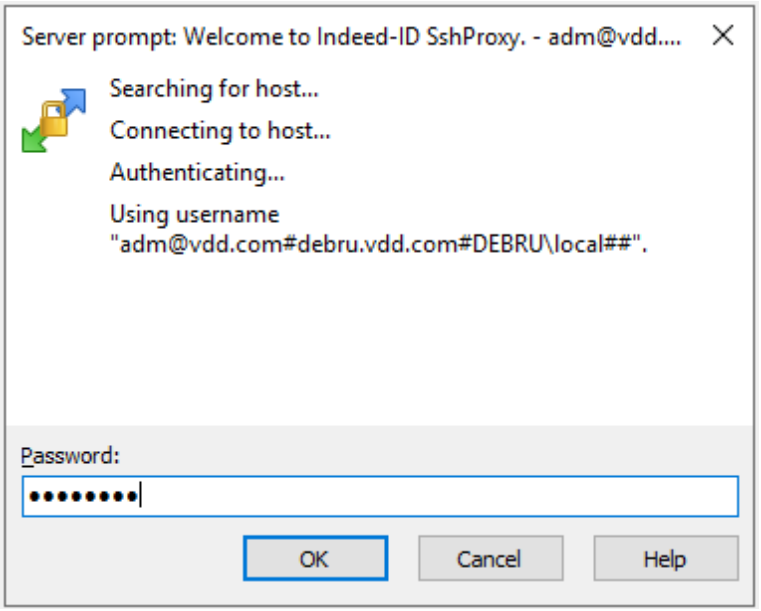
2. Откройте клиент WinSCP.

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.

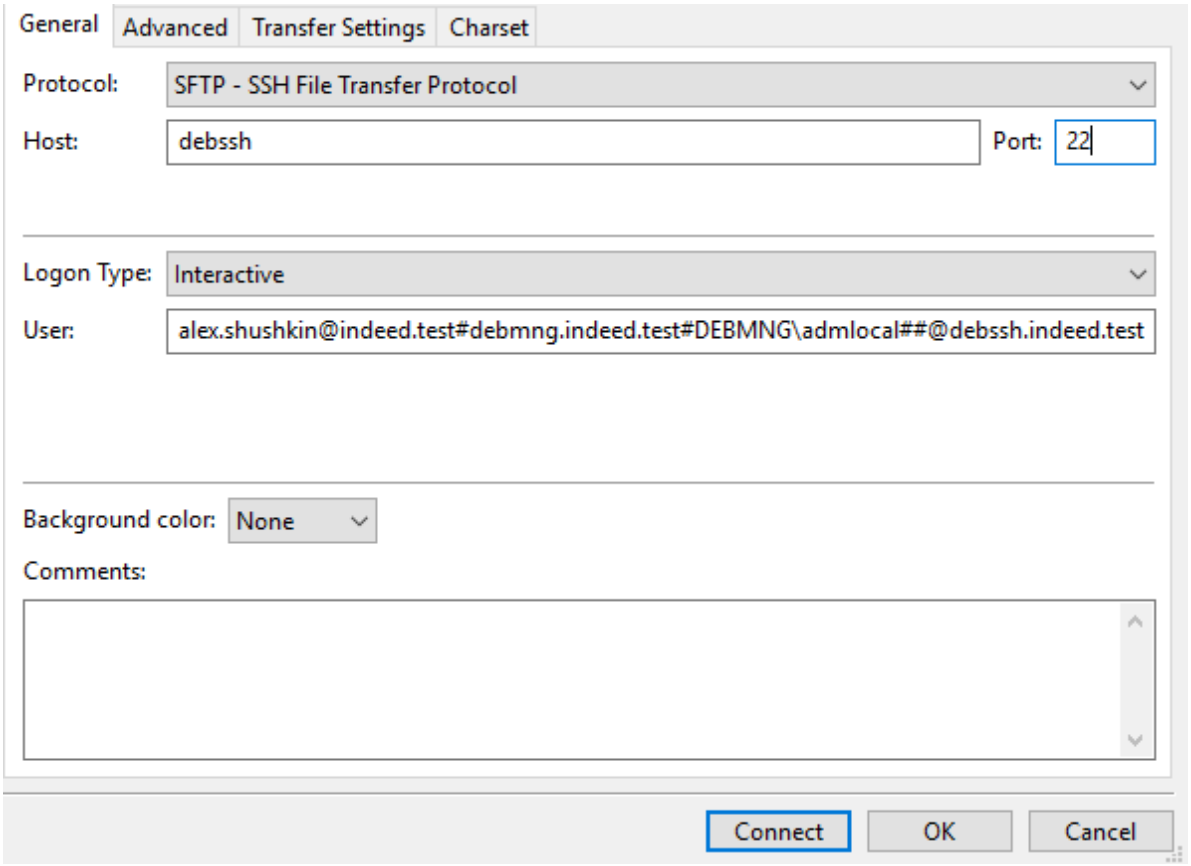


FileZilla

SFTP подключение к ресурсу

Чтобы настроить SFTP-подключение в клиенте FileZilla, выполните следующие действия:

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 требуется 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 **Connect**.

> **ПРИМЕЧАНИЕ**
>
> FileZilla не поддерживает SCP-соединение.

Интеграция с Ansible



Ansible Lookup Plugin

Управление учетными данными в Ansible-плейбуках



Подключение через SSH Proxy

Подключение к ресурсам через прокси-сервер Indeed PAM

Ansible Lookup Plugin

С помощью Lookup Plugin можно управлять учетными данными Indeed PAM прямо в Ansible-плейбуках.
Все запросы на получение и просмотр учетных данных записываются в журнал **События**.

> **ПРИМЕЧАНИЕ**
> Для управления данными учетных записей Indeed PAM используется метод Application to Application Password Management (AAPM).

Требования

Для работы с Ansible Lookup Plugin требуется:

- Python 3.9 и выше
- Ansible 2.14 и выше
- AAPM-лицензия

Предварительные действия

Чтобы настроить работу с Ansible Lookup Plugin:

1. Перейдите в папку с пакетом AAPM для Python SDK и выполните команду:

   ```
   pip install pam_aapm-3.4.0-py3-none-any.whl
   ```

2. Перейдите в папку с дистрибутивом Lookup Plugin для Ansible Collection и выполните команду:

   ```
   ansible-galaxy collection install indeed-pam-3.4.0.tar.gz
   ```

3. Перейдите в консоль администратора Indeed PAM и добавьте приложение.
4. Для приложения добавьте разрешение с включенной опцией **Разрешить просмотр учетных данных**.
   Разрешение позволит приложению использовать пароли и SSH-ключи учетных записей PAM.
5. Назначьте администраторов приложения, которые могут просматривать его пароль.
6. Откройте консоль пользователя Indeed PAM и перейдите на вкладку **Приложения**.

7. Просмотрите пароль от приложения и сохраните его.

Далее настройте конфигурацию Ansible и получите доступ к серверу Indeed PAM.

Настройка Ansible

Чтобы установить соединение с сервером Indeed PAM и получить токены доступа, настройте конфигурацию Ansible одним из способов:

- Конфигурационный файл *ansible.cfg* — укажите переменные в файле, если конфигурация между запусками сценария не меняется. Рекомендуется шифровать учетные данные или передавать их через переменные окружения.
- Переменные окружения — укажите переменные в терминале перед запуском сценария. Переменные существуют только в рамках текущей сессии. Рекомендуется использовать в CI/CD-автоматизациях.
- Ansible-плейбук — передайте параметры как именованные аргументы при вызове функции `lookup()`. Способ подходит, когда нужно обратиться к другому серверу или переопределить параметр, например `ca_cert`.

Подробнее о работе сценария, если конфигурация определена в нескольких местах, — в документации Ansible.

Параметры конфигурации

Параметр	Переменная окружения	Требование	Описание
`idp_server`	`PAM_IDP_SERVER`	Обязательный	URL-адрес компонента Indeed PAM IdP
`core_server`	`PAM_CORE_SERVER`	Обязательный	URL-адрес компонента Indeed PAM Core
`username`	`PAM_USERNAME`	Обязательный	Название приложения
`password`	`PAM_PASSWORD`	Обязательный	Пароль указанного приложения. Администратор приложения может просмотреть пароль в консоли пользователя.
`timeout`	`PAM_TIMEOUT`	Необязательный	Время ожидания ответа на запрос, сек. Значение по умолчанию: `30.0`.
`verify_ssl`	`PAM_VERIFY_SSL`	Необязательный	Проверка SSL-сертификата сервера: • `True` — требуется; • `False` — не требуется. Значение по умолчанию: `True`. **Примечание:** Включенная проверка уменьшает риск перехвата данных. Если вы отключили проверку — рекомендуется обратить на это внимание в скрипте и оставить комментарий.
`ca_cert`	`PAM_CA_CERT`	Необязательный	Путь к сертификату для проверки SSL-соединения. Укажите, если сервер PAM использует сертификат, подписанный внутренним УЦ. Сертификат должен быть в формате PEM. Пример: `ca_cert="/path/to/ca.crt"`. Значение по умолчанию: `None`.

Примеры

Файл ansible.cfg

```
[pam]
idp_server = https://pam.company.com/idp
core_server = https://pam.company.com/core
username = my-app
password = your-app-password
timeout = 30
verify_ssl = true
ca_cert = /path/to/ca.crt
```

Переменные окружения

```
export PAM_IDP_SERVER="https://pam.company.com/idp"
export PAM_CORE_SERVER="https://pam.company.com/core"
export PAM_USERNAME="my-app"
export PAM_PASSWORD="your-app-password"
export PAM_VERIFY_SSL="true"
export PAM_CA_CERT="/path/to/ca.crt"
export PAM_TIMEOUT="30"
```

Ansible-плейбук

```
- name: Получить пароль с явным указанием сервера
  ansible.builtin.set_fact:
    db_password: "{{ lookup('indeed.pam.get_password', 'SERVER/admin',
                            idp_server='https://pam.company.com/idp',
                            core_server='https://pam.company.com/core',
                            username='my-app',
                            password='app-password') }}"
  no_log: true
```

После настройки доступа используйте плагины, чтобы получить учетные данные.

Плагины

> **ПРИМЕЧАНИЕ**
> Используйте параметр `no_log: true`, чтобы не выводить учетные данные в консоль после завершения задачи.

Плагины Ansible вызываются через функцию `lookup()` и позволяют получить из Indeed PAM:

- пароль учетной записи;
- SSH-ключ учетной записи;
- список доступных учетных записей.

`get_password`

Плагин используется для получения пароля учетной записи PAM.

Параметры `get_password`

Параметр	Требование	Описание
`_terms`	Обязательный	Имя учетной записи в формате: • `LOCATION/username` — рекомендуемый формат; • `LOCATION\username` — требует экранирования в Python-скриптах, например `"SERVER\\admin"`. Передается вторым аргументом после имени плагина.
`reason`	Необязательный	Причина получения учетных данных. Указание причины определяется политикой, действующей на учетную запись.
`errors`	Необязательный	Режим обработки ошибок: • `strict` — выводит ошибку и прерывает выполнение задачи. Используйте, когда выполнение сценария без пароля невозможно. • `warn` — выводит предупреждение и присваивает переменной пустую строку. Используйте, если отсутствие пароля не влияет на сценарий. • `ignore` — не выводит сообщений и присваивает переменной пустую строку. Используйте, если ошибку обрабатываете самостоятельно.

```
- name: Получить пароль администратора
  ansible.builtin.set_fact:
    admin_password: "{{ lookup('indeed.pam.get_password', 'PROD-SERVER/admin',
                               reason='Обслуживание', errors='strict') }}"
  no_log: true
```

get_key

Плагин используется для получения SSH-ключа учетной записи PAM.

Параметры get_key

Параметр	Требование	Описание
_terms	Обязательный	Имя учетной записи в формате: • LOCATION/username — рекомендуемый формат; • LOCATION\username — требует экранирования в Python-скриптах, например "SERVER\\admin". Передается вторым аргументом после имени плагина.
decrypt	Необязательный	Вернуть расшифрованный SSH-ключ: • True — вернуть; • False — не возвращать. Значение по умолчанию: True.
reason	Необязательный	Причина получения учетных данных. Указание причины определяется политикой, действующей на учетную запись.
errors	Необязательный	Режим обработки ошибок: • strict — выводит ошибку и прерывает выполнение задачи. Используйте, когда выполнение сценария без SSH-ключа невозможно. • warn — выводит предупреждение и присваивает переменной пустую строку. Используйте, если отсутствие SSH-ключа не влияет на сценарий. • ignore — не выводит сообщений и присваивает переменной пустую строку. Используйте, если ошибку обрабатываете самостоятельно.

Параметры ответа

Параметр	Описание
Если в запросе `decrypt=True`	
`key`	SSH-ключ учетной записи в формате PEM
Если в запросе `decrypt=False`	
`key`	Зашифрованный SSH-ключ
`passphrase`	Пароль зашифрованного ключа

```yaml
# Расшифрованный ключ (по умолчанию)
- name: Развернуть SSH-ключ
  ansible.builtin.copy:
    content: "{{ lookup('indeed.pam.get_key', 'LINUX-SERVER/automation',
                              reason='Обслуживание', errors='warn')) }}"
    dest: /home/deploy/.ssh/id_rsa
    mode: '0600'
  no_log: true

# Зашифрованный ключ с паролем
- name: Получить SSH-ключ и его пароль
  ansible.builtin.set_fact:
    ssh_creds: "{{ lookup('indeed.pam.get_key', 'LINUX-SERVER/automation',
                          decrypt=false) }}"
  no_log: true
```

`get_accounts`

Плагин используется для получения списка доступных учетных записей PAM и не требует дополнительных параметров.

Параметры ответа

Ответ содержит список учетных записей в формате словаря (dict) с параметрами из таблицы.

Параметр	Описание
`display_name`	Имя учетной записи
`requires_reason`	Требуется ли согласно политике указывать причину для просмотра учетных данных: • `true` — требуется; • `false` — не требуется.

```
- name: Показать доступные учетные записи
  ansible.builtin.debug:
    msg: "{{ lookup('indeed.pam.get_accounts') }}"

- name: Показать только имена учетных записей
  ansible.builtin.debug:
    msg: "{{ lookup('indeed.pam.get_accounts') | map(attribute='display_name') | list
}}"
```

Использование Ansible Vault

Рекомендуется не хранить учетные данные в открытом виде и шифровать их с помощью компонента Ansible Vault.

Чтобы зашифровать пароль приложения:

1. Откройте терминал и выполните команду для шифрования пароля:

   ```
   ansible-vault encrypt_string --ask-vault-pass '<password>' --name '<variable>'
   ```

   - `password` — пароль приложения Indeed PAM, который нужно зашифровать;
   - `variable` — имя переменной для шифрования.

2. Введите пароль, который используется для расшифровки переменной при запуске плейбука. В результате в терминале отобразится зашифрованная переменная.

3. Создайте файл в формате YAML или JSON и сохраните в него результат команды.

YAML

```
vault_pam_password: !vault |
          $ANSIBLE_VAULT;1.1;AES256

31643864386664376639656162346664313937633035346638656139376138656163376638656164

63376639613839646661376339306264396566376661376 60a313233343536373839306162636465 66

30313233343536373839616263646566303132333435363738396162636465660a6162636465663132
```

JSON

```
{
    "vault_pam_password":
"$ANSIBLE_VAULT;1.1;AES256\n31643864386664376639656162346664313937633035346638656 1
}
```

4. Укажите переменную в плейбуке:

   - Для параметра `vars_files` укажите путь к файлу, в котором хранится зашифрованная переменная.
   - Для параметра `password` укажите имя переменной.

Пример

```
- name: Получить пароль с использованием Vault
  hosts: localhost
  gather_facts: false
  vars_files:
    - ./vault.yml
  tasks:
    - name: Запросить пароль учетной записи из PAM
      ansible.builtin.set_fact:
        db_password: "{{ lookup('indeed.pam.get_password',
                                'SERVER/admin',
                                idp_server='https://pam.company.com/idp',
                                core_server='https://pam.company.com/core',
                                username='my-app',
                                password=vault_pam_password) }}"
      no_log: true
```

Рекомендации по безопасности

1. Используйте параметр `no_log: true`, чтобы не выводить учетные данные в консоль при завершении задачи.
2. Не храните пароли в открытом виде — используйте Ansible Vault для шифрования учетных данных.
3. Проверка SSL-подключения включена по умолчанию. Отключайте ее только для тестирования в изолированных средах.
4. При одновременном запуске сценария на разных хостах рекомендуется указывать адрес хоста в причину подключения. Пример: `reason='host={{ ansible_host }}; operation=maintenance'`.

Подключение через SSH Proxy

Indeed PAM поддерживает подключение Ansible к ресурсам через прокси-сервер. При таком сценарии Ansible подключается к компоненту SSH Proxy, который предоставляет доступ к ресурсам по протоколам SSH, SCP и SFTP.

Компонент устанавливает соединение с ресурсом от имени указанной учетной записи, контролирует доступ к нему и записывает все действия на ресурсе в журналы **События**, **Активные сессии** и **Все сессии**.

> **ОГРАНИЧЕНИЯ**
> В сценарии работы Ansible через SSH Proxy не поддерживается двухфакторная аутентификация.

Требования

Для работы Ansible через SSH Proxy требуется:

- Ansible 2.14 и выше
- Доступ к компоненту Indeed PAM SSH Proxy
- Учетная запись Indeed PAM, имеющая доступ к целевому ресурсу
- AAPM-лицензия, если используется Ansible Lookup Plugin

Настройка подключения

Чтобы настроить подключение из Ansible-плейбука через SSH Proxy:

1. Сформируйте строку подключения к SSH Proxy в кодировке UTF-8 по шаблону:

   ```
   <pam_user>#<resource_address>#<account_name>#[reason]
   ```

   - `pam_user` — имя пользователя Indeed PAM для аутентификации в SSH Proxy.
   - `resource_address` — IP-адрес или DNS-имя целевого ресурса.
   - `account_name` — имя учетной записи, под которой пользователь подключается к целевому ресурсу.
   - `reason` — причина подключения к ресурсу, если ее требуется указать согласно политике.

   Пример: `pam.admin#192.168.0.100#PAM.LOCAL\pam-admin#Обслуживание`

2. Настройте конфигурацию Ansible для подключения к Indeed PAM в одном из файлов:

   - Ansible-плейбук — укажите параметры в секции `vars`.
   - Конфигурационный файл *inventory* — укажите параметры в секции `hosts`.

Параметры конфигурации

Параметр	Требование	Описание
`ansible_host`	Обязательный	DNS-имя или IP-адрес компонента SSH Proxy
`ansible_port`	Обязательный	Порт компонента SSH Proxy. Порт по умолчанию: `2222`
`ansible_user`	Обязательный	Строка подключения к SSH Proxy. Пример: `pam.admin#10.0.0.1#DOMAIN\admin`.
`ansible_password`	Необязательный	Пароль пользователя PAM. Укажите, если настроена аутентификация по паролю. Рекомендуется шифровать пароль с помощью Ansible Vault.
`ansible_ssh_private_key_file`	Необязательный	Путь к SSH-ключу пользователя PAM. Укажите, если настроена аутентификация по SSH-ключу. Пример: `/home/user/.ssh/id_rsa`.
`ansible_ssh_retries`	Необязательный	Количество повторных попыток подключения. Используйте, если необходимо подключиться заново после обрыва соединения или закрытия сессии в консоли администратора.

Примеры

Ansible-плейбук

```yaml
- name: Выполнить команду через PAM SSH Proxy
  hosts: all
  gather_facts: false

  vars:
    ansible_host: "pam.company.com"
    ansible_port: 2222
    ansible_user: "pam.admin#192.168.0.100#DOMAIN\\admin"
    ansible_password: "{{ pam_password }}"

  tasks:
    - name: Получить информацию о системе
      ansible.builtin.raw: uname -a
      register: result
      changed_when: false

    - name: Показать результат
      ansible.builtin.debug:
        msg: "{{ result.stdout | trim }}"
```

Файл inventory

Один ресурс

```yaml
---
all:
  hosts:
    target_server:
      ansible_host: pam.company.com
      ansible_port: 2222
      ansible_user: "pam.admin#192.168.0.100#DOMAIN\\admin"
      ansible_password: "{{ vault_pam_password }}"
```

Несколько ресурсов

```yaml
---
all:
  vars:
    ansible_port: 2222
    ansible_host: pam.company.com
    ansible_password: "{{ vault_pam_password }}"

  hosts:
    web_server:
      ansible_user: "pam.admin#10.11.5.10#DOMAIN\\web-admin"

    db_server:
      ansible_user: "pam.admin#10.11.5.20#DOMAIN\\db-admin"

    app_server:
      ansible_user: "pam.admin#190.160.1.100#LINUX-SERVER\\db-admin#Обслуживание"
```

Запуск сценария

Чтобы запустить сессию, откройте терминал и выполните команду для подключения к ресурсу через SSH Proxy:

```
ansible-playbook <playbook> [-i <inventory>] [-e <variable>]
```

- `playbook` — название Ansible-плейбука;
- `inventory` — имя конфигурационного файла с настройками подключения;
- `variable` — имя переменной окружения.

Примеры команд запуска

Настройки подключения указаны в плейбуке

```
ansible-playbook playbook.yml
```

Настройки подключения указаны в конфигурационном файле

```
ansible-playbook playbook.yml -i inventory.yml
```

Использование переменной окружения

```
ansible-playbook playbook.yml -i inventory.yml -e "pam_password=${PAM_PASSWORD}"
```

Использование Ansible Vault

Рекомендуется не хранить учетные данные в открытом виде и шифровать их с помощью компонента Ansible Vault.

Чтобы зашифровать пароль пользователя PAM:

1. Откройте терминал и выполните команду для шифрования пароля:

   ```
   ansible-vault encrypt_string --ask-vault-pass '<password>' --name '<variable>'
   ```

   - `password` — пароль пользователя Indeed PAM, который нужно зашифровать;
   - `variable` — имя переменной для шифрования.

2. Введите пароль, который используется для расшифровки переменной при запуске плейбука. В результате в терминале отобразится зашифрованная переменная.

3. Создайте файл в формате YAML или JSON и сохраните в него результат команды.

YAML

```
vault_pam_password: !vault |
          $ANSIBLE_VAULT;1.1;AES256

31643864386664376639656162346664313937633035346638656139376138656163376638656164

63376639613839646661376339306264396566376661376 60a313233343536373839306162636465 66

30313233343536373839616263646566303132333435363738396162636465660a6162636465663132
```

JSON

```
{
    "vault_pam_password":
"$ANSIBLE_VAULT;1.1;AES256\n31643864386664376639656162346664313937633035346638656 1
}
```

4. Укажите переменную в плейбуке:

   - Для параметра `vars_files` укажите путь к файлу, в котором хранится зашифрованная переменная.
   - Для параметра `password` укажите имя переменной.

Пример

```
---
- name: Выполнить команду через PAM SSH Proxy с использованием Ansible Vault
  hosts: all
  gather_facts: false
  vars_files:
    - ./vault.yml

  vars:
    ansible_host: "pam.company.com"
    ansible_port: 2222
    ansible_user: "pam.admin#192.168.0.100#PAM.LOCAL\\pam-admin"
    ansible_password: "{{ vault_pam_password }}"

  tasks:
    - name: Проверить подключение
      ansible.builtin.raw: id
      register: result
      changed_when: false
      no_log: true
```

Рекомендации по безопасности

1. Для аутентификации сервера и сценариев автоматизации перед первым подключением к PAM добавьте публичный ключ компонента SSH Proxy в файл *known_hosts*:

```
ssh-keyscan [-p <port>] <host> >> ~/.ssh/known_hosts
```

   - `port` — порт компонента SSH Proxy;
   - `host` — DNS-имя или IP-адрес компонента SSH Proxy.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> Убедитесь в подлинности ключа: команда `ssh-keyscan` использует механизм Trust on first use (TOFU), при котором ключ добавляется без проверки.
>
> Не отключайте проверку публичного ключа (`StrictHostKeyChecking=no`) — это снижает безопасность.

2. Не храните пароли в открытом виде — используйте Ansible Vault для шифрования учетных данных.

3. Используйте параметр `no_log: true`, чтобы учетные данные не попадали в логи Ansible при завершении задачи.

4. В CI/CD-сценариях передавайте пароль и SSH-ключ через переменные окружения.

5. Для повышения безопасности и оптимизации работы, рекомендуется использовать следующие параметры:

    - `gather_facts: false` — отключает сбор информации о хосте, что позволяет избежать появления в логах команд запуска Python-скриптов.

    - `no_log: true` — отключает вывод в консоль и запись в логи Ansible. Используйте для задач с учетными данными.

    - `become: true` и `become_method: sudo` — повышает привилегии пользователя для выполнения команд, требующих прав `root`.

    - Модуль `raw` — позволяет выполнять команды через SSH Proxy без установки Python на целевом ресурсе и предоставляет информативный лог в профиле сессии в консоли администратора.

Пример сценария

```yaml
---
- name: Выполнить команду через PAM SSH Proxy
  hosts: all
  gather_facts: false
  become: true
  become_method: sudo

  vars:
    ansible_host: "pam.company.com"
    ansible_port: 2222
    ansible_user: "pam.admin#10.10.5.190#PAM.LOCAL\\pam-admin"
    ansible_password: "{{ pam_password }}"

  tasks:
    - name: Выполнить команду (учетные данные скрыты)
      ansible.builtin.raw: uname -a
      register: result
      changed_when: false
      no_log: true

    - name: Показать результат команды (лог отображается)
      ansible.builtin.debug:
        msg: "{{ result.stdout | trim }}"
      no_log: false
```

Работа с APPM

Python SDK

Интеграция Indeed PAM в Python-приложения и скрипты автоматизации

AAPM API

Взаимодействие с AAPM через интерфейс API

Консольная утилита

Получение учетных данных с помощью утилиты

Python SDK

Python SDK предоставляет API для получения паролей и SSH-ключей учетных записей Indeed PAM. Решение подходит для интеграции PAM в CI/CD-автоматизации, Python-скрипты, системы оркестрации и в другие процессы, где требуется безопасно управлять учетными данными.

Все запросы на получение и просмотр учетных данных записываются в журнал **События**.

> ⚠ **ТРЕБОВАНИЯ**
> Для работы с Python SDK требуется Python 3.9 и выше.

> ⓘ **ПРИМЕЧАНИЕ**
> Работа с параметрами `retry` (повтор запросов) и `rate limit` (ограничение частоты запросов) не поддерживается.

Предварительные действия

Чтобы настроить работу с Python SDK:

1. Перейдите в папку с пакетом AAPM для Python SDK и выполните команду:

   ```
   pip install pam_aapm-3.4.0-py3-none-any.whl
   ```

2. Перейдите в консоль администратора Indeed PAM и добавьте приложение.
3. Для приложения добавьте разрешение с включенной опцией **Разрешить просмотр учетных данных**.
   Разрешение позволит приложению использовать пароли и SSH-ключи учетных записей PAM.
4. Назначьте администраторов приложения, которые могут просматривать его пароль.
5. Откройте консоль пользователя Indeed PAM и перейдите на вкладку **Приложения**.
6. Просмотрите пароль от приложения и сохраните его.

Далее откройте любую среду для работы с Python и настройте доступ к серверу Indeed PAM.

Быстрый старт

```python
from pam_aapm import PamClient

# Использование контекстного менеджера (рекомендуется)
with PamClient(
    idp_url="https://pam.company.com/idp",
    core_url="https://pam.company.com/core",
    username="my-app",
    password="app-password",
) as client:
    # Получение пароля
    db_password = client.get_password("DB-SERVER/admin")

    # Получение SSH-ключа
    ssh_key = client.get_ssh_key("LINUX-SERVER/deploy")

    # Получение списка доступных учетных записей
    accounts = client.get_accounts()
    for account in accounts:
        print(f"{account.display_name}: password={account.has_password}, key=
{account.has_key}")
```

Аутентификация

`PamClient` — основной класс Python SDK для взаимодействия с Indeed PAM. Он предоставляет API для аутентификации и получения учетных данных. Чтобы установить соединение с сервером PAM и получить токены доступа, укажите для класса `PamClient` параметры из таблицы.

Параметры `PamClient`

Параметр	Переменная окружения	Требование	Описание
`idp_url`	`PAM_IDP_SERVER`	Обязательный	URL-адрес компонента Indeed PAM IdP
`core_url`	`PAM_CORE_SERVER`	Обязательный	URL-адрес компонента Indeed PAM Core
`username`	`PAM_USERNAME`	Обязательный	Название приложения
`password`	`PAM_PASSWORD`	Обязательный	Пароль указанного приложения. Администратор приложения может просмотреть пароль в консоли пользователя.
`client_id`	—	Необязательный	Идентификатор клиентского приложения, которое запрашивает токен. Значение по умолчанию: `"aapm-tool"`.
`scope`	—	Необязательный	Запрос на доступ к API по протоколу OAuth2. Значение по умолчанию: `"pam-api"`.
`verify_ssl`	`PAM_VERIFY_SSL`	Необязательный	Проверка SSL-сертификата сервера: • `True` — требуется; • `False` — не требуется. Значение по умолчанию: `True`. **Примечание:** Включенная проверка уменьшает риск перехвата данных. Если вы отключили проверку — рекомендуется обратить на это внимание в скрипте и оставить комментарий.

Параметр	Переменная окружения	Требование	Описание
`ca_cert`	`PAM_CA_CERT`	Необязательный	Путь к сертификату для проверки SSL-соединения. Укажите, если сервер PAM использует сертификат, подписанный внутренним УЦ. Сертификат должен быть в формате PEM. Пример: `ca_cert="/path/to/ca.crt"`. Значение по умолчанию: `None`.
`timeout`	—	Необязательный	Время ожидания ответа на запрос, сек. Значение по умолчанию: `30.0`.
`accounts_cache_ttl`	—	Необязательный	Время жизни (TTL) кеша учетных записей, сек. Значение по умолчанию: `300`.

После настройки доступа вызовите один из методов, чтобы получить учетные данные.

> **ПРИМЕЧАНИЕ**
> Рекомендуется использовать контекстный менеджер `with`.
> В таком случае соединение с PAM закрывается автоматически, а токены доступа удаляются.

Пример с параметрами аутентификации

```python
from pam_aapm import PamClient

with PamClient(
    idp_url="https://pam.company.com/idp",
    core_url="https://pam.company.com/core",
    username="my-app",
    password="app-password",
) as client:
    password = client.get_password("SERVER/account")
```

Пример с переменными окружения (рекомендуется для CI/CD-автоматизаций)

```python
import os
from pam_aapm import PamClient

with PamClient(
    idp_url=os.environ["PAM_IDP_SERVER"],
    core_url=os.environ["PAM_CORE_SERVER"],
    username=os.environ["PAM_USERNAME"],
    password=os.environ["PAM_PASSWORD"],
    verify_ssl=os.environ.get("PAM_VERIFY_SSL", "true").lower() == "true",
    ca_cert=os.environ.get("PAM_CA_CERT"),
) as client:
    password = client.get_password("SERVER/account")
```

Методы

> ⓘ **ПРИМЕЧАНИЕ**
> Асинхронный вызов функций не поддерживается.

Методы Python SDK позволяют получить из Indeed PAM:

- пароль учетной записи;
- SSH-ключ учетной записи;
- список доступных учетных записей.

`get_password()`

Метод отправляет API-запрос к Indeed PAM и возвращает пароль указанной учетной записи.

```python
get_password(account_name, reason=None)
```

▼ **Параметры** `get_password()`

Параметр	Требование	Описание
`account_name`	Обязательный	Имя учетной записи в формате: • `LOCATION/username` — рекомендуемый формат; • `LOCATION\username` — требует экранирования в Python-скриптах, например `"DB-SERVER\\admin"`.
`reason`	Необязательный	Причина получения учетных данных. Указание причины определяется политикой, действующей на учетную запись. Значение по умолчанию: `None`.

```python
from pam_aapm import PamClient

with PamClient(
    idp_url="https://pam.company.com/idp",
    core_url="https://pam.company.com/core",
    username="my-app",
    password="app-password",
) as client:
    # Получение пароля
    password = client.get_password("DB-SERVER/db_admin")

    # Получение пароля, если требуется указать причину
    password = client.get_password(
        "PROD-SERVER/admin",
        reason="Плановое обслуживание"
    )
```

`get_ssh_key()`

Метод отправляет API-запрос к Indeed PAM и возвращает SSH-ключ указанной учетной записи.

```
get_ssh_key(account_name, decrypt=True, reason=None)
```

Параметры `get_ssh_key()`

Параметр	Требование	Описание
`account_name`	Обязательный	Имя учетной записи в формате: • `LOCATION/username` — рекомендуемый формат; • `LOCATION\username` — требует экранирования в Python-скриптах, например `"DB-SERVER\\admin"`.
`decrypt`	Необязательный	Вернуть расшифрованный SSH-ключ: • `True` — вернуть; • `False` — не возвращать. Значение по умолчанию: `True`.
`reason`	Необязательный	Причина получения учетных данных. Указание причины определяется политикой, действующей на учетную запись. Значение по умолчанию: `None`.

Параметры ответа

Параметр	Описание
Если в запросе `decrypt=True`	
`key`	SSH-ключ учетной записи в формате PEM
Если в запросе `decrypt=False`	
`key`	Зашифрованный SSH-ключ
`passphrase`	Пароль зашифрованного ключа
`file_name`	Имя файла ключа

```python
from pam_aapm import PamClient

with PamClient(
    idp_url="https://pam.company.com/idp",
    core_url="https://pam.company.com/core",
    username="my-app",
    password="app-password",
) as client:
    # Расшифрованный ключ
    key = client.get_ssh_key("LINUX-SERVER/automation")

    # Зашифрованный ключ с паролем
    key_data = client.get_ssh_key("LINUX-SERVER/automation", decrypt=False)
    print(f"Key: {key_data.key}")
    print(f"Passphrase: {key_data.passphrase}")
```

`get_accounts()`

Метод используется для получения списка доступных учетных записей PAM. Список аккаунтов кешируется в соответствии с настроенным параметром `accounts_cache_ttl` в классе `PamClient`.

```python
get_accounts(force_refresh=False)
```

Параметры `get_accounts()`

Параметр	Требование	Описание
`force_refresh`	Необязательный	Принудительное обновление кеша: • `True` — сбросить кеш; • `False` — не сбрасывать. Значение по умолчанию: `False`.

Параметры ответа

Параметр	Описание
`id`	Идентификатор учетной записи
`display_name`	Имя учетной записи
`requires_reason`	Требуется указать причину просмотра учетных данных: • `true` — требуется; • `false` — не требуется. Указание причины определяется политикой, действующей на учетную запись.
`has_password`	Пароль учетной записи: • `true` — установлен; • `false` — не установлен.
`has_key`	SSH-ключ учетной записи: • `true` — установлен; • `false` — не установлен.
`is_key_supported`	Для учетной записи доступно добавление SSH-ключа: • `true` — доступно; • `false` — недоступно.

```python
from pam_aapm import PamClient
with PamClient(
    idp_url="https://pam.company.com/idp",
    core_url="https://pam.company.com/core",
    username="my-app",
    password="app-password",
) as client:
    accounts = client.get_accounts(force_refresh=False)

    for account in accounts:
        print(f"Учетная запись: {account.display_name}")
        print(f"  - Имеет пароль: {account.has_password}")
        print(f"  - Имеет SSH-ключ: {account.has_key}")
        print(f"  - Требует причину: {account.requires_reason}")
```

`close()`

Метод освобождает системные ресурсы и вызывается автоматически при использовании контекстного менеджера `with`.

Если контекстный менеджер не используется, вызовите `close()`, когда соединение с PAM больше не требуется.

```
close()
```

Пример без использования контекстного менеджера

```python
from pam_aapm import PamClient

# Создание экземпляра клиента
client = PamClient(
    idp_url="https://pam.company.com/idp",
    core_url="https://pam.company.com/core",
    username="my-app",
    password="app-password",
)

password = client.get_password("DB-SERVER/db_admin")

client.close()
```

Исключения и обработка ошибок

Исключения (Exceptions) — события, которые сообщают об ошибках во время выполнения скрипта. Обработка исключений позволяет перехватить ошибку без принудительного завершения программы.

Список исключений

Исключение	Описание
`AuthenticationError`	Ошибка аутентификации в Indeed PAM. Измените учетные данные или обновите токен доступа.
`AccountNotFoundError`	Учетная запись не найдена или недоступна. Убедитесь, что учетная запись не удалена в Indeed PAM или имя учетной записи в запросе указано верно.
`PasswordNotSetError`	Пароль для учетной записи не установлен. Возникает при вызове метода `get_password()`, если у учетной записи не задан пароль.
`SshKeyNotSetError`	SSH-ключ для учетной записи не установлен. Возникает при вызове метода `get_ssh_key()`, если у учетной записи не задан SSH-ключ.
`ReasonRequiredError`	Согласно политике требуется указать причину запроса. В запросе заполните параметр `reason`.
`ConfigurationError`	Ошибка конфигурации. Убедитесь, что URL-адреса для IdP и Core указаны верно, или добавьте в запрос недостающие параметры.
`ApiError`	Ошибка API-сервера. Изучите код ответа HTTP.
`PamConnectionError`	Ошибка подключения к серверу. Проверьте доступность компонентов IdP и Core.
`ValidationError`	Ошибка обработки входных данных. Убедитесь, что компоненты IdP и Core доступны, а параметры запроса указаны верно.

Пример обработки исключений

```python
from pam_aapm import (
    PamClient,
    AuthenticationError,
    AccountNotFoundError,
    PasswordNotSetError,
    ReasonRequiredError,
    SshKeyNotSetError,
    PamConnectionError,
    PamError,
)

try:
    with PamClient(
        idp_url="https://pam.company.com/idp",
        core_url="https://pam.company.com/core",
        username="my-app",
        password="app-password",
    ) as client:
        password = client.get_password("SERVER/account")

except AuthenticationError as e:
    print(f"Ошибка аутентификации: {e}")
except AccountNotFoundError as e:
    print(f"Учетная запись не найдена: {e.account_name}")
except PasswordNotSetError as e:
    print(f"Пароль не установлен: {e.account_name}")
except ReasonRequiredError as e:
    print(f"Требуется указать причину: {e.account_name}")
except SshKeyNotSetError as e:
    print(f"SSH-ключ не установлен: {e.account_name}")
except PamConnectionError as e:
    print(f"Ошибка подключения: {e}")
except PamError as e:
    print(f"Ошибка PAM: {e}")
```

Рекомендации по безопасности

1. Не храните учетные данные в скриптах. Для повышения безопасности используйте переменные окружения или хранилища секретов.
2. Используйте контекстный менеджер `with`. В таком случае соединение с Indeed PAM закрывается автоматически, а токены доступа удаляются после обработки запроса.

3. Проверка SSL-подключения включена по умолчанию. Отключайте проверку только для тестирования в изолированных средах.
4. При логировании исключений обходите запись учетных данных, чтобы они не сохранялись в логах.

AAPM API

Indeed PAM поддерживает взаимодействие с Application Password Management (AAPM) через интерфейс API.
Запросы на получение и просмотр учетных данных записываются в журнал в разделе **События**.

Чтобы получить список учетных записей или их данные, аутентифицируйтесь и получите токен доступа.

> ⓘ **ПРИМЕЧАНИЕ**
> Как добавить приложение и предоставить ему доступ к учетным данным, читайте в разделе **Приложения**.

Аутентификация и получение токена

Аутентификация и получение токена происходит по протоколу OpenID Connect (OIDC) с использованием механизма Resource Owner Password Credentials (ROPC). Приложение отправляет логин и пароль в компонент IdP, а IdP возвращает токен доступа.

Чтобы аутентифицироваться и получить токен, отправьте POST-запрос к серверу управления:

```
POST https://<FQDN PAM>/idp/connect/token
```

Параметры запроса

Параметры	Описание
`Content-Type`	Формат чтения, обработки и вывода данных. Для работы с данными в формате JSON укажите `application/json`.
`grant_type`	Способ аутентификации и получения токена. Для аутентификации по логину и паролю приложения укажите `password`.
`username`	Название приложения, добавленного в Indeed PAM
`password`	Пароль указанного приложения. Администратор приложения может просмотреть пароль в консоли пользователя.
`scope`	Запрос на доступ к API. Для доступа к API Indeed PAM укажите `pam-api`.
`client_id`	Идентификатор клиентского приложения, которое запрашивает токен. Для аутентификации приложения на сервере IdP укажите `aapm-tool`.

Пример запроса на получение токена

```
POST https://pam.server/idp/connect/token
Content-Type: application/x-www-form-urlencoded
grant_type=password&username=MyApp&password=a4dGs22TfDpm31&scope=pam-
api&client_id=aapm-tool
```

Ответ содержит поле `access_token`, в котором указан токен доступа. Используйте его в запросах, чтобы получить:

- список доступных учетных записей;
- пароль и SSH-ключ учетных записей, хранящихся в Indeed PAM.

Параметры ответа

Параметры	Описание
`access_token`	Токен для доступа к API Indeed PAM
`expires_in`	Срок действия токена в секундах
`token_type`	Тип токена доступа: `Bearer` — любой пользователь, владеющий токеном, может его использовать.
`scope`	Разрешение на доступ к API: `pam-api` — токен действителен только для вызовов API Indeed PAM.

Пример ответа

```
{
    "access_token": "BB984E803AFAA449FD8C1",
    "expires_in": 60,
    "token_type": "Bearer",
    "scope": "pam-api"
}
```

Получение учетных данных

Запрос выполняется к компоненту Core с использованием токена доступа из запроса к IdP.
Чтобы получить учетные данные, отправьте POST-запрос к серверу управления:

```
POST https://<FQDN PAM>/core/accounts/<идентификатор учетной записи>/credentials-view
```

Скопируйте идентификатор учетной записи из URL-адреса профиля учетной записи.

Параметры запроса

Параметр	Описание
`Content-Type`	Формат чтения, обработки и вывода данных. Для работы с данными в формате JSON укажите `application/json`.
`Authorization`	Аутентификация пользователя и проверка прав доступа. Укажите способ аутентификации `Bearer` и токен доступа, полученный в запросе к IdP.
`account-id`	Идентификатор приложения, для которого запрашиваются учетные данные. Идентификатор отображается в URL-адресе в профиле приложения.
`UserId`	Сервисный атрибут в формате UUID. Укажите `00000000-0000-0000-0000-000000000000`.
`Reason`	Причина получения учетных данных. Указание причины определяется политикой, действующей на учетную запись.

Пример запроса на получение учетных данных

```
POST https://pam.server/core/accounts/5e852968-26ed-498c/credentials-view
Content-Type: application/json
Authorization: Bearer BB984E803AFAA449FD8C1
{
 "UserId": "00000000-0000-0000-0000-000000000000",
 "Reason": "get-data"
}
```

Ответ на запрос содержит данные учетной записи: пароль, SSH-ключ и их настройки.

Параметры ответа

Параметр	Описание
`Password`	Пароль учетной записи
`Key`	SSH-ключ учетной записи
`KeyPassphrase`	Сгенерированный пароль для SSH-ключа. Генерация пароля определяется политикой, действующей на учетную запись. Если опция **Шифровать SSH-ключ сгенерированным паролем перед показом пользователю** отключена, в поле указано `null`.
`ResetCredentialsAfterShowing`	Настройка сброса пароля после просмотра: • `true` — пароль сбрасывается; • `false` — пароль не сбрасывается. Настройка задается в разделе **Показ учетных данных** в политике, действующей на учетную запись.
`ResetCredentialsAfterShowingAfterMin`	Время, по истечении которого пароль сбрасывается, мин

Пример ответа

```
{
    "Password": "Q1w2e3r4",
    "Key": "",            // учетной записи можно установить SSH-ключ, но в данный момент он не добавлен
    "KeyPassphrase": null,
    "KeyFileName": "INDEED-ID\\Administrator_20221013_160621Z.pem",
    "ResetCredentialsAfterShowing": false,
    "ResetCredentialsAfterShowingAfterMin": 60
}
```

Получение списка учетных записей

Запрос выполняется к компоненту Core с использованием токена доступа из запроса к IdP.
Чтобы получить список учетных записей, отправьте GET-запрос к серверу управления:

```
GET https://<FQDN PAM>/core/users/permitted-accounts
```

Параметры запроса

Параметр	Описание
`Content-Type`	Формат чтения, обработки и вывода данных. Для работы с данными в формате JSON укажите `application/json`.
`Authorization`	Аутентификация пользователя и проверка прав доступа. Укажите способ аутентификации `Bearer` и токен доступа, полученный в запросе к IdP.

Пример запроса на получение списка учетных записей

```
GET https://pam.server/core/users/permitted-accounts
Content-Type: application/json
Authorization: Bearer BB984E803AFAA449FD8C1
```

Ответ на запрос содержит список учетных записей с настройками действующих разрешений и политики.

Параметры ответа

Параметр	Описание
`Account` — данные учетной записи	
`Id`	Идентификатор учетной записи
`DisplayName`	Имя учетной записи
`IsKeySupported`	Для учетной записи доступно добавление SSH-ключа: • `true` — доступно; • `false` — недоступно.
`NextCredentialsReset`	Пароль и SSH-ключ учетной записи сбрасываются после показа через указанное время в минутах. `null` — сброс учетных данных не задан политикой.
`AreCredentialsResettingNow`	Во время запроса происходит смена пароля и/или SSH-ключа учетной записи: • `true` — сейчас учетные данные меняются; • `false` — учетные данные не меняются.
`HasPassword`	Пароль учетной записи: • `true` — установлен; • `false` — не установлен.
`HasKey`	SSH-ключ учетной записи: • `true` — установлен; • `false` — не установлен.
`PolicySettings` — параметры политики, действующей на учетную запись	
`RequireCredentialsViewingReason`	Требовать указать причину просмотра пароля и SSH-ключа: • `true` — требуется; • `false` — не требуется.

Параметр	Описание
`IsCredentialsViewingConfirmationRequired`	Просмотр пароля и SSH-ключа требует подтверждения администратором: • `true` — пароль доступен после подтверждения запроса администратором; • `false` — не требуется.
`CredentialsViewingConfirmationTimeout`	Время ожидания подтверждения просмотра пароля и SSH-ключа, мин
`EncryptKeyBeforeShowing`	Шифровать SSH-ключ сгенерированным паролем перед показом пользователю: • `true` — шифровать; • `false` — не шифровать.
`IsUserCanSetAccountCredentialsIfNotSet`	Разрешить пользователям PAM задавать учетные данные для учетных записей, если они не заданы: • `true` — разрешено; • `false` — запрещено.
`PermissionSettings` — настройки разрешения	
`IsCredentialsViewAllowed`	Разрешить пользователю просмотр учетных данных: • `true` — пользователь добавлен в администраторы приложения и может просматривать его пароль в консоли пользователя; • `false` — пользователь не добавлен в администраторы и не может просмотреть пароль.
`IsCredentialsChangeAllowed`	Разрешить пользователю редактировать учетные данные: • `true` — пользователь добавлен в разрешение и может сбросить пароль приложения; • `false` — пользователь не может сбросить пароль приложения, так как не добавлен в разрешение или такая опция в его разрешении не включена.

Пример ответа


```
{
    "Accounts": [
        {
            "Account": {
                "Id": "7c0616f5-9c60-432b-a644-b57bbd176e65",
                "DisplayName": "UBUNTU-PAM.PAM-AD1.LOCAL\\root",
                "IsKeySupported": true,
                "NextCredentialsReset": null,
                "AreCredentialsResettingNow": false,
                "HasPassword": true,
                "HasKey": false
            },
            "PolicySettings": {
                "RequireCredentialsViewingReason": false,
                "IsCredentialsViewingConfirmationRequired": false,
                "CredentialsViewingConfirmationTimeout": "00:07:00",
                "EncryptKeyBeforeShowing": false,
                "IsUserCanSetAccountCredentialsIfNotSet": false
            },
            "PermissionSettings": {
                "IsCredentialsViewAllowed": true,
                "IsCredentialsChangeAllowed": false
            }
        }
    ]
}
```

Консольная утилита

Консольная утилита Pam.Tools.Aapm позволяет приложению получать пароли и SSH-ключи учетных записей, хранящихся в Indeed PAM. Установите и настройте утилиту на сервере, на котором запускается приложение.
Запросы на получение и просмотр учетных данных записываются в журнал в разделе **События**.

> ⓘ **ПРИМЕЧАНИЕ**
> Как добавить приложение и предоставить ему доступ к учетным данным, читайте в разделе **Приложения**.

Настройка

1. Перейдите в дистрибутив AAPM и откройте конфигурационный файл утилиты *appsettings.json*.
2. В секциях `Auth` и `Endpoints` укажите значения для параметров:
   - `Username` и `Password` — название и пароль приложения.
     Администратор приложения может просмотреть эти данные в консоли пользователя.
   - `CoreUrl` — адрес компонента Core.
   - `IdpUrl` — адрес компонента IdP.
   - `Certificate` — идентификатор сертификата.
     Укажите, если настроена проверка отпечатков клиентского сертификата.

Пример конфигурационного файла

```
{
  "$schema": "appsettings.schema.json",
  "Auth": {
    "Username": "124",
    "Password": "2cenQ>(/Q)",
    "Certificate": ""
  },
  "Endpoints": {
    "CoreUrl": "https://pam.server/core",
    "IdpUrl": "https://pam.server/idp"
  },
  "NLog": {
    "variables": {
      "maxArchiveFilesPerCategory": 770
    },
    "rules": {
      "0_MicrosoftExtensionsIgnored": {
        "logger": "Microsoft.Extensions.*",
        "maxLevel": "Info",
        "final": true
      },
      "0_MicrosoftEfCoreIgnored": {
        "logger": "Microsoft.EntityFrameworkCore*",
        "maxLevel": "Debug",
        "final": true
      },
      "0_SystemIgnored": {
        "logger": "System.*",
        "maxLevel": "Info",
        "final": true
      },
      "1_File": {
        "logger": "*",
        "writeTo": "appdomainFile"
      }
    }
  }
}
```

Запуск утилиты

Windows

1. Запустите PowerShell от имени администратора.

2. Перейдите в папку с утилитой и запустите ее с нужным параметром:

```
.\Pam.Tools.Aapm.exe <параметр>
```

- `get-accounts` — список учетных записей, данные которых знает и может использовать приложение.
- `get-ssh-key` — SSH-ключ указанной учетной записи.
- `get-password` — пароль указанной учетной записи.
- `help` — информация об указанной команде.
- `version` — номер версии утилиты.

Примеры команд

Выводит список учетных записей из разрешений

```
.\Pam.Tools.Aapm.exe get-accounts
```

Выводит пароль учетной записи INDEED\ServiceOps

```
.\Pam.Tools.Aapm.exe get-password -n INDEED\ServiceOps
```

Записывает результат команды в переменную и выводит результат

```
$result = .\Pam.Tools.Aapm.exe get-ssh-key -n INDEED\ServiceOps
echo $result
```

Linux

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Для работы утилиты установите dotnet-runtime-8.0.

1. Перейдите в каталог с дистрибутивом */IndeedPAM_3.4_RU/indeed-pam-tools/aapm*

2. Из каталога откройте терминал и запустите утилиту с нужным параметром:

```
dotnet ./Pam.Tools.Aapm.dll <параметр>
```

- `get-accounts` — список учетных записей, данные которых знает и может использовать приложение.
- `get-ssh-key` — SSH-ключ указанной учетной записи.
- `get-password` — пароль указанной учетной записи.
- `help` — информация об указанной команде.
- `version` — номер версии утилиты.

Примеры команд

Выводит список учетных записей из разрешений

```
dotnet ./Pam.Tools.Aapm.dll get-accounts
```

Выводит пароль учетной записи INDEED\ServiceOps

```
dotnet ./Pam.Tools.Aapm.dll get-password -n INDEED\ServiceOps
```

Записывает результат команды в переменную и выводит результат

```
result=$(dotnet ./Pam.Tools.Aapm.dll get-ssh-key -n INDEED\ServiceOps)
echo $result
```

Аутентификация в SSH Proxy по SSH-ключу

Пользователи могут подключаться к SSH Proxy по SSH-ключам. Это обеспечивает безопасный и быстрый вход в SSH Proxy без необходимости использовать пароли. Чтобы узнать, доступен ли для вас этот метод аутентификации, обратитесь к администратору PAM.

Ключ в текстовом формате

Для подключения к SSH Proxy требуется сгенерировать ключ и передать его открытую часть администратору PAM. Способ генерации зависит от используемого клиента для подключения к SSH Proxy. При использовании cmd сгенерируйте ключ утилитой ssh-keygen. При использовании PuTTY сгенерируйте ключ утилитой PuTTYgen. При использовании MobaXterm подходит любой способ.

Генерация ключа утилитой ssh-keygen

1. Сгенерируйте SSH-ключ.

   Поддерживаемые алгоритмы шифрования ключей:

   - rsa-sha2-256
   - rsa-sha2-512
   - ecdsa-sha2-nistp256
   - ecdsa-sha2-nistp384
   - ecdsa-sha2-nistp521
   - ssh-ed25519

Шаблон и пример команды для генерации SSH-ключа

Шаблон

```
ssh-keygen -t <алгоритм>
```

Пример

```
ssh-keygen -t ssh-ed25519
```

2. Передайте администратору PAM открытый ключ. Строка с ключом должна содержать алгоритм шифрования и ключ. Опционально строка может содержать комментарий, например имя пользователя и хост. Пример: ssh-ed25519 AAAAC3... user@host.

3. Дождитесь, когда администратор настроит подключение по SSH-ключу.

4. Подключитесь к SSH Proxy.

> ⓘ **ПРИМЕЧАНИЕ**
>
> Рекомендуется располагать SSH-ключ в папке *.ssh*. Например, *C:\Users\user\.ssh* для Windows и */home/user/.ssh* для Linux.
>
> Рекомендуется сохранять имя ключа по умолчанию. Например, *id_rsa*, *id_ecdsa*, *id_ed25519*.
>
> Если файлы ключей расположены в другом месте или их имена отличаются от стандартных, то при подключении к SSH Proxy требуется указать путь до закрытого ключа.

Генерация ключа утилитой PuTTYgen

1. Откройте PuTTYgen.
2. В поле **Type of key to generate** выберите одно из значений: RSA, ECDSA nistp-256, ECDSA nistp-384, ECDSA nistp-521, EdDSA Ed25519.
3. Нажмите **Generate**.
4. Двигайте мышью в пустой области окна PuTTYgen до завершения генерации ключа.
5. Очистите поле **Key comment** и введите в него имя пользователя и хост в формате user@host. Чтобы узнать имя пользователя и хост, выполните команду в терминале:

```
whoami
```

6. Сохраните текст из поля **Public key for pasting into OpenSSH authorized keys file**. Это открытый ключ.
7. Нажмите **Save private key**, чтобы сохранить закрытый ключ.
8. Во всплывающем окне нажмите **Да**.
9. Задайте имя файла, например, *key-private*.
10. Нажмите **Сохранить**.
11. Передайте администратору PAM открытый ключ. Строка с ключом должна включать в себя алгоритм шифрования, ключ, имя пользователя и хост. Пример: ssh-ed25519 AAAAC3... user@host.
12. Дождитесь, когда администратор настроит подключение по SSH-ключу.
13. Подключитесь к SSH Proxy.

Сертификат X.509

Для подключения к SSH Proxy требуется сгенерировать сертификат с ключом и передать открытую часть ключа администратору PAM.

1. Сгенерируйте сертификат X.509, в котором отсутствует цепочка сертификатов.

   Инструкция по генерации

   1. Откройте оснастку Управление сертификатами пользователей, затем откройте Личное → Сертификаты.
   2. Нажмите правой кнопкой мыши по папке Сертификаты. Выберите пункт Все задачи → Запросить новый сертификат.
   3. Нажмите Далее.
   4. Выберите политику регистрации сертификатов и нажмите Далее.
   5. Выберите сертификат.
   6. Нажмите Заявка.

2. Экспортируйте сертификат.

Инструкция по экспорту

1. Откройте оснастку Управление сертификатами пользователей, затем откройте Личное → Сертификаты.
2. Нажмите правой кнопкой мыши на сертификат, который сгенерировали на предыдущем шаге. Выберите пункт Все задачи → Экспорт.
3. В открывшемся окне нажмите Далее.
4. Выберите опцию Файлы X.509 (.CER) в кодировке DER.
5. Выберите расположение файла и заполните Имя файла. Нажмите Далее.
6. Проверьте введенные данные и нажмите Готово.

3. Передайте администратору PAM файл с сертификатом. Поддерживаемые расширения файла: PEM, DER, CRT.

4. Дождитесь, когда администратор настроит подключение по SSH-ключу.

5. Подключитесь к SSH Proxy.

Дополнительные утилиты

Использование PamSu

Прочитайте, как выполнить команду, если нужно sudo

Indeed PAM Desktop Console

Ознакомьтесь с описанием Indeed PAM Desktop Console

Использование PamSu

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 ~]$
```

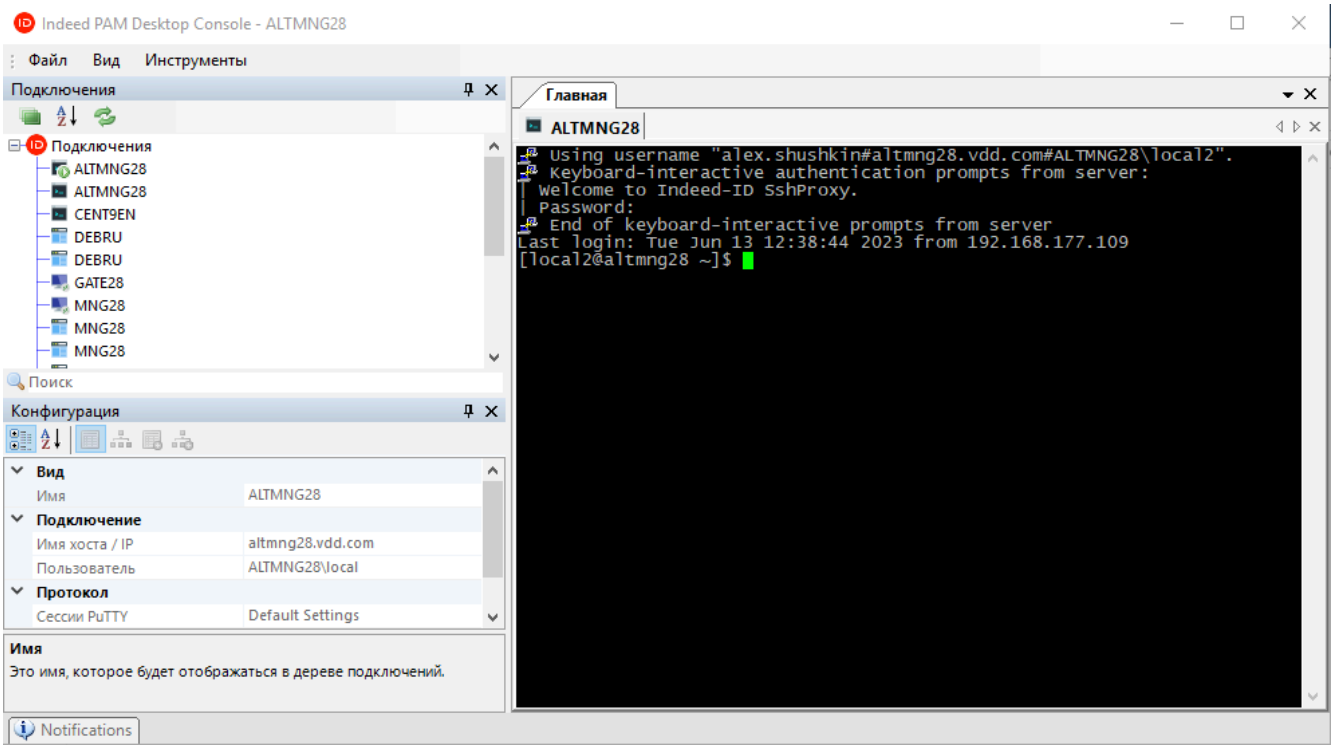
Indeed PAM Desktop Console

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 службы каталогов (в противном случае запустите утилиту Desktop Console от имени учетной записи пользователя службы каталогов), 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.



Решение проблем



Проблемы с сертификатом

Что делать, если сертификаты истекли или их необходимо заменить



Логи

Количество глав: 3



Техническая поддержка

Как создать обращение в поддержку

Проблемы с сертификатом

Сертификат обеспечивает защищенное HTTPS-соединение. Если с сертификатом возникают проблемы, браузер не может гарантировать безопасный обмен данными с сервером, а риск перехвата данных возрастает.

Когда необходимо заменить сертификат:

- Изменение данных — в сертификате указаны устаревшие данные, например, доменное имя, SAN (Subject Alternative Names) или IP-адрес сервера.
  Если оставить старый сертификат, работа с PAM станет невозможна.

- Компрометация приватного ключа сервера — ключ становится известен и может быть использован третьими лицами.
  Замените сертификаты, даже если их срок действия еще не истек.

- Истек срок действия — наиболее распространенная причина смены сертификата.
  Рекомендуем менять сертификаты до истечения срока действия, иначе PAM станет недоступен, а соединение небезопасным для пользователей.

  Как проверить срок действия сертификата?

  Если консоль пользователя или администратора не открывается, а в адресной строке браузера отображается ошибка **Не защищено** или **Небезопасно**, проверьте срок действия сертификата. Нажмите на предупреждение в адресной строке вашего браузера:
  - Microsoft Edge: перейдите **Небезопасно** → **Подключение к этому сайту не защищено** →  .
  - Google Chrome: перейдите **Не защищено** → **Сведения о сертификате**.
  - Яндекс Браузер: перейдите **Не защищено** → **Подключение не защищено** → **Недействительный сертификат**.

Корневой сертификат УЦ

Корневой сертификат УЦ необходимо заменить на всех серверах PAM, включая балансировщик нагрузки.
Сертификат должен быть в формате PEM с кодировкой Base-64 и использовать алгоритм подписи SHA-256. При замене сертификатов сохраняйте исходные имена файлов.

> ⓘ **ПРИМЕЧАНИЕ**
> Если новый сертификат УЦ создается с теми же закрытыми ключами, замена сертификатов в инсталляции PAM не требуется. При создании сертификата с новой парой ключей, необходимо заменить все ранее выданные сертификаты во всей инсталляции PAM.

Windows

1. Экспортируйте корневой сертификат без закрытого ключа с расширением .cer или .crt.
2. Нажмите правой кнопкой на файл сертификата и в контекстном меню выберите **Install Certificate** (Установить сертификат).
3. В мастере импорта сертификатов для параметра **Store Location** (Расположение хранилища) выберите **Local Machine** (Локальный компьютер) и нажмите **Next** (Далее).
4. Выберите **Place all certificates in the following store** (Поместить все сертификаты в следующее хранилище) и нажмите **Browse** (Обзор).
5. В открывшемся окне выберите **Trusted Root Certification Authorities** (Доверенные корневые центры сертификации) и нажмите **OK**.
6. Нажмите **Next** (Далее).
7. В окне подтверждения нажмите **Finish** (Готово).

Linux

1. Экспортируйте корневой сертификат без закрытого ключа с расширением .crt.

   > ⚠ **ПРЕДУПРЕЖДЕНИЕ**
   > Корневой сертификат для балансировщика нагрузки должен называться *ca.crt*.

2. Разместите сертификат по пути */etc/indeed/indeed-pam/ca-certificates/*

3. Перейдите в папку */etc/indeed/indeed-pam/* с повышением привилегий:

   ```
   sudo -i
   ```

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

4. Остановите все компоненты:

   ```
   bash scripts/stop-pam.sh
   ```

5. Обновите права на замененных файлах:

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> Обязательно запускайте команду из папки */etc/indeed/indeed-pam/*

```
bash scripts/set-permissions.sh
```

6. Запустите остановленные компоненты:

```
bash scripts/run-pam.sh
```

Сертификат сервера

Замените сертификаты на целевом сервере. Новые сертификаты должны соответствовать требованиям и сохранять исходные имена файлов.

Windows

1. Экспортируйте сертификат сервера с закрытым ключом в формате .pfx.
2. Разместите сертификат сервера в личные сертификаты компьютера:
    1. Нажмите правой кнопкой на файл сертификата и в контекстном меню выберите **Install Certificate** (Установить сертификат).
    2. В мастере импорта сертификатов для параметра **Store Location** (Расположение хранилища) выберите **Local Machine** (Локальный компьютер) и нажмите **Next** (Далее). Введите пароль от сертификата.
    3. Выберите **Place all certificates in the following store** (Поместить все сертификаты в следующее хранилище) и нажмите **Browse** (Обзор).
    4. В открывшемся окне выберите **Personal** (Личное) и нажмите **OK**.
    5. В окне подтверждения нажмите **Finish** (Готово).
3. Запустите **IIS Manager** (Диспетчер служб IIS).
4. На левой панели **Connections** (Подключения) раскройте <FQDN сервера> → **Sites** (Сайты) → **Default Web Site**.

5. Выберите **Default Web Site** и на правой панели **Actions** (Действие) нажмите **Bindings** (Привязки).

6. В открывшемся окне для всех привязок с типом HTTPS и портом 443 выполните замену сертификата:

    1. Выберите привязку и нажмите **Edit** (Изменить).
    2. В открывшемся окне нажмите **Select** (Выбрать) и выберите импортированный сертификат.

7. После замены сертификатов на левой панели **Connections** (Подключения) нажмите на FQDN сервера.

8. На правой панели **Actions** (Действие) нажмите **Restart** (Перезапустить).

9. Откройте с правами администратора конфигурационный файл *C:\Program Files\Indeed\Indeed PAM\Gateway\Pam.Gateway.Service\appsettings.json*

10. В секции `Kestrel` для параметра `Subject` укажите значение `Subject` нового сертификата.

    Структура конфигурационного файла

    ```
    "Kestrel": {
      "Endpoints": {
        "HttpsInlineCertStore": {
          "Url": "https://0.0.0.0:5443",
          "Certificate": {
            "Subject": "dc.indeed.local", // Укажите значение из нового сертификата
            "Store": "My",
            "Location": "LocalMachine",
            "AllowInvalid": "False"
          }
        }
      }
    }
    ```

    Если в новом сертификате в поле SAN не указан IP-адрес сервера, измените конфигурацию ProxyApp:

    - Откройте конфигурационный файл *C:\Program Files\Indeed\Indeed PAM\Gateway\ProxyApp\appsettings.json*
    - В секции `GatewayService` замените IP-адрес на имя сервера в формате FQDN.

Структура конфигурационного файла

```
"GatewayService": {
  "Url": "https://dc.indeed.local:5443" // Укажите имя сервера в формате FQDN
}
```

Linux

1. Экспортируйте сертификат с открытым ключом в формате PEM (Base-64) и расширением .crt.

2. Экспортируйте сертификат с закрытым ключом в формате PEM (Base-64) и расширением .pem или .pfx.
   Для сертификата с расширением .pem предварительная подготовка не требуется.

   Если сертификат с расширением .pfx, извлеките из него ключи с помощью команд:

   Извлечение закрытого ключа

   ```
   openssl pkcs12 -in <сертификат с открытым ключом> -nocerts -out <сертификат с закрытым ключом> -nodes -passin pass:<пароль>
   ```

   Извлечение сертификата

   ```
   openssl pkcs12 -in <сертификат с закрытым ключом> -clcerts -nokeys -out <сертификат с открытым ключом> -passin pass:<пароль>
   ```

   - `<сертификат с открытым ключом>` — имя экспортированного сертификата с расширением .crt;
   - `<сертификат с закрытым ключом>` — имя экспортированного сертификата с расширением .pem или .pfx.
   - `<пароль>` — пароль, заданный при экспортировании сертификата.

3. Разместите сертификаты в соответствующие папки компонентов:

   - Сервер управления: */etc/indeed/indeed-pam/certs*
     Замените сертификаты *pam.crt* и *pam.key*. Если в папке расположены сертификаты *pam-selfsigned.key* и *pam-selfsigned.crt*, менять их не нужно.

- RDP Proxy: */etc/indeed/indeed-pam/keys/rdp-proxy*
- PostgreSQL Proxy: */etc/indeed/indeed-pam/keys/sql-proxy*
- MSSQL Proxy: */etc/indeed/indeed-pam/keys/tsql-proxy*
- Web Proxy: */etc/indeed/indeed-pam/keys/web-proxy*

4. Перейдите в папку */etc/indeed/indeed-pam/* с повышением привилегий:

```
sudo -i
```

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

5. Остановите все компоненты:

```
bash scripts/stop-pam.sh
```

6. Обновите права на замененных файлах:

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
> Обязательно запускайте команду из папки */etc/indeed/indeed-pam/*

```
bash scripts/set-permissions.sh
```

7. Запустите остановленные компоненты:

```
bash scripts/run-pam.sh
```

Сертификат сервера доступа RDS

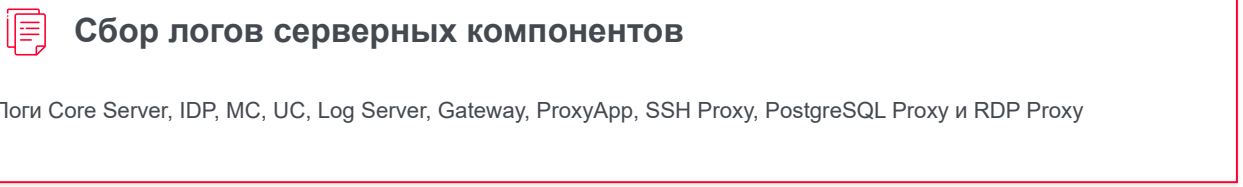
Управление сертификатами сервера доступа RDS происходит в **Server Manager** (Диспетчер серверов), так как они используются следующими службами:

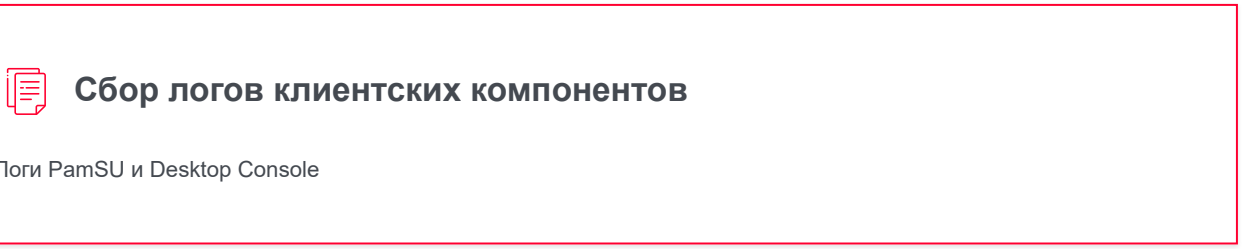
- Посредник подключений к удаленному рабочему столу: включение единого входа (RD Connection Broker: SSO).
- Посредник подключений к удаленному рабочему столу: публикация (RD Connection Broker: Publishing).

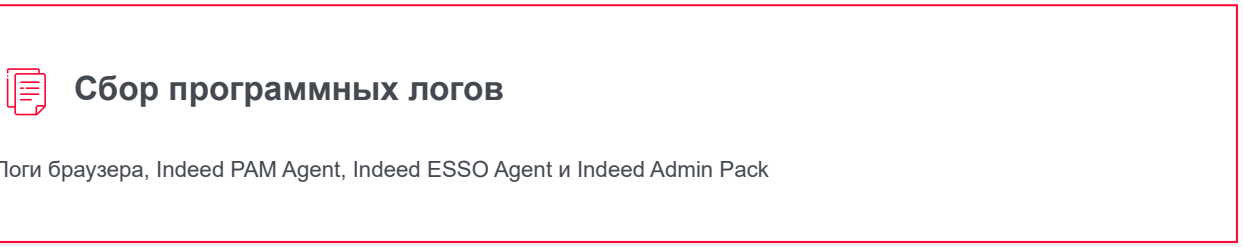
Чтобы заменить сертификат:

1. Экспортируйте два сертификата сервера с закрытым ключом в формате .pfx. Сертификаты должны соответствовать требованиям.
2. Откройте **Server Manager** (Диспетчер серверов).
3. Перейдите в **Remote Desktop Services** (Служба удаленных рабочих столов).
4. В окне **Deployment Overview** (Обзор развертывания) нажмите **Tasks** (Задачи) и из выпадающего списка выберите **Edit Deployment Properties** (Изменить свойства развертывания).
5. В открывшемся окне выберите **Сертификаты** (Certificates).
6. В окне **Role Service** (Службы ролей) выберите **RD Connection Broker - Enable Single Sign On** (Посредник подключений к удаленному рабочему столу: включение единого входа в систему).
7. Нажмите **Select existing certificate...** (Выбрать существующий сертификат).
8. Выберите **Choose a different certificate** (Выберите другой сертификат) и нажмите **Browse** (Обзор).
9. В открывшемся окне выберите импортируемый сертификат и нажмите **Open** (Открыть).
10. В поле **Password** (Пароль) введите пароль от сертификата.
11. Включите опцию **Allow the certificate to be added to the Trusted Root Certification Authorities certificate store on the destination computers** (Разрешить добавление сертификата в хранилище «Доверенные корневые центры сертификации» на конечных компьютерах).
12. Нажмите **OK** и **Apply** (Применить).
13. Повторите действия 6-12 для службы ролей **RD Connection Broker - Publishing** (Посредник подключений к удаленному рабочему столу: публикация).

Логи


Сбор логов серверных компонентов
Логи Core Server, IDP, MC, UC, Log Server, Gateway, ProxyApp, SSH Proxy, PostgreSQL Proxy и RDP Proxy


Сбор логов клиентских компонентов
Логи PamSU и Desktop Console


Сбор программных логов
Логи браузера, Indeed PAM Agent, Indeed ESSO Agent и Indeed Admin Pack

Сбор логов серверных компонентов

Уровни логирования

В зависимости от того, насколько подробную информацию о работе компонента нужно получить, можно задать разные уровни логирования. Они определяют, насколько важная и подробная информация будет записываться в лог-файлы. Это позволяет фильтровать и анализировать логи более эффективно.

Рекомендуется использовать уровень логирования *Trace*, как наиболее информативный.

Уровни логирования

Уровень логирования	Порядковый номер	Строгость логирования
Trace	0	Наиболее подробный уровень. Записывается вся информация о процессах работы компонента, в том числе детали о вызовах методов API.
Debug	1	Записываются подробности о ходе работы компонента, значимые переменные и другие данные, которые могут быть полезными при обнаружении и исправлении ошибок.
Info	2	Записываются информационные сообщения, которые оповещают о нормальном функционировании компонента. Они могут включать такие события, как запуск или завершение процессов, редактирование профиля пользователя и другие.
Warn	3	Записываются предупреждения и уведомления о потенциальных ошибках и внештатных ситуациях. События не являются критическими, но требуют внимания. При этом компонент может продолжать работу.
Error	4	Записываются ошибки, повлекшие за собой некорректную работу компонента или возникновение серьезных проблем. Логи указывают на проблемы, которые требуют вмешательства и исправления.
Fatal	5	Наименее подробный уровень логирования. Записываются только самые критические ошибки и проблемы, которые приводят к немедленному завершению работы компонента или другим серьезным последствиям. Логи обычно означают серьезные сбои, которые требуют немедленного вмешательства и исправления.

Сбор логов скрипта установки

Скрипт установки *run-deploy.sh* может прерваться с ошибкой. В этом случае нужно отправить файлы с логами в техническую поддержку.

Расположение файлов с логами: *IndeedPAM_3.4_RU/indeed-pam/logs/web-wizard/*

Пример ошибки скрипта

```
Failed: Anable playbook returned error code: 2
```

Сбор логов Indeed PAM Core

Windows

Включение логирования

1. Откройте с правами администратора конфигурационный файл *C:\inetpub\wwwroot\core\appsettings.json*
2. Для секции `NLog` в параметре `variables` установите:
   - для ключа `minlevel` значение *Trace*
   - для ключа `dbMinLevel` значение *Trace*

   Пример

   ```
   "NLog": {
     "variables": {
       "minLevel": "Trace",
       "dbMinLevel": "Trace",
       "maxArchiveFilesPerCategory": 23
     }
   ```
3. Сохраните файл.

После редактирования конфигурационного файла перезапустите сервер IIS:

1. Запустите PowerShell от имени администратора.
2. Запустите IIS Manager:

   ```
   start inetmgr
   ```
3. Нажмите на нужный сервер на левой панели.
4. Нажмите **Restart** (Перезапустить) на правой панели.

Сбор логов

1. Очистите существующие логи сервера Indeed PAM Core в папке *C:\inetpub\wwwroot\core\Logs*
2. Воспроизведите проблему.
3. Соберите архив с логами и отправьте в техническую поддержку. Опишите действия пользователя и укажите точное время воспроизведения проблемы.

Linux

Включение логирования

1. Откройте с правами администратора конфигурационный файл */etc/indeed/indeed-pam/core/appsettings.json*
2. Для секции `NLog` в параметре `variables` установите:
   - для ключа `minlevel` значение *Trace*
   - для ключа `dbMinLevel` значение *Trace*

   Пример

   ```
   "NLog": {
     "variables": {
       "minLevel": "Trace",
       "dbMinLevel": "Trace",
       "maxArchiveFilesPerCategory": 23
     }
   ```
3. Сохраните файл.
4. Перейдите в папку со скриптами PAM и выполните перезапуск компонента:

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

   ```
   bash restart-pam.sh core
   ```

Сбор логов

1. Очистите существующие логи сервера Indeed PAM Core в папке */etc/indeed/indeed-pam/logs/core*
2. Воспроизведите проблему.

3. Соберите архив с логами и отправьте в техническую поддержку. Опишите действия пользователя и укажите точное время воспроизведения проблемы.

Сбор логов Indeed PAM IDP

Windows

Включение логирования

1. Откройте с правами администратора конфигурационный файл *C:\inetpub\wwwroot\idp\appsettings.json*
2. Для секции `NLog` в параметре `variables` установите:
   - для ключа `minlevel` значение *Trace*
   - для ключа `dbMinLevel` значение *Trace*

   Пример

   ```
   "NLog": {
     "variables": {
       "minLevel": "Trace",
       "dbMinLevel": "Trace",
       "maxArchiveFilesPerCategory": 23
     }
   ```

3. Сохраните файл.

После редактирования конфигурационного файла перезапустите сервер IIS:

1. Запустите PowerShell от имени администратора.
2. Запустите IIS Manager:

   ```
   start inetmgr
   ```

3. Нажмите на нужный сервер на левой панели.
4. Нажмите **Restart** (Перезапустить) на правой панели.

Сбор логов

1. Очистите существующие логи Indeed PAM IDP в папке *C:\inetpub\wwwroot\idp\Logs*
2. Воспроизведите проблему.
3. Соберите архив с логами и отправьте в техническую поддержку. Опишите действия пользователя и укажите точное время воспроизведения проблемы.

Linux

Включение логирования

1. Откройте с правами администратора конфигурационный файл */etc/indeed/indeed-pam/idp/appsettings.json*
2. Для секции `NLog` в параметре `variables` установите:
   - для ключа `minlevel` значение *Trace*
   - для ключа `dbMinLevel` значение *Trace*

   Пример

   ```
   "NLog": {
     "variables": {
       "minLevel": "Trace",
       "dbMinLevel": "Trace",
       "maxArchiveFilesPerCategory": 23
     }
   ```

3. Сохраните файл.
4. Перейдите в папку со скриптами PAM и выполните перезапуск компонента:

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

   ```
   bash restart-pam.sh idp
   ```

Сбор логов

1. Очистите существующие логи Indeed PAM IDP в папке */etc/indeed/indeed-pam/logs/idp*
2. Воспроизведите проблему.

3. Соберите архив с логами и отправьте в техническую поддержку. Опишите действия пользователя и укажите точное время воспроизведения проблемы.

Сбор логов Indeed PAM Log Server

Windows

Включение логирования

1. Откройте с правами администратора конфигурационный файл *C:\inetpub\wwwroot\ls\appsettings.json*
2. Для секции `NLog` в параметре `variables` установите:
   - для ключа `minlevel` значение *Trace*
   - для ключа `dbMinLevel` значение *Trace*

   Пример

   ```
   "NLog": {
     "variables": {
       "minLevel": "Trace",
       "dbMinLevel": "Trace",
       "maxArchiveFilesPerCategory": 23
     }
   ```
3. Сохраните файл.

После редактирования конфигурационного файла перезапустите сервер IIS:

1. Запустите PowerShell от имени администратора.
2. Запустите IIS Manager:

   ```
   start inetmgr
   ```
3. Нажмите на нужный сервер на левой панели.
4. Нажмите **Restart** (Перезапустить) на правой панели.

Сбор логов

1. Очистите существующие логи Indeed PAM Log Server в папке *C:\inetpub\wwwroot\ls\Logs*
2. Воспроизведите проблему.
3. Соберите архив с логами и отправьте в техническую поддержку. Опишите действия пользователя и укажите точное время воспроизведения проблемы.

Linux

Включение логирования

1. Откройте с правами администратора конфигурационный файл */etc/indeed/indeed-pam/ls/appsettings.json*
2. Для секции `NLog` в параметре `variables` установите:
   - для ключа `minlevel` значение *Trace*
   - для ключа `dbMinLevel` значение *Trace*

   Пример

   ```
   "NLog": {
     "variables": {
       "minLevel": "Trace",
       "dbMinLevel": "Trace",
       "maxArchiveFilesPerCategory": 23
     }
   ```

3. Сохраните файл.
4. Перейдите в папку со скриптами PAM и выполните перезапуск компонента:

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

   ```
   bash restart-pam.sh ls
   ```

Сбор логов

1. Очистите существующие логи Indeed PAM Log Server в папке */etc/indeed/indeed-pam/logs/ls*
2. Воспроизведите проблему.

3. Соберите архив с логами и отправьте в техническую поддержку. Опишите действия пользователя и укажите точное время воспроизведения проблемы.

Сбор логов Indeed PAM Gateway Service

Windows

Включение логирования

1. Откройте с правами администратора конфигурационный файл *C:\Program Files\Indeed\Indeed PAM\Gateway\Pam.Gateway.Service\appsettings.json*
2. Для секции `NLog` в параметре `variables` установите:
   - для ключа `minlevel` значение *Trace*
   - для ключа `dbMinLevel` значение *Trace*

   Пример

   ```
   "NLog": {
     "variables": {
       "minLevel": "Trace",
       "dbMinLevel": "Trace",
       "maxArchiveFilesPerCategory": 23
     }
   ```

3. Сохраните файл.
4. Перезапустите службу Gateway Service:

   ```
   Restart-Service -Name Pam.Gateway.Service -Force
   ```

Сбор логов

1. Очистите существующие логи Indeed PAM Gateway в папке *C:\Program Files\Indeed\Indeed PAM\Gateway\Pam.Gateway.Service\logs*
2. Воспроизведите проблему.
3. Соберите архив с логами и отправьте в техническую поддержку. Опишите действия пользователя и укажите точное время воспроизведения проблемы.

Linux

Включение логирования

1. Откройте с правами администратора конфигурационный файл */etc/indeed/indeed-pam/gateway-service/appsettings.json*
2. Для секции `NLog` в параметре `variables` установите:
   - для ключа `minlevel` значение *Trace*
   - для ключа `dbMinLevel` значение *Trace*

   Пример

   ```
   "NLog": {
     "variables": {
       "minLevel": "Trace",
       "dbMinLevel": "Trace",
       "maxArchiveFilesPerCategory": 23
     }
   ```
3. Сохраните файл.
4. Перейдите в папку со скриптами PAM и выполните перезапуск компонента:

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

   ```
   bash restart-pam.sh gateway-service
   ```

Сбор логов

1. Очистите существующие логи Indeed PAM Gateway в папке */etc/indeed/indeed-pam/logs/gateway-service*
2. Воспроизведите проблему.
3. Соберите архив с логами и отправьте в техническую поддержку. Опишите действия пользователя и укажите точное время воспроизведения проблемы.

Сбор логов Indeed ProxyApp

Включение логирования

1. Откройте с правами администратора конфигурационный файл *C:\Program Files\Indeed\Indeed PAM\Gateway\ProxyApp\appsettings.json*
2. Для секции `NLog` для ключа `defaultMinLevel` установите значение *Trace*.

   Пример

   ```
   "NLog": {
     "variables": {
       "defaultMinLevel": "Trace",
       "maxArchiveFilesPerCategory": 23
     }
   ```

3. Сохраните файл.
4. Перезапустите службу ProxyApp:

   ```
   Restart-Service -Name Pam.Service -Force
   ```

Сбор логов

1. Очистите существующие логи Indeed PAM Gateway в папке *C:\Program Files\Indeed\Indeed PAM\Gateway\ProxyApp\logs*
2. Воспроизведите проблему.
3. Соберите архив с логами и отправьте в техническую поддержку. Опишите действия пользователя и укажите точное время воспроизведения проблемы.

Сбор логов Indeed PAM SSH Proxy

Включение логирования

1. Откройте с правами администратора конфигурационный файл */etc/indeed/indeed-pam/ssh-proxy/appsettings.json*
2. Для ключа `LogLevel` установите значение *Trace*.

   Пример

```
"LogLevel": "TRACE",
"LogStream": "FILE",
"MaxLogFiles": 100,
"MaxLogFileSize": 10000000,
```

3. Сохраните файл.

4. Перейдите в папку со скриптами PAM и выполните перезапуск компонента:

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

```
bash restart-pam.sh ssh-proxy
```

Сбор логов

1. Очистите существующие логи Indeed PAM SSH Proxy в папке */etc/indeed/indeed-pam/logs/ssh*
2. Воспроизведите проблему.
3. Соберите архив с логами и отправьте в техническую поддержку. Опишите действия пользователя и укажите точное время воспроизведения проблемы.

Сбор логов Indeed PAM PostgreSQL Proxy

Включение логирования

1. Откройте с правами администратора конфигурационный файл */etc/indeed/indeed-pam/sql-proxy/appsettings.json*

2. Для ключа `LogLevel` установите значение *Trace*.

Пример

```
"LogLevel": "TRACE",
"LogStream": "FILE",
"MaxLogFiles": 100,
"MaxLogFileSize": 10000000,
```

3. Сохраните файл.

4. Перейдите в папку со скриптами PAM и выполните перезапуск компонента:

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

```
bash restart-pam.sh sql-proxy
```

Сбор логов

1. Очистите существующие логи сервера Indeed PAM PostgreSQL Proxy в папке */etc/indeed/indeed-pam/logs/sql*
2. Воспроизведите проблему.
3. Соберите архив с логами и отправьте в техническую поддержку. Опишите действия пользователя и укажите точное время воспроизведения проблемы.

Сбор логов Indeed PAM MSSQL Proxy

Включение логирования

1. Откройте с правами администратора конфигурационный файл */etc/indeed/indeed-pam/tsql-proxy/appsettings.json*
2. Для ключа `LogLevel` установите значение *Trace*.

Пример

```
"LogLevel": "TRACE",
"LogStream": "FILE",
"MaxLogFiles": 100,
"MaxLogFileSize": 10000000,
```

3. Сохраните файл.
4. Перейдите в папку со скриптами PAM и выполните перезапуск компонента:

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

```
bash restart-pam.sh tsql-proxy
```

Сбор логов

1. Очистите существующие логи сервера Indeed PAM MSSQL Proxy в папке */etc/indeed/indeed-pam/logs/tsql*
2. Воспроизведите проблему.
3. Соберите архив с логами и отправьте в техническую поддержку. Опишите действия пользователя и укажите точное время воспроизведения проблемы.

Сбор логов Indeed PAM RDP Proxy

Включение логирования

1. Откройте с правами администратора конфигурационный файл */etc/indeed/indeed-pam/rdp-proxy/appsettings.json*

2. Для ключа `LogLevel` установите значение *Trace*.

   Пример

   ```
   1  "LogLevel": "TRACE",
   2  "LogStream": "FILE",
   3  "MaxLogFiles": 100,
   4  "MaxLogFileSize": 10000000,
   ```

3. Сохраните файл.

4. Перейдите в папку со скриптами PAM и выполните перезапуск компонента:

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

   ```
   bash restart-pam.sh rdp-proxy
   ```

Сбор логов

1. Очистите существующие логи сервера Indeed PAM RDP Proxy в папке */etc/indeed/indeed-pam/logs/rdp*
2. Воспроизведите проблему.
3. Соберите архив с логами и отправьте в техническую поддержку. Опишите действия пользователя и укажите точное время воспроизведения проблемы.

Сбор логов Indeed PAM Web Proxy

Включение логирования

1. Откройте с правами администратора конфигурационный файл */etc/indeed/indeed-pam/web-proxy/appsettings.json*

2. Для ключа `LogLevel` установите значение *Trace*.

Пример

```
"Settings": {
  "CoreUrl": "PAM_CORE_URL",
  "IdpUrl": "PAM_IDP_URL",
  "ClientSecret": "PAM_WEB_PROXY_SECRET",
  "LogLevel": "TRACE",
  "LogStream": "FILE",
  "MaxLogFiles": 30,
  "MaxLogFileSize": 10000000,
  "RateLimit": {
    "VolumePerTimeMBytes": 100,
    "TimeForFullVolumeSec": 60,
    "TimeForOneAdditionSec": 1
}
```

3. Сохраните файл.

4. Перейдите в папку со скриптами PAM и выполните перезапуск компонента:

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

```
bash restart-pam.sh web-proxy
```

Сбор логов

1. Очистите существующие логи сервера Indeed PAM Web Proxy в папке */etc/indeed/indeed-pam/logs/web*
2. Воспроизведите проблему.
3. Соберите архив с логами и отправьте в техническую поддержку. Опишите действия пользователя и укажите точное время воспроизведения проблемы.

Сбор логов клиентских компонентов

Сбор логов Indeed PAM PamSU

Включение логирования

1. Откройте с правами администратора конфигурационный файл */etc/pamsu.conf*
2. Найдите строку `Set log_level` и укажите уровень `INFO`:

   Пример

   ```
   # Log level is minimum level of logging
   # You can choose beetween
   # INFO, WARN ERROR and FATAL
   Set log_level INFO
   ```

3. Сохраните файл.

Сбор логов

1. Очистите существующие логи сервера Indeed PAM PamSU в папке */opt/Indeed-PAM/pamsu/logs/*
2. Воспроизведите проблему.
3. Соберите архив с логами и отправьте в техническую поддержку. Опишите действия пользователя и укажите точное время воспроизведения проблемы.

Сбор логов Indeed Desktop Console

Включение логирования

1. Откройте приложение Indeed Desktop Console от имени администратора.
2. Нажмите **Инструменты** и перейдите в раздел **Опции**.
3. Перейдите в раздел **Уведомления** в левом меню.
4. Включите опцию **Log to application directory** и оставьте путь по умолчанию.
5. Включите уровни логирования **Debug**, **Информация**, **Предупреждения** и **Ошибки**.
6. Нажмите **ОК**.
7. Перезагрузите приложение Indeed Desktop Console.

Сбор логов

1. Очистите существующие логи Indeed PAM Gateway в папке *C:\Users\Имя_пользователя\AppData\Roaming\Indeed PAM Desktop Console*
2. Воспроизведите проблему.
3. Соберите архив с логами и отправьте в техническую поддержку. Опишите действия пользователя и укажите точное время воспроизведения проблемы.

Сбор логов Indeed PAM Web Terminal

SSH Proxy

Включение логирования

1. Откройте с правами администратора конфигурационный файл */etc/indeed/indeed-pam/ssh-proxy/appsettings.json*
2. Для ключа `LogLevel` установите значение *Trace*.

   Пример

   ```
   "LogLevel": "TRACE",
   "LogStream": "FILE",
   "MaxLogFiles": 100,
   "MaxLogFileSize": 10000000,
   ```

3. Сохраните файл.
4. Перейдите в папку со скриптами PAM и выполните перезапуск компонента:

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

   ```
   bash restart-pam.sh ssh-proxy
   ```

Сбор логов

1. Очистите существующие логи Indeed PAM SSH Proxy в папке */etc/indeed/indeed-pam/logs/ssh*
2. Воспроизведите проблему.
3. Соберите архив с логами и отправьте в техническую поддержку. Опишите действия пользователя и укажите точное время воспроизведения проблемы.

RDP Proxy

Включение логирования

1. Откройте с правами администратора конфигурационный файл */etc/indeed/indeed-pam/rdp-proxy/appsettings.json*
2. Для ключа `LogLevel` установите значение *Trace*.

   Пример

   ```
   "LogLevel": "TRACE",
   "LogStream": "FILE",
   "MaxLogFiles": 100,
   "MaxLogFileSize": 10000000,
   ```

3. Сохраните файл.
4. Перейдите в папку со скриптами PAM и выполните перезапуск компонента:

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

   ```
   bash restart-pam.sh rdp-proxy
   ```

Сбор логов

1. Очистите существующие логи сервера Indeed PAM RDP Proxy в папке */etc/indeed/indeed-pam/logs/rdp*
2. Воспроизведите проблему.
3. Соберите архив с логами и отправьте в техническую поддержку. Опишите действия пользователя и укажите точное время воспроизведения проблемы.

Web Terminal

Включение логирования

1. Откройте с правами администратора конфигурационный файл */etc/indeed/indeed-pam/web-terminal-proxy/appsettings.json*
2. Для ключа `LogLevel` установите значение *Trace*.

Пример

```
{
  "Settings": {
    "Port": "4822",
    "LogLevel": "TRACE",
    "LogStream": "BOTH",
    "MaxLogFiles": 10,
    "MaxLogFileSize": 1000000
    "Host": "0.0.0.0",
  }
}
```

3. Сохраните файл.
4. Перейдите в папку со скриптами PAM и выполните перезапуск компонента:

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

```
bash restart-pam.sh web-terminal-proxy
```

Сбор логов

1. Очистите существующие логи сервера Indeed PAM Web Terminal в папке */etc/indeed/indeed-pam/logs/web-terminal*
2. Воспроизведите проблему.
3. Соберите архив с логами и отправьте в техническую поддержку. Опишите действия пользователя и укажите точное время воспроизведения проблемы.

Сбор программных логов

Indeed-Id GetLog

Приложение Indeed-Id GetLog предназначено для локального и удаленного сбора программных логов компонентов:

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

Перед воспроизведением проблемы очистите существующие логи в папке *C:\Windows\System32\LogFiles\Indeed-ID*

Подключение к компьютеру

1. Откройте утилиту Indeed-Id GetLog от имени администратора.
2. Введите DNS-имя или IP-адрес удаленного компьютера в поле **Computer**.
   Чтобы подключиться к локальному компьютеру, введите localhost или 127.0.0.1.
3. Нажмите **Connect**.

> **ПОДСКАЗКА**
> Чтобы подключиться к удаленному компьютеру под управлением Windows 7 и выше, убедитесь, что на удаленном компьютере запущена и не заблокирована служба Инструментарий управления Windows (WMI) (Windows Management Instrumentation).

Основные действия

После подключения к компьютеру:

1. Нажмите **Enable Log** для включения записи логов.
2. Воспроизведите проблему.
3. Нажмите **Disable Log** для отключения записи логов.
4. Нажмите **Get Log** для получения ZIP-архива с логами.
5. Укажите папку для сохранения ZIP-архива и нажмите **Сохранить**.
6. Нажмите **Disconnect** для отключения от компьютера и закройте приложение.

Архив с логами отправьте в техническую поддержку. Опишите действия пользователя и укажите точное время воспроизведения проблемы.

> ⓘ **ПРИМЕЧАНИЕ**
>
> По умолчанию логи записываются в каталог *\WINDOWS\System32\LogFiles\Indeed-Id*. Для доступа к логам удаленного компьютера по умолчанию используется сетевой каталог *ADMIN$\System32\LogFiles\Indeed-Id*. Каталог для записи логов можно задать в разделе **Advanced Settings** → **Use alternative location**.
>
> Если при попытке сохранить логи появляется ошибка *The system cannot find the file specified*, убедитесь, что папка *C:\Windows\System32\LogFiles\Indeed-ID* существует. Создайте папку вручную, если она отсутствует.

В некоторых случаях может потребоваться включить/отключить логирование вручную. Для этого:

1. Откройте редактор реестра.
2. Перейдите в каталог HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\Logging.
3. Задайте значение параметра Enabled:
   - 0 — отключить логирование;
   - 1 — включить логирование.

Дополнительные настройки

Настройки в утилите

Чтобы перейти к дополнительным настройкам, нажмите **Advanced Settings** в главном окне Indeed-Id GetLog.
В окне **Advanced Settings** доступны настройки:

- Max. log size (bytes) — максимальный размер в байтах всех файлов в каталоге. Значение по умолчанию — 1ГБ. При достижении указанного значения из каталога будут удалены все файлы, дата изменения которых старше значения поля Max.log file age.
- Max. log file age (s) — возраст файла лога в секундах. Если размер логов в каталоге превысил значение Max. log size, то из каталога будут удалены все файлы, дата изменения которых старше значения этого поля.
- Cleaner interval (s) — интервал проверки размера каталога с логами в секундах. Значение по умолчанию – 1 час (3600 секунд).
- Activity checking period (ms) — интервал проверки активности логирования в миллисекундах. Прежде чем начать запись логов, компонент Indeed AM проверит, включено ли на рабочей станции логирование. По умолчанию интервал проверки составляет 1 минуту (60 000 миллисекунд).
- Enable log cycling — режим циклической записи логов. Если опция включена, то логи каждого процесса будут записываться согласно заданным настройкам по количеству файлов и размеру.

    - Max. size of a log file (bytes) — максимальный размер лога в байтах. Значение по умолчанию — 10Мб (1000000 байт). При достижении заданного размера содержимое файла перезапишется новыми данными.
    - Max. number of saved log files — максимальное количество сохраняемых логов. Значение по умолчанию — 5, без учета текущего записываемого файла. Если установленное количество файлов превышено, самый ранний удалится, а запись продолжится во вновь созданный файл.
- Use alternative location — альтернативный каталог записи логов. Если опция выключена, логи записываются в каталоги по умолчанию:
    - *ADMIN$\System32\LogFiles\Indeed-Id* — сетевой путь;
    - *\WINDOWS\System32\LogFiles\Indeed-Id* — локальный путь.

Настройки в реестре

Чтобы перейти к дополнительным настройкам в реестре, откройте редактор реестра и перейдите в каталог *HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\Logging*. В реестре доступны следующие параметры:

- `CycleLogsFileCountMax` — максимальное количество сохраняемых логов. Значение по умолчанию — 5, без учета текущего записываемого файла. Если установленное количество файлов превышено, самый ранний удалится, а запись продолжится во вновь созданный файл.
- `CycleLogsFileSizeMaxBytes` — максимальный размер лога в байтах. Значение по умолчанию — 10Мб (1000000 байт). При достижении заданного размера содержимое файла перезапишется новыми данными.
- `EnabledRecheckPeriodMs` — интервал проверки активности логирования в миллисекундах. Прежде чем начать запись логов, компонент Indeed AM проверит, включено ли на рабочей станции логирование. По умолчанию интервал проверки составляет 1 минуту (60 000 миллисекунд).
- `MaxLogFileAge` — возраст файла лога в секундах. Если размер логов в каталоге превысил значение MaxlogSize, то из каталога будут удалены все файлы, дата изменения которых старше значения этого параметра.
- `MaxLogSize` — максимальный размер в байтах всех файлов в каталоге. Значение по умолчанию — 1ГБ. При достижении указанного значения из каталога будут удалены все файлы, дата изменения которых старше значения параметра MaxlogFileAge.
- `RootLogPath` — альтернативный каталог записи логов. Если параметр отключен, логи записываются в каталоги по умолчанию:
    - *ADMIN$\System32\LogFiles\Indeed-Id* — сетевой путь;
    - *\WINDOWS\System32\LogFiles\Indeed-Id* — локальный путь.

Сбор логов из браузера

Чтобы собрать логи из Google Chrome и Microsoft Edge выполните:

1. Перейдите на страницу с ошибкой и запустите **Инструменты разработчика**.
2. Перейдите на вкладку **Консоль** и нажмите ⃠.
3. Включите все уровни логирования.
4. Нажмите ⚙ на вкладке **Консоль** и включите опции **Сохранять журнал** и **Регистрировать запросы XMLHttpRequests**.
5. Перейдите на вкладку **Сеть** и включите опции **Сохранять журнал** и **Отключить кеш**.
6. Выберите тип фильтра **Все** и нажмите ⃠ для сброса списка запросов.
7. Воспроизведите проблему.
8. Нажмите ⤓ для экспорта HAR-файла и сохраните его.
9. Перейдите во вкладку **Консоль**, нажмите правой кнопкой по сообщению и нажмите **Сохранить как**.
10. Сохраните LOG-файл.

Отправьте HAR- и LOG-файлы в техническую поддержку. Опишите действия пользователя и укажите точное время воспроизведения проблемы.

Техническая поддержка

Если вы не нашли ответ на ваш вопрос в документации или базе знаний, обратитесь за помощью в службу поддержки.

Предоставьте как можно больше информации: файлы, скриншоты, логи. Это поможет решить проблему оперативно.

Чтобы отправить обращение в поддержку:

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 самостоятельно или отправить заявку на регистрацию.

   Чтобы зарегистрироваться самостоятельно:

   1. Нажмите **Зарегистрироваться**.
   2. Заполните поля формы регистрации и нажмите **Зарегистрироваться**.
   3. Перейдите по ссылке в письме, которое придет на указанный электронный адрес. После этого аккаунт активируется.

   Чтобы отправить заявку на регистрацию

   1. Нажмите **Отправить заявку**.
   2. Заполните поля формы заявки.
      Укажите, что это заявка на создание учетной записи.
   3. Перейдите по ссылке в письме, которое придет на указанный электронный адрес. После этого аккаунт активируется.
3. Нажмите **Отправить заявку**.
4. Выберите департамент и нажмите **Вперед**.
5. Заполните форму заявки и нажмите **Отправить**.

Вы можете связаться с командой поддержки по следующим телефонам:

- +7 (800) 333 09-06
- +7 (495) 640 06-09
- +7 (812) 640 06-09

Справочник

События

Список событий Indeed PAM

Привилегии

Список привилегий, которые могут быть включены в роли

Соответствие атрибутов каталога пользователей и PAM

Список значений по умолчанию для атрибутов каталога пользователей и соответствующих атрибутов Indeed PAM

События

Данный раздел содержит список событий Indeed PAM.

В Indeed PAM ведется учет событий следующих типов:

- информация — сообщение со сведениями об изменении каких-либо данных в PAM, при этом PAM работает корректно;
- ошибка — уведомление о проблеме, которая требует вмешательства администратора PAM;
- предупреждение — информирование о том, что проблема или ошибка может появиться в будущем, рекомендуется внимание администратора PAM.

Информация

Код	Текст сообщения
1000	Учетная запись успешно зарегистрирована
1003	Имя учетной записи успешно изменено
1004	Учетная запись успешно восстановлена
1008	Пароль учетной записи успешно добавлен
1009	Учетная запись успешно отключена
1010	Разрешение успешно создано
1013	Разрешение успешно отозвано
1014	Ресурс успешно зарегистрирован
1015	Ресурс успешно удален
1016	Информация о ресурсе успешно изменена
1017	Сессия успешно открыта
1018	Пользователь завершил сессию
1021	Параметры конфигурации успешно изменены

Код	Текст сообщения
1022	Домен успешно зарегистрирован
1023	Домен успешно удален
1025	Сессия успешно прервана
1024	Информация о домене успешно изменена
1026	Учетная запись успешно включена
1027	Учетная запись успешно удалена
1028	Ресурс успешно отключен
1029	Ресурс успешно включен
1033	Незарегистрированных учетных записей не обнаружено
1034	Пароль учетной записи успешно сброшен
1035	Учетная запись переведена в состояние Игнорируется
1036	Политика успешно создана
1037	Имя политики успешно изменено
1038	Настройки политики успешно изменены
1039	Политика успешно создана копированием
1040	Политика учетной записи успешно изменена
1041	Домен успешно включен
1042	Домен успешно восстановлен
1043	Ресурс успешно восстановлен
1044	Пользователь успешно аутентифицирован по второму фактору
1045	Учетная запись успешно сделана управляемой

Код	Текст сообщения
1046	SSH-ключ учетной записи успешно проверен
1048	SSH-ключ учетной записи успешно добавлен
1049	SSH-ключ учетной записи успешно сброшен
1052	Синхронизация учетных записей по расписанию запущена
1053	Синхронизация учетных записей завершена
1055	Смена учетных данных запущена по расписанию
1056	Смена учетных данных завершена
1057	Проверка учетных данных по расписанию запущена
1058	Проверка учетных данных завершена
1059	Проверка сервисного доступа по расписанию запущена
1060	Проверка сервисного доступа завершена
1064	SSH-шаблон успешно добавлен
1065	SSH-шаблон успешно удален
1066	SSH-шаблон успешно обновлен
1067	Пользовательское подключение успешно добавлено
1068	Пользовательское подключение успешно удалено
1069	Пользовательское подключение успешно обновлено
1070	Пользователь успешно посмотрел учетные данные
1071	Лицензия для пользователей и ресурсов успешно зарегистрирована
1072	Ротация артефактов сессии запущена по расписанию
1073	Ротация артефактов сессии завершена

Код	Текст сообщения
1074	Видео файлы сессии были удалены в соответствии с конфигурацией политики ротации
1075	Снимки экрана сессии были удалены в соответствии с конфигурацией политики ротации
1077	Синхронизация ресурсов по расписанию запущена
1078	Синхронизация ресурсов завершена
1080	Обнаружено изменение групп учетной записи
1081	Файлы, переданные на сервер во время сессии, были удалены в соответствии с конфигурацией политики ротации
1082	Пользователь успешно зарегистрировал второй фактор аутентификации
1083	Аутентификатор пользователя успешно удален
1085	Разрешение успешно возобновлено
1086	Разрешение успешно приостановлено
1088	Доменные привилегированные группы успешно зарегистрированы
1089	Список контейнеров для поиска доменных ресурсов успешно изменен
1090	Синхронизация доменных ресурсов по расписанию запущена
1091	Синхронизация доменных ресурсов по расписанию завершена
1095	Добавлена новая роль
1096	Удалена роль
1097	Состав привилегий роли изменен
1098	Изменено имя роли
1099	В состав роли добавлен новый пользователь
1100	Из состава роли исключен пользователь
1101	Группа ресурсов успешно создана

Код	Текст сообщения
1102	Группа ресурсов успешно удалена
1103	Информация о группе ресурсов успешно изменена
1104	Ресурс успешно добавлен в группу ресурсов
1105	Ресурс успешно удален из группы ресурсов
1106	Подтверждение запроса на открытие сессии успешно использовано
1107	Запрос на открытие сессии отклонен
1108	Пользователь отправил запрос на открытие сессии
1109	Запрос на открытие сессии подтвержден
1110	Пользователь отменил запрос на открытие сессии
1111	Истекло время использования подтверждения запроса на открытие сессии
1112	Истекло время ожидания подтверждения запроса на открытие сессии
1114	Политика сессии успешно установлена для пользователя
1115	Политика успешно удалена
1117	Лицензия для сессий успешно зарегистрирована
1118	Запрос на просмотр учетных данных отклонен
1119	Пользователь отправил запрос на просмотр учетных данных
1120	Запрос на просмотр учетных данных подтвержден
1121	Пользователь отменил запрос на просмотр учетных данных
1122	Истекло время использования подтверждения запроса на просмотр учетных данных
1123	Истекло время ожидания подтверждения запроса на просмотр учетных данных
1124	Пользовательское подключение успешно добавлено для ресурса

Код	Текст сообщения
1125	Пользовательское подключение ресурса успешно изменено
1126	Пользовательское подключение ресурса успешно удалено
1127	Политика объекта успешно изменена
1128	Пароль учетной записи успешно исправлен
1129	SSH-ключ учетной записи успешно исправлен
1130	Приоритет политики успешно изменен
1131	Набор разделов политики успешно изменен
1132	Имя политики успешно изменено
1135	SSH-ключи, не управляемые PAM, успешно удалены
1136	Контейнер для поиска доменных ресурсов успешно удален
1137	Доменная привилегированная группа успешно удалена
1138	Администратор успешно добавлен в приложение
1139	Имя приложения успешно изменено
1140	Приложение успешно добавлено
1141	Администратор успешно исключен из приложения
1142	Приложение успешно удалено
1143	Пароль приложения успешно сброшен
1144	Описание приложения успешно изменено
1145	Пользователь успешно посмотрел учетные данные приложения
1146	Подразделение успешно создано
1147	Имя подразделения успешно изменено

Код	Текст сообщения
1148	Подразделение успешно удалено
1149	Параметр требования двухфакторной аутентификации для пользователя успешно изменен
1150	Приложение успешно получило учетные данные
1151	IP-адрес приложения успешно изменен
1152	Сертификат приложения успешно изменен
1153	Подразделение объекта успешно изменено
1154	Лицензия для AAPM успешно зарегистрирована
1155	Лицензия для пользователей успешно зарегистрирована
1156	Лицензия для ресурсов успешно зарегистрирована
1157	Группа пользователей успешно создана
1158	Группа пользователей успешно удалена
1159	Информация о группе пользователей успешно изменена
1160	Пользователь успешно добавлен в группу пользователей
1161	Пользователь успешно удален из группы пользователей
1162	Пользователь успешно аутентифицирован
1163	Приложение успешно аутентифицировано
1164	Пароль учетной записи успешно удален
1165	SSH-ключ учетной записи успешно удален
1166	Лицензия для сессий успешно удалена
1167	Лицензия для AAPM успешно удалена
1168	Лицензия для пользователей успешно удалена

Код	Текст сообщения
1169	Лицензия для ресурсов успешно удалена
1170	Сетевое расположение успешно создано
1171	Сетевое расположение успешно изменено
1172	Сетевое расположение успешно удалено
1173	Синхронизация группы каталога завершена
1174	Синхронизация групп каталога по расписанию запущена
1175	Синхронизация групп каталога завершена
1176	Сессия успешно создана
1178	Пользователь успешно активирован
1179	Пользователь успешно заблокирован
1181	Восстановлена связь с PAM агентом
1182	Служба успешно зарегистрирована
1183	Служба успешно удалена
1184	Информация о службе успешно изменена
1185	Пароль учетной записи службы успешно установлен
1186	Перезапуск службы: Успешно выполнен
1187	Перезапуск службы: Не требуется
1188	Тип сервисного подключения успешно создан
1189	Тип сервисного подключения успешно обновлен
1190	Тип сервисного подключения успешно удален
1191	Пользователь успешно создан

Код	Текст сообщения
1192	Тег успешно создан
1193	Тег успешно удален
1194	Тег успешно изменен
1195	Данные пользователя успешно изменены
1196	Пользователь успешно удален
1197	Лицензия для произвольных ресурсов успешно зарегистрирована
1198	Лицензия для произвольных ресурсов успешно удалена
1199	Лицензия для SQL Proxy успешно зарегистрирована
1200	Лицензия для SQL Proxy успешно удалена
1201	Открытый ключ успешно добавлен для пользователя
1202	Открытый ключ успешно удален у пользователя
1203	Пароль пользователя успешно сброшен
1204	Для пользователя включена смена пароля при следующем входе
1205	Пользователь успешно сменил пароль
1209	Сервер PAM добавлен в мониторинг
1210	Информация о сервере PAM обновлена в мониторинге
1211	Сервер PAM удален из мониторинга
1212	Subject сертификата для пользователя успешно изменен
1214	Штатная работа сервера восстановлена
1215	Идентификатор пользователя из внешнего Identity Provider успешно удален

Ошибка

Код	Текст сообщения
2000	Не удалось зарегистрировать учетную запись
2003	Не удалось изменить имя учетной записи
2004	Не удалось восстановить учетную запись
2008	Не удалось добавить пароль для учетной записи
2009	Не удалось отключить учетную запись
2010	Не удалось создать разрешение
2013	Не удалось отозвать разрешение
2014	Не удалось зарегистрировать ресурс
2015	Не удалось удалить ресурс
2016	Не удалось изменить информацию о ресурсе
2017	Не удалось открыть сессию
2018	В ходе завершения сессии возникла ошибка
2019	Не удалось сохранить текстовый журнал сессии
2020	Не удалось сохранить видеозапись сессии
2021	Не удалось сохранить параметры конфигурации
2022	Не удалось зарегистрировать домен
2023	Не удалось удалить домен
2024	Не удалось изменить информацию о домене
2025	Не удалось прервать сессию
2026	Не удалось включить учетную запись

Код	Текст сообщения
2027	Не удалось удалить учетную запись
2028	Не удалось отключить ресурс
2029	Не удалось включить ресурс
2030	Не удалось сохранить снимок экрана сессии
2031	Не удалось выполнить проверку пароля учетной записи
2032	Не удалось выполнить поиск учетных записей
2034	Не удалось сбросить пароль учетной записи
2035	Не удалось перевести учетную запись в состояние Игнорируется
2036	Не удалось создать политику
2037	Не удалось изменить имя политики
2038	Не удалось сохранить настройки политики
2039	Не удалось скопировать политику
2040	Не удалось изменить политику учетной записи
2041	Не удалось включить домен
2042	Не удалось восстановить домен
2043	Не удалось восстановить ресурс
2044	Не удалось аутентифицировать пользователя по второму фактору
2045	Не удалось сделать учетную запись управляемой
2046	Не удалось выполнить проверку SSH-ключа учетной записи
2048	Не удалось добавить SSH-ключ для учетной записи
2049	Не удалось сбросить SSH-ключ учетной записи

Код	Текст сообщения
2051	Не удалось открыть сервисное подключение к ресурсу
2053	Не удалось завершить синхронизацию учетных записей
2054	Не удалось открыть сервисное подключение к домену
2056	Не удалось завершить смену учетных данных
2058	Не удалось завершить проверку учетных данных
2060	Не удалось завершить проверку сервисного доступа
2064	Не удалось добавить SSH-шаблон
2065	Не удалось удалить SSH-шаблон
2066	Не удалось обновить SSH-шаблон
2067	Не удалось добавить пользовательское подключение
2068	Не удалось удалить пользовательское подключение
2069	Не удалось обновить пользовательское подключение
2070	Пользователю не удалось получить учетные данные
2071	Не удалось зарегистрировать лицензию
2073	Не удалось завершить ротацию артефактов сессии
2076	Не удалось удалить логи сессии
2078	Не удалось завершить синхронизацию ресурсов
2079	Хранилище сервера недоступно
2080	Не удалось изменить группы учетной записи
2082	Пользователю не удалось зарегистрировать второй фактор аутентификации
2083	Не удалось удалить аутентификатор пользователя

Код	Текст сообщения
2085	Не удалось возобновить действие разрешения
2086	Не удалось приостановить действие разрешения
2087	Не удалось синхронизировать информацию о ресурсе
2088	Не удалось зарегистрировать доменные привилегированные группы
2089	Не удалось изменить список контейнеров для поиска доменных ресурсов
2091	Не удалось завершить синхронизацию доменных ресурсов по расписанию
2092	Не удалось выполнить поиск доменных ресурсов
2095	Не удалось создать роль
2096	Не удалось удалить роль
2097	Не удалось изменить состав привилегий для роли
2098	Не удалось переименовать роль
2099	Не удалось добавить пользователя в состав роли
2100	Не удалось исключить пользователя из состава роли
2101	Не удалось создать группу ресурсов
2102	Не удалось удалить группу ресурсов
2103	Не удалось изменить информацию о группе ресурсов
2104	Не удалось добавить ресурс в группу ресурсов
2105	Не удалось удалить ресурс из группы ресурсов
2106	Не удалось использовать подтверждение запроса на открытие сессии
2107	Не удалось отклонить запрос на открытие сессии
2108	Не удалось отправить запрос на открытие сессии

Код	Текст сообщения
2109	Не удалось подтвердить запрос на открытие сессии
2110	Не удалось отменить запрос на открытие сессии
2114	Не удалось установить политику сессии для пользователя
2115	Не удалось удалить политику
2118	Не удалось отклонить запрос на просмотр учетных данных
2119	Не удалось отправить запрос на просмотр учетных данных
2120	Не удалось подтвердить запрос на просмотр учетных данных
2121	Не удалось отменить запрос на просмотр учетных данных
2124	Не удалось добавить пользовательское подключение для ресурса
2125	Не удалось изменить пользовательское подключение ресурса
2126	Не удалось удалить пользовательское подключение ресурса
2127	Не удалось изменить политику объекта
2130	Не удалось изменить приоритет политики
2131	Не удалось изменить набор разделов политики
2132	Не удалось изменить имя политики
2133	Не удалось выполнить проверку неуправляемых SSH-ключей учетной записи
2135	Не удалось удалить SSH-ключи, не управляемые PAM
2136	Не удалось удалить контейнер для поиска доменных ресурсов
2137	Не удалось удалить доменную привилегированную группу
2138	Не удалось добавить администратора в приложении
2139	Не удалось изменить имя приложения

Код	Текст сообщения
2140	Не удалось создать приложение
2141	Не удалось исключить администратора из приложения
2142	Не удалось удалить приложение
2143	Не удалось сбросить пароль для приложения
2144	Не удалось изменить описание приложения
2145	Не удалось посмотреть учетные данные приложения
2146	Не удалось создать подразделение
2147	Не удалось изменить имя подразделения
2148	Не удалось удалить подразделение
2149	Не удалось изменить параметр требования двухфакторной аутентификации для пользователя
2150	Приложению не удалось получить учетные данные
2151	Не удалось изменить IP-адрес приложения
2152	Не удалось изменить сертификат приложения
2153	Не удалось изменить подразделение объекта
2157	Не удалось создать группу пользователей
2158	Не удалось удалить группу пользователей
2159	Не удалось изменить информацию о группе пользователей
2160	Не удалось добавить пользователя в группу пользователей
2161	Не удалось удалить пользователя из группы пользователей
2162	Не удалось аутентифицировать пользователя
2163	Не удалось аутентифицировать приложение

Код	Текст сообщения
2164	Не удалось удалить пароль для учетной записи
2165	Не удалось удалить SSH-ключ для учетной записи
2170	Не удалось создать сетевое расположение
2171	Не удалось изменить информацию о сетевом расположении
2172	Не удалось удалить сетевое расположение
2173	Не удалось синхронизировать информацию о группе пользователей с каталогом
2175	Не удалось завершить синхронизацию групп каталога
2176	Не удалось создать сессию
2178	Не удалось активировать пользователя
2179	Не удалось заблокировать пользователя
2182	Не удалось зарегистрировать службу
2183	Не удалось удалить службу
2184	Не удалось изменить информацию о службе
2185	Не удалось установить пароль учетной записи службы
2186	Перезапуск службы: Не выполнен
2188	Не удалось создать тип сервисного подключения
2189	Не удалось обновить тип сервисного подключения
2190	Не удалось удалить тип сервисного подключения
2191	Не удалось создать пользователя
2192	Не удалось создать тег
2193	Не удалось удалить тег

Код	Текст сообщения
2194	Не удалось изменить тег
2195	Не удалось изменить данные пользователя
2196	Не удалось удалить пользователя
2201	Не удалось добавить открытый ключ для пользователя
2202	Не удалось удалить открытый ключ пользователя
2203	Не удалось сбросить пароль пользователя
2204	Не удалось включить смену пароля пользователя при следующем входе
2205	Не удалось сменить пароль пользователя
2207	Не удалось выполнить проверку ротации пароля или SSH-ключа учетной записи
2209	Ошибка добавления сервера PAM в мониторинг
2210	Ошибка обновления информации о сервере PAM
2211	Ошибка удаления сервера PAM из мониторинга
2212	Не удалось изменить Subject сертификата пользователя
2213	На сервере обнаружен сбой
2215	Не удалось удалить идентификатор пользователя из внешнего Identity Provider

Предупреждение

Код	Текст сообщения
3047	Произошла рассинхронизация SSH-ключа учетной записи
3061	Учетная запись не найдена
3084	Пользователь заблокирован

Код	Текст сообщения
3087	Данные ресурса были изменены
3093	Обнаружены незарегистрированные учетные записи
3094	Произошла рассинхронизация пароля учетной записи
3113	Попытка выполнить запрещенную команду
3116	Сессия прервана
3134	Обнаружены SSH-ключи, не управляемые PAM
3177	Группа пользователей не найдена в каталоге
3180	Потеряна связь с PAM агентом
3206	Обнаружены пользователи, не использующие PAM
3208	Обнаружены неиспользуемые разрешения

Привилегии

Данный раздел содержит список привилегий, которые могут быть включены в роли.

Идентификатор	Название
Управление пользователями	
User.Create	Добавление новых пользователей
User.Read	Просмотр профилей пользователей
User.Update	Редактирование данных пользователей
User.Delete	Удаление пользователей
User.Reset2FA	Сброс 2FA аутентификации для пользователя
User.SetPolicy	Установка политики для пользователя
User.ManageSshAuthorizedKeys	Управление пользовательскими ключами
User.PasswordManagement	Управление паролем внутреннего пользователя
User.ManageX509Certificate	Управление Subject X.509 сертификатами пользователей
Управление группами пользователей	
UsersGroup.Create	Добавление новых групп пользователей
UsersGroup.Read	Просмотр групп пользователей
UsersGroup.Update	Редактирование групп пользователей
UsersGroup.Delete	Удаление групп пользователей
UsersGroup.SetPolicy	Установка политики для групп пользователей
Управление разрешениями	

Идентификатор	Название
Permission.Create	Добавление новых разрешений
Permission.Read	Просмотр и поиск разрешений
Permission.Revoke	Отзыв разрешений
Permission.Suspend	Приостановка и возобновление разрешений
Управление учетными записями	
Account.Create	Добавление новых учетных записей
Account.Read	Просмотр учетных записей
Account.Update	Редактирование данных учетных записей
Account.Restore	Восстановление учетных данных УЗ на ранее используемые
Account.Delete	Удаление учетных записей
Account.Block	Блокировка и разблокировка учетных записей
Account.Manage	Сделать учетные записи управляемыми
Account.Ignore	Сделать учетные записи игнорируемыми
Account.SetPolicy	Установка политики для учетной записи
Account.Credentials.Check	Проверка учетных данных УЗ
Account.Credentials.Update	Смена учетных данных УЗ
Управление ресурсами	
Resource.Create	Добавление новых ресурсов
Resource.Read	Просмотр ресурсов
Resource.Update	Редактирование данных ресурсов
Resource.Restore	Восстановление ранее удаленных ресурсов

Идентификатор	Название
Resource.Delete	Удаление ресурсов
Resource.Block	Блокировка и разблокировка ресурсов
Resource.CheckConnection	Проверка соединения с ресурсом
Resource.Sync	Синхронизация данных и УЗ ресурса
Resource.SetPolicy	Установка политики для ресурса
Resource.SetOrganizationalUnit	Установка подразделения для ресурса
Resource.TagManagement	Управление тегами ресурсов
Управление группами ресурсов	
ResourcesGroup.Create	Добавление новых групп ресурсов
ResourcesGroup.Read	Просмотр групп ресурсов
ResourcesGroup.Update	Редактирование групп ресурсов
ResourcesGroup.Delete	Удаление групп ресурсов
ResourcesGroup.SetOrganizationalUnit	Установка подразделения для группы ресурсов
Управление доменами	
Domain.Create	Добавление новых доменов
Domain.Read	Просмотр доменов
Domain.Update	Редактирование данных доменов
Domain.Restore	Восстановление ранее удаленных доменов
Domain.Delete	Удаление доменов
Domain.CheckConnection	Проверка соединения с доменом
Domain.AccountsSync	Синхронизация УЗ домена

Идентификатор	Название
Domain.ResourcesImport	Импорт ресурсов из домена
Domain.SetPolicy	Установка политики для домена
Domain.PrivilegedGroups.Create	Добавление привилегированных групп домена
Domain.PrivilegedGroups.Read	Просмотр привилегированных групп домена
Domain.PrivilegedGroups.Delete	Удаление привилегированных групп домена
Domain.ResourceContainer.Create	Добавление контейнеров ресурсов домена
Domain.ResourceContainer.Read	Просмотр контейнеров ресурсов домена
Domain.ResourceContainer.Delete	Удаление контейнеров ресурсов домена
Управление сессиями	
Session.Read	Просмотр и поиск сессий
Session.Abort	Прерывание сессий
Управление запросами сессий	
SessionRequest.Read	Просмотр и поиск запросов сессий
SessionRequest.Confirm	Подтверждение сессий
Управление запросами на просмотр учетных данных	
CredentialsViewingRequest.Read	Просмотр и поиск запросов на просмотр учетных данных
CredentialsViewingRequest.Confirm	Подтверждение запросов на просмотр учетных данных
Журнал событий	
Event.Read	Просмотр и поиск событий в журнале

Идентификатор	Название
Управление политиками	
Policy.Create	Добавление новых политик
Policy.Read	Просмотр политик
Policy.Update	Редактирование политик
Policy.Delete	Удаление политик
Управление системными настройками	
SystemSettings.Read	Просмотр системных настроек
SystemSettings.Update	Редактирование системных настроек
Управление лицензиями	
License.Create	Добавление новых лицензий
License.Read	Просмотр лицензий
License.Delete	Удаление лицензий
Управление сервисными подключениями	
SshTemplate.Create	Импорт новых SSH-шаблонов
SshTemplate.Read	Просмотр SSH-шаблонов
SshTemplate.Delete	Удаление SSH-шаблонов
Управление пользовательскими подключениями	
UserConnectionType.Create	Добавление новых пользовательских подключений
UserConnectionType.Read	Просмотр пользовательских подключений

Идентификатор	Название
UserConnectionType.Update	Редактирование пользовательских подключений
UserConnectionType.Delete	Удаление пользовательских подключений
Управление ролями доступа	
Role.Create	Создание новых ролей
Role.Read	Просмотр ролей
Role.Update	Редактирование ролей
Role.Delete	Удаление ролей
Role.Members	Редактирование списка участников роли
Role.Claims	Редактирование набора привилегий роли
Управление группами получателей	
SubscriptionGroup.Create	Добавление новых групп получателей
SubscriptionGroup.Read	Просмотр групп получателей
SubscriptionGroup.Update	Редактирование групп получателей
SubscriptionGroup.Delete	Удаление групп получателей
Управление рассылками	
EventSubscription.Create	Добавление новых рассылок
EventSubscription.Read	Просмотр рассылок
EventSubscription.Delete	Удаление рассылок
Управление приложениями	
Application.Create	Добавление новых приложений

Идентификатор	Название
Application.Read	Просмотр приложений
Application.Update	Редактирование данных приложения
Application.Delete	Удаление приложений
Управление подразделениями	
OrganizationalUnit.Create	Добавление новых подразделений
OrganizationalUnit.Read	Просмотр подразделений
OrganizationalUnit.Update	Редактирование подразделений
OrganizationalUnit.Delete	Удаление подразделений
Управление сетевыми расположениями	
NetworkLocation.Create	Добавление новых сетевых расположений
NetworkLocation.Update	Редактирование сетевых расположений
NetworkLocation.Delete	Удаление сетевых расположений
Управление тегами	
Tag.Create	Добавление новых тегов
Tag.Update	Редактирование тегов
Tag.Delete	Удаление тегов
Управление типами сервисных подключений	
ServiceConnectionType.Create	Добавление новых типов сервисных подключений
ServiceConnectionType.Read	Просмотр типов сервисных подключений
ServiceConnectionType.Update	Редактирование типов сервисных подключений

Идентификатор	Название
ServiceConnectionType.Delete	Удаление типов сервисных подключений
Главная страница	
Dashboard.View	Просмотр страницы
Dashboard.Edit	Изменение конфигурации страницы

Соответствие атрибутов каталога пользователей и PAM

Данный раздел содержит список значений по умолчанию для атрибутов каталога пользователей и соответствующих им атрибутов Indeed PAM.

Active Directory, Samba DC и RED ADM

Атрибут каталога	Атрибут Indeed PAM	Описание
Пользователи		
objectGUID	ID	Идентификатор сущности
name	Name	Имя пользователя
userPrincipalName	PrincipalName	Логин с доменом в формате логин@домен. Пример: pamadmin@company.local
objectSID	SID	Уникальный идентификатор сущности в каталоге в формате SID. Пример: S-1-5-21-2418255240-4279612882-1152719259
distinguishedName	DistinguishedName	Путь до сущности в каталоге в формате DN. Пример: 'cn=pamadmin,cn=users,cn=accounts,dc=my,dc=company'
sAMAccountName	SamAccountName	Логин пользователя. Пример: pamadmin
thumbnailPhoto	ThumbnailPhoto	Миниатюра фотографии пользователя в формате JPEG или бинарного файла
jpegPhoto	JpegPhoto	Фотография пользователя в формате JPEG
Группы пользователей		
objectGUID	ID	Идентификатор сущности
name	Name	Имя группы

Атрибут каталога	Атрибут Indeed PAM	Описание
canonicalName	CanonicalName	Полный путь до группы в каталоге
objectSID	SID	Уникальный идентификатор сущности в каталоге в формате SID. Пример: S-1-5-21-2418255240-4279612882-1152719259
distinguishedName	DistinguishedName	Путь до сущности в каталоге в формате DN. Пример: 'cn=pamadmins,cn=users,cn=accounts,dc=my,dc=company'
sAMAccountName	SamAccountName	Уникальное имя группы

ALD PRO и FreeIPA

Атрибут каталога	Атрибут Indeed PAM	Описание
Пользователи		
entryUUID	ID	Идентификатор сущности
cn	Name	Имя пользователя
krbPrincipalName	PrincipalName	Логин с доменом в формате логин@домен. Пример: pamadmin@company.local
ipaNTSecurityIdentifier	SID	Уникальный идентификатор сущности в каталоге в формате SID. Пример: S-1-5-21-2418255240-4279612882-1152719259
ipaUniqueID	GUID	Уникальный идентификатор сущности в каталоге в формате GUID. Пример: 176f69c4-3f2b-11eb-89aa-005056980f49
entrydn	DistinguishedName	Путь до сущности в каталоге в формате DN. Пример: 'uid=pamadmin,cn=users,cn=accounts,dc=my,dc=company'
uid	SamAccountName	Логин пользователя. Пример: pamadmin

Атрибут каталога	Атрибут Indeed PAM	Описание
jpegPhoto	ThumbnailPhoto	Миниатюра фотографии пользователя в формате JPEG или бинарного файла
jpegPhoto	JpegPhoto	Фотография пользователя в формате JPEG
Группы пользователей		
ipaUniqueID	ID	Идентификатор сущности
cn	Name	Имя группы
cn	CanonicalName	Полный путь до группы в каталоге
ipaNTSecurityIdentifier	SID	Уникальный идентификатор сущности в каталоге в формате SID. Пример: S-1-5-21-2418255240-4279612882-1152719259
ipaUniqueID	GUID	Уникальный идентификатор сущности в каталоге в формате GUID. Пример: 176f69c4-3f2b-11eb-89aa-005056980f49
entryDn	DistinguishedName	Путь до сущности в каталоге в формате DN. Пример: 'uid=pamadmin,cn=users,cn=accounts,dc=my,dc=company'
cn	SamAccountName	Уникальное имя группы

OpenLDAP

Атрибут каталога	Атрибут Indeed PAM	Описание
Пользователи		
entryUUID	ID	Идентификатор сущности
cn	Name	Имя пользователя

Атрибут каталога	Атрибут Indeed PAM	Описание
entrydn	DistinguishedName	Путь до сущности в каталоге в формате DN. Пример: 'uid=pamadmin,cn=users,cn=accounts,dc=my,dc=company'
uid	SamAccountName	Логин пользователя. Пример: pamadmin
photo	ThumbnailPhoto	Миниатюра фотографии пользователя в формате JPEG или бинарного файла
photo	JpegPhoto	Фотография пользователя в формате JPEG
Группы пользователей		
entryUUID	ID	Идентификатор сущности
cn	Name	Имя группы
cn	CanonicalName	Полный путь до группы в каталоге
entryDn	DistinguishedName	Путь до сущности в каталоге в формате DN. Пример: 'uid=pamadmin,cn=users,cn=accounts,dc=my,dc=company'
cn	SamAccountName	Уникальное имя группы

История версий

В этом разделе содержится краткое описание изменений и улучшений в продукте Indeed Privileged Access Manager по версиям.

3.4

Аутентификация

- Добавлена поддержка протокола аутентификации Kerberos для сессий, открытых через RDP Proxy.
- Добавлена поддержка аутентификации по сертификатам X.509.
- Добавлена поддержка аутентификации по протоколу OpenID Connect.
- Улучшена аутентификация в RDP- и SSH-сессиях: если разрешение выдано на пользовательскую учетную запись и аутентификация в Indeed PAM пройдена от имени пользователя PAM, его логин и пароль подставляются в форму входа на ресурсе.
- Реализована возможность указывать формат логина для учетных записей при SSH-подключении.
- Утилита ConsoleApp теперь поддерживает вход от имени конкретного пользователя Indeed PAM, что позволяет применять индивидуальные привилегии и разграничивать права доступа.

Интеграции

- Расширен функционал AAPM — добавлены интеграции с Ansible Lookup Plugin и Python SDK для управления учетными данными Indeed PAM.
- Добавлена поддержка подключения Ansible к ресурсам через SSH Proxy.

Другие изменения

- Добавлена поддержка работы буфера обмена для сессий, открытых через Web Proxy.
- Добавлен механизм проверки состояний серверов, компонентов и сервисов Indeed PAM. Результаты отображаются на дашборде в новом виджете Серверы PAM.
- Улучшен механизм создания отчетов — теперь отчеты по сессиям, событиям и разрешениям формируются в фоновом режиме. В разделе История отчетов можно скачать сформированный отчет.
- В карточках сессий и событий добавлена информация о сервере доступа.

3.3

- Добавлена возможность открывать веб-сессии через новый компонент Web Proxy.
- Добавлена возможность открывать RDP- и SSH-сессии в браузере через новый компонент Web-терминал.
- Добавлен новый раздел **Дашборд**.
- Добавлена возможность открывать сессии без повторной аутентификации.
- Добавлена возможность в разрешении задать дни недели.
- В конфигурации появилась возможность задать автоматический выход из консолей пользователя и администратора.
- Добавлена поддержка алгоритма Ed25519 для SSH-ключей.
- Улучшен механизм блокировки: теперь блокировка распространяется не только на пользователей, но и на администраторов PAM. При блокировке доступ в систему полностью прекращается.
- Добавлена поддержка Microsoft SQL Server в SQL Proxy.

3.2

- Добавлена аутентификация по SSH-ключам в SSH Proxy.
- Добавлена возможность создавать внутренних пользователей.
- Изменено лицензирование инсталляции. Для подключения к произвольным ресурсам и PostgreSQL Proxy теперь требуются отдельные лицензии. Подключение к PostgreSQL Proxy работает в режиме раннего доступа до 31 декабря 2026 г., после чего требуется приобретение лицензий.
- Добавлен механизм автоматического выявления разрешений, которыми давно не пользовались. Срок актуальности разрешений определяется в конфигурации.

3.1

- Добавлена поддержка LDAP-каталога RED ADM версий 1.1.0–1.2.2.
- Добавлена поддержка LDAP-каталога Samba DC версий 4.13–4.21.
- Добавлена возможность использовать теги для ресурсов.
- В политики сессий добавлена опция **Сообщение, которое пользователь увидит при запросе причины**.
- Улучшен поиск сессий: добавлена возможность искать по состоянию и причине завершения сессии.

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.