Indeed Access Manager

Техническая документация

Версия: 9.3

Дата: 05.05.2026

Содержание

О продукте

Indeed Access Manager (Indeed AM) позволяет построить систему централизованного управления доступом к информационным ресурсам компании.

Indeed AM включает в себя различные модули для интеграции с целевыми системами, в том числе с применением технологий SAML, OpenID Connect, FreeRADIUS, ADFS, а также с использованием агентов аутентификации.

Такой подход позволяет защитить доступ во все информационные системы предприятия и адаптировать решение под ваши нужды.

Модули интеграции в Indeed AM

Аутентификация и управление доступом

Indeed AM не только дает возможность применять надежные технологии аутентификации пользователей, но и реализует функции управления доступом, такие как SSO и разграничение доступа для разных групп пользователей.

Различные методы аутентификации можно объединять в цепочки для создания мультифакторной аутентификации (MFA). Архитектура решения позволяет оперативно добавлять поддержку новых технологий.

Технологии аутентификации в Indeed AM

Установка

Indeed Access Manager использует схему развертывания на стороне пользователя (on-premise) — непосредственно в вашем рабочем окружении или собственном дата-центре. Вы полностью контролируете среду функционирования системы аутентификации пользователей, данные которой хранятся локально и не передаются в облачное хранилище.

Indeed AM поддерживает масштабирование мощностей — установку в режиме кластера. Это обеспечивает требуемые уровни отказоустойчивости и производительности и не требует приобретения дополнительных лицензий.

Базовые компоненты

В основе платформы лежат базовые модули, которые реализуют бизнес-логику системы и обеспечивают функционирование серверной инфраструктуры и инструментов управления.

Сервер аутентификации и управления Core Server

Сервер является ядром системы и обеспечивает функционирование всей платформы, он выполняет аутентификацию пользователей и реализует бизнес-логику решения. Сервер представляет собой ASP .Net приложение и поддерживает установку в режиме кластера, позволяя обеспечить высокий уровень производительности и отказоустойчивости вне зависимости от масштабов внедрения.

Каталог пользователей

Indeed AM использует данные о конечных пользователях из каталога пользователей. Это те пользователи, которые будут проходить процедуру аутентификации с помощью Indeed AM.

Базы данных

Все данные системы хранятся в едином хранилище, к которому напрямую обращается только сервер. Хранение и передача данных к серверу или от сервера производится в зашифрованном виде. Хранилище может быть расположено в Microsoft SQL или PostgreSQL.

Management Console

Выполнена в формате веб-приложения, в котором администраторы Indeed AM могут просмотреть и изменить параметры системы и настройки пользователей, а также просмотреть журнал системы.

User Console

Дает возможность зарегистрировать или изменить аутентификационные данные (например, генераторы одноразовых паролей), а также просмотреть историю входов.

Модули интеграции

Indeed ADFS Extension

Двухфакторная аутентификация с использованием ADFS

Indeed FreeRADIUS Extension

Двухфакторная аутентификация для протокола RADIUS

Indeed Identity Provider

Многофакторная аутентификация и сквозной доступ

Indeed LDAP Proxy

Двухфакторная аутентификация по протоколу LDAP

Indeed Linux Logon

Доступ в Linux с помощью строгой аутентификации

Indeed RDP Windows Logon

Двухфакторная аутентификация для протокола Remote Desktop Protocol

Indeed Windows Logon

Доступ в Windows с помощью строгой аутентификации

Indeed ADFS Extension

Для интеграции веб-приложений с программным комплексом Indeed Access Manager может использоваться механизм ADFS в связке с компонентом Indeed ADFS Extension. Интеграция возможна для приложений, которые поддерживают аутентификацию через ADFS.

Компонент ADFS Extension реализует адаптер многофакторной аутентификации для сервера Microsoft ADFS, добавляя в процесс получения доступа второй фактор. Такой подход дает возможность интегрироваться с целевыми приложениями без их модификации.

При входе в приложение пользователь перенаправляется на веб-страницу аутентификации ADFS, где через провайдер аутентификации Indeed ADFS Extension запрашивается второй фактор. После успешной аутентификации пользователь возвращается в целевое приложение.

Установка и настройка ADFS Extension

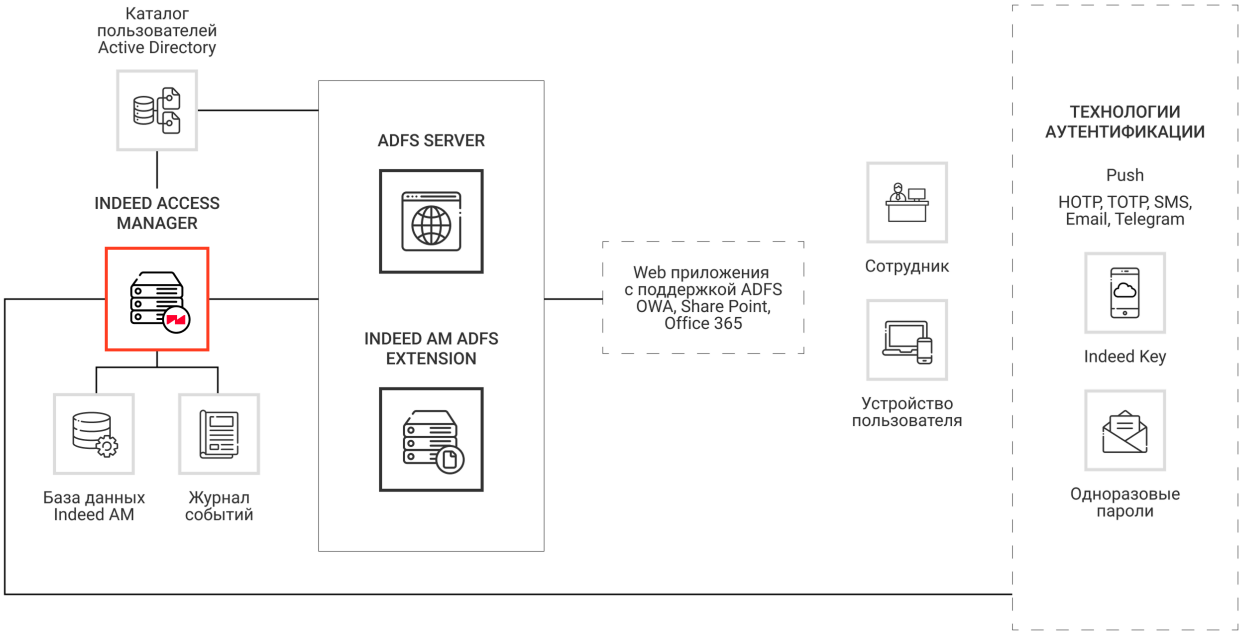
Технологии аутентификации

Indeed AM ADFS Extension в качестве второго фактора поддерживает аутентификацию с помощью следующих технологий:

- одноразовые пароли OATH, TOTP и HOTP;
- одноразовые коды через СМС и email;
- одноразовые коды и push-уведомления в мобильном приложении Indeed Key;
- самостоятельно заданный пароль.

Где можно использовать

Технологию ADFS поддерживают веб-приложения Microsoft, такие как Outlook Web Access, Sharepoint, Skype for Business и другие.


Каталог пользователей Active Directory
INDEED ACCESS MANAGER
ADFS SERVER
INDEED AM ADFS EXTENSION
База данных Indeed AM
Журнал событий
Web приложения с поддержкой ADFS OWA, Share Point, Office 365
Сотрудник
Устройство пользователя
ТЕХНОЛОГИИ АУТЕНТИФИКАЦИИ
Push
HOTP, TOTP, SMS, Email, Telegram
Indeed Key
Одноразовые пароли

Indeed FreeRADIUS Extension

Indeed FreeRADIUS Extension (FreeRADIUS Extension) позволяет реализовать технологию двухфакторной аутентификации для RADIUS-совместимых сервисов и приложений.

Установка и настройка FreeRADIUS Extension

Технологии аутентификации

FreeRADIUS Extension в качестве второго фактора поддерживает аутентификацию с помощью следующих технологий:

- одноразовые пароли TOTP и HOTP;
- одноразовые коды через СМС и email;
- push-уведомления с подтверждением входа в мобильном приложении Indeed Key.

Где можно использовать

Аутентификация по протоколу RADIUS может быть использована во многих VPN, VDI и PAM решениях, например в программных продуктах Cisco ASA, MS RAS, RDG, OpenVPN, pfSense, Check Point.

Indeed Identity Provider

Для организации многофакторной аутентификации и сквозного доступа в веб-приложения (Web Single Sign-on) используется модуль Indeed Identity Provider (IDP). Для интеграции с целевыми решениями этот модуль поддерживает следующие протоколы:

- SAML 2.0 (Security Assertion Markup Language)
- OIDC 1.0 (OpenID Connect)
- OAuth 2.0

Это гарантирует совместимость с широким спектром коммерческих систем. Применение IDP избавляет пользователя от необходимости запоминать множество учетных данных: для доступа во все интегрированные системы требуется только один комплект учетных данных. Аутентификация выполняется централизованно на стороне Identity Provider (IDP, поставщик удостоверений).

IDP выполнен в формате веб-приложения и разворачивается в инфраструктуре заказчика. В процессе получения доступа целевое приложение перенаправляет пользователя на страницу IDP для аутентификации, после чего в случае успеха пользователь перенаправляется обратно в целевое приложение с признаком *Аутентифицирован*, где ему открывается его сессия.

Установка и настройка Identity Provider

Технологии аутентификации

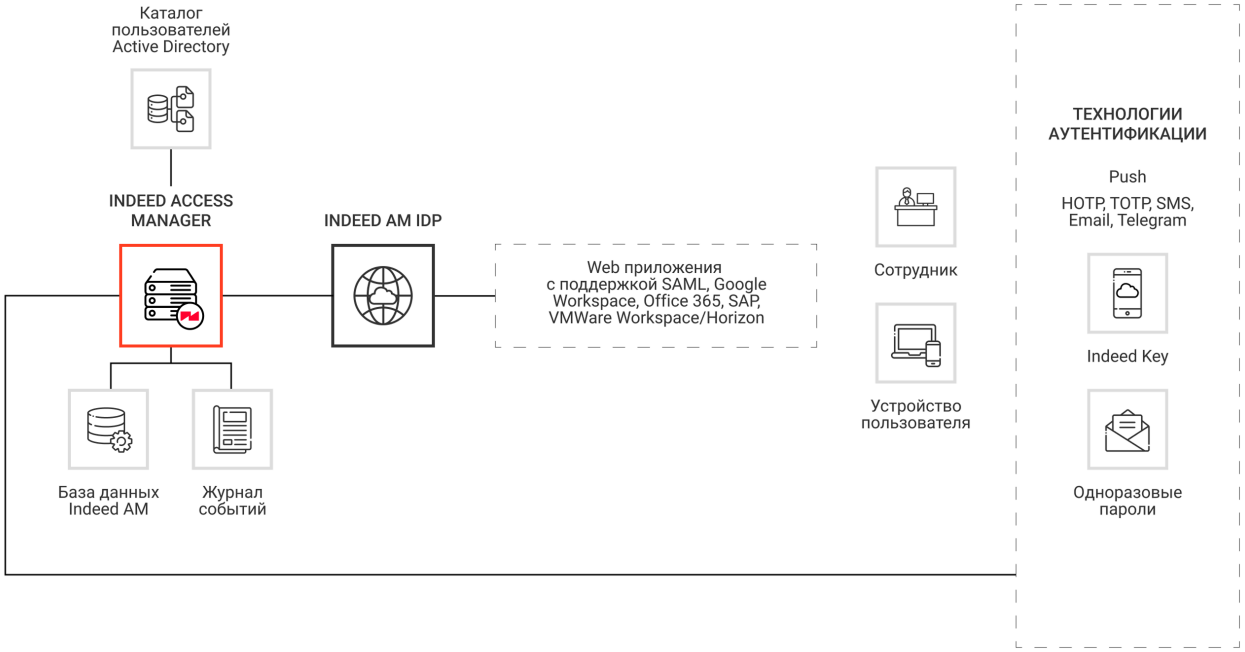
Indeed IDP поддерживает следующие технологии аутентификации пользователей:

- доменный пароль;
- одноразовые пароли OATH, TOTP и HOTP;
- одноразовые коды через СМС и email;
- одноразовые коды и push-уведомления через бот в мессенджере Telegram;
- одноразовые коды и push-уведомления в мобильном приложении Indeed Key.

Где можно использовать

В контур WebSSO и MFA могут быть включены как корпоративные on-premise приложения (например решения от компаний SAP, Citrix и др.), так и облачные сервисы, такие как Office 365, Salesforce, Slack, Google Workspace (ранее G Suite) и другие.

Интеграция выполняется на серверной стороне, что дает возможность использовать MFA и WebSSO подход на любых устройствах, где есть браузер: ПК, смартфон или планшет.


Каталог пользователей Active Directory
INDEED ACCESS MANAGER
INDEED AM IDP
Web приложения с поддержкой SAML, Google Workspace, Office 365, SAP, VMWare Workspace/Horizon
Сотрудник
Устройство пользователя
База данных Indeed AM
Журнал событий
ТЕХНОЛОГИИ АУТЕНТИФИКАЦИИ
Push
HOTP, TOTP, SMS, Email, Telegram
Indeed Key
Одноразовые пароли

Indeed LDAP Proxy

Модуль Indeed LDAP Proxy (LDAP Proxy) используется для реализации двухфакторной аутентификации в приложениях с LDAP-аутентификацией.

Основные возможности LDAP Proxy:

- работа по протоколам LDAP и LDAPS через зашифрованный TLS-канал;
- перехват запросов на аутентификацию с использованием механизма Simple;
- возможность настройки доступа сервисных учетных записей без использования второго фактора аутентификации, основываясь на политике доступа;
- использование второго фактора аутентификации в зависимости от того, принадлежит ли пользователь к группе в каталоге пользователей, основываясь на политике доступа;
- запись журналов в Log Server.

Установка и настройка LDAP Proxy

Технологии аутентификации

LDAP Proxy поддерживает следующие технологии аутентификации пользователей:

- доменный пароль,
- push-уведомления в мобильном приложении Indeed Key,
- push-уведомления в Telegram.

Indeed Linux Logon

Indeed AM Linux Logon — это модуль аутентификации, позволяющий реализовать двухфакторную аутентификацию для операционной системы Linux.

Работа модуля реализована через автоматизированную интеграцию с инфраструктурой Pluggable Authentication Modules (PAM) — с помощью этого Linux Logon может обращаться к Core Server напрямую.

Установка и настройка Linux Logon

Технологии аутентификации

Linux Logon поддерживает следующие технологии аутентификации пользователей:

- доменный пароль,
- одноразовые пароли TOTP,
- самостоятельно заданный пароль.

Indeed RDP Windows Logon

Модуль Indeed RDP Windows Logon (RDP Windows Logon) используется для реализации двухфакторной аутентификации при подключениях по протоколу RDP. В этом случае первым фактором выступает доменный пароль, а вторым — одноразовый пароль (one-time password) или подтверждение входа в отдельном приложении.

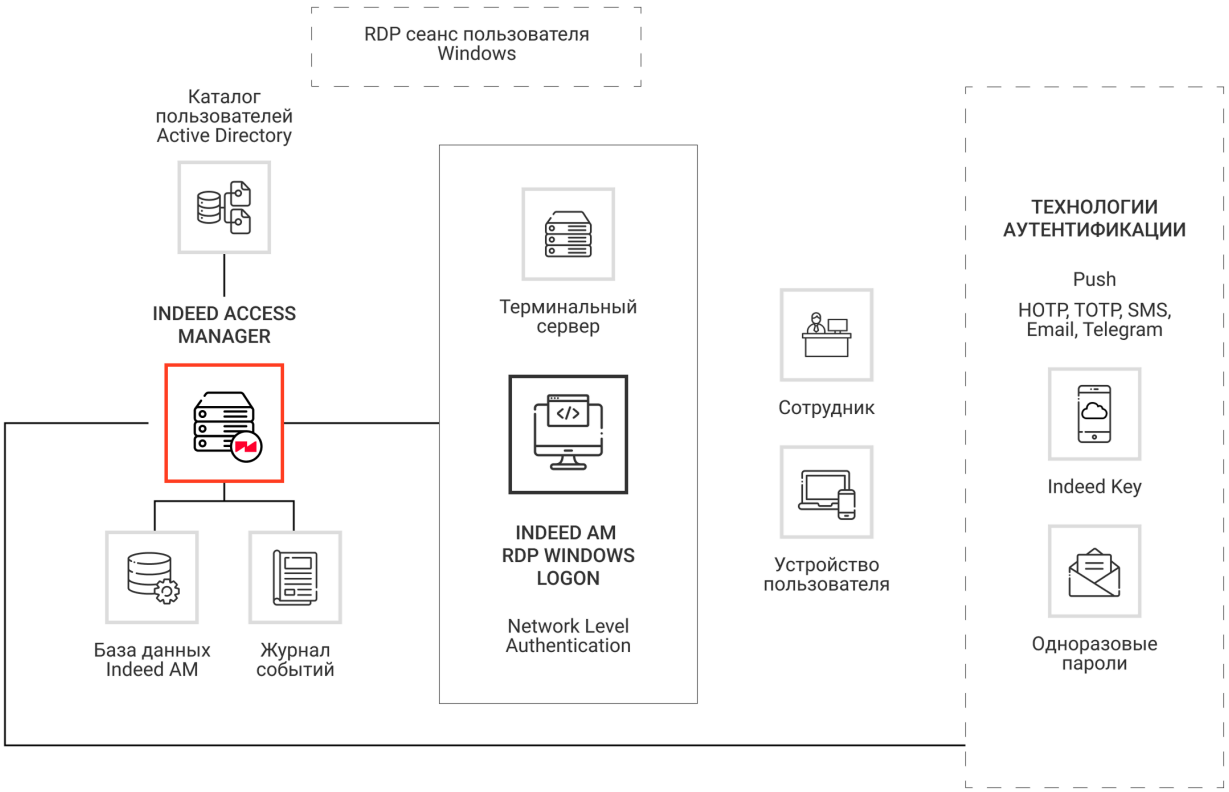
RDP Windows Logon устанавливается на конечный терминальный сервер, куда выполняет вход пользователь. Установка каких-либо компонентов на клиентский компьютер не требуется. Поддерживается конфигурация с Remote Desktop Gateway.

Установка и настройка RDP Windows Logon

Технологии аутентификации

RDP Windows Logon поддерживает следующие технологии аутентификации пользователей:

- одноразовые пароли TOTP и HOTP;
- одноразовые коды через СМС и email;
- push-уведомления в мобильном приложении Indeed Key;
- самостоятельно заданный пароль.



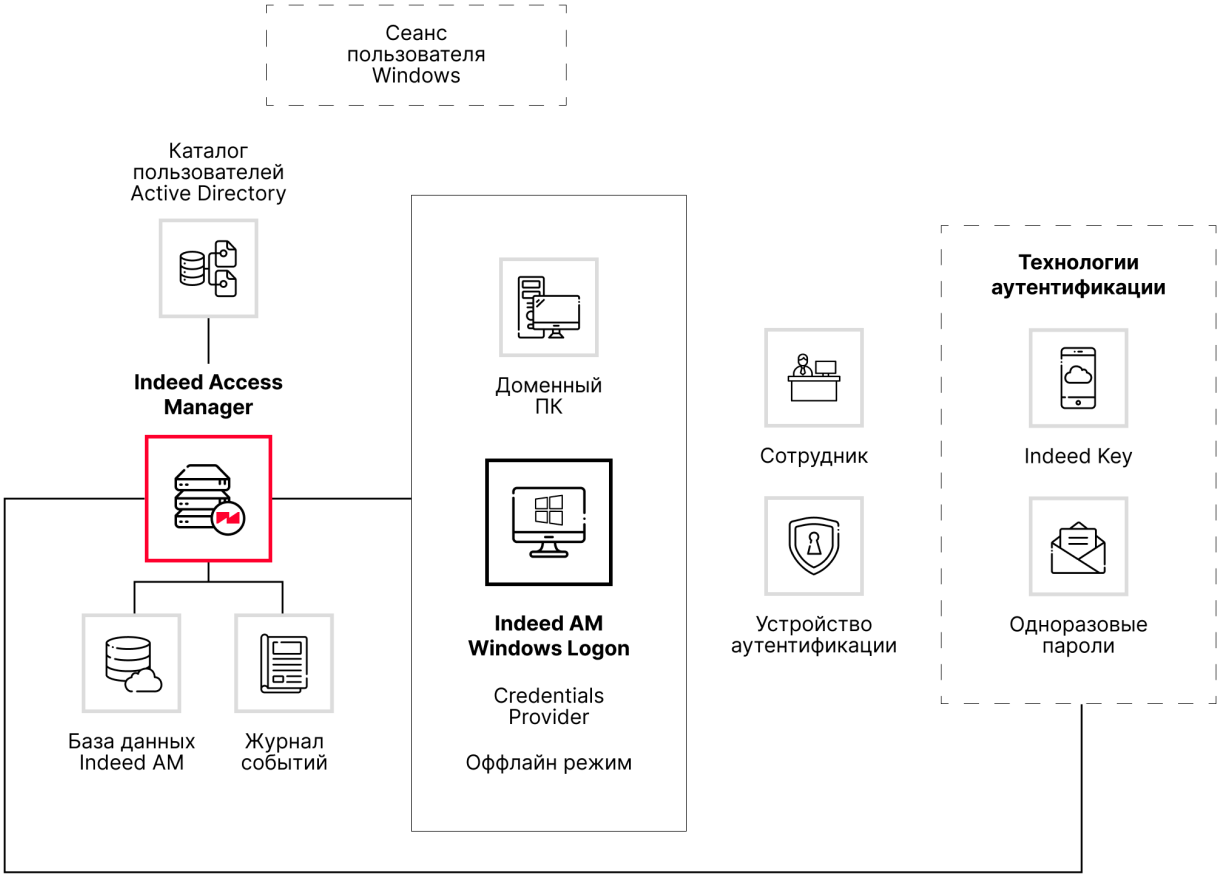
Indeed Windows Logon

Indeed Windows Logon (Windows Logon) представляет возможность получать доступ в Windows с использованием технологий строгой аутентификации в среде Microsoft Active Directory. Для этого на рабочие места пользователей устанавливается агент Windows Logon.

Инсталлятор агента реализован как стандартный пакет установщика MSI (Microsoft Windows Installer). Это позволяет оперативно производить установку и обновление системы в массовом порядке с использованием различных инструментов: групповых политик Active Directory, Microsoft System Center Configuration Manager (SCCM) и других.

Для интеграции с операционной системой Windows используется стандартный механизм для реализации собственного интерфейса аутентификации пользователей Credentials Provider. Данная технология позволяет сторонним разработчикам интегрировать собственные технологии аутентификации с интерфейсом Windows, предоставляет возможность не только выполнять вход в Windows с помощью технологии Indeed AM, но и аутентифицироваться с помощью Indeed AM внутри ОС, например, при доступе к доменным ресурсам или веб-приложениям.

Установка и настройка Windows Logon



Технологии аутентификации

Windows Logon поддерживает следующие технологии аутентификации:

- доменный пароль;
- одноразовые пароли TOTP и HOTP;
- одноразовые коды через СМС и email;
- одноразовые коды и push-уведомления в мобильном приложении Indeed Key.

Управление паролями пользователей Active Directory

Indeed Access Manager не заменяет штатную систему аутентификации Active Directory, а автоматизирует управление паролями пользователей. В такой конфигурации парольная аутентификация становится внутренним механизмом, который используется только на программном уровне.

Администратор Indeed Access Manager может настроить систему таким образом, чтобы в момент регистрации первого для пользователя аутентификатора его пароль автоматически менялся на случайное значение, которое не сообщается ни пользователю, ни администратору системы. Таким образом доступ в домен становится возможным только с использованием Windows Logon. В дальнейшем пароль пользователя меняется автоматически либо по требованию операционной системы, либо по заданному расписанию.

Технологии аутентификации

Провайдеры аутентификации обеспечивают Indeed AM возможность работы с технологиями аутентификации пользователей.

Провайдер аутентификации предоставляет системе унифицированный интерфейс для выполнения операций по работе с конкретной технологией аутентификации: получение аутентификационных данных от пользователя для хранения, а также верификацию (проверку) данных.

Установка и настройка провайдеров аутентификации

Indeed Access Manager поддерживает следующие технологии аутентификации:

- аппаратные и программные токены генерации одноразовых паролей по протоколам OATH, TOTP и HOTP;
- одноразовые коды, высылаемые по СМС или email;
- одноразовые коды и push-уведомления через бот в мессенджере Telegram;
- одноразовые коды и push-уведомления в мобильном приложении Indeed Key.

Мобильное приложение Indeed Key доступно для операционных систем iOS, Android и HarmonyOS. Используя Indeed Key, пользователь подтверждает операцию входа в приложении на смартфоне. Детали операции отображаются на экране смартфона, где пользователь может убедиться, в какую именно систему выполняется вход. Кроме этого, Indeed Key поддерживает генерацию одноразовых паролей по протоколу TOTP.

Различные методы аутентификации можно объединять в цепочки для создания мультифакторной аутентификации (MFA).

Политики доступа

Политика — это набор настроек, которые применяются к определенной группе пользователей из пользовательского каталога.

На всех пользователей, которые попадают под действие политики, распространяются настройки базовых компонентов и модулей интеграции. Также пользователи получают доступ к бизнес-приложениям с настроенными учетными записями.

У политики могут быть определены:

- область действия: пользователи, которые попадают под действие правил, заданных в этой политике;
- роли: администратор, оператор и инспектор;
- набор и настройки доступных способов аутентификации;
- набор доступных бизнес-приложений и учетных записей eSSO;
- приоритет политики.

Если пользователь попадает в область действия более одной политики, он получает доступ ко всем приложениям, добавленным в эти политики.

Если пользователь попадает в область действия нескольких политик, где одно и то же приложение встречается более одного раза, пользователю присваиваются настройки доступа в это приложение из политики с наибольшим приоритетом.

Лицензирование

В продуктах Indeed Access Manager (Indeed AM) используются схема лицензирования CAL (Client Access License). Такая лицензия дает право на использование продуктов Indeed AM для одного пользователя. Учитывается количество учетных записей пользователей Indeed AM, при этом количество установок клиентского программного обеспечения не ограничивается.

Лицензии можно докупить. При необходимости можно отозвать лицензию у одних сотрудников и выделить другим.

Как управлять лицензиями в Management Console

Лицензии Indeed Access Manager делятся на следующие типы:

- основная лицензия Indeed Access Manager,
- лицензии для дополнительных модулей.

Основная лицензия

Это базовая лицензия. Она дает право на регистрацию пользователя в системе, хранение его аутентификационной информации в базе данных и использование базовых функций — консоли администратора, консоли пользователя и журнала событий. Приобретение этой лицензии требуется в любом случае вне зависимости от требуемой функциональности решения.

Лицензии для дополнительных модулей

Лицензия позволяет использовать определенный модуль. Лицензии требуются для всех модулей интеграции. Все бизнес-приложения модуля работают под лицензией модуля, отдельные лицензии для них не требуются.

Лицензия на модуль содержит разрешенное количество ее использований. После регистрации лицензии ее объекты могут быть выданы пользователям автоматически, это происходит при процессе аутентификации.

Отзыв лицензии для конкретного пользователя также происходит автоматически, с помощью регулярно возобновляемой задачи, если пользователь в каталоге был заблокирован или потерял права на использование модуля.

- *Лицензия Indeed AM Windows Logon*. Дает право на использование модуля Windows Logon для строгой и многофакторной аутентификации в операционных системах Microsoft Windows.
- *Лицензия Indeed AM RDP Windows Logon*. Дает право на использование модуля RDP Windows Logon для двухфакторной аутентификации с использованием одноразовых паролей при терминальном доступе в операционные системы Microsoft Windows.
- *Лицензия Indeed AM Linux Logon*. Дает право на использование модуля Linux Logon для строгой и многофакторной аутентификации в операционных системах Linux.

- *Лицензия Indeed AM Identity Provider*. Дает право на использование модуля Identity Provider для построения системы Web Single Sign-On с применением протоколов SAML и OpenID Connect.
- *Лицензия Indeed AM FreeRADIUS Extension*. Дает право на использование модуля FreeRADIUS для реализации двухфакторной аутентификации в приложениях, совместимых с протоколом RADIUS (VPN, VDI и другими).
- *Лицензия Indeed AM LDAP Proxy*. Дает право на использование модуля LDAP Proxy для реализации двухфакторной аутентификации в приложениях, в которых основным методом аутентификации пользователей является LDAP-каталог.
- *Лицензия Indeed AM API*. Дает право на использование программного интерфейса для интеграции со сторонними системами.
- *Лицензия Indeed AM ADFS Extension*. Дает право на использование модуля ADFS для построения системы с применением протокола ADFS.

Системные требования

Серверные компоненты

Системные требования для серверных компонентов

Модули интеграции

Системные требования для модулей интеграции

Серверные компоненты

В разделе описаны системные требования для серверных компонентов Indeed Access Manager.

Мастер конфигурации

Аппаратные требования	• Не менее 4 ГБ оперативной памяти • Не менее 50 ГБ свободного пространства на диске
Операционная система	Linux с поддержкой 64-битной архитектуры: • Astra Linux 1.7 и выше • РЕД ОС 7.3 и выше • Ubuntu 22.04 и выше
Пакеты	• Docker 19.03.0 и выше • Docker Compose 2.0.0 и выше Рекомендуется устанавливать Docker из официального репозитория по инструкции на сайте docs.docker.com. Примечание: При установке Access Manager на операционной системе Ubuntu убедитесь, что Docker или Docker Compose установлены с помощью системы управления пакетами apt (Advanced Package Tool).
Сертификаты (опционально)	• Публичный сертификат домена в формате Base-64 • Сертификат, выписанный на DNS-имя машины
Соединение	• SSH-соединение между мастером конфигурации и целевым хостом, на котором будет установлен Access Manager • Соединение с базой данных (опционально)
Веб-браузер	• Google Chrome • Mozilla Firefox • Microsoft Edge

Indeed Core Server

Аппаратные требования	• Не менее 4 ГБ оперативной памяти • Не менее 50 ГБ свободного пространства на диске

Операционная система	Linux с поддержкой 64-битной архитектуры: • Astra Linux • РЕД ОС • Ubuntu
Домен	• Active Directory • FreeIPA 4.10 и выше
База данных	• Microsoft SQL Server 2012 всех редакций и более новые версии • PostgreSQL 14.4 и выше с пакетом contrib • PostgreSQL Pro 14.4 и выше с пакетом contrib
Пакеты	• Docker 19.03.0 и выше • Docker Compose 2.0.0 и выше Рекомендуется устанавливать Docker из официального репозитория по инструкции на сайте docs.docker.com.
Сертификаты	• Публичный сертификат домена в формате Base-64 • Сертификат, выписанный на DNS-имя машины
Соединение	• Соединение по протоколу LDAPS между сервером Access Manager и Active Directory • Соединение между сервером Access Manager и базой данных
Веб-браузер	• Google Chrome • Mozilla Firefox • Microsoft Edge

Indeed Log Server

Аппаратные требования	• Не менее 4 ГБ оперативной памяти • Не менее 50 ГБ свободного пространства на диске
Операционная система	Linux с поддержкой 64-битной архитектуры: • Astra Linux • РЕД ОС • Ubuntu

База данных	• Microsoft SQL Server 2012 всех редакций и более новые версии • PostgreSQL 14.4 и выше с пакетом contrib • PostgreSQL Pro 14.4 и выше с пакетом contrib
Пакеты	• Docker 19.03.0 и выше • Docker Compose 2.0.0 и выше Рекомендуется устанавливать Docker из официального репозитория по инструкции на сайте docs.docker.com.
Сертификаты	• Публичный сертификат домена в формате Base-64 • Сертификат, выписанный на DNS-имя машины
Соединение	• Соединение между сервером Access Manager и базой данных

Indeed Management Console

Аппаратные требования	• Не менее 4 ГБ оперативной памяти • Не менее 50 ГБ свободного пространства на диске
Операционная система	Linux с поддержкой 64-битной архитектуры: • Astra Linux • РЕД ОС • Ubuntu
Пакеты	• Docker 19.03.0 и выше • Docker Compose 2.0.0 и выше Рекомендуется устанавливать Docker из официального репозитория по инструкции на сайте docs.docker.com.
Сертификаты	• Публичный сертификат домена в формате Base-64 • Сертификат, выписанный на DNS-имя машины
Соединение	• Соединение с Core Server, Log Server, Identity Provider
Веб-браузер	• Google Chrome • Mozilla Firefox • Microsoft Edge

Indeed User Console

Аппаратные требования	• Не менее 4 ГБ оперативной памяти • Не менее 50 ГБ свободного пространства на диске
Операционная система	Linux с поддержкой 64-битной архитектуры: • Astra Linux • РЕД ОС • Ubuntu
Пакеты	• Docker 19.03.0 и выше • Docker Compose 2.0.0 и выше Рекомендуется устанавливать Docker из официального репозитория по инструкции на сайте docs.docker.com.
Сертификаты	• Публичный сертификат домена в формате Base-64 • Сертификат, выписанный на DNS-имя машины
Соединение	• Соединение с Core Server, Identity Provider
Веб-браузер	• Google Chrome • Mozilla Firefox • Microsoft Edge

Indeed Key Server

> **ИНФОРМАЦИЯ**
>
> Сервер поддерживает работу вне домена.

Операционная система	Linux с поддержкой 64-битной архитектуры: • Astra Linux • РЕД ОС • Ubuntu

База данных	• Microsoft SQL Server 2012 SP2 всех редакций • Microsoft SQL Server 2014 всех редакций • Microsoft SQL Server 2016 всех редакций • Microsoft SQL Server 2019 всех редакций • PostgreSQL с пакетом contrib • PostgreSQL Pro с пакетом contrib
Аппаратные требования	Аппаратные требования совпадают с требованиями, предъявляемыми к операционным системам, на которых функционирует ПО. • Не менее 8 ГБ оперативной памяти • Не менее 200 ГБ свободного пространства на диске

Взаимодействие с мобильным приложением Indeed Key	• Для отправки push-уведомлений серверу Indeed Key требуется внешний доступ к интернету (для доступа к *fcm.googleapis.com:443* и *oauth2.googleapis.com:443*).
	• Сервер Indeed Key должен быть доступен по указанному в настройках имени dns и порту (данные параметры задаются при настройке Indeed Key) из внешней сети.
	• Имя DNS-сервера Indeed Key не должно содержать нижнего подчеркивания _.
	• Для отправки push-уведомлений на устройства Huawei требуется доступ к сервису HUAWEI Push по следующим адресам:
	  ◦ push-api.cloud.huawei.com
	  ◦ oauth-login.cloud.huawei.com

Требования к сертификатам для устройств

При использовании сертификатов стороннего удостоверяющего центра (УЦ) необходимо убедиться, что выпускаемые им сертификаты соответствуют установленным требованиям, описанным далее. При использовании собственных сертификатов корневой сертификат должен быть установлен на устройстве и должно быть настроено доверие к сертификату.

Также вы можете связаться с командой поддержки и запросить сертификаты для клиентских IKS. Такие сертификаты будут автоматически признаны приложением Indeed AM без необходимости дополнительной установки на устройстве.

> **ИНФОРМАЦИЯ**
>
> Требования к расширению ExtendedKeyUsage (EKU) и сроку действия появились осенью 2019 года для сертификатов, выпущенных после 1 июля 2019. Сертификаты, выпущенные ранее, принимаются устройствами на базе iOS без указания идентификатора объекта и сроком действия.

- сертификаты и выдающие их центры сертификации, использующие ключи RSA, должны использовать ключи размером 2048 бит или более;
- сертификаты и выдающие их центры сертификации должны использовать алгоритм хеширования из семейства SHA-2 для создания цифровой подписи;
- сертификаты должны содержать имя сервера DNS с использованием расширения Subject Alternative Name сертификата;
- сертификаты должны включать расширение ExtendedKeyUsage (EKU), содержащее идентификатор объекта id-kp-serverAuth;
- срок действия сертификатов сервера должен составлять 825 дней или менее.

Модули интеграции

Программные требования

Для установки каждого модуля необходима развернутая система Indeed Access Manager с зарегистрированными лицензиями для соответствующего модуля.

Как работает лицензирование в Indeed Access Manager

Indeed Identity Provider

Операционная система	Linux с поддержкой 64-битной архитектуры: • Astra Linux • РЕД ОС • Ubuntu
Пакеты	• Docker 19.03.0 и выше • Docker Compose 2.0.0 и выше • Tar • OpenSSL Рекомендуется устанавливать Docker из официального репозитория по инструкции на сайте docs.docker.com.
Сертификаты	• Публичный сертификат домена в формате Base-64 • Сертификат, выписанный на DNS-имя машины
Требования к окружению клиентской части	• Internet Explorer 11 • Google Chrome 42.0 и выше • Mozilla FireFox 37.0 и выше • Opera 28.0 и выше • MS Edge

ИНФОРМАЦИЯ

Чтобы избежать потенциальных уязвимостей, рекомендуется регулярно обновлять ядро операционной системы хоста.

Indeed FreeRADIUS Extension

Операционная система	Linux с поддержкой 64-битной архитектуры: • Astra Linux • РЕД ОС • Ubuntu
Пакеты	• Docker 19.03.0 и выше • Docker Compose 2.0.0 и выше • Tar Рекомендуется устанавливать Docker из официального репозитория по инструкции на сайте docs.docker.com.
Сертификаты	• Публичный сертификат домена в формате Base-64 • Сертификат доверенного УЦ, выписанный на DNS-имя машины
Соединение	• Соединение между сервером с FreeRADIUS Extension и сервером с установленным Access Manager по протоколу LDAPS • Соединение с Active Directory и DNS по протоколу LDAP
Доменный пользователь (для выполнения запросов LDAP при двухфакторной аутентификации)	От имени доменного пользователя выполняется запрос по протоколу LDAP для поиска пользователя. Доменный пользователь указывается в настройках FreeRADIUS Extension. При использовании однофакторной аутентификации не требуется. Требуется только при использовании Windows Password в качестве первого фактора.

ИНФОРМАЦИЯ

Чтобы избежать потенциальных уязвимостей, рекомендуется регулярно обновлять ядро операционной системы хоста.

Indeed LDAP Proxy

Операционная система	Linux с поддержкой 64-битной архитектуры: • Astra Linux • РЕД ОС • Ubuntu

Пакеты	• Docker 19.03.0 и выше • Docker Compose 2.0.0 и выше • Tar Рекомендуется устанавливать Docker из официального репозитория по инструкции на сайте docs.docker.com.
Сертификаты	• Сертификат доверенного УЦ, выписанный на DNS-имя машины • Публичный сертификат домена в формате Base-64 (если LDAP Proxy находится на отдельном от Core Server хосте) • (Опционально) Сертификат для установки TLS-соединения между сервером Indeed LDAP Proxy и сервером LDAP
Соединение	• Соединение между сервером с LDAP Proxy и сервером с установленным Access Manager • Соединение между сервером с LDAP Proxy с Active Directory и DNS по протоколу LDAPS

Indeed Linux Logon

Операционная система	Linux с поддержкой 64-битной архитектуры: • Astra Linux Special Edition 1.8.2.x • РЕД ОС 7.3.5.x
Сертификаты	• Публичный сертификат домена в формате Base-64 • Сертификат доверенного УЦ, выписанный на DNS-имя машины
Соединение	• Соединение между сервером с Linux Logon и сервером с установленным Access Manager по протоколу LDAPS • Соединение с Active Directory и DNS по протоколу LDAP

Indeed ADFS Extension

- Windows Server 2012 R2 и выше;
- Установленная роль *Active Directory Federation Services*;

Indeed RDP Windows Logon

Поддерживаемые операционные системы:

- Windows Server 2012 R2 и выше;
- Windows 7 32/64bit;
- Windows 8.1 32/64bit;

- Windows 10 32/64bit.

Аппаратные требования

- Не менее 4 ГБ оперативной памяти;
- Не менее 50 ГБ свободного дискового пространства.

Indeed Windows Logon

Аппаратные требования к рабочим станциям пользователей	• не менее 50 МБ свободного пространства на диске • наличие .NET Framework версии 4.5 и выше
Поддерживаемые операционные системы	• Windows 7 SP1 32/64bit • Windows 8.1 32/64bit • Windows 10 32/64bit • Windows 11 32/64bit • Windows Server 2012/2012 R2 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022
Требования к окружению	Настроенный DNS-сервер (необходимо добавление Reverse lookup zones). Параметры DNS-сервера необходимо указать в настройках сетевого подключения на каждой рабочей станции.
Требуемые административные права	Для установки Indeed Windows Logon требуются права локального Администратора (Adminstrator).
Настройки межсетевого экрана	Для корректной работы системы Indeed AM измените следующие настройки межсетевого экрана на Indeed AM Server и на рабочих станциях, на которых установлен компонент Indeed Windows Logon: • Открыть порт 53 (DNS) (TCP и UDP) для всех процессов в обоих направлениях. Этот порт используется системой Indeed AM для определения наличия сети. • Открыть порт 135 (RPC) для всех процессов в обоих направлениях. Этот порт используется системой для коммуникации между рабочими станциями пользователей и Core Server. • Открыть порт 389 (LDAP) для всех процессов в обоих направлениях. Этот порт используется системой для получения доступа в Active Directory (в том числе при поиске Core Server).

Настройка окружения

Размещение компонентов

Требования для работы компонентов Indeed AM

Сетевое взаимодействие

Взаимодействие компонентов Indeed AM

Хранилище данных

Содержит данные для Core Server, Log Server и Key Server

Каталог пользователей

Количество глав: 2

Размещение компонентов

Размещение №1

Данное размещение рекомендуется использовать при пилотных внедрениях для ознакомления с Indeed AM и проведения демонстраций.

Все компоненты системы, требуемые провайдеры и модули интеграции устанавливаются на одной машине.

Модули интеграции могут быть развернуты на отдельных машинах.

Наименование сервера	Требование	Компоненты Indeed AM
Indeed AM Server PC	Обязательный компонент	Indeed AM Server, Indeed AM Log Server, Indeed AM Management Console
Indeed AM Server PC	Опциональный компонент	Indeed AM Identity Provider
Indeed AM Server PC	Обязательный компонент. Тип метода аутентификации зависит от конечного сценария.	Indeed AM Providers
Indeed AM Server PC	Обязательный компонент. Тип модуля интеграции зависит от конечного сценария.	Модули интеграции системы Indeed AM
Indeed AM External PC	Опциональный компонент	Indeed AM Indeed Key Server, Indeed AM User Console

Системные требования

Наименование сервера	CPU	RAM	HDD	Network
Indeed AM Server PC	4 cores	8 ГБ	200 ГБ	100 Мбит/с
Indeed AM External PC	4 cores	8 ГБ	100 ГБ	100 Мбит/с

Размещение №2

Данное размещение рекомендуется использовать при боевых внедрениях. Критические узлы системы дублируются для обеспечения отказоустойчивости. Компонент Indeed AM Management Console устанавливается на один из серверов Indeed AM. Для настройки распределения нагрузки между компонентами необходимо использовать сторонний балансировщик нагрузки.

Наименование сервера	Требование	Компоненты Indeed AM
Indeed AM Server\Indeed AM Log Server	Обязательный компонент	Indeed AM Server, Indeed AM Log Server
Indeed AM Server\Indeed AM Management Console\Indeed AM Identity Provider	Обязательный компонент. Indeed AM Identity Provider обязателен только для сценариев, где требуется выполнять обучение аутентификаторов внешним пользователям.	Indeed AM Server, Indeed AM Management Console, Indeed AM Identity Provider
Indeed AM Indeed Key Server\Indeed AM User Console	Опциональный компонент. Indeed Key Server требуется только для сценариев с использование push-аутентификации. Indeed AM User Console требуется для обучения аутентификаторов внешним пользователям системы.	Indeed AM Indeed Key Server, Indeed AM User Console
Indeed AM Indeed Key Server\Indeed AM User Console	Опциональный компонент. Только для сценариев с использование push-аутентификации.	Indeed AM Indeed Key Server, Indeed AM User Console
Indeed AM Extensions	Обязательный компонент. Тип модуля интеграции зависит от конечного сценария.	Модули интеграции системы Indeed AM
Балансировщик нагрузки	Системные требования зависят от выбранного балансировщика.	Балансировка осуществляется сторонними компонентами.

Системные требования

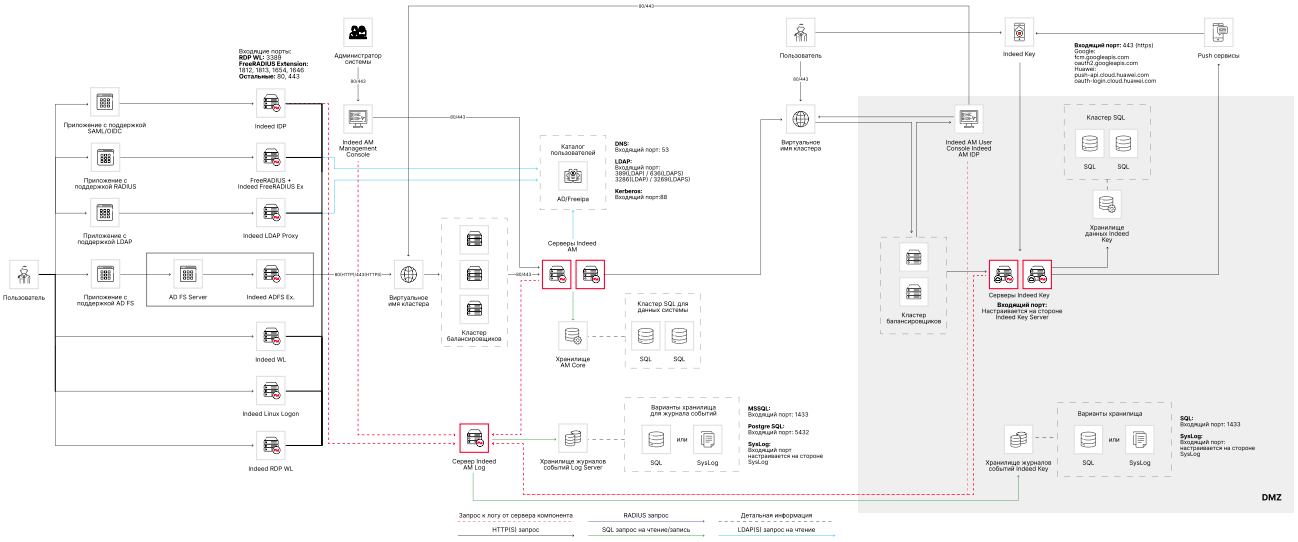
В таблице указаны рекомендуемые системные требования при развертывании боевой инфраструктуры до 10000 пользователей.

Наименование сервера	CPU	RAM	HDD	Network
Indeed AM Server\Indeed AM Log Server	8 cores	8 ГБ	200ГБ	100 Мбит/с
Indeed AM Server\Indeed AM Management Console\Indeed AM Identity Provider	8 cores	8 ГБ	200ГБ	100 Мбит/с
Indeed AM Indeed Key Server\Indeed AM User Console	8 cores	8 ГБ	150ГБ	100 Мбит/с
Indeed AM Indeed Key Server\Indeed AM User Console	8 cores	8 ГБ	150ГБ	100 Мбит/с
Indeed AM Extensions	Системные требования зависят от выбранного модуля интеграции			
ПК с БД Indeed и событиями Indeed №1	8 cores	8 ГБ	500ГБ	100 Мбит/с
ПК с БД Indeed и событиями Indeed №2	8 cores	8 ГБ	500ГБ	100 Мбит/с

Сетевое взаимодействие

На изображении представлена схема взаимодействия компонентов Indeed AM. Вы можете адаптировать ее в зависимости от сценариев использования и потребностей.

Взаимодействие между основными компонентами Indeed AM в сетевой инфраструктуре осуществляется через протоколы HTTP и HTTPS.



Наименование	Протокол	Входящий порт	Исходящий порт
Indeed AM Core Server	TCP/UDP	80(http) 443(https)	49152- 65535
Indeed AM Management Console	TCP/UDP	80(http) 443(https)	49152- 65535
Indeed AM Log Сервер (Windows Event)	TCP/UDP	80(http) 443(https)	49152- 65535
Indeed AM Log Сервер (PostgreSQL)	TCP/UDP	5432	49152- 65535
PostgreSQL База Данных Indeed AM	TCP/UDP	5432	49152- 65535
Active Directory/FreeIPA	DNS	53	49152- 65535
	LDAP	389 (LDAP) / 636 (LDAPS)3268 (LDAP) / 3269 (LDAPS)	49152- 65535
	Kerberos	88	49152- 65535

Наименование	Протокол	Входящий порт	Исходящий порт
Indeed AM Indeed Key Server	TCP/UDP	Настраивается на стороне сервера АК	49152- 65535
PostgreSQL База Данных Indeed AM Indeed Key Server	TCP/UDP	5432	49152- 65535
Indeed AM User Console	TCP/UDP	80(http) 443(https)	49152- 65535
Indeed AM ADFS Extension	TCP/UDP	80(http) 443(https)	49152- 65535
Indeed AM FreeRADIUS Extension	TCP/UDP	80(http) 443(https)	49152- 65535
Indeed AM RDP Windows Logon	TCP	3389	49152- 65535
	TCP/UDP	80(http) 443(https)	49152- 65535
Indeed AM Identity Provider	TCP/UDP	80(http) 443(https)	49152- 65535

Балансировщики нагрузки являются опциональным элементом системы, они не встроены в Indeed Access Manager и могут быть использованы в любом количестве. Число компонентов Indeed Core Server, Indeed Key Server, Indeed Log Server также может варьироваться в зависимости от потребностей клиента.

Проверка состояния сервера

Для проверки рабочего состояния контейнера в Docker используйте метод Healthcheck:

http(s)://<dns_имя_сервера>/am/<серверный_компонент>/healthcheck/isHealthy

Хранилище данных

Для работы Indeed Access Manager нужны следующие базы данных:

- Core Server
- Log Server
- Key Server (для сервера Indeed Key)

Для каждой базы данных требуется сервисная учетная запись, от имени которой будут выполняться запросы на чтение и запись информации. Сервисная учетная запись может быть общей для нескольких баз или отдельной для каждой базы.

Indeed Access Manager работает с базами данных Microsoft SQL и PostgreSQL.

Microsoft SQL

На сервере с установленным Microsoft SQL Server создайте сервисную учетную запись и базы данных для Indeed AM Core Server и Indeed AM Log Server.

Создание базы данных

Чтобы создать базу данных, выполните следующие действия:

1. Откройте SQL Server Management Studio и подключитесь к серверу.
2. Правой кнопкой мыши нажмите узел Databases.
3. В появившемся окне выберите New Database.
4. Введите имя новой базы данных в поле Database Name и нажмите OK.

Создание сервисной учетной записи

Indeed Access Manager поддерживает сервисные учетные записи сс режимом проверки подлинности SQL Server.

> ⚠ **ВАЖНО!**
>
> При создании сервисной учетной записи отключите обязательную смену пароля при следующем входе и срок действия пароля. В противном случае по истечении срока жизни пароля компоненты Indeed AM не смогут получить доступ к базе данных, что вызовет сбои в работе.

Создание сервисной учетной записи с режимом проверки подлинности SQL Server

Чтобы создать сервисную учетную запись с режимом проверки подлинности SQL Server, выполните следующие действия:

1. Раскройте узел Security.

2. Правой кнопкой мыши нажмите узел Logins.

3. В появившемся окне выберите New Login.

4. В окне Login - New выполните следующие действия:

    1. Введите имя пользователя.
    2. Выберите опцию SQL Server authentication.
    3. Отключите опцию Enforce password Policy.
    4. В меню слева выберите User Mapping.
    5. Выберите ранее созданные базы.
    6. Для каждой базы выберите роль db_owner и нажмите OK.

5. Включите смешанную аутентификацию:

    1. Правой кнопкой мыши нажмите узел экземпляра сервера SQL Server и выберите Properties.
    2. На странице Security в разделе Server authentication выберите SQL Server and Windows Authentication mode.

6. Убедитесь, что у сервисной учетной записи включена следующая настройка:

    1. Правой кнопкой мыши нажмите на созданную учетную запись и выберите Properties.
    2. На странице Status в разделе Login выберите Enabled.

7. Откройте SQL Server Configuration Manager и включите протокол TCP/IP:

    1. Во вкладке Настройка клиента Native client SQL выберите Клиентские протоколы.
    2. Нажмите правой кнопкой мыши на TCP/IP, выберите Свойства и установите значение Да для включения протокола TCP/IP.
    3. Включите TCP/IP во всех вкладках Настройка клиента Native client SQL.

PostgreSQL

На сервере с установленным PostgreSQL Server создайте сервисную учетную запись и базы данных для Indeed AM Core Server и Indeed AM Log Server.

База данных AM Core Server должна быть доступна с сервера AM Core Server, база AM Log Server — с сервера AM Log Server. Для настройки используйте схему сетевого взаимодействия.

Создание сервисной учетной записи

Чтобы создать сервисную учетную запись, выполните следующие действия:

1. Откройте pgAdmin и подключитесь к серверу.

2. Правой кнопкой мыши нажмите Login/Group Roles.
3. В появившемся окне выберите Create→Login/Group Role…
4. В окне Create-Login/Group Role выполните следующие действия:

    1. На вкладке General в поле Name введите имя пользователя.
    2. На вкладке Definition в поле Password введите пароль. В поле Account Expires укажите значение No Expiry.
    3. На вкладке Privileges включите опцию Can login? и нажмите Save.

Создание базы данных

Чтобы создать базу данных, выполните следующие действия:

1. Откройте pgAdmin и подключитесь к серверу.
2. Раскройте компоненты вашего сервера SQL.
3. Правкой кнопкой мыши нажмите Databases.
4. Выберите Create→Database…
5. В окне Create-Database выполните следующие действия:

    1. В поле Database введите имя базы данных.
    2. В поле Owner из списка выберите ранее созданного пользователя и нажмите Save.

Настройка удаленного подключения к базе данных

Чтобы настроить удаленное подключение к базе данных, выполните следующие действия:

1. Откройте конфигурационный файл *pg_hba.conf* из *C:\Program Files\PostgreSQL\<номер версии>\data*.
2. Добавьте строку следующего формата:

    ```
    host databaseName UserName HostIP scram-sha-256
    ```

    - `host` — тип подключения. Если вы не указываете тип подключения, по умолчанию используется подключение по TCP/IP.
    - `databaseName` — имя базы данных, для которой вы настраиваете подключение.
    - `UserName` — имя пользователя, который будет подключаться к этой базе данных.
    - `HostIP` — IP-адрес машины, на которой установлен компонент Indeed AM. Укажите значение с маской.
    - `scram-sha-256` — метод аутентификации пользователя.

    Пример

    ```
    host all all 192.168.1.0/24 scram-sha-256
    ```

3. Откройте конфигурационный файл *postgresql.conf* из *C:\Program Files\PostgreSQL\<номер версии>\data*.

4. Измените строку `listen_addresses = 'localhost'` на `listen_addresses = '*'`.

Каталог пользователей

Каталог пользователей используется для получения данных о конечных пользователях, которые будут аутентифицироваться с помощью Indeed Access Manager.

Чтобы эти данные появились в Indeed Access Manager, подготовьте в каталоге объект с конечными пользователями и создайте сервисную учетную запись с правами на чтение.

Вы можете настроить Indeed Access Manager на чтение данных из всего домена пользователей целиком, из отдельного подразделения (OU) или отдельного контейнера (CN). Не обязательно помещать всех пользователей в отдельный объект — в дальнейшем вы можете дополнительно настроить видимость объектов каталога с помощью фильтров DN и LDAP.

LDAP-фильтр при поиске пользователей и групп в службе каталогов

> ⚠ **ВАЖНО**
>
> Если вы планируете использовать отдельное подразделение, все необходимые объекты — группы, администраторы, конечные пользователи — должны находиться внутри этого подразделения.

Indeed Access Manager работает с каталогами только в режиме чтения данных (read-only), без создания и редактирования объектов.

Поддерживаются следующие каталоги пользователей:

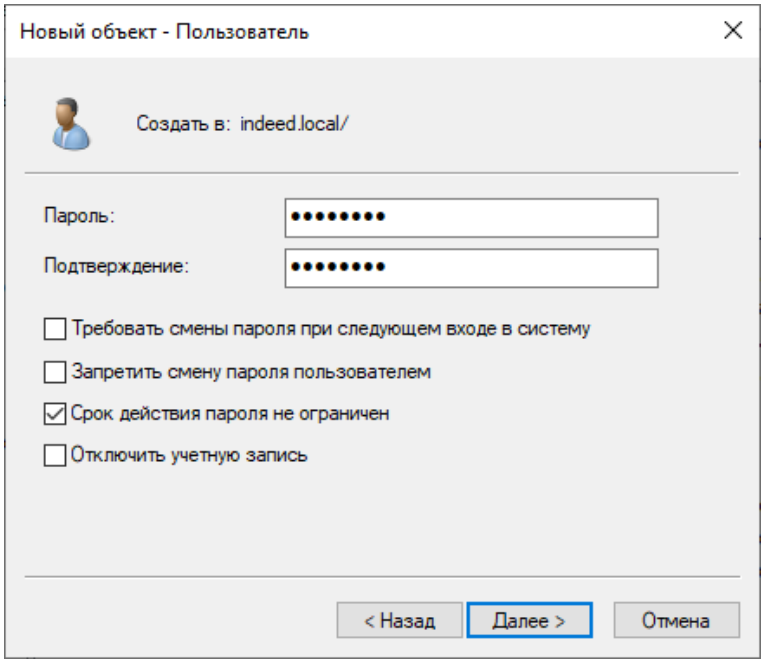
- Active Directory
- FreeIPA

Active Directory

Создание сервисной учетной записи

Чтобы создать сервисную учетную запись, выполните следующие действия:

1. Откройте Active Directory Users and Computers.
2. Выберите каталог, в котором планируете создать учетную запись.
3. Нажмите значок .
4. В открывшемся окне New Object→User введите имя пользователя и нажмите Next.
5. Введите пароль.
6. Отключите опцию User must change password at next logon.
7. Выберите опцию Password never expires и нажмите Finish.

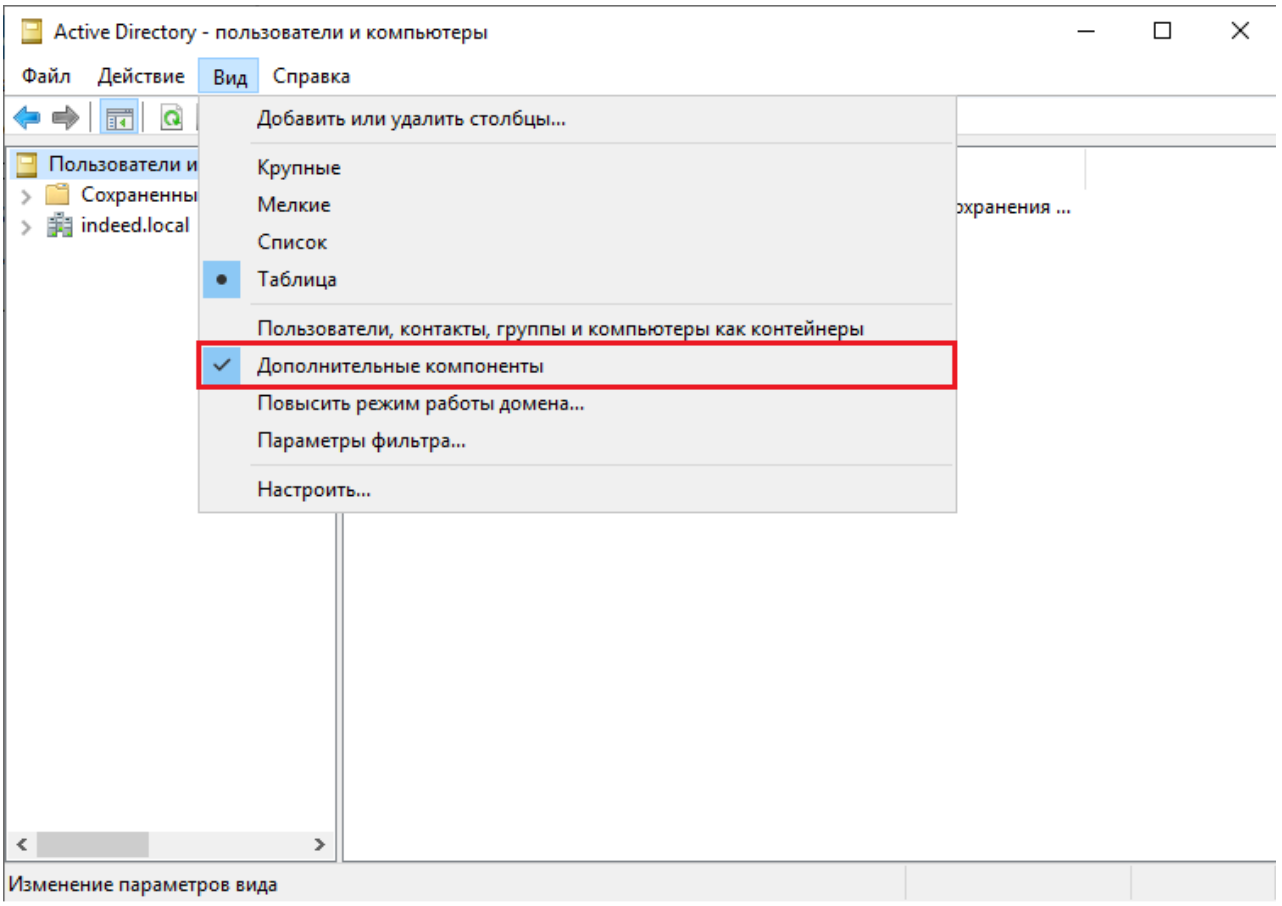


Предоставление прав на чтение данных

Если политика безопасности вашей компании разрешает всем пользователям в домене читать данные всех объектов в домене, вы не должны выполнять эту настройку.

Если настроено ограничение на чтение данных, выполните следующие действия:

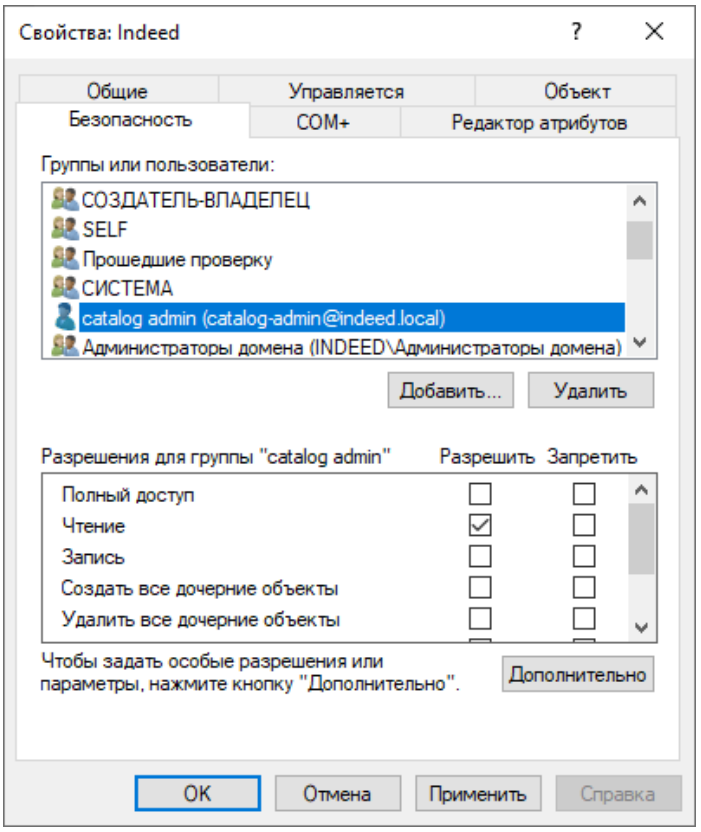
1. Откройте Active Directory Users and Computers.
2. Во вкладке View включите опцию Advanced Features.



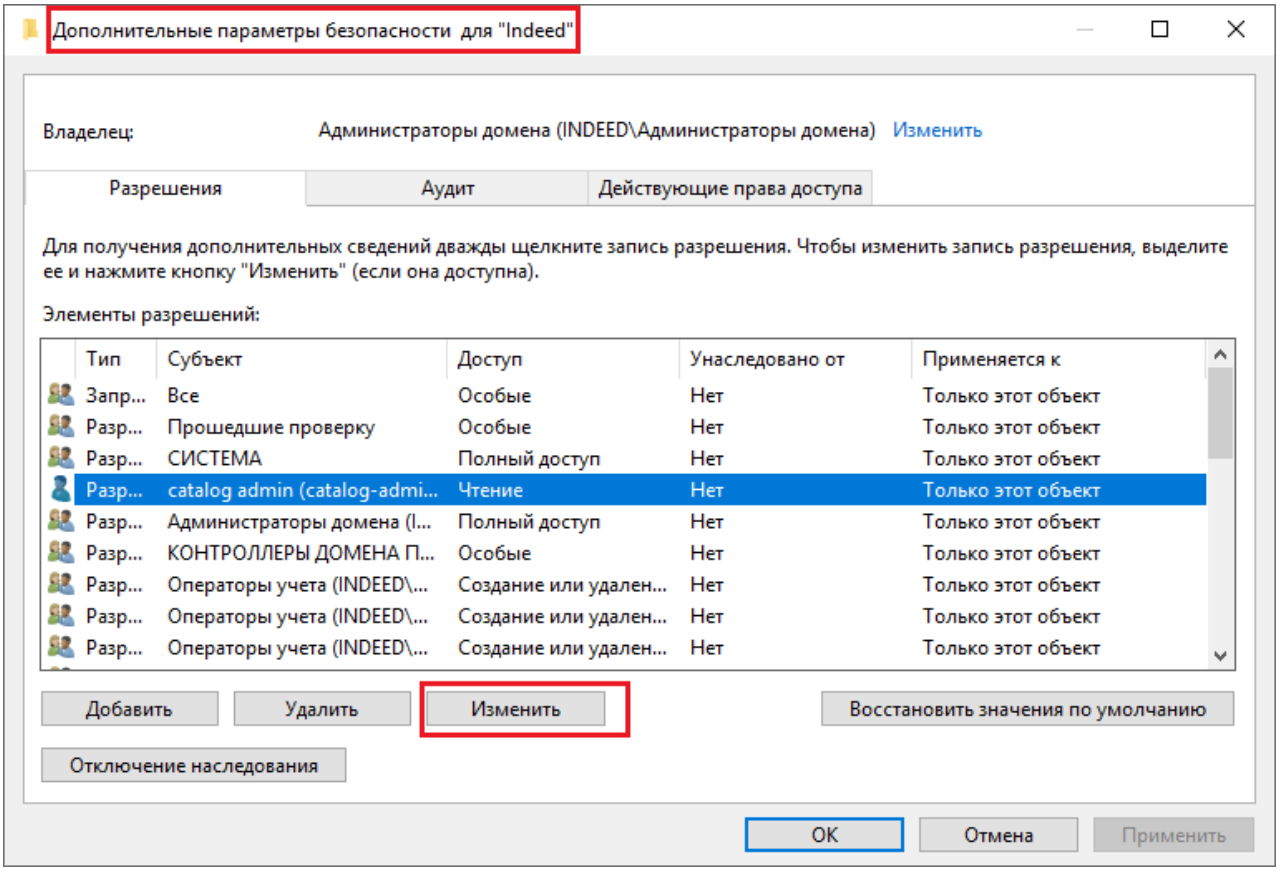
3. Правой кнопкой мыши нажмите объект с пользователями и выберите Properties.

4. В окне Properties выполните следующие действия:

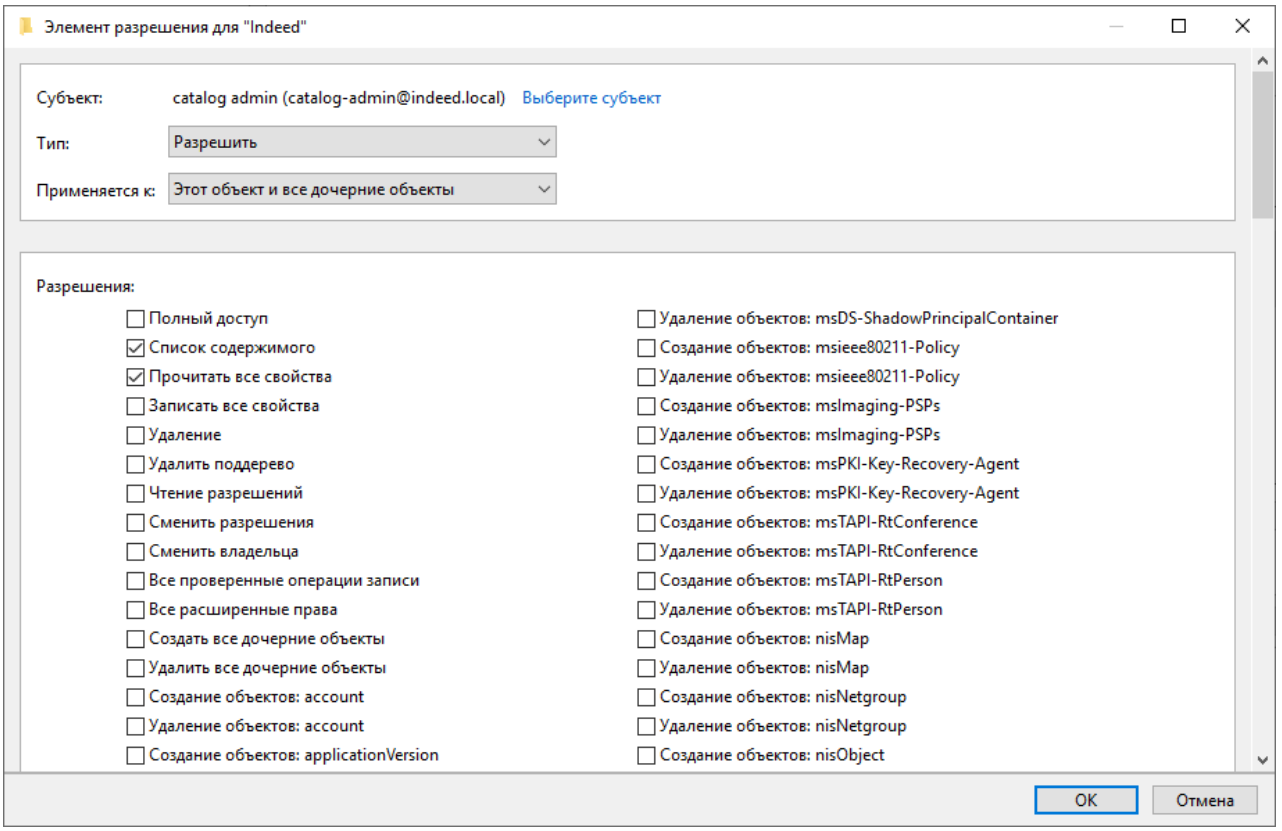
    1. Откройте вкладку Security.
    2. В разделе Group or user names добавьте созданную ранее сервисную учетную запись.
    3. В разделе Permissions for выберите опцию Read и нажмите кнопку Advanced.



5. В открывшемся окне Advanced Security Settings выберите сервисную учетную запись и нажмите Edit.



6. В открывшемся окне Permission Entry в списке Applies to выберите This object and all descendant objects и нажмите OK.



Атрибуты пользователей Active Directory

Атрибут пользователя	Описание
FirstName	Имя пользователя
MiddleName	Отчество пользователя
LastName	Фамилия пользователя
mail	Адрес электронной почты пользователя
Phone	Номер телефона пользователя
Name	Отображаемое имя пользователя
CanonicalName	Каноническое имя пользователя, например *domain.com/Users/testuser*
PrincipalName	Уникальное имя пользователя в определенном формате, например *testuser@domain.com*
SamCompatibleName	Имя пользователя, совместимое с системой учетных записей Security Account Manager (SAM). Например, *domain\testuser*

Атрибут пользователя	Описание
DistinguishedName	Уникальное имя объекта в иерархии Active Directory, состоящее из полного пути к объекту. Например, *CN=testuser,OU=Users,DC=domain,DC=com*
Sid	Уникальный идентификатор безопасности, присваиваемый каждому объекту в Active Directory. Sid используется для управления доступом к ресурсам и аутентификации пользователей и объектов

FreeIPA

Прежде чем создать сервисную учетную запись, создайте необходимые разрешения, привилегии, роли.

Добавление разрешений, привилегий, ролей

1. Войдите в веб-версию FreeIPA по адресу *https://<dns_имя_сервера>/ipa/ui/#* под учетной записью администратора в формате *admin@<dns_имя_сервера>*.

2. Перейдите на вкладку IPA Server и в выпадающем списке Role-Based Access Control выберите Permissions и нажмите Add.

Чтение и поиск пользователей

- Permission name — укажите имя разрешения, например *am-user-read*.
- Granted Rights — выберите `read`, `search`.
- Subtree — введите имя домена в формате Distinguished name, например `cn=users,cn=accounts,dc=test,dc=realm`.
- Extra target filter — `(objectClass=person)`.
- Effective attributes — укажите каждый атрибут по одному в отдельной строке:
  - `cn`
  - `entryDN`
  - `entryUUID`
  - `givenName`
  - `initials`
  - `ipaNTSecurityIdentifier`
  - `jpegPhoto`
  - `krbCanonicalName`
  - `krbLastFailedAuth`
  - `krbLoginFailedCount`
  - `krbPrincipalExpiration`
  - `krbPrincipalName`
  - `krbPwdPolicyReference`
  - `mail`
  - `memberOf`
  - `nsAccountLock`
  - `photo`
  - `sn`
  - `telephoneNumber`
  - `uid`

Чтение и поиск групп

- Permission name — укажите имя разрешения, например *am-group-read*.
- Granted Rights — выберите `read`, `search`.
- Subtree — введите имя домена в формате Distinguished name, например `cn=groups,cn=accounts,dc=test,dc=realm`.
- Extra target filter — `(objectClass=ipaUserGroup)`.
- Effective attributes — укажите каждый атрибут по одному в отдельной строке:
  - `cn`
  - `entryDN`
  - `entryUUID`
  - `ipaNTSecurityIdentifier`
  - `member`
  - `memberOf`

Чтение и поиск контейнеров

- Permission name — укажите имя разрешения, например *am-container-read*.
- Granted Rights — выберите `read`, `search`.
- Subtree — введите имя домена в формате Distinguished name, например `dc=test,dc=realm`.
- Extra target filter — `(|(objectClass=nsContainer)(objectClass=domain))`.
- Effective attributes — укажите каждый атрибут по одному в отдельной строке:
  - `cn`
  - `entryDN`
  - `entryUUID`
  - `ipaNTSecurityIdentifier`
  - `member`
  - `memberOf`

Чтение и поиск политик паролей

- Permission name — укажите имя разрешения, например *am-password-policy-read*.
- Granted Rights — выберите `read`, `search`.
- Subtree — введите имя домена в формате Distinguished name, например `cn=TEST.REALM,cn=kerberos,dc=test,dc=realm`.
- Extra target filter — `(objectClass=krbPwdPolicy)`.
- Effective attributes — укажите каждый атрибут по одному в отдельной строке:
  - `krbPwdLockoutDuration`
  - `krbPwdMaxFailure`
  - `krbPwdMinDiffChars`
  - `krbPwdMinLength`
  - `objectClass`

Смена пароля

- Permission name — укажите имя разрешения, например *am-user-password-change*.
- Granted Rights — выберите `write`.
- Subtree — введите имя домена в формате Distinguished name, например `cn=users,cn=accounts,dc=test,dc=realm`.
- Extra target filter — `(objectClass=person)`.
- Effective attributes — укажите каждый атрибут по одному в отдельной строке:
  - `krbPrincipalKey`

Чтение истории паролей

Выдайте права на чтение истории паролей, если у вас настроена смена пароля пользователя под сервисной учетной записью, а также в политиках паролей FreeIPA настроена проверка истории паролей.

- Permission name — укажите имя разрешения, например *am-user-password-read*.
- Granted Rights — выберите `read`.
- Subtree — введите имя домена в формате Distinguished name, например `cn=users,cn=accounts,dc=test,dc=realm`.
- Extra target filter — `(objectClass=person)`.
- Effective attributes — укажите каждый атрибут по одному в отдельной строке:
  - `passwordHistory`

3. В выпадающем списке Role-Based Access Control выберите Privileges и нажмите Add.

Чтение объектов

- Privilege name — укажите имя разрешения, например *am-read*.
- В созданное разрешение добавьте *am-user-read*, *am-group-read*, *am-container-read*, *am-password-policy-read*.

Смена пароля пользователя

- Privilege name — укажите имя разрешения, например *am-password-change*.
- В созданное разрешение добавьте *am-user-password-read*, *am-user-password-change*.

4. В выпадающем списке Role-Based Access Control выберите Roles и нажмите Add.

Роль сервисной учетной записи

- Role name — укажите имя разрешения, например *am-server*.
- В созданное разрешение добавьте *am-read*, *am-password-change*.

Создание сервисной учетной записи

Чтобы создать сервисную учетную запись для работы с каталогом пользователей:

1. На вкладке Identity→Users нажмите Add.
2. В поле User login задайте имя пользователя, например *am-server*.
3. В полях First name, Last name, Password укажите имя, фамилию и задайте пароль для новой учетной записи.
4. Добавьте пользователю роль `am-server`.

> ⚠ **ВАЖНО**
>
> Чтобы срок действия паролей для системных учетных записей игнорировался:
>
> 1. Создайте политику для администраторов FreeIPA, если эта политика не была создана ранее.
> 2. Добавьте системную учетную запись для подключения к каталогу пользователей Core Server в эту политику.
> 3. В поле Приоритет задайте значение, которое будет ниже приоритета, установленного в парольной политике для группы всех пользователей.
> 4. В поле Grace login limit установите значение -1.

Политика паролей

Чтобы настроить блокировку входа после истечения срока действия пароля, перейдите в раздел Политика→Политики паролей и установите значение Grace login limit.

Параметр Grace login limit определяет, сколько раз пользователь может войти в систему после истечения срока действия своего пароля, прежде чем его учетная запись будет заблокирована. Этот параметр является частью политик паролей пользователей в каталоге FreeIPA и позволяет пользователям с устаревшим паролем войти в систему и сменить пароль, вместо немедленной блокировки учетной записи.

Возможные значения для параметра Grace login limit:

- *-1* (значение по умолчанию) — пользователь может неограниченно входить в систему даже с истекшим паролем, срок действия пароля игнорируется;
- *0* (рекомендуемое значение) — пользователь не может войти в систему после истечения срока действия своего пароля;
- *1* — пользователь может войти в систему с истекшим паролем один раз;
- *2* — пользователь может войти в систему с истекшим паролем два раза.

Диапазон значений: от *-1* до *2147483647*.

Смена пароля пользователя FreeIPA в User Console

Если пользователь FreeIPA самостоятельно меняет пароль в Indeed User Console, дата окончания срока действия пароля по умолчанию устанавливается на текущую дату. Для корректной настройки срока действия пароля необходимо выполнить следующие изменения на каждом сервере FreeIPA:

1. Создайте файл */tmp/passSyncManagersDNs* со следующим содержимым:

   ```
   dn: cn=ipa_pwd_extop,cn=plugins,cn=config
   changetype: modify
   add: passSyncManagersDNs
   passSyncManagersDNs: uid=my-am-admin,cn=users,cn=accounts,dc=test,dc=realm
   ```

   Для параметра `passSyncManagersDNs` укажите значение соответствующего DN сервисной учетной записи, используемой в Core Server.

2. В терминале выполните команду:

   ```
   ldapmodify -x -D "cn=Directory Manager" -W -H LDAPS://ipa.test.realm:636 -f
   /tmp/passSyncManagersDNs
   ```

Атрибуты пользователей FreeIPA

Атрибут пользователя	Описание
entryUUID	Универсальный уникальный идентификатор записи
entryDN	Уникальное имя записи в каталоге
uid	Идентификатор пользователя
mail	Адрес электронной почты
telephoneNumber	Телефон
givenName	Имя
sn	Фамилия
cn	Общее имя
krbPrincipalName	Имя участника-пользователя Kerberos (UPN)
krbCanonicalName	Каноническое имя учетной записи Kerberos
ipaNTSecurityIdentifier	Атрибут, хранящий идентификатор безопасности SID
photo	Фото
userPassword	Пароль
krbPasswordExpiration	Атрибут, хранящий дату и время истечения срока действия текущего пароля

Установка и настройка серверных компонентов

Мастер конфигурации

Количество глав: 2

Ручная установка

Количество глав: 6

Indeed Key Server

Сервер для работы приложения Indeed Key

Установка Access Manager на нескольких хостах

Установка Indeed Access Manager на нескольких хостах

Расположение конфигурационных файлов

Как найти конфигурационные файлы

Мастер конфигурации

Мастер конфигурации — это веб-приложение, которое позволяет установить Indeed Access Manager или изменить конфигурацию. Мастер поставляется в составе дистрибутива Access Manager. Мастер конфигурации позволяет автоматически заполнить файлы конфигурации компонентов Access Manager.

Запуск мастера конфигурации

Перед запуском мастера конфигурации убедитесь, что ваше окружение соответствует системным требованиям.

1. Скачайте архив *distrib_am-<номер версии>.tar.gz*, загрузите его на целевой хост в необходимый каталог.
2. Перейдите в каталог с архивом и распакуйте его с помощью команды:

   ```
   sudo tar -xf <имя архива>.tar.gz
   ```

3. (Опционально) Подготовьте собственные сертификаты:

   - добавьте *<публичный сертификат домена>.cer* в каталог *distrib_am/wizard/ssl/* и переименуйте его в *ca.cer*,
   - добавьте *<серверный сертификат>.pfx* в каталог *distrib_am/wizard/ssl/* и переименуйте его в *<dns_имя_сервера>.pfx*.

     > **ПРИМЕЧАНИЕ**
     >
     > Если не подготовить собственные сертификаты, то при запуске мастера конфигурации автоматически генерируются самоподписанные сертификаты *ca.crt* и *<dns_имя_сервера>.pem*. Добавьте сертификат *ca.crt* в список доверенных центров сертификации.

4. Перейдите в каталог *distrib_am/*, откройте терминал и выполните команду для запуска мастера конфигурации:

   ```
   sudo bash ./setup.sh start
   ```

5. Перейдите по URL-адресу, указанному в консоли после выполнения скрипта.
6. В поле Код доступа введите `AutenticationCode`, указанный в консоли после выполнения скрипта.

   Пример кода: `0f4734a520d74b27b790df6344fd4710`.

7. Нажмите Войти.

Сценарий мастера

(Опционально) Как отредактировать шаблоны конфигурационных файлов?

Шаблоны конфигурационных файлов используются при генерации файлов конфигураций для компонентов Access Manager. Редактирование шаблонов может потребоваться в случаях, когда необходимо изменить значения по умолчанию, например при использовании нестандартного порта.

Чтобы внести изменения в шаблоны конфигурационных файлов:

1. Скопируйте шаблоны из Docker-контейнера с помощью команды:

   ```
   docker cp <container_id_or_name>:<path_in_container> <path_on_local_host>
   ```

   Пример: `docker cp ebbc6c41f1a5:./app/deploy/templates ./distrib_am/wizard`

2. В файле *wizard.docker-compose.yml* для сервиса `wizard` в разделе `volumes` добавьте монтирование директорий в контейнере Docker:

   ```
   ./templates/:/app/deploy/templates/:Z
   ```

> ⚠ **ВАЖНО**
>
> В шаблонах конфигурационных файлов нельзя изменять переменные формата `{{HostSchemes.Schemes.0.Endpoint.Host}}`, так как это может привести к ошибкам при инсталляции Access Manager и генерации конфигурации.

Чтобы начать работу, выберите сценарий:

- Инсталляция AM — новая установка Access Manager.
- Изменение конфигурации AM — внесение изменений в текущую инсталляцию Access Manager.

Инсталляция Access Manager

Сценарий Инсталляция AM — это новая установка Access Manager. Чтобы начать инсталляцию, после выбора сценария нажмите Далее.

Схема хостов

Под хостом понимается физический или виртуальный сервер, на котором располагаются компоненты Access Manager. В текущей версии мастера доступно добавление только одного хоста.

1. Нажмите Добавить хост.
2. Введите информацию о хосте и сервисной учетной записи, используя подсказки мастера настройки, и нажмите Проверить хост.

   Сервисная учетная запись должна состоять в группе sudo.

   > **ПРИМЕЧАНИЕ**
   >
   > При проверке хоста происходит SSH-подключение для попытки соединения с сервером. Введенные данные можно добавить в мастер конфигурации без проверки соединения.

   При необходимости данные хоста можно будет отредактировать после добавления.
3. Добавьте на хост компоненты и провайдеры.

   Обязательные:

   - Core Server
   - Log Server
   - Management Console
   - Identity Provider
   - Доменный пароль
4. Нажмите Далее для перехода к следующему шагу.

Удалить хост

При необходимости удалите хост из мастера конфигурации. При этом компоненты Access Manager с хоста не удаляются автоматически. При удалении хоста дальнейшее прохождение сценария мастера конфигурации будет недоступно.

Сертификаты

Загрузите заранее подготовленные сертификаты для добавленного хоста.

1. Добавьте публичные сертификаты домена или стороннего УЦ с расширением .pem, .crt или .cer.
2. Добавьте серверные сертификаты с расширением .pfx, выписанные на DNS-имя хоста, и укажите пароль.

   Сертификат .pfx должен иметь расширение Использование ключа (Key Usage) с разрешениями Цифровая подпись (Digital Signature) и Шифрование ключей (Key Encipherment).
3. Нажмите Далее для перехода к следующему шагу.

Каталоги пользователей

1. Нажмите Добавить каталог.
2. Заполните поля, используя подсказки мастера конфигурации.

   При необходимости данные каталога можно отредактировать после добавления.
3. При необходимости отредактируйте соответствие атрибутов пользователей.
   - Атрибуты пользователей Active Directory
   - Атрибуты пользователей FreeIPA
4. Нажмите Добавить.
5. Нажмите Далее для перехода к следующему шагу.

Базы данных

Access Manager поддерживает работу с Microsoft SQL и PostgreSQL.

1. Заполните информацию о выбранной СУБД, используя подсказки мастера конфигурации.
2. Введите логин и пароль пользователя базы данных.
3. Выберите тип алгоритма шифрования и сгенерируйте ключ.

   > ⚠ **ВАЖНО**
   >
   > Если вы используете такие алгоритмы шифрования, как RC2, TripleDes или DES, сначала добавьте ключ в мастер конфигурации, а затем внесите изменения в конфигурационный файл *am/core/app-settings.json*.
   >
   > В блоке `Storage` в строке `Algorithm` добавьте тип используемого алгоритма.
4. Введите данные для подключения к Log Server.
5. Нажмите Добавить.

6. Нажмите Далее для перехода к следующему шагу.

Сессионный ключ

1. Нажмите Сгенерировать новый ключ. При генерации нового ключа шифрования все текущие сессии станут недоступными.
2. Нажмите Далее для перехода к следующему шагу.

Логирование

1. При необходимости измените уровень логирования серверных компонентов.
2. Нажмите Далее для перехода к следующему шагу.

Syslog

Опционально добавьте соединение с Syslog-сервером, чтобы использовать хранилище данных Syslog в компоненте Log Server.

Первичный администратор

На этом шаге укажите ID пользователю, которому будут выданы права первичного администратора. Выдать права администратора другим пользователям можно в Management Console после установки.

Как задать ID первичного администратора?

Резервное копирование

Резервная копия мастера конфигурации — это зашифрованный файл, который используется для восстановления настроек мастера. Этот файл потребуется для изменения конфигурации текущей версии Access Manager.

> ⚠ **ПРЕДУПРЕЖДЕНИЕ**
>
> Без резервной копии и пароля вы не сможете в дальнейшем изменить конфигурацию Access Manager с помощью мастера.

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

Установка AM

1. Выберите сценарий установки Access Manager:

- Автоматическая установка — автоматическая установка с помощью мастера конфигурации.
- Ручная установка — с помощью мастера создается архив с заполненными конфигурационными файлами.

2. Нажмите Начать и отслеживайте процесс установки с помощью прогресс-бара. Дождитесь завершения установки.

   В случае возникновения ошибки, скачайте лог-файл и при необходимости обратитесь в техническую поддержку.

3. Если вы выбрали ручную установку, нажмите Скачать архив, переместите архив на необходимый хост и распакуйте его. Конфигурационные файлы были заполнены с помощью мастера конфигурации.

4. Чтобы завершить работу мастера, выполните следующую команду в терминале:

   ```
   sudo bash ./setup.sh stop
   ```

Изменение конфигурации Access Manager

Сценарий Изменение конфигурации AM позволяет внести изменения в текущую инсталляцию Access Manager. Во время обновления Access Manager будет недоступен. Все текущие сессии будут прерваны.

После выбора сценария нажмите Далее.

> **ПРИМЕЧАНИЕ**
>
> Прежде чем изменять конфигурацию, сохраните SAML-сертификат и пароли к нему. Так как при внесении изменений будут сгенерированы новые SAML-сертификаты, работа интегрированных приложений может быть нарушена.
>
> После завершения обновлений замените файл сертификата и внесите прежние пароли в конфигурационные файлы *app-settings.json* для Management Console, User Console и Identity Provider.
>
> Однако если вы планируете использовать новый сгенерированный SAML-сертификат, замените сертификат в конфигурации для интегрированных приложений.

Начало работы

1. Загрузите резервную копию мастера конфигурации и введите пароль.
2. После проверки данных нажмите Далее.

Схема хостов

> **ВАЖНО**
>
> Если вы меняете схему хоста, после сохранения подтвердите данные на последующих шагах.

Чтобы изменить текущую схему хоста:

1. Нажмите .
2. Введите новую информацию о хосте и сервисной учетной записи. Сервисная учетная запись должна состоять в группе sudo.
3. Измените компоненты и провайдеры.
4. Нажмите Сохранить.

Сертификаты

Чтобы обновить загруженные ранее сертификаты для добавленного хоста:

1. Удалите неактуальные публичные сертификаты или добавьте новые с расширением .pem, .crt или .cer.
2. Удалите неактуальный серверный сертификат, чтобы добавить новый с расширением .pfx.

   Сертификат .pfx должен иметь расширение Использование ключа (Key Usage) с разрешениями Цифровая подпись (Digital Signature) и Шифрование ключей (Key Encipherment).
3. Нажмите Далее.

Каталоги пользователей

Чтобы изменить данные каталога пользователей:

1. Нажмите .
2. Отредактируйте поля, используя подсказки мастера конфигурации.
3. Нажмите Сохранить.

Базы данных

Чтобы изменить данные для подключения к Core Server и Log Server:

1. Отредактируйте поля, используя подсказки мастера конфигурации.
2. Отредактируйте данные для подключения к Log Server.
3. Нажмите Далее.

Сессионный ключ

1. Нажмите Сгенерировать новый ключ. При генерации нового ключа шифрования все текущие сессии станут недоступными.
2. Нажмите Далее.

Логирование

1. При необходимости измените уровень логирования серверных компонентов.
2. Нажмите Далее.

Syslog

Опционально добавьте соединение с Syslog-сервером, чтобы использовать хранилище данных Syslog в компоненте Log Server.

Резервное копирование

После изменений в текущей конфигурации сохраните файл резервной копии мастера и запомните пароль:

1. Задайте пароль для резервной копии мастера конфигурации.
2. Нажмите Скачать резервную копию.

Ручная установка

Все компоненты Access Manager входят в состав архива с Docker-контейнером. Большинство компонентов устанавливается автоматически при распаковке архива.

Порядок ручной установки

Ознакомьтесь с системными требованиями

Шаг 1. Перед установкой компонентов Access Manager убедитесь, что ваше окружение соответствует системным и программным требованиям.

Подготовьте окружение

Шаг 2. Распакуйте архив *am-<номер_версии>.tar.gz* и импортируйте образы Docker для автоматической установки компонентов.

Шаг 3. Настройте переменные окружения `ENDPOINT_NAME_*` в файле *am/.env* для Core Server.

Шаг 4. Создайте каталоги для хранение кеша, логов и ключей шифрования.

Шаг 5. Выдайте права пользователю, под которым планируете запускать Access Manager в Docker.

Подготовьте необходимые сертификаты

Шаг 6. Настройте работу служебных сертификатов с помощью соответствующих скриптов и/или собственного клиентского сертификата.

Настройте Indeed Log Server

Шаг 7. Настройте Log Server с помощью конфигурационного файла *am/ls/clientApps.config*.

Настройте Indeed Core Server

Шаг 8. Настройте Core Server с помощью конфигурационного файла *am/core/app-settings.json*.

Шаг 9. На этом этапе создайте и запустите контейнер с приложением с помощью команды `sudo docker-compose up -d`.

Шаг 10. Настройте начальную аутентификацию, сформируйте значение параметра `StringValue` в конфигурационном файле *am/core/initial-settings.json*.

Компоненты Access Manager

Отдельно устанавливать и настраивать Management Console, User Console, Identity Provider, а также провайдеры аутентификации не нужно. Компоненты устанавливается автоматически при распаковке архива *am-*

<номер_версии>.tar.gz.

Запустите контейнер с приложением

После выполнения всех шагов перезапустите контейнер с приложением с помощью команды `sudo docker-compose up -d`.

Начало установки

Для установки и дальнейшей настройки компонентов Access Manager, выполните следующие обязательные действия:

1. Подготовьте образы Docker для автоматической установки компонентов.
2. Настройте переменные окружения.
3. Создайте каталоги для хранения кеша, логов и ключей шифрования.
4. Выдайте права пользователю, под которым планируете запускать Access Manager в Docker.

Импорт образа Docker

1. Скачайте архив нужного компонента *am_images/<имя компонента>.tar.gz* и загрузите его на целевой хост в необходимый каталог.

   Если компонент устанавливается на отдельном хосте, вместе с архивом компонента скопируйте и импортируйте архивы *haproxy.tar.gz* и *tools.tar.gz*.

   > **ПРИМЕЧАНИЕ**
   >
   > Если в вашей версии АМ нет каталога *am_images*, для установки используйте общий архив *am-<номер_версии>.tar.gz*.

2. Перейдите в каталог с архивом и распакуйте его с помощью команды:

   ```
   sudo tar -xf <имя компонента>.tar.gz
   ```

3. Перейдите в каталог, в который распаковался архив, и импортируйте образ Docker с помощью команды:

   ```
   sudo docker load -i <имя компонента>.tar.gz
   ```

   Чтобы импортировать все образы, используйте команду:

   ```
   for f in *.tar.gz; do docker load -i "$f"; done
   ```

4. Чтобы сгенерировать архив для ручной установки, перейдите в мастер конфигурации и выполните сценарий Ручная установка.

Переменные окружения

Переменные окружения находятся в файле *am/.env* и доступны пользователю с заданными по умолчанию значениями. При установке и настройке серверных компонентов необходимо отредактировать значения для переменных `ENDPOINT_NAME_*`.

> **ВАЖНО**
>
> Если вы не планируете устанавливать все компоненты Access Manager, в переменной `COMPOSE_PROFILES` удалите соответствующие значения.
>
> При этом необходимо обязательно указать в списке провайдеров Windows Password (`amwp`), чтобы реализовать начальную аутентификацию в Core Server.

Пример файла *.env*

```
TAG=am_9.2.0-rc7164-9dc554f.ru-ru
LS_TAG=9.5.0-beta

AM_UID=200000
AM_GID=200000

CERT_STORE=/etc/ssl/certs
CA_CERTS=/usr/local/share/ca-certificates

# Specify in the COMPOSE_PROFILES variable providers separated by commas.
# Example: COMPOSE_PROFILES=passcode,indeed-key,sms-otp,storage-sms-otp
# Full list of services: core,idp,mc,uc,ls,amsmtp,amwp,encrypted-software-
totp,hardware-totp,hotp,indeed-key,mfa,passcode,radius,secured-totp,sms-
otp,software-totp,storage-sms-otp,indeed-key-server,sms-proxy
COMPOSE_PROFILES=core,idp,mc,uc,ls,indeed-key-server,sms-
proxy,amsmtp,amwp,encrypted-software-totp,hardware-totp,hotp,indeed-
key,mfa,radius,secured-totp,sms-otp,software-totp,storage-sms-otp,passcode

ENDPOINT_NAME_THIS_HOST=indeed_core.indeed.ru
ENDPOINT_NAME_CORE=indeed_core.indeed.ru
ENDPOINT_NAME_IDP=indeed_idp.indeed.ru
ENDPOINT_NAME_MC=indeed_mc.indeed.ru
ENDPOINT_NAME_UC=indeed_srv.indeed.ru
ENDPOINT_NAME_LS=indeed_srv.indeed.ru
ENDPOINT_HTTPS_PORT=443

INDEED_KEY_EXTERNAL_ENDPOINT_NAME=indeed_srv.indeed.ru
INDEED_KEY_HTTPS_PORT=81
INDEED_KEY_HTTPS_PORT_EXTERNAL=83

CUSTOM_SP_1=
CUSTOM_SP_2=
CUSTOM_SP_3=
CUSTOM_SP_4=
CUSTOM_SP_5=

COMPOSE_PATH_SEPARATOR=:
COMPOSE_FILE=haproxy.docker-compose.yml:access-manager.docker-compose.yml:log-
server.docker-compose.yml:indeed-key.docker-compose.yml:sms-proxy.docker-
compose.yml
COMPOSE_PROJECT_NAME=am
```

В следующей таблице описаны все переменные окружения, находящиеся в файле *.env*.

Переменная	Описание
`TAG`	Версия сборки. В этой переменной указаны теги образов Docker. Пр правильность тегов. Используйте команду `sudo docker images`, ч получить тег.
`LS_TAG`	Версия компонента Log Server.
`AM_UID`	Идентификатор пользователя, под которым будет работать Access Ma Docker. Убедитесь, что этот идентификатор отличается от идентифи локальных пользователей хоста. Значение по умолчанию: `AM_UID=200000`.
`AM_GID`	Идентификатор группы, под которой будет работать Access Manager Docker. Убедитесь, что этот идентификатор отличается от идентифи локальных пользователей хоста. Значение по умолчанию: `AM_GID=200000`.
`CERT_STORE`	Путь хранения сертификатов внутри контейнера.
`CA_CERTS`	Путь хранения сертификатов центров сертификации (CA).
`COMPOSE_PROFILES`	Компоненты Access Manager и провайдеры (через запятую), которые планируете установить. По умолчанию добавлены все компоненты, к indeed-key-server, sms-proxy. Полный список компонентов: `core,idp,mc,uc,ls,amsmtp,amwp,encrypted-software-totp,hardware-totp,hotp,indeed-key,mfa,passcode,radius,secured-totp,sms-otp,software totp,storage-sms-otp,indeed-key-server,sms-proxy,ldap`

`ENDPOINT_NAME_*`	В этих переменных указываются DNS-имена хостов (в нижнем реги которые разворачиваются компоненты Access Manager. Пример: `am.domain.local`. Если вы используете https-порт, который отличается от стандартного укажите его в имени хоста. Пример: `am.domain.local:1443`. Доступные переменные: `ENDPOINT_NAME_THIS_HOST`, `ENDPOINT_NAME_CORE`, `ENDPOINT_NAME_IDP`, `ENDPOINT_NAME_MC`, `ENDPOINT_NAME_UC`, `ENDPOINT_NAME_LS`, `INDEED_KEY_EXTERNAL_ENDPOINT_NAME`. В переменной `ENDPOINT_NAME_THIS_HOST` необходимо указать им текущего хоста. Если используется один хост, необходимо продубли одно и то же значение для всех переменных.
`ENDPOINT_HTTPS_PORT`	Https-порт по умолчанию 443.
`INDEED_KEY_HTTPS_PORT`	Внутренний https-порт для Indeed Key по умолчанию 81.
`INDEED_KEY_HTTPS_PORT_EXTERNAL`	Внешний https-порт для Indeed Key по умолчанию 83.

`CUSTOM_SP_*`	Адрес приложения (DNS-имя и порт, если явно указан), которое поп политику безопасности для доступа к IDP (белый список).
	Примеры:
	• Если при подключении к приложению используется адрес `https://provider.test.local:333/..`, то значение перем будет `provider.test.local:333`.
	• `*.test.local`
	Если такие приложения отсутствуют, оставьте переменные с пустым значениями.
	
	При необходимости добавить более пяти сервисных провайдеров:
	1. Добавьте дополнительные переменные в файл *.env* по аналогии добавленными по умолчанию (`CUSTOM_SP_6=`, `CUSTOM_SP_7=`
	2. Добавьте переменные в файл *access-manager.docker-compose.ym* раздел `idp:environment`.
	Пример
	`idp:`
	` environment:`
	`...`
	`AMIDP_ContentSecurityPolicy__FormAction__From_`
	`"${CUSTOM_SP_6}"`
	`AMIDP_ContentSecurityPolicy__FormAction__From_`
	`"${CUSTOM_SP_7}"`

Создание каталогов

Чтобы создать каталоги *EventCache* (хранение кеша), *Logs* (логи) и *DataProtectionKeys* (ключи шифрования), из каталога *am* запустите команду:

```
sudo mkdir \
core/EventCache/ core/Logs/ core/DataProtectionKeys/ \
idp/EventCache/ idp/Logs/ idp/DataProtectionKeys/ \
mc/EventCache/ mc/Logs/ mc/DataProtectionKeys/ \
uc/EventCache/ uc/Logs/ uc/DataProtectionKeys/ \
ls/EventCache/ ls/Logs/ ls/DataProtectionKeys/ \
indeed-key/EventCache/ indeed-key/Logs/ indeed-key/DataProtectionKeys/ \
sms-proxy/Logs/ sms-proxy/DataProtectionKeys/
```

Настройка прав

Перед запуском Access Manager выдайте права пользователю, под которым планируете запускать Access Manager в Docker.

Сделайте владельцем пользователя, указанного в файле *.env* в переменных `AM_UID` и `AM_GID`, запустив следующую команду:

```
sudo chown -R <AM_UID>:<AM_GID> ./*
```

Подготовка сертификатов

Генерация служебных сертификатов

Серверный и публичный сертификаты

Настройка собственного клиентского сертификата

Добавление собственного клиентского сертификата

Генерация служебных сертификатов

Добавьте следующие сертификаты в каталог *ssl/*:

- *ssl/<серверный сертификат>.pfx* — серверный сертификат, выписанный на DNS-имя машины.
- *ssl/ca/<публичный сертификат>.cer* — публичный сертификат домена в формате Base64. Если публичный сертификат выдан не доменным удостоверяющим центром (УЦ), добавьте публичный сертификат стороннего УЦ.

Запуск скриптов

Чтобы настроить работу встроенного сертификата, запустите следующие скрипты в каталоге *ssl*. Убедитесь, что в каталоге *ssl* находятся только скрипты и добавленные ранее сертификаты.

- *convertPfxForReverseProxy.sh*
- *convertPfxForReverseProxy_ik_external.sh*
- *generateHttpsCerts.sh*
- *generateSamlCerts.sh*
- *generateSmsCert.sh*
- *prepareCaFile.sh*

Перед запуском скриптов ограничьте права запуска для всех пользователей системы, не имеющих прав `sudo`. Для этого, находясь в каталоге *ssl*, выполните команду `sudo chmod 400 *.sh`.

1. Сконвертируйте *.pfx* в сертификат HAProxy:

   ```
   sudo bash ./convertPfxForReverseProxy.sh -f <серверный сертификат>.pfx -p
   <пароль>
   ```

   Результат: создается серверный сертификат *am/ssl/https/reverse_proxy_server.pem*, предоставляющий HAProxy для внешних клиентов (Api Core, WebUI MC, UC и IDP).

2. При установке Indeed Key Server сконвертируйте *.pfx* в сертификат HAProxy:

   ```
   sudo bash ./convertPfxForReverseProxy_ik_external.sh -f <серверный
   сертификат>.pfx -p <пароль>
   ```

   Результат: создается серверный сертификат *am/ssl/https/reverse_proxy_server_ik.pem*, предоставляющий HAProxy для внешних клиентов к Indeed Key Server.

3. Сгенерируйте HTTPS-сертификаты контейнеров, используемые внутри сети Docker.

```
sudo bash ./generateHttpsCerts.sh
```

Результат: создаются сертификаты *am/ssl/https/<service>.pfx* для сервисов Core, MC, UC, IDP и Log Server. Расположение и пароли сертификатов указаны в конфигурационных файлах компонентов.

4. Сгенерируйте служебные сертификаты, которые используются в IDP при SAML-соединении.

```
sudo bash ./generateSamlCerts.sh
```

Результат: создается три сертификата *am/ssl/saml_certs/<service>.pfx*. Расположение и пароли сертификатов указаны в конфигурационных файлах компонентов UC, MC и IDP.

> **ПРИМЕЧАНИЕ**
>
> При использовании балансировщика нагрузки добавьте каталог *saml_certs* с содержимым на всех серверах.

5. Сгенерируйте сертификат, которому будут доверять контейнеры.

```
sudo bash ./prepareCaFile.sh
```

Результат: создается сертификат *am/ssl/ca/trusted_ca.crt*, который содержит список всех добавленных в *am/ssl/ca* публичных сертификатов.

> **ПРИМЕЧАНИЕ**
>
> При изменении состава каталога *am/ssl/ca* необходимо перезапустить скрипт *prepareCaFile.sh*.

Настройка собственного клиентского сертификата

> ⚠ **ВАЖНО**
>
> Для повышения безопасности рекомендуется использовать собственный клиентский сертификат.
>
> Собственный клиентский сертификат не поддерживается в модулях RDP Windows Logon и Windows Logon.

Чтобы использовать собственный сертификат, выпишите сертификат для аутентификации на Core Server.

1. Чтобы сгенерировать сертификат, перейдите в каталог *am/tools* и запустите скрипт *tool_gen_client_cert.sh*.

   ```
   sudo bash ./tool_gen_client_cert.sh -f mycert
   ```

   Важно: После отработки скрипта в терминале отображается пароль от сертификата *<certName>.pfx*, который необходимо сохранить.

   Результат:

   - *am/tools/certName.pfx* — сертификат с приватным ключом для аутентификации на Core Server,
   - *am/ssl/ca/certName.cer* — публичный ключ для доверия *certName.pfx*,
   - значение отпечатка сертификата автоматически подставляется в конфигурационный файл Core Server *am/core/app-settings.json* в разделе `Authentication:Certificate:Thumbprints`.

Пример раздела `Certificate`

```
“Certificate”: {
“ForwardingHeader”: “X-IndeedAM-ClientCert”,
“Thumbprint”: “01de449b6f4b49e00d1a5b20ffb5d6605cf6cd2a”,
“Thumbprints”: [
                "31650135EFE9CFEB83500A3DFE9FB747DC77480E",
                "E2163AF0B2D72C8C5CEC2A6E289DFD0C8B7940B3",
                "8FEEC416480E0F69A1E67BCBAE3DBBE7D1F449F2"
                ]
}
```

Где:

- `Thumbprint` — отпечаток встроенного клиентского сертификата,
- `Thumbprints` — отпечатки собственных клиентских сертификатов, которым будет доверять Core Server.

> **ПРИМЕЧАНИЕ**
>
> При использовании балансировщика нагрузки:
>
> - добавьте сертификаты *certName.pfx* и *certName.cer* на все сервера в соответствующие директории,
> - добавьте значения отпечатка сертификата в соответствующие файлы на всех серверах.

2. Создайте каталог *am/ssl/client* и скопируйте *certName.pfx* в этот каталог.

3. Из каталога *am/ssl* запустите скрипт *prepareCaFile.sh* для повторной генерации *trusted_ca.crt*.

```
sudo bash ./prepareCaFile.sh
```

Результат: создается сертификат *am/ssl/ca/trusted_ca.crt*, который содержит список всех добавленных в *am/ssl/ca* публичных сертификатов.

> **ПРИМЕЧАНИЕ**
>
> При изменении состава каталога *am/ssl/ca* необходимо перезапустить скрипт *prepareCaFile.sh*.

4. Сделайте владельцем пользователя Access Manager в Docker-контейнере для обновленного сертификата *am/ssl/ca/trusted_ca.crt*.

```
sudo chown <AM_UID>:<AM_GID> ./ssl/ca/trusted_ca.crt
```

5. Перезапустите контейнер с приложением с помощью команды `sudo docker-compose up -d`.

Indeed Log Server

Indeed Log Server (Log Server) — это веб-приложение, работающее на базе HTTP-сервера Kestrel. Данный модуль отвечает за централизованный сбор и аудит событий системы.

События записываются в базы данных.

Как создать и настроить базу данных?

Установка Log Server

Системные требования

Отдельно устанавливать Log Server не нужно. Компонент устанавливается автоматически при распаковке архива *am_images/indeed-log-server.tar.gz* или, если в вашей версии AM нет каталога *am_images*, при распаковке *am-<номер версии>.tar.gz*.

Для корректной работы компонента Log Server необходимо настроить соединение с базой данных.

Настройка Log Server с разным типом хранилища данных

Вы можете выбрать доступное вам хранилище данных:

- базы данных Microsoft SQL или PostgreSQL
- хранилище в Syslog
- резервное хранилище

Microsoft SQL

Microsoft SQL

1. Откройте файл *am/ls/targets/DbTargetMssqlAM.config* и в строке `ConnectionString` укажите данные:

   - `Data Source` — DNS/IP-адрес сервера с базой данных.
   - `Initial Catalog` — имя базы данных.
   - `User ID` — имя пользователя, который имеет полные права для базы данных Database.
   - `Password` — пароль пользователя.
   - `TrustServerCertificate` — доверие серверному сертификату. Убедитесь, что задано значение `True` для подключения Microsoft SQL к серверу.

     Порт подключения в строке `ConnectionString` не прописан, но задан по умолчанию — 1433. В примере ниже порт указан через запятую в строке `Data Source`.

   Пример

```
    <?xml version="1.0" encoding="utf-8"?>
     <Settings>
       <ConnectionString>Data Source=192.168.1.22,57974;Initial
Catalog=IndeedAM9log;User
ID=IndeedAMservice;Password=Q12345qq;TrustServerCertificate=true;
</ConnectionString>
     </Settings>
```

2. Откройте конфигурационный файл сервера *am/ls/clientApps.config* и раскомментируйте блок `<Application Id="ea" SchemaId="eaSchema">`.

   В тегах `ReadTargetId` и `TargetId` укажите значение `DbTargetMssqlAM`, где `DbTargetMssqlAM` — это название конфигурационного файла в каталоге *am/ls/targets*.

   Пример

```
 <Application Id="ea" SchemaId="eaSchema">
  <ReadTargetId>DbTargetMssqlAM</ReadTargetId>
  <WriteTargets>
      <TargetId>DbTargetMssqlAM</TargetId>
  </WriteTargets>
  <AccessControl>
      <CertificateAccessControl
CertificateThumbprint="01de449b6f4b49e00d1a5b20ffb5d6605cf6cd2a"
Rights="Write" />
  </AccessControl>
 </Application>
```

- В тегах `ReadTargetId` указывается идентификатор хранилища, откуда будет осуществляться чтение событий.
- В блоке `WriteTargets`, в тегах `TargetId`, указывается идентификатор хранилища, куда будет осуществляться запись событий.
- Идентификаторы заданы в теге `Targets`, конфигурационные файлы для каждого типа находятся в каталоге *am/ls/targets/* с соответствующим именем.
- При использовании собственного клиентского сертификата в `CertificateThumbprint` указывается отпечаток клиентского сертификата Core Server.

3. При необходимости использовать дополнительное хранилище данных откройте конфигурационный файл сервера *am/ls/clientApps.config* и раскомментируйте необходимые значения в секции `Targets`.

Пример

```
<Targets>
<!-- <Target Id="DbTargetSqlAM" Type="pgsql" /> -->
<Target Id="DbTargetMssqlAM" Type="mssql" />
<!-- <Target Id="DbTargetSqlIndeedKey" Type="pgsql" /> -->
<!-- <Target Id="DbTargetMssqlIndeedKey" Type="mssql" /> -->
<Target Id="TargetSyslog" Type="syslog" />
</Targets>
```

PostgreSQL

PostgreSQL

1. Откройте файл *am/ls/targets/DbTargetSqlAM.config* и в блоке `Settings` укажите данные:

   - В строке `ConnectionString`:
     - `Server` — DNS/IP-адрес сервера с базой данных PostgreSQL.
     - `Database` — имя базы данных.
     - `User ID` — имя пользователя, который имеет полные права для базы данных Database.
     - `Password` — пароль пользователя.
     - `SSL Mode` — для подключения с использованием SSL.

       Если после добавления параметра `SSL Mode` возникает ошибка *08P01: unsupported startup parameter: ssl_renegotiation_limit*, добавьте параметр `Server Compatibility Mode=Redshift`.
   - Добавьте блок `Options` и в строке `Option Name` добавьте параметр `EnableShortStringEqualsSearch` в значении `True`. Параметр ускоряет поиск в больших БД. По умолчанию настройка отключена.

   Пример

   ```
   <?xml version="1.0" encoding="utf-8"?>
   <Settings>
     <ConnectionString>server=192.168.80.30;port=5432;user
   id=amservice;password=Q1w2e3r4;database=am_deb_db;SSL Mode=Require;Server
   Compatibility Mode=Redshift</ConnectionString>
     <Options>
       <Option Name="EnableShortStringEqualsSearch" Value="True" />
     </Options>
   </Settings>
   ```

2. Откройте конфигурационный файл сервера *am/ls/clientApps.config* и раскомментируйте блок `<Application Id="ea" SchemaId="eaSchema">`.

   В тегах `ReadTargetId` и `TargetId` укажите значение `DbTargetSqlAM`, где `DbTargetSqlAM` — это название конфигурационного файла в каталоге *am/ls/targets*.

   Пример

```
 <Application Id="ea" SchemaId="eaSchema">
  <ReadTargetId>DbTargetSqlAM</ReadTargetId>
  <WriteTargets>
      <TargetId>DbTargetSqlAM</TargetId>
  </WriteTargets>
  <AccessControl>
      <CertificateAccessControl
CertificateThumbprint="01de449b6f4b49e00d1a5b20ffb5d6605cf6cd2a"
Rights="Write" />
  </AccessControl>
 </Application>
```

- В тегах `ReadTargetId` указывается идентификатор хранилища, откуда будет осуществляться чтение событий.
- В блоке `WriteTargets`, в тегах `TargetId`, указывается идентификатор хранилища, куда будет осуществляться запись событий.
- Идентификаторы заданы в теге `Targets`, конфигурационные файлы для каждого типа находятся в каталоге *am/ls/targets/* с соответствующим именем.
- При использовании собственного клиентского сертификата в `CertificateThumbprint` указывается отпечаток клиентского сертификата Core Server.

3. При необходимости использовать дополнительное хранилище данных откройте конфигурационный файл сервера *am/ls/clientApps.config* и раскомментируйте необходимые значения в секции `Targets`.

Пример

```
<Targets>
<Target Id="DbTargetSqlAM" Type="pgsql" />
<!-- <Target Id="DbTargetMssqlAM" Type="mssql" /> -->
<!-- <Target Id="DbTargetSqlIndeedKey" Type="pgsql" /> -->
<!-- <Target Id="DbTargetMssqlIndeedKey" Type="mssql" /> -->
<Target Id="TargetSyslog" Type="syslog" />
</Targets>
```

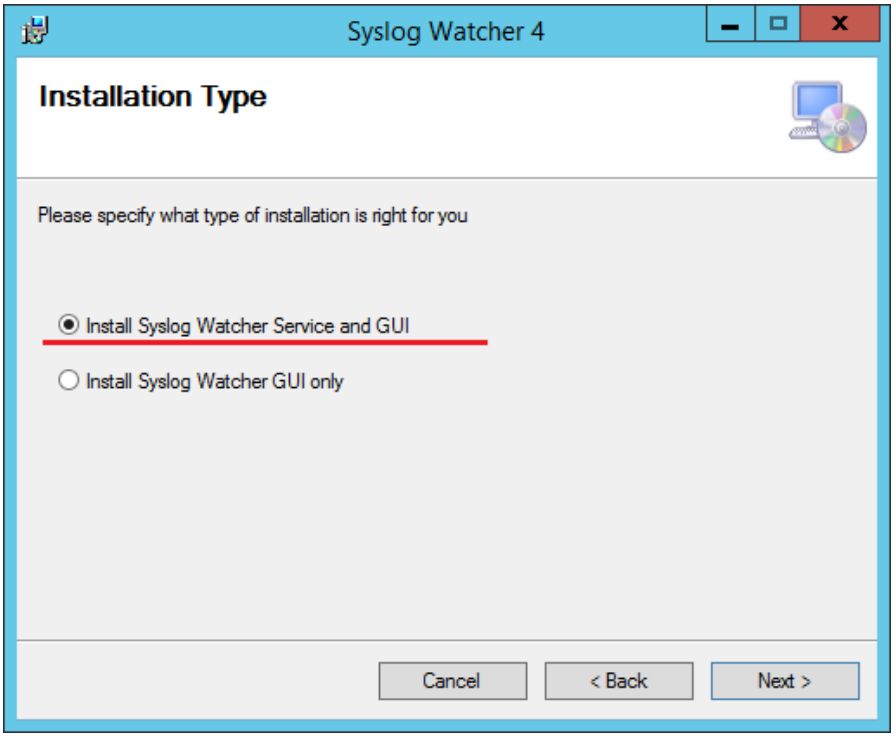
Хранилище в Syslog

Хранилище в Syslog

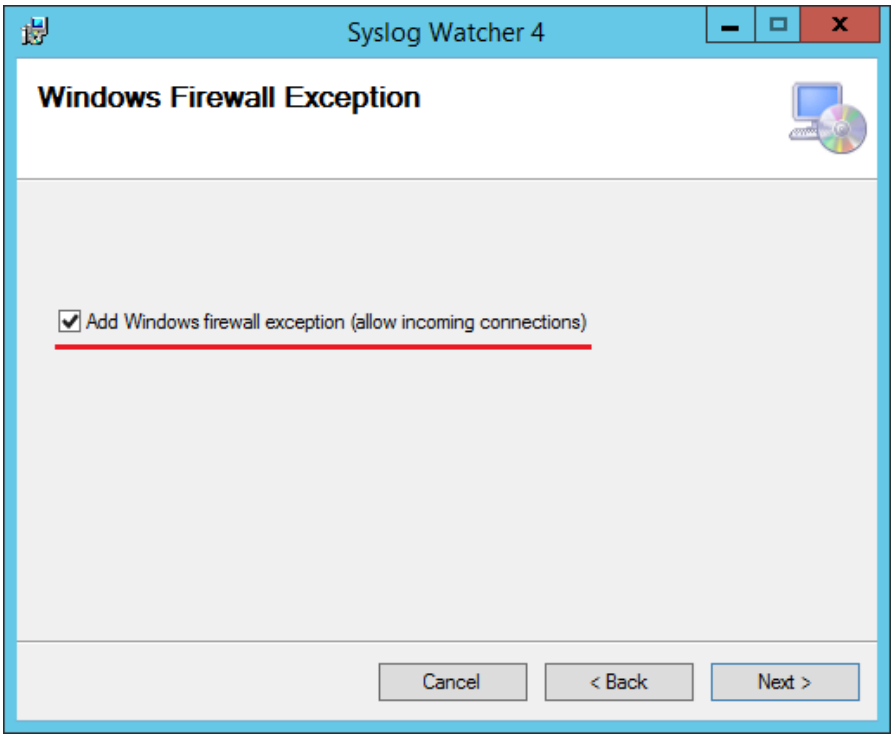
Log Server поддерживает формат syslog, вы можете использовать любой сервер, работающий с данным форматом. В качестве примера далее рассмотрена настройка syslog сервера Syslog Watcher v4.8.6.

Вы можете скачать утилиту на официальном сайте https://syslogwatcher.com

1. Запустите установочный файл *SyslogWatcherSetup-*.*.*-win32.msi*.
2. В окне License Agreement примите лицензионное соглашение.
3. В окне Installation Type выберите тип установки Install Syslog Watcher Service and GUI.



4. В окне Select installation Folder выберите путь установки для sys-log сервера.
5. В окне Windows Firewall Exception разрешите добавление правила на все входящие соединения для Syslog Watcher в брандмауэр Windows.

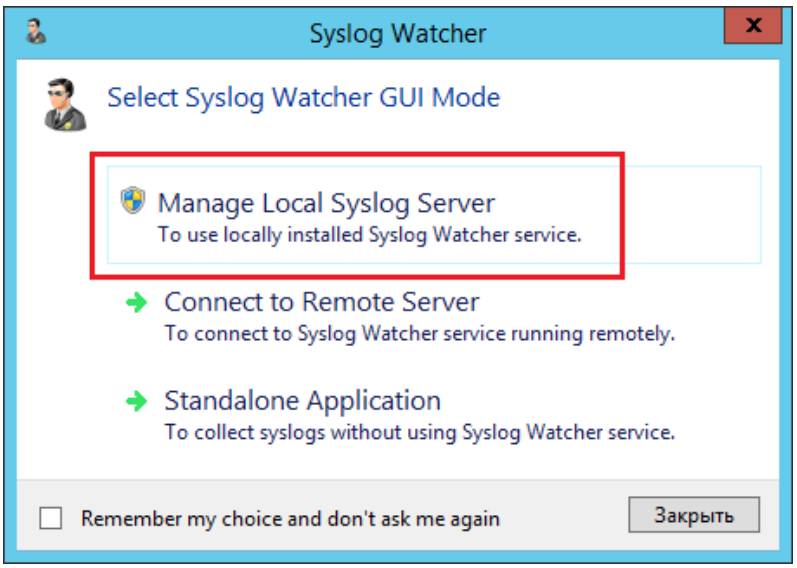


6. В окне Confirm Installation нажмите Next для подтверждения установки.

7. Дождитесь завершения установки сервера.

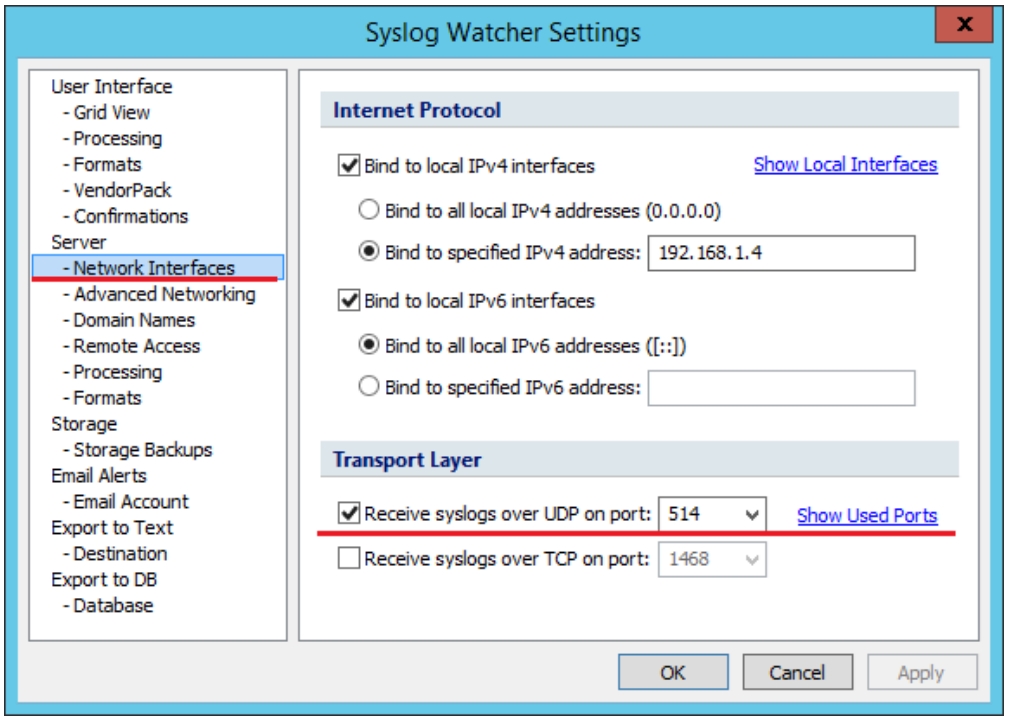
Настройка Syslog-сервера

1. Запустите Syslog Watcher и выберите Manage Local Syslog Server.

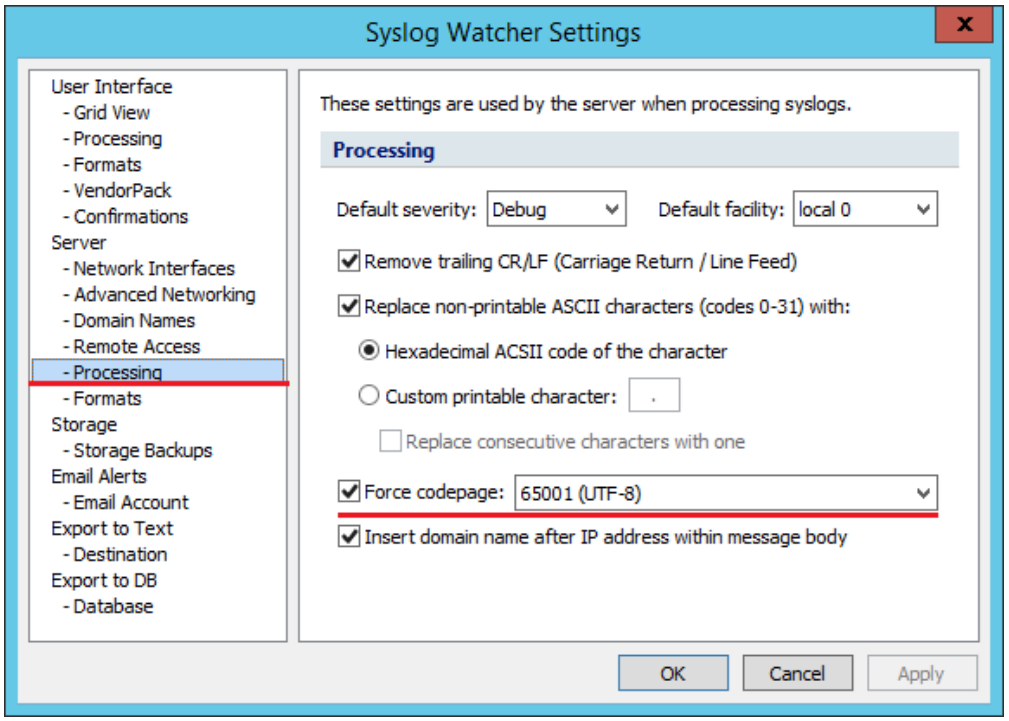


2. Нажмите Settings в верхнем меню программы.

    1. Выберите пункт Network Interfaces.
    2. Проверьте, что выбрано использование протокола udp и указан порт.



3. Выберите пункт Processing. Выберите кодировку UTF-8.



Редактирование конфигурационного файла

1. Откройте конфигурационный файл *am/ls/sampleSyslog.config* и укажите следующие параметры в теге *ConnectionString*:

   - `HostName` — имя или IP-адрес Syslog-сервера.
   - `Port` — порт Syslog-сервера (514 — порт по умолчанию).
   - `Protocol` — тип подключения к Syslog-серверу: UDP, TCP, TCPoverTLS.

- `Format` — опциональный параметр, определяет формат логов: Plain (по умолчанию), CEF, LEEF.
- `SyslogVersion` — опциональный параметр, спецификация протокола: RFC3164, RFC5424.

Пример настройки для Syslog Watcher

```
<Settings HostName="localhost" Port="514" Protocol="UDP" Format="Plain"  />
```

2. Откройте конфигурационный файл *am/ls/clientApps.config*.

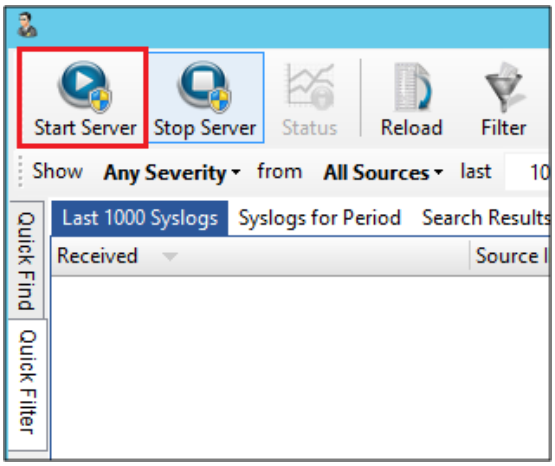
3. Для блока с `Application Id"="ea"` в теге `TargetId` для `WriteTargets` укажите `sampleSyslog`. Тег `ReadTargetId` оставьте пустым, так как чтение выполняется сторонней программой, в данном примере Syslog Watcher.

> **ИНФОРМАЦИЯ**
>
> В тегах `ReadTargetId` указывается идентификатор хранилища, откуда будет осуществляться чтение событий.
>
> В блоке `WriteTargets`, в тегах `TargetId` указывается идентификатор хранилища, куда будет осуществляться запись событий.
>
> Идентификаторы заданы в теге `Targets`, конфигурационные файлы для каждого типа находятся в каталоге *am/ls/target/* с соответствующим именем.
>
> В `CertificateThumbprint` указывается отпечаток клиентского сертификата Core Server.

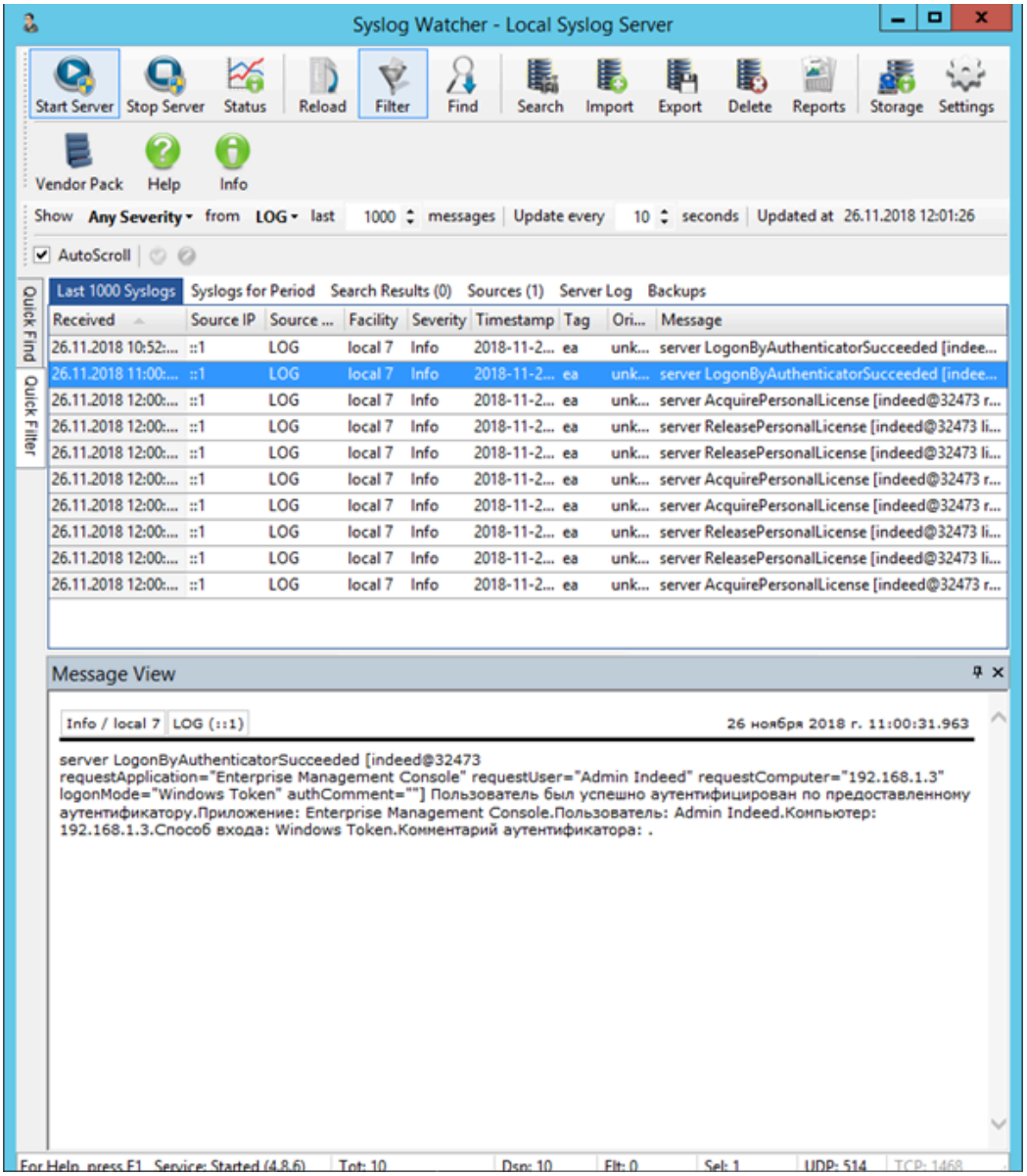
Пример

```
 <Application Id="ea" SchemaId="eaSchema">
    <ReadTargetId> </ReadTargetId>
        <WriteTargets>
            <TargetId>sampleSyslog</TargetId>
        </WriteTargets> <AccessControl>
<CertificateAccessControl CertificateThumbprint="001122...AA11"
Rights="Read" /> </AccessControl>
</Application>
```

4. Нажмите Start Server в верхнем левом углу программы Syslog Watcher.



Пример отображения



Резервное хранилище

Резервное хранилище

Настройка с резервным хранилищем в базе данных

1. Откройте конфигурационный файл сервера *am/ls/clientApps.config*.
2. В блоке `Targets` скопируйте тег `Target` с `Id="sqlTargetAM"` и измените id на произвольное значение, например `sqlDbBackup`.

   Пример

   ```
   <Targets>
       <Target Id="sampleEventLog" Type="pgsql"/>
       <Target Id="sqlDbBackup" Type="pgsql"/>
       <Target Id="sampleSyslog" Type="syslog"/>
   </Targets>
   ```

3. Для блока с `Application Id="ea"` в тегах `ReadTargetId` указать `sqlTargetAM`.

   ИНФОРМАЦИЯ

   В тегах `ReadTargetId` указывается идентификатор хранилища, откуда будет осуществляться чтение событий.

   В блоке `WriteTargets` в тегах `TargetId` указывается идентификатор хранилища, куда будет осуществляться запись событий.

   Идентификаторы заданы в теге `Targets`, конфигурационные файлы для каждого типа находятся в каталоге *am/ls/target/* с соответствующим именем.

4. В блоке `WriteTargets` укажите `<TargetId>sqlTargetAM</TargetId>` и `<TargetId>sqlDbBackup</TargetId>`.

   ИНФОРМАЦИЯ

   При такой конфигурации чтение событий будет осуществляться из базы данных, указанной в конфигурационном файле *am/ls/sqlTargetAM.config*. Запись будет осуществляться в базы данных указанные в файлах:

   - *am/ls/sqlTargetAM.config*
   - *am/ls/sqlDbBackup.config*

Пример

```
<Application Id="ea" SchemaId="eaSchema">
  <ReadTargetId>sqlTargetAM</ReadTargetId>
  <WriteTargets>
    <TargetId>sqlTargetAM</TargetId>
    <TargetId>sqlDbBackup</TargetId>
  </WriteTargets>
  <AccessControl>
    <CertificateAccessControl CertificateThumbprint="001122...AA11"
Rights="Read" />
  </AccessControl>
</Application>
```

5. Откройте конфигурационный файл *am/ls/sqlTargetAM.config* и укажите данные в строке `ConnectionString`:

   - `Server` — DNS/IP-адрес сервера с базой данных.
   - `Database` — имя базы данных.
   - `User ID` — имя пользователя, который имеет полные права для базы данных Database.
   - `Password` — пароль пользователя.

   Пример

```
<?xml version="1.0" encoding="utf-8"?>
<Settings>
  <ConnectionString>Server=Server;Database=Name;User
ID=User;Password=Password</ConnectionString>
</Settings>
```

6. Создайте файл *sqlDbBackup* с расширением .config.

> ⚠ **ВАЖНО**
>
> Имя файла должно в точности повторять значение Id, заданного в пункте 2.

7. Укажите данные для подключения к резервной базе данных в теге `connectionString`, аналогично пункту 6.

Включить/отключить шифрование конфигурационных файлов Log Server

С помощью утилиты для шифрования можно зашифровать пароль серверного сертификата в конфигурационном файле *am/ls/app-settings.json*, а также значение параметра `ConnectionString` в конфигурационных файлах в каталоге *am//ls/targets/*.

1. В терминале перейдите в каталог с утилитой для шифрования *am/protection*.

```
cd /am/protection
```

2. Выдайте права для запуска скрипта `protector.sh`.

```
sudo chmod 500 protector.sh
```

3. Чтобы зашифровать конфигурационные файлы, запустите скрипт `protector.sh` с параметром `protect`.

```
sudo bash ./protector.sh protect
```

4. Чтобы расшифровать конфигурационные файлы, запустите скрипт `protector.sh` с параметром `unprotect`.

```
sudo bash ./protector.sh unprotect
```

Настройка кеширования событий

Если Log Server недоступен, события кешируются в локальный каталог *am/ls/EventCash*.

Информация о недоступности Log Server отображается в событиях Windows во вкладке *Приложение*.

- Код события — 500.
- Текст — *Log server client fluentSchedulerBackgroundLoaderTask. Iteration WEB exception: Время ожидания операции истекло*.

Чтобы изменить параметры хранения событий:

1. Откройте конфигурационный файл *app-settings.json* серверного компонента (Core Server, Management Console, User Console).
2. Внесите следующие изменения:

- Чтобы задать путь к каталогу для хранения событий, измените значение параметра `location` в теге `logServer`. Значение по умолчанию — *./EventCache*.
- Чтобы изменить время отправки логов после возобновления работы LogServer, измените значение параметра `FlushInterval` в теге `logServer`. Значение по умолчанию — *10 минут*.

Не рекомендуется устанавливать значение для параметра `EventCacheSendingIntervalSec` менее 30 секунд.

Локализация

В данный момент в схеме есть локализация событий ru-Ru и en-En. Когда с сервера поступает запрос на ru-Ru события, будут выбраны имеющиеся события с локализацией ru-Ru.

Если с сервера поступает запрос с неизвестной локализацией, то будут выбраны события с локализацией, заданной по умолчанию.

Чтобы настроить локализацию:

1. Откройте конфигурационный файл *am/ls/eaSchema.config*.
2. Измените значение параметра `DefaultLanguage`.

Пример локализации событий en-En

```
<Languages DefaultLanguage="en-En">
```

Пример локализации событий ru-RU

```
<Languages DefaultLanguage="ru-RU">
```

3. Сохраните изменения.

Сбор логов

Информация по включению логирования и сбору логов компонента Log Server находится в разделе Сбор логов серверных компонентов.

Indeed Core Server

Indeed Core Server (Core Server) — это основной модуль системы, который отвечает за:

- централизованное хранение аутентификаторов, паролей и настроек пользователей;
- централизованное управление и администрирование;
- централизованный прием и обработку запросов от других модулей системы;
- координирование действий отдельных модулей и системы в целом.

Core Server кеширует данные при получении пользователя, группы, контейнера, сценариев авторизации и бизнес логики. Основные запросы в каталог — получение пользователя, группы, контейнера по ID — отдаются из кеша. Все остальные запросы — по имени, по телефону, email — только обновляют кеш данными из каталога. Первый запрос пользователя по ID также обновляет кеш, последующие берутся из кеша. Время жизни объекта в кеше — 10 минут.

Установка Core Server

Системные требования

Отдельно устанавливать Core Server не нужно. Компонент устанавливается автоматически при распаковке архива *am_images/core.tar.gz* или, если в вашей версии AM нет каталога *am_images*, при распаковке *am-<номер версии>.tar.gz*.

Для корректной работы компонента Core Server необходимо выполнить следующие шаги:

1. Отредактируйте конфигурационный файл Core Server.
2. Запустите контейнер с приложением.
3. Настройте начальную аутентификацию.
4. При необходимости задайте опциональные настройки.

Редактирование конфигурационного файла

Для настройки Core Server внесите изменения в конфигурационный файл *am/core/app-settings.json*.

> ⚠ **ВАЖНО!**
>
> Измените только параметры со значениями вида *!!! комментарий !!!*.

1. В блоке `Behavior` для параметра `Administration` в строке `RootAdministrator` укажите имя привилегированного пользователя.

> **ПРИМЕЧАНИЕ**
>
> Пользователь, заданный в этом параметре, автоматически получит права первичного администратора при первой аутентификации в Management Console.

Active Directory

Укажите имя привилегированного пользователя в формате `UserId_GUID`.

Где:

- `UserId` — произвольный уникальный идентификатор каталога (параметр `Id`). Идентификатор может состоять только из букв и цифр, спецсимволы не поддерживаются.
- `GUID` — уникальный идентификатор пользователя из Active Directory.

Получить `GUID` можно с помощью команды на контроллере домена:

```
Get-ADUser -Filter 'Name -like "<User logon name>"' | FT Name,ObjectGUID -A
```

FreeIPA

Укажите имя привилегированного пользователя в формате `UserId_entryUUID`.

Где:

`entryUUID` — уникальный идентификатор пользователя из FreeIPA.

Получить `entryUUID` можно с помощью команды на контроллере домена:

```
ldapsearch -x -D "uid=admin-indeed,cn=users,cn=accounts,dc=test,dc=local" -W -b
"cn=users,cn=accounts,dc=test,dc=local" "uid=admin-indeed" entryUUID
```

2. Задайте каталог конечных пользователей, для этого измените следующие строки в параметре `UserCatalog`.

Active Directory

Пример настройки каталога

```
      "Administration": {
            "RootAdministrator": "UserId_15511150-6804-4bf2-ac7c-
b8a8520ea357"
        }
    },
      "UserCatalog": {
    "RootProvider": "UserId",
    "Providers": {
      "Ldap": [
        {
          "Id": "UserId",
          "Domain": "second.com",
          "Port": 636,
          "SecureSocketLayer": true,
          "LdapServerType": "ActiveDirectory",
          "ContainerPath": "CN=users,DC=second,DC=com",
          "UserName": "admin@second.com",
          "Password": "password"
        }
      ]
    },
```

- `RootProvider` — идентификатор корневого пользовательского каталога. Также с помощью этого параметра вы можете объединить несколько каталогов через правило `OR`.
- `Id` — произвольный уникальный идентификатор каталога. Если вы планируете использовать базу данных от версии Access Manager 8.2.x, идентификаторы каталога должны совпадать.
- `Domain` — имя домена или имя конкретного контроллера домена Active Directory, в котором находится каталог.
- `Port` — порт для соединения по протоколу LDAPS/LDAP, по умолчанию задано значение 636.

> ⚠ **ВАЖНО!**
>
> Не рекомендуется использовать незащищенное LDAP-соединение ("Port": 389, "SecureSocketLayer": false). При таком соединении ваши данные не защищены.

- `SecureSocketLayer` — опция для включения или отключения SSL для защищенного соединения, по умолчанию указано значение *true*.

- `LdapServerType` — настройка определяет тип LDAP-сервера, задайте значение `ActiveDirectory`.
- `ContainerPath` — путь к контейнеру в виде Distinguished Name или весь домен, если для хранения пользователей используется весь домен.
- `UserName` — имя сервисной учетной записи для подключения к каталогу пользователей.
- `Password` — пароль сервисной учетной записи.

> ⚠ **ВАЖНО!**
>
> Не изменяйте настройки в параметре `UserCatalog` в секции `SensitiveDataEncryption`.

FreeIPA

Пример настройки каталога

```
 "Administration": {
           "RootAdministrator": "UserId_15511150-6804-4bf2-ac7c-
b8a8520ea357"
        }
    },
     "UserCatalog": {
    "RootProvider": "UserId",
    "Providers": {
      "Ldap": [
        {
          "Id": "UserId",
          "Domain": "second.com",
          "Port": 636,
          "SecureSocketLayer": true,
          "LdapServerType": "FreeIpa",
          "ContainerPath": "cn=accounts,DC=second,DC=com",
          "UserName": "uid=admin-
indeed,cn=users,cn=accounts,dc=second,dc=com",
          "Password": "password",
           "CatalogFilter": "|(objectClass=person)(objectClass=ipausergroup)
(entrydn=cn=users,cn=accounts,*)"
        }
      ]
    },
```

- `RootProvider` — идентификатор корневого пользовательского каталога. Также с помощью этого параметра вы можете объединить несколько каталогов через правило `OR`.
- `Id` — произвольный уникальный идентификатор каталога. Если вы планируете использовать базу данных от версии Access Manager 8.2.x, идентификаторы каталога должны совпадать.
- `Domain` — имя домена или имя конкретного контроллера домена FreeIPA, в котором находится каталог.
- `Port` — порт для соединения по протоколу LDAPS/LDAP, по умолчанию задано значение 636.
- `SecureSocketLayer` — опция для включения или отключения SSL для защищенного соединения, по умолчанию указано значение *true*.
- `LdapServerType` — настройка определяет тип LDAP-сервера, задайте значение `FreeIPA`.
- `ContainerPath` — путь к контейнеру в виде Distinguished Name или весь домен, если для хранения пользователей используется весь домен.
- `UserName` — имя сервисной учетной записи в формате Distinguished Name.
- `Password` — пароль сервисной учетной записи.
- `CatalogFilter` — фильтр поиска пользователей в Management Console. Чтобы не отображать среди вариантов поиска системные контейнеры, задайте значение `|(objectClass=person)(objectClass=ipausergroup)`.

3. В блоке `Storage` в секции `SensitiveDataEncryption` параметры `Algorithm` и `Key` заполняются автоматически при генерации ключа.

   Чтобы сгенерировать ключ, запустите скрипт *am/tools/tool_encryption_db.sh*. Для просмотра и выбора алгоритма, можно вывести справку.

   ```
   sudo bash ./tool_encryption_db.sh --help
   sudo bash ./tool_encryption_db.sh -a Aes
   ```

   > **ПРИМЕЧАНИЕ**
   >
   > Если при обновлении вы используете базу данных от Access Manager 8.x, укажите значения `Algorithm` и `Key` из конфигурационного файла Core Server для Access Manager 8.x (*C:\inetpub\wwwroot\am\core\Web.config*, тег `encryptionSettings`). Таким образом вы избежите повторного шифрования базы данных.

4. Укажите параметры базы данных.

   Microsoft SQL

   Измените следующие строки в блоке `Storage` для параметра `Provider`:

   - `Type` — укажите тип используемой СУБД — `Mssql`.

- `ConnectionString` — укажите следующие данные:
  - `Data Source` — IP-адрес сервера базы данных.
  - `Initial Catalog` — имя базы данных.
  - `User ID` — имя пользователя, который имеет полные права для базы данных.
  - `Password` — пароль пользователя.
  - `TrustServerCertificate` — доверие серверному сертификату. Убедитесь, что задано значение `True` для подключения Microsoft SQL к серверу.

Пример

```
"Provider": {
  "Type": "Mssql",
  "ConnectionString": "Data Source=192.168.1.22,57974;Initial
Catalog=IndeedAM9log;User
ID=IndeedAMservice;Password=Q12345qq;TrustServerCertificate=true;"
},
```

PostgreSQL

Измените следующие строки в блоке `Storage` для параметра `Provider`:

- `Type` — укажите тип используемой СУБД — `PostgreSql`.
- `ConnectionString` — укажите следующие данные:
  - `server` — IP-адрес сервера базы данных.
  - `port` — используемый порт. По умолчанию — 5432.
  - `user id` — имя пользователя, который имеет полные права для базы данных.
  - `password` — пароль пользователя.
  - `database` — база данных, содержащая данные об Indeed Core Server.
  - `SSL Mode` — для подключения с использованием SSL.

Пример

```
"Provider": {
  "Type": "PostgreSql",
  "ConnectionString": "server=192.168.80.30;port=5432;user
id=amservice;password=password;database=AMdebian2;SSL Mode=Require"
},
```

Если после добавления параметра `SSL Mode` возникает ошибка *08P01: unsupported startup parameter: ssl_renegotiation_limit*, добавьте в конец строки параметр `Server Compatibility Mode=Redshift`.

5. В параметре `Authentication` для параметра `Sign` поля `publicKey` и `privateKey` заполняются автоматически при генерации публичного и секретного ключа для подписи токена пользователя.

   Чтобы сгенерировать публичный и секретный ключи, запустите скрипт *am/tools/tool_keygen.sh*:

```
sudo bash ./tool_keygen.sh
```

Пример

```
"Authentication": {
     "Token": {
         "Sign": {
             "privateKey": "значение секретного ключа",
             "publicKey": "значение публичного ключа"
             }
     },
```

Запуск контейнера

Для создания и запуска контейнера выполните следующую команду:

```
sudo docker-compose up -d
```

Настройка начальной аутентификации

> **ПРИМЕЧАНИЕ**
>
> Для аутентификации рекомендуется использовать защищенное соединение по протоколу LDAPS с использованием 636 порта.

Для начальной аутентификации в Core Server и приложениях Management Console и User Console настройте провайдер Windows Password.

Чтобы настроить начальную аутентификацию, необходимо сформировать значение параметра `StringValue` в конфигурационном файле *am/core/initial-settings.json*:

1. Перейдите в каталог *am/tools/initial_settings* и откройте для редактирования файл *initial_settings.json*.

   - В поле `Filter` укажите регулярное выражение.
   - (Опционально) Если LDAPS-сертификат не позволяет устанавливать соединение по имени домена (не задано Дополнительное имя субъекта), в поле `FallbackHost` укажите значение своего домена. При использовании параметра `FallbackHost` увеличивается нагрузка на данный контроллер домена.

Пример файла initial_settings.json

```
{
    "Filter": "^domain1\\.com$",
    "Port": 636,
    "Secure": true,
    "FallbackHost": "dc.domain1.com"
},
{
    "Filter": ".*(\\.domain2.com)|(\\.domain3)$",
    "Port": 389,
    "Secure": false
},
{
    "Filter": "^domain4\\.com$",
    "Port": 636,
    "Secure": true,
    "FallbackHost": "dc.domain4.com"
}
```

2. Сохраните файл *initial_settings.json*.

3. Перейдите в каталог *am/tools/initial_settings* и запустите скрипт tool_initial_settings.sh.

В результате выполнения скрипта в конфигурационном файле *am/core/initial-settings.json* записывается значение параметра `StringValue`.

Пример параметра StringValue

```
[{\u0022F\u0022:\u0022^domain\\\\.com$\u0022,\u0022P\u0022:636,\u0022S\u0022:true,
```

Включить/Отключить шифрование конфигурационного файла

1. В терминале перейдите в каталог с утилитой для шифрования *am/protection*.

   ```
   cd /am/protection
   ```

2. Выдайте права для запуска скрипта `protector.sh`.

   ```
   sudo chmod 500 protector.sh
   ```

3. Чтобы зашифровать конфигурационные файлы, запустите скрипт `protector.sh` с параметром `protect`.

   ```
   sudo bash ./protector.sh protect
   ```

4. Чтобы расшифровать конфигурационные файлы, запустите скрипт `protector.sh` с параметром `unprotect`.

   ```
   sudo bash ./protector.sh unprotect
   ```

Проверка состояния сервера

Чтобы проверить состояние сервера, в браузере введите адрес Core Server в формате *https://<полное_dns_имя_сервера>/am/core*.

Автоматически вы будете перенаправлены на *https://<полное_dns_имя_сервера>/am/core/api/v6/healthCheck/index*.

Страница обновляется автоматически каждые 60 секунд.

На странице доступна следующая информация о состоянии сервера:

- статус доступности каталога пользователей, время обработки запроса к нему;
- статус хранилища, время обработки запроса к нему;
- список установленных провайдеров аутентификации, их статус и время загрузки;
- статус компонента Indeed Log Server;

> ⚠ **ВАЖНО!**
>
> Чтобы не получать ошибки при проверке состояния, рекомендуется использовать версию Log Server 9.3 и выше.

- список ошибок при наличии.

> ⓘ **ИНФОРМАЦИЯ**
>
> В целях безопасности список установленных провайдеров аутентификации и информация об ошибках доступны, только если вы открыли страницу с локального адреса.

Пример результата проверки

```
User Catalog{
  "PreviousCheckSucceeded": true,
  "CheckState": "Succeeded",
  "CheckStartDate": "2025-02-27T11:18:53.4937754+00:00",
  "CheckDuration": "00:00:00.0088105"
}

Storage{
  "PreviousCheckSucceeded": true,
  "CheckState": "Succeeded",
  "CheckStartDate": "2025-02-27T11:18:53.4947917+00:00",
  "CheckDuration": "00:00:00.0033496"
}

Authentication Providers{
  "PreviousCheckSucceeded": false,
  "CheckState": "Succeeded",
  "CheckStartDate": "2025-02-27T11:12:53.5523742+00:00",
  "CheckDuration": "00:00:00.0089791"
}

LogServer{
  "PreviousCheckSucceeded": false,
  "CheckState": "Succeeded",
  "CheckStartDate": "2025-02-27T11:12:53.5643188+00:00",
  "CheckDuration": "00:00:00.0457894"
}
```

Сбор логов

Информация по включению логирования и сбору логов компонента Core Server находится в разделе Сбор логов серверных компонентов.

Опциональные настройки

- Включение защиты от перебора
- Настройка нескольких пользовательских каталогов

- LDAP-фильтр при поиске пользователей и групп в службе каталогов
- Настройка времени ожидания для LDAP-соединения
- Настройка механизма отзыва лицензий
- Настройка прав пользователей вне политики

Включение защиты от перебора

В Indeed Access Manager вы можете настроить защиту от подбора учетных записей для компонента Indeed AM Identity Provider.

Если эта настройка включена, то при вводе несуществующего имени пользователя Indeed Access Manager имитирует вход существующего пользователя через Identity Provider: отображает способы аутентификации, запрашивает пароль, а затем отображает ошибку *Неверное имя пользователя или аутентификатор или заблокировано устройство*.

Если эта настройка выключена, то при вводе несуществующего имени пользователя Indeed Access Manager отображает ошибку *Внутренняя ошибка сервера: Пользователь не найден*.

По умолчанию данная настройка отключена.

Чтобы настроить защиту от перебора, выполните следующие действия:

1. Откройте конфигурационный файл сервера Indeed AM *am/core/app-settings.json*.
2. В блоке `Authentication` в строке `bruteForceProtection` через запятую укажите значение модулей, для которых вы хотите включить защиту от перебора.

   Пример

   ```
   "Authentication": {
       "BruteForceProtection": {
           "Applications": ["Windows Logon", "Identity Provider"]
       }
   }
   ```

3. Сохраните изменения и перезапустите контейнер с приложением.

Настройка нескольких пользовательских каталогов

> **ИНФОРМАЦИЯ**
>
> Если вы одновременно используете несколько различных служб каталогов (например и Active Directory, и FreeIPA), в которых находятся дублирующиеся пользователи, Access Manager воспринимает их как разных пользователей. В таком случае, используется две лицензии для одного пользователя.

Если настройка нескольких каталогов осуществляется в уже используемой системе Indeed (после выдачи первичных прав для администратора системы), и изменяется расположение администратора системы или префикс, заданный в параметре *RootAdministrator*, то потребуется удалить выданные ранее права и выполнить повторный запуск утилиты первичной конфигурации.

Для удаления прав необходимо удалить все данные из таблицы *DbAccessGroupMembers*, расположенной в базе данных системы Indeed.

> **СОВЕТ**
>
> Если контейнеры находятся в разных доменах/лесах, то требуется создать пользователя для чтения данных с контейнера в своем домене/лесе.

1. В теге `RootProvider` укажите значение `orUCP`.
2. Внутри тега `Ldap` добавьте блоки для подключения к контейнерам с параметром `Id`, в котором указывается идентификатор пользовательского контейнера.

   > **ИНФОРМАЦИЯ**
   >
   > Значение параметра `Id` в разделе `Or` должно соответствовать значению, заданному в параметре `rootProvider`.

3. Внутри тега `UserCatalog` добавьте тег `Or`. Внутри тега `Or` добавьте тег `Providers`. В теге `Providers` создайте блоки с параметром `Id`, в котором указывается идентификатор пользовательского контейнера, и `ignoreExceptions` со значением `true`, данный параметр игнорирует ошибку подключения к каталогу, если данный каталог не доступен.

   > **ИНФОРМАЦИЯ**
   >
   > Если теги отсутствуют, то добавьте их вручную. Полная структура файла представлена ниже.

Пример

```
"UserCatalog": {
    "RootProvider": "orUCP",
    "Providers": {
      "Ldap": [
        {
          "Id": "UserId",
          "Domain": "domain",
          "Port": 636,
          "SecureSocketLayer": true,
          "ContainerPath": "user_catalog_path",
          "UserName": "username@domain",
          "Password": "password"
        },
        {
          "Id": "UserId2",
          "Domain": "domaindomain",
          "Port": 636,
          "SecureSocketLayer": true,
          "ContainerPath": "user_catalog_path2",
          "UserName": "usernameusername@domaindomain",
          "Password": "passwordpassword"
        }
      ],
      "Or": [
        {
           "Id": "orUCP",
           "Providers": {
           "UserId": {
              "IgnoreExceptions": true
            },
            "UserId2": {
              "IgnoreExceptions": true
            }
          }
        }
      ]
    }
  }
```

4. При добавлении каждого нового каталога необходимо заново сформировать значение `StringValue` в конфигурационном файле *am/core/initial-settings.json*.

Поиск пользователей по нескольким каталогам

Чтобы оптимизировать работу с несколькими каталогами пользователей, выполните следующую опциональную настройку. Настройка позволяет быстрее выполнять поиск пользователей и взаимодействовать с доступными каталогами Active Directory в случае отказа некоторых каталогов.

Чтобы настроить поиск пользователей при работе с несколькими каталогами:

1. В конфигурационном файле *am/core/app-settings.json* перейдите в раздел `UserCatalog`.
2. В разделе `Providers`, в теге `Ldap` добавьте секцию `RegularExpression` и задайте необходимые параметры.

   После добавления секции включите настройку поиска в Management Console.

   В следующем примере проверяется, соответствуют ли атрибуты `PrincipalName` или `SamCompatibleName` домену *@indeed.demo*. Параметры и возможные значения описаны в следующей таблице.

Пример настройки

```
  "UserCatalog": {
      "RootProvider": "UserId0",
      "Providers": {
          "Ldap": [{
                  "Id": "UserId2",
                  "Domain": "rodc.indeed.demo",
                  "Port": 636,
                  "SecureSocketLayer": true,
                  "ContainerPath": "OU=Indeed_Users,DC=indeed,DC=demo",
                  "UserName": "indeed\\admin",
                  "Password": "password",
                  "RegularExpression": {
                      "Users": {
                          "Value": "^(?:([a-zA-Z0-
9._*-]+)@indeed\\.demo|indeed\\\\([a-zA-Z0-9._*-]+))$",
                          "Attributes": ["PrincipalName",
"SamCompatibleName"]
                      },
                  }
              },
```

Параметр	Описание
`RegularExpression`	Секция позволяет задавать регулярные выражения для фильтрации пользователей, групп и контейнеров.
• `Users` • `Groups` • `Containers`	В зависимости от выбранного параметра, фильтрация может производиться по пользователям (`Users`), группам (`Groups`) или контейнерам (`Containers`).

`Value`	Поле, в котором задается само регулярное выражение. Рекомендуется задать регулярное выражение, содержащее доменную часть данного каталога. Примеры регулярных выражений приведены после таблицы. Параметр применяется только к тем атрибутам, которые указаны в параметре `Attributes`. Поиск по каталогу осуществляется в следующих случаях: • если регулярное выражение совпадает с параметром поиска, • если для каталога не указано регулярное выражение, поиск по этому каталогу осуществляется без применения фильтрации.

`Attributes`	Переменная, содержащая атрибуты, которые применяются для проверки регулярных выражений.
	Эти атрибуты не относятся к полям Active Directory напрямую, а представляют собой переменные уровня приложения из класса `UserCatalog`.
	Возможные значения параметра `Attributes`:
	• `Users`:
	  ◦ `PrincipalName`
	  ◦ `SamCompatibleName`
	  ◦ `DistinguishedName`
	• `Groups` и `Containers`:
	  ◦ `Name`

Примеры настройки поиска по атрибутам

Пример поиска по PrincipalName

```
"RegularExpression": {
  "Users": {
    "Value": "^\\*?[a-zA-Z0-9._*-]*@company\\.local\\*?$", // учтены wildcard *
для корректной работы поиска в MC по UPN
    "Attributes": ["PrincipalName"]
  }
}
```

Пример поиска по SamCompatibleName

```
"RegularExpression": {
  "Users": {
    "Value": "^COMPANY\\\\([a-zA-Z0-9._*-]+)$",
    "Attributes": ["SamCompatibleName"]
  }
}
```

Пример поиска по DistinguishedName

```
"RegularExpression": {
  "Users": {
    "Value": "^CN=[\\w\\s.*-]+(?:,OU=[\\w\\s.*-]+)+,DC=company,DC=local$",
    "Attributes": ["DistinguishedName"]
  }
}
```

LDAP-фильтр при поиске пользователей и групп в службе каталогов

Если при поиске пользователей и групп нужно исключить дублирующие учетные записи или нужно обращаться только к части каталога пользователей, а не ко всему каталогу, настройте LDAP-фильтр.

Для этого:

1. На сервере с Core Server открыть файл конфигурации сервера *am/core/app-settings.json*.
2. Найти секцию *UserCatalog* и в параметре *Providers* для *Ldap* задать атрибуты *catalogFilter* и *dnFilter* для фильтрации элементов пользовательского каталога:
   - *catalogFilter* — строка LDAP-запрос для фильтрации элементов на этапе выполнения запроса к каталогу пользователей. Не поддерживает фильтрацию по частичному совпадению атрибутов distinguishedName и canonicalName (для этих целей добавлен dnFilter);
   - *dnFilter* (фильтр distinguishedName) — регулярное выражение для фильтрации результатов после выполнения LDAP-запроса к каталогу пользователей.

Дополнительная настройка при использовании FreeIPA

Если вы используете каталог FreeIPA, вы можете скрыть системные каталоги (контейнеры) при поиске пользователей в Management Console.

Для этого:

1. На сервере с Core Server открыть файл конфигурации сервера *am/core/app-settings.json*.
2. Найти секцию *UserCatalog* и в параметре *Providers* для *Ldap* задать атрибут *CatalogFilter*:
   - `“|(objectClass=person)(objectClass=ipausergroup)”` — значение, при котором в качестве объектов службы каталогов при поиске пользователей будут отображаться только пользователи и группы;
   - `“|(objectClass=person)(objectClass=ipausergroup)(entrydn=cn=users,cn=accounts,*)”` — значение, при котором добавляется корневой каталог.

Примеры использования фильтров

catalogFilter

- исключение определенных пользователей:

  ```
  &(!(name=AmUser1))(!(name=AmUser2)(!(name=AmUser3)))
  ```

- исключение всех дочерних элементов первого уровня указанной OU:

  ```
  !(msDS-parentdistname=OU=AmOrgUnit,OU=AmUserCatalog,DC=dom,DC=local)
  ```

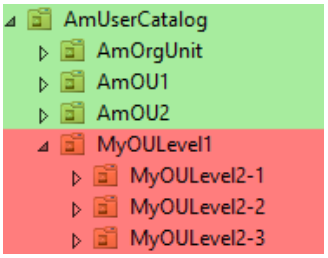
- исключение всех членов группы:

  `!(memberOf=CN=AmGroup,OU=AmUserCatalog,DC=dom,DC=local)`

dnFilter

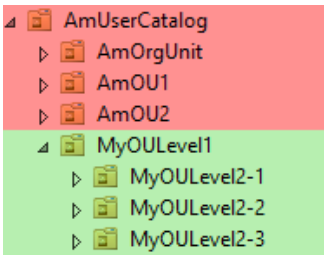
- исключение OU и всех дочерних элементов:

  `(?!^.*OU=MyOULevel1,OU=AmUserCatalog,DC=dom,DC=local$)(^.*$)`



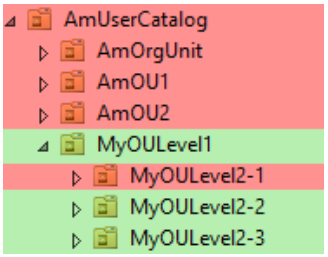
- использование только указанной OU:

  `(^.*OU=MyOULevel1,OU=AmUserCatalog,DC=dom,DC=local$)`



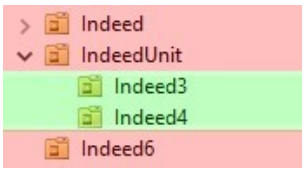
- комбинированный фильтр — использование только указанной OU без определенных дочерних элементов:

  `(?!.*OU=MyOULevel2-1,OU=MyOULevel1,OU=AmUserCatalog,DC=dom,DC=local$)`
  `(^.*OU=MyOULevel1,OU=AmUserCatalog,DC=dom,DC=local$)`



- конструкция с фильтрацией нескольких OU через оператор `|` *(или)* — любое количество условий может быть соблюдено, использование полных `distinguishedName` указанной OU:

  `((^.*OU=Indeed3,OU=IndeedUnit,DC=indeed,DC=local$)|`
  `(^.*OU=Indeed4,OU=IndeedUnit,DC=indeed,DC=local$))`


Indeed
IndeedUnit
Indeed3
Indeed4
Indeed6

Настройка времени ожидания для LDAP-соединения

Если один из LDAP-каталогов недоступен, настройте время ожидания (тайм-аут) для LDAP-соединения, чтобы предотвратить остановку работы Core Server и сделать его более стабильным:

1. Откройте файл *am/access-manager.docker-compose.yml*.
2. В блоке `core` для переменной `LDAPNETWORK_TIMEOUT` установите необходимое значение. Если LDAP-сервер не отвечает в течение указанного времени, происходит разрыв соединения.

   Примеры значений для переменной `LDAPNETWORK_TIMEOUT`:

   - 20 секунд — значение по умолчанию;
   - Более 100 секунд — при проблемах с доступом к LDAP-каталогу возможны задержки в работе;
   - 0 секунд — неограниченное время ожидания, разрыв соединения не происходит.

Настройка механизма отзыва лицензий

В Indeed Access Manager используется механизм автоматического освобождения лицензий. Этот механизм по умолчанию включен и раз в сутки (каждые 86 400 секунд) проверяет, выполнены ли условия для отзыва лицензий.

Лицензия отзывается у пользователя, если:

- пользователь удален из политики;
- пользователь отключен или перемещен из области действия политики;
- пользователь заблокирован/удален из каталога пользователей.

Если механизм отзыва лицензий отключен, то лицензии не будут освобождаться даже при выполнении этих условий.

Чтобы изменить время, после которого лицензия будет отозвана:

1. Откройте конфигурационный файл сервера *am/core/app-settings.json*.
2. В секции `Licenses` в теге `Cleanup` внесите следующие изменения:

- Для параметра `Enabled` укажите значение `true`.
- Для параметра `Interval` укажите необходимое значение. Значение по умолчанию — 1.00:00:00 (раз в день).

3. Сохраните изменения и перезапустите контейнер с приложением.

Если лицензии не отзываются автоматически, нужно перезапустить механизм отзыва лицензий. Для этого:

1. Откройте конфигурационный файл сервера *am/core/app-settings.json*.
2. В теге `Cleanup` для параметра `Enabled` установите значение `false`.
3. Сохраните изменения и перезапустите контейнер с приложением.
4. В файле *app-settings.json* в теге `Cleanup` верните значение `true` для параметра `Enabled`.
5. Повторно сохраните изменения и перезапустите контейнер с приложением.

> **ИНФОРМАЦИЯ**
>
> По результатам отзыва лицензий в журнале событий создается запись с кодом 1094. Запись о событии содержит общее число лицензий, которые были отозваны.

Настройка прав пользователей вне политики

По умолчанию пользователи, не состоящие в политиках, не могут аутентифицироваться в User Console. При необходимости снять это ограничение, добавьте следующие параметры в конфигурационный файл *am/core/app-settings.json*.

- Чтобы разрешить пользователю аутентификацию в User Console, в раздел `Behavior` добавьте следующие параметры со значением `false`:

  ```
    "Authentication": {
    "RequirePolicy": {
      "Enabled": false
    }
  },
  ```

- Чтобы разрешить пользователю самому обучать аутентификаторы, в раздел `Behavior` добавьте следующие параметры со значением `false`:

  ```
  "Enrollment": {
    "RequirePolicy": {
      "Enabled": false
    }
  },
  ```

  Параметр `RequirePolicy` в разделе `Enrollment` регулирует любое управление аутентификаторами, включая их добавление и удаление.

Настройки не распространяются:

- На привилегированные учетные записи Access Manager. Администраторы политик и глобальные администраторы могут не быть членами политик.
- Если администраторы сами обучают, изменяют и удаляют аутентификаторы пользователей, не состоящих в политиках.

Получение первичных прав администратора

Права первичного администратора по умолчанию получает пользователь `RootAdministrator` при первой аутентификации в Management Console.

Альтернативный способ выдачи первичных прав с помощью скрипта:

1. Перед настройкой первичных прав администратора выполните настройку собственного клиентского сертификата.
2. Перейдите в каталог *am/tools* и запустите скрипт *tool_set_admin.sh*.
3. Задайте необходимые параметры. Все параметры (кроме справки `-h`) являются обязательными.

   Пример

   ```
   sudo bash tool_set_admin.sh -u amadmin@test.local -n 2 -p userpassword -c
   mycert.pfx -s certpassword
   ```

Параметры:

- `-u <имя пользователя>`
- `-n <формат имени пользователя>`

  Возможные значения:

  - 2 - PrincipalName
  - 3 - SamCompatibleName
  - 4 - DistinguishedName
  - 5 - Sid
- `-p <пароль пользователя>`
- `-c <имя/путь client.pfx>` — собственный клиентский сертификат, созданный на этапе подготовки сертификатов.
- `-s <пароль client.pfx>` — пароль от собственного клиентского сертификата.
- `-h` — вызов справки.

При успешном выполнении скрипта пользователь будет добавлен как первичный администратор. После использования скрипт можно удалить.

ПОДСКАЗКА

В качестве пользователя в скрипте укажите того же пользователя, которого вы указываете в параметре `RootAdministrator` конфигурационного файла Core Server *app-settings.json*.

Indeed Management Console

Indeed Management Console (Management Console) — это веб-приложение, работающее на базе HTTP-сервера Kestrel. В Management Console осуществляется администрирование системы, через которую производятся все настройки системы и пользователей.

> **КАК ОТКРЫТЬ MANAGEMENT CONSOLE**
>
> *http(s)://<dns_имя_сервера>/am/mc*

Установка Management Console

Системные требования

Отдельно устанавливать Management Console не нужно. Компонент устанавливается автоматически при распаковке архива *am_images/mc.tar.gz* или, если в вашей версии AM нет каталога *am_images*, при распаковке *am-<номер версии>.tar.gz*.

Редактирование конфигурационного файла Management Console

> **ИНФОРМАЦИЯ**
>
> Настройки, описанные в данном разделе, не являются обязательными. Конфигурационный файл *am/mc/app-settings.json* можно изменить в любой момент.

Настройка срока жизни сессии

Чтобы изменить срок жизни сессии в Management Console, выполните следующее:

1. Откройте конфигурационный файл *am/mc/app-settings.json*.
2. Для параметра `SessionExpiration` установите необходимое значение. Если параметр не задан, используется значение по умолчанию — 30 минут ("00:30:00").

Пример

```
"Authentication": {
    "Mode": "Saml",
    "SessionExpiration": "00:30:00",
    "EnableLogout": true
},
```

3. Сохраните изменения в файле и запустите контейнер с приложением с помощью команды `sudo docker-compose up -d`.

Игнорирование ошибок сертификата

1. Откройте конфигурационный файл консоли *am/mc/app-settings.json*.
2. Измените параметр `isIgnoreCertErrors` на значение *true* в файле *am/mc/app-settings.json*.
3. Сохраните изменения в файле и запустите контейнер с приложением с помощью команды `sudo docker-compose up -d`.

Настройка поиска по пользователям

Чтобы настроить поиск пользователей в Management Console, откройте файл *am/mc/app-settings.json* и в объекте `UserSearch` задайте следующие параметры:

- `FindUsersMaxResultCount` — параметр устанавливает максимальное количество результатов поиска на странице. Значение по умолчанию `200`.
- `SearchTemplate` (обязательный параметр) — в параметре задается шаблон поиска. Примеры допустимых шаблонов (в виде строки): `*{0}, {0}*, *{0}*, {0}`. Значение по умолчанию `""` (пустая строка), что соответствует шаблону `*{0}*`.

  Для корректной работы поиска пользователей, установите хотя бы один из следующих параметров в значение `true`:

- `SearchByGivenName` — поиск по имени. Значение по умолчанию `true`.
- `SearchBySn` — поиск по фамилии. Значение по умолчанию `true`.
- `SearchByUpn` — поиск по логину. Значение по умолчанию `true`.
- `SearchByGivenNameAndSn` — поиск по имени+фамилии и фамилии+имени. Значение по умолчанию `true`.

- `SearchByName` — поиск по имени, которое отображается в списке каталога пользователей. Значение по умолчанию `true`.
- `SearchByEmail` — поиск по адресу электронной почты. Значение по умолчанию `true`.
- `SearchByUpnStrictMatchPriority` — поиск по User Principal Name (UPN) в соответствии с регулярными выражениями из секции `RegularExpression` файла *am/core/app-settings.json*.

  Если UPN совпадает с регулярным выражением каталога, поиск выполняется только в этом каталоге. Если совпадений не найдено, поиск выполняется как при выключенной настройке.

  Значение по умолчанию `false`.

После настройки критерии поиска отображаются в Management Console на странице Пользователи в поле ввода поискового запроса.

Проверка состояния сервера

Для проверки рабочего состояния контейнера в Docker используйте метод Healthcheck:

http(s)://<dns_имя_сервера>/am/mc/healthcheck/isHealthy

На странице отображается следующая информация о состоянии компонента:

- статус компонента Management Console, время обработки запроса к нему;
- статус последнего запроса;
- статус компонента Indeed Log Server;
- список ошибок при наличии.

Пример результата проверки


```
{
  "Status": "Healthy",
  "Entries": {
    "CoreServer": {
      "PreviousCheckSucceeded": true,
      "CheckState": "Succeeded",
      "CheckStartDate": "2025-03-04T08:59:00.9465204+00:00",
      "CheckDuration": "00:00:00.0214301"
    },
    "LogServer": {
      "PreviousCheckSucceeded": true,
      "CheckState": "Succeeded",
      "CheckStartDate": "2025-03-04T08:59:00.9389229+00:00",
      "CheckDuration": "00:00:00.0169765"
    }
  }
}
```


Если Log Server не работает, то в параметре `Status` и в параметре `CheckState` для `LogServer` отображается значение `Degraded` (ухудшенное состояние). При этом запрос выполнен успешно (HTTP-код 200). При запуске команды `docker ps` возвращается статус состояния сервера `Healthy`.

Неработающий Log Server не влияет на работоспособность Management Console с некоторыми ограничениями — не доступно логирование в Log Server и просмотр страниц/частей страниц, которые связаны с отображением данных с Log Server.

Сбор логов

Информация по включению логирования и сбору логов компонента Management Console находится в разделе Сбор логов серверных компонентов.

Indeed User Console

Indeed User Console (User Console) — это веб-приложение, работающее на базе HTTP-сервера Kestrel. В User Console пользователь может управлять своими аутентификаторами.

> **КАК ОТКРЫТЬ USER CONSOLE**
>
> *http(s):///<dns_имя_сервера>/am/uc*

Установка User Console

Системные требования

Отдельно устанавливать User Console не нужно. Компонент устанавливается автоматически при распаковке архива *am_images/uc.tar.gz* или, если в вашей версии AM нет каталога *am_images*, при распаковке *am-<номер версии>.tar.gz*.

Редактирование конфигурационного файла User Console

> **ИНФОРМАЦИЯ**
>
> Настройки, описанные в данном разделе, не являются обязательными. Конфигурационный файл *am/uc/app-settings.json* можно изменить в любой момент.

Настройка срока жизни сессии

Чтобы изменить срок жизни сессии в User Console, выполните следующее:

1. Откройте конфигурационный файл *am/uc/app-settings.json*.
2. Для параметра `SessionExpiration` установите необходимое значение. Если параметр не задан, используется значение по умолчанию — 30 минут ("00:30:00").

Пример

```
"Authentication": {
    "Mode": "Saml",
    "SessionExpiration": "00:30:00",
    "EnableLogout": true
},
```

3. Сохраните изменения в файле и запустите контейнер с приложением с помощью команды `sudo docker-compose up -d.`

Включение защиты от перебора

В Indeed Access Manager вы можете настроить защиту от подбора учетных записей для компонента User Console.

Если эта настройка включена, то при вводе несуществующего имени пользователя Indeed Access Manager имитирует вход существующего пользователя: отображает способы аутентификации, запрашивает пароль, а затем отображает ошибку *Неверное имя пользователя или аутентификатор или заблокировано устройство*.

Если эта настройка выключена, то при вводе несуществующего имени пользователя Indeed Access Manager отображает ошибку *Внутренняя ошибка сервера: Пользователь не найден*.

По умолчанию данная настройка отключена.

Чтобы включить защиту от перебора:

1. Откройте конфигурационный файл сервера Core Server *am/core/app-settings.json*.
2. В блоке `Authentication` в строке `bruteForceProtection` укажите значения *Self Service* и *Identity Provider*.

   Пример

   ```
   "Authentication": {
       "BruteForceProtection": {
           "Applications": ["Self Service", "Identity Provider"]
       }
   }
   ```

3. Сохраните изменения и запустите контейнер с приложением с помощью команды `sudo docker-compose up -d`.

Отключение смены локализации

Чтобы запретить пользователю менять язык в User Console:

1. Откройте конфигурационный файл консоли *am/uc/app-settings.json*.
2. В параметре `Localization` в теге `CanCustomChange` укажите значение `false`.

Пример

```
"Localization": {
    "DefaultCulture": "ru-RU",
    "CanCustomChange": true
},
```

3. Сохраните изменения в файле и запустите контейнер с приложением с помощью команды `sudo docker-compose up -d`.

Пример входа в User Console с использованием Identity Provider

1. Откройте в браузере интерфейс User Console. Пример адреса консоли: *http(s)://полное_dns_имя_сервера/am/uc*.

2. В появившемся окне аутентификации нажмите Back для выбора способа аутентификации. По умолчанию используется последний используемый способ.

3. Выберите способ аутентификации и нажмите Select.

> **ИНФОРМАЦИЯ**
>
> Если у пользователя нет обученного аутентификатора, выберите *Windows Password*.

> **ПРИМЕЧАНИЕ**
>
> Выход в сессии пользователя из Identity Provider не влечет за собой выход пользователя из User Console, до перезапуска браузера или истечения срока хранения cookie. Время хранения cookie для Identity Provider — 30 минут.

4. Введите пароль и нажмите Sing in. Если ввод данных был успешный, то отобразится карточка пользователя.

5. Для выхода из User Console выполните следующее:

   - Нажмите имя пользователя в верхней части окна.
   - Выберите Выйти из выпадающего списка.

   > **ИНФОРМАЦИЯ**
   >
   > При выходе из User Console происходит автоматический выход из Identity Provider.

Проверка состояния сервера

Для проверки рабочего состояния контейнера в Docker используйте метод Healthcheck:

http(s)://<dns_имя_сервера>/am/uc/healthcheck/isHealthy

На странице отображается следующая информация о состоянии компонента:

- статус компонента User Console, время обработки запроса к нему;
- статус последнего запроса;
- список ошибок при наличии.

Пример результата проверки


```
{
  "Status": "Healthy",
  "Entries": {
    "CoreServer": {
      "PreviousCheckSucceeded": true,
      "CheckState": "Succeeded",
      "CheckStartDate": "2025-03-04T08:58:00.9648416+00:00",
      "CheckDuration": "00:00:00.0161041"
    }
  }
}
```


Сбор логов

Информация по включению логирования и сбору логов компонента User Console находится в разделе Сбор логов серверных компонентов.

Indeed Key Server

Indeed Key Server (Key Server) — это сервер, необходимый для реализации аутентификации пользователей через Indeed Key Provider. С помощью Key Server отправляются push-уведомления и одноразовые пароли из мобильного приложения Indeed Key.

Core Server устанавливает связь с Key Server по URL-адресу, а Key Server — с мобильным приложением Indeed Key по протоколу HTTPS.

Для записи событий сервера необходима отдельная база данных Microsoft SQL или PostgreSQL.

Создание базы данных и сервисной учетной записи

Key Server поддерживает работу с базами PostgreSQL и Microsoft SQL.

Подробнее о создании базы данных и сервисной учетной записи — в разделе Хранилище данных.

> **ПРИМЕЧАНИЕ**
>
> После создания базы данных (после первого запроса) можно понизить привилегии для пользователя. Достаточно права *db_owner* для созданной базы данных.

Установка и настройка

Системные требования

Чтобы установить Key Server на отдельном сервере с операционной системой Linux:

1. Импортируйте образ Docker.
2. Сгенерируйте служебные сертификаты.
3. Внесите изменения в конфигурационные файлы.
4. Выполните настройку прав пользователя.
5. Запустите контейнер с приложением Key Server.

Импорт образа Docker

1. Скачайте архив компонента *am_images/indeed-key-server.tar.gz* и загрузите его на целевой хост в необходимый каталог.

   Если компонент устанавливается на отдельном хосте, вместе с архивом компонента скопируйте и импортируйте архивы *haproxy.tar.gz* и *tools.tar.gz*.

> **ПРИМЕЧАНИЕ**
>
> Если в вашей версии АМ нет каталога *am_images*, для установки используйте общий архив *am-<номер_версии>.tar.gz*.

2. Перейдите в каталог с архивом и распакуйте его:

```
sudo tar -xf indeed-key-server.tar.gz
```

3. Перейдите в каталог, в который распаковался архив, и импортируйте образ Docker:

```
sudo docker load -i indeed-key-server.tar
```

4. Ограничьте права запуска для всех пользователей системы, не имеющих прав `sudo`. Для этого, находясь в каталоге *ssl*, выполните `sudo chmod 400 *.sh`.

5. Чтобы сгенерировать архив для ручной установки, перейдите в мастер конфигурации и выполните сценарий Ручная установка.

Генерация служебных сертификатов

Добавьте следующие сертификаты в каталог *ssl/*:

- *ssl/<серверный сертификат>.pfx* — сертификат веб-сервера, выписанный доменным удостоверяющим центром (УЦ) на внутреннее DNS-имя машины, на которой будет установлен Key Server.
- *ssl/ca/<публичный сертификат>.cer* — публичный сертификат в формате Base64 вашего доменного УЦ.
- *ssl/<сертификат стороннего УЦ>.pfx* — глобальный сертификат веб-сервера, выписанный сторонним УЦ на внешнее DNS-имя машины, на которой будет установлен Key Server.
- *ssl/ca/<сертификат стороннего УЦ>.cer* — публичный сертификат домена в формате Base64 стороннего УЦ.

> **ПРИМЕЧАНИЕ**
>
> Требования к сертификату стороннего удостоверяющего центра смотрите в разделе Системные требования.

Перед запуском скриптов ограничьте права запуска для всех пользователей системы, не имеющих прав `sudo`. Для этого, находясь в каталоге *ssl*, выполните команду `sudo chmod 400 *.sh`.

1. Запустите скрипт *convertPfxForReverseProxy.sh* с использованием сертификата *<серверный сертификат>.pfx*, выписанного на DNS-имя текущего хоста:

```
sudo bash ./convertPfxForReverseProxy.sh -f <серверный сертификат>.pfx -p <пароль>
```

2. Запустите скрипт *convertPfxForReverseProxy_ik_external.sh* с использованием сертификата *<сертификат стороннего УЦ>.pfx*:

   `sudo bash ./convertPfxForReverseProxy_ik_external.sh -f <сертификат стороннего УЦ>.pfx -p <пароль>`

   Результат: создается серверный сертификат *am/ssl/https/reverse_proxy_server_ik.pem*, предоставляющий HAProxy для внешних клиентов к Key Server.

3. Сгенерируйте HTTPS-сертификаты контейнеров, используемые внутри сети Docker.

   ```
   sudo bash ./generateHttpsCerts.sh
   ```

   Результат: создаются сертификаты *am/ssl/https/<service>.pfx* для сервисов Core, MC, UC, IDP, Log Server и Indeed Key. Расположение и пароли сертификатов указаны в конфигурационных файлах компонентов.

4. Сгенерируйте служебный сертификат, который используются при SAML-соединении

   ```
   sudo bash ./generateSamlCerts.sh
   ```

5. Сгенерируйте сертификат, которому будут доверять контейнеры.

   `sudo bash ./prepareCaFile.sh`

Редактирование конфигурационных файлов

Редактирование файла am/.env

1. `COMPOSE_PROFILES` — добавьте значение `indeed-key-server` и удалите значения компонентов, которые установлены на других машинах.
2. `ENDPOINT_NAME_THIS_HOST` — DNS-имя машины, на которой вы устанавливаете Key Server.
3. `INDEED_KEY_EXTERNAL_ENDPOINT_NAME` — внешний адрес для подключения мобильного приложения к Key Server.
4. `INDEED_KEY_HTTPS_PORT` и `INDEED_KEY_HTTPS_PORT_EXTERNAL` — внутренний и внешний порты.

Редактирование конфигурационного файла am/haproxy.docker-compose.yml

1. В блоке `depends_on` раскомментируйте строку `indeed-key` и закомментируйте строки с остальными компонентами, установленными на других машинах.

Пример

```
 depends_on:
# - core
# - idp
# - mc
# - uc
# - ls
- indeed-key # Uncomment if you need an Indeed Key server
```

2. В блоке `ports` раскомментируйте строки с указанием портов:

```
"${INDEED_KEY_HTTPS_PORT}:7443"
"${INDEED_KEY_HTTPS_PORT_EXTERNAL}:8443"
```

Редактирование конфигурационного файла am/haproxy/haproxy.cfg

1. Раскомментируйте строку `default_backend IK_Backend`.
2. Раскомментируйте следующие строки с параметром `backend IK_Backend`.

```
backend IK_Backend
    server docker indeed-key:5443 check inter 5000ms ssl verify required ca-file
trusted_ca.crt
```

3. Закомментируйте строки, связанные с компонентами, которые установлены на других машинах.
   - Строки с параметром `acl`, в которых упоминаются компоненты. Пример: `acl path-mc path_beg -i /am/mc`.
   - В параметре `http-request reject unless` удалите компоненты, которые установлены на других машинах, и лишние разделители `||`.
   - Строки с параметром `use_backend`. Пример: `use_backend MC_Backend if path-mc`.
   - Строки с адресом компонента в параметре `backend <серверный_компонент>_Backend`.

Редактирование конфигурационного файла am/indeed-key/app-settings.json

1. В разделе `Storage` в параметре `ConnectionString` укажите строку подключения к базе данных.

Пример для Microsoft SQL

```
"Storage": {
  "Provider": {
    "Type": "Mssql",
    "ConnectionString": "Data Source=[Db host address];Initial Catalog=[AM
Db];User ID=[Db service account];Password=[Db service
password];TrustServerCertificate=True;"
  },
```

Пример для PostgreSQL

```
"Storage": {
  "Provider": {
    "Type": "PostgreSql",
    "ConnectionString": "server=192.168.80.30;port=5432;user
id=amservice;password=Q1w2e3r4;database=IndeedKey"
  },
```

2. В разделе `Server` в параметре `Url` укажите URL-адрес для подключения к Key Server.

Пример

```
  "Server": {
    "Url": "http(s)://[Server address]:{port}",
    "Logon": {
      "Delay": "00:05:00"
    },
```

Где:

- `[Server address]` — значение переменной `INDEED_KEY_EXTERNAL_ENDPOINT_NAME`, заданное в файле *am/.env*.
- `{port}` — значение переменной `INDEED_KEY_HTTPS_PORT_EXTERNAL`, заданное в файле *am/.env*.

> **ПРИМЕЧАНИЕ**
>
> URL-адрес Key Server должен быть доступен с мобильного телефона.

3. В параметре `TrustedClients` укажите произвольный уникальный идентификатор. Это же значение нужно указать в настройке Доверенный ID Indeed Key Server в Management Console.

> **ПОДСКАЗКА**
>
> На этом этапе рекомендуем перейти в Management Console в раздел Конфигурация→Аутентификаторы→Indeed Key→Серверные настройки и, помимо настройки доверенного ID Indeed Key Server, задать внутренний URL-адрес Indeed Key Server.
>
> Также в разделе Настройки регистрации при выборе способа регистрации по email заполните обязательные поля и сохраните изменения.

Настройка прав

Выдайте права пользователю, которого вы указали в файле *.env* в переменных `AM_UID` и `AM_GID`, запустив следующую команду:

```
sudo chown -R <AM_UID>:<AM_GID> ./*
```

Запуск Key Server

Запустите контейнер с приложением с помощью команды `sudo docker-compose up -d`.

Настройка событий сервера

Установка и настройка осуществляется на Log Server.

В качестве хранилища можно использовать все способы хранения, которые поддерживает Log Server.

Отслеживать события можно следующими способами:

- При хранении в базе данных — сторонними средствами мониторинга или с помощью SQL-запросов.
- При использовании Syslog — сторонними средствами мониторинга с поддержкой Syslog.

> **ВАЖНО!**
>
> В текущей версии Indeed AM просмотр событий Key Server с помощью Management Console не поддерживается.

Чтобы настроить события Key Server

Microsoft SQL

1. Откройте конфигурационный файл *am/ls/clientApps.config* и расскоментируйте строку:

```
<Target Id="DbTargetMssqlIndeedKey" Type="mssql" />
```

Где `"DbTargetMssqlIndeedKey"` — это название конфигурационного файла в папке *am/ls/targets*.

2. Раскомментируйте блок `<Application Id="akc" SchemaId="akcSchema">`.

Пример

```
<Application Id="akc" SchemaId="akcSchema">
    <ReadTargetId>DbTargetMssqlIndeedKey</ReadTargetId>
    <WriteTargets>
        <TargetId>DbTargetMssqlIndeedKey</TargetId>
    </WriteTargets>
    <AccessControl>
        <CertificateAccessControl
CertificateThumbprint="01de449b6f4b49e00d1a5b20ffb5d6605cf6cd2a"
Rights="Write" />
    </AccessControl>
</Application>
```

- В тегах `ReadTargetId` указывается идентификатор хранилища, откуда будет осуществляться чтение событий.
- В блоке `WriteTargets`, в тегах `TargetId`, указывается идентификатор хранилища, куда будет осуществляться запись событий.
- Идентификаторы заданы в теге `Targets`, конфигурационные файлы для каждого типа находятся в папке *am/ls/targets/* с соответствующим именем.
- При использовании собственного клиентского сертификата в `CertificateThumbprint` указывается отпечаток клиентского сертификата Core Server.

3. При необходимости использовать дополнительное хранилище данных, укажите его в секции `Targets`:

Пример

```
<Targets>
  ...
  <Target Id="mssqlTargetAM" Type="mssql"/>
</Targets>
```

4. Перейдите в каталог *am/ls/targets* и откройте конфигурационный файл *DbTargetMssqlIndeedKey.config*.

В строке `ConnectionString` укажите следующие данные:

- `Data Source` — DNS/IP-адрес сервера с базой данных.
- `Initial Catalog` — имя базы данных.
- `User ID` — имя пользователя, который имеет полные права для базы данных Database.
- `Password` — пароль пользователя.

Пример

```
<?xml version="1.0" encoding="utf-8"?>
<Settings>
  <ConnectionString>Data Source=[Db host address];Initial Catalog=[AM
Db];User ID=[Db service account];Password=[Db service
password];TrustServerCertificate=True</ConnectionString>
</Settings>
```

⚠ **ВАЖНО!**

Для событий Key Server необходимо использовать отдельную базу данных.

PostgreSQL

1. Откройте конфигурационный файл *am/ls/clientApps.config* и расскоментируйте строку:

```
<Target Id="DbTargetSqlIndeedKey" Type="pgsql" />
```

Где `"DbTargetSqlIndeedKey"` — это название конфигурационного файла в папке *am/ls/targets*.

2. Раскомментируйте блок `<Application Id="akc" SchemaId="akcSchema">`.

Пример

```
<Application Id="akc" SchemaId="akcSchema">
    <ReadTargetId>DbTargetSqlIndeedKey</ReadTargetId>
    <WriteTargets>
        <TargetId>DbTargetSqlIndeedKey</TargetId>
    </WriteTargets>
    <AccessControl>
        <CertificateAccessControl
CertificateThumbprint="01de449b6f4b49e00d1a5b20ffb5d6605cf6cd2a"
Rights="Write" />
    </AccessControl>
</Application>
```

- В тегах `ReadTargetId` указывается идентификатор хранилища, откуда будет осуществляться чтение событий.
- В блоке `WriteTargets`, в тегах `TargetId`, указывается идентификатор хранилища, куда будет осуществляться запись событий.
- Идентификаторы заданы в теге `Targets`, конфигурационные файлы для каждого типа находятся в папке *am/ls/targets/* с соответствующим именем.
- При использовании собственного клиентского сертификата в `CertificateThumbprint` указывается отпечаток клиентского сертификата Core Server.

3. При необходимости использовать дополнительное хранилище данных, укажите его в секции `Targets`:

Пример

```
<Targets>
  ...
  <Target Id="sqlTargetAM" Type="pgsql"/>
</Targets>
```

4. Перейдите в каталог *am/ls/targets* и откройте конфигурационный файл *DbTargetSqlIndeedKey.config*.

В строке `ConnectionString` укажите следующие данные:

- `Server` — DNS/IP-адрес сервера с базой данных.

- `Database` — имя базы данных.
- `Port` — порт подключения.
- `User ID` — имя пользователя, который имеет полные права для базы данных Database.
- `Password` — пароль пользователя.

Пример

```
<?xml version="1.0" encoding="utf-8"?>
<Settings>
  <ConnectionString>server=[database host address];port=5432;user id=
[database service account];password=[database service password];database=
[log server]</ConnectionString>
</Settings>
```

⚠ **ВАЖНО!**

Для событий Key Server необходимо использовать отдельную базу данных.

Сервис очистки старых данных

В файле *am/indeed-key/app-settings.json* можно задать параметры сервиса очистки старых данных.

Пример

```
"CleanAkData": {
    "Enabled": true,
    "FirstRunTime": "00:00",
    "Interval": "1.00:00:00",
    "AkDataLifeTime": "1.00:00:00"
  }
```

Описание атрибутов примера

Имя атрибута	Описание	Значение	Значение по умолчанию	Минимально допустимое значение
`Enabled`	Флаг включения сервиса	`true`, `false`	`true`	Отсутствует
`FirstRunTime`	Время первого запуска сервиса	Строка в формате времени `hh:mm` (ЧЧ:ММ)	`00:00` (полночь)	Отсутствует
`Interval`	Интервал запуска сервиса	Временной интервал	`1.00:00:00` (ДД:ЧЧ:ММ:СС)	`00:10:00` (10 минут)
`AkDataLifeTime`	Время жизни данных	Временной интервал	`1.00:00:00` (ДД:ЧЧ:ММ:СС)	`00:10:00` (10 минут)

Включить/Отключить шифрование конфигурационного файла

1. В терминале перейдите в каталог с утилитой для шифрования *am/protection*.

   ```
   cd /am/protection
   ```

2. Выдайте права для запуска скрипта `protector.sh`.

   ```
   sudo chmod 500 protector.sh
   ```

3. Чтобы зашифровать конфигурационные файлы, запустите скрипт `protector.sh` с параметром `protect`.

   ```
   sudo bash ./protector.sh protect
   ```

4. Чтобы расшифровать конфигурационные файлы, запустите скрипт `protector.sh` с параметром `unprotect`.

   ```
   sudo bash ./protector.sh unprotect
   ```

Проверка состояния сервера

Для проверки рабочего состояния контейнера в Docker используйте метод Healthcheck:

http(s)://<dns_имя_сервера>:<порт>/healthcheck/isHealthy

На странице отображается следующая информация о состоянии компонента:

- статус компонента Key Server, время обработки запроса к нему;
- статус последнего запроса;
- список ошибок при наличии.

Пример результата проверки


```
{
  "Entries": {
    "Storage": {
      "Data": {
        "HealthCheckStatus": {
          "PreviousCheckSucceeded": true,
          "CheckState": "Succeeded",
          "CheckStartDate": "2025-03-17T11:07:55.9606294+00:00",
          "CheckDuration": "00:00:00.0014040"
        }
      },
      "Description": null,
      "Duration": "00:00:00.0000052",
      "Exception": null,
      "Status": 2,
      "Tags": []
    }
  },
  "Status": 2,
  "TotalDuration": "00:00:00.0003921"
}
```


Сбор логов

Информация по включению логирования и сбору логов компонента Key Server находится в разделе Сбор логов серверных компонентов.

Установка Access Manager на нескольких хостах

> **ИНФОРМАЦИЯ**
>
> Прежде чем перейти к установке Access Manager на нескольких хостах, рекомендуется сначала установить и настроить Access Manager на одном хосте.

1. После успешной установки на одном хосте создайте архивную копию каталога с установленным Access Manager и переместите архив на все хосты, где планируется установка компонентов продукта.
2. Распакуйте архив и на каждом хосте внесите все изменения, описанные далее.
3. Перед запуском скриптов ограничьте права запуска для всех пользователей системы, не имеющих прав `sudo`. Для этого, находясь в каталоге *ssl*, выполните команду `sudo chmod 400 *.sh`.
4. Выполните запуск скриптов *convertPfxForReverseProxy.sh* и *prepareCaFile.sh* с использованием сертификата *<серверный сертификат>.pfx*, выписанного на DNS-имя текущего хоста:
   - ```
     sudo bash ./convertPfxForReverseProxy.sh -f <серверный сертификат>.pfx -p <пароль>
     ```
   - (Опционально) При установке Indeed Key Server выполните запуск следующего скрипта:

     ```
     sudo bash ./convertPfxForReverseProxy_ik_external.sh -f <серверный сертификат>.pfx -p <пароль>
     ```

     В результате запуска создается серверный сертификат *am/ssl/https/reverse_proxy_server_ik.pem*, предоставляющий HAProxy для внешних клиентов к Indeed Key Server.
   - Перезапустите скрипт:

     ```
     sudo bash ./prepareCaFile.sh
     ```
5. Откройте файл *am/.env* и внесите следующие изменения в переменные окружения:
   - В переменной `COMPOSE_PROFILES` укажите провайдеры аутентификации, которые вы планируете установить на текущем хосте. Список обозначений для провайдеров смотрите в таблице Переменные окружения.
     ```

> ⚠ **ВАЖНО**
>
> Установка провайдеров возможна только на одном хосте с серверным компонентом Core Server.

- Измените значение переменной `ENDPOINT_NAME_THIS_HOST`. При установке Access Manager на нескольких хостах компонент HAProxy устанавливается на каждом хосте, поэтому в переменной `ENDPOINT_NAME_THIS_HOST` необходимо указать DNS-имя текущего хоста.
- На каждом используемом хосте измените значения всех переменных `ENDPOINT_NAME_<компонент>` в зависимости от того, на каких хостах установлены компоненты.
- (Опционально) При установке Indeed Key Server задайте значения переменных на каждом используемом хосте:
  - `INDEED_KEY_EXTERNAL_ENDPOINT_NAME` — внешний адрес, по которому будет доступно приложение Indeed Key;
  - `INDEED_KEY_HTTPS_PORT` — внутренний порт;
  - `INDEED_KEY_HTTPS_PORT_EXTERNAL` — внешний порт.

6. (Опционально) При установке Indeed Key Server откройте конфигурационный файл *am/indeed-key/app-settings.json* на хосте с Key Server и задайте параметры:
   - `ConnectionString` — строка подключения к базе данных;
   - `Url` — внешний адрес Key Server;
   - `TrustedClients` — произвольный уникальный идентификатор. Этот идентификатор необходим для подтверждения удаления аутентификатора Indeed Key. Значение идентификатора должно совпадать со значением, указанным в серверных настройках аутентификатора Indeed Key в Management Console.
7. Внесите изменения в файл *am/haproxy.docker-compose.yml*. Необходимо удалить или закомментировать зависимость от сервисов, которые не будут установлены на текущем хосте.

Пример

```
depends_on:
 - core
 - idp
#- mc
#- uc
 - ls
#- indeed-key # Remove if Indeed Key server not needed
```

8. Внесите изменения в конфигурационный файл *am/haproxy/haproxy.cfg*.

Удалите или закомментируйте строки с параметрами, относящимися к серверным компонентам, которые вы не планируете устанавливать на текущем хосте:

- Строки с параметром `acl`, в которых упоминаются серверные компоненты.

```
acl path-ls         path_beg -i /ls
acl path-idp        path_beg -i /am/idp
acl path-mc         path_beg -i /am/mc
acl path-uc         path_beg -i /am/uc
acl path-core       path_beg -i /am/core
acl path-sms-proxy  path_beg -i /am/proxies/sms
```

- В параметре `http-request reject unless` удалите не используемые на данном хосте компоненты и лишние разделители `||`.

```
http-request reject unless path-core || path-idp || path-mc || path-uc ||
path-ls || path-sms-proxy
```

- Строки с параметром `use_backend`.

```
use_backend LS_Backend         if path-ls
use_backend IDP_Backend        if path-idp
use_backend MC_Backend         if path-mc
use_backend UC_Backend         if path-uc
use_backend CORE_Backend       if path-core
use_backend Sms_Proxy_Backend  if path-sms-proxy
```

- Строки с адресами компонентов в параметре `backend <серверный_компонент>_Backend`.

```
backend CORE_Backend
 server docker core:5443 check inter 5000ms ssl verify required ca-file
trusted_ca.crt

backend MC_Backend
 server docker mc:5443 check inter 5000ms ssl verify required ca-file
trusted_ca.crt

backend UC_Backend
 server docker uc:5443 check inter 5000ms ssl verify required ca-file
trusted_ca.crt

backend IDP_Backend
 server docker idp:5443 check inter 5000ms ssl verify required ca-file
trusted_ca.crt
```

9. Выполните настройку прав пользователя.

10. Для создания и запуска контейнера с серверными компонентами, выполните следующую команду:

```
sudo docker-compose up -d
```

Опциональные настройки безопасности

В некоторых сценариях можно ограничить доступ к любому серверному компоненту Access Manager, оставив только доступ в пределах Docker-сети. Для этого удалите соответствующие строки в конфигурационном файле *am/haproxy/haproxy.cfg* (шаг 8).

В таком случае этот компонент должен быть доступен в пределах Docker-сети для остальных компонентов, которые требуют соединения. При таком сценарии в переменных `ENDPOINT_NAME_<компонент>` следует задать имя контейнера с указанием порта 5443.

Пример

```
ENDPOINT_NAME_CORE=core:5443
ENDPOINT_NAME_LS=ls:5443
```

Расположение конфигурационных файлов

После установки Access Manager конфигурационные файлы компонентов создаются автоматически. По умолчанию они хранятся в директории *C:\inetpub\wwwroot*.

В таблице ниже представлены полные пути к конфигурационным файлам.

Компонент	Конфигурационный файл
Основной конфигурационный файл Log Server	*am/ls/clientApps.config*
Core Server	*am/core/app-settings.json*
Management Console	*am/mc/app-settings.json*
User Console	*am/uc/app-settings.json*
Key Server (Indeed Key)	*am/indeed-key/app-settings.json*
Identity Provider (IDP)	*am/idp/app-settings.json*
Хранение событий AM в Microsoft SQL	*am/ls/targets/DbTargetMssqlAM.config*
Хранение событий Indeed Key в Microsoft SQL	*am/ls/targets/DbTargetMssqlIndeedKey.config*
Хранение событий AM в PostgreSQL	*am/ls/targets/DbTargetSqlAM.config*
Хранение событий Indeed Key в PostgreSQL	*am/ls/targets/DbTargetSqlIndeedKey.config*
Хранение событий в SysLog	*am/ls/targets/TargetSyslog.config*

Установка и настройка модулей интеграции

Indeed Identity Provider

Количество глав: 4

Indeed ADFS Extension

Количество глав: 2

Indeed FreeRADIUS Extension

Количество глав: 3

Indeed LDAP Proxy

Двухфакторная аутентификация по протоколу LDAP Proxy

Indeed RDP Windows Logon

Количество глав: 3

Indeed Linux Logon

Доступ в Linux с помощью строгой аутентификации

Indeed Windows Logon

Количество глав: 5

Утилита управления аутентификаторами

Количество глав: 4

Indeed Identity Provider

Модуль Indeed Identity Provider (ранее Indeed AM SAML IDP) используется для организации многофакторной аутентификации и сквозного доступа в веб-приложения.

Модуль Indeed Identity Provider поддерживает следующие протоколы:

- OpenID Connect и OAuth 2.0
- SAML

Identity Provider избавляет пользователя от необходимости запоминать множество учетных данных: для доступа во все интегрированные системы требуется только один комплект учетных данных. Аутентификация выполняется централизованно на стороне Identity Provider.

В Identity Provider вы можете выполнить аутентификацию по следующим аутентификаторам:

- мобильное приложение Indeed Key (в режиме отправки одноразовых паролей и push-уведомлений с подтверждением входа)
- Telegram (в режиме отправки одноразовых паролей и push-уведомлений с подтверждением входа)
- Email OTP
- SMS OTP
- Storage SMS OTP
- Secured TOTP
- Software OTP
- Windows Password
- Passcode
- Hardware TOTP
- Hardware OTP

Установка Identity Provider

Отдельно устанавливать Identity Provider не нужно. Компонент устанавливается автоматически при распаковке архива *am_images/idp.tar.gz* или, если в вашей версии AM нет каталога *am_images*, при распаковке *am-<номер версии>.tar.gz*.

Переменные окружения

Переменные окружения находятся в файле *am/.env* и доступны пользователю с заданными по умолчанию значениями. При настройке Identity Provider необходимо отредактировать значение для переменной `CUSTOM_SP_*`.

В ней задается адрес приложения (DNS-имя и порт, если явно указан), которое попадает в политику безопасности для доступа к IDP (белый список).

Примеры:

- Если при подключении к приложению используется адрес `https://provider.test.local:333/..`, то значение переменной будет `provider.test.local:333`.
- `*.test.local`.

Если такие приложения отсутствуют, оставьте переменные с пустыми значениями.

При необходимости добавить более пяти сервисных провайдеров:

1. Добавьте дополнительные переменные в файл *.env* по аналогии с уже добавленными по умолчанию (`CUSTOM_SP_6=`, `CUSTOM_SP_7=`).
2. Добавьте переменные в файл *access-manager.docker-compose.yml* в раздел `idp:environment`.

   Пример

   ```
   idp:
    environment:
   ...
   AMIDP_ContentSecurityPolicy__FormAction__From__7: "${CUSTOM_SP_6}"
   AMIDP_ContentSecurityPolicy__FormAction__From__8: "${CUSTOM_SP_7}"
   ```

Редактирование конфигурационного файла

1. Откройте конфигурационный файл *am/idp/app-settings.json*.
2. В параметре `AuthenticationMethods` удалите ненужные строки и добавьте идентификаторы провайдеров, которые вы планируете использовать, в следующем формате:
   - В параметре `Name` укажите произвольное уникальное значение.
   - В параметре `Providers` укажите идентификатор используемого провайдера.

     Доступные идентификаторы для Identity Provider

```
SMS OTP {EBB6F3FA-A400-45F4-853A-D517D89AC2A3}
Storage SMS OTP {3F2C1156-B5AF-4643-BFCB-9816012F3F34}
Email OTP {093F612B-727E-44E7-9C95-095F07CBB94B}
Passcode {F696F05D-5466-42b4-BF52-21BEE1CB9529}
Software OTP {0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0}
Secured TOTP {F15FD7EC-19EA-4384-846E-A2D0BE149FA2}
Hardware OTP {AD3FBA95-AE99-4773-93A3-6530A29C7556}
Hardware TOTP {CEB3FEAF-86ED-4A5A-BD3F-6A7B6E60CA05}
Indeed Key {DEEF0CB8-AD2F-4B89-964A-B6C7ECA80C68}
Windows Password {CF189AF5-01C5-469D-A859-A8F2F41ED153}
```

Пример использования одного провайдера

```
"AuthenticationMethods": [
          {
            "Name": "Passcode",
            "Providers": [
              "F696F05D-5466-42b4-BF52-21BEE1CB9529"
            ]
          }
```

Пример использования нескольких провайдеров

```
"AuthenticationMethods": [
         {
            "Name": "HOTP_Passcode",
            "Providers": [
              "AD3FBA95-AE99-4773-93A3-6530A29C7556",
              "F696F05D-5466-42b4-BF52-21BEE1CB9529"
            ]
          }
```

> **ИНФОРМАЦИЯ**
>
> Если вы одновременно используете аутентификацию по Windows Password и по провайдеру, журнал событий отображает следующее:
>
> - Windows Password был введен верно, провайдер неверно — в событиях пользователя регистрируется успешный вход в Identity Provider с помощью Windows Password.
> - Windows Password был введен верно, провайдер верно — в событиях пользователя регистрируется успешный вход с помощью провайдера.

3. Сохраните конфигурационный файл и запустите контейнер с приложением с помощью команды `sudo docker-compose up -d`.

Настройка срока жизни сессии

> **ИНФОРМАЦИЯ**
>
> Данная настройка не обязательна.

Чтобы изменить срок жизни сессии, выполните следующее:

1. Откройте конфигурационный файл *am/idp/app-settings.json*.
2. Для параметра `SessionExpiration` установите необходимое значение. Если параметр не задан, используется значение по умолчанию — 30 минут (`"00:30:00"`).

   Пример

   ```
   "Authentication": {
       "SessionExpiration": "00:30:00"
   },
   ```

3. Сохраните изменения в файле и запустите контейнер с приложением с помощью команды `sudo docker-compose up -d`.

Проверка состояния сервера

Для проверки рабочего состояния контейнера в Docker используйте метод Healthcheck:

http(s)://<dns_имя_сервера>/am/idp/healthcheck/isHealthy

На странице отображается следующая информация о состоянии модуля:

- статус компонента Indeed Identity Provider, время обработки запроса к нему;
- статус последнего запроса;
- статус компонента Indeed Log Server;
- список ошибок при наличии.

Пример результата проверки


```
{
  "Status": "Healthy",
  "Entries": {
    "CoreServer": {
      "PreviousCheckSucceeded": true,
      "CheckState": "Succeeded",
      "CheckStartDate": "2025-03-04T09:00:04.7856489+00:00",
      "CheckDuration": "00:00:00.0315420"
    },
    "LogServer": {
      "PreviousCheckSucceeded": true,
      "CheckState": "Succeeded",
      "CheckStartDate": "2025-03-04T09:00:04.7983677+00:00",
      "CheckDuration": "00:00:00.0178414"
    }
  }
}
```


Если Log Server не работает, то в параметре `Status` и в параметре `CheckState` для `LogServer` отображается значение `Degraded` (ухудшенное состояние). При этом запрос выполнен успешно (HTTP-код 200). При запуске команды `docker ps` возвращается статус состояния сервера `Healthy`.

Неработающий Log Server не влияет на работоспособность Management Console с некоторыми ограничениями — не доступно логирование в Log Server и просмотр страниц/частей страниц, которые связаны с отображением данных с Log Server.

Сбор логов

Информация по включению логирования и сбору логов компонента Identity Provider находится в разделе Сбор логов серверных компонентов.

Опциональные настройки

- Интеграция с приложениями по протоколам OpenID Connect и OAuth 2.0
- Интеграция с приложениями по протоколу SAML
- Включение защиты от перебора
- Аутентификация по имени пользователя без указания домена

Интеграция с приложениями по протоколам OpenID Connect и OAuth 2.0

Для интеграции Identity Provider с приложениями по протоколам OpenID Connect и OAuth 2.0 используйте следующие параметры конфигурационного файла *am/idp/app-settings.json*.

Для получения метаданных сервера перейдите по ссылке: *https://<dns_имя_сервера>/am/idp/.well-known/openid-configuration*.

При интеграции по протоколу OpenID Connect аутентификация может быть выполнена по одному из двух потоков: по потоку авторизационного кода (Authorization Code Flow) или по имплицитному потоку (Implicit Flow). Чтобы выбрать поток, задайте соответствующий тип гранта (параметр `gt`).

Параметр	Описание
`CustomAttributes`	В блоке указываются атрибуты `ServiceProvider` и `Attributes` (с параметрами `Name` и `UserNameFormat`).
`ServiceProvider`	Значение параметра соответствует `ClientId` из секции `OIDC`.
`Name`	Определяет, с каким ключом будет отображаться передаваемый атрибут в результате расшифровки значения IdToken или запроса к Userinfo. При этом если параметр `Name` не соответствует одному из возможных значений (`email`, `name`, `family_name`, `given_name`, `middle_name`), то передаваемый атрибут не будет отображаться в ответе на запрос к Userinfo, но в расшифровке IdToken атрибут будет отображаться.
`UserNameFormat`	Определяет, какая информация о пользователе будет передана OIDC-клиенту. Данный параметр может принимать строго определенный перечень значений: Id, ObjectGUID, Name, CanonicalName, PrincipalName, SamCompatibleName, DistinguishedName, Sid, FirstName, MiddleName, LastName, Email, Phone.
`CertificateThumbprint`	Указывается отпечаток сертификата Identity Provider. Сертификат загружается в хранилище компьютера, где установлен Indeed AM Identity Provider.
`Clients`	В блоке указываются настройки для каждого клиентского приложения. Клиентских приложений может быть несколько.

Параметр	Описание
`ClientId`	Уникальный идентификатор, который используется для определения клиентского приложения при обмене токенов, а также для аутентификации и авторизации пользователя. Когда клиентское приложение запрашивает доступ к защищенным ресурсам, оно предоставляет свой `ClientId` вместе с другими учетными данными для получения токена доступа. Значение по умолчанию: *example-client*.
`ClientSecret`	Представляет собой строку символов, которая известна только клиентскому приложению и серверу IDP. `ClientSecret` используется в процессе обмена токенов для подтверждения идентификации клиентского приложения. При запросе токена доступа клиент должен предоставить свой `ClientId` и `ClientSecret` для аутентификации. Значение по умолчанию: *secret_secret_secret*.
`DisplayName`	Имя клиентского приложения. Используется для отображения информации в интерфейсе клиента. Значение по умолчанию: *Example client application*.
`Permissions`	В блоке указываются атрибуты, которые будут разрешены приложению. После успешной аутентификации и предоставления разрешений приложение может использовать полученные данные. Данные, указанные в `Permissions`, могут быть переданы в ответе по протоколу OIDC (ept — Endpoints, gt — GrantTypes, rst — ResponseTypes, scp — Scopes).
`ept:authorization`	Инициирование авторизации.
`ept:logout`	Завершение сессии, связанной с токеном по идентификатору.
`ept:token`	Используется для получения токена.
`gt:authorization_code`	Тип гранта по потоку авторизационного кода (Authorization Code). Используется для получения токенов (ID Token и Access Token) с помощью промежуточного кода авторизации.
`gt:implicit`	Тип гранта по имплицитному потоку (Implicit Flow). Используется для получения клиентом токена доступа напрямую в перенаправляющем URI.
`gt:refresh_token`	Используется для получения нового токена доступа без необходимости повторной аутентификации пользователя.
`rst:code`	Тип возвращаемой авторизации для использования кода авторизации.

Параметр	Описание
`rst:id_token` `rst:id_token token`	Тип возвращаемой авторизации для использования Implicit Flow. Параметры содержат информацию о пользователе, закодированную в формате JWT.
`scp:email`	Адрес электронной почты пользователя.
`scp:profile`	Информация о профиле пользователя. Включает следующие компоненты: `name`, `given_name`, `family_name`, `middle_name`.
`scp:openid`	Указывает, что клиентское приложение запрашивает аутентификацию пользователя.
`scp:offline_access`	Позволяет клиентскому приложению запрашивать токен обновления (`refresh token`).
`PostLogoutRedirectUris`	Содержит допустимые URL-адреса, на которые перенаправляется пользователь после выхода из клиентского приложения.
`RedirectUris`	Содержит допустимые URL-адреса, на которые перенаправляется пользователь после успешного входа в клиентское приложение.
`Requirements`	Определяет дополнительные требования к клиентским запросам, которые должны быть выполнены для успешной аутентификации и авторизации пользователя.

В следующей таблице перечислены атрибуты, которые Identity Provider передает клиентскому приложению после успешной аутентификации пользователя.

Параметр	Описание
`exp`	Определяет время, после которого ID Token не принимается.
`iat`	Время выдачи JWT.
`sub`	Уникальный идентификатор субъекта. В качестве значения указывается идентификатор пользователя.
`iis`	Организация, выпустившая маркер. Указывается URL.
`aud`	Адресат маркера, указывается `client_id` приложения, направившего запрос на аутентификацию.

Подробнее о настройке интеграции с приложениями по протоколам OpenID Connect и OAuth 2.0 вы можете узнать в базе знаний в статье Настройка OIDC на примере Keycloak.

Интеграция с приложениями по протоколу SAML

- Identity Provider Login URL — *http(s)://<полное_DNS_имя_сервера_Identity_Provider>/am/idp/Account/SsoService*.
- Identity Provider Logout URL — *http(s)://<полное_DNS_имя_сервера_Identity_Provider>/am/idp/Account/Logout*.
- Identity Provider Name — *urn:indeedid:saml_idp*.

Для интеграции Identity Provider с приложениями по протоколу SAML используйте следующие параметры конфигурационного файла *am/idp/app-settings.json*.

Параметр	Описание
`SingleSignOnServiceUrl`	Содержит URL-адрес Single SignOn Service, который получает сообщения SAML о входе в клиентское приложение
`LocalCertificates`	Указывается сертификат Identity Provider. Сертификат загружается в хранилище компьютера, где развернут Indeed AM Identity Provider. Сертификат указывается в параметре `Thumbprint`.
`SingleLogoutServiceUrl`	Содержит URL-адрес Single Logout, который получает сообщения SAML о выходе из клиентского приложения.
`PartnerCertificates`	Указывается сертификат клиентского приложения. Сертификат указывается в параметре `Thumbprint`.
`Name`	Указывается имя клиентского приложения.
`Description`	Указывается описание клиентского приложения.
`WantAuthnRequestSigned`	Параметр указывает, должен ли запрос аутентификации SAML быть подписанным. Рекомендуемое значение: *true*.
`SignSAMLResponse`	Параметр указывает, должны ли быть подписаны ответы SAML, отправляемые клиентскому приложению. Рекомендуемое значение: *true*.
`WantSamlResponseSigned`	Параметр указывает, должны ли утверждения SAML шифроваться. Рекомендуемое значение: *true*.

Параметр	Описание
`SignLogoutRequest`	Параметр указывает, должны ли быть подписаны запросы SAML, отправляемые клиентскому приложению, на выход из клиентского приложения. Рекомендуемое значение: *true*.
`SignLogoutResponse`	Параметр указывает, должны ли быть подписаны ответы SAML, отправляемые клиентскому приложению, на выход из клиентского приложения. Рекомендуемое значение: *true*.
`SignAssertion`	Параметр указывает, должны ли утверждения SAML быть подписаны. Рекомендуемое значение: *true*.
`WantLogoutRequestSigned`	Параметр указывает, должны ли быть подписаны запросы SAML, полученные от клиентского приложения, на выход из клиентского приложения. Рекомендуемое значение: *true*.
`WantLogoutResponseSigned`	Параметр указывает, должны ли быть подписаны ответы SAML, полученные от клиентского приложения, на выход из клиентского приложения. Рекомендуемое значение: *true*.
`AssertionConsumerServiceUrl`	Параметр содержит URL-адрес Assertion Consumer Service клиентского приложения, который получает запросы SAML.

Пример интеграции по протоколу SAML IDP и Nextcloud вы можете посмотреть в базе знаний.

Включение защиты от перебора

В Indeed Access Manager вы можете настроить защиту от подбора учетных записей для компонента Identity Provider.

Если эта настройка включена, то при вводе несуществующего имени пользователя Indeed Access Manager имитирует вход существующего пользователя через Identity Provider: отображает способы аутентификации, запрашивает пароль, а затем отображает ошибку *Неверное имя пользователя или аутентификатор или заблокировано устройство*.

Если эта настройка выключена, то при вводе несуществующего имени пользователя Indeed Access Manager отображает ошибку *Внутренняя ошибка сервера: Пользователь не найден*.

По умолчанию данная настройка отключена.

Чтобы включить защиту от перебора, выполните следующее:

1. Откройте конфигурационный файл *am/core/app-settings.json*.
2. В блоке `Authentication` в строке `bruteForceProtection` укажите значение *Identity Provider*.

   Пример

   ```
   "Authentication": {
       "BruteForceProtection": {
           "Applications": ["Identity Provider"]
       }
   }
   ```

3. Сохраните изменения и запустите контейнер с приложением с помощью команды `sudo docker-compose up -d`.

Аутентификация по имени пользователя без указания домена

Вы можете настроить выбор домена из выпадающего списка.

Если вы указываете несколько доменов, по умолчанию выбирается домен, указанный первым в списке.

Для настройки выполните следующие действия:

1. Откройте конфигурационный файл *am/idp/app-settings.json*.
2. Измените параметр `Authentication`. В строке `Domains` укажите значения необходимых доменов.

```
"Authentication": {
    "SessionExpiration": "00:30:00",
    "Domains": [
      ""
    ]
```

Пример

```
  "Authentication": {
    "SessionExpiration": "00:30:00",
    "Domains": [
      "test.local",
      "demo.local",
      "indeed.local"
    ]
```

3. Сохраните файл и запустите контейнер с приложением с помощью команды `sudo docker-compose up -d`.

Indeed ADFS Extension

Indeed ADFS Extension (2012)

Двухфакторная аутентификация с использованием ADFS

Indeed ADFS Extension (2016)

Двухфакторная аутентификация с использованием ADFS

Indeed ADFS Extension (2012)

С помощью модуля ADFS Extension вы можете реализовать мультифакторную аутентификацию для сервера Microsoft ADFS, добавляя в процесс получения доступа второй фактор.

В ADFS Extension вы можете выполнить аутентификацию по следующим аутентификаторам:

- мобильное приложение Indeed Key (в режиме отправки одноразовых паролей и push-уведомлений с подтверждением входа),
- Telegram (в режиме отправки одноразовых паролей и push-уведомлений с подтверждением входа),
- Email OTP,
- SMS OTP,
- Storage SMS OTP,
- Secured TOTP,
- Software OTP,
- Passcode,
- Hardware TOTP,
- Hardware OTP.

Примеры внедрения расширения:

- Настройка двухфакторной аутентификации для приложений, опубликованных в WAP
- Настройка двухфакторной аутентификации в AD FS для интеграции с Exchange Server 2016
- Настройка двухфакторной аутентификации в Microsoft Office 365 при помощи Indeed AM ADFS Extension

Предварительные требования

Прежде чем перейти к установке и настройке ADFS Extension, необходимо установить .NET Runtime версии 8.0.0.0 или выше.

Для установки на Windows Server 2012 R2 также требуется установить .NET Framework версии 4.5.2 или выше.

Настройка собственного клиентского сертификата

Если вы планируете использовать встроенный клиентский сертификат, пропустите этот шаг и перейдите к установке и настройке ADFS Extension.

> ⚠ **ВАЖНО**
>
> Для повышения безопасности рекомендуется использовать собственный клиентский сертификат.

Чтобы использовать собственный клиентский сертификат, выполните следующее:

1. Выполните все шаги из раздела Настройка собственного клиентского сертификата.
2. С помощью мастера импорта сертификатов расположите сертификат на локальном компьютере:
   - *<сертификат>.pfx* — Личное
   - *<сертификат>.cer* — Доверенные корневые центры
3. Настройте права на чтение сертификата сервисной учетной записи, от которой работает служба ADFS:
   1. Перейдите в Личное→Сертификаты и для *<сертификат>.pfx* выберите Все задачи→Управление закрытыми ключами.
   2. Нажмите Добавить, затем нажмите Дополнительно.
   3. Нажмите Типы объектов и выберите Учетные записи служб.
   4. Добавьте сервисную учетную запись и выдайте права на чтение.

Файлы для установки

Файлы для ADFS Extension расположены в папке *indeed AM <Номер версии>\Indeed AM ADFS Extension\<Номер версии>*:

- *IndeedAM.ADFS.Extension-<номер версии>.x64.ru-ru.msi* — пакет для установки Indeed ADFS Extension.

Установка и настройка ADFS Extension

1. Запустите файл для установки и следуйте шагам мастера установки. Установить провайдер нужно как на компьютере с установленным Core Server, так и на клиентском компьютере.
2. Создайте конфигурационный файл *MFAAdapter.json*, содержащий следующие параметры:
   - `EANetServerURL` — адрес сервера Indeed;
   - `ModeId` — идентификатор используемого метода аутентификации;
   - `ClientCertificateThumbprint` — отпечаток собственного клиентского сертификата. Если параметр не задан, используется встроенный клиентский сертификат.

Пример

```
{
"ServerType":"eaNet",
"EANetServerURL":"https://YourDomainName/am/core/",
"ModeId":"{0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0}",
"ClientCertificateThumbprint":
"D3F29C665C6E420DC42AEB4D3618CF1FB93E0485"
}
```

MODEID МОЖЕТ ИМЕТЬ СЛЕДУЮЩИЕ ЗНАЧЕНИЯ:

- SMS OTP {EBB6F3FA-A400-45F4-853A-D517D89AC2A3}
- Storage SMS OTP {3F2C1156-B5AF-4643-BFCB-9816012F3F34}
- Secured TOTP {F15FD7EC-19EA-4384-846E-A2D0BE149FA2}
- Email OTP {093F612B-727E-44E7-9C95-095F07CBB94B}
- Passcode {F696F05D-5466-42b4-BF52-21BEE1CB9529}
- Software OTP {0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0}
- Hardware OTP {AD3FBA95-AE99-4773-93A3-6530A29C7556}
- Hardware TOTP {CEB3FEAF-86ED-4A5A-BD3F-6A7B6E60CA05}
- Indeed Key Provider {DEEF0CB8-AD2F-4B89-964A-B6C7ECA80C68}

ПРИМЕЧАНИЕ

При использовании соединения по протоколу HTTPS требуется выполнить установку клиентского сертификата на каждый сервер Indeed AM.

3. Запустите PowerShell с правами администратора. Для регистрации адаптера введите следующие данные:

- `YourPath\MFAAdapter.json` — укажите полный путь к конфигурационному файлу *MFAAdapter.json*, созданному в шаге 2.
- В переменной `$typeName` в параметре `Version` указывается номер версии используемого ADFS Extension.

ВАЖНО!

При регистрации, изменении или удалении адаптера перезапустите службы ADFS на каждом сервере ADFS.

Пример

```
$typeName = "IndeedId.ADFS.MFAAdapter.MFAAdapter,
IndeedId.ADFS.MFAAdapter, Version=2.0.0.0, Culture=neutral,
PublicKeyToken=1ebb0d9282100d91"
Register-AdfsAuthenticationProvider -TypeName $typeName -Name "Indeed Id
MFA Adapter" -ConfigurationFilePath 'YourPath\MFAAdapter.json'
```

- Для регистрации нескольких провайдеров измените имя провайдера в параметре `Name`.

Пример

```
Register-AdfsAuthenticationProvider -TypeName $typeName -Name "Indeed Id
MFA Passcode" -ConfigurationFilePath 'YourPath\MFAAdapter.json'
```

- Измените отображаемое имя провайдера. Для параметра `Name` укажите значение из предыдущего шага, для параметра `DisplayName` задайте имя, которое будет отображаться при выполнении аутентификации через ADFS.

Пример

```
Set-AdfsAuthenticationProviderWebContent -Name "Indeed Id MFA Adapter
Passcode" -DisplayName "Passcode"
```

4. Чтобы удалить адаптер, выполните следующую команду:

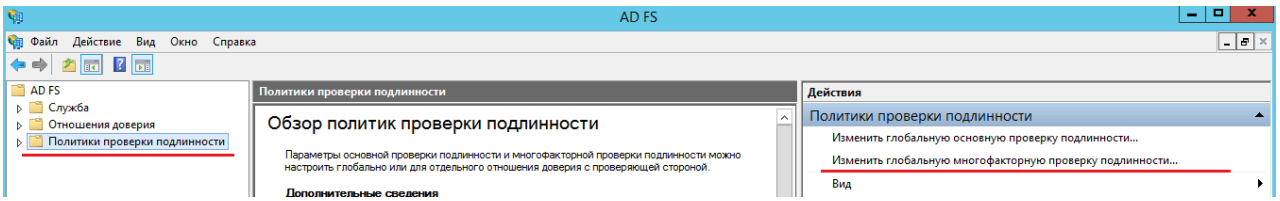
```
Unregister-AdfsAuthenticationProvider -Name "Indeed Id MFA Adapter"
```

5. Чтобы обновить конфигурацию, выполните следующую команду:

```
Import-AdfsAuthenticationProviderConfigurationData -Name "Indeed Id MFA Adapter"
-FilePath 'YourPath\MFAAdapter.json'
```

Включение многофакторной аутентификации для ADFS

1. Откройте консоль управления ADFS.
2. Выберите Политики проверки подлинности.
3. В окне Действия выберите Изменить глобальную многофакторную проверку подлинности....



4. Добавьте пользователя/группу и включите следующие параметры:
    - Во вкладке Многофакторная в пункте Расположение выберите Экстрасеть и Интрасеть;
    - Выберите использование провайдера *Indeed Id MFA Adapter*;
5. Для применения изменений перезапустите службу ADFS.

Регистрация аутентификатора при первом входе в ADFS

При первом входе в ADFS пользователь получит запрос на указание телефонного номера, если:

- у пользователя не указан номер телефона в Active Directory;
- номер телефона указан, но при этом отключена политика *Использовать номер телефона из Active Directory, если аутентификатор не обучен*.

После указания номера телефона пользователь получит одноразовый пароль на указанный номер телефона, который необходимо ввести в форме ADFS, чтобы завершить вход в целевое приложение.

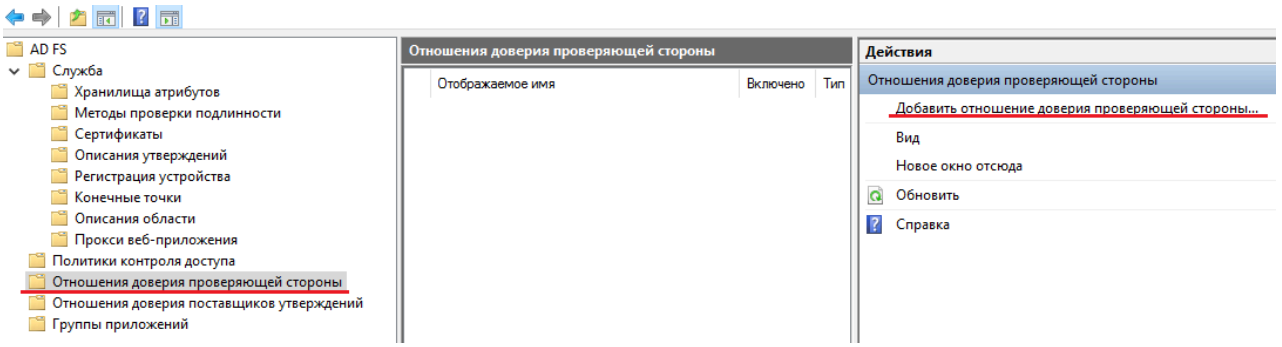
Пример работы модуля на странице ADFS idpinitiatedsignon

Пример работы расширения показан на странице *idpinitiatedsignon.htm*.

По умолчанию данная страница не настроена. Настройка данной страницы не обязательна.

Настройка тестовой страницы

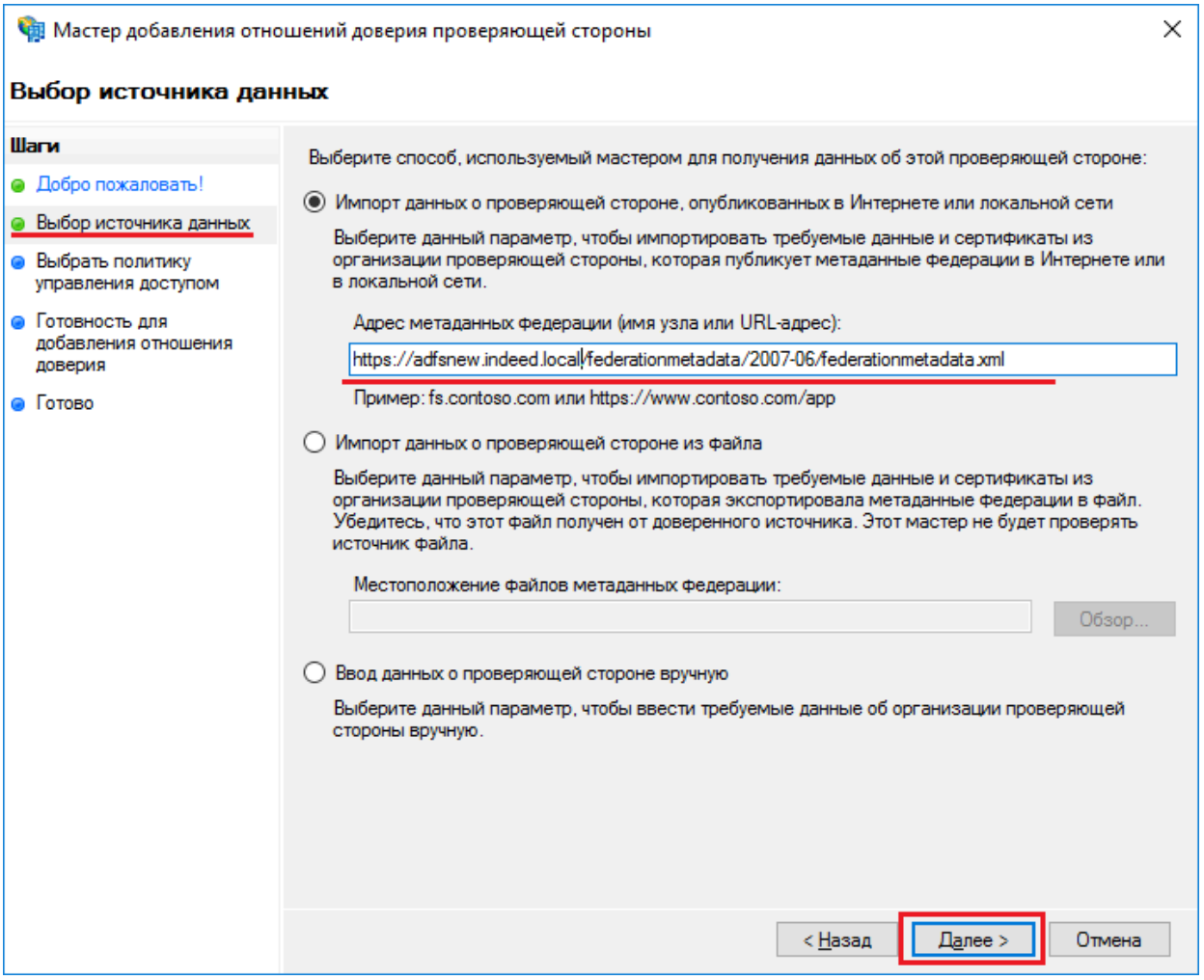
1. Выберите Отношение доверия проверяющей стороны и нажмите Добавить отношение доверия проверяющей стороны....



2. На вкладке Добро пожаловать! выберите Поддерживающие утверждения и нажмите Запустить.

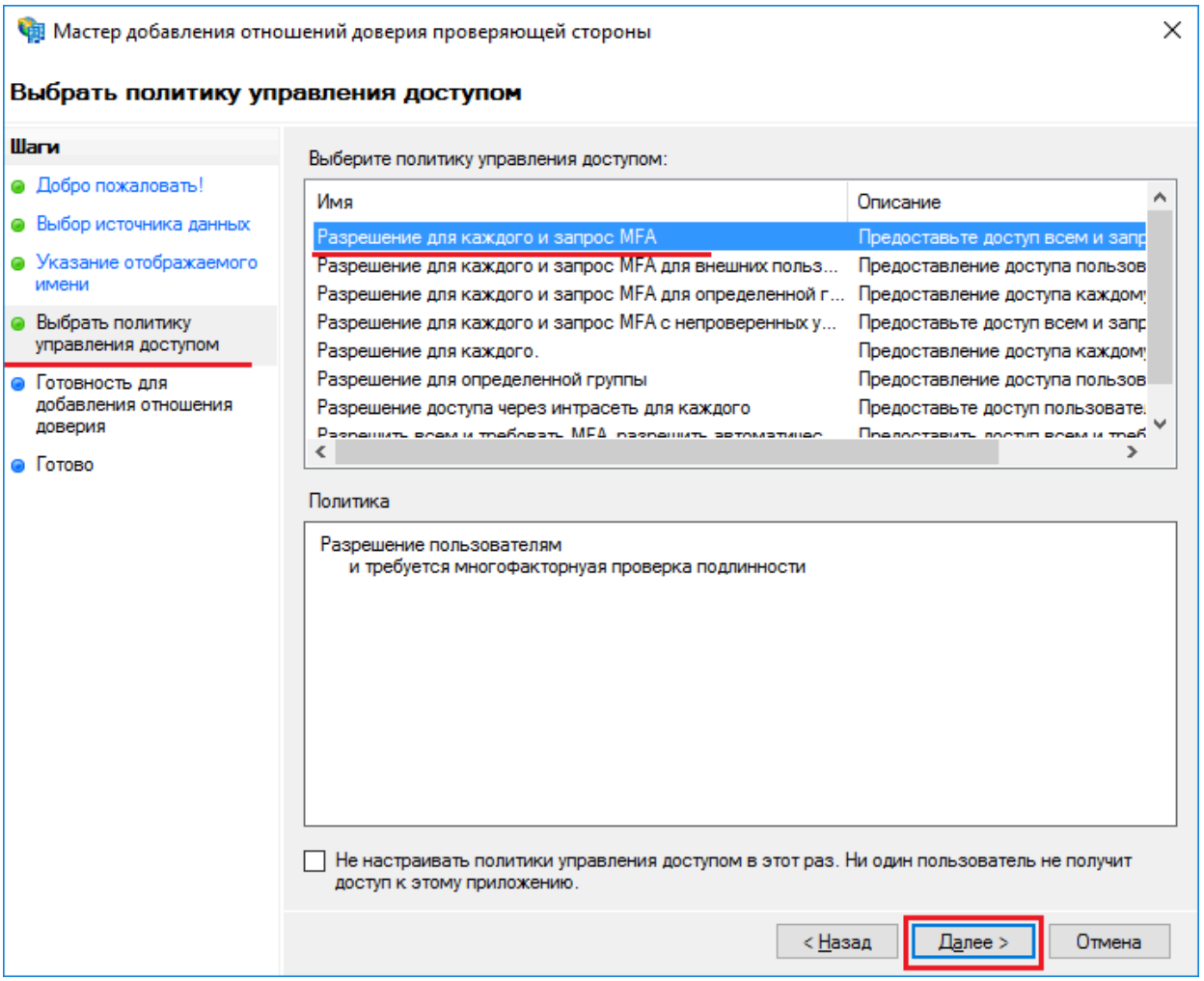
3. На вкладке Выбор источника данных укажите URL вашего приложения и нажмите Далее.

> **ИНФОРМАЦИЯ**
>
> В качестве примера работы расширения используется стандартная страница ADFS *idpinitiatedsignon.htm*. Используется адрес метаданных для данной страницы.



4. На вкладке Указание отображаемого имени введите имя и описание для вашего отношения доверия и нажмите Далее.

5. На вкладке Выбрать политику управления доступом выберите подходящую вам политику с запросом MFA из предложенных по умолчанию, также вы можете добавить произвольные политики контроля доступа.



6. Остальные параметры оставьте по умолчанию.

7. Для применения изменений перезапустите службу ADFS.

Работа модуля

1. Откройте тестовую страницу ADFS: https://YourDomainName/adfs/ls/idpinitiatedsignon.htm.
2. Выполните вход.
3. После ввода доменного логина и пароля укажите данные для второго фактора аутентификации.

4. После корректного ввода данных будет выполнен вход.

Indeed ADFS Extension (2016)

С помощью модуля ADFS Extension вы можете реализовать мультифакторную аутентификацию для сервера Microsoft ADFS, добавляя в процесс получения доступа второй фактор.

В ADFS Extension вы можете выполнить аутентификацию по следующим аутентификаторам:

- мобильное приложение Indeed Key (в режиме отправки одноразовых паролей и push-уведомлений с подтверждением входа),
- Telegram (в режиме отправки одноразовых паролей и push-уведомлений с подтверждением входа),
- Email OTP,
- SMS OTP,
- Storage SMS OTP,
- Secured TOTP,
- Software OTP,
- Passcode,
- Hardware TOTP,
- Hardware OTP.

Примеры внедрения расширения

- Настройка двухфакторной аутентификации для приложений опубликованных в WAP
- Настройка двухфакторной аутентификации в AD FS для интеграции с Exchange Server 2016
- Настройка двухфакторной аутентификации в Microsoft Office 365 при помощи Indeed AM ADFS Extension

Предварительные требования

Прежде чем перейти к установке и настройке ADFS Extension, необходимо установить .NET Runtime версии 8.0.0.0 или выше.

Настройка собственного клиентского сертификата

Если вы планируете использовать встроенный клиентский сертификат, пропустите этот шаг и перейдите к установке и настройке ADFS Extension.

> ⚠ **ВАЖНО**
>
> Для повышения безопасности рекомендуется использовать собственный клиентский сертификат.

Чтобы использовать собственный клиентский сертификат, выполните следующее:

1. Выполните все шаги из раздела Настройка собственного клиентского сертификата.

2. С помощью мастера импорта сертификатов расположите сертификат на локальном компьютере:

   - *<сертификат>.pfx* — Личное
   - *<сертификат>.cer* — Доверенные корневые центры

3. Настройте права на чтение сертификата сервисной учетной записи, от которой работает служба ADFS:

   1. Перейдите в Личное→Сертификаты и для *<сертификат>.pfx* выберите Все задачи→Управление закрытыми ключами.
   2. Нажмите Добавить, затем нажмите Дополнительно.
   3. Нажмите Типы объектов и выберите Учетные записи служб.
   4. Добавьте сервисную учетную запись и выдайте права на чтение.

Файлы для установки

Файлы для ADFS Extension расположены в папке *indeed AM <Номер версии>\Indeed AM ADFS Extension\<Номер версии>*:

- *IndeedAM.ADFS.Extension-<номер версии>.x64.ru-ru.msi* — пакет для установки Indeed ADFS Extension.

Установка и настройка ADFS Extension

> **ИНФОРМАЦИЯ**
>
> Перед запуском пакета для установки Indeed ADFS Extension необходимо добавить роль службы федерации Active Directory (AD FS).

1. Запустите файл для установки и следуйте шагам мастера установки. Установить провайдер нужно как на компьютере с установленным Core Server, так и на клиентском компьютере.

2. Создайте конфигурационный файл *MFAAdapter.json*, содержащий следующие параметры:

   - `EANetServerURL` — адрес сервера Indeed;
   - `ModeId` — идентификатор используемого метода аутентификации;
   - `ClientCertificateThumbprint` — отпечаток собственного клиентского сертификата. Если параметр не задан, используется встроенный клиентский сертификат.

Пример

```
{
"ServerType":"eaNet",
"EANetServerURL":"https://YourDomainName/am/core/",
"ModeId":"{0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0}",
"ClientCertificateThumbprint":
"D3F29C665C6E420DC42AEB4D3618CF1FB93E0485"
}
```

MODEID МОЖЕТ ИМЕТЬ СЛЕДУЮЩИЕ ЗНАЧЕНИЯ:

- SMS OTP {EBB6F3FA-A400-45F4-853A-D517D89AC2A3}
- Storage SMS OTP {3F2C1156-B5AF-4643-BFCB-9816012F3F34}
- Secured TOTP {F15FD7EC-19EA-4384-846E-A2D0BE149FA2}
- Email OTP {093F612B-727E-44E7-9C95-095F07CBB94B}
- Passcode {F696F05D-5466-42b4-BF52-21BEE1CB9529}
- Software OTP {0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0}
- Hardware OTP {AD3FBA95-AE99-4773-93A3-6530A29C7556}
- Hardware TOTP {CEB3FEAF-86ED-4A5A-BD3F-6A7B6E60CA05}
- Indeed Key Provider {DEEF0CB8-AD2F-4B89-964A-B6C7ECA80C68}

ПРИМЕЧАНИЕ

При использовании соединения по протоколу HTTPS требуется выполнить установку клиентского сертификата на каждый сервер Indeed AM.

3. Запустите PowerShell с правами администратора. Для регистрации адаптера введите следующие данные:

- `YourPath\MFAAdapter.json` — укажите свой полный путь к конфигурационному файлу *MFAAdapter.json*, созданному в шаге 2.
- В переменной `$typeName` в параметре `Version` указывается номер версии используемого ADFS Extension.

ВАЖНО!

При регистрации, изменении или удалении адаптера перезапустите службы ADFS на каждом сервере ADFS.

Пример

```
$typeName = "IndeedId.ADFS.MFAAdapter.MFAAdapter,
IndeedId.ADFS.MFAAdapter, Version=2.0.0.0, Culture=neutral,
PublicKeyToken=1ebb0d9282100d91"
Register-AdfsAuthenticationProvider -TypeName $typeName -Name "Indeed Id
MFA Adapter" -ConfigurationFilePath 'YourPath\MFAAdapter.json'
```

- Для регистрации нескольких провайдеров измените имя провайдера в параметре `Name`.

Пример

```
Register-AdfsAuthenticationProvider -TypeName $typeName -Name "Indeed Id
MFA Passcode" -ConfigurationFilePath 'YourPath\MFAAdapter.json'
```

- Измените отображаемое имя провайдера. Для параметра `Name` укажите значение из предыдущего шага, для параметра `DisplayName` задайте имя, которое будет отображаться при выполнении аутентификации через ADFS.

Пример

```
Set-AdfsAuthenticationProviderWebContent -Name "Indeed Id MFA Adapter
Passcode" -DisplayName "Passcode"
```

4. Чтобы удалить адаптер, выполните следующую команду:

```
Unregister-AdfsAuthenticationProvider -Name "Indeed Id MFA Adapter"
```

5. Чтобы обновить конфигурацию, выполните следующую команду:

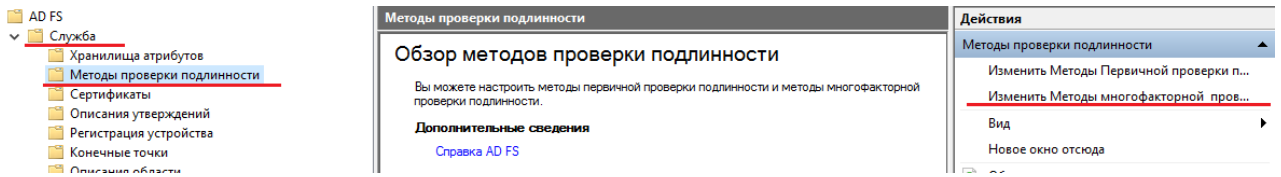
```
Import-AdfsAuthenticationProviderConfigurationData -Name "Indeed Id MFA Adapter"
-FilePath 'YourPath\MFAAdapter.json'
```

Включение многофакторной аутентификации для ADFS

1. Откройте консоль управления ADFS.

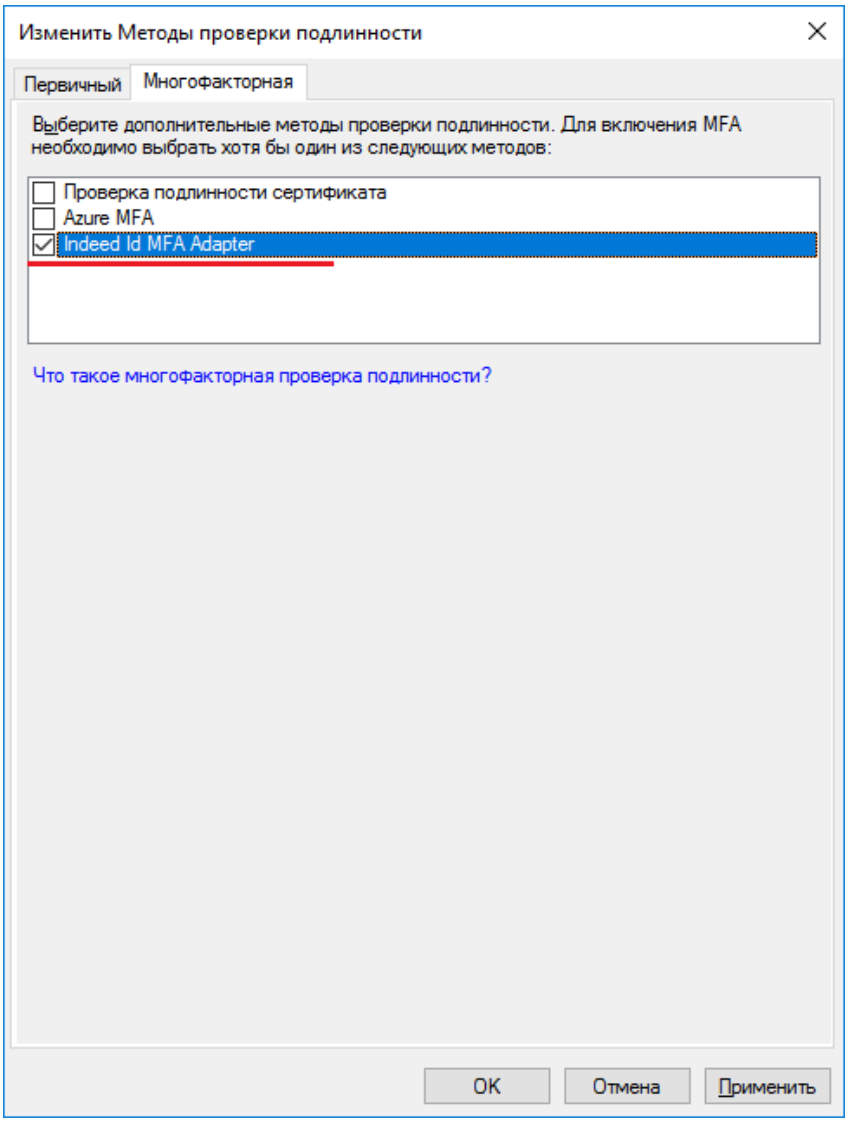
2. Выберите Служба→Методы проверки подлинности.

3. В окне Действия выберите Изменить методы многофакторной проверки....



4. На вкладке Многофакторная выберите созданный ранее провайдер и нажмите Применить.

5. Для применения изменений перезапустите службу AD FS.



Регистрация аутентификатора при первом входе в ADFS

При первом входе в ADFS пользователь получит запрос на указание телефонного номера, если:

- у пользователя не указан номер телефона в Active Directory;
- номер телефона указан, но при этом отключена политика *Использовать номер телефона из Active Directory, если аутентификатор не обучен*.

После указания номера телефона пользователь получит одноразовый пароль на указанный номер телефона, который необходимо ввести в форме ADFS, чтобы завершить вход в целевое приложение.

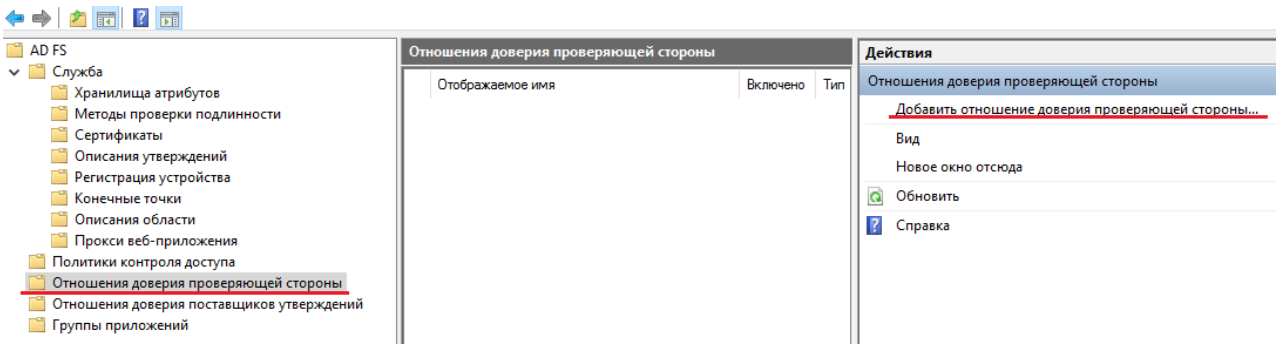
Пример работы модуля на странице ADFS idpinitiatedsignon

Пример работы расширения показан на странице *idpinitiatedsignon.htm*.

По умолчанию данная страница не настроена. Настройка данной страницы не обязательна.

Настройка тестовой страницы

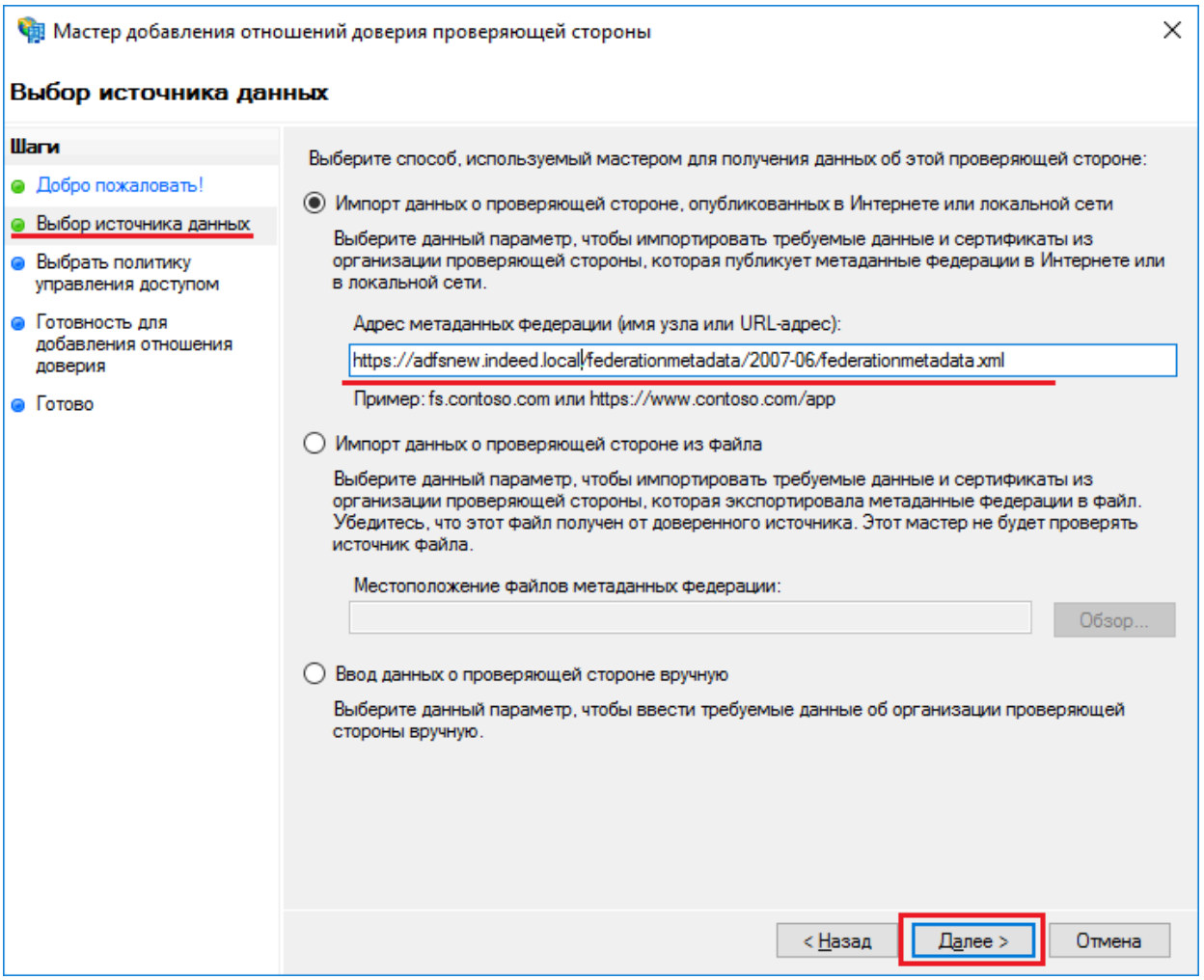
1. Выберите Отношение доверия проверяющей стороны и нажмите Добавить отношение доверия проверяющей стороны....



2. На вкладке Добро пожаловать! выберите Поддерживающие утверждения и нажмите Запустить.

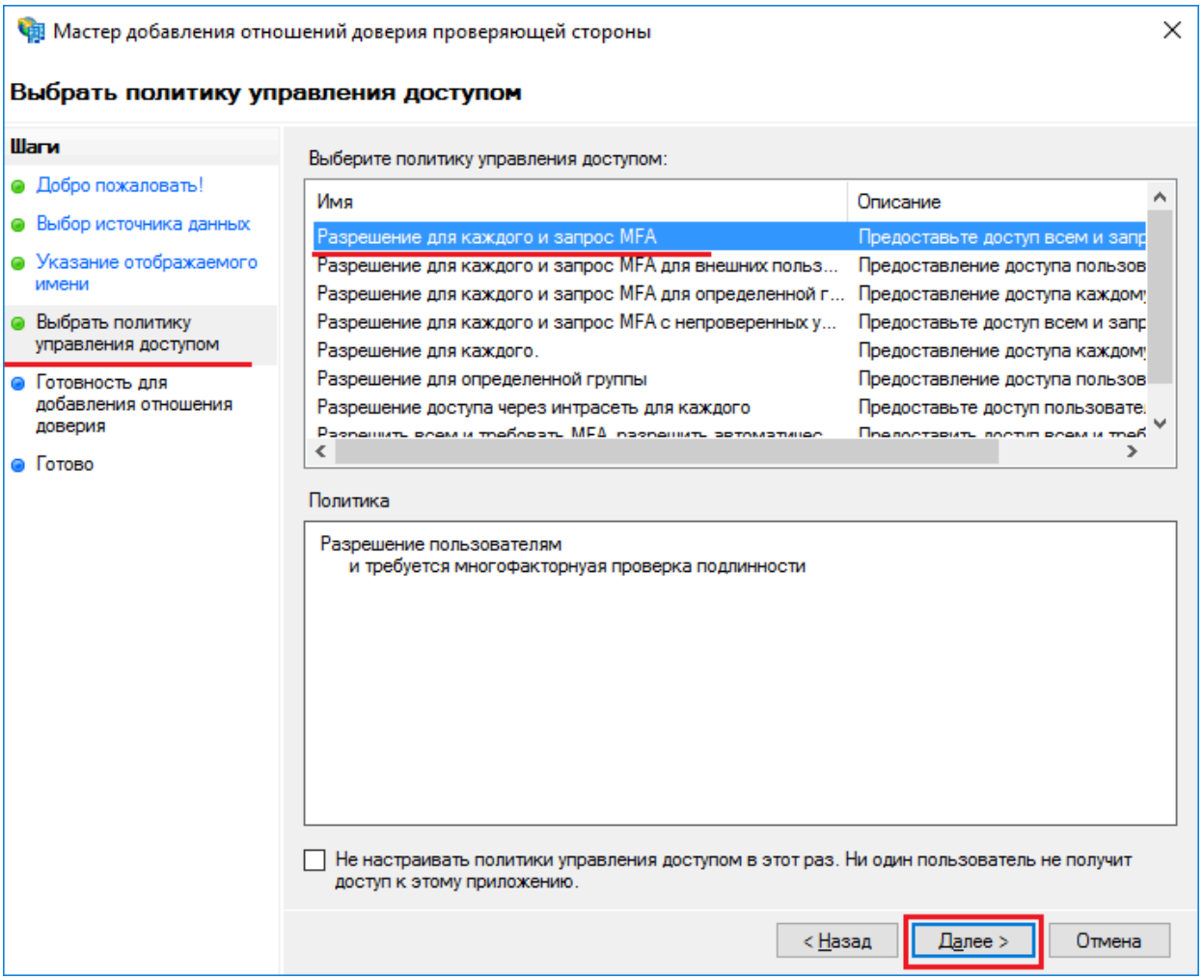
3. На вкладке Выбор источника данных укажите URL вашего приложения и нажмите Далее.

> **ИНФОРМАЦИЯ**
>
> В качестве примера работы расширения используется стандартная страница ADFS *idpinitiatedsignon.htm*. Используется адрес метаданных для данной страницы, например, *https://<полное_dns_имя_сервера>/federationmetadata/2007-06/federationmetadata.xml*.



4. На вкладке Указание отображаемого имени введите имя и описание для вашего отношения доверия и нажмите Далее.

5. На вкладке Выбрать политику управления доступом выберите подходящую вам политику с запросом MFA из предложенных по умолчанию, также вы можете добавить произвольные политики контроля доступа.



6. Остальные параметры оставьте по умолчанию.

7. Для применения изменений перезапустите службу ADFS.

Работа модуля

По умолчанию страница *idpinitiatedsignon.htm* отключена в ADFS 2016, для включения запустите PowerShell от имени администратора и выполните команду:

```
Set-AdfsProperties -EnableIdpInitiatedSignonPage $True
```

1. Откройте тестовую страницу ADFS: https://YourDomainName/adfs/ls/idpinitiatedsignon.htm.

2. Выполните вход.

3. После ввода доменного логина и пароля укажите данные для второго фактора аутентификации.

4. После корректного ввода данных будет выполнен вход.

Indeed FreeRADIUS Extension

Indeed FreeRADIUS Extension (FreeRADIUS Extension) представляет собой модуль, позволяющий реализовать технологию двухфакторной аутентификации для RADIUS-совместимых сервисов и приложений. Модуль FreeRADIUS Extension основан на открытом исходном коде FreeRADIUS-сервера.

В модуле FreeRADIUS вы можете выполнить аутентификацию по следующим методам аутентификации.

Однофакторная аутентификация

- КЛЮЧ: Сервис Паролей;
- Hardware OTP;
- Hardware TOTP;
- Passcode;
- Secured TOTP;
- Software TOTP;
- Indeed Key (OTP).

Двухфакторная аутентификация

- Passcode + Indeed Key (в режиме отправки push-уведомлений с подтверждением входа);
- Passcode + Indeed Key (OTP);
- Passcode + Telegram (в режиме отправки push-уведомлений с подтверждением входа);
- Passcode + Telegram (OTP);
- Passcode + Secured TOTP;
- Passcode + Software TOTP;
- Passcode + SMS OTP;
- Windows Password + КЛЮЧ: Сервис Паролей;
- Windows Password + Email OTP;
- Windows Password + Hardware OTP;
- Windows Password + Hardware TOTP;
- Windows Password + Indeed Key (в режиме отправки push-уведомлений с подтверждением входа);
- Windows Password + Indeed Key (OTP);
- Windows Password + Telegram (в режиме отправки push-уведомлений с подтверждением входа);
- Windows Password + Telegram (OTP);
- Windows Password + Passcode;
- Windows Password + SMS OTP;
- Windows Password + Storage SMS OTP;
- Windows Password + Secured TOTP.

Установка и настройка

Чтобы установить и настроить модуль FreeRADIUS Extension:

1. Импортируйте образ Docker.
2. Настройте переменные окружения.
3. Укажите адреса клиентов сервера FreeRADIUS.
4. Создайте новые каталоги и настройте права.
5. Запустите контейнер с приложением.

Импорт образа Docker

1. Скачайте архив *ea-freeradius-<номер версии>.tar.gz*, загрузите его на целевую машину в необходимый каталог.
2. Распакуйте в этот каталог архив с помощью команды:

```
sudo tar -xvf <имя архива>.tar.gz
```

3. Перейдите в целевую папку с архивом и импортируйте образ Docker с помощью команды:

```
sudo docker load -i <имя архива>
```

> **ПОДСКАЗКА**
>
> Вы можете просмотреть список всех импортируемых образов с помощью команды:
>
> ```
> docker images
> ```

Настройка переменных окружения

1. Сделайте копию файла *freeradius/.example-env* и переименуйте его в *.env*.
2. В файле *.env* укажите необходимые значения для переменных окружения:
   - Задайте значения для переменных `RAD_UID` и `RAD_GID`.
   - В переменной `INDEED_AM_URI` укажите URL-адрес сервера Core Server.

Полное описание переменных окружения смотрите в разделе Переменные окружения FreeRADIUS.

Пример файла *.env*

```
RADIUS_TAG=9.3.0-master.3261-40314f2

#User id and group id
RAD_UID=200000
RAD_GID=200000

#Radius variables
INDEED_AM_URI=https://amdeb3.company.local/am/core
INDEED_AM_VALIDATE_CERT=false
INDEED_AM_CA_CERT_PATH=/tmp/certs
# INDEED_AM_CLIENT_CERT=client.crt
# INDEED_AM_CLIENT_KEY_CERT=client.key
LDAP_SERVER=ldaps://dc.company.local
LDAP_PORT=636
LDAP_IDENTITY=cn=amadm,cn=users,dc=company,dc=local
LDAP_PASSWORD=password
LDAP_BASE_DN=cn=users,dc=company,dc=local
LDAP_CERT=ca.crt
AM_PUSH_TIMEOUT_SEC=30
AM_CACHE_LIFETIME_SEC=600
# AM_DEBUG=true
# AM_MT_DEBUG=true

# DEFAULT_DOMAIN_NAME=company.local
# DEFAULT_NETBIOS_NAME=EXAMPLE

# DISABLE_RLM_PREPROCESS=false
```

Настройка клиентов

1. Сделайте копию файла *freeradius/example-clients.conf* и переименуйте его в *clients.conf*.

2. Откройте файл *clients.conf*.

3. Укажите адреса клиентов, которые будут подключаться к серверу FreeRADIUS Extension, и секретные ключи. Поддерживается формат IPv4.

   В файле уже есть примеры адресов, вы можете отредактировать их или создать новые. При создании новых учитывайте формат *client NAME*, *client NAME_WITH_SPACE*.

4. Если клиентское приложение отправляет атрибут *Message-Authenticator*, добавьте параметры со значениями `require_message_authenticator=yes` и `limit_proxy_state=yes`, чтобы защитить FreeRadius от уязвимости Blast-RADIUS.

5. При любых изменениях в файле *clients.conf* перезапустите контейнер с приложением.

> **ИНФОРМАЦИЯ**
>
> Подробнее о файле *clients.conf*, атрибуте *Message-Authenticator* и Blast-RADIUS вы можете узнать в документации FreeRADIUS.

Пример файла *clients.conf* с одним клиентским приложением

```
client <Name>_wifi {
  ipaddr = 192.168.3.100
  secret = secret123
}
```

Создание каталогов и настройка прав

1. Перейдите в каталог *freeradius* и создайте новые каталоги *common_certs*, *radius_certs*, *logs* с помощью команды:

```
sudo mkdir common_certs radius_certs logs
```

2. Установите права доступа к каталогам с помощью команды:

```
sudo chmod 744 common_certs radius_certs logs
```

3. В каталог *common_certs* положите доменный сертификат в формате Base64 с именем файла, которое вы указали в переменной `LDAP_CERT`.

4. Сделайте владельцем пользователя, которого вы указали в файле *.env* в переменных `RAD_UID` и `RAD_GID`, через следующую команду:

```
sudo chown <RAD_UID>:<RAD_GID> ./*
```

Запуск контейнера

Чтобы создать и запустить контейнер, используйте следующую команду:

```
sudo docker-compose up -d
```

После запуска настройте интеграцию с бизнес-приложениями в Management Console.

Клиентские приложения должны быть добавлены в файл *clients.conf*.

Переменные окружения FreeRADIUS

Переменные окружения находятся в файле *freeradius/.env* и доступны пользователю с заданными по умолчанию значениями.

Пример файла *freeradius/.env*

```
RADIUS_TAG=9.3.0-unstable.1728-dad05d0e

#User id and group id
RAD_UID=200000
RAD_GID=200000

#Installation variables
INDEED_AM_URI=https://amdeb3.company.local/am/core
INDEED_AM_VALIDATE_CERT=false
INDEED_AM_CA_CERT_PATH=/tmp/certs
# INDEED_AM_CLIENT_CERT=client.crt
# INDEED_AM_CLIENT_KEY_CERT=client.key

#LDAP variables
#LDAP_SERVER=ldaps://dc.company.local
#LDAP_PORT=636
#LDAP_IDENTITY=cn=amadm,cn=users,dc=company,dc=local
#LDAP_PASSWORD=password
#LDAP_BASE_DN=cn=users,dc=company,dc=local
#LDAP_CERT=ca.crt
#LDAP_NETBIOS_NAME=COMPANY
#LDAP_DOMAIN_NAME=company.local
#LDAP_START_SERVERS=5
#LDAP_NET_TIMEOUT=1
#MAX_LDAP_SERVER=20

#Other Radius variables
AM_PUSH_TIMEOUT_SEC=30
AM_CACHE_LIFETIME_SEC=600
# LDAP_START_SERVERS=0
# AM_ALLOW_PASSWORDLESS_AUTH=false
# DISABLE_RLM_PREPROCESS=false
# DEFAULT_DOMAIN_NAME=company.local
# DEFAULT_NETBIOS_NAME=EXAMPLE
# default_prompt_2fa=Введите второй фактор:

#Logging
# AM_DEBUG=true
# AM_MT_DEBUG=false
```

В следующей таблице описаны все переменные окружения, находящиеся в файле *freeradius/.env*.

Переменная	Описание
`RADIUS_TAG`	Тег docker-образа. Необходимо указать тег образа, который вы импортировали из архива через команду `sudo docker load -i <имя архива>.tar`. Также тег можно посмотреть после импорта образа через команду `sudo docker images`.
`RAD_UID`	ID пользователя, под которым будет работать сервис (рекомендуется, чтобы ID не пересекалось с ID локальных пользователей хоста). Пример: 200000.
`RAD_GID`	ID группы пользователя, под которым будет работать сервис (рекомендуется, чтобы ID не пересекалось с ID локальных пользователей хоста). Пример: 200000.
`INDEED_AM_URI`	URL-адрес сервера Core Server. Пример: `https://127.0.0.1/am/core/`.
`INDEED_AM_VALIDATE_CERT`	Валидация серверного сертификата. Значения: `true`, `false`.
`INDEED_AM_CA_CERT_PATH`	Путь внутри контейнера к каталогу с сертификатами сервера. Обычно монтируется к каталогу хоста *common_certs*. Если в `INDEED_AM_VALIDATE_CERT` задано значение `true`, то для каталога должен быть разрешен доступ на запись. Пример: `./common_certs:${INDEED_AM_CA_CERT_PATH}:rw,Z`.
`AM_PUSH_TIMEOUT_SEC`	Настройка таймаута времени ожидания получения push-сообщения для провайдеров Indeed Key Push.
`AM_DEBUG`	Запуск в режиме отладки, выводятся отладочные сообщения, модуль запускается в однопоточном режиме. Переменная закомментирована (`false` — не работает). Для включения необходимо раскомментировать. Значения: `true`, `false`.
`AM_MT_DEBUG`	Запуск в режиме отладки, выводятся отладочные сообщения, модуль запускается в многопоточном режиме, флаг имеет приоритет над `AM_DEBUG`.

Переменная	Описание
`LDAP_SERVER`	IP-адрес LDAP-сервера. Если указан, то первый фактор аутентификации будет проверятся непосредственно на LDAP-сервере.
`LDAP_PORT`	Порт AD-сервера. Для LDAPS-соединения обычно используется 636. Значение по умолчанию: `389`.
`LDAP_IDENTITY`	Учетная запись AD в формате значения атрибута `distinguishedName`, с правами на чтение AD. Пример: `cn=someuser,cn=users,dc=mycompany,dc=com`.
`LDAP_PASSWORD`	Пароль к учетной записи из переменной `LDAP_IDENTITY`.
`LDAP_BASE_DN`	Каталог пользователей AD в формате значения атрибута `distinguishedName`, с которыми будет взаимодействие. Пример: `cn=users,dc=bond,dc=test`.
`LDAP_CERT`	Имя доменного сертификата, который находится в директории *common_certs*. Используется для установки ldaps-соединения с AD-сервером. Если используется LDAP, то переменную необходимо закомментировать. Пример: `ad.crt`.
`LDAP_NETBIOS_NAME`	Задает имя NETBIOS LDAP-сервера. Позволяет осуществлять вход пользователям в виде *EXAMPLE\user*.
`LDAP_DOMAIN_NAME`	Задает доменное имя сервера. Используется для определения LDAP-сервера, если задано несколько LDAP-серверов. Для режима нескольких LDAP-серверов для каждого сервера необходимо указать либо `LDAP_DOMAIN_NAME`, либо `LDAP_NETBIOS_NAME`.
`DEFAULT_DOMAIN_NAME`	Содержит имя домена, которое добавляется к имени пользователя в виде суффикса, и таким образом создается имя пользователя в формате *User Principal Name*. Имя в формате *UPN* используется для запросов к LDAP и AM-серверам. Исходное имя пользователя во FreeRADIUS Extension атрибуте `User-Name` не изменяется. Переменная имеет приоритет над `DEFAULT_NETBIOS_NAME`.

Переменная	Описание
`DEFAULT_NETBIOS_NAME`	Содержит имя NetBIOS AD-сервера, которое добавляется к имени пользователя в виде префикса, и таким образом создается имя пользователя в формате *Down-Level Logon Name*. Имя в формате *Down-Level Logon Name* используется для запросов к AM-серверу. Для запроса к LDAP-серверу используется исходное имя в формате *SAM Account Name*. Исходное имя пользователя во FreeRADIUS Extension атрибуте `User-Name` не изменяется.
`LDAP_DEFAULT_DOMAIN_NAME`	Задается только при использовании нескольких LDAP-серверов. Можно задать переменную для каждого LDAP-сервера. Используется для конфигурации входа пользователя по SAM Account Name (имя без доменной части). Чтобы задать переменную для конкретного сервера, добавьте соответствующий индекс к наименованию LDAP, например: для `LDAP2_SERVER` настройте переменную `LDAP2_DEFAULT_DOMAIN_NAME`. Переменная имеет приоритет над `LDAP_DEFAULT_NETBIOS_NAME`.
`LDAP_DEFAULT_NETBIOS_NAME`	Задается только при использовании нескольких LDAP-серверов. Можно задать переменную для каждого LDAP-сервера. Используется для конфигурации входа пользователя по SAM Account Name (имя без доменной части). Чтобы задать переменную для конкретного сервера, добавьте соответствующий индекс к наименованию LDAP, например: для `LDAP2_SERVER` настройте переменную `LDAP2_DEFAULT_NETBIOS_NAME`.
`LDAP_START_SERVERS`	Задает количество потоков в пуле соединений с LDAP-серверами при запуске контейнера. Стартовые потоки позволяют увеличить скорость обработки запросов. Значение по умолчанию: 5 потоков. Диапазон значений: от 0 до 64.
`LDAP_NET_TIMEOUT`	Задает таймаут подключения к LDAP/LDAPS при установленном соединении. По истечении заданного времени происходит разрыв соединения. Значение по умолчанию 1 (секунда). Диапазон значений: от 0 до 2147483647.
`MAX_LDAP_SERVER`	Задает максимальное количество обрабатываемых LDAP-серверов. Значение по умолчанию: 20.

Переменная	Описание
`default_prompt_2fa`	Задает запрос второго фактора, используемый по умолчанию. По умолчанию задано сообщение: `Enter the second factor`.
`prompt_2fa_<индентификатор провайдера с нижними подчеркиваниями, вместо тире>`	Задает запрос второго фактора для конкретного метода. Идентификатор провайдера можно задавать либо в нижнем, либо в верхнем регистре. Пример: `prompt_2fa_f696f05d_5466_42b4_bf52_21bee1cb9529`.
`INDEED_AM_CLIENT_CERT`	Имя файла с клиентским сертификатом. Расположен в каталоге, который монтируется к `INDEED_AM_CA_CERT_PATH`. По умолчанию в файле *docker-compose.yml* указано соответствие значению `common_certs`.
`INDEED_AM_CLIENT_KEY_CERT`	Имя файла с приватным ключом сертификата. Расположен в каталоге, который монтируется к `INDEED_AM_CA_CERT_PATH`. По умолчанию в файле *docker-compose.yml* указано соответствие значению `common_certs`.
`AM_CACHE_LIFETIME_SEC`	Определяет время кеширования. Если задать значение 0 секунд, то кеширование не производится. Значение по умолчанию: 600 секунд.
`DISABLE_RLM_PREPROCESS`	Параметр отвечает за предварительную обработку RADIUS-атрибутов. Параметр используется, если в запросе от клиентского приложения к FreeRADIUS отсутствует атрибут `NAS-IP-Address`. При отключении предварительной обработки (значение `true`) данный модуль не будет преобразовывать другие атрибуты (например Src-IP-Address) в NAS-IP-Address, если NAS-IP-Address не был получен. При отсутствии NAS-IP-Address в запросе модуль добавляет такой атрибут и устанавливает его значение из атрибута Src-IP-Address request-пакета. В этом случае в настройках в Management Console необходимо указать Src-IP-Address. Значение по умолчанию: `false`.

Переменная	Описание
`AM_ALLOW_PASSWORDLESS_AUTH`	Параметр отключает проверку первого фактора аутентификации. Важно: Используйте параметр только при работе со службой Remote Desktop Gateway (RD Gateway). При использовании метода аутентификации Windows Password + Indeed Key (в режиме отправки push-уведомления) проверка первого фактора Windows Password происходит на стороне самой службы RD Gateway. Для корректной работы в таком сценарии необходимо для переменной `AM_ALLOW_PASSWORDLESS_AUTH` установить значение `true` и закомментировать или удалить переменные LDAP. Примечание: Для работы со службой RD Gateway рекомендуется подготовить отдельный образ Docker с FreeRadius.

Настройка переменных окружения

Формат имени пользователя

User Principal Name

User Principal Name (UPN) — имя для входа пользователя в формате email адреса, например user@indeed.domain. UPN-имя используется во FreeRADIUS Extension по умолчанию.

SAM Account Name

SAM Account Name — имя для входа пользователя без суффиксов и префиксов, например *username*. Для обработки имени формата *SAM Account Name* используются две переменные окружения:

- `DEFAULT_DOMAIN_NAME` — содержит имя домена, которое добавляется к имени пользователя в виде суффикса. Таким образом создается имя пользователя в формате *UPN*. Имя в формате *UPN* используется для запросов к серверам LDAP и AM. Эта переменная имеет приоритет над `DEFAULT_NETBIOS_NAME`.
- `DEFAULT_NETBIOS_NAME` — содержит NetBIOS-имя сервера AD, которое добавляется к имени пользователя в виде префикса. Таким образом создается имя пользователя в формате *Down-Level Logon Name*.

Down-Level Logon Name

Down-Level Logon Name — формат имени входа, используемый для указания домена и учетной записи пользователя в этом домене, например INDEED\user. Используется для запросов к AM-серверу.

> **ПРИМЕЧАНИЕ**
>
> Чтобы использовать формат имени *INDEED\user* для запросов к LDAP-серверу, необходимо настроить переменную `LDAP_NETBIOS_NAME`.

Настройка сообщения при запросе второго фактора

При запросе второго фактора многофакторной аутентификации для пользователя выводится сообщение по умолчанию — `Enter the second factor` («Введите второй фактор»). Чтобы изменить сообщение, задайте переменную окружения `default_prompt_2fa`.

Также можно задать отдельное сообщение для конкретного провайдера. Для этого настройте переменную окружения `prompt_2fa_<идентификатор провайдера с нижними подчеркиваниями, вместо тире>`. Настройка сообщения для конкретного провайдера имеет приоритет над переменной окружения `default_prompt_2fa`.

Идентификатор провайдера в переменной задается либо только в нижнем, либо только в верхнем регистре. Например, для провайдера Software OTP переменная окружения может выглядеть

`prompt_2fa_7e87866d_1b9b_45a1_961e_bc48697f0020` или `prompt_2fa_7E87866D_1B9B_45A1_961E_BC48697F0020`.

Для следующих методов многофакторной аутентификации (MFA) можно указать как отдельно идентификатор провайдера второго фактора, так и идентификатор для всей цепочки многофакторной аутентификации.

Идентификатор для цепочки MFA

`2FA: Passcode + Indeed Key (OTP) – e5d3185c-9a13-4538-be8f-d4e1c50a329e`
`2FA: Passcode + Secured TOTP – 882c1787-fd32-44a2-ba89-f1f529fbe7ab`
`2FA: Passcode + SMS OTP – 4e32199b-9a21-4cd7-8646-c70c48b55ed9`
`2FA: Passcode + Software TOTP – cb3d3b0a-29c6-4ba4-939d-09b126c10c2e`

Настройка клиентского сертификата

По умолчанию используется встроенный клиентский сертификат, если в файле *.env* отсутствуют переменные окружения `INDEED_AM_CLIENT_CERT` и `INDEED_AM_CLIENT_KEY_CERT`.

> ⚠ **ВАЖНО**
>
> Для повышения безопасности рекомендуется использовать собственный клиентский сертификат.

Чтобы настроить собственный клиентский сертификат на стороне FreeRADIUS:

1. В каталог *common_certs* добавьте клиентский сертификат (в формате .cer или .crt) и приватный ключ сертификата (в формате .key или .pem).
2. Настройте права владельца файла с сертификатом для пользователя, указанного в переменных окружения `RAD_UID` и `RAD_GID` в файле *.env* для FreeRADIUS.

   ```
   sudo chown <RAD_UID:RAD_GID> * 755
   ```

Кеширование запросов к Core Server

Некоторые запросы к Core Server могут кешироваться:

- `/api/v6/module/getApplicationsDAL`
- `/api/v6/user/searchUserId`
- `/api/v6/logon/getAvailableMethods`
- `/api/v6/authenticationMethod/getEffectiveClientSettings`

Вызов `getApplicationsDAL` кешируется глобально для всех независимых запросов к FreeRADIUS. Время кеширования определяется переменной `AM_CACHE_LIFETIME_SEC` и равно по умолчанию 600 секунд. Если

для `AM_CACHE_LIFETIME_SEC` задать значение 0 секунд, то кеширование не производится.

Для вызовов `searchUserId`, `getAvailableMethods` и `getEffectiveClientSettings` настройка `AM_CACHE_LIFETIME_SEC` не действует, кеширование происходит в рамках сессии всегда:

- внутри сессии многофакторной аутентификации со вторым фактором в виде OTP (challenge-response);
- внутри сессии многофакторной аутентификации со вторым фактором в виде push-уведомления;
- внутри обработчика запроса FreeRADIUS — запрос на доступ (access-request) выполняется один раз, при необходимости данные запроса берутся из кеша.

Настройка LDAP-сервера

Настройте LDAP-сервер, если вы планируете использовать доменный пароль в качестве первого фактора аутентификации. LDAP-сервер используется для проверки первого фактора.

Чтобы настроить LDAP-сервер, откройте файл *.env* с переменными окружения и добавьте или раскомментируйте переменные `LDAP*`. Если переменные `LDAP*` не заданы, проверка первого фактора осуществляется на Core Server.

Подробнее о настройке в Management Console — в разделе Настройка политик.

Настройка одного LDAP-сервера

Настройка одного LDAP-сервера

Чтобы настроить LDAP-сервер, необходимо в файле *.env* раскомментировать переменные `LDAP*` и задать для них значения:

- `LDAP_SERVER` — IP-адрес LDAP-сервера;
- `LDAP_PORT` — порт AD-сервера;
- `LDAP_IDENTITY` — учетная запись AD в формате значения атрибута `distinguishedName`;
- `LDAP_PASSWORD` — пароль к этой учетной записи;
- `LDAP_BASE_DN` — каталог пользователей AD в формате значения атрибута `distinguishedName`, с которыми будет взаимодействие.

Чтобы настроить подключение по защищенному ldaps-соединению, задайте переменную `LDAP_CERT`, указав для нее название файла сертификата. В этом сценарии необходимо оставить значение по умолчанию для переменной `LDAP_PORT` — 636.

Чтобы добавить возможность входа пользователя с использованием NetBIOS имени LDAP-сервера, задайте переменную окружения `LDAP_NETBIOS_NAME`.

Пример

```
LDAP_SERVER=ldaps://dc.example.com
LDAP_PORT=636
LDAP_IDENTITY=cn=Администратор,cn=users,dc=example,dc=com
LDAP_PASSWORD=12345
LDAP_BASE_DN=cn=users,dc=example,dc=com
LDAP_CERT=example.crt
LDAP_NETBIOS_NAME=EXAMPLE
```

Настройка нескольких LDAP-серверов (в одном домене)

Настройка нескольких LDAP-серверов (в одном домене)

Чтобы настроить несколько LDAP-серверов, которые находятся в одном домене, в переменной `LDAP_SERVER` перечислите через пробел IP-адреса LDAP-серверов, например:

```
LDAP_SERVER=dc1.example.com dc2.example.com dc3.example.com
```

Настройка нескольких LDAP-серверов (в разных доменах)

Настройка нескольких LDAP-серверов (в разных доменах)

Чтобы настроить несколько LDAP-серверов, необходимо к наименованию `LDAP` добавить индекс (номер очередного сервера), например: `LDAP_SERVER`, `LDAP1_SERVER`, `LDAP2_SERVER`. Переменная `LDAP_SERVER` без номера в названии также является валидной переменной.

> **ИНФОРМАЦИЯ**
>
> Все переменные, соответствующие LDAP-серверу, задаются с таким же индексом.

Пример

```
LDAP1_SERVER=ldaps://dc.example.com
LDAP1_PORT=636
LDAP1_IDENTITY=cn=Администратор,cn=users,dc=example,dc=com
LDAP1_PASSWORD=12345
LDAP1_BASE_DN=cn=users,dc=example,dc=com
LDAP1_CERT=example.crt
LDAP1_NETBIOS_NAME=EXAMPLE
```

Для нескольких LDAP-серверов необходимо задать значения всех доменов. Значения задаются в одну строку через пробел, например:

```
LDAP1_DOMAIN_NAME=example.com test.com example.org
```

Если задано несколько LDAP-серверов, то выбор LDAP-сервера осуществляется в соответствии со значениями `LDAPN_NETBIOS_NAME` и `LDAPN_DOMAIN_NAME`. Поэтому обязательно должно быть указано либо доменное имя, либо NetBIOS-имя.

Количество LDAP-серверов можно задать переменной окружения `MAX_LDAP_SERVER`. `MAX_LDAP_SERVER` влияет только на переменные `LDAP_SERVER` с индексами. `LDAP_SERVER` (название без индекса) можно задать при значении `MAX_LDAP_SERVER=0`.

Настройка стартовых потоков в пуле соединений

Стартовые потоки — это предварительно созданные соединения с LDAP-сервером. Они позволяют ускорить обработку запросов.

Чтобы задать количество стартовых потоков в пуле соединений с LDAP-серверами при запуске контейнера, настройте переменную `LDAP_START_SERVERS`. Необходимое количество потоков зависит от пропускной

способности сети при соединении FreeRADIUS с LDAP-серверами.

Значение по умолчанию: 5 потоков.

Диапазон значений: от 0 до 64.

- Если установить значение больше 0, то успешное подключение возможно, только если все LDAP-серверы доступны. При этом приложение успешно запустится и все запросы аутентификации или авторизации завершатся успешно.
- Если установить значение 0, то успешное подключение возможно, даже если один из LDAP-серверов недоступен, однако при этом:
    - предварительные соединения не будут созданы, что замедлит обработку запросов;
    - все запросы аутентификации или авторизации завершатся неудачей, если FreeRADIUS не сможет подключиться хотя бы к одному LDAP-серверу.

Indeed LDAP Proxy

Модуль Indeed LDAP Proxy (LDAP Proxy) позволяет реализовать двухфакторную аутентификацию в приложениях, в которых основным методом аутентификации пользователей выступает LDAP-каталог. Модуль LDAP Proxy действует как посредник между LDAP-клиентами и серверами: он перехватывает запросы от клиентов и перенаправляет их на LDAP-серверы.

LDAP Proxy не влияет на проверку имени и пароля пользователя. Проверка доменного пароля происходит при перенаправлении запроса в каталог пользователей. Второй фактор запрашивается только после успешной проверки учетной записи в конечном каталоге пользователей.

С помощью модуля LDAP Proxy вы можете выполнить аутентификацию по следующим методам:

- доменный пароль;
- доменный пароль + Indeed Key (в режиме отправки push-уведомлений с подтверждением входа);
- доменный пароль + Telegram (в режиме отправки push-уведомлений с подтверждением входа).

> ⚠ **ВАЖНО**
>
> Чтобы настроить доступ для сервисных учетных записей без использования второго фактора, в Management Console создайте отдельную политику, в которой в качестве метода аутентификации выбран доменный пароль.
>
> Добавьте в эту политику сервисную учетную запись Access Manager и сервисные учетные записи, которые используются в клиентах LDAP Proxy для чтения каталога.

Установка LDAP Proxy

Чтобы установить и настроить модуль LDAP Proxy на отдельном хосте:

1. Импортируйте образ Docker.
2. Сгенерируйте служебные сертификаты.
3. Внесите изменения в конфигурационные файлы.
4. Создайте каталог для хранения логов и настройте права пользователя.
5. Запустите контейнер с приложением.

Импорт образа Docker

1. Скачайте архив компонента *am_images/ldap-proxy.tar.gz* и загрузите его на целевой хост в необходимый каталог.

   Если компонент устанавливается на отдельном хосте, вместе с архивом компонента скопируйте и импортируйте архивы *haproxy.tar.gz* и *tools.tar.gz*.

> **ПРИМЕЧАНИЕ**
>
> Если в вашей версии АМ нет каталога *am_images*, для установки используйте общий архив *am-<номер_версии>.tar.gz*.

2. Перейдите в каталог с архивом и распакуйте его с помощью команды:

```
sudo tar -xf ldap-proxy.tar.gz
```

3. Перейдите в каталог с распакованным архивом и импортируйте образ Docker с помощью команды:

```
sudo docker load -i ldap-proxy.tar
```

4. Ограничьте права запуска для всех пользователей системы, не имеющих прав `sudo`. В каталоге *ssl* выполните команду:

```
sudo chmod 400 *.sh
```

Генерация служебных сертификатов

Перед запуском скриптов убедитесь, что в каталоге *ssl* находятся только скрипты и добавленные ранее сертификаты:

- *ssl/<серверный сертификат>.pfx* — серверный сертификат, выписанный на DNS-имя машины.
- *ssl/ca/<публичный сертификат>.cer* — публичный сертификат домена в формате Base64. Если публичный сертификат выдан не доменным удостоверяющим центром (УЦ), добавьте публичный сертификат стороннего УЦ.

Запустите следующие скрипты в каталоге *ssl*:

1. Сконвертируйте *.pfx* в сертификат HAProxy:

```
sudo bash ./convertPfxForReverseProxy.sh -f <серверный сертификат>.pfx -p
<пароль>
```

   Результат: создается серверный сертификат *am/ssl/https/reverse_proxy_server.pem*, предоставляющий HAProxy для внешних клиентов (Api Core, WebUI MC, UC и IDP).

2. Сгенерируйте HTTPS-сертификаты контейнеров для использования внутри сети Docker:

```
sudo bash ./generateHttpsCerts.sh
```

Результат: создаются сертификаты *am/ssl/https/<service>.pfx* для сервисов LDAP Proxy, Core, MC, UC, IDP и Log Server. Расположение и пароли сертификатов указаны в конфигурационных файлах компонентов.

3. Сгенерируйте сертификат, которому будут доверять контейнеры:

```
sudo bash ./prepareCaFile.sh
```

Результат: создается сертификат *am/ssl/ca/trusted_ca.crt*, который содержит список всех добавленных в *am/ssl/ca* публичных сертификатов.

> **ПРИМЕЧАНИЕ**
>
> При изменении состава каталога *am/ssl/ca* перезапустите скрипт *prepareCaFile.sh*.

Редактирование конфигурационных файлов

Редактирование файла am/.env

- `COMPOSE_PROFILES` — добавьте значение `ldap-proxy` и удалите значения компонентов, которые установлены на других хостах.
- `ENDPOINT_NAME_THIS_HOST` — укажите DNS-имя хоста, на котором вы устанавливаете LDAP Proxy.
- `ENDPOINT_NAME_CORE` — укажите DNS-имя хоста, на котором установлен Core Server.
- `LDAP_PROXY_PORT` — укажите порт, на который будут отправляться запросы. Для настройки подключения по протоколу LDAPS задайте значение 636, для LDAP — 389.

Редактирование файла am/haproxy.docker-compose.yml

1. В блоке `depends_on` раскомментируйте строку `ldap-proxy` и при необходимости закомментируйте строки с остальными компонентами, установленными на других хостах.

Пример

```
 depends_on:
#  - core
#  - idp
#  - mc
#  - uc
#  - ls
#  - indeed-key
  - ldap-proxy
```

2. В блоке `ports` раскомментируйте строку с указанием порта.

   - Для настройки подключения по протоколу LDAPS:

     ```
     -"${LDAP_PROXY_PORT}:9636"
     ```

   - Для настройки подключения по протоколу LDAP:

     ```
     -"${LDAP_PROXY_PORT}:9389"
     ```

Редактирование файла am/haproxy/haproxy.cfg

Чтобы задать подключение по протоколу LDAPS или LDAP, внесите следующие правки.

LDAPS (рекомендуется)

1. Убедитесь, что следующая строка раскомментирована:

   ```
   bind *:9636 ssl crt server.pem crt-ignore-err all ssl-min-ver TLSv1.2 ssl-
   max-ver TLSv1.2 verify optional ca-file trusted_ca.crt
   ```

2. Раскомментируйте строки:

   ```
   default_backend LDAP_Proxy_Backend
   ```

   ```
   server haproxy localhost:9999 send-proxy track
   ldaps_transmitter_backend/docker
   ```

   ```
   backend LDAP_Proxy_Backend
   mode tcp
   ```

```
frontend ldap_reciever_frontend
mode tcp
bind localhost:9999
default_backend ldaps_transmitter_backend

backend ldaps_transmitter_backend
mode tcp
server docker ldap-proxy:636 check port 637 inter 5000ms ssl verify required
ca-file trusted_ca.crt
```

LDAP

1. Закомментируйте строку:

```
#    bind *:9636 ssl crt server.pem crt-ignore-err all ssl-min-ver TLSv1.2
ssl-max-ver TLSv1.2 verify optional ca-file trusted_ca.crt
```

2. Раскомментируйте строки:

```
bind *:9389
```

```
default_backend LDAP_Proxy_Backend
```

```
backend LDAP_Proxy_Backend
mode tcp
```

```
server docker ldap-proxy:389 check port 637 inter 5000ms send-proxy
```

При необходимости закомментируйте строки, связанные с компонентами, которые установлены на других хостах.

- Строки с параметром `acl`, в которых упоминаются компоненты. Пример: `acl path-mc path_beg -i /am/mc`.
- В параметре `http-request reject unless` удалите компоненты, которые установлены на других хостах, и лишние разделители `||`.
- Строки с параметром `use_backend`. Пример: `use_backend MC_Backend if path-mc`.

- Строки с адресом компонента в параметре `backend <серверный_компонент>_Backend`.

Редактирование файла am/ldap-proxy/app-settings.json

Пример файла *am/ldap-proxy/app-settings.json*

```
{
  "ProxyServer": {
    "Port": "636",
    "HealthCheckPort": "637",
    "UseTls": true,
    "Certificate": {
      "Path": "/ssl/proxy.pfx",
      "Password": "Q1w2e3r4"
    }
  },
  "LdapServer": {
    "Address": "dc.indeed.local",
    "Port": "636",
    "UseTls": true,
    "Certificate": {
      "Path": "/ssl/ldap-proxy/server_cert.pfx",
      "Password": "Q1w2e3r4"
    },
    "ConnectTimeout": "00:00:03"
  },
  "AuthenticationServer": {
    "IgnoreCertErrors": true
  },
  "InteractionTimeouts": {
    "IdleTimeout": "00:10:00",
    "PushTimeout": "00:00:30"
  }
}
```

1. В блоке `ProxyServer` задайте настройки для приема входящих LDAP-запросов от клиентов.
   - `Port` — порт, на который будут отправляться запросы. Доступные значения: `636` для LDAPS, `389` для LDAP.
2. В блоке `LdapServer` задайте настройки для запросов между LDAP Proxy и сервером LDAP.

- `Address` — IP-адрес LDAP-сервера. Если в параметре задано имя домена, то автоматически выбирается один из доступных контроллеров домена. Пример: `gma.local`.
- `Port` — порт, на который будут отправляться запросы. Доступные значения: `636` для LDAPS, `389` для LDAP.
- `UseTls` — параметр задает подключение по протоколу LDAPS или LDAP между LDAP Proxy и сервером LDAP. Доступные значения: `true` для LDAPS, `false` для LDAP.

3. (Опционально) В блоке `InteractionTimeouts` можно задать настройки тайм-аута.
   - `IdleTimeout` — максимальное время, в течение которого не происходит чтение и запись данных. По истечении заданного времени прерывается соединение с клиентом. Значение по умолчанию: 00:10:00 (10 минут).
   - `PushTimeout` — максимальное время, в течение которого пользователь может подтвердить второй фактор аутентификации. По истечении заданного времени прерывается соединение с клиентом. Значение по умолчанию: 00:00:30 (30 секунд).

Создание каталогов и настройка прав

1. Чтобы создать каталоги для хранения логов и ключей шифрования, из каталога *am* запустите команду:

```
sudo mkdir ldap-proxy/Logs/ ldap-proxy/DataProtectionKeys/
```

2. Чтобы выдать права пользователю, указанному в файле *.env* в переменных `AM_UID` и `AM_GID`, запустите команду:

```
sudo chown -R <AM_UID>:<AM_GID> ./*
```

Запуск контейнера

Запустите контейнер с приложением с помощью команды:

```
sudo docker-compose up -d
```

После запуска настройте интеграцию с бизнес-приложениями в Management Console.

Включить/Отключить шифрование конфигурационного файла

1. В терминале перейдите в каталог с утилитой для шифрования *am/protection*.

```
cd /am/protection
```

2. Выдайте права для запуска скрипта `protector.sh`.

```
sudo chmod 500 protector.sh
```

3. Чтобы зашифровать конфигурационные файлы, запустите скрипт `protector.sh` с параметром `protect`.

```
sudo bash ./protector.sh protect
```

4. Чтобы расшифровать конфигурационные файлы, запустите скрипт `protector.sh` с параметром `unprotect`.

```
sudo bash ./protector.sh unprotect
```

Двустороннее TLS-соединение

Чтобы установить двустороннее TLS-соединение между серверами Indeed LDAP Proxy и сервером LDAP:

1. Сгенерируйте клиентский сертификат.

   Этот сертификат выпускается в центре сертификации на DNS-имя машины с установленным LDAP Proxy. За основу можно взять шаблон сертификата *Компьютер* в доменном центре сертификации Windows.

2. Добавьте *<клиентский сертификат>.pfx* в каталог *am/ssl/ldap-proxy* на хосте, где установлен модуль LDAP Proxy.

3. В конфигурационном файле *am/ldap-proxy/app-settings.json* укажите следующие параметры, которые требуются при взаимной проверке сертификатов между LDAP-сервером и клиентом (взаимная TLS-аутентификация):

   - `LdapServer:Certificate:Path` — имя клиентского сертификата.
   - `LdapServer:Certificate:Password` — пароль сертификата.

   ```
   "LdapServer": {
    "Address": "dc.indeed.local",
    "Port": "636",
    "UseTls": true,
    "Certificate": {
      "Path": "/ssl/ldap-proxy/<клиентский сертификат>.pfx",
      "Password": "Q1w2e3r4"
    },
   ```

Сбор логов

Информация по включению логирования и сбору логов компонента LDAP Proxy находится в разделе Сбор логов компонентов Access Manager.

Indeed RDP Windows Logon

Модуль Indeed RDP Windows Logon (RDP Windows Logon) позволяет реализовать двухфакторную аутентификацию с помощью Indeed Access Manager в процессе подключения по протоколу RDP (Remote Desktop Protocol) или в приложении Remote App.

В качестве второго фактора могут выступать:

- push-уведомления с подтверждением входа в мобильном приложении Indeed Key,
- Email OTP,
- SMS OTP,
- Secured TOTP,
- Software OTP,
- Passcode,
- Hardware TOTP,
- Hardware OTP.

Порядок установки

Чтобы использовать модуль RDP Windows Logon:

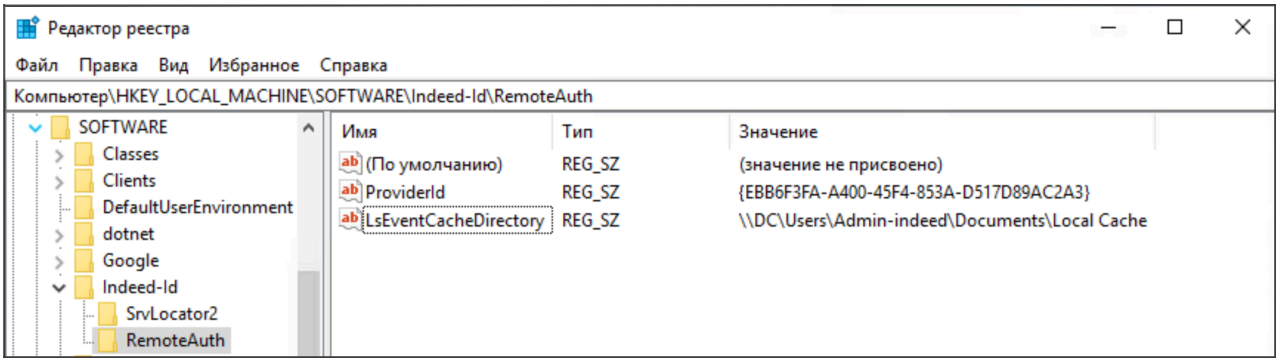
1. Включите NLA (Network Level Authentication) для пользователя.
2. При использовании соединения по протоколу HTTPS установите клиентский сертификат на каждый сервер Indeed.
3. Установите и настройте RDP Windows Logon.
4. Настройте выбор провайдера аутентификации на стороне пользователя.
5. При необходимости задайте опциональные настройки.

Установка и настройка RDP Windows Logon

1. Запустите файл для установки, расположенный по пути *Indeed AM <номер версии>/Indeed AM RDP Windows Logon/<номер версии>*, и следуйте шагам мастера установки.
2. Откройте редактор реестра Windows.
3. В разделе *HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID* создайте раздел `RemoteAuth`.
4. В разделе `RemoteAuth` создайте строковый параметр `ProviderId` и задайте значение, соответствующее используемому провайдеру.

Возможные значения `ProviderId`

- SMS OTP {EBB6F3FA-A400-45F4-853A-D517D89AC2A3}
- Email OTP {093F612B-727E-44E7-9C95-095F07CBB94B}
- Passcode {F696F05D-5466-42b4-BF52-21BEE1CB9529}
- Software OTP {0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0}
- Secured TOTP {F15FD7EC-19EA-4384-846E-A2D0BE149FA2}
- Hardware OTP {AD3FBA95-AE99-4773-93A3-6530A29C7556}
- Hardware TOTP {CEB3FEAF-86ED-4A5A-BD3F-6A7B6E60CA05}
- Indeed Key (только в режиме push-уведомлений с подтверждением входа) {DEEF0CB8-AD2F-4B89-964A-B6C7ECA80C68}

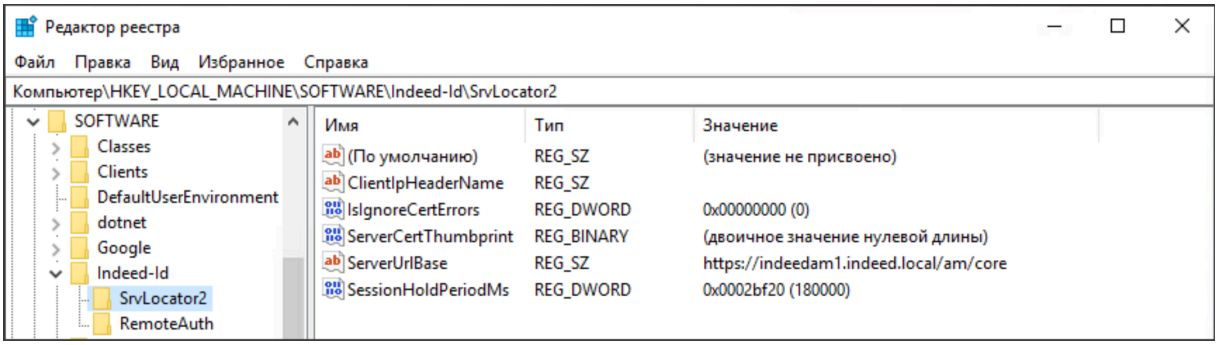


5. В разделе *HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\SrvLocator2* измените следующие параметры:

- В параметре `ServerUrlBase` укажите URL вашего Core Server в формате *http(s)://полное_dns_имя_сервера/am/core*.

> ⚠ **ВАЖНО!**
>
> В настройках приложения URL не должен содержать косую черту (/) в конце адреса.

- В параметре `IsIgnoreCertErrors` укажите значение *0* или *1*. Этот параметр предназначен для проверки сертификата Core Server, при значении *1* ошибки сертификата игнорируются.



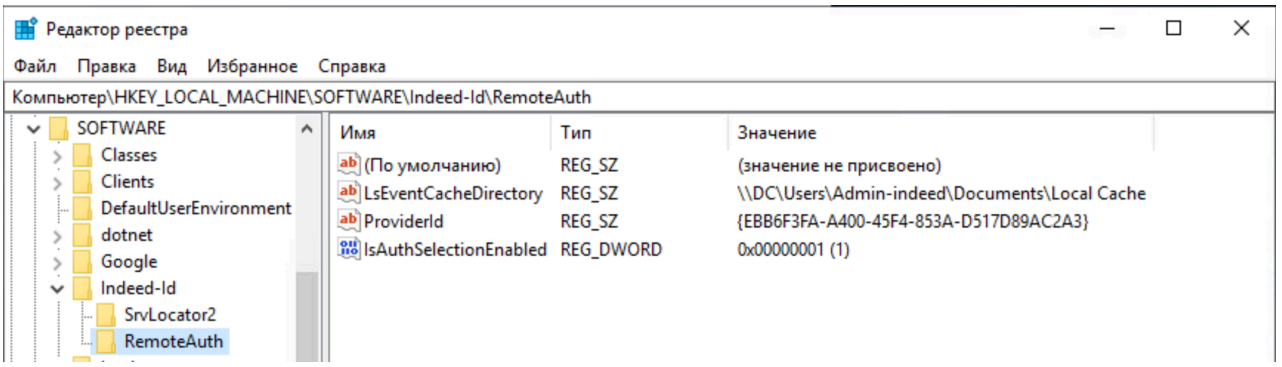
Настройка выбора провайдера аутентификации для пользователя

1. В реестре Windows в разделе *HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\RemoteAuth* создайте параметр DWORD с именем `IsAuthSelectionEnabled`.

2. В значении параметра `IsAuthSelectionEnabled` укажите *1*.

   Если параметр не задан или его значение равно *0*, то выбор провайдера аутентификации предоставляться не будет. В этом случае будут отображаться все доступные методы аутентификации.

   Если `IsAuthSelectionEnabled=1` и указан провайдер в `ProviderId`, то при подключении пользователя будет выбран указанный провайдер. При этом пользователь сможет выбрать любой другой из числа поддерживаемых.

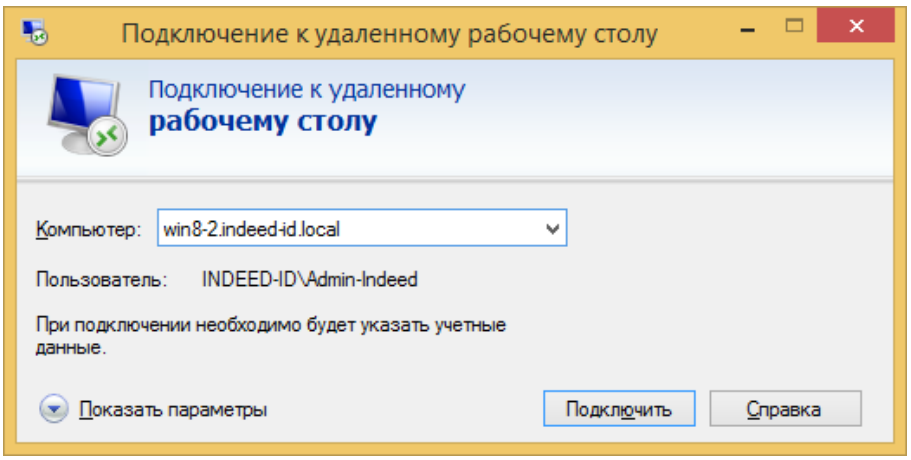


Опциональные настройки

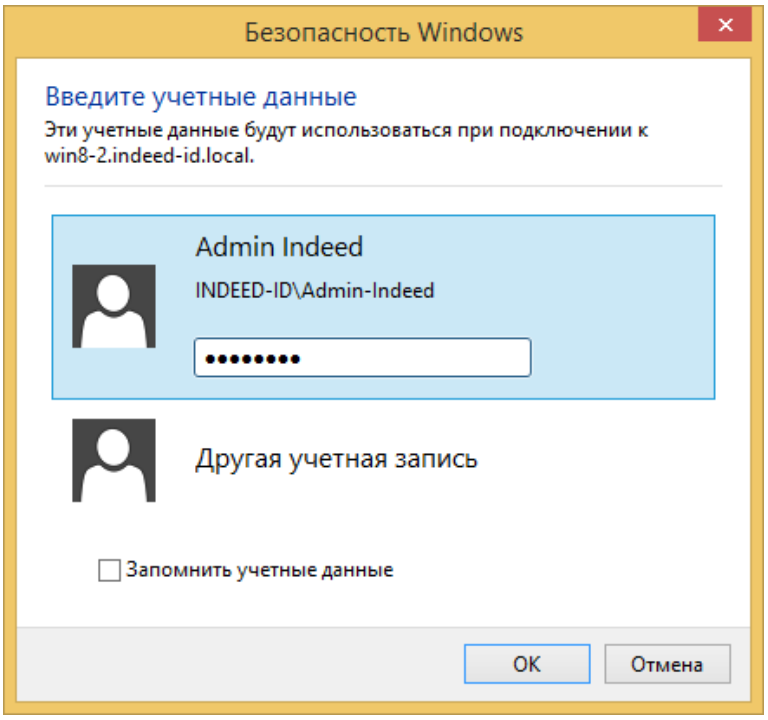
- Аутентификация пользователей без лицензии.
- Настройка срока хранения сессии.
- Одновременная работа с Indeed Windows Logon.

Пример работы модуля

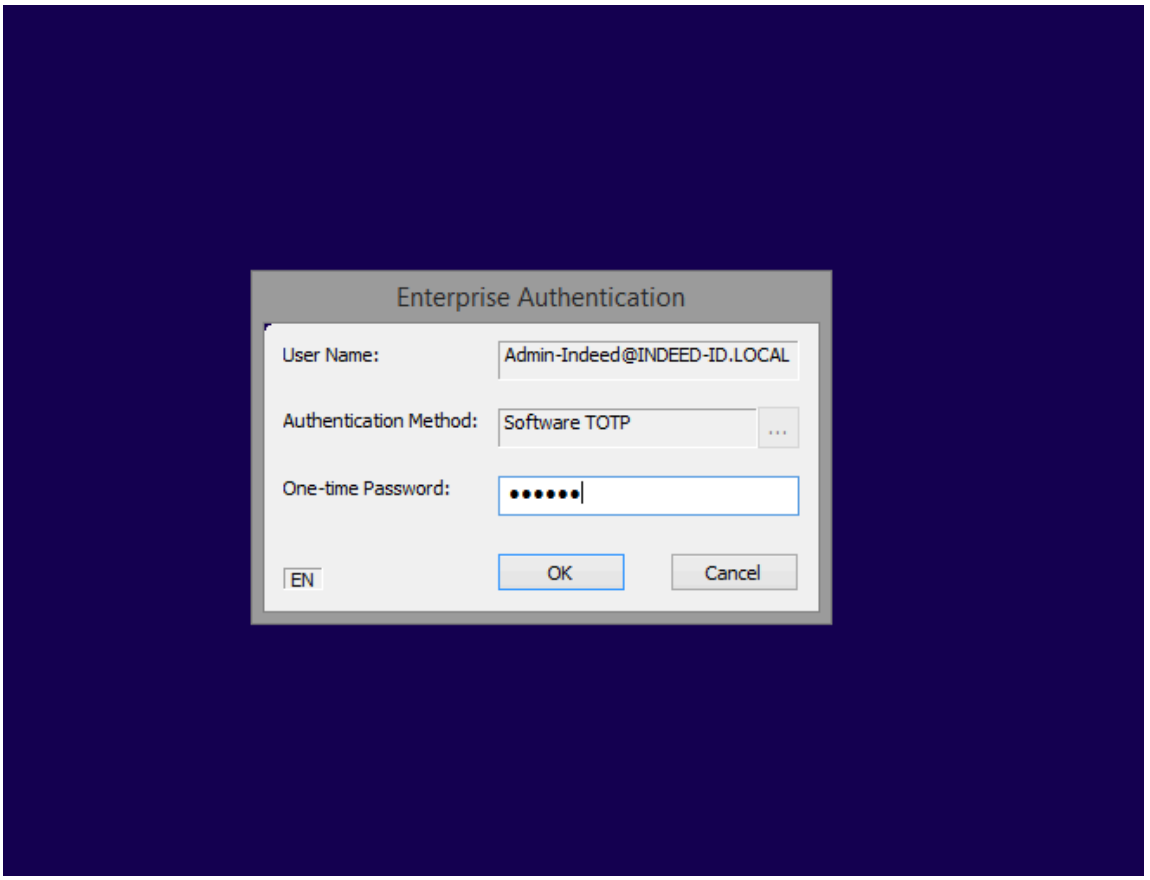
1. Подключитесь к машине, на которой установлен RDP Windows Logon.



2. Укажите пользователя и доменный пароль и нажмите ОК.



3. Введите одноразовый пароль.



ПРИМЕЧАНИЕ

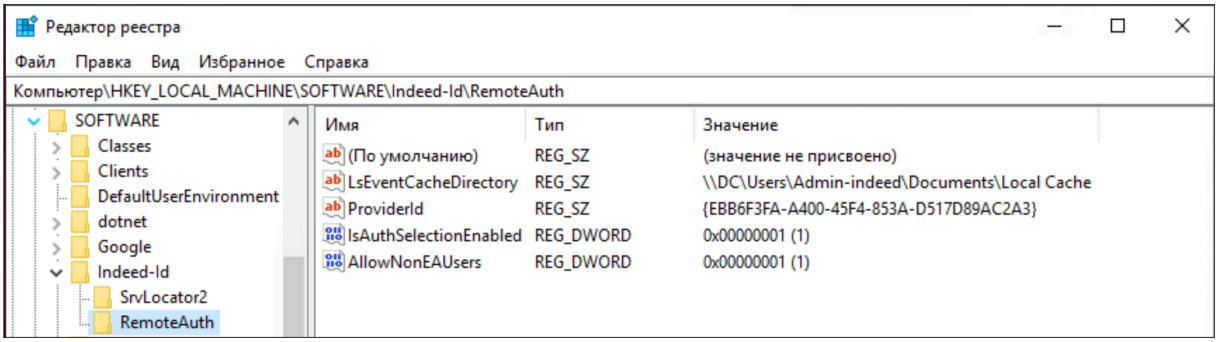
Если у пользователя нет доступных способов аутентификации, отображается сообщение *Нет доступных способов аутентификации. Доступ запрещен.* и сессия Remote Desktop завершается.

Аутентификация пользователей без лицензии

По умолчанию RDP Windows Logon работает с пользователями, обладающими лицензией *AM RDP Windows Logon*.

Тем не менее, можно настроить аутентификацию пользователей без лицензии. Для этого:

1. Откройте редактор реестра Windows.
2. В разделе *HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\RemoteAuth* создайте параметр `DWORD` с именем `AllowNonEAUsers`:
   - Если значение параметра `AllowNonEAUsers` равно *1*, то пользователи без лицензии RDP Windows Logon смогут аутентифицироваться по доменному паролю (без использования технологии Indeed).
   - Если значение параметра `AllowNonEAUsers` равно *0* или не задано, то аутентификация осуществляется только для пользователей с лицензией RDP Windows Logon. Пользователь без лицензии аутентифицироваться не сможет.



Сценарии работы параметра

- Если пользователь находится вне пользовательского каталога Indeed — на пользователя действует настройка *AllowNonEAUsers*, пользователь не сможет аутентифицироваться, если значение параметра не равно *1*.
- Если пользователь находится в пользовательском каталоге без лицензии, но в политике для пользователя нет приложения или пользователь не состоит в политике — на пользователя действует настройка *AllowNonEAUsers*, пользователи не смогут аутентифицироваться, если значение параметра не равно *1*.
- Если пользователь находится в пользовательском каталоге без лицензии и в политике пользователя есть приложение — на пользователя не действует настройка *AllowNonEAUsers*. Всегда происходит попытка входа с автозахватом лицензии.

Настройка срока хранения сессии

При кратковременных разрывах подключения к Core Sever можно настроить период, в течение которого сессию можно будет использовать повторно.

В течение заданного периода сессия хранится в кеше и может быть повторно использована при запросе на новое соединение с сервером. При этом проверка работоспособности сервера повторно не происходит, вместо этого используется закешированный результат проверки.

По истечении периода хранения сессия завершается. По новому запросу на соединение с сервером создается новая сессия.

Чтобы настроить срок хранения сессии в кеше:

Через GPO

1. Откройте редактор GPO.
2. Откройте раздел Конфигурация компьютера → Административные шаблоны → Indeed ID → Client Connection.
3. Включите политику Настройки подключения к серверу.
4. В свойствах политики задайте нужное значение для параметра Период удержания объекта сессии (мс). Значение по умолчанию — 180000 мс (3 минуты).

Через реестр

1. Откройте редактор реестра.
2. Откройте раздел Компьютер\HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\SrvLocator2.
3. Для параметра `SessionHoldPeriodMs` типа *DWORD* установите нужное значение. Значение по умолчанию — 180000 мс (3 минуты).

Одновременная работа с Indeed Windows Logon

Если модули Windows Logon и RDP Windows Logon установлены на одном устройстве, настройте политику для Windows Logon.

Через GPO

1. Перейдите на устройство, на котором установлены модули RDP Windows Logon и Windows Logon.
2. Откройте редактор GPO.
3. Откройте раздел Конфигурация компьютера → Административные шаблоны → Indeed ID → Windows Logon.
4. Включите политику Настройки Credential Provider.
5. Для параметра Отображение способов входа выберите значение Все, кроме пароля.

Через реестр

1. Перейдите на устройство, на котором установлены модули RDP Windows Logon и Windows Logon.
2. Откройте редактор реестра.
3. Откройте раздел Компьютер\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Logon for Windows.
4. Создайте параметр типа *DWORD* с именем `CredProvFilter` и установите ему значение *2*.

Indeed Linux Logon

Indeed Linux Logon (Linux Logon) позволяет реализовать двухфакторную аутентификацию в операционной системе Linux. Первым фактором выступает пароль учетной записи, вторым — следующие технологии аутентификации:

- доменный пароль
- Passcode
- Secured TOTP
- Software OTP
- MFA Provider

> ⚠ **ВАЖНО**
>
> При настройке модуля Linux Logon в Management Console отобразится полный список аутентификаторов, доступных в Access Manager. На данный момент Linux Logon поддерживает только описанные выше аутентификаторы — выбирайте нужные из этого списка.

Предварительные настройки

Системные требования

Прежде чем перейти к установке и настройке модуля Linux Logon:

1. Установите доверенный сертификат.
2. Установите системные библиотеки.

Установка доверенного сертификата

Для повышения уровня безопасности Linux Logon должен подключаться к Core Server по протоколу HTTPS.

Для этого добавьте серверный сертификат Core Server в список доверенных:

1. Перейдите в машину с Core Server и скопируйте серверный сертификат, выписанный на DNS-имя этой машины. Он расположен в директории *ssl/<серверный сертификат>.pfx*.
2. Добавьте *<серверный сертификат>.pfx* на машину с Linux Logon.
3. Преобразуйте сертификат из *.pfx* в *.pem* и введите пароль от сертификата *.pfx*:

```
openssl pkcs12 -in <серверный сертификат>.pfx -clcerts -nokeys -out <серверный сертификат>.pem
```

4. Проверьте содержимое преобразованного сертификата и его формат:

```
cat <серверный сертификат>.pem
file <серверный сертификат>.pem
```

Файл должен содержать блок с данными в формате:

```
-----BEGIN CERTIFICATE-----
[данные сертификата]
-----END CERTIFICATE-----
```

5. Добавьте сертификат в список доверенных. Процесс различается в зависимости от операционной системы и выполняется под пользователем root.

Astra Linux

1. Скопируйте PEM-сертификат в директорию:

```
sudo cp <серверный сертификат>.pem /usr/local/share/ca-certificates/
```

2. Установите права доступа к сертификату:

```
sudo chmod 644 /usr/local/share/ca-certificates/<серверный сертификат>.pem
```

3. Обновите системное хранилище сертификатов:

```
sudo update-ca-certificates
```

В выводе команды должно быть указано:

```
Updating certificates in /etc/ssl/certs...
1 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.
```

РЕД ОС

1. Скопируйте PEM-сертификат в директорию:

```
sudo cp <серверный сертификат>.pem /etc/pki/ca-trust/source/anchors/
```

2. Установите права доступа к сертификату:

```
sudo chmod 644 /etc/pki/ca-trust/source/anchors/<серверный сертификат>.pem
```

3. Обновите системное хранилище сертификатов:

```
sudo update-ca-trust
```

В выводе команды должно быть указано:

```
Updating certificates in /etc/pki/tls/certs/ca-bundle.crt...
Certificate added successfully.
```

Установка зависимостей

Установите системные библиотеки для корректной работы модуля Linux Logon. Установка библиотек различается в зависимости от операционной системы.

Astra Linux

Чтобы установить библиотеки, выполните команду:

```
sudo apt update
sudo apt install libqt5core5a/stable libqt5network5/stable libqt5xml5/stable
libpam0g/stable libfmt9/stable libkrb5-3/stable
```

РЕД ОС

Чтобы установить библиотеки, выполните команду:

```
sudo dnf install qt5-qtbase-5.15.1 pam-1.4.0 fmt9-9.1.0 krb5-libs-1.20.1
```

Установка и настройка Linux Logon

Чтобы установить и настроить Linux Logon:

1. Установите модуль Linux Logon.
2. Настройте интеграцию с инфраструктурой Pluggable Authentication Modules (PAM).

Установка Linux Logon

Модуль Linux Logon устанавливается на машинах под управлением Linux, включенных в домен. Поддерживается только каталог пользователей Active Directory.

Модуль поставляется в виде файла *.deb* для Astra Linux или *.rpm* для РЕД ОС. Установка Linux Logon различается в зависимости от операционной системы.

Astra Linux

1. Чтобы установить Linux Logon, выполните команду:

```
dpkg -i <имя файла>.deb
```

РЕД ОС

1. Чтобы установить Linux Logon, выполните команду:

```
rpm -i <имя файла>.rpm
```

2. Сделайте копию файла */etc/amsvc/amsvc.ini.example* и переименуйте его в *amsvc.ini*.
3. В файле *amsvc.ini* раскомментируйте строки и укажите значения для переменных окружения:
   - `AmURL` — URL-адрес сервера Core Server;
   - `DefaultDomain` — DNS-имя домена;
   - `DefailtNetbiosDomain` — NetBIOS-имя домена.

Пример файла *amsvc.ini*

```
[Service]
AmUrl=https://amdc.indeed.local/am/core/api/v6
DefaultDomain=indeed.local
DefailtNetbiosDomain=INDEED
```

Настройка подключаемых модулей аутентификации (PAM)

Аутентификация через модуль Indeed Linux Logon работает только при интеграции с инфраструктурой Pluggable Authentication Modules (PAM). Настройте конфигурацию цепочки модулей PAM:

1. Настройте SSH.
2. Добавьте Indeed Access Manager в файлы конфигурации с PAM-таблицами.

Настройка SSH

1. Чтобы модуль поддерживал интерактивный режим (Interactive shell) в PAM, добавьте указанные ниже параметры в конфигурационный файл `/etc/ssh/sshd_config`:

   ```
   ChallengeResponseAuthentication yes
   UsePAM yes
   PasswordAuthentication no
   KbdInteractiveAuthentication yes
   ```

2. Если эти параметры активны в других частях файла `sshd_config`, закомментируйте их, иначе SSH может работать некорректно.

3. Чтобы перезапустить службу SSH, используйте команду:

   ```
   systemctl restart sshd
   ```

Настройка ScreenSaver

> **ПРИМЕЧАНИЕ**
>
> Настройка ScreenSaver необходима только для ОС Astra Linux.

Для корректной работы модуля Linux Logon с хранителем экрана (ScreenSaver):

1. Отредактируйте конфигурационный файл `/usr/share/fly-wm/theme.master/themerc` — в переменной `ScreenSaver` поменяйте значение на `internal`:

```
[Variables]
#ScreenSaver="internal fly-modern-locker"
ScreenSaver="internal"
```

2. Сохраните файл и перезагрузите систему.

Генерация PAM-таблиц с помощью скрипта

В состав пакета Linux Logon `/usr/share/amsvc/am-setup` входит скрипт `am-setup.py`, а также файл `README.md` с подробной инструкцией по работе скрипта. Скрипт создает модифицированную версию PAM-таблиц: добавляет в них связи с Indeed Access Manager, не нарушая структуру.

1. Чтобы запустить скрипт, выполните команду:

```
sudo python3 /usr/share/amsvc/am-setup/am-setup.py -i -a
```

2. Проверьте, что в каталоге `/etc/pam.d/` созданы версии PAM-таблиц с расширением `.pam_am`.

   Например, файл *common-auth* в Astra Linux до модификации содержал следующую информацию:

   Пример

```
auth    [success=ignore default=2]      pam_localuser.so
auth    [success=1 default=ignore]      pam_succeed_if.so quiet user ingroup
astra-admin
auth    requisite                       pam_faillock.so preauth audit
per_user deny=8
auth    [success=3 default=ignore]      pam_unix.so nullok try_first_pass
auth    [success=2 default=ignore]      pam_sss.so use_first_pass
auth    required                        pam_faillock.so authfail audit
per_user deny=8

auth    requisite                       pam_deny.so
auth    required                        pam_permit.so
```

   После модификации с помощью скрипта в каталоге появился файл *common-auth.pam_am*:

Пример

```
auth    [success=ignore default=3]      pam_localuser.so
auth    [success=1 default=ignore]      pam_succeed_if.so quiet user ingroup
astra-admin
auth    requisite                       pam_faillock.so preauth audit
per_user deny=8
auth    [success=4 default=ignore]      pam_unix.so nullok try_first_pass
auth    requisite                       pam_am.so
auth    [success=2 default=ignore]      pam_sss.so forward_pass
auth    required                        pam_faillock.so authfail audit
per_user deny=8

auth    requisite                       pam_deny.so
auth    required                        pam_permit.so
```

3. Проверьте, что полученные файлы не противоречат принятой в вашей компании политике безопасности. Так как скрипт выполняет настройку модуля `pam_am.so` на основе конфигурационных файлов с PAM-таблицами, он только предлагает вариант модификации этих таблиц.

   Если предложенный вариант требует корректировки, исправьте файлы `.pam_am` вручную.

4. Удалите из названий файлов расширение `.pam_am`.

Пример для Astra Linux

В каталоге `/etc/pam.d/` созданы файлы `common-auth.pam_am` и `common-password.pam_am`.

Переименуйте файлы в `common-auth` и `common-password`.

Пример для РЕД ОС

В каталоге `/etc/pam.d/` созданы файлы `system-auth.pam_am` и `password-auth.pam_am`.

Переименуйте файлы в `system-auth` и `password-auth`.

5. После настройки таблиц перезапустите сервис:

```
sudo systemctl restart amsvcd.service
```

6. Перезагрузите машину с Linux Logon.
7. (Опционально) Чтобы удалить Access Manager из системных PAM-таблиц:
   - Удалите свои изменения, если вы редактировали таблицы вручную.
   - Выполните команду:

     ```
     sudo python3 /usr/share/amsvc/am-setup/am-setup.py -u -a
     ```

     Скрипт удалит добавленные при установке строки и вернет таблицы в исходное состояние.
   - Проверьте, что из файлов с расширением `.pam_am` удален модуль `pam_am.so`, и удалите расширение из названий файлов.
   - Перезагрузите машину с Linux Logon.

Вход в систему

Перед входом в систему:

1. Зарегистрируйте лицензию модуля и настройте политику в Management Console.
2. Добавьте пользователя в настроенную политику.
3. Настройте провайдеры аутентификации.

Настройка различается в зависимости от операционной системы.

Astra Linux

1. Выберите один метод аутентификации для пользователя в Management Console:
   - MFA,
   - Software OTP,
   - доменный пароль,
   - Secured OTP,
   - Passcode.
2. Зарегистрируйте аутентификатор для пользователя.
3. Сообщите пользователю о выбранном для него методе.

РЕД ОС

1. Выберите один или несколько методов аутентификации для пользователя в Management Console.
2. Если вы выберете несколько провайдеров, они будут предложены пользователю в указанном ниже порядке:
   - MFA,
   - Software OTP,
   - доменный пароль,
   - Secured OTP,
   - Passcode.

> **ПРИМЕР**
>
> В политике выбрано два аутентификатора: Software OTP и Passcode. Software OTP по условиям сортировки стоит в списке выше, поэтому для входа в систему пользователю будет предложен именно он.

3. Зарегистрируйте аутентификаторы для пользователя.

При первом входе в систему пользователю нужно ввести доменный пароль, а при последующих будет использоваться выбранный в политике аутентификатор. Если для пользователя в Management Console уже зарегистрированы доменный пароль и Passcode, при входе в систему ему сразу будет предложен выбранный в политике аутентификатор.

Особенности работы Linux Logon при подключении через RDP

При подключении к системе через протокол Remote Desktop Protocol (RDP) модуль Linux Logon работает со следующими особенностями:

- При аутентификации с помощью MFA в поле пароля необходимо вводить значения аутентификаторов в одну строку без разделителя.

  Пример: в политике выбрано два аутентификатора: Passcode и Software OTP. Значение Passcode — `passcode`, значение Software OTP — `213443`.

  В поле пароля нужно ввести оба значения в одну строку без разделителя: `passcode213443`.

- Нет возможности настроить цепочку многофакторной аутентификации с помощью доменного пароля и Passcode.

- Нет возможности синхронизировать или сменить пароль.

Дополнительные возможности

Модуль Linux Logon позволяет:

Включить генерацию случайного пароля

Чтобы настроить генерацию случайного пароля в свойствах пользователя в Active Directory, отключите опции Запретить смену пароля пользователя и Срок действия пароля не ограничен.

Случайный пароль для учетной записи будет сгенерирован по истечении срока действия текущего пароля. Если для учетной записи был сгенерирован случайный пароль, то следующий вход в систему возможен только с использованием аутентификатора.

Чтобы включить генерацию случайного пароля:

1. На боковой панели Management Console в разделе Политики выберите политику из списка.
2. На вкладке Приложения выберите Linux Logon.
3. Для настройки Пароль учетной записи Active Directory выберите Генерировать случайный.
4. Нажмите Сохранить.

Пароли для всех пользователей в данной политике будут изменены, если это не противоречит их свойствам в Active Directory.

В журнале событий Management Console отобразится событие *1091* Пароль пользователя был успешно сменен автоматически. Пользователи смогут войти в систему только с помощью добавленных аутентификаторов, не используя доменный пароль.

Если доменный пароль изменен администратором, при входе в систему появится сообщение о рассинхронизации пароля. Нажмите ОК и введите пароль, заданный администратором. После этого пароль будет автоматически изменен.

Поддерживать локализацию

Модуль Linux Logon поддерживает вывод системных сообщений на двух языках: русском и английском. Выбор языка происходит автоматически и зависит от языковых настроек операционной системы Linux.

Поддержка локализованных сообщений доступна при смене пользователя и работе в графическом интерфейсе. При входе в систему и подключению по SSH сообщения выводятся только на английском языке.

Список системных сообщений

EN	RU
Can't authenticate	Невозможно аутентифицировать
Input domain password	Введите доменный пароль
An exception occurred: domain password mismatch. To fix the problem, input the domain password or contact your AM administrator.	Возникла исключительная ситуация: сохраненный доменный пароль не подходит. Для решения проблемы введите доменный пароль или обратитесь к вашему администратору AM.
Select method:	Выберите метод:
There are N methods available:	Доступно N методов:
Your password has been successfully updated	Ваш пароль был успешно обновлен
Can't update your password. Please, contact your administrator	Не получилось обновить ваш пароль. Пожалуйста, сообщите об этом вашему администратору

Indeed Windows Logon

Indeed Windows Logon (Windows Logon) предоставляет пользователям:

- доступ в операционную систему по паролю учетной записи;
- доступ в операционную систему с применением доступных технологий аутентификации;
- доступ к удаленному рабочему столу с применением доступных технологий аутентификации;
- доступ в операционную систему по кешированному аутентификатору при отсутствии связи с Core Server.

Windows Logon поддерживает двухфакторную аутентификацию, сертификаты, одноразовые пароли по SMS, электронной почте.

В Windows Logon вы можете выполнить аутентификацию по следующим аутентификаторам:

- Email OTP,
- Hardware OTP,
- Hardware TOTP,
- мобильное приложение Indeed Key в режиме отправки одноразовых паролей и push-уведомлений с подтверждением входа,
- MFA Provider,
- Passcode,
- Secured TOTP,
- SMS OTP,
- Software TOTP,
- Storage SMS OTP,
- Windows Password.

Для безопасности данных при отсутствии пользователя на рабочем месте Windows Logon поддерживает ручную и автоматическую блокировку рабочей станции — при извлечении устройства аутентификации или включении экранной заставки. Независимо от способа блокировки для разблокирования рабочей станции всегда требуется повторное подтверждение личности пользователя с помощью аутентификатора.

Часто задаваемые вопросы о работе Windows Logon

Порядок установки

Чтобы использовать Windows Logon для входа в систему:

1. Установите и настройте модуль Windows Logon.
2. Зарегистрируйте лицензию модуля в Management Console.
3. Установите и настройте провайдеры аутентификации.

Войти в систему по аутентификатору и управлять аутентификаторами можно только при разрешении, выданном администратором системы.

Установка Windows Logon

1. Запустите файл для установки, расположенный по пути *\windows\modules\windows-logon*.
2. После завершения установки компонента нужно перезагрузить систему. В окне мастера установки нажмите Да, чтобы выполнить перезагрузку сразу, или Нет, чтобы сделать это позднее вручную.

> **ПРИМЕЧАНИЕ**
>
> Развернуть Windows Logon на рабочих станциях пользователей в автоматическом режиме можно с помощью механизма групповых политик (Microsoft Group Policy) или любого другого инструмента, который позволяет массово распространять и устанавливать MSI-пакеты на рабочие станции пользователей (например, Microsoft System Center Configuration Manager).

Настройка Windows Logon

Настроить Windows Logon можно через редактор реестра или с помощью групповых политик.

При этом настройки через групповые политики будут приоритетнее настроек, заданных через реестр вручную. Посмотреть настройки групповых политик в реестре можно по пути *HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\SrvLocator2*.

Подробнее о групповых политиках модуля — в разделе Windows Logon.

Через реестр

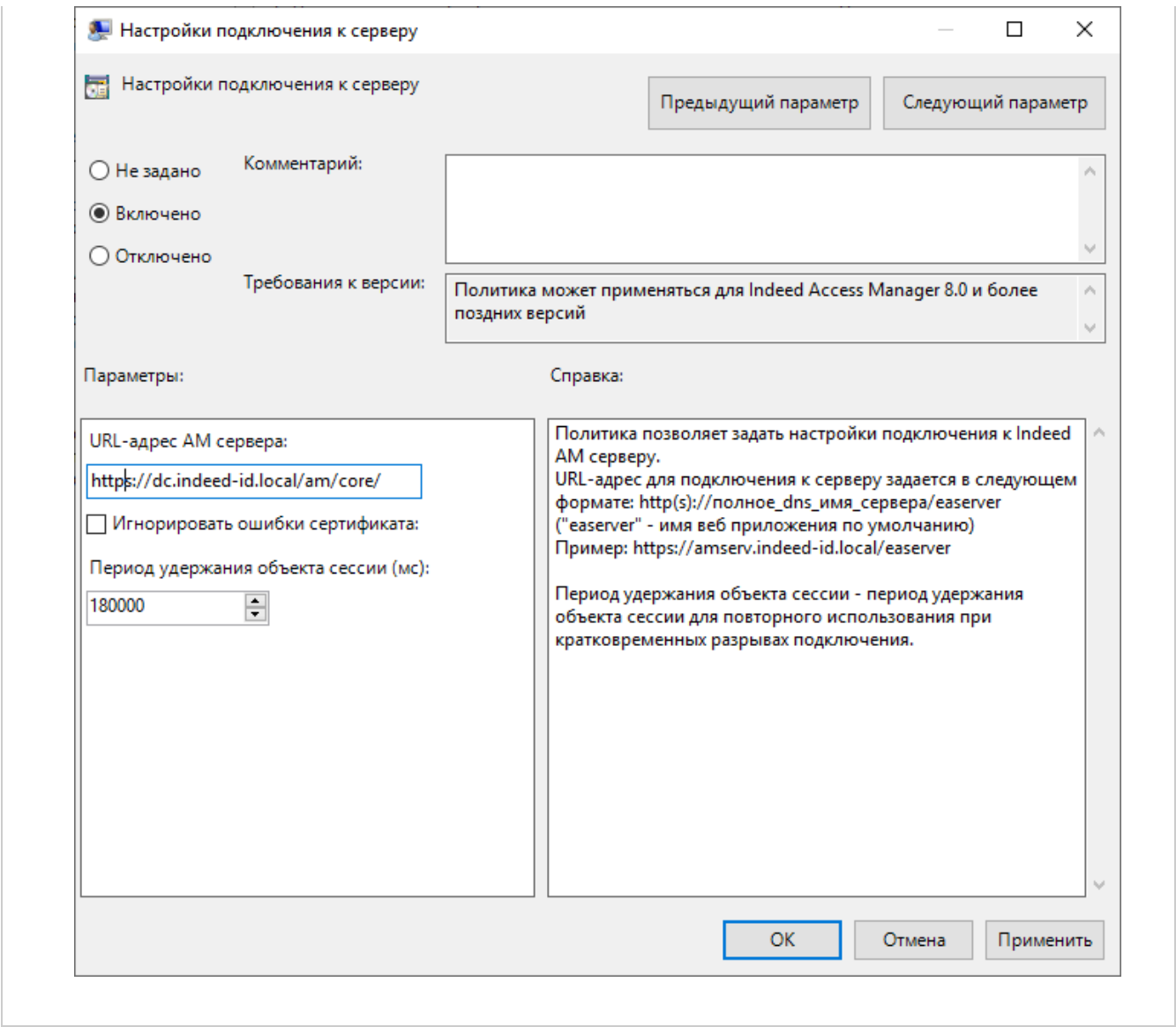
1. Откройте редактор реестра Windows.
2. Перейдите в раздел *HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\SrvLocator2*.
3. Откройте свойства строкового параметра `ServerUrlBase`.
4. В поле Значение укажите URL вашего Core Server в формате *http(s)://полное_dns_имя_сервера/am/core*.

> **ПРИМЕЧАНИЕ**
>
> При использовании соединения по протоколу HTTPS установите клиентский сертификат на каждый Core Server.

Через GPO

> **ПРИМЕЧАНИЕ**
>
> Шаблоны групповых политик расположены в папке *\windows\misc\ADMX Templates*.

1. Добавьте политику *IndeedID.ServerUrl.admx* на устройство с установленным Indeed AM Windows Logon.
2. Откройте редактор GPO.
3. Откройте раздел Конфигурация компьютера → Административные шаблоны → Indeed ID → ClientConnection.
4. Включите политику Настройки подключения к серверу.
5. В поле URL-адрес AM сервера укажите адрес вашего Core Server в формате *http(s)://полное_dns_имя_сервера/am/core*.



Дополнительные возможности

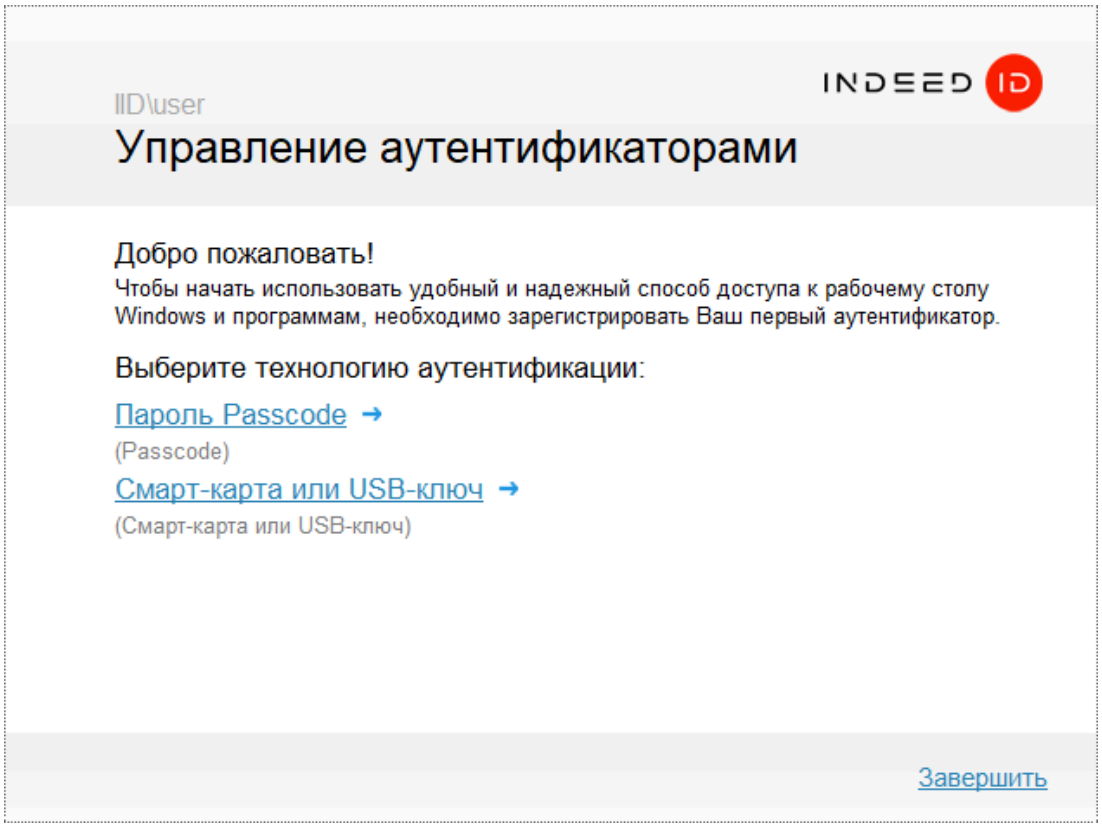
Дополнительные возможности Windows Logon:

- Самостоятельная регистрация и управления аутентификаторами с помощью утилиты управления.
- Генерация случайного пароля для пользователя в Active Directory.
- Функция Indeed AM Paste, которая позволяет автоматически подставить пароль в скрытом виде при нажатии определенной комбинации клавиш.
- Одновременная работа модуля с Indeed RDP Windows Logon.
- Аутентификация средствами Indeed AM при запуске приложения от имени администратора.

Первый вход в систему

Если у пользователя нет зарегистрированных аутентификаторов, для первого входа в систему нужно использовать доменный пароль.

Если пользователю разрешено регистрировать аутентификаторы, то при входе в систему запустится *Мастер первого входа* и предложит зарегистрировать первый аутентификатор.



Можно зарегистрировать аутентификатор сразу или позднее в любое удобное время.

- Чтобы зарегистрировать аутентификатор, в окне Управление аутентификаторами выберите один из доступных способов аутентификации.
- Чтобы войти в систему без регистрации аутентификатора, нажмите Завершить. В этом случае *Мастер первого входа* будет отображаться при каждом следующем входе в систему до регистрации первого аутентификатора.

Если на рабочей станции не обнаружены провайдеры аутентификации, зарегистрировать аутентификаторы будет невозможно. Отобразится ошибка *В системе не обнаружено ни одного провайдера аутентификации. Необходимо установить провайдер и повторно выполнить настройку защищенного входа в систему.*

Если у пользователя настроена аутентификация по SMS OTP или Email OTP, то вход систему будет выполнен по настроенному аутентификатору, после чего появится сообщение о рассинхронизации пароля.

Зарегистрировать первый аутентификатор

Чтобы зарегистрировать первый аутентификатор:

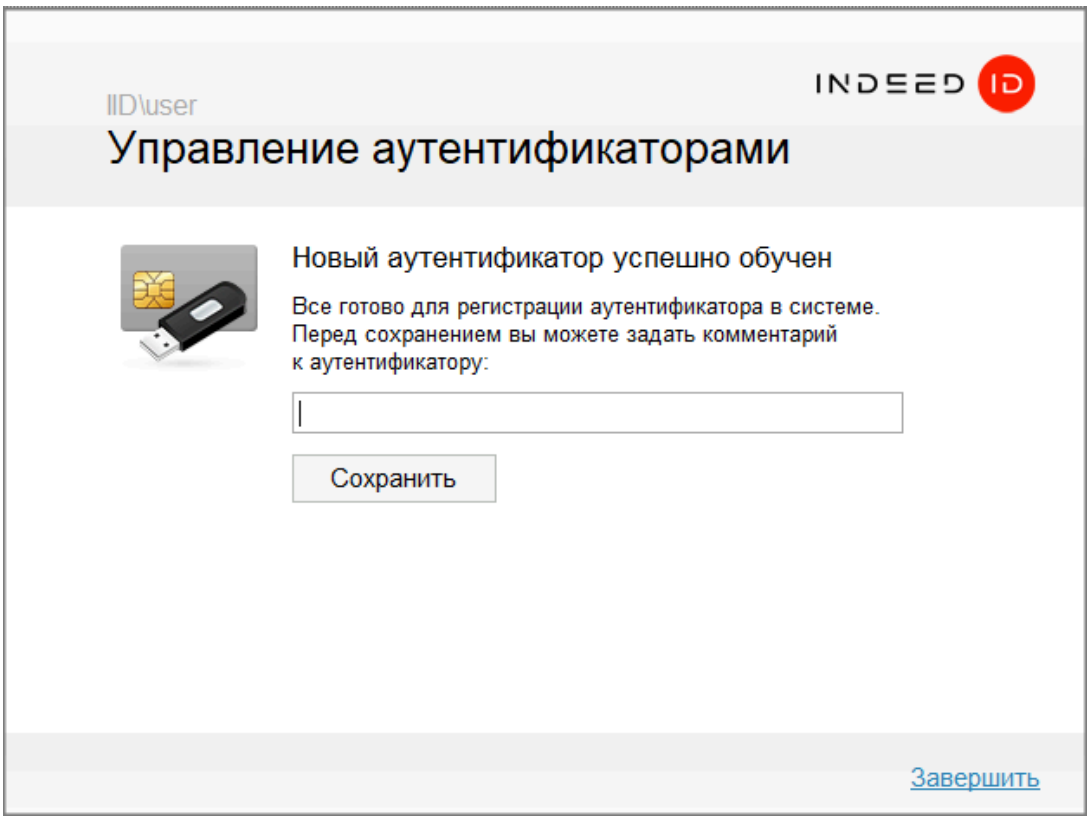
1. В окне мастера выберите способ аутентификации. В окне мастера отображаются установленные аутентификаторы, которые включены в свойствах Windows Logon в карточке политики.

2. Выполните необходимые действия, следуя подсказкам в окне Управление аутентификаторами. Внешний вид окна и действия зависят от выбранного способа аутентификации.

   Если вы хотите вернуться на предыдущую страницу и изменить настройки или выбрать другой способ входа, нажмите Вернуться.

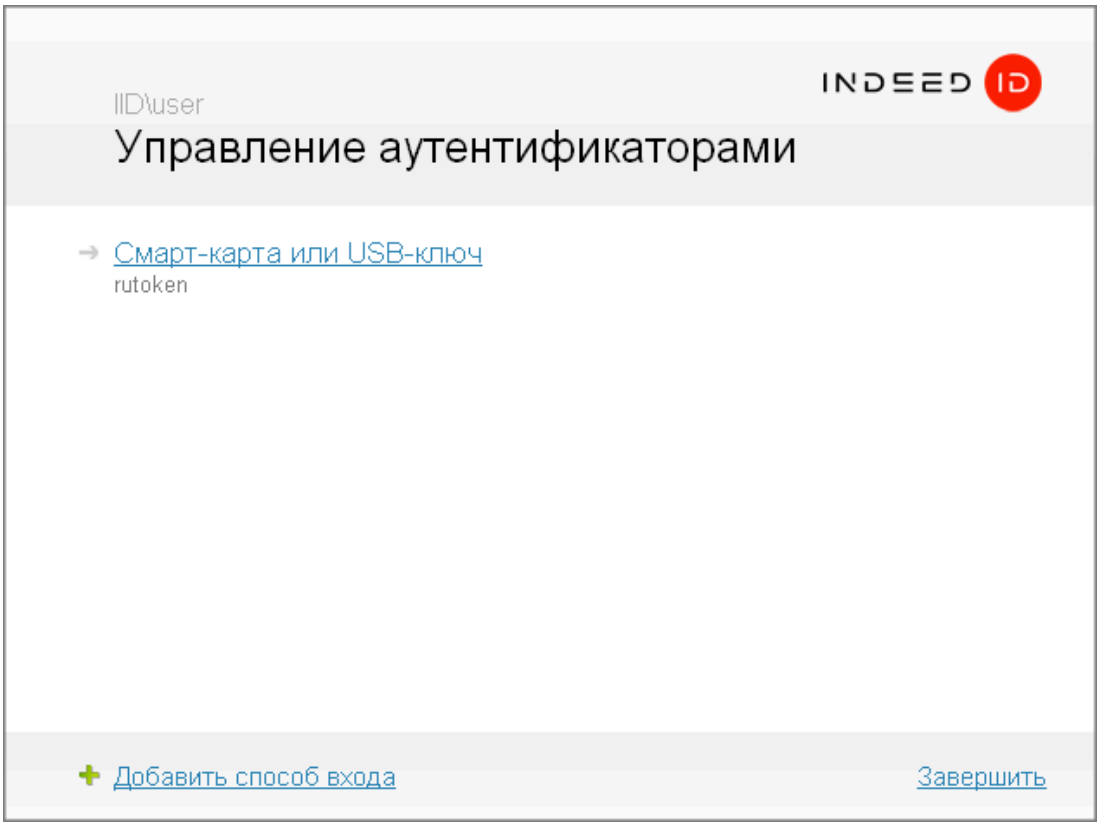
3. После регистрации аутентификатора в окне Управление аутентификаторами отображается сообщение *Новый аутентификатор успешно обучен*. Можно добавить произвольный текстовый комментарий к зарегистрированному аутентификатору, если данное действие разрешено администратором системы.

   Чтобы завершить регистрацию аутентификатора, нажмите Сохранить.



   Тип зарегистрированного аутентификатора и комментарий к нему отобразятся в окне Управление аутентификаторами.

4. Если для пользователю разрешено добавление нескольких аутентификаторов, можно перейти к их регистрации, нажав Добавить способ входа. В зависимости от выданных разрешений, можно также изменить, проверить или удалить зарегистрированный аутентификатор.



При следующем входе в систему будет доступен способ входа по зарегистрированному аутентификатору.

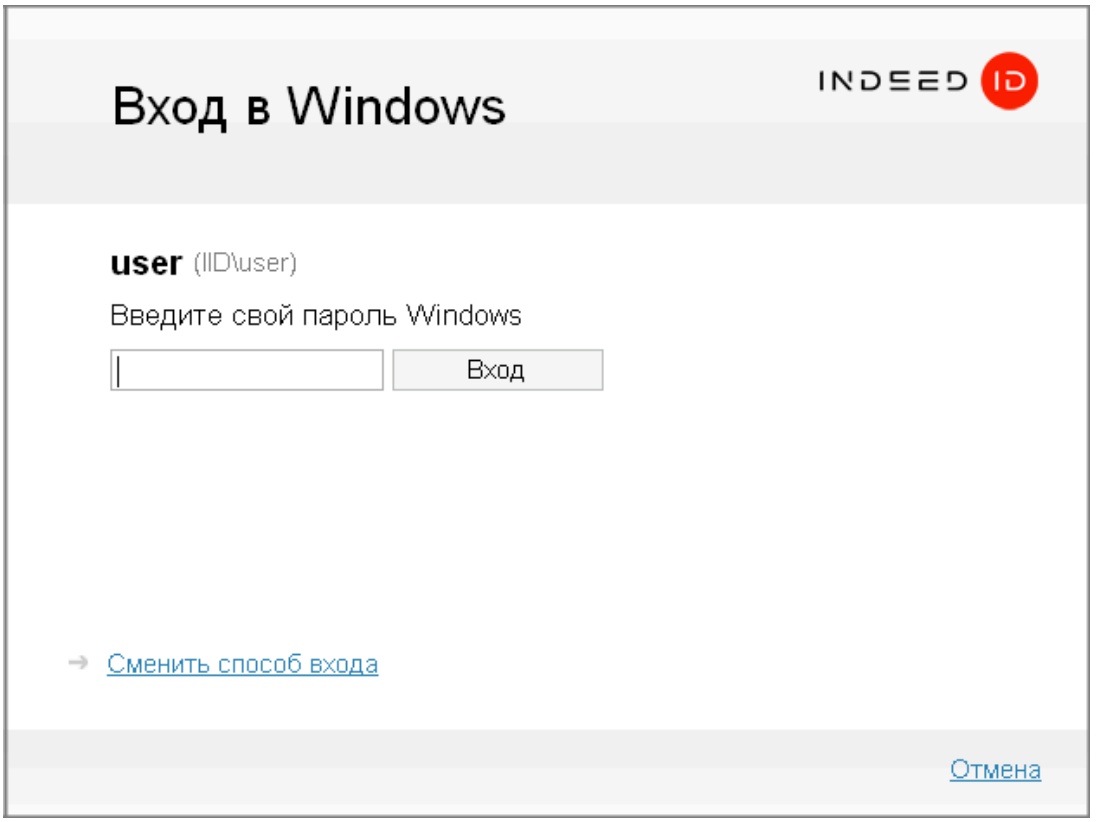
Вход в систему по аутентификатору

Этот способ входа доступен только если:

- вы являетесь лицензированным пользователем Indeed AM,
- для вашей учетной записи разрешена регистрация аутентификаторов,
- вы уже зарегистрировали хотя бы один аутентификатор.

Чтобы войти в систему:

1. После загрузки операционной системы выберите нужного пользователя.
2. В открывшемся окне Вход в Windows отобразится имя пользователя, выполнявшего вход в систему последним и используемый им способ входа.



   Если вы хотите сменить пользователя, нажмите Отмена и выберите учетную запись нужного пользователя.

   Если вы хотите выбрать другой способ входа, нажмите Сменить способ входа и выберите один из способов входа, соответствующий зарегистрированному аутентификатору.

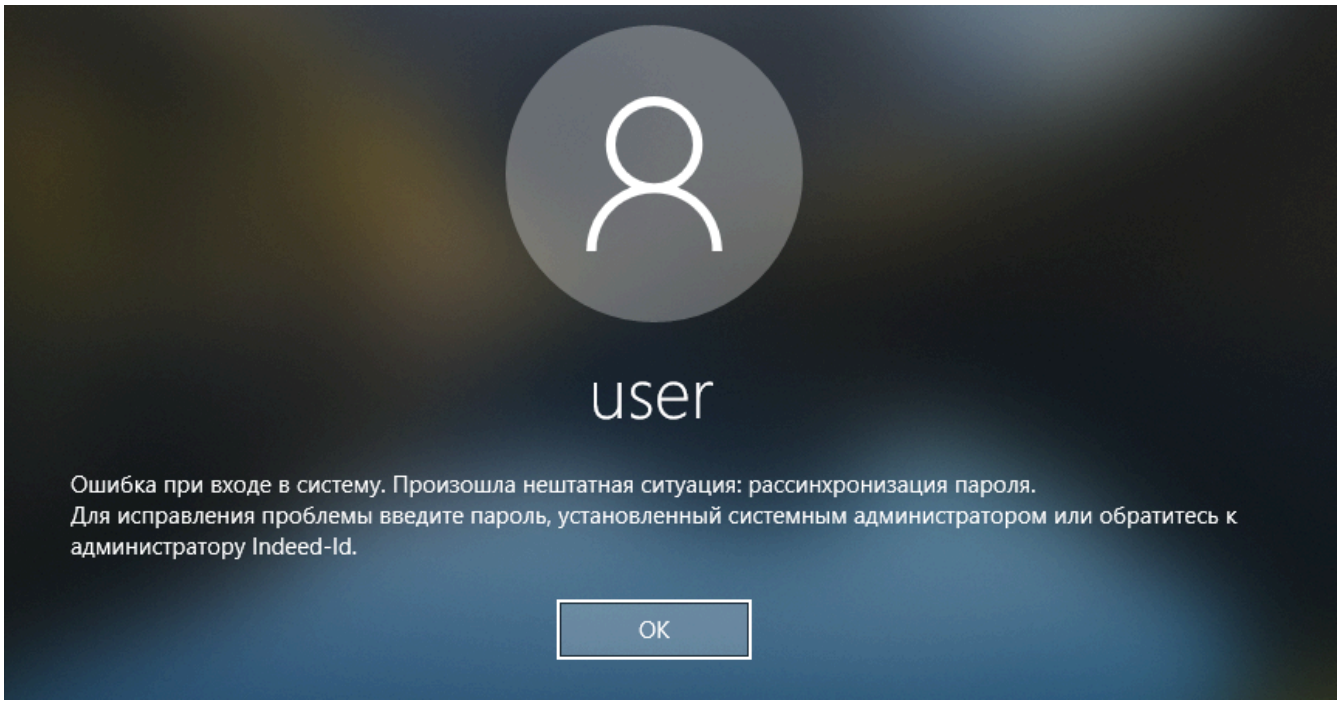
3. После выбора способа входа следуйте подсказкам в окне аутентификации. Внешний вид окна аутентификации и требуемые действия зависят от выбранного типа аутентификатора.

Рассинхронизация пароля

В ряде случаев может произойти рассинхронизация пароля:

- Если доменный пароль сброшен администратором системы, а у пользователя зарегистрирован хотя бы один зарегистрированный аутентификатор.
- Если при запросе на изменение пароля недоступен ни один Core Server, но доступен хотя бы один контроллер домена. В этом случае отображается сообщение *Ошибка связи с сервером. Сервер не найден. Если Вы продолжите, произойдет рассинхронизация пароля.*
- При первом входе в систему, если для пользователя настроена аутентификация по SMS OTP или Email OTP.

Это происходит, когда новый пароль невозможно синхронизировать с базой данных Core Server.



Чтобы синхронизировать пароль:

1. В окне с предупреждением о рассинхронизации нажмите OK.
2. Введите новый пароль.

   Если рассинхронизация произошла из-за недоступности Core Server, выполните эти действия, когда доступен хотя бы один сервер.

Актуальный пароль из Active Directory синхронизируется с паролем в базе данных Core Server. После успешной синхронизации будет выполнен вход в систему.

Доступ к удаленному рабочему столу

Для доступа к удаленному рабочему столу по аутентификатору требуются:

- стандартная утилита Windows *Подключение к удаленному рабочему столу* (mstsc.exe/Remote Desktop) на устройстве, с которого происходит подключение (терминальный клиент);
- модуль Indeed AM Windows Logon, установленный на устройстве, к которому требуется удаленный доступ (терминальный сервер);
- соответствующий провайдер аутентификации, установленный на устройстве, к которому требуется удаленный доступ;
- при использовании Hardware OTP Provider аппаратное устройство аутентификации, подключенное к устройству, с которого происходит подключение;
- отключенная аутентификация на сетевом уровне на устройстве, к которому требуется получить доступ.

Как отключить аутентификацию на сетевом уровне

Через GPO

1. Откройте редактор GPO.
2. Откройте раздел Конфигурация компьютера → Административные шаблоны → Компоненты Windows → Службы удаленных рабочих столов → Узел сеансов удаленных рабочих столов → Безопасность.
3. Отключите политику Требовать проверку подлинности пользователя для удаленных подключений путем проверки подлинности на уровне сети.
4. Включите политику Установить уровень шифрования для клиентских подключений.
5. В параметрах политики для настройки Уровень шифрования выберите значение Высокий уровень.
6. Включите политику Требовать использования специального уровня безопасности для удаленных подключений по протоколу RDP.
7. В параметрах политики для настройки Уровень безопасности выберите значение RDP.

Через реестр

1. Откройте редактор реестра.
2. Откройте раздел Компьютер\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services.
3. Для параметра `UserAuthentication` типа *DWORD* установите значение *0*.
4. Для параметра `MinEncryptionLevel` типа *DWORD* установите значение *3*.
5. Для параметра `SecurityLayer` типа *DWORD* установите значение *0*.

⚠ **ПРЕДУПРЕЖДЕНИЕ**

Если Аутентификация на сетевом уровне (Network Level Authentication, NLA) отключена, снижается уровень безопасности. Поэтому для подключения к удаленному рабочему столу рекомендуется использовать модуль RDP Windows Logon.

Можно также настроить одновременную работу Windows Logon и RDP Windows Logon.

Чтобы подключиться к удаленному рабочему столу по аутентификатору:

1. Запустите Подключение к удаленному рабочему столу.

2. Введите имя или адрес устройства, к которому нужно получить доступ, и нажмите Подключить.
3. В окне Безопасность Windows введите пароль учетной записи и дождитесь подключения.
4. В отобразившемся окне Вход в Windows выберите учетную запись, способ входа (тип аутентификатора) и пройдите аутентификацию.

> **ПРИМЕЧАНИЕ**
>
> Если для учетной записи не включена генерация случайного пароля, можно получить доступ к удаленному рабочему столу по доменному паролю.

Чтобы при подключении к удаленному рабочему столу не запрашивались логин и пароль пользователя, нужно изменить системные настройки. Подробнее — в статье Отключение запроса логина и пароля на стороне терминального клиента.

Опциональные настройки

С помощью Windows Logon вы можете:

Включить генерацию случайного пароля

При использовании модуля Windows Logon можно задать генерацию случайного пароля для пользователя в Active Directory. Для работы этой настройки в свойствах пользователя в Active Directory отключите опции Запретить смену пароля пользователя и Срок действия пароля не ограничен.

Случайный пароль для учетной записи будет сгенерирован по истечении срока действия текущего пароля. Если для учетной записи был сгенерирован случайный пароль, то следующий вход в систему возможен только с использованием аутентификатора.

Чтобы включить генерацию случайного пароля:

1. На боковой панели Management Console перейдите в раздел Политики.
2. Откройте нужную политику.
3. На вкладке Приложения нажмите Windows Logon.
4. Для настройки Пароль учетной записи Active Directory выберите Генерировать случайный.
5. Нажмите Сохранить.

Пароли для всех пользователей в данной политике будут изменены, если это не противоречит их свойствам в Active Directory.

В журнале событий Management Console отобразится событие *1091* Пароль пользователя был успешно сменен автоматически. Пользователи смогут войти в систему только с помощью добавленных аутентификаторов, не используя доменный пароль.

Если у пользователя нет зарегистрированных аутентификаторов, то при первом входе в систему после ввода доменного пароля откроется утилита управления аутентификаторами и предложит зарегистрировать первый аутентификатор.

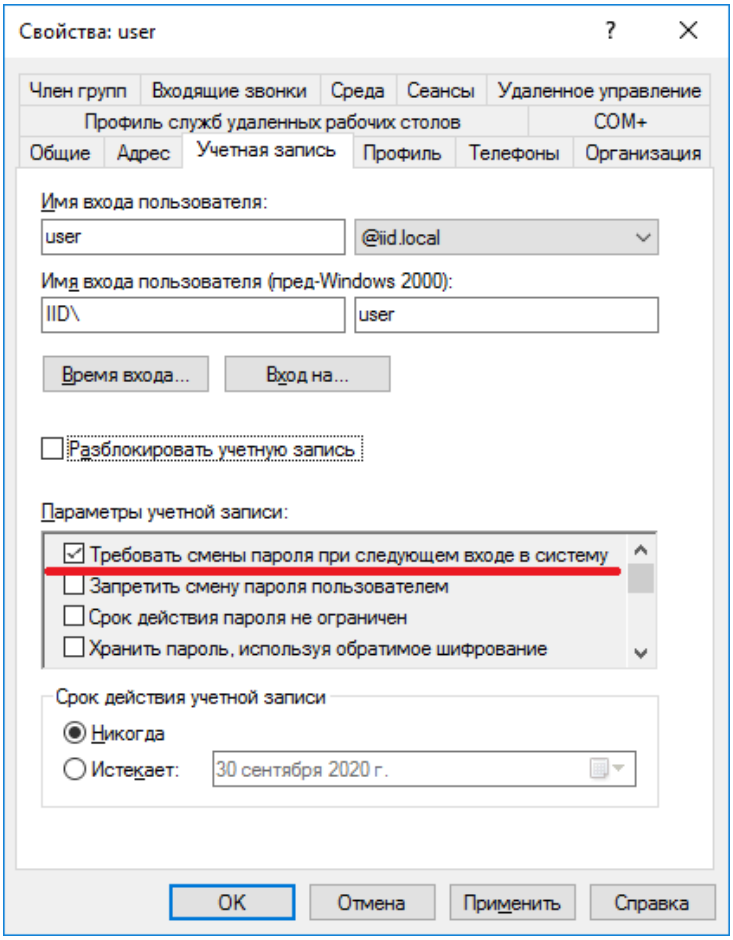
После регистрации аутентификатора происходит генерация и смена пароля пользователя.

Если доменный пароль изменен администратором, при входе в систему появится сообщение о рассинхронизации пароля. Нажмите ОК и введите пароль, заданный администратором. После этого пароль будет автоматически изменен.

> **ИНФОРМАЦИЯ**
>
> Если для учетной записи разрешено кеширование аутентификаторов, то при последующем входе в систему по аутентификатору будет выполнено сохранение данных в локальную память компьютера. Тогда при отсутствии подключения к Core Server войти в систему можно будет с помощью кешированных данных аутентификатора.

Если для пользователя включено требование на смену пароля

Если в свойствах пользователя в Active Directory включено требование на смену доменного пароля и разрешена генерация случайного пароля, то при следующей аутентификации с помощью технологии Indeed будет сгенерирован случайный пароль. При этом отобразится сообщение об успешной автоматической смене пароля.



Настроить автоматическую подстановку скрытого пароля с помощью Indeed AM Paste

Когда для входа в приложение требуется ввести пароль, можно сделать это безопасно с помощью функции Indeed AM Paste. Она позволяет автоматически подставлять скрытый пароль в поле ввода, используя определенную комбинацию клавиш. По умолчанию это *[CTRL] + [ALT] + [V]*.

Включить и отключить функцию Indeed AM Paste можно в приложении Indeed-Id Paste Tool. Для этого:

1. Нажмите правой кнопкой мыши  в области уведомлений Windows.
2. Выберите нужный пункт контекстного меню:

- Разрешить Indeed-Id Paste, чтобы включить или отключить функцию. Функция по умолчанию включена.
- Запускать при загрузке, чтобы Indeed-Id Paste Tool запускалась при загрузке Windows. Эта настройка по умолчанию включена.
- Выход.

Чтобы подставить пароль в скрытом виде:

1. В окне приложения установите курсор в поле ввода пароля.
2. Нажмите комбинацию клавиш для подстановки пароля.
3. Откроется окно Аутентификация. Подтвердите свою личность любым доступным способом.

После успешной аутентификации в поле ввода отображается скрытый пароль.

Настроить одновременную работу с Indeed RDP Windows Logon

Если модули Windows Logon и RDP Windows Logon установлены на одном устройстве, настройте политику для Windows Logon.

Через GPO

1. Перейдите на устройство, на котором установлены модули RDP Windows Logon и Windows Logon.
2. Откройте редактор GPO.
3. Откройте раздел Конфигурация компьютера → Административные шаблоны → Indeed ID → Windows Logon.
4. Включите политику Настройки Credential Provider.
5. Для параметра Отображение способов входа выберите значение Все, кроме пароля.

Через реестр

1. Перейдите на устройство, на котором установлены модули RDP Windows Logon и Windows Logon.
2. Откройте редактор реестра.
3. Откройте раздел Компьютер\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Logon for Windows.
4. Создайте параметр типа *DWORD* с именем `CredProvFilter` и установите ему значение *2*.

Использовать аутентификацию при запуске от имени администратора

На устройствах под управлением Windows 7 модуль Windows Logon выполняет запрос на аутентификацию при использовании команды Запуск от имени администратора. После запуска этой команды отображается диалог выбора учетной записи, затем окно Аутентификация системы Indeed AM. В зависимости от версии операционной системы окно выбора учетной записи может иметь разный вид.

Утилита управления аутентификаторами

> ⚠ **ВАЖНО!**
>
> Утилита управления аутентификаторами работает только в сценариях с модулем Windows Logon.
>
> Утилита устанавливается автоматически при установке этих модулей.

Вы можете управлять аутентификаторами с помощью приложения Indeed AM Управление аутентификаторами. Данное приложение позволяет добавлять новые аутентификаторы, редактировать, проверять и удалять существующие.

> ⓘ **ПРИМЕЧАНИЕ**
>
> Возможности управления аутентификаторами доступны при наличии разрешения, установленного администратором системы.

Для перехода к управлению аутентификаторами выполните следующие действия:

1. Откройте приложение Indeed AM Управление аутентификаторами (Пуск→Indeed AM→Indeed AM Управление аутентификаторами).
2. В окне Аутентификация выберите свою учетную запись и способ входа (тип аутентификатора). По умолчанию автоматически выбирается последний использованный способ входа.

   > ⓘ **ИНФОРМАЦИЯ**
   >
   > Для входа в приложение Управление аутентификаторами следует использовать ранее зарегистрированный аутентификатор. При использовании пароля для доступа к приложению будут недоступны функции изменения, удаления и добавления аутентификаторов.

3. Выполните требуемые действия (в зависимости от выбранного способа входа).

   > ⓘ **ПРИМЕЧАНИЕ**
   >
   > Возможности добавления, редактирования и удаления аутентификаторов доступны после авторизации с использованием аутентификатора. Возможность проверки аутентификаторов доступна как после авторизации с использованием аутентификатора, так и после авторизации с использованием пароля.

4. После успешной аутентификации отображается окно Управление аутентификаторами.

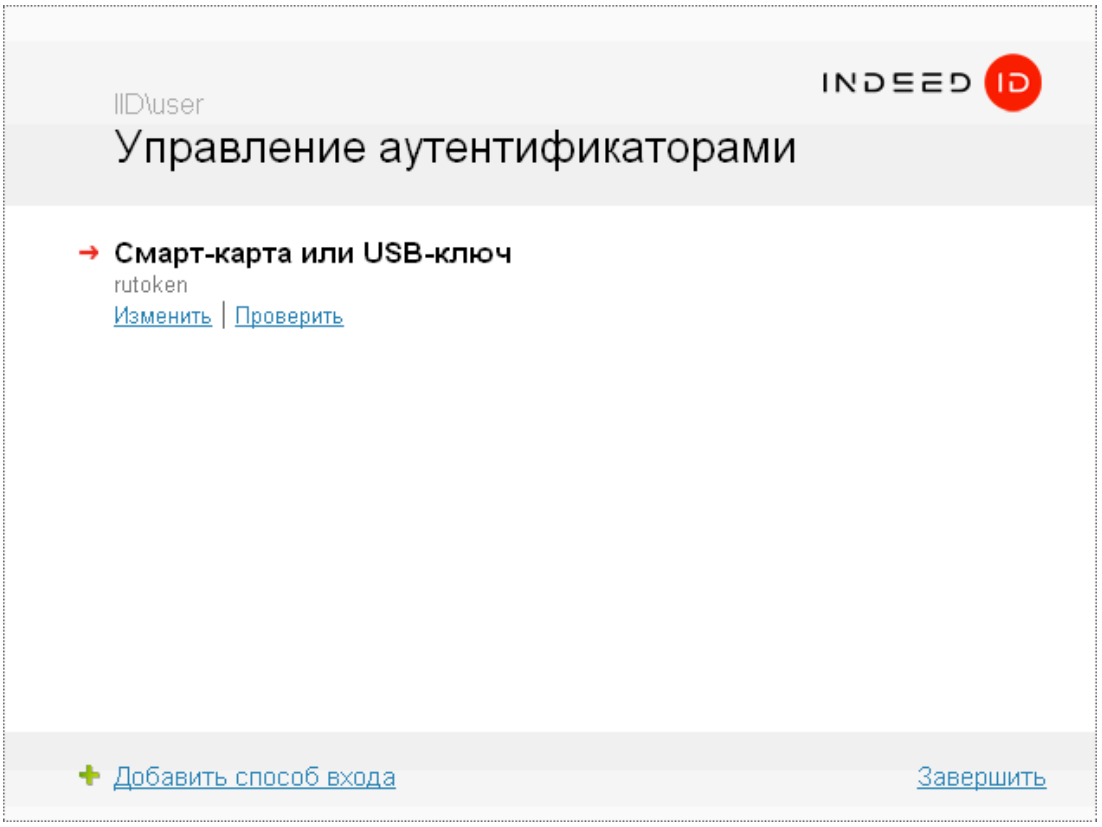
Добавление аутентификатора

> ⚠ **ВАЖНО!**
>
> Перед регистрацией аутентификаторов необходимо создать политику и распространить на целевых пользователей

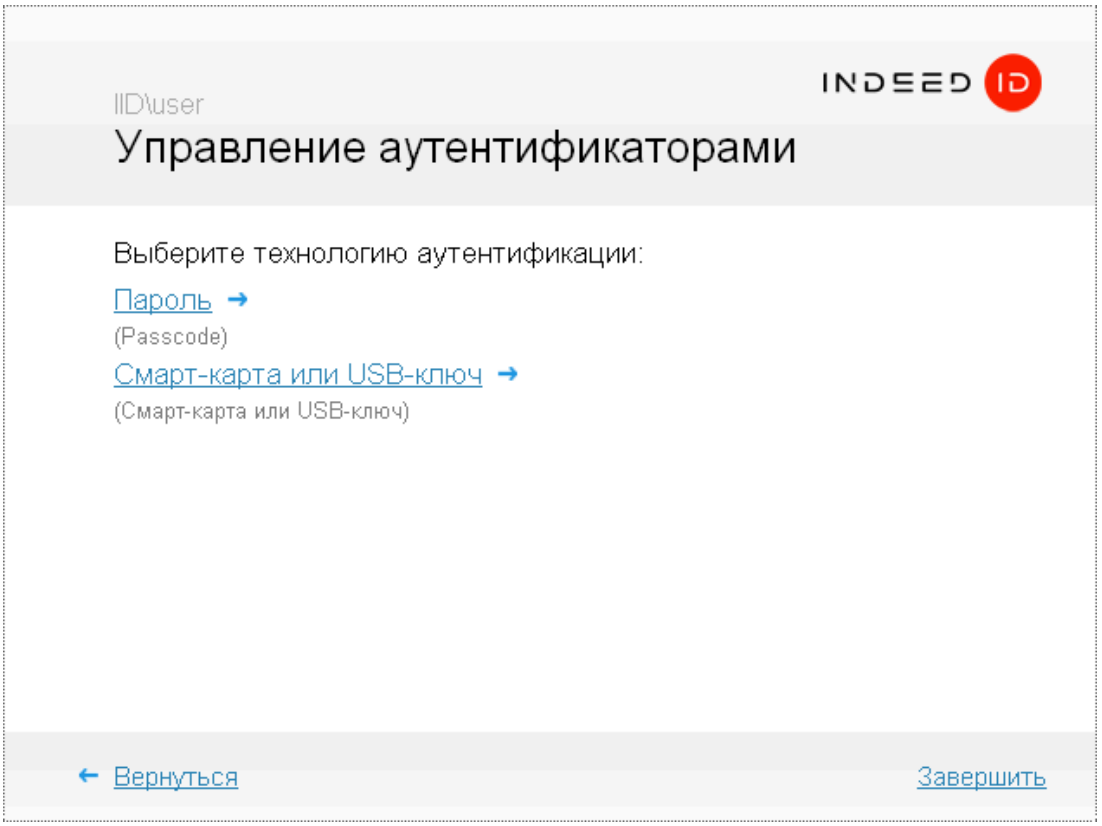
Количество аутентификаторов, которое вы можете добавить, устанавливается администратором системы. После достижения максимального количества аутентификаторов кнопка Добавить способ входа в окне Управление аутентификаторами становится неактивна.

Для добавления аутентификатора выполните следующие действия:

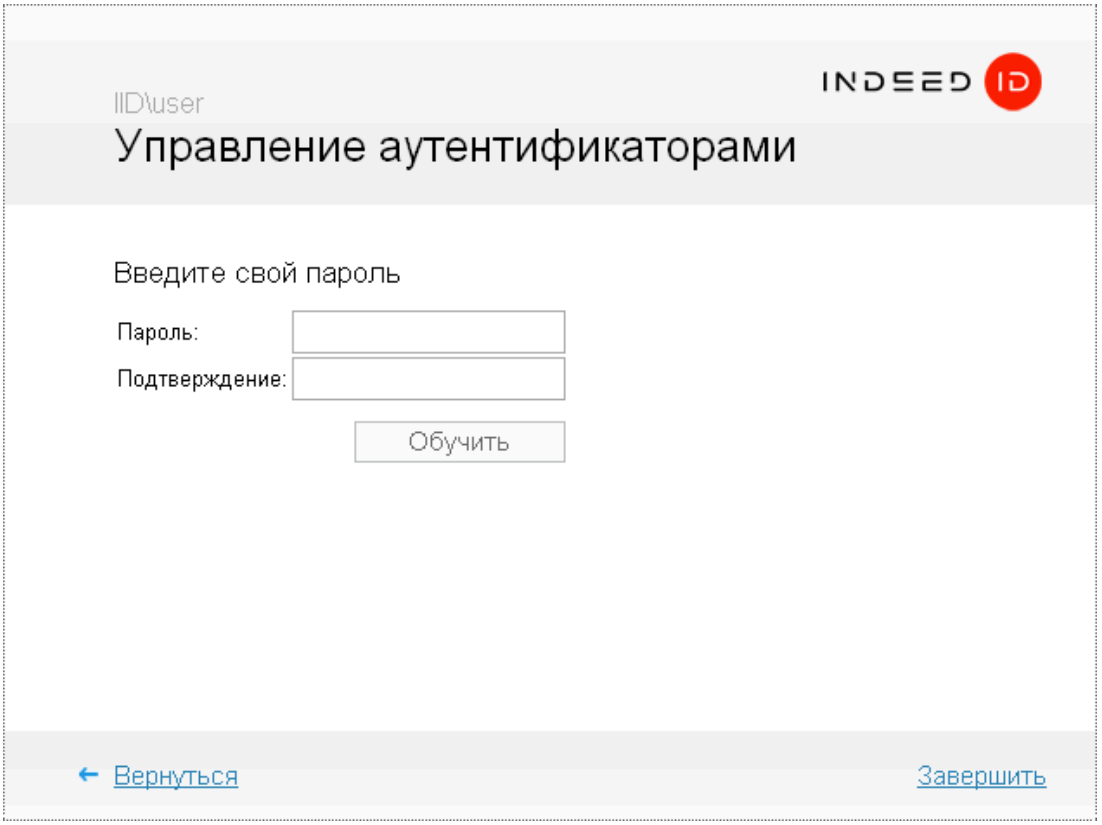
1. В окне Управление аутентификаторами нажмите Добавить способ входа



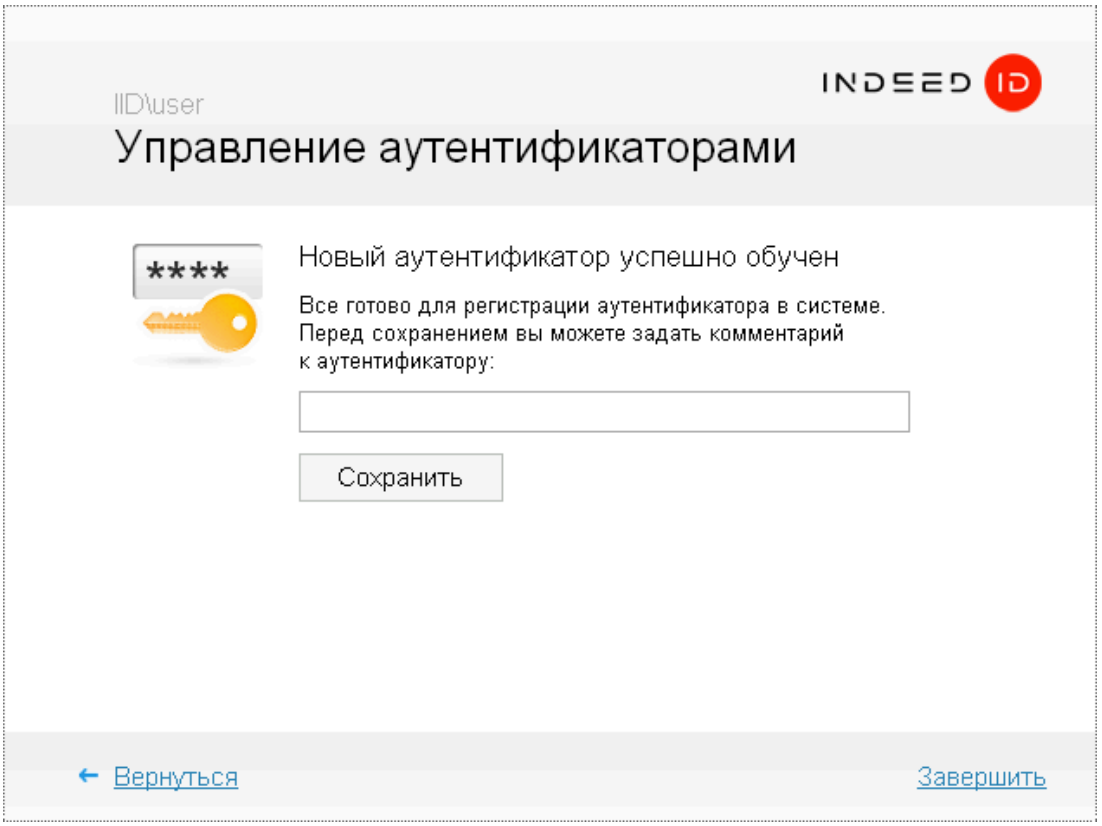
2. Выберите технологию аутентификации.



3. Следуйте инструкциям по регистрации аутентификатора. Внешний вид окна и текст подсказок зависят от выбранного типа аутентификатора.



После успешной регистрации аутентификатора в окне Управление аутентификаторами отображается сообщение *Новый аутентификатор успешно обучен*.



4. Вы можете добавить произвольный текстовый комментарий к зарегистрированному аутентификатору (если данное действие разрешено администратором системы). Для завершения регистрации аутентификатора нажмите Сохранить.

Тип зарегистрированного аутентификатора и комментарий к нему отображаются в окне Управление аутентификаторами. Если для вашей учетной записи разрешено добавление нескольких аутентификаторов, вы можете перейти к их регистрации, нажав кнопку Добавить аутентификатор.

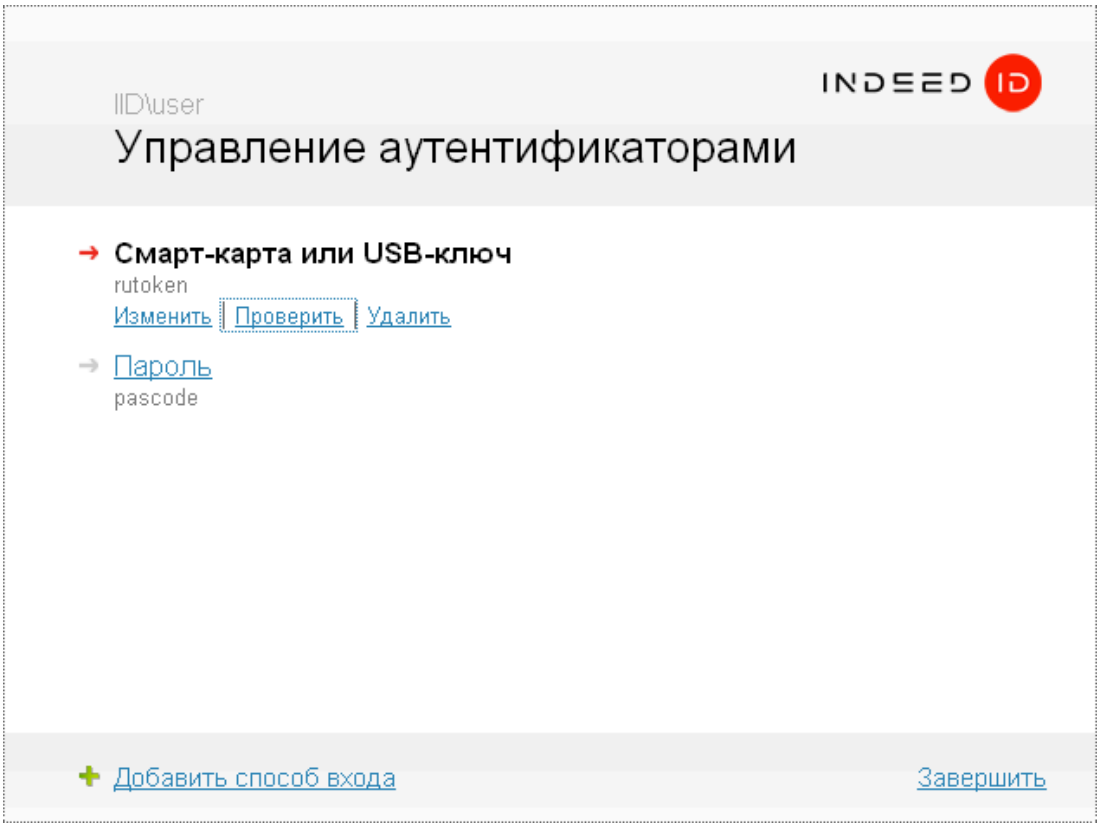
ИНФОРМАЦИЯ

При использовании определенных моделей биометрических устройств (например сканеров отпечатков пальцев Digent IZZIX FD 2000, FD/FM 1000) возможны ошибки при регистрации и распознавании аутентификатора, связанные с уровнем чувствительности сканера и индивидуальными особенностями человека (температура тела, уровень влажности кожи, способ прикладывания пальца). Во избежание таких ошибок рекомендуется проверять аутентификатор сразу после регистрации.

Проверка аутентификатора

Для проверки аутентификатора выполните следующие действия:

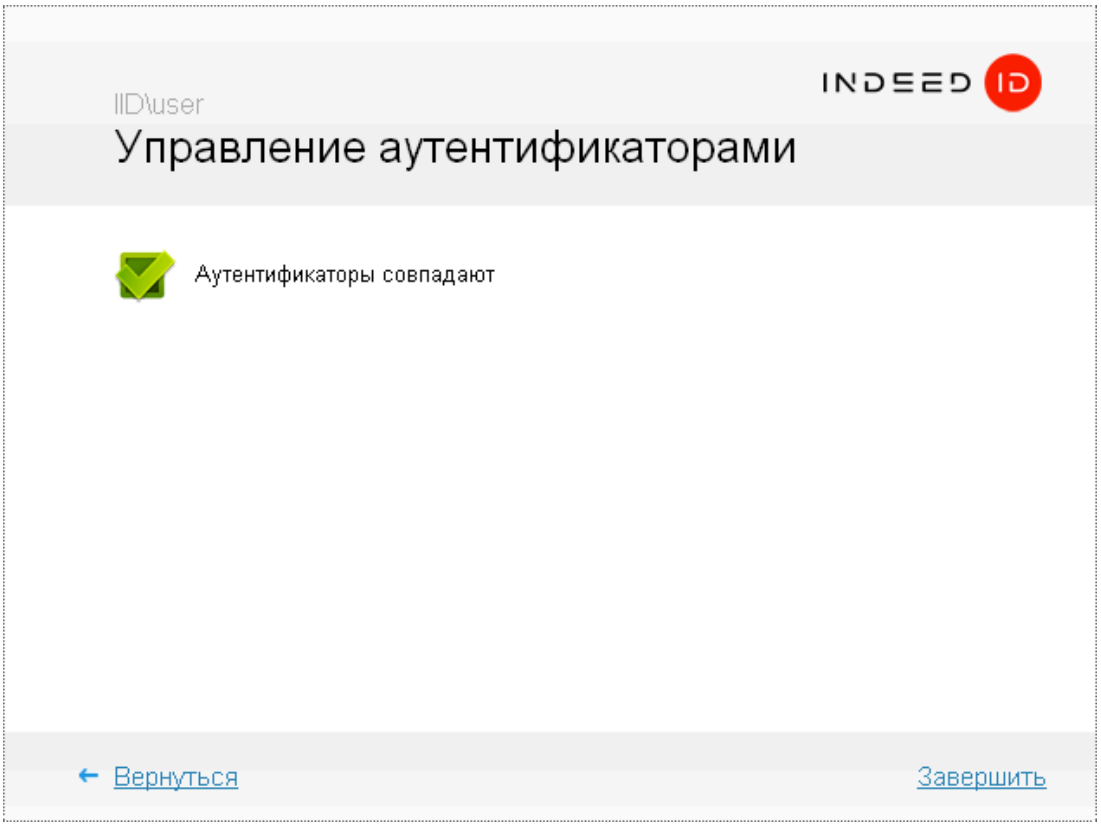
1. В окне Управление аутентификаторами выберите аутентификатор и нажмите Проверить.



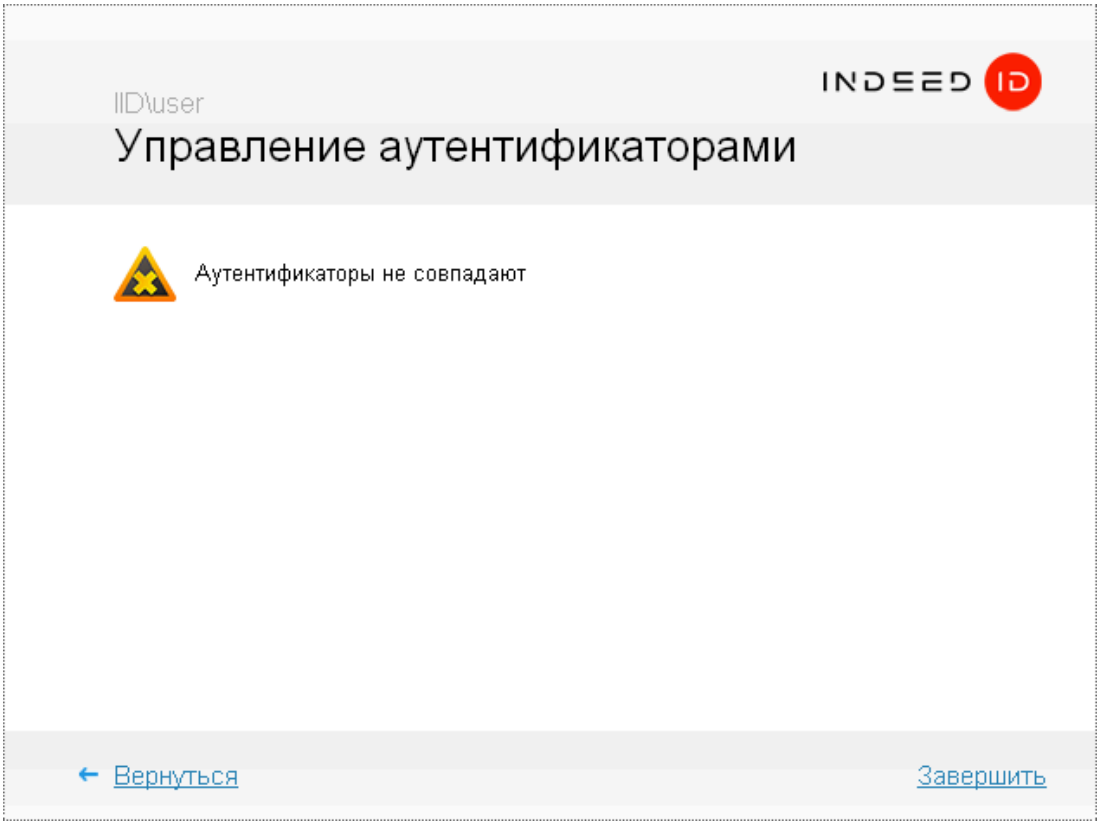
2. Далее в окне Управление аутентификаторами отображаются инструкции по регистрации аутентификатора. Внешний вид окна и текст подсказок зависят от выбранного типа аутентификатора. Выполните требуемые действия.

3. После завершения проверки в окне Управление аутентификаторами отображается сообщение о результате.

    - Если аутентификаторы совпадают;



- Если аутентификаторы не совпадают;



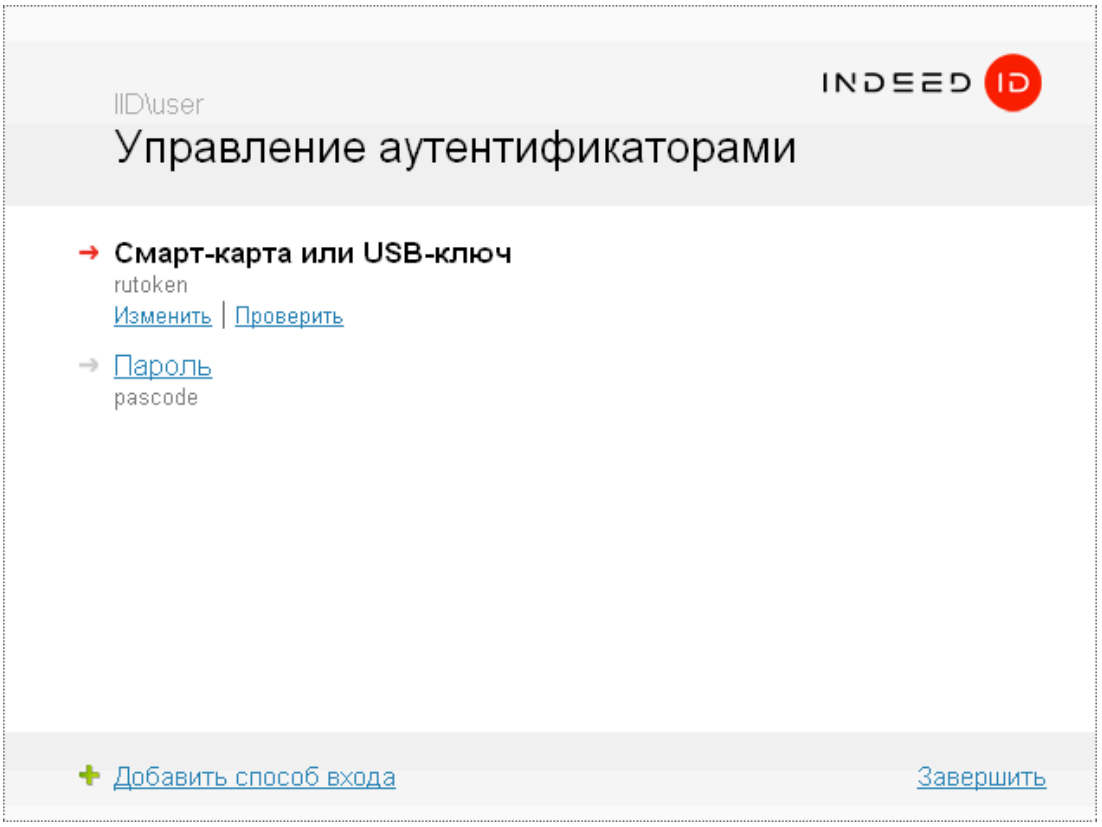
4. Если аутентификаторы не совпадают, нажмите Вернуться и повторите процедуру проверки или заново обучите аутентификатор.

Редактирование аутентификатора

> ⚠ **ВАЖНО!**
>
> Доступные действия:
>
> - отредактировать (повторно зарегистрировать) аутентификатор;
> - изменить только комментарий к аутентификатору (если это действие разрешено администратором системы).

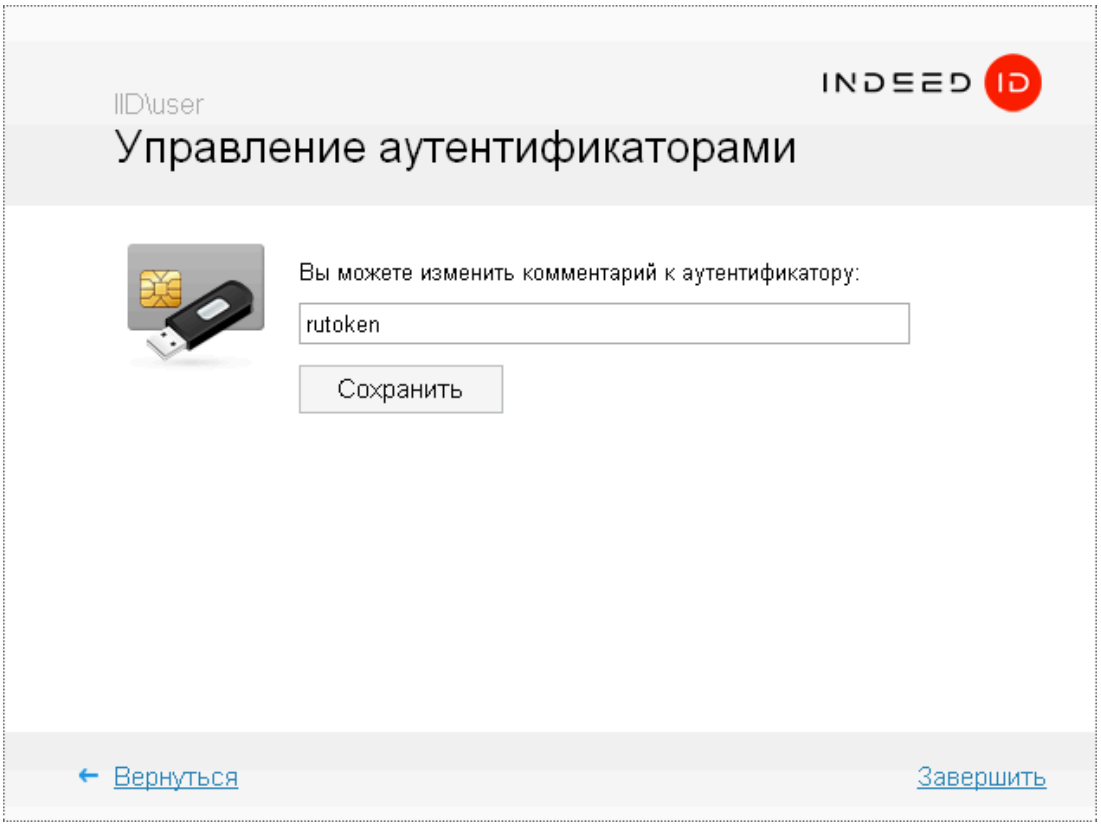
Для редактирования аутентификатора выполните следующие действия:

1. В окне Управление аутентификаторами выберите аутентификатор и нажмите Изменить.

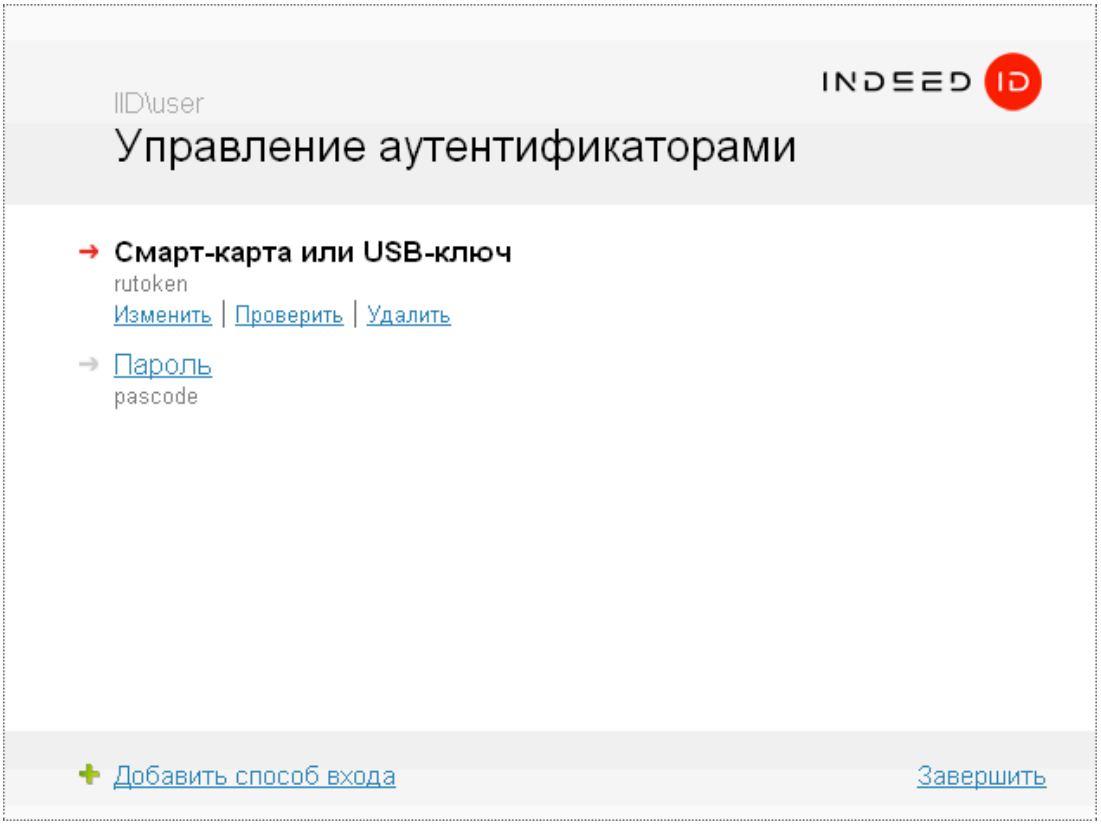


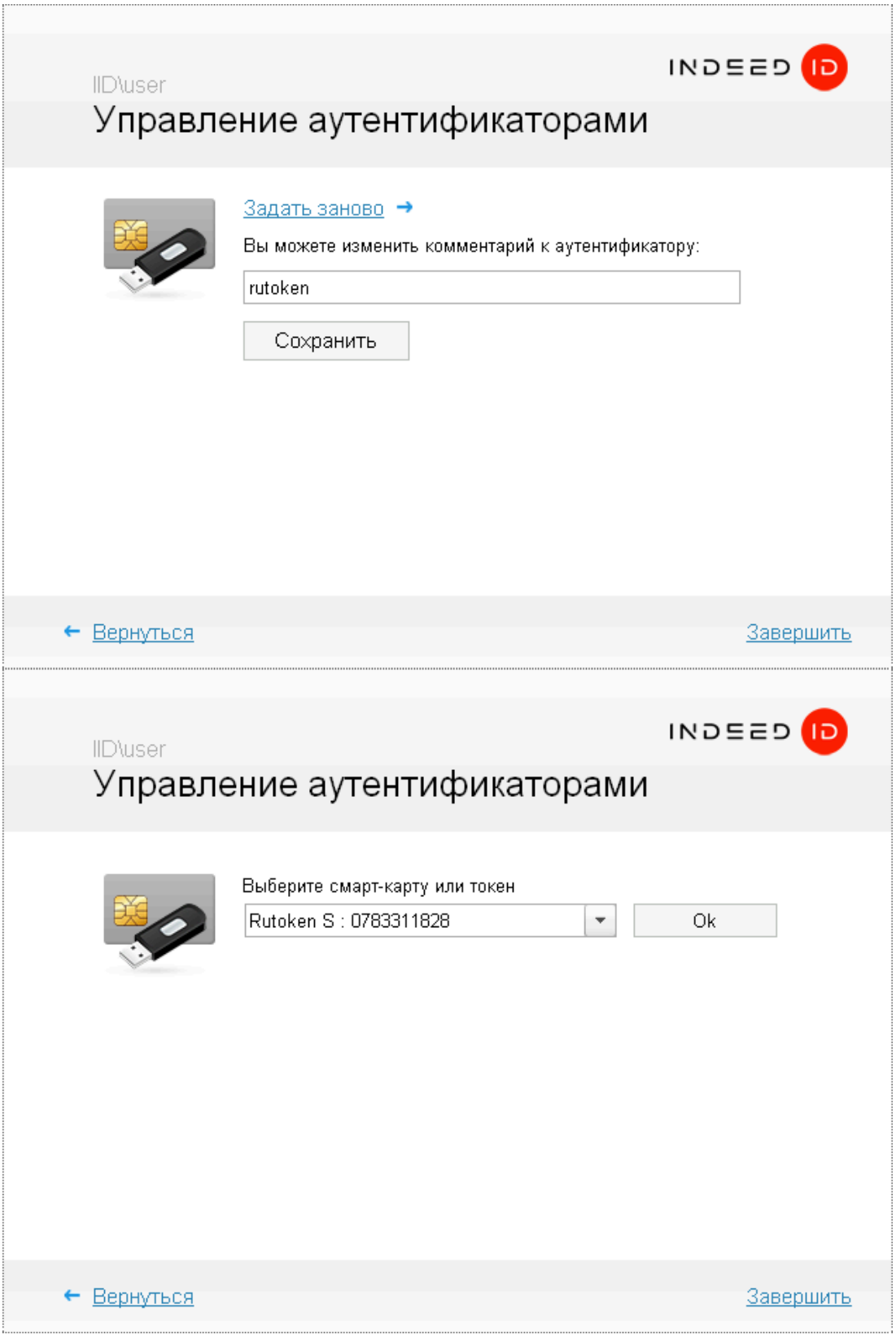
2. Выполните одно из указанных действий:

   - Чтобы отредактировать только комментарий к аутентификатору, введите комментарий в соответствующее поле и нажмите Сохранить.

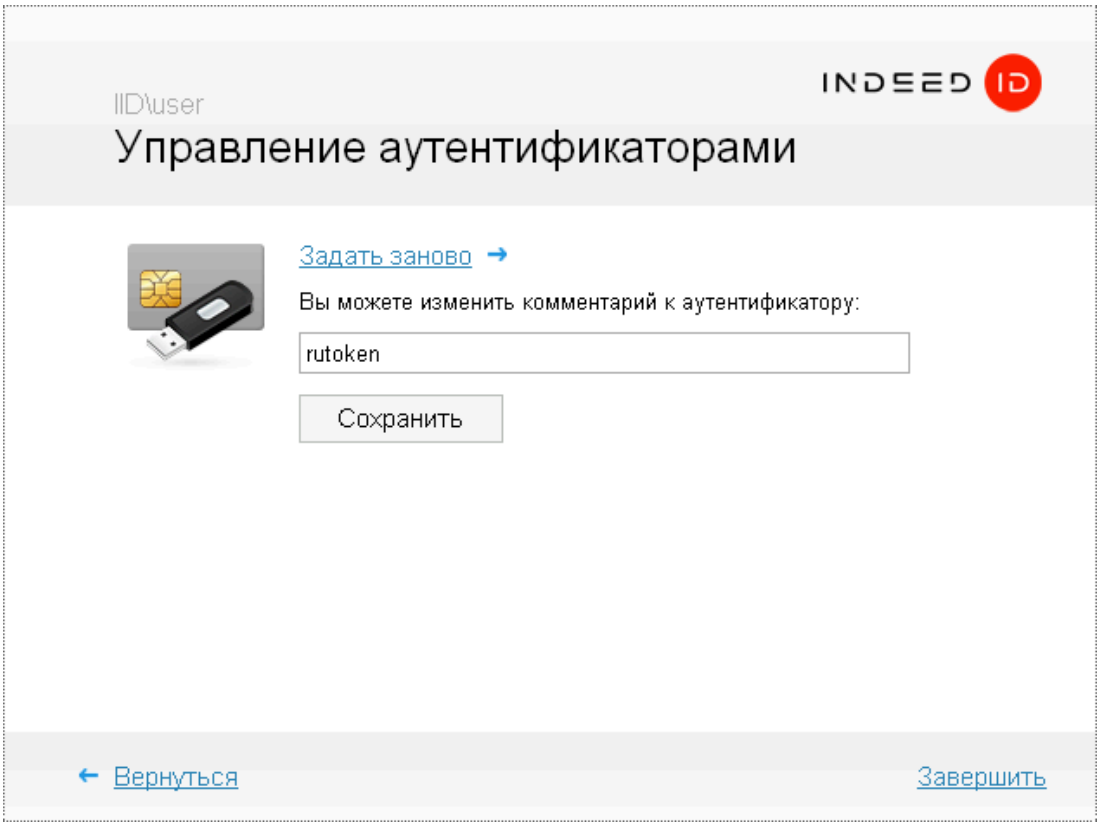


- Чтобы перейти к редактированию самого аутентификатора, нажмите Задать заново. Далее в окне отобразятся инструкции по регистрации аутентификатора. Внешний вид окна и текст подсказок зависят от выбранного типа аутентификатора. Выполните требуемые действия.



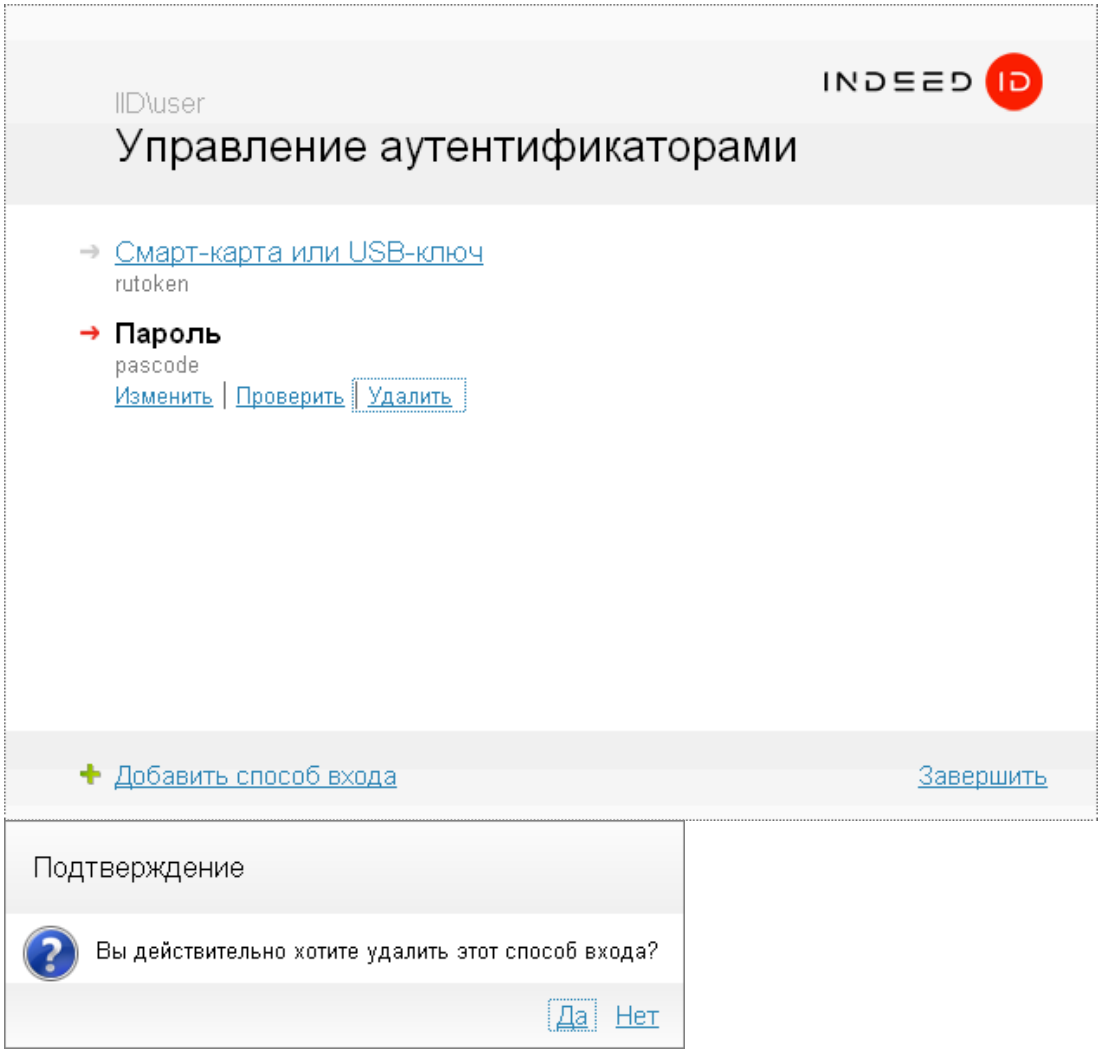


3. После успешной регистрации аутентификатора нажмите Сохранить.

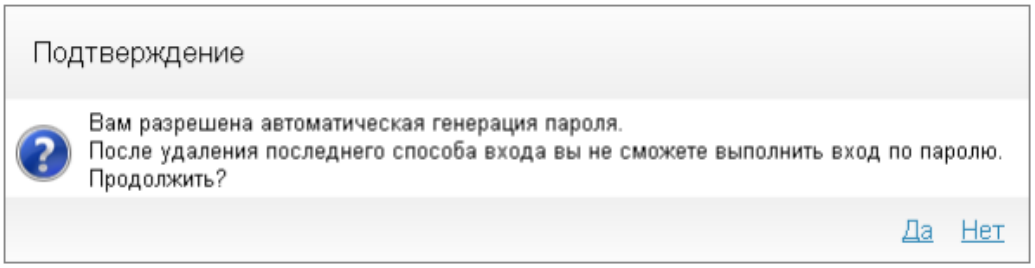

lID\user
Управление аутентификаторами
Задать заново
Вы можете изменить комментарий к аутентификатору:
rutoken
Сохранить
Вернуться
Завершить

Удаление аутентификатора

Для удаления аутентификатора в окне Управление аутентификаторами выберите аутентификатор и нажмите Удалить. Для подтверждения действия нажмите Да.



Если для вашей учетной записи был сгенерирован случайный пароль, при попытке удалить единственный имеющийся аутентификатор система отображает диалог-предупреждение:



СОВЕТ

Если вы удалили все аутентификаторы и не можете выполнить вход в систему по паролю, обратитесь к администратору системы. После сброса пароля вы снова сможете выполнить вход в систему и зарегистрировать новые аутентификаторы.

После удаления всех аутентификаторов вход в систему может быть выполнен только по паролю. Если для вашей учетной записи был сгенерирован случайный пароль, вход в систему станет невозможен.

Установка и настройка провайдеров аутентификации

Indeed AM Windows Password Provider

Аутентификация по паролю Windows

Indeed AM Passcode Provider

Аутентификация по заданному паролю

Indeed AM Software OTP Provider

Одноразовый пароль в дополнение к своему логину и паролю

Indeed AM Secured TOTP Provider

Одноразовый пароль на основе идентификатора устройства

Indeed AM SMS OTP Provider

Количество глав: 1

Indeed AM Storage SMS OTP Provider

Аутентификация по номерам телефонов из базы Microsoft SQL

Indeed AM Email OTP Provider

Одноразовый пароль по электронной почте

Indeed AM Hardware OTP

Аутентификация по Hardware OTP от Рутокен и eToken PASS

Indeed AM Hardware TOTP

Аутентификация по TOTP от eToken PASS

Indeed Key Provider

Одноразовый пароль и push-уведомления в приложении Indeed Key

Indeed AM Telegram Provider

Одноразовый пароль и push-уведомления в приложении Telegram

Indeed AM MFA Provider

Многофакторная аутентификация

Indeed AM Windows Password Provider

Провайдер Indeed AM Windows Password может быть использован для аутентификации в следующих модулях:

- Identity Provider,
- LDAP Proxy,
- Windows Logon,
- Linux Logon.

Идентификатор провайдера
`{CF189AF5-01C5-469D-A859-A8F2F41ED153}`

Установка провайдера Windows Password

> ⚠ **ВАЖНО**
>
> Если в инфраструктуре используется несколько серверов Indeed AM, то установку провайдера необходимо выполнить на всех серверах инфраструктуры.

Чтобы установить провайдер на сервере с операционной системой Linux, выполните следующие действия:

1. Откройте файл *am/.env*.
2. В переменной `COMPOSE_PROFILES` добавьте значение `amwp`.

   > ⓘ **ПРИМЕЧАНИЕ**
   >
   > Для первичной аутентификации в Core Server необходимо обязательно задать значение `amwp`.

Настройка провайдера Windows Password в Management Console

Для настройки Windows Password в Management Console перейдите в раздел Конфигурация→Аутентификаторы и выберите аутентификатор Windows Password.

Права доступа

Чтобы выдать или отозвать права на использование аутентификатора, выполните следующее:

1. Перейдите в секцию Основные настройки.
2. В настройке Запретить использовать укажите, может ли пользователь использовать или регистрировать выбранный аутентификатор.

Блокировка аутентификатора

Чтобы заблокировать аутентификатор, в секции Настройки блокировки аутентификатора выполните следующие настройки:

1. Разрешите или заблокируйте использование Windows Password в случае серии неудачных попыток аутентификации.
2. В поле Количество попыток аутентификации до блокировки укажите, сколько раз пользователь может совершить неудачную аутентификацию до блокировки способа аутентификации.
3. В поле Сброс счетчика блокировки укажите, сколько минут должно пройти после неудачной попытки аутентификации, прежде чем сбросится счетчик.
4. В поле Таймаут до разблокировки способа входа укажите, через сколько минут заблокированный способ аутентификации станет вновь доступным.

Indeed AM Passcode Provider

Indeed AM Passcode Provider предназначен для аутентификации пользователей по самостоятельно заданному паролю и совместного использования с продуктами Indeed AM.

Идентификатор провайдера
`{F696F05D-5466-42b4-BF52-21BEE1CB9529}`

Установка провайдера Passcode

> ⚠ **ВАЖНО**
>
> Если в инфраструктуре используется несколько серверов Indeed AM, то установку провайдера необходимо выполнить на всех серверах инфраструктуры.

На сервере с Linux

Чтобы установить провайдер на сервере с операционной системой Linux, выполните следующие действия:

1. Откройте файл *am/.env*.
2. В переменной `COMPOSE_PROFILES` добавьте значение `passcode`.

На клиентских машинах с Windows

Чтобы установить провайдер на клиентских машинах с операционной системой Windows, выполните следующие действия:

1. Для работы провайдера требуется установка Indeed AM Bsp Broker. Из папки *Indeed AM <Номер версии>\Indeed AM Providers\Indeed AM Bsp Broker\<Номер версии>* запустите пакет *IndeedEA.AuthProviders.BspBroker-<номер версии>.<разрядность>.ru-ru.msi*.
2. Из папки *Indeed AM <Номер версии>\Indeed AM Providers\Indeed AM Passcode Provider\<Номер версии>* запустите пакет *IndeedID.Passcode.Provider-<номер версии>.<разрядность>.ru-ru.msi*.
3. Если программа установки предлагает выполнить перезагрузку, подтвердите данное действие. После завершения установки может потребоваться перезагрузка системы.

Удаление/Восстановление продукта осуществляется стандартным для поддерживаемых ОС способом, через меню Панель управления.

Файлы шаблонов политик расположены в папке *Indeed AM <номер версии>*\Misc\ADMX Templates*.

Настройка провайдера Passcode в Management Console

Для настройки Passcode в Management Console перейдите в раздел Конфигурация→Аутентификаторы и выберите аутентификатор Passcode.

Максимальное количество аутентификаторов

В секции Основные настройки в поле Максимальное количество задайте максимальное количество паролей Passcode для пользователя.

Права доступа

Чтобы выдать или отозвать права на использование аутентификатора, выполните следующее:

1. В секции Основные настройки выполните следующие настройки:
   - В настройке Запретить использовать укажите, может ли пользователь использовать или регистрировать выбранный аутентификатор.
2. В секции Доступные пользователю действия выполните следующие настройки:
   - В настройке Регистрация новых аутентификаторов укажите, может ли пользователь регистрировать новые аутентификаторы.
   - В настройке Редактирование имеющихся аутентификаторов укажите, может ли пользователь изменять уже зарегистрированные аутентификаторы.
   - В настройке Удаление имеющихся аутентификаторов укажите, может ли пользователь удалять уже зарегистрированные аутентификаторы.
   - В настройке Разрешить редактирование комментария к аутентификатору укажите, в какой момент пользователь может редактировать комментарии к уже зарегистрированным аутентификаторам.

Блокировка аутентификатора

Чтобы заблокировать аутентификатор, в секции Настройки блокировки аутентификатора выполните следующие настройки:

1. Разрешите или заблокируйте использование Passcode в случае серии неудачных попыток аутентификации.
2. В поле Количество попыток аутентификации до блокировки укажите, сколько раз пользователь может совершить неудачную аутентификацию до блокировки способа аутентификации.
3. В поле Сброс счетчика блокировки укажите, сколько минут должно пройти после неудачной попытки аутентификации, прежде чем сбросится счетчик.
4. В поле Таймаут до разблокировки способа входа укажите, через сколько минут заблокированный способ аутентификации станет вновь доступным.

Настройка требований к паролю

В секции Настройки требований к паролю можно задать следующие требования к Passcode паролю:

- минимальная длина пароля;
- максимальное количество вхождений каждого символа;
- допустимые символы (латинские буквы, цифры, специальные символы, пользовательские символы);
- минимальное число символов из группы.

Максимальное количество вхождений каждого символа может быть от 1 до 63 или 0.

Группы символов:

- цифры: 0-9
- строчные латинские буквы: a-z
- прописные латинские буквы: A-Z
- специальные символы: . , < > / ? [ ] { } = + - _ \ | ! @ # $ % ^ & * ( )
- пользовательская группа символов (группу символов задает пользователь для каждого приложения)

> **ИНФОРМАЦИЯ**
>
> Если настройки не заданы, то пароль может состоять только из цифр, строчных латинских букв и содержать не менее 6 символов.

Indeed AM Software OTP Provider

С помощью Software OTP Provider вы можете реализовать двухфакторную аутентификацию, основанную на программном обеспечении. Аутентификатор представляет собой одноразовый пароль, который пользователь должен предоставить в дополнение к своему логину и паролю, чтобы получить доступ к приложению.

Одноразовый пароль генерируется автономно на мобильном устройстве (телефон, смартфон, планшет) с использованием специализированного приложения (например, Indeed Key, Google Authenticator, Яндекс.Ключ). Генерация одноразового пароля производится на основе двух параметров: секретного ключа, задаваемого на этапе регистрации аутентификатора, и текущего времени.

Технология аутентификации основана на системе, где для заданного секретного ключа пользователя в каждый момент времени существует единственный верный одноразовый пароль. Таким образом, имея информацию о секретном ключе, сервер может проверить переданный пользователем одноразовый пароль. Для правильного функционирования технологии время на мобильном устройстве и сервере аутентификации должно совпадать (при этом допускается погрешность, величина которой может регулироваться администратором).

Идентификатор провайдера
`{0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0}`

Идентификатор провайдера для Indeed AM FreeRADIUS Extension
`{B772829C-4076-482B-B9BD-53B55EA1A302}`

Установка провайдера Software OTP

> ⚠ **ВАЖНО**
>
> Если в инфраструктуре используется несколько серверов Indeed AM, то установку провайдера необходимо выполнить на всех серверах инфраструктуры.

На сервере с Linux

Чтобы установить провайдер на сервере с операционной системой Linux, выполните следующие действия:

1. Откройте файл *am/.env*.
2. В переменной `COMPOSE_PROFILES` добавьте значение `software-totp`.

На клиентских машинах с Windows

Чтобы установить провайдер на клиентских машинах с операционной системой Windows, выполните следующие действия:

1. Из папки *Indeed AM <Номер версии>\Indeed AM Providers\Indeed AM Software OTP Provider\<Номер версии>* запустите пакет *IndeedAM.AuthProviders.SoftwareTOTP.Provider-<номер версии>.<разрядность>.ru-ru.msi*.
2. Если программа установки предлагает выполнить перезагрузку, подтвердите данное действие. После завершения установки может потребоваться перезагрузка системы.

Удаление/Восстановление продукта осуществляется стандартным для поддерживаемых ОС способом, через меню Панель управления.

Файлы шаблонов политик расположены в папке *Indeed AM <номер версии>*\Misc\ADMX Templates*.

Настройка провайдера Software OTP в Management Console

Для настройки Software OTP в Management Console перейдите в раздел Конфигурация→Аутентификаторы и выберите аутентификатор Software OTP.

Права доступа

Чтобы выдать или отозвать права на использование аутентификатора, выполните следующее:

1. В секции Основные настройки выполните следующие настройки:
   - В настройке Запретить использовать укажите, может ли пользователь использовать или регистрировать выбранный аутентификатор.
2. В секции Доступные пользователю действия выполните следующие настройки:
   - В настройке Регистрация новых аутентификаторов укажите, может ли пользователь регистрировать новые аутентификаторы;
   - В настройке Редактирование имеющихся аутентификаторов укажите, может ли пользователь изменять уже зарегистрированные аутентификаторы;
   - В настройке Удаление имеющихся аутентификаторов укажите, может ли пользователь удалять уже зарегистрированные аутентификаторы;
   - В настройке Разрешить редактирование комментария к аутентификатору укажите, в какой момент пользователь может редактировать комментарии к уже зарегистрированным аутентификаторам.

Принудительная проверка аутентификатора

1. В разделе Основные настройки включите принудительную проверку. При регистрации появится дополнительное окно подтверждения для ввода данных аутентификации.

2. Введите полученные данные аутентификации и нажмите Подтвердить.

Блокировка аутентификатора

Чтобы заблокировать аутентификатор, в секции Настройки блокировки аутентификатора выполните следующие настройки:

1. Разрешите или заблокируйте использование Software OTP в случае серии неудачных попыток аутентификации.
2. В поле Количество попыток аутентификации до блокировки укажите, сколько раз пользователь может совершить неудачную аутентификацию до блокировки способа аутентификации.
3. В поле Сброс счетчика блокировки укажите, сколько минут должно пройти после неудачной попытки аутентификации, прежде чем сбросится счетчик.
4. В поле Таймаут до разблокировки способа входа укажите, через сколько минут заблокированный способ аутентификации станет вновь доступным.

Настройки одноразового пароля

Чтобы настроить генерацию одноразового пароля, в секции Настройки OTP выполните следующее:

1. В настройке Период обновления OTP укажите, на протяжение какого времени будет актуален одноразовый пароль;
2. В настройке Количество периодов сравнения укажите, сколько периодов обновления OTP должно пройти, по истечении которых пароль будет считаться недействительным;
3. В настройке Формат имени пользователя задайте имя пользователя, которое будет передаваться в мобильное приложение;
4. В настройке Алгоритм генерации OTP-кода выберите, по какому алгоритму будет генерироваться одноразовый пароль;
5. В настройке Количество цифр в OTP-коде выберите, сколько цифр будет содержать одноразовый пароль.

Indeed AM Secured TOTP Provider

Indeed AM Secured TOTP — это провайдер с привязкой к идентификатору устройства пользователя.

Секретный ключ для генерации одноразового кода зашифрован и расшифровывается только ключом на основе идентификатора устройства. Таким образом, регистрация одного конкретного аутентификатора возможна лишь на одном устройстве.

Для работы с несколькими устройствами необходимо получить разрешение администратора AM и установить провайдер на каждое из устройств по отдельности.

Secured TOTP может быть использован для аутентификации в следующих модулях:

- Identity Provider,
- ADFS Extension,
- FreeRadius Extension,
- RDP Windows Logon,
- Windows Logon,
- Linux Logon.

Идентификаторы провайдера для интеграции с модулем FreeRadius Extension

```
{F15FD7EC-19EA-4384-846E-A2D0BE149FA2} — Secured TOTP
{882C1787-FD32-44A2-BA89-F1F529FBE7AB} — Passcode + Secured TOTP
{7F3DE86F-59D1-4476-AA5D-F277E5DD5938} — Windows Password + Secured TOTP
```

Установка провайдера Secured TOTP

> ⚠ **ВАЖНО**
>
> Если в инфраструктуре используется несколько серверов Indeed AM, то установку провайдера необходимо выполнить на всех серверах инфраструктуры.

Предварительные требования

Для работы провайдера необходимы следующие условия:

- установлен провайдер Secured TOTP,
- установлено мобильное приложение Indeed Key версии 2.6 и выше,
- для регистрации Secured TOTP по ссылке из письма необходимы:
  - установленный и настроенный провайдер Email OTP,
  - заполненный email пользователя в каталоге пользователей.

На сервере с Linux

Чтобы установить провайдер на сервере с операционной системой Linux, выполните следующие действия:

1. Откройте файл *am/.env*.
2. В переменной `COMPOSE_PROFILES` добавьте значение `secured-totp`.

На клиентских машинах с Windows

Чтобы установить провайдер на клиентских машинах с операционной системой Windows, выполните следующие действия:

1. Из папки *Indeed AM <Номер версии>\Indeed AM Providers\Indeed AM Secured TOTP Provider\<Номер версии>* запустите пакет *IndeedAM.AuthProviders.SecuredTOTP-<номер версии>.<разрядность>.ru-ru.msi*.

2. Если программа установки предлагает выполнить перезагрузку, подтвердите данное действие. После завершения установки может потребоваться перезагрузка системы.

Удаление/Восстановление продукта осуществляется стандартным для поддерживаемых ОС способом, через меню Панель управления.

Настройка провайдера Secured TOTP в Management Console

Для настройки провайдера Secured TOTP в Management Console перейдите в раздел Конфигурация→Аутентификаторы и выберите аутентификатор Secured TOTP.

Права доступа

Чтобы выдать или отозвать права на использование аутентификатора, выполните следующее:

1. В секции Основные настройки выполните следующие настройки:
   - В настройке Запретить использовать укажите, может ли пользователь использовать или регистрировать выбранный аутентификатор.
2. В секции Доступные пользователю действия выполните следующие настройки:
   - В настройке Регистрация новых аутентификаторов укажите, может ли пользователь регистрировать новые аутентификаторы.
   - В настройке Редактирование имеющихся аутентификаторов укажите, может ли пользователь изменять уже зарегистрированные аутентификаторы.
   - В настройке Удаление имеющихся аутентификаторов укажите, может ли пользователь удалять уже зарегистрированные аутентификаторы.

- В настройке Разрешить редактирование комментария к аутентификатору укажите, в какой момент пользователь может редактировать комментарии к уже зарегистрированным аутентификаторам.

Принудительная проверка аутентификатора

Для регистрации аутентификатора можно настроить принудительную проверку аутентификатора.

1. В разделе Основные настройки включите принудительную проверку. При регистрации появится дополнительное окно подтверждения для ввода данных аутентификации.
2. Введите полученные данные аутентификации и нажмите Подтвердить.

Блокировка аутентификатора

Чтобы заблокировать аутентификатор, перейдите в секцию Настройки блокировки аутентификатора и выполните следующие настройки:

1. Разрешите или заблокируйте использование Secured TOTP в случае серии неудачных попыток аутентификации.
2. В поле Количество попыток аутентификации до блокировки укажите, сколько раз пользователь может совершить неудачную аутентификацию до блокировки способа аутентификации.
3. В поле Сброс счетчика блокировки укажите, сколько минут должно пройти после неудачной попытки аутентификации, прежде чем сбросится счетчик.
4. В поле Таймаут до разблокировки способа входа укажите, через сколько минут заблокированный способ аутентификации станет вновь доступным.

Генерация одноразового пароля

В секции Настройки OTP выполните следующие настройки:

1. В настройке Период обновления OTP укажите, на протяжение какого времени будет актуален одноразовый пароль.
2. В настройке Количество периодов сравнения укажите, сколько периодов обновления OTP должно пройти, по истечении которых пароль будет считаться недействительным.
3. В настройке Формат имени пользователя задайте имя пользователя, которое будет передаваться в мобильное приложение.
4. В настройке Отображаемое имя сервера задайте имя сервера, которое будет передаваться в мобильное приложение.
5. В настройке Количество цифр в OTP-коде выберите, сколько цифр будет содержать одноразовый пароль.

Регистрация в Management Console

Secured TOTP можно зарегистрировать по ссылке из письма или по QR-коду. В Management Console доступны оба способа регистрации.

Для регистрации по ссылке из письма необходимы следующие условия:

- установленный и настроенный провайдер Email OTP,
- установлено мобильное приложение Indeed Key версии 2.6 и выше,
- заполненный email пользователя в каталоге пользователей.

Ссылка отправляется на электронный адрес, указанный для пользователя в каталоге пользователей. Опционально вы можете продублировать ссылку на другой электронный адрес, например руководителю сотрудника.

Чтобы зарегистрировать аутентификатор по email, выполните следующее:

1. В Management Console в настройке Способ регистрации аутентификатора в Management Console выберите способ регистрации аутентификатора по email.
2. Укажите текст темы электронного письма.
3. Укажите текст сообщения электронного письма. Ссылка на регистрацию указывается специальным тегом *<regLink>*.
4. Укажите текст ссылки, чтобы заменить написание в явном виде.
5. Далее перейдите в раздел Пользователи, выберите пользователя, выберите вкладку Аутентификаторы.
6. Нажмите кнопку Зарегистрировать и выберите из списка *Secured TOTP*.
7. В открывшемся окне введите идентификатор устройства пользователя. Его можно получить в настройках приложения Indeed Key и скопировать или отправить кнопкой Поделиться. Опционально на этом шаге вы можете указать дополнительные электронные адреса через запятую.
8. Нажмите кнопку Далее. После этого пользователю придет письмо со ссылкой на регистрацию аутентификатора. По ссылке пользователь перейдет в приложение Indeed Key, где начнется регистрация аутентификатора.
9. В Management Console нажмите кнопку Сохранить.

Конфигурация ссылки на регистрацию Secured TOTP (и скачивание Indeed Key)

Ссылку на регистрацию Secured TOTP и скачивание приложения Indeed Key можно задать вручную.

1. Перейдите в раздел Конфигурация→Аутентификаторы в секцию Настройки регистрации.

2. В настройке Адрес сервера, участвующий в формировании ссылки на регистрацию аутентификатора (диплинк) укажите ссылку для регистрации, отправляемую по email.

   Доступны следующие ссылки для регистрации (в скобках указано местонахождение сервера):

   - https://indeedkey.drru.agconnect.link (Россия)
   - https://indeedkey.dre.agconnect.link (Германия)
   - https://indeedkey.drcn.agconnect.link (Китай)
   - https://indeedkey.dra.agconnect.link (Сингапур)

3. В секции Дополнительные настройки укажите ссылку для скачивания Indeed Key.

Доступны следующие ссылки для скачивания (в скобках указано местонахождение сервера):

- https://indeedkey.drru.agconnect.link/XwZr (Россия)
- https://indeedkey.dre.agconnect.link/MJyW (Германия)
- https://indeedkey.drcn.agconnect.link/NDbK (Китай)
- https://indeedkey.dra.agconnect.link/i1RD (Сингапур)

Регистрация в User Console

Пользователь может зарегистрировать новый аутентификатор в User Console, если администратор разрешил пользователю регистрировать новые аутентификаторы в настройках Secured TOTP в Management Console.

На устройстве пользователя должно быть установлено приложение Indeed Key 2.6 и выше.

Чтобы зарегистрировать аутентификатор по QR-коду, выполните следующее:

1. В Management Console в разделе Доступные пользователю действия разрешите пользователю регистрировать новые аутентификаторы Secured TOTP.
2. В настройке Способ регистрации аутентификатора в User Console выберите способ регистрации аутентификатора по QR-коду.
3. В User Console у пользователя в списке доступных аутентификаторов появится Secured TOTP.

Пользователю нужно выполнить следующие действия:

1. Нажать значок шестеренки.
2. Нажать кнопку Зарегистрировать.
3. Указать ID устройства. Чтобы получить ID, пользователю нужно зайти в приложение Indeed Key, нажать значок шестеренки и скопировать значение из поля ID устройства.
4. Отсканировать появившийся код устройством с открытым приложением Indeed Key.
5. Если настроена принудительная проверка аутентификатора, дополнительно ввести полученный одноразовый пароль.

Indeed AM SMS OTP Provider

Компонент Indeed AM SMS OTP Provider предназначен для аутентификации пользователей с применением технологии одноразовых паролей, доставляемых пользователям по СМС.

Одноразовый пароль представляет собой набор случайных символов (цифр, специальных символов и латинских букв). Генерация пароля происходит на сервере Indeed AM, затем пароль передается на СМС-шлюз, имеющийся в инфраструктуре клиента, после одноразовый код отправляется на номер телефона пользователя. Передача данных происходит по протоколу SMPP (Short Message Peer-to-Peer).

Идентификатор провайдера
`{EBB6F3FA-A400-45F4-853A-D517D89AC2A3}`

Установка провайдера SMS OTP

> ⚠ **ВАЖНО**
>
> Если в инфраструктуре используется несколько серверов Indeed AM, то установку провайдера необходимо выполнить на всех серверах инфраструктуры.

Предварительные требования

Для использования Indeed AM SMS OTP Provider необходимо наличие СМС- шлюза. Данный шлюз должен быть доступен с каждого сервера Indeed AM, на котором предполагается установка SMS OTP Provider.

Для использования провайдера у пользователя должен быть задан номер телефона в атрибуте по умолчанию `telephoneNumber` или в другом настроенном атрибуте, иначе провайдер будет недоступен для использования.

Регистрация аутентификатора в User Console не требуется.

На сервере с Linux

Чтобы установить провайдер на сервере с операционной системой Linux, выполните следующие действия:

1. Откройте файл *am/.env*.
2. В переменной `COMPOSE_PROFILES` добавьте значение `sms-otp`.

На клиентских машинах с Windows

Чтобы установить провайдер на клиентских машинах с операционной системой Windows, выполните следующие действия:

1. Из папки *Indeed AM <Номер версии>\Indeed AM Providers\Indeed AM SMS OTP Provider\Client\<Номер версии>* запустите пакет *IndeedID.SMSOTP.Provider.msi*.

2. Если программа установки предлагает выполнить перезагрузку, подтвердите данное действие. После завершения установки может потребоваться перезагрузка системы.

Удаление/Восстановление продукта осуществляется стандартным для поддерживаемых ОС способом, через меню Панель управления.

Файлы шаблонов политик расположены в папке *Indeed AM <номер версии>\Misc\ADMX Templates*.

Настройка атрибута с номером телефона

Чтобы изменить значение атрибута по умолчанию, добавьте следующие параметры в конфигурационный файл сервера *am/core/app-settings.json*:

1. В секцию `Ldap` добавьте параметр `userMapRules`.
2. В параметр `userMapRules` добавьте параметр `Attributes`.
3. В `Attributes` добавьте параметр `Phone` и задайте ему значение, соответствующее необходимому атрибуту из службы каталога.

Пример

```
"Ldap": [{
  ...
  "userMapRules": {
    "Attributes": {
      "Phone": "mobile"
    }
  }
}
```

Настройка провайдера SMS OTP в Management Console

Для настройки SMS OTP в Management Console перейдите в раздел Конфигурация→Аутентификаторы и выберите аутентификатор SMS OTP.

Права доступа

Чтобы выдать или отозвать права на использование аутентификатора, выполните следующее:

1. Перейдите в секцию Основные настройки.

2. В настройке Запретить использовать укажите, может ли пользователь использовать или регистрировать выбранный аутентификатор.

Блокировка аутентификатора

Чтобы заблокировать аутентификатор, в секции Настройки блокировки аутентификатора выполните следующие настройки:

1. Разрешите или заблокируйте использование SMS OTP в случае серии неудачных попыток аутентификации.
2. В поле Количество попыток аутентификации до блокировки укажите, сколько раз пользователь может совершить неудачную аутентификацию до блокировки способа аутентификации.
3. В поле Сброс счетчика блокировки укажите, сколько минут должно пройти после неудачной попытки аутентификации, прежде чем сбросится счетчик.
4. В поле Таймаут до разблокировки способа входа укажите, через сколько минут заблокированный способ аутентификации станет вновь доступным.

Защита от спама

Механизм защиты от спама основан на расчете процента успешных аутентификаций относительно всех отправленных сообщений за указанный интервал времени. При этом расчет запускается, только если количество отправленных сообщений превышает количество, заданное вами в настройке Окно оценки.

При обнаружении спам-атаки дальнейшая отправка сообщений блокируется на заданный период времени, а при попытке входа возникает ошибка *Potential spam attack detected*.

Отправка сообщений возобновляется либо по истечении заданного периода, либо по достижении определенного количества (в процентном отношении) успешных аутентификаций.

Чтобы настроить защиту от спама, выполните следующее:

1. В Management Console в разделе Конфигурация→Аутентификаторы выберите аутентификатор.
2. В секции Настройки защиты от спама выполните следующие настройки:
   - включите или отключите защиту от спама;
   - в поле Окно оценки попыток аутентификации укажите, в течение какого времени будет выполняться расчет процента успешных попыток входа;
   - в поле Пороговое окно попыток аутентификации укажите, сколько попыток входа должно производиться за время, указанное в окне оценки попыток аутентификации;
   - в поле Процент успешных попыток аутентификации укажите минимальный процент успешных входов относительно всех отправленных сообщений.

Пример

Настройка включена со следующими значениями:

- Окно оценки попыток аутентификации — 600
- Пороговое окно попыток аутентификации — 20
- Процент успешных попыток аутентификации — 85

Защита от спама включится, если произойдет 21 попытка входа (отправлено 21 сообщение). Произойдет блокировка аутентификатора на 600 секунд.

Аутентификатор разблокируется в одном из случаев:

- процент успешных входов (пользователь успешно ввел одноразовый пароль из сообщения) достигнет значения 85;
- прошло 600 секунд с момента блокировки.

ИНФОРМАЦИЯ

События лог-сервера:

- 2090: Обнаружена потенциальная спам-атака. Отправка сообщений приостановлена.
- 1118: Отправка сообщений пользователям возобновлена.

Настройки шлюза

1. В секции Настройка шлюза выберите один из типов подключения:
   - SMS Proxy
   - OneGate
   - MFMSolutions
   - Megafon
2. Укажите адрес подключения к серверу.
3. В зависимотри от типа подключения заполните остальные поля:
   - SMS Proxy: Отпечаток сертификата клиента и Отпечаток сертификата сервера;
   - MFMSolutions: Логин — имя учетной записи для подключения к серверу и Пароль — пароль учетной записи для подключения к серверу;
   - Megafon: Логин — имя учетной записи для подключения к серверу и Пароль — пароль учетной записи для подключения к серверу.

Формат сообщения

1. В поле Отправитель укажите имя отправителя, которое будет отображаться при получении СМС.
2. В поле Дополнительный текст перед OTP введите произвольный текст сообщения, предшествующий одноразовому паролю. По умолчанию отправляется только OTP.
3. Из выпадающего списка Формат даты выберите формат, в котором будет отображаться дата (или дата и время) отправки сообщения в тексте сообщения.

Формат телефонного номера

1. Чтобы настроить формат телефонного номера, укажите количество символов и префикс (символы, которые добавляются в начало телефонного номера, например, код страны).
2. В секции Дополнительные настройки телефонного номера можно указать альтернативный атрибут из каталога пользователей, из которого будет браться телефонный номер для отправки СМС, а также шифровать этот атрибут.

При включении настройки формата происходит нормализация телефонного номера. Это означает следующее:

- пробелы, табуляция, скобочки, дефисы будут удаляться;
- если в строке записаны несколько номеров и разделены запятой или точкой с запятой, будет браться первый номер в строке до разделителя;
- 8 будет заменяться на +7;
- если в номере не хватает +7 или 8 в начале строки, то будет добавляться +7 перед номером;
- в номерах могут быть символы О вместо цифры 0, они будут заменяться обратно на цифры.

Генерация одноразового пароля

В секции Настройки генерации одноразового пароля выполните следующие настройки:

1. В поле Длина одноразового пароля укажите, сколько символов будет содержать одноразовый пароль.
2. В настройке Цифры укажите, будет ли одноразовый пароль содержать цифры.
3. В настройке Строчные латинские буквы укажите, будет ли одноразовый пароль содержать строчные латинские буквы.
4. В настройке Прописные латинские буквы укажите, будет ли одноразовый пароль содержать прописные латинские буквы.
5. В настройке Специальные символы укажите, будет ли одноразовый пароль содержать специальные символы.

Indeed AM SMS Proxy

Indeed AM SMS Proxy (SMS Proxy) — это веб-приложение, которое напрямую подключается к SMPP-шлюзу и отправляет SMS, при этом Indeed Core Server не производит разрыв сессии с SMPP-шлюзом, и запросы отправляются в рамках одного подключения, а не в отдельных для каждого запроса.

Установка SMS Proxy

Чтобы установить SMS Proxy на сервере с операционной системой Linux, выполните следующие действия:

1. Откройте файл *am/.env*.
2. В переменной `COMPOSE_PROFILES` добавьте значение `sms-proxy`.
3. Откройте конфигурационный файл *am/haproxy/haproxy.cfg* и раскомментируйте строки, связанные с компонентом SMS Proxy.
   - Строку с параметром `acl`, в которой упоминается компонент.

     ```
     acl path-sms-proxy  path_beg -i /am/proxies/sms
     ```

   - В параметре `http-request reject unless` добавьте компонент `path-sms-proxy` и разделитель `||` (при необходимости).

     ```
     http-request reject unless path-core || path-idp || path-mc || path-uc ||
     path-ls || path-sms-proxy
     ```

   - Строку с параметром `use_backend`.

     ```
     use_backend Sms_Proxy_Backend  if path-sms-proxy
     ```

   - Строку с адресом компонента в параметре `backend Sms_Proxy_Backend`.

     ```
     backend Sms_Proxy_Backend
      server docker sms-proxy:5443 check inter 5000ms ssl verify required ca-file
     trusted_ca.crt
     ```

4. Перезапустите контейнер с приложением.

Подготовка сертификата для SMS Proxy

1. Чтобы создать сертификат для SMS Proxy, запустите скрипт *am/ssl/generateSmsCert.sh* на хосте, где установлен SMS Proxy:

   ```
   sudo bash ./generateSmsCert.sh
   ```

   > **ПРИМЕЧАНИЕ**
   >
   > Скрипт автоматически заполнит поле с отпечатком сертификата в конфигурационном файле *am/sms-proxy/app-settings.json*.
   >
   > Если SMS Proxy установлен на отдельном от Core Server хосте, то необходимо перенести файл *am/ssl/client/sms-client.pfx* в каталог *am/ssl/client/* хоста, где установлен Core Server.

   Результат:

   - *sms-client.pfx* — сертификат с секретным ключом для Core Server,
   - *sms-client.cer* — публичный ключ сертификата для Core Server.

2. Добавьте сертификат *sms-client.cer* в директорию *am/ssl/ca/* и сертификат *sms-client.pfx* в директорию *am/ssl/client/* на хосте, где установлен Core Server.

3. Запустите скрипт *prepareCaFile.sh* для повторной генерации *trusted_ca.crt*.

   ```
   sudo bash ./prepareCaFile.sh
   ```

   Результат: создается сертификат *am/ssl/ca/trusted_ca.crt*.

   > **ПРИМЕЧАНИЕ**
   >
   > При изменении состава каталога *am/ssl/ca* необходимо перезапустить скрипт *prepareCaFile.sh*.

4. На хосте с Core Server откройте *access-manager.docker-compose.yml* и раскомментируйте строку:

   ```
   #- ./ssl/client/sms-
   client.pfx:/tmp/am_user/.dotnet/corefx/cryptography/x509stores/my/sms-
   client.pfx:ro,Z
   ```

Настройка SMS Proxy в Management Console

1. Откройте Management Console и в разделе Конфигурация→Аутентификаторы выберите SMS OTP или Storage SMS OTP.

2. В разделе Настройки шлюза выберите тип подключения SMS Proxy.

3. В поле Адрес подключения к серверу укажите внешний URL хоста (или балансировщика).

   Пример: *https://!!!HOST_DNS!!!:<номер порта>/am/proxies/sms*

   > **ПОДСКАЗКА**
   >
   > В настройке указывается номер порта, который задан в переменной `ENDPOINT_HTTPS_PORT` в файле *am/.env*.

4. Заполните поле Отпечаток сертификата клиента. Значение можно посмотреть в конфигурационном файле *am/sms-proxy/app-settings.json* в разделе `Authentication": {"Certificate": {"Thumbprint": "" } }`. Значение в параметре задается автоматически после запуска скрипта *am/ssl/generateSmsCert.sh*.

5. В поле Отпечаток сертификата сервера укажите отпечаток сертификата, выпущенный для Docker (или балансировщика).

Редактирование конфигурационного файла

1. Откройте конфигурационный файл *am/sms-proxy/app-settings.json*.

2. В секции `Smpp` заполните следующие параметры:

   - `SystemId` и `Password` — укажите данные аутентификации для подключения к серверу SMPP;
   - `Host` — укажите адрес подключения к серверу SMPP;
   - `Port` — укажите заданный порт для подключения к серверу SMPP;
   - `SystemType` — опциональный параметр входа в систему со стороны сервера SMPP, например S1;
   - `EsmeAddressTon` — тип нумерации. Возможные значения: Unknown, International, National, NetworkSpecific, SubscriberNumber, Alphanumeric, Abbreviated;
   - `EsmeAddressNpi` — индикатор плана нумерации. Возможные значения: Unknown, ISDN, Data, Telex, LandMobile, National, Private, ERMES, IP;
   - `AddressEncoding` — кодировка адреса отправителя и получателя. Возможные значения: GSM 01.38 (по умолчанию), ASCII, utf-8, iso-8859-1;
   - `SslProtocols` — опциональный параметр для указания протокола. Возможные значения: None (по умолчанию), Ssl2, Ssl3, Tls, Default, Tls11, Tls12, Tls13;
   - `LoggingPermissions` — укажите параметр, отвечающий за отображение в логах информации об отправителе и получателе. Можно указать значения через запятую. Возможные параметры:
     - `Source`— отправитель сообщения,
     - `Destination`— получатель сообщения,
     - `None` (значение по умолчанию) — скрываются значения всех логируемых полей,
     - `All` — показываются значения всех логируемых полей.

3. Поле `Publication` включает опциональный параметр `DefaultSource`, содержащий имя отправителя в запросах, например Indeed-AM.

4. В поле `Authentication": {"Certificate":}` указывается отпечаток сертификата, по которому провайдер (SMS или Storage SMS) может быть аутентифицирован в SMS Proxy для отправки сообщений. Заполняется автоматически после запуска скрипта *am/ssl/generateSmsCert.sh*.

   > **ПРИМЕЧАНИЕ**
   >
   > Рекомендуется сначала настроить систему без установки двустороннего TLS-соединения, то есть без использования сертификатов. При настройке SMS Proxy в Management Console оставьте значения отпечатков сертификатов пустыми.

5. Сохраните *app-settings.json* и запустите контейнер с приложением с помощью команды `sudo docker-compose up -d`.

Пример конфигурационного файла

```
{
  "Smpp": {
    "SslProtocols": "Tls12",
    "SystemId": "test",
    "Password": "test",
    "SystemType": "S1",
    "Host": "192.168.0.1",
    "Port": "7777",
    "ReconnectionDelay": "00:02:00",
    "LoggingPermissions": "Source"
  },
  "Publication": {
    "DefaultSource": "OOOIndeed"
  },
  "Documentation": {
    "Enabled": true
  },
  "Debug": {
    "ExceptionResponsesEnabled": true
  },
  "Authentication": {
    "Certificate": {
      "Enabled": false,
      "Thumbprint": "DA38B312C78B5155A2FCC3C1DDC3394D23EEDBF8",
      "ForwardingHeader": "X-IndeedAM-ClientCert"
    },
  "NetworkAddress": {
            "Enabled": true,
            "AnyAddress": true
        }
  },
  "ReverseProxyIntegration": {
    "BasePath": "/am/proxies/sms"
  },
  "Security": {
    "HttpsRedirectionEnabled": false,
    "HttpsExcludePaths": [
      "/healthcheck/",
      "/health-check"
    ]
  },
  "Logging": {
```

```
    "LogLevel": {
      "Default": "Trace",
      "Microsoft.Hosting.Lifetime": "Information"
    }
  },
  "Server": {
    "Certificates": {
      "Default": {
        "Path": "/ssl/server.pfx",
        "Password": "ulRiX7lZ3p4A4kd"
      }
    }
  }
}
```

Двустороннее TLS-соединение

Чтобы установить двустороннее TLS-соединение между серверами Indeed Core Server и Indeed AM SMS Proxy, выполните следующие действия:

1. В конфигурационном файле SMS Proxy укажите следующие параметры.

```
 "Authentication": {
     "Certificate": {
         "Enabled": true,
         "Thumbprint": "!!! Client certificate thumbprint !!!",
         "ForwardingHeader": "X-IndeedAM-ClientCert"
     },
```

- `Authentication:Certificate:Enabled` — для использования двустороннего TLS-соединения необходимо значение true.
- `Authentication:Certificate:ForwardingHeader` — ожидается закодированный Base64 сертификат. Пример: X-IndeedAM-ClientCert.
- `Authentication:Certificate:Thumbprint` — отпечаток клиентского сертификата.

2. Добавьте отпечаток сертификата в Management Console.

Сбор логов

Информация по включению логирования и сбору логов SMS Proxy находится в разделе Сбор логов серверных компонентов.

Indeed AM Storage SMS OTP Provider

Если в качестве хранилища данных Indeed AM вы используете Microsoft SQL, вы можете использовать провайдер Indeed AM Storage SMS OTP. Этот провайдер предоставляет возможность хранения, получения и обновления телефонных номеров пользователей системы Indeed AM в базе данных. Номера телефонов хранятся в зашифрованном виде.

Storage SMS OTP Provider может быть использован для аутентификации в следующих модулях:

- Identity Provider,
- Windows Logon,
- ADFS Extension,
- FreeRadius Extension.

Идентификатор провайдера
`{3F2C1156-B5AF-4643-BFCB-9816012F3F34}`

Установка провайдера Storage SMS OTP

> ⚠ **ВАЖНО**
>
> Если в инфраструктуре используется несколько серверов Indeed AM, то установку провайдера необходимо выполнить на всех серверах инфраструктуры.

Предварительные требования

Для использования Storage SMS OTP Provider необходимо наличие СМС-шлюза. Данный шлюз должен быть доступен с каждого сервера Indeed AM, на котором предполагается установка Storage SMS OTP Provider.

На сервере с Linux

Чтобы установить провайдер на сервере с операционной системой Linux, выполните следующие действия:

1. Откройте файл *am/.env*.
2. В переменной `COMPOSE_PROFILES` добавьте значение `storage-sms-otp`.

На клиентских машинах с Windows

Чтобы установить провайдер на клиентских машинах с операционной системой Windows, выполните следующие действия:

1. Из папки *Indeed AM <Номер версии>\Indeed AM Providers\Indeed AM Storage SMS OTP Provider\Client\<Номер версии>* запустите пакет *IndeedID.SMSOTP.Provider.msi*.

2. Если программа установки предлагает выполнить перезагрузку, подтвердите данное действие. После завершения установки может потребоваться перезагрузка системы.

Удаление/Восстановление продукта осуществляется стандартным для поддерживаемых ОС способом, через меню Панель управления.

Файлы шаблонов политик расположены в папке *Indeed AM <номер версии>\Misc\ADMX Templates*.

Права доступа

Чтобы выдать или отозвать права на использование аутентификатора, выполните следующее:

1. В секции Основные настройки выполните следующие настройки:
   - В настройке Запретить использовать укажите, может ли пользователь использовать или регистрировать выбранный аутентификатор.
2. В секции Доступные пользователю действия выполните следующие настройки:
   - В настройке Регистрация новых аутентификаторов укажите, может ли пользователь регистрировать новые аутентификаторы.
   - В настройке Редактирование имеющихся аутентификаторов укажите, может ли пользователь изменять уже зарегистрированные аутентификаторы.
   - В настройке Удаление имеющихся аутентификаторов укажите, может ли пользователь удалять уже зарегистрированные аутентификаторы.
   - В настройке Разрешить редактирование комментария к аутентификатору укажите, в какой момент пользователь может редактировать комментарии к уже зарегистрированным аутентификаторам.

Блокировка аутентификатора

Чтобы заблокировать аутентификатор, в секции Настройки блокировки аутентификатора выполните следующие настройки:

1. Разрешите или заблокируйте использование Storage OTP в случае серии неудачных попыток аутентификации.
2. В поле Количество попыток аутентификации до блокировки укажите, сколько раз пользователь может совершить неудачную аутентификацию до блокировки способа аутентификации.
3. В поле Сброс счетчика блокировки укажите, сколько минут должно пройти после неудачной попытки аутентификации, прежде чем сбросится счетчик.
4. В поле Таймаут до разблокировки способа входа укажите, через сколько минут заблокированный способ аутентификации станет вновь доступным.

Защита от спама

Механизм защиты от спама основан на расчете процента успешных аутентификаций относительно всех отправленных сообщений за указанный интервал времени. При этом расчет запускается, только если количество отправленных сообщений превышает количество, заданное вами в настройке Окно оценки.

При обнаружении спам-атаки дальнейшая отправка сообщений блокируется на заданный период времени, а при попытке входа возникает ошибка *Potential spam attack detected*.

Отправка сообщений возобновляется либо по истечении заданного периода, либо по достижении определенного количества (в процентном отношении) успешных аутентификаций.

Чтобы настроить защиту от спама, выполните следующее:

1. В Management Console в разделе Конфигурация→Аутентификаторы выберите аутентификатор.
2. В секции Настройки защиты от спама выполните следующие настройки:
   - включите или отключите защиту от спама;
   - в поле Окно оценки попыток аутентификации укажите, в течение какого времени будет выполняться расчет процента успешных попыток входа;
   - в поле Пороговое окно попыток аутентификации укажите, сколько попыток входа должно производиться за время, указанное в окне оценки попыток аутентификации;
   - в поле Процент успешных попыток аутентификации укажите минимальный процент успешных входов относительно всех отправленных сообщений.

Пример

Настройка включена со следующими значениями:

- Окно оценки попыток аутентификации — 600
- Пороговое окно попыток аутентификации — 20
- Процент успешных попыток аутентификации — 85

Защита от спама включится, если произойдет 21 попытка входа (отправлено 21 сообщение). Произойдет блокировка аутентификатора на 600 секунд.

Аутентификатор разблокируется в одном из случаев:

- процент успешных входов (пользователь успешно ввел одноразовый пароль из сообщения) достигнет значения 85;
- прошло 600 секунд с момента блокировки.

ИНФОРМАЦИЯ

События лог-сервера:

- 2090: Обнаружена потенциальная спам-атака. Отправка сообщений приостановлена.
- 1118: Отправка сообщений пользователям возобновлена.

Настройки шлюза

1. В секции Настройка шлюза выберите один из типов подключения:
    - SMS Proxy
    - OneGate
    - MFMSolutions
    - Megafon
2. Укажите адрес подключения к серверу.
3. В зависимотри от типа подключения заполните остальные поля:
    - SMS Proxy: Отпечаток сертификата клиента и Отпечаток сертификата сервера;
    - MFMSolutions: Логин — имя учетной записи для подключения к серверу и Пароль — пароль учетной записи для подключения к серверу;
    - Megafon: Логин — имя учетной записи для подключения к серверу и Пароль — пароль учетной записи для подключения к серверу.

Формат сообщения

1. В поле Отправитель укажите имя отправителя, которое будет отображаться при получении СМС.
2. В поле Дополнительный текст перед OTP введите произвольный текст сообщения, предшествующий одноразовому паролю. По умолчанию отправляется только OTP.
3. Из выпадающего списка Формат даты выберите формат, в котором будет отображаться дата (или дата и время) отправки сообщения в тексте сообщения.

Формат телефонного номера

1. Чтобы настроить формат телефонного номера, укажите количество символов и префикс (символы, которые добавляются в начало телефонного номера, например, код страны).
2. В секции Дополнительные настройки телефонного номера можно настроить, будет ли использоваться номер телефона из каталога пользователей, вместо номера из базы данных.

При включении настройки формата происходит нормализация телефонного номера. Это означает следующее:

- пробелы, табуляция, скобочки, дефисы будут удаляться;

- если в строке записаны несколько номеров и разделены запятой или точкой с запятой, будет браться первый номер в строке до разделителя;
- 8 будет заменяться на +7;
- если в номере не хватает +7 или 8 в начале строки, то будет добавляться +7 перед номером;
- в номерах могут быть символы О вместо цифры 0, они будут заменяться обратно на цифры.

Генерация одноразового пароля

В секции Настройки генерации одноразового пароля выполните следующие настройки:

1. В поле Длина одноразового пароля укажите, сколько символов будет содержать одноразовый пароль.
2. В настройке Цифры укажите, будет ли одноразовый пароль содержать цифры.
3. В настройке Строчные латинские буквы укажите, будет ли одноразовый пароль содержать строчные латинские буквы.
4. В настройке Прописные латинские буквы укажите, будет ли одноразовый пароль содержать прописные латинские буквы.
5. В настройке Специальные символы укажите, будет ли одноразовый пароль содержать специальные символы.

Indeed AM Email OTP Provider

Компонент Email OTP Provider предназначен для аутентификации пользователей с применением технологии одноразовых паролей, доставляемых пользователям по электронной почте.

Одноразовый пароль представляет собой набор случайных символов (цифр, специальных символов и латинских букв). Генерация пароля происходит на сервере Indeed AM, затем пароль передается на сервис рассылки электронной почты, который пересылает его пользователю в виде письма. Передача данных происходит по протоколу SMTP (Simple Mail Transfer Protocol).

Идентификатор провайдера
`{093F612B-727E-44E7-9C95-095F07CBB94B}`

Установка провайдера Email OTP

> ⚠ **ВАЖНО**
>
> Если в инфраструктуре используется несколько серверов Indeed AM, то установку провайдера необходимо выполнить на всех серверах инфраструктуры.

Предварительные требования

Для использования Email OTP Provider необходимо наличие сервера электронной почты. Данный сервер должен быть доступен с каждого сервера Indeed Access Manager, на котором предполагается установка Email OTP Provider.

Для использования аутентификатора у пользователя должен быть задан адрес электронной почты в атрибуте службы каталогов *mail*, иначе аутентификатор будет не доступен для использования.

Регистрация аутентификатора в User Console не требуется.

На сервере с Linux

Чтобы установить провайдер на сервере с операционной системой Linux, выполните следующие действия:

1. Откройте файл *am/.env*.
2. В переменной `COMPOSE_PROFILES` добавьте значение `amsmtp`.

На клиентских машинах с Windows

Чтобы установить провайдер на клиентских машинах с операционной системой Windows, выполните следующие действия:

1. Из папки *Indeed AM <Номер версии>\Indeed AM Providers\Indeed AM Email OTP Provider\Server\<Номер версии>* запустите пакет *IndeedAM.AuthProviders.AMSMTP-<номер версии>.<разрядность>.ru-ru.msi*.
2. Если программа установки предлагает выполнить перезагрузку, подтвердите данное действие. После завершения установки может потребоваться перезагрузка системы.

Удаление/Восстановление продукта осуществляется стандартным для поддерживаемых ОС способом, через меню Панель управления.

Файлы шаблонов политик расположены в папке *Indeed AM <номер версии>*\Misc\ADMX Templates*.

Настройка параметра с электронной почтой

Чтобы изменить значение параметра с электронной почтой, заданного по умолчанию: добавьте следующие параметры в :

1. Откройте конфигурационный файл сервера *am/core/app-settings.json*.
2. В секцию `Ldap` добавьте параметры `userMapRules:Attributes:Email`.
3. В параметре `Email` задайте значение, соответствующее необходимому атрибуту из каталога пользователей.

Пример

```
"Ldap": [{
  ...
  "userMapRules": {
    "Attributes": {
      "Email": "otherMailbox"
    }
  }
}
```

Настройка провайдера Email OTP в Management Console

Права доступа

Чтобы выдать или отозвать права на использование аутентификатора, выполните следующее:

1. В Management Console в разделе Конфигурация→Аутентификаторы из списка выберите аутентификатор Email OTP.
2. В секции Основные настройки выполните следующие настройки:
    - В настройке Запретить использовать укажите, может ли пользователь использовать или регистрировать выбранный аутентификатор.

Блокировка аутентификатора

Чтобы заблокировать аутентификатор, выполните следующее:

1. В Management Console в разделе Конфигурация→Аутентификаторы из списка выберите аутентификатор Email OTP.
2. В секции Настройки блокировки аутентификатора выполните следующие настройки:
    - Разрешите или заблокируйте использование Email OTP в случае серии неудачных попыток аутентификации;
    - В поле Количество попыток аутентификации до блокировки укажите, сколько раз пользователь может совершить неудачную аутентификацию до блокировки способа аутентификации;
    - В поле Сброс счетчика блокировки укажите, сколько минут должно пройти после неудачной попытки аутентификации, прежде чем сбросится счетчик;
    - В поле Таймаут до разблокировки способа входа укажите, через сколько минут заблокированный способ аутентификации станет вновь доступным.

Защита от спама

Механизм защиты от спама основан на расчете процента успешных аутентификаций относительно всех отправленных сообщений за указанный интервал времени. При этом расчет запускается, только если количество отправленных сообщений превышает количество, заданное вами в настройке Окно оценки.

При обнаружении спам-атаки дальнейшая отправка сообщений блокируется на заданный период времени, а при попытке входа возникает ошибка *Potential spam attack detected*.

Отправка сообщений возобновляется либо по истечении заданного периода, либо по достижении определенного количества (в процентном отношении) успешных аутентификаций.

Чтобы настроить защиту от спама, выполните следующее:

1. В Management Console в разделе Конфигурация→Аутентификаторы выберите аутентификатор.
2. В секции Настройки защиты от спама выполните следующие настройки:
    - включите или отключите защиту от спама;

- в поле Окно оценки попыток аутентификации укажите, в течение какого времени будет выполняться расчет процента успешных попыток входа;
- в поле Пороговое окно попыток аутентификации укажите, сколько попыток входа должно производиться за время, указанное в окне оценки попыток аутентификации;
- в поле Процент успешных попыток аутентификации укажите минимальный процент успешных входов относительно всех отправленных сообщений.

Пример

Настройка включена со следующими значениями:

- Окно оценки попыток аутентификации — 600
- Пороговое окно попыток аутентификации — 20
- Процент успешных попыток аутентификации — 85

Защита от спама включится, если произойдет 21 попытка входа (отправлено 21 сообщение). Произойдет блокировка аутентификатора на 600 секунд.

Аутентификатор разблокируется в одном из случаев:

- процент успешных входов (пользователь успешно ввел одноразовый пароль из сообщения) достигнет значения 85;
- прошло 600 секунд с момента блокировки.

ИНФОРМАЦИЯ

События лог-сервера:

- 2090: Обнаружена потенциальная спам-атака. Отправка сообщений приостановлена.
- 1118: Отправка сообщений пользователям возобновлена.

Настройки SMTP-сервера

Чтобы задать настройки для работы с SMTP-сервером, перейдите в секцию Настройки SMTP и выполните следующие действия:

1. Укажите адрес подключения к серверу (DNS-имя, IP-адрес).
2. Укажите порт подключения к серверу.
3. Укажите имя учетной записи для подключению к серверу и пароль учетной записи для подключения к серверу.
4. В поле Тип соединения выберите необходимое значение:
   - Незащищенное
   - TLS

- SSL

5. В поле Таймаут сервера укажите время ожидания ответа от сервера в секундах.

Настройки Email

1. В секции Настройки Email укажите почту и имя отправителя, тему и текст письма.
2. В поле Текст письма необходимо указать место вставки одноразового пароля с помощью тега <`otp`>.
3. Из выпадающего списка Формат даты выберите формат, в котором будет отображаться дата (или дата и время) отправки сообщения.

Настройка одноразового пароля

Настройки применяются к серверам Indeed AM и позволяет задать длину и вхождение групп символов при генерации одноразового пароля.

Чтобы настроить генерацию одноразового пароля, в секции Настройки генерации одноразового пароля выполните следующие настройки:

1. В поле Длина одноразового пароля укажите, сколько символов будет содержать одноразовый пароль;
2. В настройке Цифры укажите, будет ли одноразовый пароль содержать цифры;
3. В настройке Строчные латинские буквы укажите, будет ли одноразовый пароль содержать строчные латинские буквы;
4. В настройке Прописные латинские буквы укажите, будет ли одноразовый пароль содержать прописные латинские буквы;
5. В настройке Специальные символы укажите, будет ли одноразовый пароль содержать специальные символы.

Indeed AM Hardware OTP

Автономный генератор одноразовых паролей eToken PASS можно использовать для аутентификации в любых приложениях и службах, поддерживающих протокол аутентификации RADIUS: VPN, Microsoft ISA, Microsoft IIS, Outlook Web Access и др. Подробную информацию об устройстве eToken PASS вы можете получить на официальном сайте компании Aladdin.

В eToken PASS реализован алгоритм генерации одноразовых паролей (One-Time Password – OTP). Этот алгоритм основан на алгоритме HMAC и хеш-функции SHA-1. Для расчета значения OTP принимаются два входных параметра – секретный ключ (начальное значение для генератора) и текущее значение счетчика (количество необходимых циклов генерации). Начальное значение хранится как в самом устройстве, так и на сервере в системе Indeed. Счетчик в устройстве увеличивается при каждой генерации OTP, на сервере – при каждой удачной аутентификации по OTP.

Провайдер Indeed AM Hardware OTP может быть использован для аутентификации в следующих модулях:

- Identity Provider,
- ADFS Extension,
- FreeRADIUS Extension,
- RDP Windows Logon,
- Windows Logon.

Идентификатор провайдера
`{AD3FBA95-AE99-4773-93A3-6530A29C7556}`

Установка провайдера Hardware OTP

> ⚠ **ВАЖНО**
>
> Если в инфраструктуре используется несколько серверов Indeed AM, то установку провайдера необходимо выполнить на всех серверах инфраструктуры.

На сервере с Linux

Чтобы установить провайдер на сервере с операционной системой Linux, выполните следующие действия:

1. Откройте файл *am/.env*.
2. В переменной `COMPOSE_PROFILES` добавьте значение `hotp`.

На клиентских машинах с Windows

Чтобы установить провайдер на клиентских машинах с операционной системой Windows, выполните следующие действия:

1. Из папки *Indeed AM <Номер версии>\Indeed AM Providers\Indeed AM HOTP Provider\<Номер версии>* запустите пакет *IndeedAM.AuthProviders.HOTP-<номер версии>.<разрядность>.ru-ru.msi*.
2. Если программа установки предлагает выполнить перезагрузку, подтвердите данное действие. После завершения установки может потребоваться перезагрузка системы.

Удаление/Восстановление продукта осуществляется стандартным для поддерживаемых ОС способом, через меню Панель управления.

Файлы шаблонов политик расположены в папке *Indeed AM <номер версии>\Misc\ADMX Templates*.

Настройка провайдера Hardware OTP в Management Console

Для настройки Hardware OTP в Management Console перейдите в раздел Конфигурация→Аутентификаторы и выберите аутентификатор Hardware HOTP.

Права доступа

Чтобы выдать или отозвать права на использование аутентификатора, выполните следующее:

1. В секции Основные настройки выполните следующие настройки:
   - В настройке Запретить использовать укажите, может ли пользователь использовать или регистрировать выбранный аутентификатор.
2. В секции Доступные пользователю действия выполните следующие настройки:
   - В настройке Регистрация новых аутентификаторов укажите, может ли пользователь регистрировать новые аутентификаторы.
   - В настройке Редактирование имеющихся аутентификаторов укажите, может ли пользователь изменять уже зарегистрированные аутентификаторы.
   - В настройке Удаление имеющихся аутентификаторов укажите, может ли пользователь удалять уже зарегистрированные аутентификаторы.
   - В настройке Разрешить редактирование комментария к аутентификатору укажите, в какой момент пользователь может редактировать комментарии к уже зарегистрированным аутентификаторам.

Блокировка аутентификатора

Чтобы заблокировать аутентификатор, перейдите в секцию Настройки блокировки аутентификатора и выполните следующие настройки:

1. Разрешите или заблокируйте использование Hardware OTP в случае серии неудачных попыток аутентификации.
2. В поле Количество попыток аутентификации до блокировки укажите, сколько раз пользователь может совершить неудачную аутентификацию до блокировки способа аутентификации.
3. В поле Сброс счетчика блокировки укажите, сколько минут должно пройти после неудачной попытки аутентификации, прежде чем сбросится счетчик.
4. В поле Таймаут до разблокировки способа входа укажите, через сколько минут заблокированный способ аутентификации станет вновь доступным.

Настройки одноразового пароля

Чтобы настроить генерацию одноразового пароля, выполните следующее:

1. Перейдите в секцию Настройки OTP.
2. В настройке Количество периодов сравнения укажите, сколько периодов обновления OTP должно пройти, по истечении которых пароль будет считаться недействительным.
3. В настройке Окно синхронизации задайте значение счетчика при синхронизации.

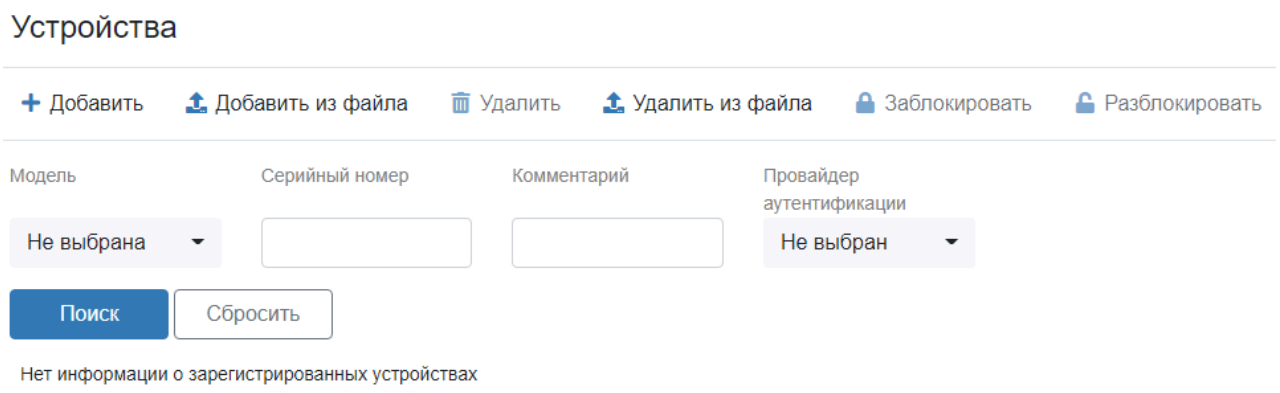
Добавление устройства

> **ИНФОРМАЦИЯ**
>
> Одно устройство может быть зарегистрировано только для одного пользователя

Для добавления устройства необходимо выполнить следующее:

1. Откройте консоль управления Management Console.
2. Перейдите на вкладку Устройства.
3. Нажмите Добавить или Добавить из файла.

> **ПРИМЕЧАНИЕ**
>
> Вы можете добавить устройство, выбрав файл с параметрами устройства (Добавить из файла), либо указать параметры вручную (Добавить).



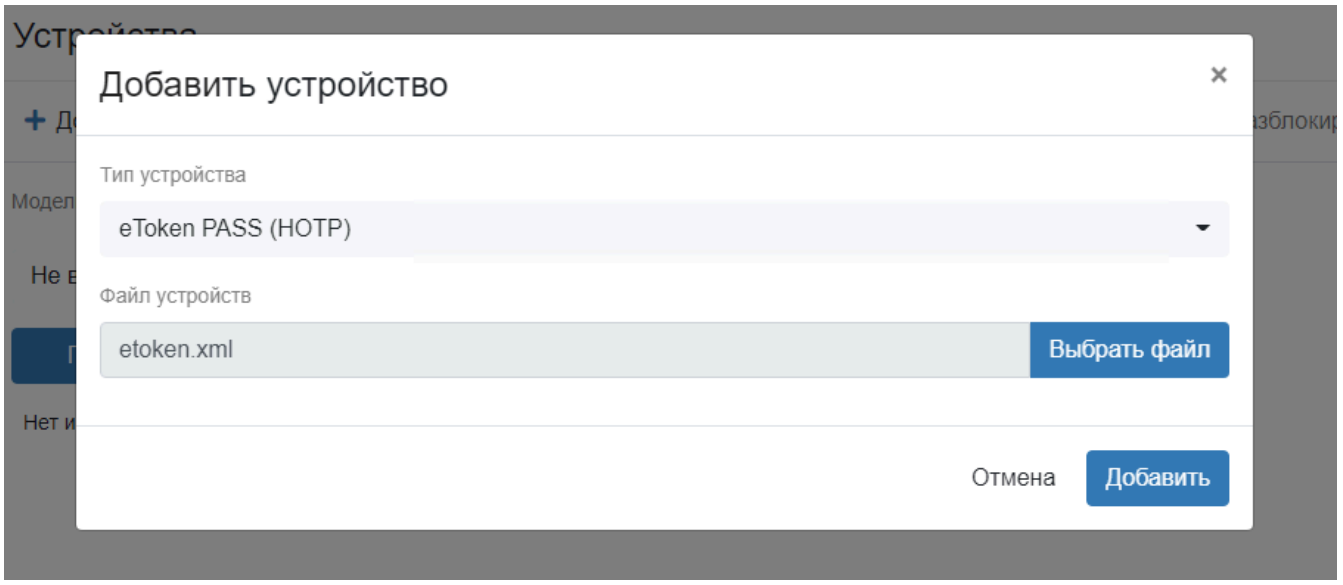
Добавление из файла

1. Нажмите Добавить из файла.
2. Выберите файл формата XML с параметрами устройства и нажмите Добавить.

Пример конфигурации устройства

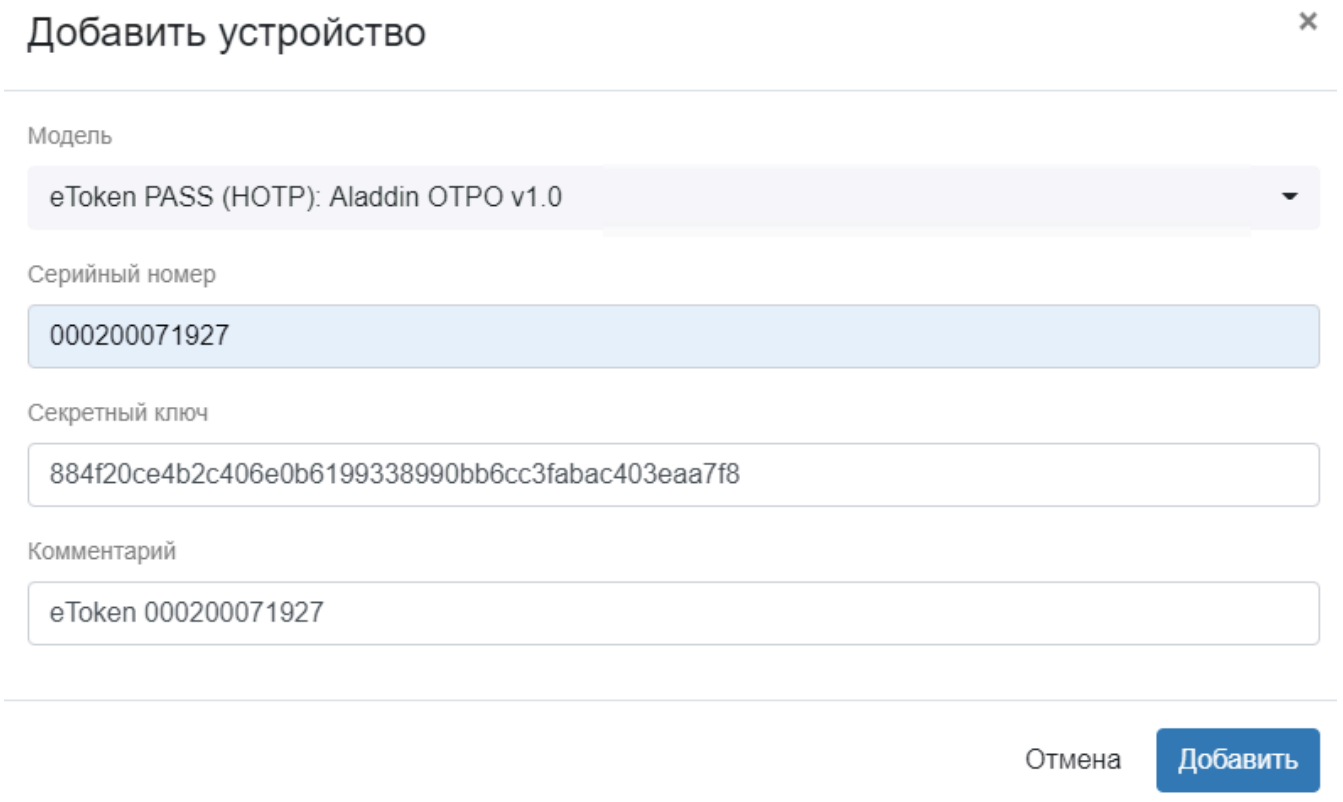
```
            <Tokens xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
                <Token serial="000200071927">
                        <CaseModel>5</CaseModel>
                        <Model>109</Model>
                        <ProductionDate>11/4/2008</ProductionDate>
                        <ProductName>Aladdin OTPO v1.0</ProductName>
                    <Applications>
                        <Application ConnectorID="{a61c4073-2fc8-4170-99d1-
9f5b70a2cec6}">

<Seed>884f20ce4b2c406e0b6199338990bb6cc3fabac403eaa7f8</Seed>
                        <MovingFactor>1</MovingFactor>
                        </Application>
                    </Applications>
                </Token>
            </Tokens>
```



Добавление вручную

1. Нажмите Добавить.
2. В поле Серийный номер укажите серийный номер устройства.
3. В поле Секретный ключ укажите seed устройства.
4. Поле Комментарий — необязательный параметр.
5. Нажмите Добавить.

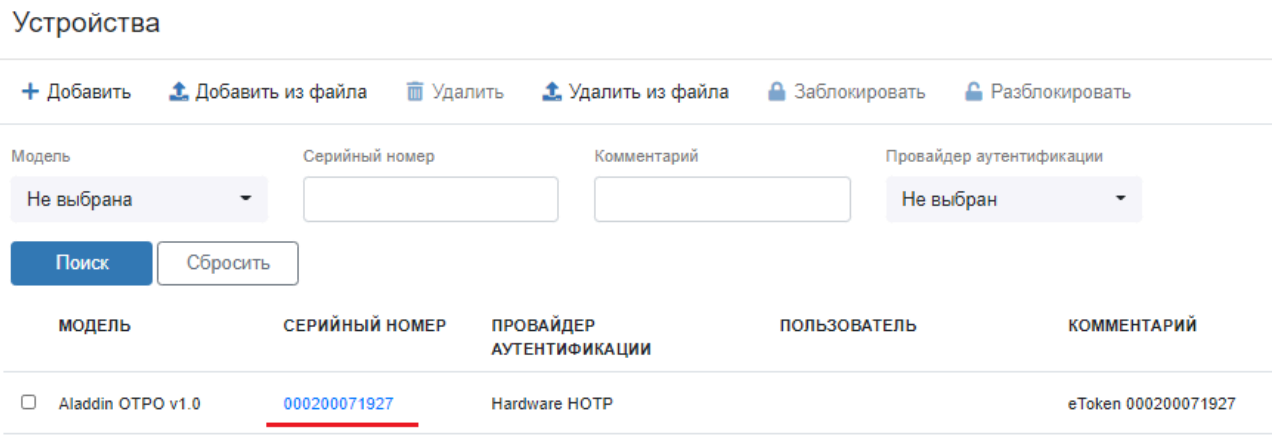


Редактирование устройства

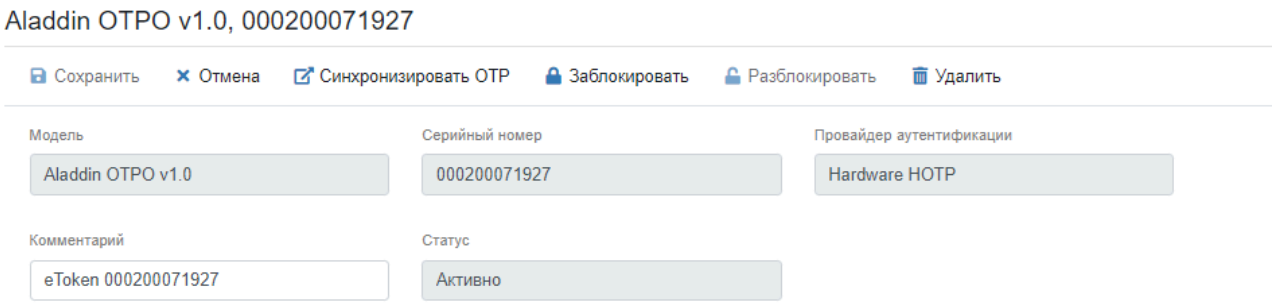
Для редактирования устройства выполните следующие действия:

1. Откройте консоль управления Management Console.
2. Перейдите на вкладку Устройства.
3. Нажмите серийный номер устройства.

> **ИНФОРМАЦИЯ**
>
> При необходимости можно выполнить поиск, используя фильтры в верхней части страницы.



4. В окне редактирования можно изменить комментарий, заблокировать устройство или синхронизировать.
5. После внесения изменений нажмите Сохранить.



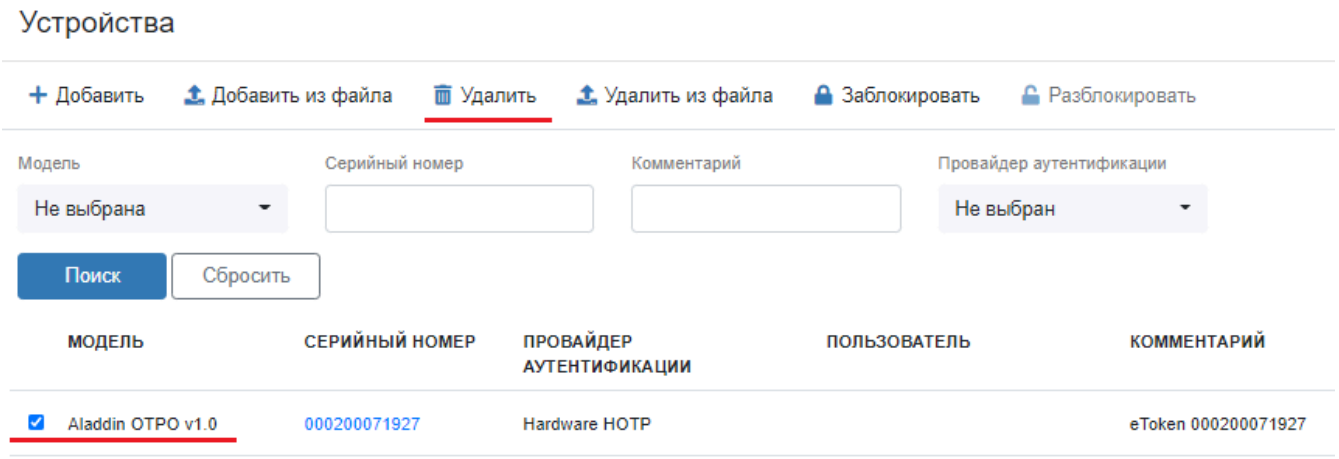
Удаление устройства

Для удаления устройства выполните следующие действия:

1. Откройте консоль управления Management Console.
2. Перейдите на вкладку Устройства.
3. Выберите устройство и нажмите Удалить.

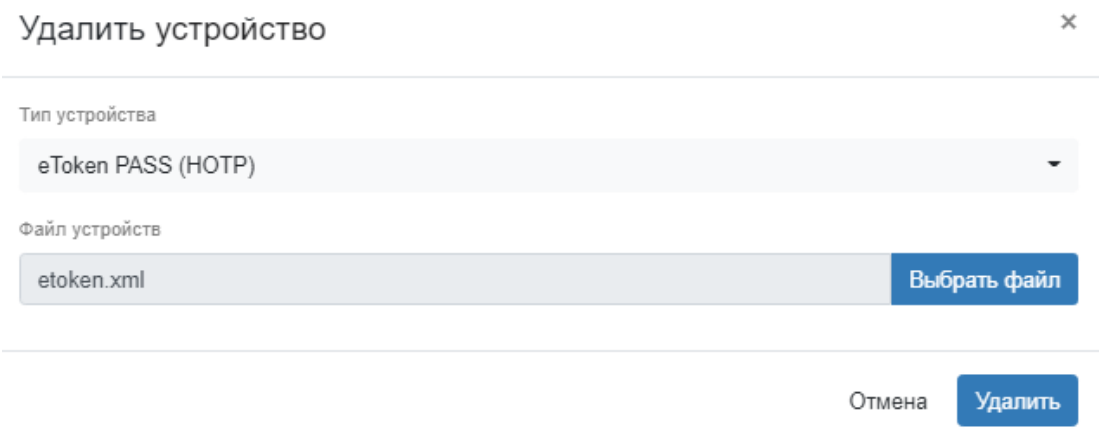
ИНФОРМАЦИЯ

При необходимости можно выполнить поиск, используя фильтры в верхней части страницы.



Удаление из файла

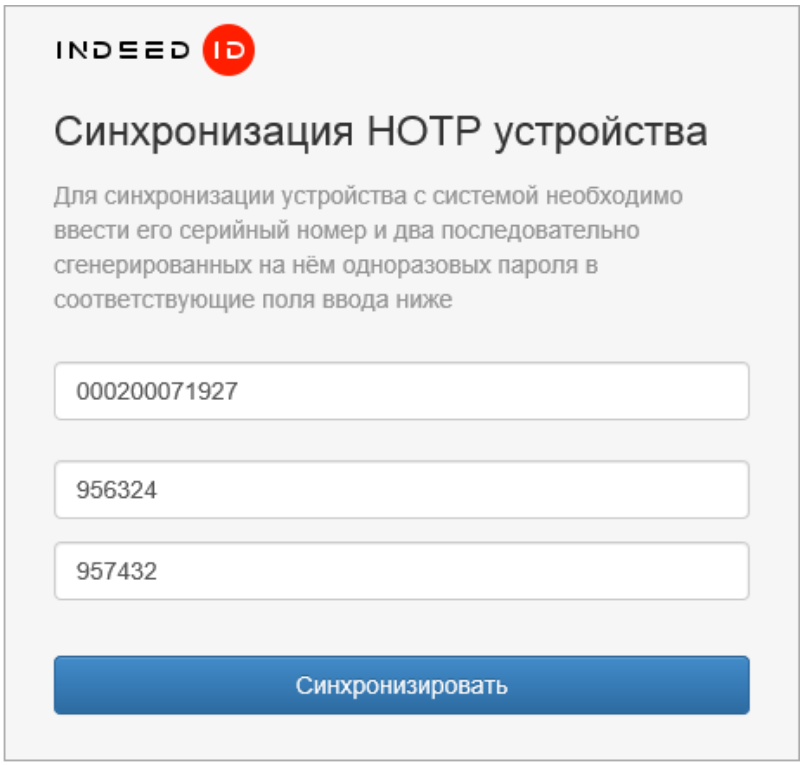
1. Для удаления устройства по информации из файла нажмите Удалить из файла.
2. Выберите файл конфигурации устройства.
3. Нажмите Удалить.



Синхронизация устройства

Для синхронизации устройства выполните следующие действия:

1. Откройте консоль управления Management Console.
2. Перейдите на вкладку Устройства.
3. Нажмите серийный номер устройства.
4. Выберите Синхронизировать OTP.
5. В поле Одноразовый пароль 1 и Одноразовый пароль 2 укажите пароли с устройства и нажмите Синхронизировать.


INDEED ID
Синхронизация HOTP устройства
Для синхронизации устройства с системой необходимо ввести его серийный номер и два последовательно сгенерированных на нём одноразовых пароля в соответствующие поля ввода ниже
000200071927
956324
957432
Синхронизировать

Indeed AM Hardware TOTP

Провайдер Indeed AM Hardware TOTP может быть использован для аутентификации в следующих модулях:

- Identity Provider,
- ADFS Extension,
- FreeRadius Extension,
- RDP Windows Logon.

Hardware TOTP позволяет получать одноразовые пароли с помощью следующих устройств:

- Автономный генератор одноразовых паролей eToken PASS. Его можно использовать для аутентификации в любых приложениях и службах, поддерживающих протокол аутентификации FreeRADIUS — VPN, Microsoft ISA, Microsoft IIS, Outlook Web Access и других.
- Токен для надежной защиты доступа к данным аккаунтов Рутокен OTP. Он используется для аутентификации в корпоративных сервисах и порталах, сервисах аутентификации, приложениях и сервисах управления паролями, а также в других сервисах, поддерживающих технологию OATH TOTP.

Таблица сравнения характеристик устройств

Устройство	Формат файла	Алгоритм	Период обновления
eToken Pass	XML	SHA1	30 секунд
Рутокен OTP	CSV	SHA1, SHA256	30, 60 секунд

Идентификатор провайдера
`{CEB3FEAF-86ED-4A5A-BD3F-6A7B6E60CA05}`

Установка провайдера Hardware TOTP

> ⚠ **ВАЖНО**
>
> Если в инфраструктуре используется несколько серверов Indeed AM, то установку провайдера необходимо выполнить на всех серверах инфраструктуры.

На сервере с Linux
Чтобы установить провайдер на сервере с операционной системой Linux, выполните следующие действия:

1. Откройте файл *am/.env*.
2. В переменной `COMPOSE_PROFILES` добавьте значение `hardware-totp`.

На клиентских машинах с Windows

Чтобы установить провайдер на клиентских машинах с операционной системой Windows, выполните следующие действия:

1. Из папки *Indeed AM <Номер версии>\Indeed AM Providers\Indeed AM Hardware TOTP Provider\<Номер версии>* запустите пакет *IndeedAM.AuthProviders.HardwareTOTP-<номер версии>.<разрядность>.ru-ru.msi*.

2. Если программа установки предлагает выполнить перезагрузку, подтвердите данное действие. После завершения установки может потребоваться перезагрузка системы.

Удаление/Восстановление продукта осуществляется стандартным для поддерживаемых ОС способом, через меню Панель управления.

Файлы шаблонов политик расположены в папке *Indeed AM <номер версии>\Misc\ADMX Templates*.

Настройка провайдера Hardware TOTP в Management Console

Для настройки Hardware TOTP в Management Console перейдите в раздел Конфигурация→Аутентификаторы и выберите аутентификатор Hardware TOTP.

Права доступа

Чтобы выдать или отозвать права на использование аутентификатора, выполните следующее:

1. В секции Основные настройки выполните следующие настройки:
   - В настройке Запретить использовать укажите, может ли пользователь использовать или регистрировать выбранный аутентификатор.
2. В секции Доступные пользователю действия выполните следующие настройки:
   - В настройке Регистрация новых аутентификаторов укажите, может ли пользователь регистрировать новые аутентификаторы.
   - В настройке Редактирование имеющихся аутентификаторов укажите, может ли пользователь изменять уже зарегистрированные аутентификаторы.
   - В настройке Удаление имеющихся аутентификаторов укажите, может ли пользователь удалять уже зарегистрированные аутентификаторы.
   - В настройке Разрешить редактирование комментария к аутентификатору укажите, в какой момент пользователь может редактировать комментарии к уже зарегистрированным аутентификаторам.

Блокировка аутентификатора

Чтобы заблокировать аутентификатор, в секции Настройки блокировки аутентификатора выполните следующие настройки:

1. Разрешите или заблокируйте использование Hardware TOTP в случае серии неудачных попыток аутентификации.
2. В поле Количество попыток аутентификации до блокировки укажите, сколько раз пользователь может совершить неудачную аутентификацию до блокировки способа аутентификации.
3. В поле Сброс счетчика блокировки укажите, сколько минут должно пройти после неудачной попытки аутентификации, прежде чем сбросится счетчик.
4. В поле Таймаут до разблокировки способа входа укажите, через сколько минут заблокированный способ аутентификации станет вновь доступным.

Настройки одноразового пароля

Чтобы настроить генерацию одноразового пароля, выполните следующее:

1. Перейдите в секцию Настройки OTP.
2. В настройке Количество периодов сравнения укажите, сколько периодов обновления OTP должно пройти, по истечении которых пароль будет считаться недействительным.
3. В настройке Окно синхронизации задайте значение счетчика при синхронизации.

Добавление устройства

Вы можете добавить устройство вручную или через загрузку файла с параметрами устройства.

Устройство может быть зарегистрировано только для одного пользователя

Добавление вручную

Устройство Рутокен OTP

Для добавления устройства Рутокен OTP выполните следующие действия:

1. Откройте консоль управления Management Console.
2. В меню слева выберите Устройства.
3. Нажмите Добавить устройство.
4. В открывшемся окне выберите *Rutoken OTP*.
5. Заполните поля Серийный номер, Секретный ключ, Период обновления и Комментарий (это необязательное поле) и нажмите Добавить.

> ⚠ **ВАЖНО**
>
> При добавлении Рутокен OTP вручную вы можете указать секретный ключ в двух форматах — HEX и Base32.

Устройство eToken PASS

Для добавления устройства eToken PASS выполните следующие действия:

1. Откройте консоль управления Management Console.
2. В меню слева выберите Устройства.
3. Нажмите Добавить устройство.
4. В открывшемся окне выберите модель eToken PASS.
5. Заполните поля Серийный номер, Секретный ключ и Комментарий (это необязательное поле) и нажмите Добавить.

Добавление из файла

Устройство Рутокен OTP

Для добавления устройства Рутокен OTP выполните следующие действия:

> ⚠ **ВАЖНО**
>
> При добавлении Рутокен OTP через файл вы можете указать секретный ключ только в одном формате — Base32.

1. Откройте консоль управления Management Console.
2. В меню слева выберите Устройства.
3. Нажмите Добавить из файла.
4. В открывшемся окне выберите *Rutoken OTP* и нажмите Выбрать файл.
5. В открывшемся окне выберите файл формата CSV с параметрами устройства и нажмите Добавить.

> 💡 **СОВЕТ**
>
> Подробную информацию по настройке устройства вы можете найти в руководстве по использованию Рутокен OTP.

Устройство eToken PASS

Для добавления устройства eToken PASS выполните следующие действия:

1. Откройте консоль управления Management Console.
2. В меню слева выберите Устройства.
3. Нажмите Добавить из файла.
4. В открывшемся окне выберите модель eToken PASS.
5. В открывшемся окне выберите файл формата XML с параметрами устройства и нажмите Добавить.

Синхронизация устройства

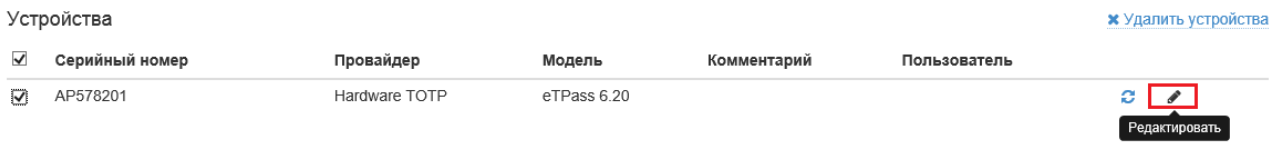
Для синхронизации устройства выполните следующие действия:

1. Откройте консоль управления Management Console.
2. В меню слева выберите Устройства.
3. Из списка выберите устройство и нажмите Синхронизировать.
4. В открывшемся новом окне в поле Одноразовый пароль 1 и Одноразовый пароль 2 укажите пароли с устройства и нажмите Синхронизировать.

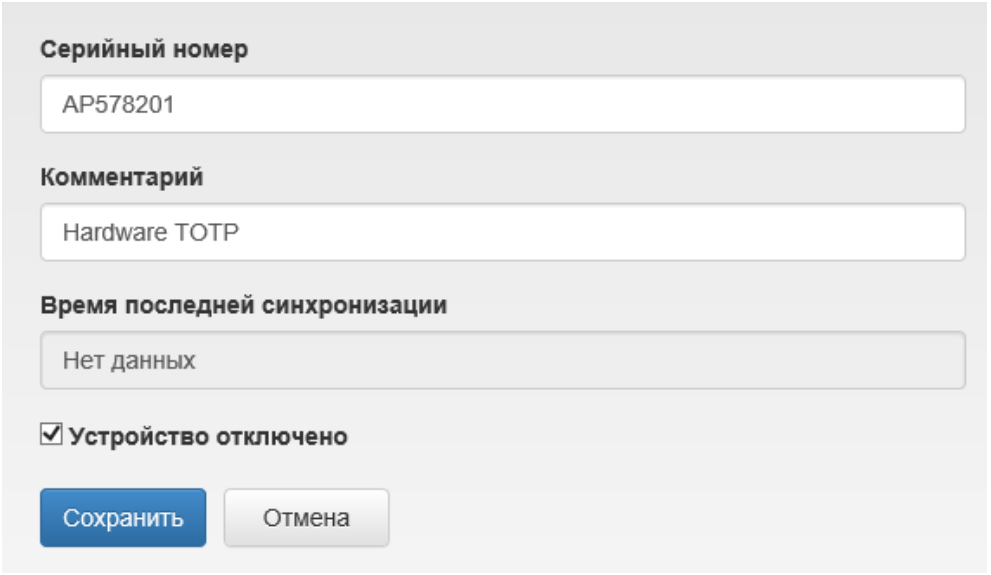
Изменение серийного номера и отключение устройства

Для редактирования устройства выполните следующие действия:

1. Откройте консоль управления Management Console.
2. В меню слева выберите Устройства.
3. В выпадающем списке Провайдер аутентификации выберите *Hardware TOTP*, в поле Серийный номер, если известно, укажите серийный номер устройства и нажмите Поиск.
4. Выберите найденное устройство и нажмите значок редактирования.



5. В окне редактирования можно изменить серийный номер устройства, комментарий или отключить устройство. После внесения изменений нажмите Сохранить.



Удаление устройства

Вы можете удалить устройство вручную или через загрузку файла с параметрами устройства.

Удаление вручную

Для удаления устройства выполните следующие действия:

1. Откройте консоль управления Management Console.
2. В меню слева выберите Устройства.
3. В выпадающем списке Провайдер аутентификации выберите *Hardware TOTP*, в поле Серийный номер, если известно, укажите серийный номер устройства и нажмите Поиск.
4. Выберите найденное устройство и нажмите Удалить устройство.
5. В открывшемся окне подтвердите удаление.

Удаление из файла

Устройство Рутокен OTP

Для удаления устройства Рутокен OTP выполните следующие действия:

1. Откройте консоль управления Management Console.
2. В меню слева выберите Устройства.
3. Нажмите Удалить из файла.
4. В открывшемся окне выберите *Rutoken OTP* и нажмите Выбрать файл.
5. В открывшемся окне выберите файл формата CSV с параметрами устройства и нажмите Удалить.

СОВЕТ

Подробную информацию по настройке устройства вы можете найти в руководстве по использованию Рутокен OTP.

Устройство eToken PASS

Для удаления устройства eToken PASS выполните следующие действия:

1. Откройте консоль управления Management Console.
2. В меню слева выберите Устройства.
3. Нажмите Удалить из файла.
4. В открывшемся окне выберите модель eToken PASS.
5. В открывшемся окне выберите файл формата XML с параметрами устройства и нажмите Удалить.

Indeed Key Provider

Для аутентификации с помощью push-уведомлений есть следующие требования:

- В сетевой инфраструктуре:
  - Установка сервера Indeed Key Server. Данный сервер выполняет отправку уведомлений на смартфон пользователя с помощью сервисов API Google.
  - Установка провайдера аутентификации Indeed Key. Установка провайдера позволит использовать данную технологию аутентификации в целевых сценариях.
- На стороне клиента:
  - Установка приложения Indeed Key. Приложение необходимо для получения уведомлений об аутентификации в целевых приложениях с помощью компонентов Indeed Access Manager.

Без установки Indeed Key Server, Indeed Key Provider и приложения Indeed Key аутентификация с помощью push-уведомлений невозможна.

Indeed Key Provider может быть использован для аутентификации в следующих модулях:

- Identity Provider,
- Windows Logon,
- ADFS Extension,
- FreeRadius Extension,
- LDAP Proxy,
- RDP Windows Logon (только в режиме отправки push-уведомлений с подтверждением входа).

Идентификатор провайдера
`{DEEF0CB8-AD2F-4B89-964A-B6C7ECA80C68}`

Установка провайдера Indeed Key

> ⚠ **ВАЖНО**
>
> Если в инфраструктуре используется несколько серверов Indeed AM, то установку провайдера необходимо выполнить на всех серверах инфраструктуры.

На сервере с Linux

Чтобы установить провайдер на сервере с операционной системой Linux, выполните следующие действия:

1. Откройте файл *am/.env*.
2. В переменной `COMPOSE_PROFILES` добавьте значение `indeed-key`.

На клиентских машинах с Windows

Чтобы установить провайдер на клиентских машинах с операционной системой Windows, выполните следующие действия:

1. Из папки *Indeed AM <Номер версии>\Indeed AM Providers\Indeed AM AirKey Provider\Client\<Номер версии>* запустите пакет *IndeedID.IndeedKey.Provider.msi* на клиентской машине с компонентом Windows Logon.
2. Если программа установки предлагает выполнить перезагрузку, подтвердите данное действие. После завершения установки может потребоваться перезагрузка системы.

Удаление/Восстановление продукта осуществляется стандартным для поддерживаемых ОС способом, через меню Панель управления.

Файлы шаблонов политик расположены в папке *Indeed AM <номер версии>*\Misc\ADMX Templates*.

Настройка провайдера Indeed Key в Management Console

Для настройки Indeed Key в Management Console в разделе Конфигурация→Аутентификаторы выберите аутентификатор Indeed Key.

Настройка прав доступа

Чтобы выдать или отозвать права на использование аутентификатора, выполните следующее:

1. В секции Основные настройки выполните следующие настройки:
   - В настройке Запретить использовать укажите, может ли пользователь использовать или регистрировать выбранный аутентификатор.
2. В секции Доступные пользователю действия выполните следующие настройки:
   - В настройке Регистрация новых аутентификаторов укажите, может ли пользователь регистрировать новые аутентификаторы;
   - В настройке Редактирование имеющихся аутентификаторов укажите, может ли пользователь изменять уже зарегистрированные аутентификаторы;
   - В настройке Удаление имеющихся аутентификаторов укажите, может ли пользователь удалять уже зарегистрированные аутентификаторы;
   - В настройке Разрешить редактирование комментария к аутентификатору укажите, в какой момент пользователь может редактировать комментарии к уже зарегистрированным аутентификаторам.

Настройка блокировки аутентификатора

Чтобы заблокировать аутентификатор, в секции Настройки блокировки аутентификатора выполните следующие настройки:

1. Разрешите или заблокируйте использование Indeed Key в случае серии неудачных попыток аутентификации.
2. В поле Количество попыток аутентификации до блокировки укажите, сколько раз пользователь может совершить неудачную аутентификацию до блокировки способа аутентификации.
3. В поле Сброс счетчика блокировки укажите, сколько минут должно пройти после неудачной попытки аутентификации, прежде чем сбросится счетчик.
4. В поле Таймаут до разблокировки способа входа укажите, через сколько минут заблокированный способ аутентификации станет вновь доступным.

Защита от спама

Механизм защиты от спама основан на расчете процента успешных аутентификаций относительно всех отправленных сообщений за указанный интервал времени. При этом расчет запускается, только если количество отправленных сообщений превышает количество, заданное вами в настройке Окно оценки.

При обнаружении спам-атаки дальнейшая отправка сообщений блокируется на заданный период времени, а при попытке входа возникает ошибка *Potential spam attack detected*.

Отправка сообщений возобновляется либо по истечении заданного периода, либо по достижении определенного количества (в процентном отношении) успешных аутентификаций.

Чтобы настроить защиту от спама, выполните следующее:

1. В Management Console в разделе Конфигурация→Аутентификаторы выберите аутентификатор.
2. В секции Настройки защиты от спама выполните следующие настройки:
    - включите или отключите защиту от спама;
    - в поле Окно оценки попыток аутентификации укажите, в течение какого времени будет выполняться расчет процента успешных попыток входа;
    - в поле Пороговое окно попыток аутентификации укажите, сколько попыток входа должно производиться за время, указанное в окне оценки попыток аутентификации;
    - в поле Процент успешных попыток аутентификации укажите минимальный процент успешных входов относительно всех отправленных сообщений.

Пример

Настройка включена со следующими значениями:

- Окно оценки попыток аутентификации — 600
- Пороговое окно попыток аутентификации — 20
- Процент успешных попыток аутентификации — 85

Защита от спама включится, если произойдет 21 попытка входа (отправлено 21 сообщение). Произойдет блокировка аутентификатора на 600 секунд.

Аутентификатор разблокируется в одном из случаев:

- процент успешных входов (пользователь успешно ввел одноразовый пароль из сообщения) достигнет значения 85;
- прошло 600 секунд с момента блокировки.

ИНФОРМАЦИЯ

События лог-сервера:

- 2090: Обнаружена потенциальная спам-атака. Отправка сообщений приостановлена.
- 1118: Отправка сообщений пользователям возобновлена.

Серверные настройки

Чтобы настроить сервер, к которому обращается приложение Indeed Key, в секции Серверные настройки выполните следующие настройки:

1. В поле URL-адрес Indeed Key Server укажите адрес, по которому сервер Indeed Key доступен с машины Indeed AM;
2. В поле Доверенный ID Indeed Key Server укажите произвольный уникальный идентификатор. Значение идентификатора должно совпадать со значением, указанным в конфигурационном файле Indeed Key Server (тег `TrustedClients`).

Режим работы Indeed Key

В настройке Режим работы выберите, какой способ подтверждения входа будет использоваться в приложении:

- Push — пользователь будет получать push-уведомления с возможностью отклонить или подтвердить вход.
- OTP — вместо push-уведомлений пользователь получит одноразовый код.

Настройки мобильного приложения

Чтобы настроить мобильное приложение Indeed Key, в секции Настройки мобильного приложения выполните следующие настройки:

1. В поле Отображаемое имя сервера укажите название сервера Indeed Key, которое будет отображаться в мобильном приложении.
2. В настройке Способ подтверждения Push выберите, как у пользователя будет запрашиваться подтверждение входа:
   - Подтверждение не требуется — у пользователя не будет запрашиваться дополнительная аутентификация на устройстве;
   - Подтверждение биометрическими средствами — у пользователя будет запрашиваться дополнительная аутентификация на устройстве с помощью биометрии;
   - Подтверждение любыми средствами, доступными на устройстве — у пользователя будет запрашиваться дополнительная аутентификация на устройстве с помощью любого доступного на устройстве метода;
3. В настройке Отображать одноразовый пароль в мобильном приложении для новых аутентификаторов укажите, будет ли отображаться одноразовый код в карточке аутентификатора в приложении. По умолчанию одноразовый код скрыт.
4. В настройке Способ подтверждения для отображения OTP выберите, как пользователь будет подтверждать право просматривать одноразовые коды:
   - Подтверждение не требуется — у пользователя не будет запрашиваться дополнительная аутентификация на устройстве;
   - Подтверждение биометрическими средствами — у пользователя будет запрашиваться дополнительная аутентификация на устройстве с помощью биометрии;
   - Подтверждение любыми средствами, доступными на устройстве — у пользователя будет запрашиваться дополнительная аутентификация на устройстве с помощью любого доступного на устройстве метода;
5. В поле Время отображения OTP укажите, в течение какого времени будет актуален одноразовый пароль. Значение указывается в секундах.

Настройки одноразового пароля

Чтобы настроить генерацию одноразового пароля, в секции Настройки OTP выполните следующие настройки:

1. В поле Период обновления OTP укажите, на протяжение какого времени будет актуален одноразовый пароль.
2. В настройке Количество периодов сравнения укажите, сколько периодов обновления должно пройти, пока одноразовый пароль не будет считаться недействительным.
3. В настройке Формат имени пользователя укажите, в каком виде передаются данные в мобильное приложение.
4. В настройке Алгоритм генерации OTP-кода выберите, по какому алгоритму будет генерироваться одноразовый пароль.

5. В настройке Количество цифр в OTP-коде выберите, сколько цифр будет содержать одноразовый пароль.

Регистрация аутентификатора Indeed Key по ссылке

Для регистрации аутентификатора Indeed Key по ссылке из письма необходимы следующие условия:

- установленный и настроенный провайдер Email OTP,
- заполненный email пользователя в каталоге пользователей.

Ссылка отправляется на электронный адрес, указанный для пользователя в каталоге.

Чтобы зарегистрировать Indeed Key по ссылке, выполните следующие действия:

1. В разделе Конфигурация→Аутентификаторы, в секции Настройки регистрации выполните следующие настройки:
    1. В настройке Способ регистрации аутентификатора выберите способ регистрации по ссылке из электронного письма.
    2. Далее укажите следующее:
        - В поле Тема уведомления укажите заголовок письма для регистрации.
        - В поле Сообщение укажите тело письма.
        - В поле Текст ссылки на регистрацию аутентификатора укажите текст, который в сообщении будет выводиться как ссылка для регистрации OTP. Если поле оставить пустым, ссылка выводится в сообщении как URL.
        - При необходимости укажите адрес сервера, участвующий в формировании ссылки.
    3. Задайте настройку Регистрация аутентификатора без подтверждения администратора.
        - Если настройка включена:

          После успешной регистрации через email аутентификатор автоматически переводится в статус *Действующий* без дополнительных действий администратора.

        - Если настройка выключена:

          После того как пользователь успешно пройдет регистрацию в приложении, администратор в Management Console должен нажать на значок обновления статуса и далее нажать Сохранить. Статус *Ожидает* поменяется на *Действующий*, а аутентификатор будет готов к использованию.
2. Перейдите в раздел Пользователи, выберите пользователя, затем выберите вкладку Аутентификаторы.
3. Нажмите кнопку Зарегистрировать и выберите из списка Indeed Key. После этого пользователю отправляется письмо со ссылкой на регистрацию аутентификатора.

> **ПРИМЕЧАНИЕ**
>
> Как только письмо отправлено, в Management Console и User Console добавляется аутентификатор Indeed Key в статусе *Ожидает*.

Дальнейшие шаги:

1. Пользователь переходит по ссылке в приложение Indeed Key, где начинается регистрация аутентификатора.
2. После того как пользователь успешно прошел регистрацию в приложении, может потребоваться дополнительное подтверждение администратора, если выключена настройка Регистрация аутентификатора без подтверждения администратора. В таком случае администратор в Management Console должен нажать на значок обновления статуса и далее нажать Сохранить. Статус *Ожидает* поменяется на *Действующий*, а аутентификатор будет готов к использованию.
3. После успешной регистрации администратор должен ее подтвердить: в Management Console нажмите на значок обновления статуса и далее нажмите Сохранить. Статус *Ожидает* поменяется на *Действующий*, а аутентификатор будет готов к использованию.

Если у пользователя возникли ошибки во время регистрации Indeed Key, то после обновления статуса в Management Console статус *Ожидает* поменяется на *Ошибка*. Удалите аутентификатор и снова пройдите процедуру регистрации.

Регистрация аутентификатора Indeed Key по QR-коду

Чтобы зарегистрировать Indeed Key по QR-коду, выполните следующее:

1. В разделе Доступные пользователю действия разрешите пользователю регистрировать новые аутентификаторы.
2. В настройке Способ регистрации аутентификатора выберите способ регистрации аутентификатора по QR-коду.

В User Console у пользователя в списке доступных аутентификаторов появится Indeed Key.

Пользователю нужно выполнить следующие действия:

1. Нажать значок шестеренки.
2. Нажать кнопку Зарегистрировать.
3. Откройте приложение Indeed Key, нажмите значок +.
4. Сканируйте появившийся QR-код.

Конфигурация ссылки на регистрацию и скачивание Indeed Key

Ссылку на регистрацию аутентификатора и скачивание приложения Indeed Key можно задать вручную.

1. Перейдите в раздел Конфигурация→Аутентификаторы в секцию Настройки регистрации.

2. В настройке Адрес сервера, участвующий в формировании ссылки на регистрацию аутентификатора (диплинк) укажите ссылку для регистрации, отправляемую по email.

   Доступны следующие ссылки для регистрации (в скобках указано местонахождение сервера):

   - https://indeedkey.drru.agconnect.link (Россия)
   - https://indeedkey.dre.agconnect.link (Германия)
   - https://indeedkey.drcn.agconnect.link (Китай)
   - https://indeedkey.dra.agconnect.link (Сингапур)

3. В секции Дополнительные настройки укажите ссылку для скачивания Indeed Key.

   Доступны следующие ссылки для скачивания (в скобках указано местонахождение сервера):

   - https://indeedkey.drru.agconnect.link/XwZr (Россия)
   - https://indeedkey.dre.agconnect.link/MJyW (Германия)
   - https://indeedkey.drcn.agconnect.link/NDbK (Китай)
   - https://indeedkey.dra.agconnect.link/i1RD (Сингапур)

Настройка доверенного идентификатора для Indeed Key Server

По умолчанию при удалении аутентификатора в User Console, в утилите управления аутентификаторами или в консоли администратора аутентификатор будет удален из системы без уведомлений и продолжит отображаться в приложении.

Для настройки push-уведомления с информацией об удалении аутентификатора и удалением в приложении необходимо выполнить дополнительные настройки:

1. Откройте конфигурационный файл Indeed Key Server *am/indeed-key/app-settings.json*.
2. В параметре `TrustedClients` укажите доверенный ID Indeed Key Server.

   Пример

   ```
   "TrustedClients": [
   "!!! TRUSTED_CLIENT_ID !!!"
   ]
   ```

3. После применения параметров пользователь будет получать уведомления об удалении ключа.

Настройка приложения Indeed Key на смартфоне

Приложение Indeed Key доступно для смартфонов с iOS 13.0 и выше, Android 7.0 и выше.

Корректная работа приложения Indeed Key гарантируется, только если оно скачано из официальных магазинов приложений. Чтобы скачать или обновить приложение, выберите магазин приложений:

- App Store
- Google Play
- Huawei AppGallery
- RuStore

> ⚠ **ВАЖНО!**
>
> Чтобы обновить приложение, скачивайте обновление в том же магазине, где вы устанавливали предыдущую версию.

Примечание для владельцев Android-устройств

Для корректной работы push-уведомлений на Android-устройствах убедитесь, что выполнены следующие обязательные требования:

- Вы разрешили приложению отправку уведомлений;
- На устройствах с Android 9 и выше отключите режим энергосбережения.

Примечание: корректная работа push-уведомлений возможна не на всех модификациях Android.

1. Откройте приложение. В панели Аутентификаторы нажмите значок + для добавления аутентификатора.
2. Разрешите приложению доступ к камере и отсканируйте QR-код.
3. Подтвердите регистрацию аутентификатора, нажав кнопку Подтвердить.
4. После успешной регистрации аутентификатор будет отображаться на главном окне программы.

Для удаления выберите необходимый аутентификатор и нажмите Удалить аутентификатор.

Indeed AM Telegram Provider

Indeed AM Telegram Provider предназначен для аутентификации пользователей с помощью следующих технологий:

- одноразовые пароли;
- push-уведомления с запросом подтвердить или отклонить вход.

Одноразовые пароли и push-уведомления пользователи получают через бота в мессенджере Telegram.

Telegram Provider может быть использован для аутентификации в следующих модулях:

- Identity Provider,
- ADFS Extension,
- FreeRADIUS Extension,
- LDAP Proxy.

> **ПРИМЕЧАНИЕ**
>
> Для работы компонента требуется доступ к серверам Telegram для сервисной службы и для провайдера.

Идентификатор провайдера
`{CA4645CC-5896-485E-A6CA-011FCC20DF1D}`

Порядок установки

Чтобы настроить Telegram Provider:

1. Установите сервисную службу и провайдер.
2. Настройте атрибут с номером телефона.
3. Создайте бот в приложении Telegram.
4. Настройте сервисную службу.
5. Задайте настройки в Management Console.
6. Зарегистрируйте аутентификатор.

Установка сервисной службы и провайдера Telegram

> ⚠ **ВАЖНО**
>
> Если в инфраструктуре используется несколько серверов Core Server, то установку провайдера необходимо выполнить на всех серверах инфраструктуры.

На сервере с Linux

Чтобы установить Telegram на сервере с операционной системой Linux:

1. Откройте файл *am/.env*.
2. Для установки сервисной службы Telegram Service:
    1. В переменной `COMPOSE_PROFILES` добавьте значение `telegram-service`, если оно отсутствует.
    2. В переменной `COMPOSE_FILES` добавьте значение `telegram-service.docker-compose.yml`, если оно отсутствует.

    > ⚠ **ВАЖНО**
    >
    > Для корректной работы провайдера Telegram убедитесь, что установлен только один экземпляр Telegram Service, даже если в инфраструктуре используется несколько серверов Core Server.
3. Для установки провайдера Telegram в переменной `COMPOSE_PROFILES` добавьте значения `telegram-otp`, если оно отсутствует.
4. Сохраните файл.

На клиентских машинах с Windows

Чтобы установить провайдер на клиентских машинах с операционной системой Windows:

1. Запустите файл для установки, расположенный по пути *Indeed AM <Номер версии>\Indeed AM Providers\Indeed AM Telegram OTP Provider\<Номер версии>*.

> ⚠ **ВАЖНО**
>
> Если в инфраструктуре используется несколько Core Server, установите провайдер на всех серверах инфраструктуры.

2. Если программа установки предлагает выполнить перезагрузку, подтвердите данное действие. После завершения установки может потребоваться перезагрузка системы.

Удаление/Восстановление продукта осуществляется стандартным для поддерживаемых ОС способом, через меню Панель управления.

Файлы шаблонов политик расположены в папке *Indeed AM <номер версии>\Misc\ADMX Templates*.

Настроить атрибут с номером телефона

Чтобы использовать провайдер, задайте номер телефона в атрибуте пользователя службы каталогов. По умолчанию это атрибут `telephoneNumber`. Также можно настроить любой другой атрибут. Если номер не задан, использовать провайдер будет невозможно.

Создать бот

1. Откройте приложение Telegram, найдите специального бота @botfather и откройте диалог с ботом.
2. Нажмите Start и отправьте команду `/newbot`.
3. Укажите имя создаваемого бота. Данное название будет отображаться в окне диалога с ботом. Введите любое имя, например *IndeedOTP*.
4. Укажите имя пользователя для аккаунта с ботом с *bot* в конце, например *IndeedOTP_bot*. Данное имя пользователя используется для ссылок на бота.
5. При успешной регистрации отобразится токен для доступа к API. Данный токен потребуется для настройки службы AM Telegram Service и бота в Management Console.

Настроить сервисную службу

Для настройки службы нужен сервисный пользователь с правами глобального администратора Indeed AM. От имени этого пользователя будут регистрироваться аутентификаторы. В целях безопасности рекомендуется создать в каталоге пользователей отдельного пользователя для регистрации Telegram Provider.

Чтобы настроить службу Telegram Service:

1. Откройте для редактирования файл *am/telegram-service/app-settings.json*.

> **ПРИМЕЧАНИЕ**
>
> Для редактирования файла *am/telegram-service/app-settings.json* рекомендуется использовать текстовые редакторы Nano или Visual Studio Code.

2. Задайте значения для следующих параметров:

- `Token` — токен, полученный при создании бота в Telegram.
- `Username` — имя сервисного пользователя с правами глобального администратора Indeed AM, от имени которого будет осуществляться регистрация аутентификаторов.
- `Password` — пароль сервисного пользователя.
- `TrustedId` — произвольный уникальный идентификатор. Значение идентификатора должно совпадать с тем, что указано в настройке Доверенный ID Telegram Service в Management Console.
- (Опционально) `UseProxy`, `ProxyAddress` — заполните при использовании прокси сервера.

Пример app-settings.json

```
{
  "Logging": {
    "LogLevel": {
      "Default": "Information",
      "Microsoft.Hosting.Lifetime": "Information"
    }
  },
  "Localization": {
    "DefaultCulture": "ru-RU"
  },
  "Bot": {
    "Token": "8042256635:AAF-AIINR5CzlfP2PFZr3cr5__jA7zubHIw",
    "UseProxy": false,
    "ProxyAddress": ""
  },
  "AuthenticationServer": {
    "Username": "telegrambot@test.local",
    "Password": "Q1w2e3r4",
    "Lognames": "Name",
    "TrustedId": "11111"
  },
  "Audit": {
    "LogServer": {
      "Buffer": {
        "Location": "./EventCache",
        "FlushInterval": "00:10:00"
      }
    }
  }
}
```

3. Сохраните изменения и запустите контейнер с приложением с помощью команды `sudo docker-compose up -d`. Для применения изменений без перезапуска контейнера можно выполнить дополнительную настройку.

> **ПРИМЕЧАНИЕ**
>
> Если вы используете несколько Core Server, одновременно можно запустить службу только на одном из серверов.

Чтобы применить изменения am/telegram-service/app-settings.json без перезапуска контейнера:

1. Откройте для редактирования файл *am/telegram-service.docker-compose.yml*.

   > **ПРИМЕЧАНИЕ**
   >
   > Для редактирования файла рекомендуется использовать текстовые редакторы Nano или Visual Studio Code.

2. В разделе `environment` добавьте параметр `DOTNET_USE_POLLING_FILE_WATCHER` со значением `1` или `true`.

   Пример

   ```
    environment:
      AMTELEGRAM_AuthenticationServer__Url:
   "https://${ENDPOINT_NAME_CORE}/am/core"
      AMTELEGRAM_Audit__LogServer__Url: "https://${ENDPOINT_NAME_LS}/ls/api"
      DOTNET_USE_POLLING_FILE_WATCHER: "true"
   ```

Включить/Отключить шифрование конфигурационного файла

1. В терминале перейдите в каталог с утилитой для шифрования *am/protection*.

   ```
   cd /am/protection
   ```

2. Выдайте права для запуска скрипта `protector.sh`.

   ```
   sudo chmod 500 protector.sh
   ```

3. Чтобы зашифровать конфигурационный файл, запустите скрипт `protector.sh` с параметром `protect`.

   ```
   sudo bash ./protector.sh protect
   ```

4. Чтобы расшифровать конфигурационный файл, запустите скрипт `protector.sh` с параметром `unprotect`.

   ```
   sudo bash ./protector.sh unprotect
   ```

Задать настройки в Management Console

Для корректной работы провайдера задайте остальные настройки в Management Console. Для этого:

1. На боковой панели Management Console откройте раздел Конфигурация.
2. Перейдите на вкладку Аутентификаторы.
3. Выберите аутентификатор Telegram.
4. При необходимости задайте общие настройки.
5. В секции Настройки Telegram Service укажите произвольный уникальный идентификатор. Значение идентификатора должно совпадать с тем, что указано в конфигурационном файле службы *am/telegram-service/app-settings.json*.
6. В секции Режим работы выберите режим работы провайдера — *Push* или *OTP*.
7. В секции Настройки бота:
   - В поле Идентификатор бота укажите токен, полученный при создании бота в Telegram.
   - В поле Шаблон для сообщения настройте вид сообщения. Сообщение может содержать одноразовый код для входа в приложение, название приложения, имя пользователя, дату и время входа, IP-адрес компьютера, с которого выполняется вход.
8. Если вы планируете использовать Telegram Provider в режиме отправки одноразовых паролей, в секции Настройки генерации одноразового пароля:
   - В поле Длина одноразового пароля укажите, сколько символов будет содержать одноразовый пароль.
   - В настройке Цифры укажите, будет ли одноразовый пароль содержать цифры.
   - В настройке Строчные латинские буквы укажите, будет ли одноразовый пароль содержать строчные латинские буквы;
   - В настройке Прописные латинские буквы укажите, будет ли одноразовый пароль содержать прописные латинские буквы;
   - В настройке Специальные символы укажите, будет ли одноразовый пароль содержать специальные символы.
9. При необходимости выполните следующие настройки:

Настройте работу Telegram Provider через прокси

В секции Настройки бота:

- В настройке Использовать прокси выберите *Да*. По умолчанию выбрано *Нет*.
- В поле Адрес прокси укажите адрес прокси-сервера.

Настройте защиту от спама

Механизм защиты от спама основан на расчете процента успешных аутентификаций относительно всех отправленных сообщений за указанный интервал времени. При этом расчет запускается, только если количество отправленных сообщений превышает количество, заданное вами в настройке Окно оценки.

При обнаружении спам-атаки дальнейшая отправка сообщений блокируется на заданный период времени, а при попытке входа возникает ошибка *Potential spam attack detected*.

Отправка сообщений возобновляется либо по истечении заданного периода, либо по достижении определенного количества (в процентном отношении) успешных аутентификаций.

Чтобы настроить защиту от спама, выполните следующее:

1. В Management Console в разделе Конфигурация→Аутентификаторы выберите аутентификатор.
2. В секции Настройки защиты от спама выполните следующие настройки:
   - включите или отключите защиту от спама;
   - в поле Окно оценки попыток аутентификации укажите, в течение какого времени будет выполняться расчет процента успешных попыток входа;
   - в поле Пороговое окно попыток аутентификации укажите, сколько попыток входа должно производиться за время, указанное в окне оценки попыток аутентификации;
   - в поле Процент успешных попыток аутентификации укажите минимальный процент успешных входов относительно всех отправленных сообщений.

Пример

Настройка включена со следующими значениями:

- Окно оценки попыток аутентификации — 600
- Пороговое окно попыток аутентификации — 20
- Процент успешных попыток аутентификации — 85

Защита от спама включится, если произойдет 21 попытка входа (отправлено 21 сообщение). Произойдет блокировка аутентификатора на 600 секунд.

Аутентификатор разблокируется в одном из случаев:

- процент успешных входов (пользователь успешно ввел одноразовый пароль из сообщения) достигнет значения 85;
- прошло 600 секунд с момента блокировки.

> **ИНФОРМАЦИЯ**
>
> События лог-сервера:
>
> - 2090: Обнаружена потенциальная спам-атака. Отправка сообщений приостановлена.
> - 1118: Отправка сообщений пользователям возобновлена.

Зарегистрировать аутентификатор

> **ПРИМЕЧАНИЕ**
>
> При регистрации провайдера пользователь получит запрос номера телефона из аккаунта Telegram. Необходимо, чтобы номер телефона пользователя в каталоге пользователей полностью совпадал и был одного формата. Поддерживаемые форматы: +7xxxxxxxxxx или 8xxxxxxxxxx.

1. Откройте чат с созданным ботом. Для этого введите в поисковой строке мессенджера имя вашего бота либо перейдите по ссылке из сообщения BotFather.
2. Нажмите Start.
3. Введите команду `/register`.
4. Введите номер телефона аккаунта Telegram.
5. При успешной регистрации аутентификатора отобразится сообщение *Вы были успешно зарегистрированы*.

Indeed AM MFA Provider

Провайдер Indeed AM Multi-factor authentication Provider (MFA) позволяет задать последовательность провайдеров в цепочке многофакторной аутентификации.

MFA Provider может быть использован для аутентификации в следующих модулях:

- Windows Logon,
- FreeRadius Extension,
- Linux Logon.

Идентификатор провайдера
`{070719BA-EB57-4EA8-BB4D-D15A33E7363D}`

Установка провайдера MFA

> ⚠ **ВАЖНО**
>
> Если в инфраструктуре используется несколько серверов Indeed AM, то установку провайдера необходимо выполнить на всех серверах инфраструктуры.

На клиентских машинах с Windows

Чтобы установить провайдер на клиентских машинах с операционной системой Windows, выполните следующие действия:

1. Из папки *Indeed AM <Номер версии>\Indeed AM Providers\Indeed AM MFA Provider\Client\<Номер версии>* запустите пакет *IndeedID.MFA.Provider.msi*.
2. Если программа установки предлагает выполнить перезагрузку, подтвердите данное действие. После завершения установки может потребоваться перезагрузка системы.

Удаление/Восстановление продукта осуществляется стандартным для поддерживаемых ОС способом, через меню Панель управления.

Файлы шаблонов политик расположены в папке *Indeed AM <номер версии>\Misc\ADMX Templates*.

На сервере с Linux

Чтобы установить провайдер на сервере с операционной системой Linux, выполните следующие действия:

1. Откройте файл *am/.env*.

2. В переменной `COMPOSE_PROFILES` добавьте значение `mfa`.

Настройка провайдера

1. Убедитесь, что в access-manager.docker-compose.yml в параметре `volumes` не закомментирована строка с `auth-mfa`.

2. В конфигурационном файле *am/core/app-settings.json* в блоке `PlatformCompatibility` для параметра `Registry` в теге `"File":` укажите название файла, в котором будут прописываться настройки провайдера MFA. Значение по умолчанию `server-registry.json`. Остальные параметры не изменяйте.

3. Откройте файл *am/core/server-registry.json* и добавьте строки со следующими параметрами:

   - `KeyName` — имя ключа в реестре, не изменять;
   - `ValueName` — имя значения, можно изменять;
   - `StringValue` — указание цепочки многофакторной аутентификации;
   - `StringArrayValue` — указание идентификаторов провайдеров в цепочке.

   Пример

   ```
   {
        “KeyName”: “HKEY_LOCAL_MACHINE\\SOFTWARE\\Policies\\Indeed-Id\\BSPs\\MFA”,
        “ValueName”: “MFADeviceName”,
        “StringValue”: “WP + STOTP”
    },
    {
        “KeyName”: “HKEY_LOCAL_MACHINE\\SOFTWARE\\Policies\\Indeed-Id\\BSPs\\MFA”,
        “ValueName”: “BSPChain”,
        “StringArrayValue”: [
            “{CF189AF5-01C5-469D-A859-A8F2F41ED153}”,
            “{0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0}”
        ]
    }
   ```

4. Сохраните изменения в файле и перезапустите контейнер с приложением.

5. Перейдите к настройке цепочки многофакторной аутентификации.

> ⚠ **ВАЖНО**
>
> Провайдеры цепочки многофакторной аутентификации, указанные в *am/core/app-settings.json*, должны совпадать с провайдерами в групповой политике.

Список поддерживаемых провайдеров для Windows Logon

```
SMS OTP {EBB6F3FA-A400-45F4-853A-D517D89AC2A3}
Passcode {F696F05D-5466-42b4-BF52-21BEE1CB9529}
Software OTP {0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0}
Windows Password {CF189AF5-01C5-469D-A859-A8F2F41ED153}
Indeed Key {DEEF0CB8-AD2F-4B89-964A-B6C7ECA80C68}
Hardware OTP {AD3FBA95-AE99-4773-93A3-6530A29C7556}
Secured TOTP {F15FD7EC-19EA-4384-846E-A2D0BE149FA2}
```

Список поддерживаемых провайдеров для FreeRadius Extension

```
Hardware OTP {AD3FBA95-AE99-4773-93A3-6530A29C7556}
Hardware TOTP {CEB3FEAF-86ED-4A5A-BD3F-6A7B6E60CA05}
Secured TOTP {F15FD7EC-19EA-4384-846E-A2D0BE149FA2}
Software TOTP {0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0}
Windows Password {CF189AF5-01C5-469D-A859-A8F2F41ED153}
Passcode {F696F05D-5466-42b4-BF52-21BEE1CB9529}
```

Список поддерживаемых провайдеров для Linux Logon

```
Secured TOTP {F15FD7EC-19EA-4384-846E-A2D0BE149FA2}
Software TOTP {0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0}
Windows Password {CF189AF5-01C5-469D-A859-A8F2F41ED153}
Passcode {F696F05D-5466-42b4-BF52-21BEE1CB9529}
```

Пример аутентификации

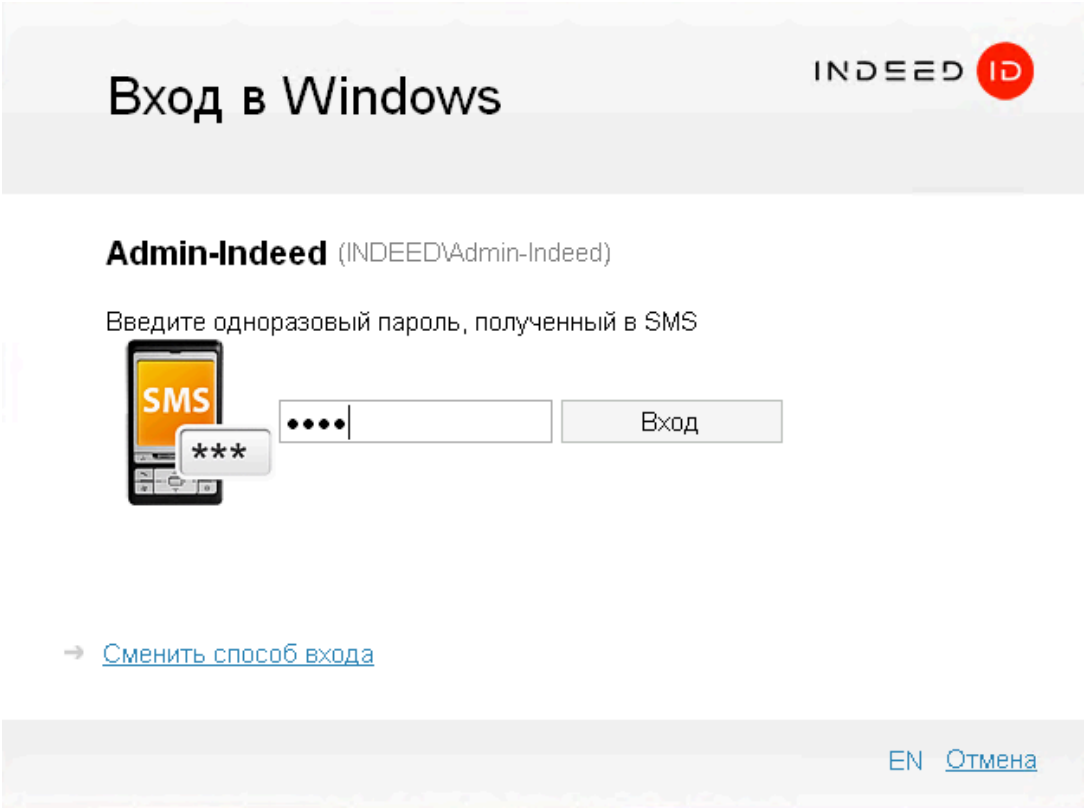
В примере используется компонент Indeed AM Windows Logon и цепочка провайдеров Indeed AM Passcode + Indeed AM SMS OTP.

Чтобы выполнить вход с помощью MFA Provider, выполните следующее:

1. Выберите провайдер аутентификации Многофакторная аутентификация.

2. Введите данные для первого провайдера в цепочке.

3. Введите данные для второго провайдера в цепочке и выполните вход.



Настройка провайдера Multi-factor authentication в Management Console

Для настройки MFA в Management Console перейдите в раздел Конфигурация→Аутентификаторы и выберите аутентификатор Multi-factor authentication.

Права доступа

Чтобы выдать или отозвать права на использование аутентификатора, выполните следующее:

1. Перейдите в секцию Основные настройки.
2. В настройке Запретить использовать укажите, может ли пользователь использовать или регистрировать выбранный аутентификатор.

Блокировка аутентификатора

Чтобы заблокировать аутентификатор, в секции Настройки блокировки аутентификатора выполните следующие настройки:

1. Разрешите или заблокируйте использование MFA в случае серии неудачных попыток аутентификации.
2. В поле Количество попыток аутентификации до блокировки укажите, сколько раз пользователь может совершить неудачную аутентификацию до блокировки способа аутентификации.
3. В поле Сброс счетчика блокировки укажите, сколько минут должно пройти после неудачной попытки аутентификации, прежде чем сбросится счетчик.
4. В поле Таймаут до разблокировки способа входа укажите, через сколько минут заблокированный способ аутентификации станет вновь доступным.

Административные шаблоны групповых политик (ADMX)

Некоторые настройки Indeed AM задаются групповыми политиками Microsoft.

> **ПРИМЕЧАНИЕ**
>
> Перед настройкой групповых политик добавьте шаблоны политик Indeed AM в список административных шаблонов. Файлы шаблонов политик входят в состав дистрибутива Indeed AM и расположены в каталоге *Misc\ADMX Templates*.

Действие политики представляет из себя добавление определенных ключей в реестр, при необходимости значения политик можно добавить в реестр вручную. При добавлении вручную создайте недостающие разделы реестра.

Добавление административных шаблонов

1. Скопируйте файлы шаблонов групповых политик из каталога дистрибутива *C:\Indeed\Indeed AM <номер версии>\Misc\ADMX Templates* в один из следующих каталогов:

   - *C:\Windows\PolicyDefinitions* — локальное хранилище ADMX-файлов.
   - *C:\Windows\SYSVOL\sysvol\indeed.local\Policies\PolicyDefinitions* — хранилище ADMX-файлов на контроллере домена.

   Если каталог *PolicyDefinitions* отсутствует, создайте его.

2. Скопируйте файл *IndeedID.BaseFile.admx* и все необходимые ADMX-файлы в каталог *\PolicyDefinitions*.

3. Скопируйте файл *IndeedID.BaseFile.adml* и все ADML-файлы, аналогичные скопированным ADMX-файлам, из каталога *\Indeed AM <номер версии>\Misc\GroupPolicyTemplates\<en-US или ru-RU>* в каталог *\PolicyDefinitions\en-US* (для англоязычной локализации сервера) или *\PolicyDefinitions\ru-RU* (для русскоязычной локализации сервера).

4. Скопируйте шаблоны из папки *ADMX Templates\BSPs* в корневую папку *PolicyDefinitions* рядом с остальными ADMX-файлами.

5. Добавьте шаблоны политик и провайдеров аутентификации в раздел Конфигурация компьютера (Computer Configuration). Добавьте шаблоны политик Indeed AM Paste в раздел Конфигурация пользователя (User Configuration).

После загрузки групповые политики Indeed ID станут доступны в Редакторе локальных групповых политик (Group Policy Management Editor в разделе ADMX files).

Настройка с помощью Редактора локальной групповой политики

При настройке политик можно использовать консоль редактора групповой политики gpedit.msc для управления параметрами в реестре.

Настройка с помощью Редактор реестра

При настройке политик вручную откройте Редактор реестра:

1. В поле поиска на панели задач введите regedit, затем выберите Редактор реестра.
2. Перейдите в необходимый раздел в зависимости от провайдера, который вы настраиваете, или создайте этот раздел. Например, *Компьютер\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID*.

> ⚠ **ВАЖНО**
>
> Будьте осторожны при использовании Редактора реестра. Если вы неправильно отредактируете реестр, могут возникнуть серьезные проблемы, требующие полной переустановки операционной системы или приводящие к потере данных.

Провайдеры аутентификации

Indeed Key

Политики распространяются на машины с установленным компонентом Indeed

Hardware TOTP

Настройка времени вручную

MFA

Настройка цепочки многофакторной аутентификации

Indeed Key

> **ПРИМЕЧАНИЕ**
>
> Политики распространяются на машины с установленным компонентом Indeed AM Windows Logon.

Таймаут операции для приложения Indeed Key

Политика определяет время ожидания операции для приложения Indeed Key.

Требовать команды от пользователя

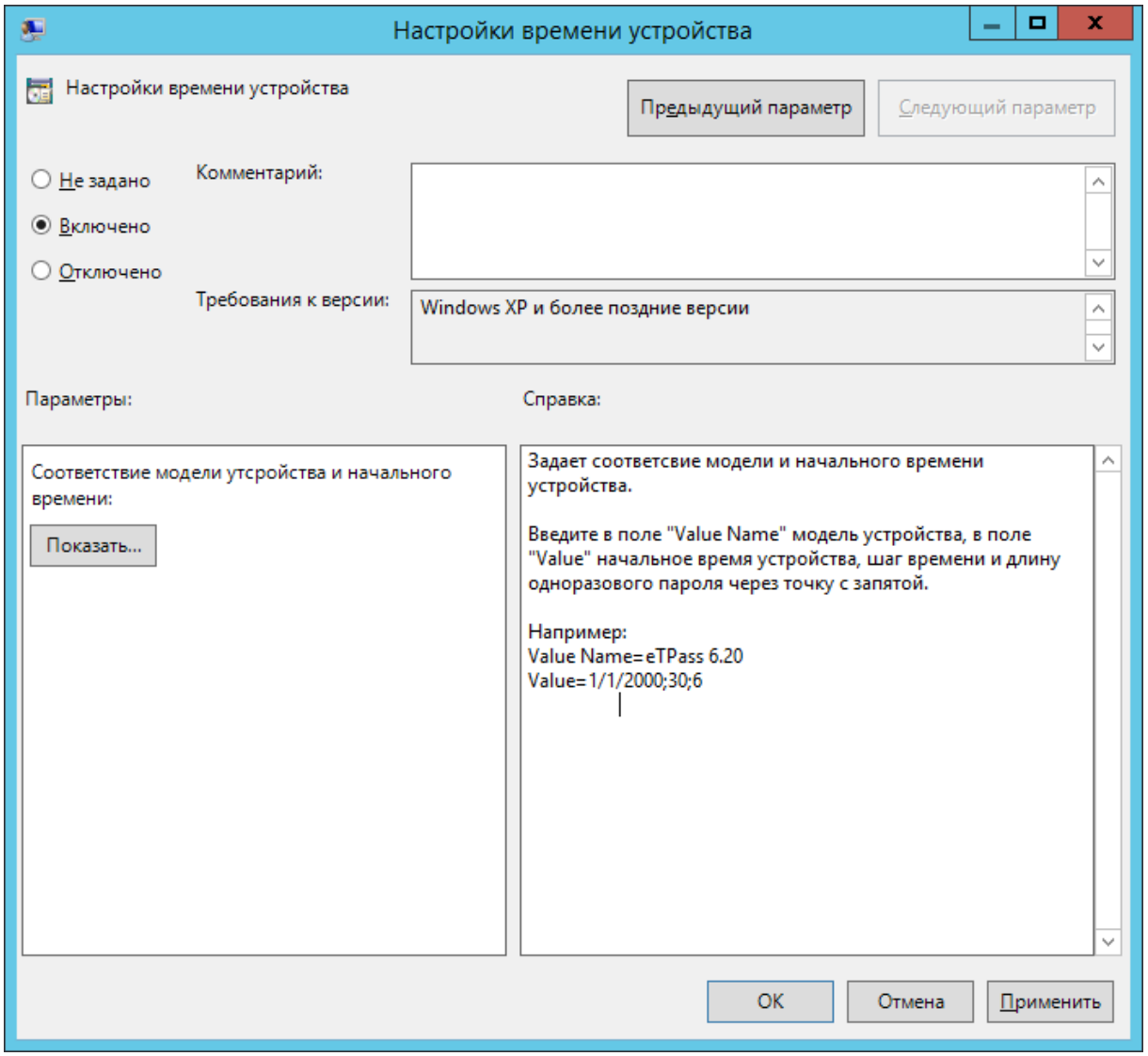
Политика указывает ждать команды от пользователя для активации процедуры входа.

Hardware TOTP

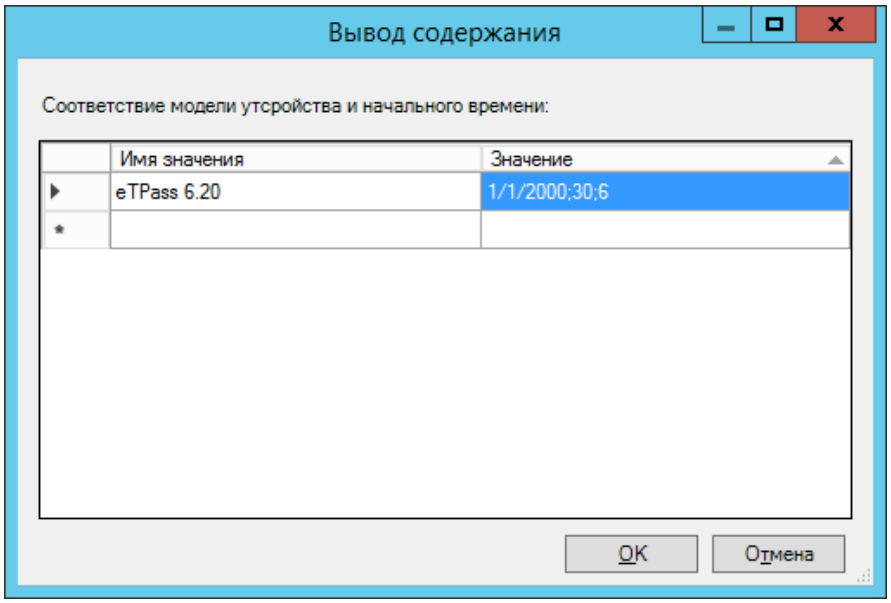
Настройка времени вручную

Задает соответствие модели и начального времени устройства.

> **ИНФОРМАЦИЯ**
>
> Для модели «eTPass 6.20» по умолчанию (если политика не задана) считаем шаг времени: 30 сек, начальное время: 1/1/2000.
>
> По умолчанию для всех остальных устройств — шаг времени: 30, начальное время: 1/1/1970.



> **ИНФОРМАЦИЯ**
>
> В поле Имя значения указывается имя устройства, в поле Значение указываются параметры: *Начальное время*, *Шаг*, *Длина пина*.


Вывод содержания
Соответствие модели утсройства и начального времени:
Имя значения
Значение
eTPass 6.20
1/1/2000;30;6
OK
Отмена

MFA

Настройка цепочки многофакторной аутентификации

> ⚠ **ВАЖНО**
>
> Политика должна распространяться на все клиентские машины.

Через GPO

1. Откройте политику Настройки цепочки многофакторной аутентификации. Политика расположена по следующему пути: *Административные шаблоны→Indeed-ID→Id Providers→MFA*.
2. Установите значение политики *Включено*.
3. В параметре *Цепочка многофакторной аутентификации* укажите идентификаторы провайдеров аутентификации, которые будут использоваться в цепочке. Каждый идентификатор указывайте в фигурных скобках и с новой строки без пробелов и других символов.

   > ⓘ **ПРИМЕЧАНИЕ**
   >
   > Запрещенный для использования провайдер может быть использован в цепочке провайдера MFA.

   Список поддерживаемых провайдеров для Windows Logon

   ```
   SMS OTP {EBB6F3FA-A400-45F4-853A-D517D89AC2A3}
   Passcode {F696F05D-5466-42b4-BF52-21BEE1CB9529}
   Software OTP {0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0}
   Windows Password {CF189AF5-01C5-469D-A859-A8F2F41ED153}
   Indeed Key {DEEF0CB8-AD2F-4B89-964A-B6C7ECA80C68}
   Hardware OTP {AD3FBA95-AE99-4773-93A3-6530A29C7556}
   Hardware TOTP {CEB3FEAF-86ED-4A5A-BD3F-6A7B6E60CA05}
   Secured TOTP {F15FD7EC-19EA-4384-846E-A2D0BE149FA2}
   ```

   Список поддерживаемых провайдеров для FreeRadius Extension

```
Hardware OTP {AD3FBA95-AE99-4773-93A3-6530A29C7556}
Hardware TOTP {CEB3FEAF-86ED-4A5A-BD3F-6A7B6E60CA05}
Secured TOTP {F15FD7EC-19EA-4384-846E-A2D0BE149FA2}
Software TOTP {0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0}
Windows Password {CF189AF5-01C5-469D-A859-A8F2F41ED153}
Passcode {F696F05D-5466-42b4-BF52-21BEE1CB9529}
```

Пример цепочки Indeed AM Passcode + Indeed AM SMS OTP

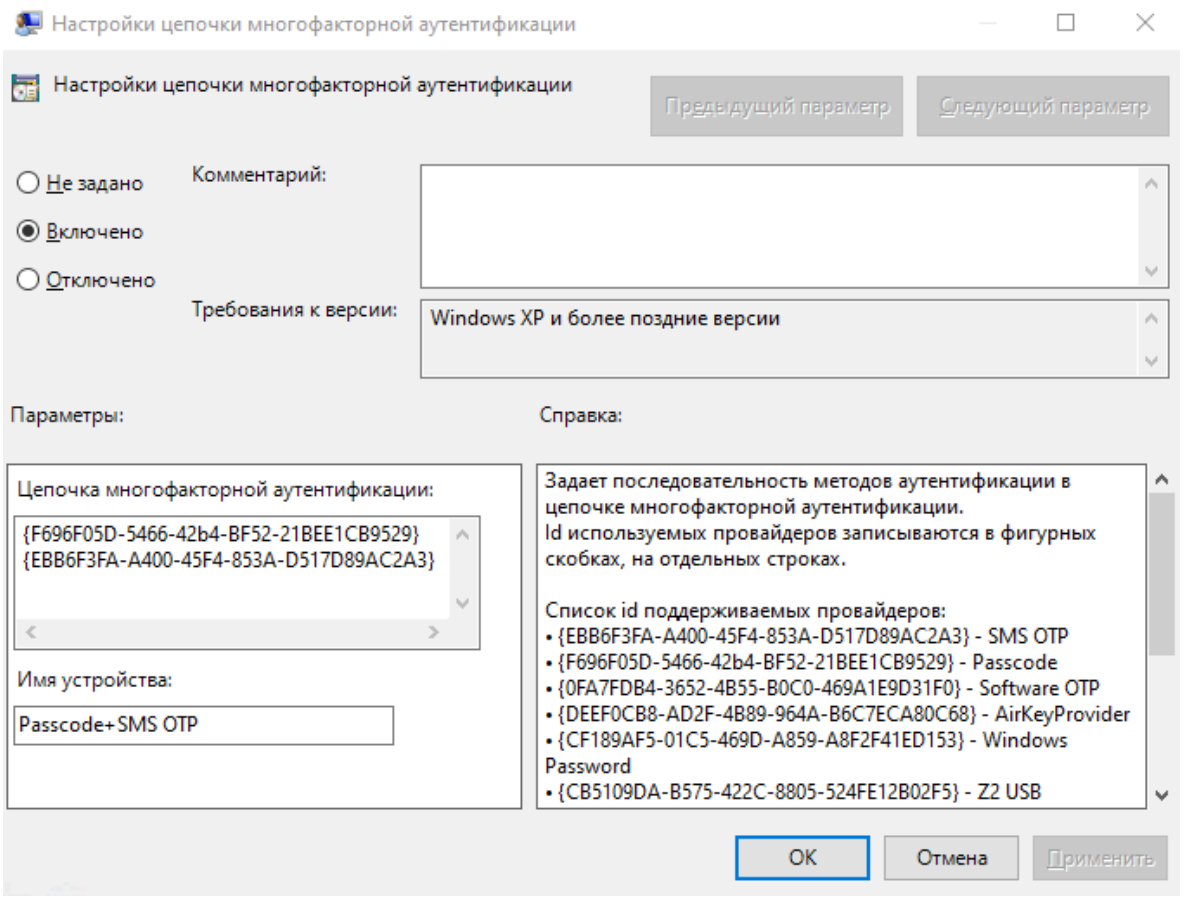
{F696F05D-5466-42b4-BF52-21BEE1CB9529}

{EBB6F3FA-A400-45F4-853A-D517D89AC2A3}

4. В параметре *Имя устройства* указывается имя для созданной цепочки. Значение по умолчанию — *MFA*.

ИНФОРМАЦИЯ

Данное значение будет отображаться в названии устройства MFA для пользователя и в событиях системы.



В реестре

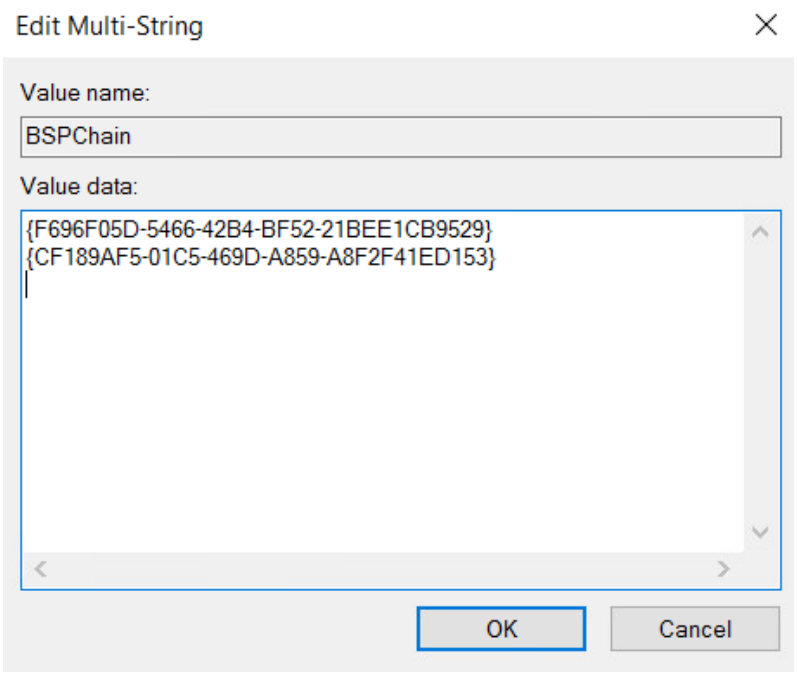
1. Откройте редактор реестра.
2. Откройте раздел `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\BSPs\MFA`.
3. Создайте параметр `BSPChain` типа `REG_MULTI_SZ` и укажите идентификаторы провайдеров аутентификации, которые будут использоваться в цепочке. Каждый идентификатор указывайте в фигурных скобках и с новой строки без пробелов и других символов.

   Список поддерживаемых провайдеров для Windows Logon

   ```
   SMS OTP {EBB6F3FA-A400-45F4-853A-D517D89AC2A3}
   Passcode {F696F05D-5466-42b4-BF52-21BEE1CB9529}
   Software OTP {0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0}
   Windows Password {CF189AF5-01C5-469D-A859-A8F2F41ED153}
   Indeed Key {DEEF0CB8-AD2F-4B89-964A-B6C7ECA80C68}
   Hardware OTP {AD3FBA95-AE99-4773-93A3-6530A29C7556}
   Secured TOTP {F15FD7EC-19EA-4384-846E-A2D0BE149FA2}
   ```

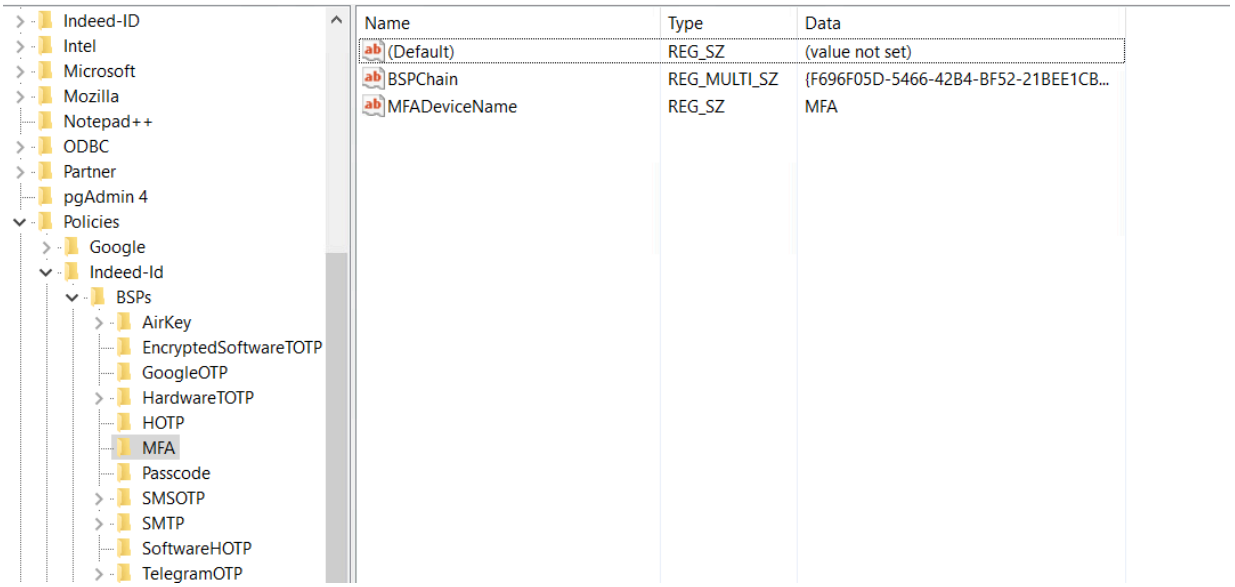
   Список поддерживаемых провайдеров для FreeRadius Extension

   ```
   Hardware OTP {AD3FBA95-AE99-4773-93A3-6530A29C7556}
   Hardware TOTP {CEB3FEAF-86ED-4A5A-BD3F-6A7B6E60CA05}
   Secured TOTP {F15FD7EC-19EA-4384-846E-A2D0BE149FA2}
   Software TOTP {0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0}
   Windows Password {CF189AF5-01C5-469D-A859-A8F2F41ED153}
   Passcode {F696F05D-5466-42b4-BF52-21BEE1CB9529}
   ```



4. Создайте параметр `MFADeviceName` типа `REG_SZ` и укажите имя для созданной цепочки.

> **ИНФОРМАЦИЯ**
>
> Данное значение будет отображаться в названии устройства MFA для пользователя и в событиях системы.



RDP Windows Logon

Настройка одновременной работы с модулем Indeed Windows Logon

При условии, что используется сценарий с установкой на одной машине RDP Windows Logon и Windows Logon, необходимо настроить политику для Windows Logon.

Через GPO

1. Перейдите на машину, на которой установлены модули RDP Windows Logon и Windows Logon.
2. Откройте редактор GPO.
3. Перейдите к Конфигурация компьютера→Административные шаблоны→ Indeed ID→Windows Logon.
4. Включите политику Настройки Credential Provider и установите параметр Отображение способов входа на *Все, кроме пароля*.

В реестре

1. Перейдите на машину, на которой установлены компоненты RDP Windows Logon и Windows Logon.
2. Откройте редактор реестра.
3. Перейдите к Компьютер\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Logon for Windows.
4. Создайте параметр `DWORD` с именем `CredProvFilter` и установите значение *2*.

Windows Logon

Настройка Windows Logon

Через GPO

> ⚠ **ВАЖНО!**
>
> При настройке через политики значения будут указаны по пути реестра: *HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\SrvLocator2* и будут приоритетнее ручной настройки.

1. Добавьте политику *IndeedID.ServerUrl.admx* на рабочее место с установленным Indeed AM Windows Logon.
2. Через *gpedit.msc* пройдите по пути Конфигурация компьютера→ Административные шаблоны→Indeed ID→ClientConnection→Настройки подключения к серверу.

   Включите политику.
3. В поле URL-адрес AM сервера укажите URL вашего Indeed Core Server, например `http(s)://dc.indeed-id.local/am/core`.

В реестре

1. Откройте редактор реестра Windows.
2. Перейдите в раздел *HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\SrvLocator2*.
3. Измените строковый параметр `ServerUrlBase` и укажите URL вашего Indeed Core Server, например `http(s)://dc.indeed-id.local/am/core`.

   > ⓘ **ПРИМЕЧАНИЕ**
   >
   > При использовании соединения по протоколу HTTPS требуется выполнить установку клиентского сертификата на каждый сервер Indeed AM.

Настройка одновременной работы с Indeed RDP Windows Logon

Если используется сценарий с установкой Windows Logon и RDP Windows Logon на одной машине, необходимо настроить политику для Windows Logon.

Через GPO

1. Перейдите на машину, на которой установлены модули RDP Windows Logon и Windows Logon.
2. Откройте редактор GPO.
3. Перейдите Конфигурация компьютера→Административные шаблоны→Indeed ID→Windows Logon.
4. Включите политику *Настройки Credential Provider* и установите параметр Отображение способов входа на Все, кроме пароля.

Через реестр

1. Перейдите на машину, на которой установлены модули RDP Windows Logon и Windows Logon.
2. Откройте редактор реестра.
3. Перейдите Компьютер\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Logon for Windows.
4. Создайте параметр типа *DWORD* с именем `CredProvFilter` и установите ему значение *2*.

Резервное копирование

Рекомендуется подготовить резервные копии базы данных, конфигурационных файлов и настройки реестра после того, как вы развернули Indeed Access Manager и проверили его работоспособность.

Периодичность создания резервных копий зависит от того, как вы эксплуатируете Access Manager. Например, резервные копии конфигурационных файлов рекомендуется создавать, если проводились изменения параметров в файлах конфигурации, а далее каждый месяц.

Резервные копии базы данных Access Manager рекомендуется создавать после периода внедрения и отладки. В период, когда пользователи регистрируют аутентификаторы, рекомендуется создавать резервные копии базы данных ежедневно, так как база данных меняется, когда вносятся изменения политик, настройки аутентификаторов, и при регистрации или изменении аутентификаторов пользователями.

Рекомендуется создавать резерные копии следующих компонентов:

Базы данных

- база данных Core Server;
- база данных Key Server (при наличии);
- база событий Log Server (при наличии).

Конфигурационные файлы компонентов

- конфигурационные файлы Log Server:
  - *am/ls/clientApps.config*;
  - *am/ls/targets/DbTargetMssqlAM.config*, *am/ls/targets/DbTargetMssqlIndeedKey.config*, если логи хранятся в Microsoft SQL;
  - *am/ls/targets/DbTargetSqlAM.config*, *am/ls/targets/DbTargetSqlIndeedKey.config*, если логи хранятся в PostgreSQL;
  - *am/ls/targets/TargetSyslog.config*, если логи хранятся в Syslog.

> **ПРИМЕЧАНИЕ**
>
> Перед созданием резервной копии расшифруйте файл конфигурации с помощью утилиты *protector.sh* (расположена в каталоге дистрибутива *am/protection/protector.sh*). Подробную информацию про отключение шифрования вы найдете в разделе Включить/Отключить шифрование конфигурационного файла. Если использовались резервные базы для логов, сохраните все настроенные файлы.

- конфигурационный файл консоли администратора *am/mc/app-settings.json*;
- конфигурационный файл User Console *am/uc/app-settings.json*;
- конфигурационный файл Identity Provider *am/idp/app-settings.json*;
- конфигурационный файл Key Server (при наличии) *am/indeed-key/app-settings.json*.

Настройки реестра

Настройки реестра с клиентских машин, где используются модули Windows Logon и/или ESSO Agent, расположенные в разделе *HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID*, *HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID*.

Руководство администратора

Получение лицензий

Операции с лицензиями

Настройка политик

Управление доступами и правами пользователей

Пользователи

Управление пользователями Indeed Access Manager

События

Управление событиями пользователей

Приложения

Количество глав: 2

Аутентификаторы

Общие настройки аутентификаторов в Management Console

Модули интеграции

Количество глав: 2

Получение лицензий

В Indeed Access Manager используется два типа лицензий:

- основная лицензия Indeed Access Manager;
- лицензии для дополнительных модулей.

Подробнее о лицензировании — в Лицензирование.

Получить

Лицензии генерируются на основе идентификатора инсталляции. Чтобы найти его и получить лицензии:

1. На боковой панели Management Console в блоке Настройки выберите Лицензии.
2. На вкладке Файлы лицензий скопируйте значение из поля Идентификатор инсталляции.
3. Отправьте скопированное значение закрепленному за вашей организацией менеджеру или в службу технической поддержки support@indeed-id.com.

Зарегистрировать

После получения лицензию нужно зарегистрировать. Для этого:

1. На боковой панели Management Console в блоке Настройки выберите Лицензии.
2. На вкладке Файлы лицензий нажмите Загрузить лицензию.
3. Нажмите Выбрать файл.
4. Выберите файл с лицензией и нажмите Зарегистрировать.

После успешной регистрации лицензии отображаются в таблице.

Выдать лицензию пользователю

Для всех пользователей, которые включены в политики доступа, выдача лицензий происходит автоматически. Лицензия закрепляется за пользователем после успешной аутентификации в соответствующем модуле.

Отозвать лицензию у пользователя

Для отзыва лицензий используется механизм автоматического освобождения лицензий. Этот механизм включен по умолчанию.

Лицензия отзывается у пользователя, если:

- пользователь удален из политики;
- пользователь отключен или перемещен из области действия политики;

- пользователь заблокирован/удален из каталога пользователей.

Если механизм отзыва лицензий отключен, то лицензии не будут освобождаться даже при выполнении этих условий.

В Indeed Access Manager также можно настроить время, по истечении которого лицензия будет отозвана, и перезапустить механизм отзыва, если лицензии не освобождаются автоматически. Для этого нужно отредактировать конфигурационный файл сервера *am/core/app-settings.json*. Подробнее — в Настройка механизма отзыва лицензий.

Распределить по политикам (отделам)

Чтобы ограничить количество используемых лицензий для подразделения, вы можете задать доступное количество лицензий для определенной политики.

Чтобы задать доступное количество лицензий для политики:

1. На боковой панели Management Console перейдите в раздел Политики.
2. Выберите в списке политику.
3. На странице политики перейдите на вкладку Лицензии.
4. Выберите лицензии.
5. Нажмите Доступное количество.
6. В открывшемся окне введите количество доступных лицензий для политики и нажмите Сохранить.

В разделе Распределение лицензий по политикам отобразится количество используемых лицензий в рамках каждой политики.

На странице политики вы можете просмотреть количество используемых лицензий в этой политике и общее доступное количество лицензий для этой политики.

Обновить

Чтобы обновить лицензии:

1. Обратитесь к закрепленному за вашей организацией менеджеру или в службу технической поддержки support@indeed-id.com с запросом на генерацию новых лицензий.
2. Зарегистрируйте новые лицензии в Management Console.

После окончания срока действия старых лицензий новые вступят в силу согласно заданным дате и времени.

Отслеживать срок действия лицензий можно в Management Console в разделе Лицензии.

Настройка политик

Политики позволяют задать настройки доступа для определенной группы пользователей. Подробнее о применении настроек политики — в разделе Политики доступа.

Создать политику

1. На боковой панели Management Console откройте раздел Политики.
2. Нажмите Создать политику.
3. Укажите значения для следующих параметров:
   - Приоритет. Чем больше значение, тем выше приоритет. Подробнее о приоритетах — в разделе Политики доступа.
   - Имя.
   - Описание (необязательно).

Настроить политику

В карточке политики можно настроить настроить параметры политики. Для этого:

1. На боковой панели Management Console откройте раздел Политики.
2. Откройте политику, нажав на ее название.
3. Перейдите на нужную вкладку и выполните соответствующие настройки.

Изменить информацию

В карточке политики можно изменить заданные ранее имя, приоритет и описание политики. Для этого:

1. На вкладке Информация нажмите Редактировать.

2. Внесите изменения.
3. Нажмите Сохранить.

Добавить/удалить приложение

Чтобы настроить политику, нужно добавить приложения, на которые будет распространяться ее действие. Для этого:

1. В карточке политики перейдите на вкладку Приложения.
2. Нажмите Добавить приложение.
3. В окне Добавить приложение выберите приложение и нажмите Добавить.

Приложение отобразиться в таблице добавленных приложений.

> **ПРИМЕЧАНИЕ**
>
> Добавить приложение можно только при наличии зарегистрированной лицензии для данного модуля.

Чтобы удалить приложение:

1. В карточке политики перейдите на вкладку Приложения.
2. Выберите приложение.
3. Нажмите Удалить.
4. Подтвердите удаление.

Приложение будет удалено из списка добавленных приложений.

Подробнее о настройках приложений — в разделе Приложения.

Настроить способ проверки доменного пароля

> **ПРИМЕЧАНИЕ**
>
> Только для приложений, интегрированных с модулем FreeRADIUS Extension.
>
> Настройка доступна только при выборе доменного пароля в качестве первого фактора аутентификации.

В разделе Политики можно настроить способ проверки первого фактора аутентификации.

1. В карточке политики перейдите на вкладку Приложения.
2. Выберите метод аутентификации из списка.
3. Если вы планируете использовать доменный пароль в качестве первого фактора аутентификации, выберите опцию:
   - Core Server, чтобы проверка первого фактора аутентификации осуществлялась на Core Server без дополнительных настроек;

- LDAP, чтобы проверка первого фактора аутентификации осуществлялась на LDAP-сервере.

4. Для корректной работы LDAP-сервера откройте файл *freeradius/.env* с переменными окружения и добавьте или раскомментируйте необходимые переменные `LDAP*`. Подробнее о настройке LDAP-сервера — в разделе Настройка LDAP-сервера.

Добавить/удалить объекты в области действия

Чтобы распространить настройки политики на определенных пользователей, нужно добавить объекты в области действия. В качестве таких объектов можно добавить отдельных пользователей, группы или подразделения.

Чтобы добавить объект в области действия:

1. В карточке политики перейдите на вкладку Область действия.
2. Нажмите Добавить.
3. В поле Тип объекта выберите тип — Пользователь, Группа или Подразделение.
4. В поле Расположение выберите расположение объекта. Это может быть весь пользовательский каталог или отдельное подразделение.
5. В поле Название укажите полное или часть имени объекта и нажмите Поиск.

Если оставить поле Название пустым, в результате поиска отобразятся все объекты заданного типа, имеющие выбранное расположение.

6. Выберите объект.
7. Нажмите Добавить.

Объект отобразится в списке объектов области действия.

Глобальный администратор может также искать и удалять объекты из области действия политики.

Для поиска объектов можно использовать шаблоны, заданные в конфигурационном файле Management Console.

Чтобы удалить объект область действия:

1. В карточке политики перейдите на вкладку Область действия.
2. Выберите объект.
3. Нажмите Удалить.
4. Подтвердите удаление. Объект будет удален из списка объектов в области действия.

Глобальный администратор может также воспользоваться функцией поиска объекта.

Чтобы найти и удалить объект в области действия политики:

1. В карточке политики перейдите на вкладку Область действия.
2. Нажмите Поиск. Откроется страница поиска.

3. В поле Тип объекта выберите тип — Пользователь, Группа или Подразделение. Выберите тип объекта и расположение.
4. В поле Расположение выберите расположение объекта. Это может быть весь пользовательский каталог или отдельное подразделение.
5. В поле Название укажите полное или часть имени объекта и нажмите Поиск.

Если оставить поле Название пустым, в результате поиска отобразятся все объекты заданного типа, имеющие выбранное расположение.

6. Выберите объект в результатах поиска и нажмите кнопку Удалить.
7. Подтвердите удаление. Объект будет удален из списка объектов в области действия.

Задать роли

Для политики также можно назначить пользователей, которые смогут выполнять роль администратора, оператора или инспектора относительно этой политики. Назначить роль можно отдельным пользователям или группе пользователей. Каждая роль имеет свой набор прав.

Чтобы назначить роль:

1. В карточке политики перейдите на вкладку Администраторы.
2. Нажмите Добавить.
3. Выберите роль — Администратор, Оператор или Инспектор.
4. В поле Тип объекта выберите тип — Пользователь или Группа.
5. В поле Расположение выберите расположение объекта. Это может быть весь пользовательский каталог или отдельное подразделение.
6. В поле Название укажите полное или часть имени объекта и нажмите Поиск. Если оставить поле Название пустым, в результате поиска отобразятся все объекты заданного типа, имеющие выбранное расположение.
7. Выберите объект.
8. Нажмите Добавить.

После добавления объект отобразится в списке на вкладке Администраторы.

Распределить лицензии

Можно задать доступное количество лицензий для определенной политики, чтобы ограничить количество используемых лицензий для подразделения. О том, как это сделать — в разделе Лицензии.

Удалить политику

Чтобы удалить политику:

1. На боковой панели Management Console откройте раздел Политики.
2. В списке политик выберите нужную политику.

3. Нажмите Удалить.
4. Подтвердите удаление.

Удаленная политика исчезнет из списка политик.

Также удалить политику можно в карточке политики. Для этого:

1. В карточке политики перейдите на вкладку Информация.
2. Нажмите Удалить.
3. Подтвердите удаление.

Пользователи

В карточке пользователя содержится информация о пользователе из подключенного каталога пользователей и настройки для пользователя в системе Indeed.

Найти пользователя

1. На боковой панели Management Console откройте раздел Пользователи.
2. В поле Имя введите имя пользователя, часть имени или UserPrincipalName (UPN, имя пользователя в формате адреса электронной почты, например username@domain.com).
3. В поле Контейнер выберите место поиска — весь контейнер или отдельное подразделение. Если оставить поле Имя пустым, в результате поиска отобразятся все пользователи в выбранном контейнере.
4. Нажмите Поиск.

В окне отобразится список пользователей, попадающих под критерии поиска.

Настроить поиск

Вы можете настроить поиск пользователей в Management Console по следующим запросам:

- по имени,
- по фамилии,
- по логину,
- по email,
- по имени пользователя в каталоге пользователей,
- по имени и фамилии.

Критерии поиска отображаются в Management Console на странице Пользователи в поле ввода поискового запроса. Поиск настраивается в конфигурационном файле Management Console (*am/mc/app-settings.json*).

Для удобства поиска вы можете использовать шаблоны.

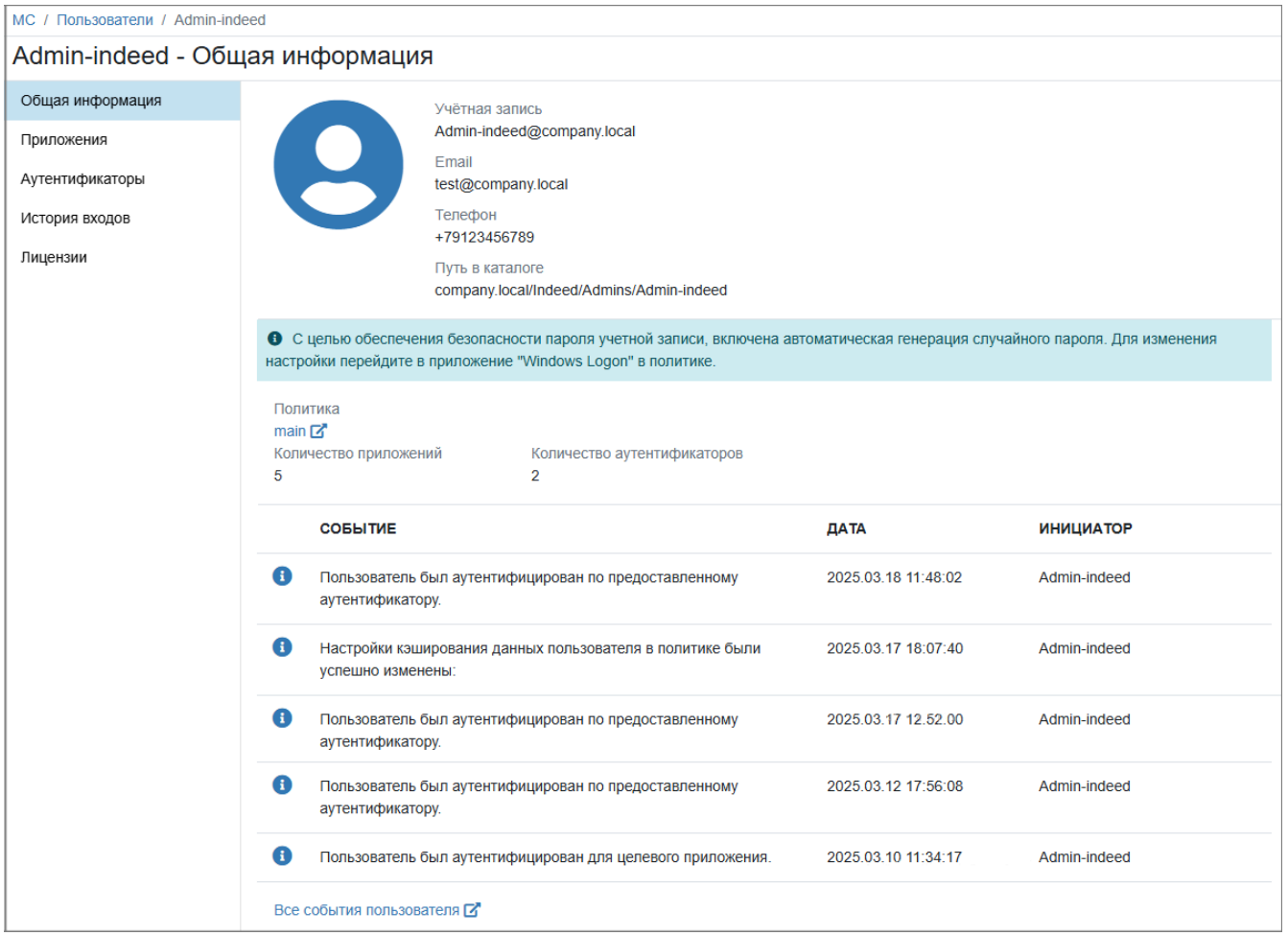
Пример запроса	Комментарий
иван*	В зависимости от ваших настроек ищет пользователя с именем, фамилией, логином или именем+фамилией, именем пользователя в AD, начинающиеся на «иван».
ва	В зависимости от ваших настроек ищет пользователя с именем, фамилией, логином или именем+фамилией, именем пользователя в AD, содержащие «ва» в начале, середине или конце.

Пример запроса	Комментарий
*нов	В зависимости от ваших настроек ищет пользователя с именем, фамилией, логином или именем+фамилией, именем пользователя в AD, заканчивающиеся на «нов».
иван	Запрос без * будет приведен к шаблону, который вы указали в параметре `searchTemplate`. Если шаблон searchTemplate не указан, то к запросу будут добавлены * с обеих сторон.
иван ** иван	Примеры неправильных запросов. Не возвращают результат поиска.

Просмотреть общую информацию

1. Найдите пользователя.
2. Откройте карточку пользователя, нажав на его имя.
3. Вкладка Общая информация содержит следующие данные:

- Информация о пользователе из каталога пользователей. Пример для пользователя из Active Directory:
  - Фото — атрибут `jpegPhoto` или `thumbnailPhoto`. Если атрибуты пустые, то используется изображение-заглушка.
  - Учетная запись — атрибут `userPrincipalName`.
  - Email — атрибут `mail`.
  - Телефон — атрибут `telephoneNumber`.
  - Путь в каталоге — расположение пользователя в каталоге Active Directory.
- Данные из системы Indeed AM:
  - Политика — название политики, которая распространяется на пользователя. Чтобы перейти в карточку политики, нажмите ее название.
  - Количество приложений — число приложений, которые доступны пользователю.
  - Количество аутентификаторов — общее число зарегистрированных аутентификаторов для пользователя.
  - События — пять последних событий, связанных с данным пользователем. Чтобы просмотреть все события, связанные с пользователем, нажмите Все события пользователя.



Добавить в политику

Чтобы распространить настройки политики на пользователя, нужно добавить его в область действия политики. Подробнее — в разделе Политики.

Просмотреть информацию о приложениях

Если пользователь попадает в область действия более одной политики, он получает доступ ко всем приложениям и модулям, добавленным в эти политики. Подробнее о политиках и их приоритетах — в разделе Политики доступа. Узнать, как управлять политиками в Management Console, можно в разделе Политики.

Чтобы просмотреть список доступных пользователю приложений и модулей:

1. В карточке пользователя перейдите на вкладку Приложения.
2. В открывшемся окне отобразится таблица со списком приложений и модулей, доступных пользователю.
3. Чтобы просмотреть более подробную информацию о методах аутентификации, настроенных для модуля или приложения, нажмите на его название.

Настроить аутентификаторы

В карточке пользователя также можно управлять настройками аутентификаторов для целевого пользователя. Подробнее — в статье Аутентификаторы.

Просмотреть историю входов

В карточке пользователя можно просмотреть историю входов пользователя в модули Indeed AM, а также выгрузить эту информацию в файл в форматах CSV, XLSX или PDF.

Чтобы просмотреть историю входов пользователя:

1. В карточке пользователя перейдите на вкладку История входов.
2. При необходимости задайте фильтры для выборочного поиска записей о входах:

- Укажите начальную и конечную даты периода, за который хотите посмотреть историю входов.
- Выберите приложение или модуль.
- Выберите тип аутентификатора, используемый для входа.
- Выберите статус события — Успешный вход, Не удалось войти или Не задано.

3. Нажмите Применить.
4. Чтобы выгрузить историю входов, нажмите Экспортировать и выберите формат файла — CSV, XLSX или PDF.

Просмотреть лицензии

Для всех пользователей, которые включены в политики доступа, выдача лицензий происходит автоматически. Лицензия закрепляется за пользователем после успешной аутентификации в соответствующем модуле.

Чтобы просмотреть доступные пользователю лицензии, в карточке пользователя перейдите на вкладку Лицензии.

Задать роль

Пользователю можно назначить роль относительно всей системы Indeed AM — глобальный администратор, оператор или инспектор. Каждая роль имеет свой набор прав. Подробнее о ролях — в разделе Роли.

Чтобы назначить роль:

1. На боковой панели Management Console откройте раздел Конфигурация.
2. Перейдите на вкладку Глобальные администраторы.
3. Нажмите Добавить и выберите необходимую роль.
4. В поле Имя введите имя пользователя, часть имени или UPN.
5. В поле Тип объекта выберите тип — Пользователь или Группа.

6. В поле Расположение выберите расположение объекта. Это может быть весь пользовательский каталог или отдельное подразделение. Если оставить поле Имя пустым, в результате поиска отобразятся все объекты заданного типа, имеющие выбранное расположение.
7. Выберите объект.
8. Нажмите Добавить.

Пользователь с назначенной ролью отобразится в списке на вкладке Глобальные администраторы.

Также можно назначить пользователю роль в рамках одной политики.

События

Записи обо всех операциях Indeed AM отражаются в журнале событий на каждом сервере Indeed AM.

В Indeed AM ведется учет событий следующих типов:

- ошибка;
- информация;
- предупреждение.

Чтобы открыть журнал событий, в левом меню в блоке Аудит выберите События.

Для более узкого поиска событий используйте параметры фильтра:

- *Пользователь или инициатор* — в поле требуется выбрать учетную запись, от имени которой было совершено событие;
- *Приложение* — фильтрация событий по выбранному компоненту Indeed AM.
- *Начальная\Конечная дата* — в полях указывается временной интервал, в котором будет выполнена выборка событий.
- *Тип аутентификатора* — фильтрация событий по выбранному методу аутентификации Indeed AM.
- *Модуль* — фильтрация событий по выбранному модулю системы Indeed AM.

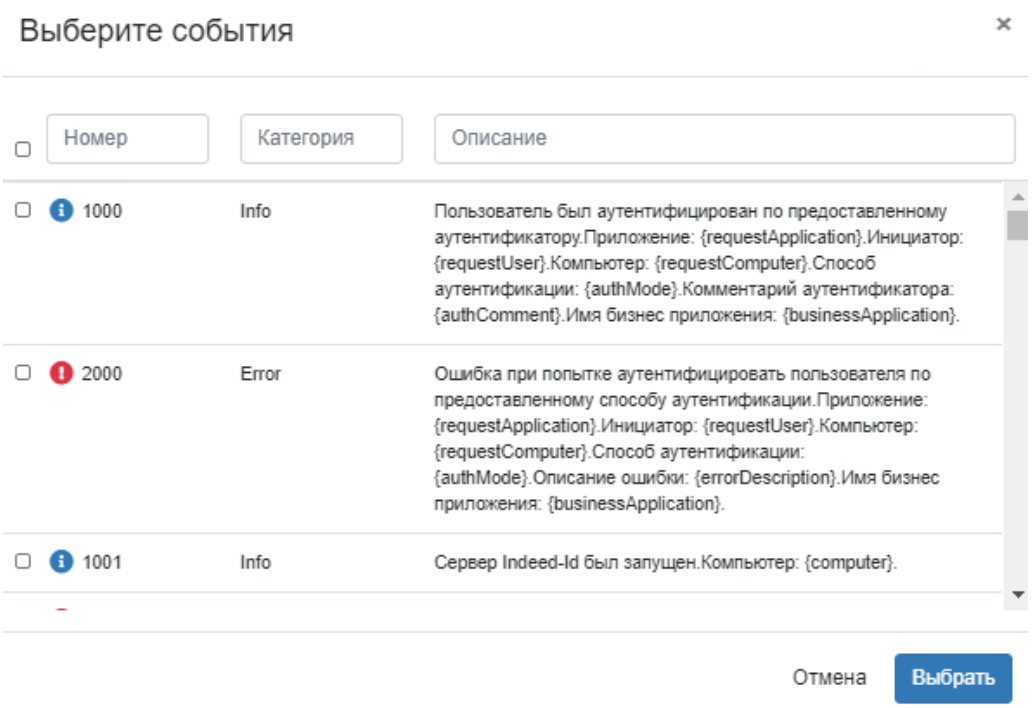
> **ПРИМЕЧАНИЕ**
>
> При поиске событий будут отображены события для конкретного модуля системы, в отличие от параметра *Приложение*, где события отображаются для конкретного приложения системы, но могут присутствовать различные модули.

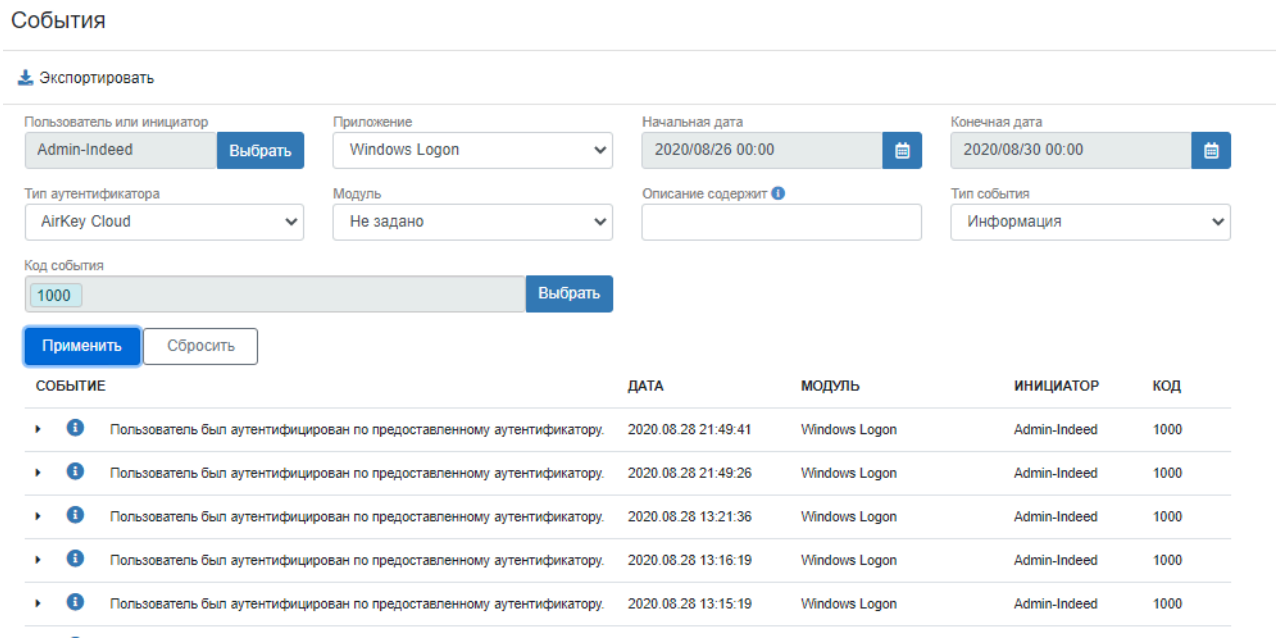
- *Описание содержит* — в поле указывается полное значение атрибута события (приложение, администратор, компьютер и др.).

> **ИНФОРМАЦИЯ**
>
> Поиск по части запроса с использованием символа * невозможен: это связано с ограничениями хранилища EventLog Microsoft. Возможности поиска с использованием остальных поддерживаемых методов хранения ограничены по возможностям самого ограниченного источника — EventLog.

- *Тип события* — в поле указывается тип события: ошибка, информация, предупреждение. Если выбран параметр *Не задано*, осуществляется выборка всех событий.

- *Код события* — в поле можно выбрать конкретное событие системы Indeed AM.





Для экспорта событий нажмите кнопку Экспортировать в верхней части страницы. Экспорт возможен в форматах csv, xlsx, pdf.

Список событий Indeed Core Server и Indeed Key Server вы можете просмотреть в Справочнике.

Приложения

Данный раздел содержит приложения и модули, для которых в Indeed AM зарегистрированы лицензии. Также в этом разделе можно вручную добавить приложения, интегрированные с модулями FreeRADIUS Extension и LDAP Proxy, по инструкциям:

- для FreeRADIUS Extension;
- для LDAP Proxy.

> **ПРИМЕЧАНИЕ**
>
> Перед тем как добавить приложение, зарегистрируйте лицензию соответствующего модуля.

Другие модули интеграции автоматически отображаются в разделе Приложения после регистрации лицензии.

Общие настройки

Изменить общую информацию

1. В карточке приложения на вкладке Общая информация нажмите Редактировать.
2. Измените название или описание приложения.
3. Нажмите Сохранить.

Загрузить логотип

1. На вкладке Общая информация в разделе Логотип нажмите Загрузить. Поддерживаются изображения формата JPG и PNG, максимальный размер — 512KB.
2. Выберите файл.
3. Нажмите Загрузить.

Модуль FreeRADIUS Extension

Предварительная настройка

Перед добавлением интегрированного приложения:

1. Настройте модуль FreeRADIUS Extension;
2. Установите и настройте провайдеры аутентификации;
3. Интегрируйте бизнес-приложение с FreeRADIUS Extension.

> ⚠ **ВАЖНО**
>
> Если аутентификация для приложений будет осуществляться не через Access Manager, настройте доступ для таких приложений в Management Console в разделе Конфигурация. В противном случае вход в эти приложения будет невозможен.

Добавить приложение

Чтобы добавить приложение, интегрированное с FreeRADIUS Extension:

1. На боковой панели Management Console откройте раздел Приложения.
2. Нажмите Добавить приложение.
3. В открывшемся окне выберите FreeRADIUS Extension и введите название приложения. Название должно быть уникальным.
4. Нажмите Создать.

   > ⓘ **ПРИМЕЧАНИЕ**
   >
   > Нельзя добавить еще одно приложение, если вы не изменили IP-адрес по умолчанию у ранее добавленного приложения.

5. В открывшемся окне приложения перейдите на вкладку RADIUS.
6. Измените значение поля IP-адрес сервера приложений. Можно указать несколько значений через запятую.

   Поддерживается формат IPv4. Также можно использовать маску или префикс для указания подсети.

Примеры адресов

Корректные адреса

```
- 192.168.0.1/24
- 172.16.3.251
- 10.0.0.1
```

Некорректные адреса

```
- 192.168.0.300 — некорректный IPv4;
- 172.16.3.251/33 — некорректная маска сети;
- example.com — не является IP-адресом.
```

7. В настройке Если для пользователя не заданы параметры доступа в приложение при необходимости разрешите или запретите доступ в приложения для тех пользователей, на которых не распространяются политики доступа Access Manager (например, для пользователей из другого домена).

Добавить в политику

Чтобы настройки приложения были применены для пользователей, добавьте приложение в политику. Сделать это можно только при наличии зарегистрированной лицензии для данного модуля.

Чтобы добавить приложение в политику:

1. Перейдите в раздел Политики.
2. Выберите политику из списка.
3. В карточке политики перейдите на вкладку Приложения.
4. Нажмите Добавить приложение.
5. Из выпадающего списка выберите приложение.
6. Нажмите Добавить.

Приложение отобразится в списке добавленных приложений.

Настроить аутентификатор

Для приложений, интегрированных с FreeRADIUS Extension, можно выбрать только один способ входа. При добавлении приложения в политику по умолчанию включается первый способ входа из доступных.

В списке доступных методов аутентификации отображаются провайдеры, установленные на Core Server и поддерживаемые RADIUS-приложениями.

Поддерживается как однофакторная, так и двухфакторная аутентификация.

Предварительная настройка

Прежде чем настроить однофакторную или двухфакторную аутентификацию, установите провайдеры.

Однофакторная аутентификация

Чтобы настроить однофакторную аутентификацию:

1. На боковой панели Management Console откройте раздел Политики.
2. Выберите политику.
3. Перейдите на вкладку Приложения.
4. Выберите приложение, интегрированное с FreeRADIUS Extension.
5. В списке Метод аутентификации выберите провайдер с префиксом 1FA.
6. Нажмите Сохранить.

Доступные способы входа по однофакторной аутентификации:

- Secured TOTP;
- Hardware OTP;
- Passcode;
- Software TOTP;
- Hardware TOTP,
- Indeed Key (OTP);
- КЛЮЧ: Сервис Паролей.

Двухфакторная аутентификация

Чтобы настроить двухфакторную аутентификацию:

1. На боковой панели Management Console откройте раздел Политики.
2. Выберите политику.
3. Перейдите на вкладку Приложения.
4. Выберите приложение, интегрированное с FreeRADIUS Extension.
5. В списке Метод аутентификации выберите провайдер с префиксом 2FA.
6. Нажмите Сохранить.

Доступные способы входа по двухфакторной аутентификации:

- Passcode + Secured TOTP;
- Passcode + SMS OTP;
- Passcode + Software TOTP;
- Passcode + Indeed Key;
- Windows Password + Hardware OTP;
- Windows Password + Hardware TOTP;
- Windows Password + Secured TOTP;
- Windows Password + Software TOTP;
- Windows Password + Storage SMS OTP;
- Windows Password + Indeed Key;
- Windows Password + Email OTP;
- Windows Password + SMS OTP;
- Windows Password + КЛЮЧ: Сервис Паролей.

Опциональные настройки

Изменить общую информацию

1. В карточке приложения на вкладке Общая информация нажмите Редактировать.
2. Измените название или описание приложения.
3. Нажмите Сохранить.

Загрузить логотип

1. На вкладке Общая информация в разделе Логотип нажмите Загрузить. Поддерживаются изображения формата JPG и PNG, максимальный размер — 512KB.
2. Выберите файл.
3. Нажмите Загрузить.

Настроить обработку повторных запросов на аутентификацию

FreeRadius-сервер по умолчанию обрабатывает дубликаты запросов в соответствии со стандартом RFC 5080. Если клиентское приложение не включает поддержку RFC 5080, можно настроить расширенную обработку дубликатов запросов на аутентификацию на стороне Access Manager.

Эта необязательная настройка может быть полезна, когда наблюдаются повторные запросы. Например, если пользователь не успевает подтвердить вход через push-уведомление и получает его повторно.

Чтобы настроить расширенную обработку повторных запросов на аутентификацию:

1. В карточке приложения на вкладке RADIUS включите опцию Включить расширенную обработку дубликатов.
2. В поле Атрибуты запроса для поиска дубликатов введите значения атрибутов RADIUS. Можно указать несколько значений через запятую. Значения по умолчанию — *1* (User-Name) и *4* (NAS-IP-Address).

   В качестве атрибутов могут выступать имя пользователя, пароль, IP-адрес, с которого отправляется запрос на аутентификацию, и другие параметры. Запрос считается повторным, если значения всех указанных атрибутов в настройке совпадают со значениями в кешированном запросе. Подробнее о поддерживаемых атрибутах RADIUS — в официальной документации Cisco.
3. Нажмите Сохранить.

Модуль LDAP Proxy

Предварительная настройка

Перед добавлением интегрированного приложения:

1. Настройте модуль LDAP Proxy;
2. Установите и настройте провайдеры аутентификации;
3. Интегрируйте бизнес-приложение с LDAP Proxy.

> ⚠ **ВАЖНО**
>
> Если аутентификация для приложений будет осуществляться не через Access Manager, настройте доступ для таких приложений в Management Console в разделе Конфигурация. В противном случае вход в эти приложения будет невозможен.

Добавить приложение

Чтобы добавить приложение, интегрированное с LDAP Proxy:

1. На боковой панели Management Console откройте раздел Приложения.
2. Нажмите Добавить приложение.
3. В открывшемся окне выберите LDAP Proxy и введите название приложения. Название должно быть уникальным.
4. Нажмите Создать.

   > ⓘ **ПРИМЕЧАНИЕ**
   >
   > Нельзя добавить еще одно приложение, если вы не изменили IP-адрес по умолчанию у ранее добавленного приложения.

5. В открывшемся окне приложения перейдите на вкладку LDAP Proxy.
6. Измените значение поля IP-адрес сервера приложений. Можно указать несколько значений через запятую.

   Поддерживается формат IPv4. Также можно использовать маску или префикс для указания подсети.

7. В настройке Если для пользователя не заданы параметры доступа в приложение при необходимости разрешите или запретите доступ в приложения для тех пользователей, на которых не распространяются политики доступа Access Manager (например, для пользователей из другого домена).

Добавить в политику

Чтобы настройки приложения были применены для пользователей, добавьте приложение в политику. Сделать это можно только при наличии зарегистрированной лицензии для данного модуля.

Чтобы добавить приложение в политику:

1. Перейдите в раздел Политики.
2. Выберите политику из списка.
3. В карточке политики перейдите на вкладку Приложения.
4. Нажмите Добавить приложение.
5. Из выпадающего списка выберите приложение.
6. Нажмите Добавить.

Приложение отобразится в списке добавленных приложений.

Настроить аутентификатор

Для приложений, интегрированных с LDAP Proxy, можно выбрать только один способ входа. При добавлении приложения в политику по умолчанию включается первый способ входа из доступных.

В списке доступных методов аутентификации отображаются провайдеры, установленные на Core Server и поддерживаемые приложениями LDAP Proxy.

Поддерживается как однофакторная, так и двухфакторная аутентификация.

Предварительная настройка

Прежде чем настроить однофакторную (1FA) или двухфакторную (2FA) аутентификацию, установите поддерживаемые провайдеры.

Чтобы настроить аутентификацию:

1. На боковой панели Management Console откройте раздел Политики.
2. Выберите политику.
3. Перейдите на вкладку Приложения.
4. Выберите приложение, интегрированное с LDAP Proxy.
5. В списке Метод аутентификации выберите провайдер:
   - 2FA: Windows Password + Indeed Key (Push)
   - 2FA: Windows Password + Telegram (Push)
   - 1FA: Windows Password
6. Нажмите Сохранить.

Опциональные настройки

Изменить общую информацию

1. В карточке приложения на вкладке Общая информация нажмите Редактировать.
2. Измените название или описание приложения.
3. Нажмите Сохранить.

Загрузить логотип

1. На вкладке Общая информация в разделе Логотип нажмите Загрузить. Поддерживаются изображения формата JPG и PNG, максимальный размер — 512KB.
2. Выберите файл.
3. Нажмите Загрузить.

Аутентификаторы

Настроить аутентификаторы можно в трех разделах Indeed Access Manager:

- Конфигурация→Аутентификаторы
- Вкладка Приложения карточки политики
- Вкладка Аутентификаторы карточки пользователя

Общие настройки

Раздел Конфигурация→Аутентификаторы содержит общие для всех пользователей настройки всех аутентификаторов, установленных на сервере Indeed AM. Настройки могут отличаться в зависимости от аутентификатора.

Разрешить/Запретить использование и редактирование

Чтобы настроить использование и редактирование аутентификаторов:

1. Выберите аутентификатор.
2. В секции Основные настройки:
    - В настройке Запретить использовать укажите, могут ли пользователи использовать или регистрировать выбранный аутентификатор.
    - Задайте другие настройки в зависимости от типа аутентификатора.
3. Для аутентификаторов, которые требуют регистрации, в секции Доступные пользователю действия:
    - В настройке Регистрация новых аутентификаторов укажите, могут ли пользователи регистрировать новые аутентификаторы.
    - В настройке Редактирование имеющихся аутентификаторов укажите, могут ли пользователи изменять уже зарегистрированные аутентификаторы.
    - В настройке Удаление имеющихся аутентификаторов укажите, могут ли пользователи удалять уже зарегистрированные аутентификаторы.
    - В настройке Разрешить редактирование комментария к аутентификатору укажите, в какой момент пользователи могут редактировать комментарии к уже зарегистрированным аутентификаторам.

Изменить максимальное количество

В разделе Конфигурация→Аутентификаторы можно задать максимальное количество аутентификаторов, которое пользователи могут зарегистрировать для себя. Эта настройка доступна для Passcode Provider. Чтобы задать максимальное количество:

1. Выберите аутентификатор.

2. В поле Максимальное количество введите значение.
3. Нажмите Сохранить.

Настроить автоматическую блокировку

Для аутентификаторов можно настроить автоматическую блокировку и разблокировку в случае неудачных попыток входа.

> **ПРИМЕЧАНИЕ**
>
> Настройка блокировки аутентификаторов в Management Console не поддерживается для двухфакторной аутентификации для приложений RADIUS Extension.

Чтобы настроить автоматическую блокировку в Management Console:

1. Выберите аутентификатор.
2. Для параметра Блокировать способ аутентификации в случае серии неудачных попыток установите значение *Да*.
3. Задайте значения для следующих параметров:
   - Количество попыток аутентификации до блокировки. Этот параметр определяет количество неудачных попыток аутентификации до блокировки способа входа. Способ входа остается заблокированным до момента разблокировки администратором или до истечения таймаута до разблокировки. Значение параметра по умолчанию — *5*. Заданное значение должно быть больше или равно *1*.
   - Сброс счетчика блокировки через (минут). Этот параметр определяет, сколько минут должно пройти после неудачной попытки входа, прежде чем счетчик неудачных попыток будет обнулен. Значение параметра по умолчанию — *5*. Заданное значение должно быть больше или равно *1*. Интервал сброса счетчика блокировки не должен быть больше таймаута до разблокировки способа входа, только если значение последнего не равно *0*.
   - Таймаут до разблокировки способа входа (минут). Этот параметр определяет период, на который заданный способ входа будет заблокирован. По истечении таймаута способ входа будет автоматически разблокирован. Значение параметра по умолчанию — *5*. Если установлено значение *0*, способ входа остается недоступным для пользователя, пока администратор не разблокирует его в Management Console.
4. Нажмите Сохранить.

Настроить принудительную проверку

Для регистрации аутентификаторов Software TOTP и Secured TOTP можно настроить принудительную проверку аутентификатора.

Данная настройка работает в версии Management Console 8.2.6 или выше. Если установлена более старая версия, необходимо обновление. Посмотреть номер установленной версии можно в разделе Помощь и поддержка боковой панели Management Console.

Чтобы включить принудительную проверку:

1. В разделе Конфигурация→Аутентификаторы выберите аутентификатор Software TOTP или Secured TOTP.
2. В разделе Основные настройки включите принудительную проверку.

> **ПРИМЕЧАНИЕ**
>
> При регистрации Storage SMS принудительная проверка выполняется по умолчанию.

Если принудительная проверка аутентификатора включена, при регистрации появится дополнительное окно подтверждения для ввода данных аутентификации.

Для подтверждения регистрации введите полученные данные аутентификации и нажмите Подтвердить.

Настройки для политик

Можно также задать настройки аутентификаторов, которые распространяются на всех пользователей, включенных в политику. Эти настройки доступны в карточке политики в Management Console.

Чтобы задать настройки аутентификаторов для пользователей, включенных в политику:

1. На боковой панели Management Console выберите Политики.
2. Выберите политику.
3. Перейдите на вкладку Приложения. Эта вкладка содержит информацию о приложениях и модулях интеграции, добавленных в политику. Подробнее о настройках политик — в Политики.
4. Выберите приложение.
5. В секции Доступные методы аутентификации разрешите/запретите использование аутентификаторов.
6. Для модулей Identity Provider, Windows Logon, ADFS Extension выберите режим работы Indeed Key Provider.

Настройки для отдельного пользователя

Задать настройки аутентификаторов для отдельного пользователя можно в его карточке в Management Console.

Чтобы открыть карточку пользователя:

1. На боковой панели Management Console выберите Пользователи.
2. Найдите пользователя. Подробнее о настройках поиска — в Пользователи.
3. В карточке пользователя перейдите на вкладку Аутентификаторы. Эта вкладка содержит информацию о количестве зарегистрированных аутентификаторов пользователя и их параметры.

Зарегистрировать

Перед регистрацией аутентификаторов создайте политику и распространите ее на целевых пользователей.

> **ПРИМЕЧАНИЕ**
>
> Провайдеры Email OTP и SMS OTP не требуют регистрации и могут использоваться, если у пользователя задан email или номер телефона соответственно. Если параметры не заданы, то аутентификаторы не отображаются в списке доступных для пользователя.

Чтобы зарегистрировать аутентификатор:

1. Нажмите Зарегистрировать и выберите метод аутентификации из выпадающего списка.

   Если у пользователя зарегистрировано максимальное количество аутентификаторов для определенного метода, то данный метод аутентификации отображаться не будет.

2. Выполните дополнительные настройки для регистрации аутентификатора. Для различных аутентификаторов отличаются окна и действия для регистрации.

3. После успешной регистрации статус аутентификатора — *Действующий*.

4. Если был удален провайдер, имеющий зарегистрированные аутентификаторы, то статус аутентификатора — *Не установлен*.

Аутентификатор появится в списке зарегистрированных для пользователя аутентификаторов.

Запретить

Пользователю можно запретить использовать определенный аутентификатор. Чтобы запретить пользователю использовать метод аутентификации со всеми аутентификаторами, относящимися к этому методу, выберите Настроить методы аутентификации.

> **ПРИМЕЧАНИЕ**
>
> Способ аутентификации Windows Password не может быть запрещен. Рекомендуем отключить учетную запись пользователя в каталоге пользователей, если нужно заблокировать доменный пароль.

Чтобы запретить пользователю использовать аутентификатор:

1. Выберите аутентификатор.
2. Нажмите Запретить.

После отключения аутентификатора пользователь не сможет использовать данный способ входа. Статус аутентификатора — *Запрещен*.

> **ПРИМЕЧАНИЕ**
>
> При запрете использовать необучаемый аутентификатор, например Email OTP, автоматически запрещается метод аутентификации. Статус — *Метод запрещен*.

В карточке пользователя можно запретить использовать аутентификатор только для одного пользователя. Запретить использовать аутентификатор всем пользователям можно в разделе Конфигурация→Аутентификаторы.

Разрешить

Чтобы разрешить пользователю использовать аутентификатор:

1. Выберите аутентификатор.
2. Нажмите Разрешить использовать.

После включения аутентификатора пользователь сможет использовать данный способ входа. Статус аутентификатора — *Действующий*.

> **ПРИМЕЧАНИЕ**
>
> В карточке пользователя можно разрешить использовать аутентификатор, только если запрет был установлен для отдельного пользователя. Снять запрет на использование аутентификатора для всех пользователей можно только в разделе Конфигурация→Аутентификаторы.

Разблокировать

Если для аутентификатора отключена автоматическая разблокировка после неудачных попыток входа, его нужно разблокировать вручную в карточке пользователя. Для этого:

1. Выберите заблокированный аутентификатор.
2. Нажмите Разблокировать.

Способ входа снова будет доступен для пользователя.

Удалить

1. Выберите аутентификатор.
2. Нажмите Удалить.
3. Подтвердите удаление.

Аутентификатор исчезнет из списка зарегистрированных для пользователя аутентификаторов.

Запретить метод аутентификации

Чтобы запретить пользователю использовать метод аутентификации:

1. Нажмите Настроить методы аутентификации. Откроется окно со всеми доступными методами аутентификации для выбранного пользователя.
2. В колонке Статус нажмите ○, чтобы запретить выбранный метод аутентификации.

После запрета метода пользователь не сможет использовать аутентификаторы, относящиеся к этому методу. Статус аутентификаторов — *Метод запрещен*.

Если вы запретили пользователю использовать метод аутентификации:

- Пользователь не сможет использовать данный способ входа.
- Для пользователя будет недоступна регистрация аутентификаторов, относящихся к этому способу входа.
- Если запрещенный метод аутентификации состоит в цепочке MFA, аутентификация по этой цепочке будет недоступна.

В карточке пользователя можно запретить использовать метод аутентификации только для одного пользователя. Запретить использовать метод аутентификации всем пользователям можно только в разделе Конфигурация→Аутентификаторы.

Модули интеграции

В данном разделе содержится описание глобальных настроек для модулей интеграции Access Manager. Настроить модули интеграции можно в разделе Конфигурация→Модули интеграции. Чтобы настроить интеграцию с бизнес-приложениями, перейдите в раздел Приложения.

Настройки для FreeRADIUS Extension

Доступ к недобавленным приложениям

Если аутентификация для приложений осуществляется не через Access Manager, настройте для таких приложений доступ в Management Console. В противном случае вход в эти приложения будет невозможен.

Чтобы настроить доступ для RADIUS-приложений, не добавленных в Access Manager:

1. На боковой панели Management Console откройте раздел Конфигурация.
2. На вкладке Модули интеграции выберите FreeRADIUS Extension.
3. Разрешите или запретите доступ в настройке Доступ для Radius-приложений, которые не добавлены Management Console.
4. Нажмите Сохранить и перезапустите контейнер с приложением FreeRADIUS Extension.

Время ввода второго фактора аутентификации

1. На боковой панели Management Console откройте раздел Конфигурация.
2. На вкладке Модули интеграции выберите FreeRADIUS Extension.
3. Установите период в секундах, за который пользователь должен ввести второй фактор аутентификации.
4. Нажмите Сохранить и перезапустите контейнер с приложением FreeRADIUS Extension.

Поиск клиентского приложения по IP-адресу

1. На боковой панели Management Console откройте раздел Конфигурация.
2. На вкладке Модули интеграции выберите FreeRADIUS Extension.
3. В настройке Определение IP-адреса клиента Radius установите очередность атрибутов, по которым будет производиться поиск IP-адреса клиентского приложения. Если IP-адрес найден в первом заданном атрибуте, поиск останавливается.

   Возможные значения:

   - NASIPAddress (по умолчанию),
   - SrcIPAddress.
4. Нажмите Сохранить и перезапустите контейнер с приложением FreeRADIUS Extension.

Настройки для LDAP Proxy

Доступ к недобавленным приложениям

Если аутентификация для приложений осуществляется не через Access Manager, настройте для таких приложений доступ в Management Console. В противном случае вход в эти приложения будет невозможен.

Чтобы настроить доступ для приложений LDAP Proxy, не добавленных в Access Manager:

1. На боковой панели Management Console откройте раздел Конфигурация.
2. На вкладке Модули интеграции выберите LDAP Proxy.
3. Разрешите или запретите доступ в настройке Доступ для Radius-приложений, которые не добавлены Management Console.
4. Нажмите Сохранить и перезапустите контейнер с приложением LDAP Proxy.

Руководство пользователя

Карточка пользователя

Информация о пользователе

Управление аутентификаторами

Управление аутентификаторами пользователя

Локализация

Смена языка в консоли пользователя

Управление Windows Password

Изменить или зарегистрировать доменный пароль

Карточка пользователя

В карточке пользователя содержится следующая информация:

- Данные из профиля в каталоге пользователей:
  - Имя учетной записи — атрибут *userPrincipalName*;
  - Путь;
  - E-mail — атрибут *mail*;
  - Телефон — атрибут *telephoneNumber*;
  - Фото — атрибут *jpegPhoto* или *thumbnailPhoto*. Если атрибуты пустые, то используется изображение-заглушка;
  - Сведения о зарегистрированных аутентификаторах.

Управление аутентификаторами

В карточке пользователя на вкладке Аутентификаторы содержится информация о количестве зарегистрированных аутентификаторов пользователя и их параметры. По умолчанию пользователи могут только регистрировать аутентификаторы. Для остальных действий с аутентификаторами запросите права у администратора.

Зарегистрировать

> **ПРИМЕЧАНИЕ**
>
> Провайдеры Email OTP и SMS OTP регистрируются автоматически, если у пользователя задан email или номер телефона в каталоге пользователей.

Чтобы зарегистрировать аутентификатор:

1. Выберите аутентификатор.
2. Нажмите .
3. Выберите Зарегистрировать.
4. Введите запрашиваемые данные и нажмите Сохранить. Запрашиваемые данные и действия при регистрации могут отличаться в зависимости от аутентификатора.
5. При необходимости введите данные аутентификации, чтобы подтвердить регистрацию.

После успешной регистрации аутентификатор отобразится как зарегистрированный.

Если у пользователя зарегистрировано максимальное количество аутентификаторов, регистрация завершится ошибкой *Доступ запрещен: Достигнуто максимальное количество аутентификаторов.*

Если зарегистрированный аутентификатор удален администратором, он перестанет отображаться в карточке пользователя.

Изменить

Чтобы изменить аутентификатор:

1. Выберите аутентификатор.
2. Нажмите .
3. Выберите Изменить.
4. Введите новые данные для аутентификатора.

5. Нажмите Сохранить. При необходимости введите данные аутентификации, чтобы подтвердить регистрацию.

Удалить

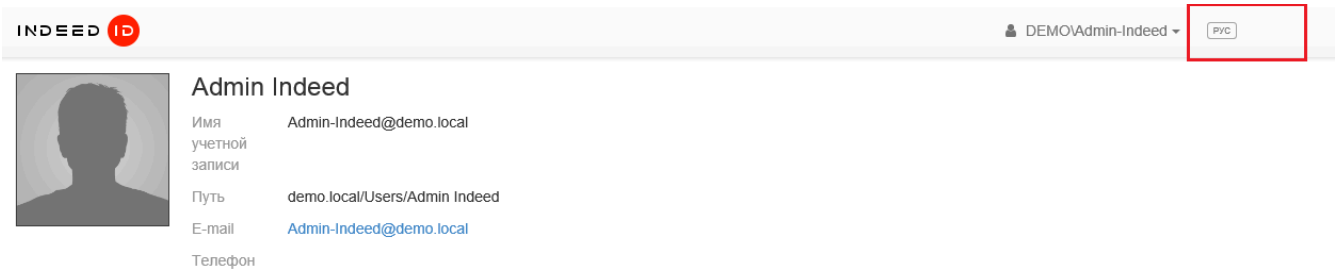
Чтобы удалить аутентификатор:

1. Выберите аутентификатор.
2. Нажмите  .
3. Выберите Удалить.
4. Подтвердите удаление.

Локализация

Чтобы сменить язык:

1. Нажмите кнопку с названием языка в правом верхнем углу.
2. В выпадающем списке выберите нужный язык.



Управление Windows Password

В User Console можно зарегистрировать или изменить доменный пароль.

Зарегистрировать

Чтобы зарегистрировать доменный пароль:

1. Откройте User Console.
2. Перейдите на вкладку Аутентификаторы.
3. В списке аутентификаторов выберите Windows Password.
4. Нажмите  .
5. Выберите Зарегистрировать пароль.
6. В открывшемся окне введите пароль и нажмите Сохранить.

Изменить

Чтобы сменить доменный пароль:

1. Откройте User Console.
2. Перейдите на вкладку Аутентификаторы.
3. В списке аутентификаторов выберите Windows Password.
4. Нажмите  .
5. Выберите Изменить пароль.
6. В появившемся окне введите текущий пароль, новый пароль, подтвердите новый пароль и нажмите Сохранить.

API

Общая информация

Общая информация

Быстрый старт

Быстрый старт

Методы API

Количество глав: 8

Сценарии использования

Количество глав: 6

Общая информация

API Indeed AM предназначен для интеграции с приложениями.

В данном разделе описаны основные моменты и общие параметры, которые необходимы для использования API Indeed.

Запрос к API

Для обращения к методу необходимо выполнить запрос `POST` или, для некоторых методов, запрос `GET` по *http(s)://<dns_indeedam_server>/am/core/<url_api_method>*, где:

- *dns_indeedam_server* — полное DNS-имя сервера, где развернут Indeed Core Server;
- *url_api_method* — адрес соответствующего метода. Адреса указаны в документации к методу либо в Swagger.

Пример для метода `openVerifySession`, где DNS-имя сервера Indeed AM: *indeedam.indeed.local*:

```
https://indeedam.indeed.local/am/core/api/v6/templateSession/openVerifySession
```

> ⚠ **ВАЖНО!**
>
> При использовании протокола HTTPS загрузите на сервер Indeed AM действующий сертификат.

`UserId`

Уникальный идентификатор пользователя из системы Indeed.

Идентификатор состоит из строкового ID, указанного в *app-settings.json* AM в параметре `userId`, и `objectGuid` пользователя из Active Directory.

Например, в параметре `userId` указано значение GUID пользователя *10efa04f-7ba9-47d8-89db-56e166f1679f*. `UserId` пользователя будет `UserId\_10efa04f-7ba9-47d8-89db-56e166f1679f`.

Для получения `userId` можно воспользоваться методом `[POST]/api/v6/user/searchUserId`.

`modeId`

Уникальный идентификатор способа аутентификации Indeed.

Способы аутентификации:

- Indeed AM Windows Password Provider {CF189AF5-01C5-469D-A859-A8F2F41ED153}

- Indeed AM Passcode Provider {F696F05D-5466-42b4-BF52-21BEE1CB9529}
- Indeed AM Email OTP Provider {093F612B-727E-44E7-9C95-095F07CBB94B}
- Indeed AM Hardware TOTP Provider {CEB3FEAF-86ED-4A5A-BD3F-6A7B6E60CA05}
- Indeed AM HOTP Provider {CEB3FEAF-86ED-4A5A-BD3F-6A7B6E60CA05}
- Indeed AM Storage SMS OTP Provider {3F2C1156-B5AF-4643-BFCB-9816012F3F34}
- Indeed AM SMS OTP Provider {EBB6F3FA-A400-45F4-853A-D517D89AC2A3}
- Indeed AM Software OTP Provider {0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0}
- Indeed Key Provider {DEEF0CB8-AD2F-4B89-964A-B6C7ECA80C68}
- Indeed AM MFA Provider {070719BA-EB57-4EA8-BB4D-D15A33E7363D}

`ApplicationId`

Внутренний модуль

> ⚠ **ВАЖНО!**
>
> Для работы с внутренним модулем не требуется лицензия, достаточно иметь права на операции, предоставляемые внутренними модулями.

Функциональность Access Manager разбита на группы, за которые отвечают внутренние модули. Они реализуют внутреннюю бизнес-логику решения. Их строковые идентификаторы используются для обращения к разным частям API Core Server.

Внутренние модули Core Server:

- User Profile Setting Management
- User Access Control Management
- Hardware Devices Management
- License Management
- Authenticator Management
- Authenticator Enrollment
- User Accounts Management
- Policy Management
- User Cache Management
- Business Applications Management

Кроме того, есть еще набор внутренних приложений:

- Enterprise Management Console
- Self Service
- Native Enroller

Модуль интеграции

> ⚠ **ВАЖНО!**
>
> Для работы с модулями интеграции требуется лицензия для соответствующего модуля.

Это модуль, реализующий взаимосвязь Access Manager и внешних систем, с которыми выполняется интеграция. К ним относятся:

- Windows Logon
- FreeRADIUS Extension
- Identity Provider
- ADFS Extension
- RDP Windows Logon
- Authentication API

Идентификатор политики

Чтобы узнать идентификатор политик:

1. Откройте Management Console.
2. Перейдите на вкладку Политики.
3. Выберите целевую политику.
4. Скопируйте идентификатор политики из параметра `policyId` в URL.

Быстрый старт

Для вызова методов API и тестирования запросов вы можете использовать интерфейс Swagger, который встроен в Core Server.

Для включения доступа к интерфейсу:

1. Откройте конфигурационный файл *am/core/app-settings.json*.
2. В параметре `Documentation` в теге `Enabled` установите значение *true*.
3. Выпишите и настройте собственный клиентский сертификат и добавьте его в доверенные сертификаты.

Интерфейс Swagger будет доступен по ссылке *http(s)://<DNS_IndeedAM_Server>/am/core/swagger/*. Для доступа к интерфейсу выберите созданный ранее клиентский сертификат.

Токен администратора запроса

Для выполнения большинства запросов API требуются определенные права в системе Indeed. Для успешного выполнения таких запросов необходимо выполнить аутентификации в API под пользователем с требуемым набором прав. После выполнения аутентификации будет получен токен сессии, который используется в запросах API.

Чтобы получить токен:

1. `/api/v6/templateSession/openVerifySession`
2. `/api/v6/templateSession/prepareTemplateData`
3. `/api/v6/templateSession/createTemplate`
4. `/api/v6/logon/authenticate`

При успешной аутентификации возвращается токен в формате JSON.

Подробнее об этом сценарии смотрите в разделе Как работает скрипт.

Методы API

Authenticator

getUserAuth, findByUserIds

License

getAllLicenses, getCatalogObjectLicenses

Logon

isAvailable, authenticate, getAvailableMethods

Policy

get

TemplateSession

createTemplate, openEnrollSession, openVerifySession, openIdentifySession, prepareTemplateData

User

searchUserId

UserCatalog

getObjects, searchUsers, searchGroups, searchContainers

UserProfile

findLogonInfoByUser

Authenticator

`getUserAuth`

Возвращает все обученные аутентификаторы пользователя по внутреннему идентификатору в Indeed Access Manager.

```
POST /api/v6/authenticator/getUserAuth
```

Объект запроса

```
{
  "Id": "00000000-0000-0000-0000-000000000000",
  "UserId": "string",
  "AccessToken": "string",
  "ApplicationId": "string"
}
```

в объекте запроса:

- `Id` — обязательный параметр. Внутренний идентификатор Indeed Access Manager.
- `UserId` — обязательный параметр. Внутренний идентификатор пользователя в Indeed Access Manager.
- `AccessToken` — обязательный параметр. Токен администратора, от имени которого выполняется запрос к API.
- `ApplicationId` — обязательный параметр. Строковый идентификатор модуля Indeed AM.

Объект ответа

```
{
  "AuthenticationCountLimit": 0,
  "CreatedOn": "2022-10-26T07:23:08.550Z",
  "Description": "string",
  "ExpirationDate": "2022-10-26T07:23:08.550Z",
  "Flags": 1,
  "Id": "00000000-0000-0000-0000-000000000000",
  "IsDisabled": true,
  "IsLocked": true,
  "ModeDeviceName": "string",
  "ModeId": "00000000-0000-0000-0000-000000000000",
  "ModeType": 0,
  "ModeTypeName": "string",
  "UserId": "string",
  "SerialNumber": "string",
  "Device": {
    "Id": "00000000-0000-0000-0000-000000000000",
    "AuthType": "00000000-0000-0000-0000-000000000000",
    "SerialNumber": "string",
    "RegistrationDate": "2022-10-26T07:23:08.550Z",
    "IsEnabled": true,
    "LastUserId": "string",
    "Comment": "string",
    "Model": "string"
  },
  "CreatedBy": "string"
}
```


findByUserIds

Возвращает внутренний идентификатор пользователя в Indeed Access Manager.

```
POST /api/v6/authenticator/findByUserIds
```

Объект запроса

```
{
  "UserId": "string",
  "AccessToken": "string",
  "ApplicationId": "string"
}
```

В объекте запроса:

- `UserId` — обязательный параметр. Внутренний идентификатор пользователя в Indeed Access Manager.
- `AccessToken` — обязательный параметр. Токен администратора, от имени которого выполняется запрос к API.
- `ApplicationId` — обязательный параметр. Строковый идентификатор модуля Indeed AM.

Объект ответа

```
[
  "00000000-0000-0000-0000-000000000000"
]
```

License

`getAllLicenses`

Возвращает все зарегистрированные в Indeed Access Manager лицензии.

```
POST /api/v6/license/getAllLicenses
```

Объект запроса

```
{
  "AccessToken": "string",
  "ApplicationId": "string"
}
```

в объекте запроса:

- `AccessToken` — обязательный параметр. Токен администратора, от имени которого выполняется запрос к API.
- `ApplicationId` — обязательный параметр. Строковый идентификатор модуля Indeed AM.

Объект ответа

```
{
  "LicenseUid": "string",
  "InstanceId": "string",
  "Type": "string",
  "Amount": 0,
  "BeginDate": "2022-10-26T08:43:22.406Z",
  "EndDate": "2022-10-26T08:43:22.406Z",
  "Description": "string",
  "Issuer": "string",
  "IssuedTo": "string",
  "IssueDate": "2022-10-26T08:43:22.406Z",
  "Id": "00000000-0000-0000-0000-000000000000",
  "ControlValue": "string"
}
```

getCatalogObjectLicenses

Возвращает зарегистрированные лицензии для конкретного объекта каталога.

```
POST /api/v6/license/getCatalogObjectLicenses
```

Объект запроса

```
{
  "ObjectId": "string",
  "AccessToken": "string",
  "ApplicationId": "string"
}
```

в объекте запроса:

- `ObjectId` — идентификатор каталога, для которого будут получены зарегистрированные лицензии.
- `AccessToken` — обязательный параметр. Токен администратора, от имени которого выполняется запрос к API.
- `ApplicationId` — обязательный параметр. Строковый идентификатор модуля Indeed AM.

Объект ответа

```
{
  "ApplicationId": "string",
  "CatalogObjectId": "string",
  "PolicyId": "00000000-0000-0000-0000-000000000000"
}
```

getAcquiredLicenseCount

Возвращает количество используемых лицензий указанного типа в выбранной политике.

```
POST /api/v6/license/getAcquiredLicenseCount
```

Объект запроса

```
{
  "LicenseType": "string",
  "PolicyId": "00000000-0000-0000-0000-000000000000",
  "AccessToken": "string",
  "ApplicationId": "string"
}
```

в объекте запроса:

- `LicenseType` — тип лицензии.
- `PolicyId` — идентификатор политики. Идентификатор можно получить в URL-адресе политики в Management Console или с помощью метода `/api/v6/policy/getAll`.
- `AccessToken` — обязательный параметр. Токен администратора, от имени которого выполняется запрос к API.
- `ApplicationId` — обязательный параметр. Строковый идентификатор модуля Indeed AM.

Объект ответа

```
"0"
```

Logon

`isAvailable`

Выполняет проверку доступности аутентификации пользователя в приложении.

- В параметре `ApplicationId` указывается идентификатор приложения.
- В параметре `UserId` указывается идентификатор целевого пользователя.
- В параметре `ExcludeWindowsPassword` указывается *true\false*:
  - Если указано *true*, значит из проверки исключается возможность аутентификации по доменному паролю. В таком случае пользователю должен быть доступен любой другой метод аутентификации, иначе запрос вернет *false*.
  - Если указано *false*, доменный пароль не исключается из возможных способов аутентификации в сценарии.

```
[POST] /api/v6/logon/isAvailable
```

Объект запроса

```
{
  "ApplicationId": "string",
  "UserId": "string",
  "ExcludeWindowsPassword": true
}
```

в объекте запроса:

- `ApplicationId` — обязательный параметр. Строковый идентификатор модуля Indeed AM.
- `UserId` — обязательный параметр. Идентификатор пользователя в Indeed AM.
- `ExcludeWindowsPassword` — опциональный параметр. Значение по умолчанию *true*.

Объект ответа

```
true\false
```

`authenticate`

Выполняет аутентификацию пользователя в приложении *BusinessApplication* по зарегистрированному шаблону *TemplateId*.

```
[POST] /api/v6/logon/authenticate
```

Объект запроса

```
{
  "TemplateId": "00000000-0000-0000-0000-000000000000",
  "BusinessApplication": "string"
}
```

Объект ответа

```
{
  "Token": "string",
  "LogonResult": {
    "Result": "string"
  },
  "UserId": "string"
}
```

Пример успешного объекта ответа

```
{
  "ValidPropertiesMask": 5,
  "Token": "eyJ0e----.eyJleH----",
  "LogonResult": {
    "ValidPropertiesMask": 0,
    "Result": null
  },
  "UserId": "UserId_b1cfaa29-6368-4c50-9868-06dbbe21fe23"
}
```

`getAvailableMethods`

Возвращает массив доступных способов аутентификации для пользователя *UserId* в указанном в *ApplicationId* приложении.

```
[POST] /api/v6/logon/getAvailableMethods
```

Объект запроса

```
{
  "ApplicationId": "string",
  "UserId": "string",
  "IncludeModeIds": [
    "00000000-0000-0000-0000-000000000000"
  ],
  "ExcludeModeIds": [
    "00000000-0000-0000-0000-000000000000"
  ]
}
```

в объекте запроса:

- `ApplicationId` — обязательный параметр. Строковый идентификатор модуля Indeed AM.
- `UserId` — обязательный параметр. Идентификатор пользователя в Indeed AM.
- `IncludeModeIds` — опциональный параметр. GUID методов аутентификации Indeed, которые будут учитываться при проверке возможности аутентификации.
- `ExcludeModeIds` — опциональный параметр. GUID методов аутентификации Indeed, которые будут исключаться при проверке возможности аутентификации.

Объект ответа

```
{
  "AutheticationMethods": [
    "00000000-0000-0000-0000-000000000000"
  ]
}
```

Примеры ответов

Нет доступных методов

```
{
  "ValidPropertiesMask": 1,
  "AutheticationMethods": []
}
```

Доступен доменный пароль

```
{
  "ValidPropertiesMask": 1,
  "AutheticationMethods": [
    "cf189af5-01c5-469d-a859-a8f2f41ed153"
  ]
}
```

Policy

`get`

Возвращает информацию и настройки политик по идентификатору.

```
POST /api/v6/policy/get
```

Объект запроса

```
{
  "Id": "00000000-0000-0000-0000-000000000000",
  "AccessToken": "string",
  "ApplicationId": "string"
}
```

в объекте запроса:

- `Id` — обязательный параметр. Идентификатор политики.
- `AccessToken` — обязательный параметр. Токен администратора, от имени которого выполняется запрос к API.
- `ApplicationId` — обязательный параметр. Строковый идентификатор модуля Indeed AM.

Объект ответа

```
{
  "Id": "00000000-0000-0000-0000-000000000000",
  "Name": "string",
  "Description": "string",
  "Settings": \[
    {
      "Id": "00000000-0000-0000-0000-000000000000",
      "SettingType": 0,
      "Value": {},
      "ParentId": "00000000-0000-0000-0000-000000000000"
    }
  \],
  "CreatedById": "string",
  "CreatedTime": "2022-10-26T07:23:08.768Z",
  "LastEditedById": "string",
  "LastEditedTime": "2022-10-26T07:23:08.768Z"
}
```


в объекте ответа:

- `SettingType`:
  - 0 — область действия политики. Возвращается внутренний GUID объектов области действия.
  - 1 — приложения политики.
  - 2 — приоритет политики.

TemplateSession

`createTemplate`

Создает шаблон для аутентификации по идентификатору открытой сессии.

```
[POST] /api/v6/templateSession/createTemplate
```

Объект запроса

```
{
 "SessionId": "00000000-0000-0000-0000-000000000000"
}
```

в объекте запроса:

- `SessionId` — обязательный параметр. Указывается GUID открытой сессии, полученный из метода `openVerifySession`.

Объект ответа

```
"00000000-0000-0000-0000-000000000000"
```

`openEnrollSession`

```
[POST] /api/v6/templateSession/openEnrollSession
```

`openVerifySession`

Открывает сессию для аутентификации пользователя, указанного в `UserSearchParams` в приложении `ApplicationId`, с использованием способа аутентификации `ModeId`.

```
[POST] /api/v6/templateSession/openVerifySession
```

Объект запроса

```
{
  "UserSearchParams": {
    "Id": "string",
    "Email": "string",
    "Phone": "string",
    "NameFormat": 0,
    "Name": "string",
    "ApplicationId": "string"
  },
  "ModeId": "00000000-0000-0000-0000-000000000000",
  "ApplicationId": "string"
}
```

в объекте запроса:

- `UserSearchParams` — массив параметров для поиска пользователя;
  - `Id` — внутренний идентификатор пользователя в Indeed AM;
  - `Email` — адрес электронной почты пользователя из каталога пользователей;
  - `Phone` — номер телефона пользователя из каталога пользователей;
  - `NameFormat` — числовое значение формата имени, которое будет указано в `Name`. Поддерживаются следующие форматы:
    - 0 — Undefined;
    - 1 — CanonicalName;
    - 2 — PrincipalName: *name@domain.name*;
    - 3 — SamCompatibleName: *domain\logon-name*;
    - 4 — DistinguishedName;
    - 5 — Sid;
- `ModeId` — обязательный параметр. Строковый идентификатор используемого способа аутентификации.
- `ApplicationId` — обязательный параметр. Строковый идентификатор модуля Indeed AM.

Объект ответа

```
GUID открытой сессии

"00000000-0000-0000-0000-000000000000"
```

`openIdentifySession`

```
[POST] /api/v6/templateSession/openIdentifySession
```

`prepareTemplateData`

Добавляет информацию о шаблоне пользователя.

```
[POST] /api/v6/templateSession/prepareTemplateData
```

Объект запроса

```
{
  "Data": {},
  "SessionId": "00000000-0000-0000-0000-000000000000"
}
```

в объекте запроса:

- `Data` — аутентификационные данные пользователя (одноразовый код или пароль или другие данные в зависимости от используемого способа аутентификации);
- `SessionId` — идентификатор открытой сессии, полученный в `openVerifySession`.

Объект ответа

```
{
  "EnoughData": true,
  "BinaryData": "string",
  "StringData": "string"
}
```

в объекте ответа:

- `EnoughData` — признак того, что данных от клиента для формирования шаблона достаточно.

Пример объекта ответа

```
{
  "ValidPropertiesMask": 1,
  "EnoughData": true,
  "BinaryData": null,
  "StringData": null
}
```

User

`searchUserId`

Возвращает `UserId` по входным параметрам.

```
POST /api/v6/user/searchUserId
```

Объект запроса

```
{
  "Id": "string",
  "Email": "string",
  "Phone": "string",
  "NameFormat": 0,
  "Name": "string",
  "ApplicationId": "string"
}
```

в объекте запроса:

- `NameFormat`:
  - 0 — Undefined,
  - 1 — CanonicalName,
  - 2 — PrincipalName,
  - 3 — SamCompatibleName,
  - 4 — DistinguishedName,
  - 5 — Sid.

Объект ответа

```
"xxxx\_0000000-0000-0000-0000-000000000000"
```

UserCatalog

`getObjects`

Возвращает данные объекта каталога пользователя Indeed AM по внутреннему идентификатору.

```
POST /api/v6/userCatalog/getObjects
```

Объект запроса

```
{
  "Ids": [
    "string"
  ],
  "AccessToken": "string",
  "ApplicationId": "string"
}
```

в объекте запроса:

- `Ids` — массив внутренних идентификаторов.
- `AccessToken` — обязательный параметр. Токен администратора, от имени которого выполняется запрос к API.
- `ApplicationId` — обязательный параметр. Строковый идентификатор модуля Indeed AM.

Объект ответа

```
{
  "Id": "string",
  "RawObjectId": "string",
  "Name": "string",
  "CanonicalName": "string",
  "PrincipalName": "string",
  "SamCompatibleName": "string",
  "DistinguishedName": "string",
  "Sid": "string",
  "IsGroup": true,
  "IsContainer": true,
  "IsRemoved": true,
  "GroupsIds": [
    "string"
  ],
  "ContainerId": "string"
}
```

searchUsers

Поиск пользователя по входным параметрам.

```
POST /api/v6/userCatalog/searchUsers
```

Объект запроса

```
{
  "Operation": 0,
  "Filters": [
    {
      "AttributeName": "string",
      "Value": {},
      "Negation": true
    }
  ],
  "Limit": 0,
  "LoadParentObjects": true,
  "AccessToken": "string",
  "ApplicationId": "string"
}
```

в объекте запроса:

- `Operation`:
  - 0 — ИЛИ;
  - 1 — И;
- `Filters` - массив фильтров для поиска:
  - `AttributeName` — имя атрибута из используемого каталога пользователей для поиска;
  - `Value` — значение атрибута из используемого каталога пользователей для поиска;
  - `Negation` — отрицание заданного фильтра. Значения *true\false*.

Объект ответа

```
[
  {
    "FirstName": "string",
    "MiddleName": "string",
    "LastName": "string",
    "Email": "string",
    "Phone": "string",
    "IsDisabled": true,
    "IsLocked": true,
    "Id": "string",
    "RawObjectId": "string",
    "Name": "string",
    "CanonicalName": "string",
    "PrincipalName": "string",
    "SamCompatibleName": "string",
    "DistinguishedName": "string",
    "Sid": "string",
    "IsGroup": true,
    "IsContainer": true,
    "IsRemoved": true,
    "GroupsIds": [
      "string"
    ],
    "ContainerId": "string"
  }
]
```

`searchGroups`

Поиск группы по входным параметрам.

```
POST /api/v6/userCatalog/searchGroups
```

Объект запроса

```
{
  "Operation": 0,
  "Filters": [
    {
      "AttributeName": "string",
      "Value": {},
      "Negation": true
    }
  ],
  "Limit": 0,
  "LoadParentObjects": true,
  "AccessToken": "string",
  "ApplicationId": "string"
}
```

в объекте запроса:

- `Operation`:
  - 0 — ИЛИ;
  - 1 — И;
- `Filters` — массив фильтров для поиска:
  - `AttributeName` — имя атрибута из используемого каталога пользователей для поиска;
  - `Value` — значение атрибута из используемого каталога пользователей для поиска;
  - `Negation` — отрицание заданного фильтра. Значения *true\false*.

Объект ответа

```
[
  {
    "FirstName": "string",
    "MiddleName": "string",
    "LastName": "string",
    "Email": "string",
    "Phone": "string",
    "IsDisabled": true,
    "IsLocked": true,
    "Id": "string",
    "RawObjectId": "string",
    "Name": "string",
    "CanonicalName": "string",
    "PrincipalName": "string",
    "SamCompatibleName": "string",
    "DistinguishedName": "string",
    "Sid": "string",
    "IsGroup": true,
    "IsContainer": true,
    "IsRemoved": true,
    "GroupsIds": [
      "string"
    ],
    "ContainerId": "string"
  }
]
```


searchContainers

Поиск подразделения по входным параметрам.

```
POST /api/v6/userCatalog/searchContainers
```

Объект запроса

```
{
  "Operation": 0,
  "Filters": [
    {
      "AttributeName": "string",
      "Value": {},
      "Negation": true
    }
  ],
  "Limit": 0,
  "LoadParentObjects": true,
  "AccessToken": "string",
  "ApplicationId": "string"
}
```

в объекте запроса:

- `Operation`:
  - 0 — ИЛИ;
  - 1 — И;
- `Filters` — массив фильтров для поиска:
  - `AttributeName` — имя атрибута из используемого каталога пользователей для поиска;
  - `Value` — значение атрибута из используемого каталога пользователей для поиска;
  - `Negation` — отрицание заданного фильтра. Значения *true\false*.

Объект ответа

```
[
  {
    "FirstName": "string",
    "MiddleName": "string",
    "LastName": "string",
    "Email": "string",
    "Phone": "string",
    "IsDisabled": true,
    "IsLocked": true,
    "Id": "string",
    "RawObjectId": "string",
    "Name": "string",
    "CanonicalName": "string",
    "PrincipalName": "string",
    "SamCompatibleName": "string",
    "DistinguishedName": "string",
    "Sid": "string",
    "IsGroup": true,
    "IsContainer": true,
    "IsRemoved": true,
    "GroupsIds": [
      "string"
    ],
    "ContainerId": "string"
  }
]
```

UserProfile

`findLogonInfoByUser`

Возвращает информацию об аутентификациях пользователя.

```
POST /api/v6/userProfile/findLogonInfoByUser
```

Объект запроса

```
{
  "UserId": "string",
  "AccessToken": "string",
  "ApplicationId": "string"
}
```

Объект ответа

```
{
  "UserId": "xxxx\_000000-0000-0000-0000-00000000000",
  "ApplicationId": "Native Enroller",
  "LogonDate": "2022-05-04T10:54:05.821+03:00",
  "ModeId": "000000-0000-0000-0000-00000000000"
}
```

в объекте ответа:

- `UserId` — внутренний идентификатор пользователя;
- `ApplicationId` — идентификатор приложения, в которое был выполнен вход;
- `LogonDate` — дата и время входа;
- `ModeId` — идентификатор способа входа.

Сценарии использования

Создание отчетов

Создание отчетов

Сбор статистики по обученным аутентификаторам пользователей

Сбор статистики по обученным аутентификаторам пользователей

Получение списка пользователей с лицензиями

Получение списка пользователей с лицензиями

Двухфакторная аутентификация в API

Настройка двухфакторной аутентификации через API

Удаление пользователей из политики

Удаление пользователей из политики

Получение списка пользователей из политики

Получение списка пользователей из политики

Создание отчетов

> **ИНФОРМАЦИЯ**
>
> Скрипт для создания отчетов вы можете скачать по этой ссылке.

Предварительные требования

- Установленный модуль Active Directory для PowerShell в Windows Server.
- Работоспособный сервер Indeed AM.
- Пользователь, от имени которого будет запускаться скрипт, должен обладать минимальными глобальными правами *Инспектор* в системе Indeed AM.

Как работает скрипт

Скрипт формирует отчеты по подготовленным сценариям. Для создания отчетов используется API Indeed AM Core и Indeed AM Log Server.

Скрипт поддерживает настройку фильтрации для формирования отчета:

- выборка из контейнера пользовательского каталога,
- выборка по конкретному пользователю,
- выборка по дате.

Фильтры

Поле *Container*

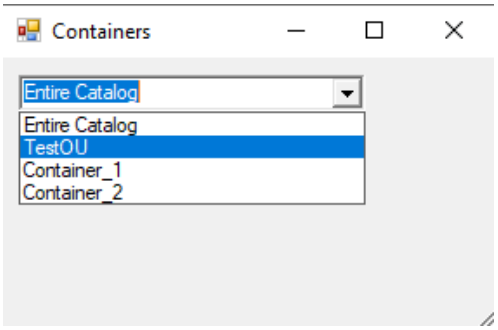
Поле предназначено для выбора подразделений, в домене в которых будет выполняться поиск пользователей. Значение *Entire Catalog* означает, что выбран корневой каталог с каталогом пользователей, который используется сервером Indeed AM.

Поиск подразделений из пользовательского каталога выполняется с использованием метода `searchContainers` в соответствующей функции в файле *Base/AMAPI/UserCatalog.ps1*.

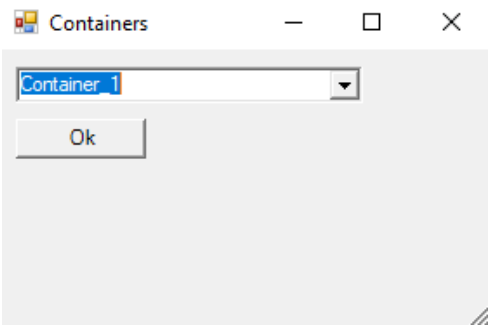
> **ПРИМЕЧАНИЕ**
>
> Выгрузка контейнеров выполняется из пользовательского каталога. Значение в поле не редактируемое.
>
> Имя корневых каталогов пользователей, заданных в конфигурационном файле Core Server, не отображается.

Для выбора необходимого подразделения из каталога выполните следующие действия:

1. Нажмите кнопку Select.



2. В выпадающем списке окна Containers выберите контейнер и нажмите Ok.



Поле *Groups*

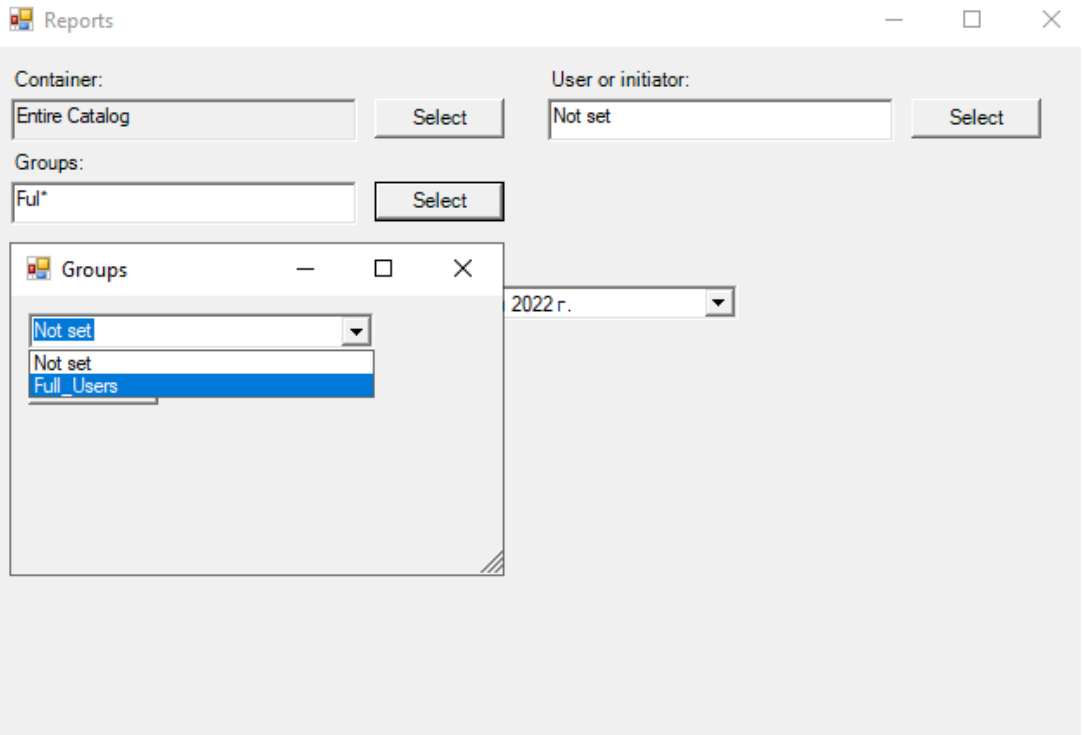
Поле предназначено для поиска групп в домене или в подразделении, которое было выбрано в поле *Container*. Значение по умолчанию *Not set*.

Поиск пользователя выполняется с использованием метода `searchGroups` в соответствующей функции в файле *Base/AMAPI/UserCatalog.ps1*.

Подготовка запроса с использованием заданных фильтров выполняется в функции `searchGropsUseFilters` в файле *Scenarios/Reports/SearchUseFilters.ps1*.

В поиске учитывается параметр Active Directory `Name`.

Для поиска группы при необходимости выберите контейнер и введите имя группы. Если данные не указаны, то будут найдены все группы из каталога пользователя.



Поле *User or initiator*

Поле предназначено для поиска пользователя в домене; в подразделении, которое было выбрано в поле *Container*; группе из поля *Groups*. Значение по умолчанию *Not set*.

Поиск пользователя выполняется с использованием метода `searchUsers` в соответствующей функции в файле *Base/AMAPI/UserCatalog.ps1*.

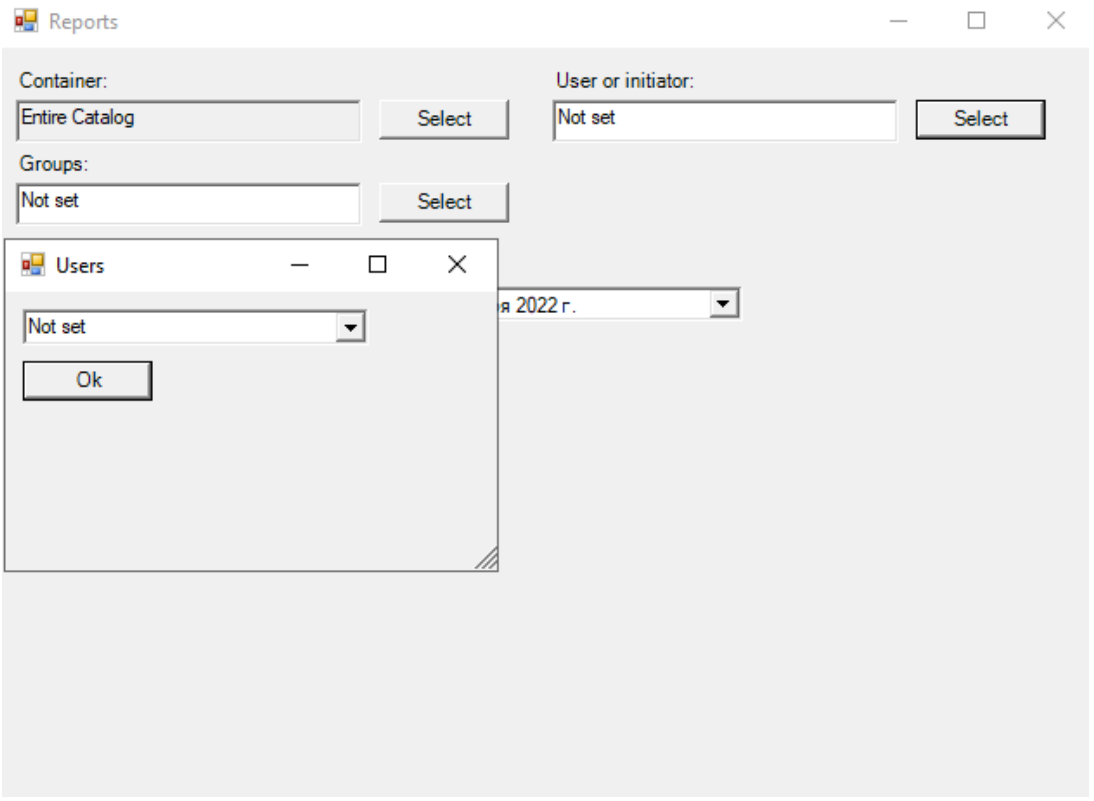
Подготовка запроса с использованием заданных фильтров выполняется в функции `searchUsersUseFilters` в файле *Scenarios/Reports/SearchUseFilters.ps1*.

В поиске учитываются следующие параметры:

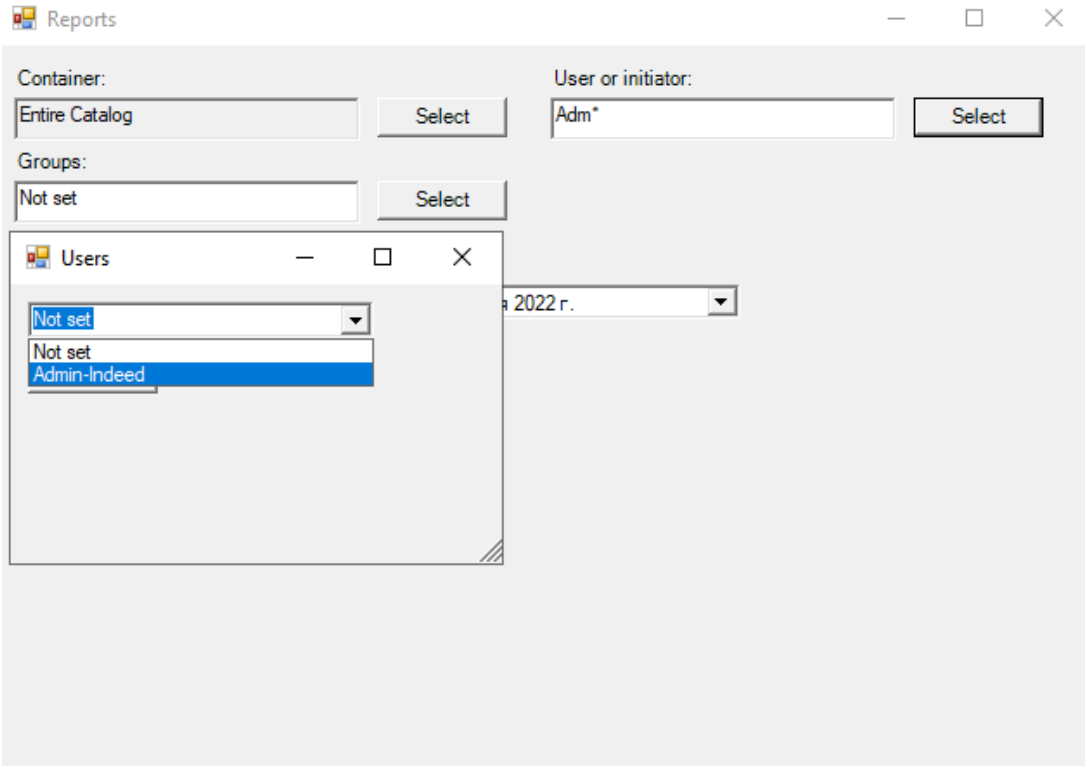
- `ContainerId` — идентификатор контейнера, в котором будет выполнен поиск пользователя. Параметр используется, если было выбрано подразделение в поле *Container*.
- `FirstName`, `MiddleName`, `LastName`, `PrincipalName`, `Name` — соответствующие значения атрибутов пользователя из Active Directory.

> **ПРИМЕЧАНИЕ**
>
> Все параметры используются с логической операцией *OR*.

Для поиска пользователей можно нажать кнопку Select и выбрать всех найденных пользователей.



Для поиска пользователя можно указать часть имени, в конце указанной части добавьте символ *.



Настройка

Для работы скрипта необходимо сконфигурировать файл *Config.ps1*, который находится в корне папки со скриптом.

> ⚠ **ВАЖНО!**
>
> В данном разделе описана общая настройка скрипта. Для отдельных отчетов может потребоваться дополнительная настройка.

В файле:

- `$domainName` — указывается имя домена. Обязательный параметр.
- `$eventsCount` — ограничение по выгрузке событий. Опциональный параметр. По умолчанию количество получаемых событий не ограничено, параметр закомментирован.
- `$serverUrl` — URL сервера Indeed AM. Обязательный параметр.
- `$logServerUrl` — URL Indeed AM Log Server. Обязательный параметр.
- `$logsOnFile` — включение\отключение логирования в файл. Обязательный параметр. По умолчанию включено.
- `$logsOnConsole` — включение\отключение логирования в консоль. Обязательный параметр. По умолчанию отключено.
- `$apiVersion` — версия API, используемая в скрипте. Обязательный параметр.

Создание отчета с количеством аутентификаций по указанным провайдерам

В данном отчете формируется таблица с количеством аутентификаций пользователя по массиву аутентификаторов в конкретном приложении Indeed, указанному в файле *Config.ps1*.

Создание отчета выполняется в функции `createLogonsByProviderReport` в файле *Create-reports/Scenarios/Reports/CreateReports.ps1*.

Настройка

> ⚠ **ВАЖНО!**
>
> В разделе описаны настройки для конкретного отчета. Перед началом работы необходимо выполнить базовую настройку, описанную в разделе Настройка.

Для настройки откройте файл *Config.ps1* и выполните следующее:

1. В переменной `AuthForReport` задайте идентификатор провайдера Indeed и наименование для отчета:
   - Значения должны задаваться в формате *GUID провайдера Indeed=Наименование для отчета*.
   - Значения GUID провайдеров можно найти в разделе Идентификаторы способов аутентификации.
   - Наименование для отчета может быть произвольным. Данное наименование будет использовано при создании таблицы.

Пример настройки с доменным паролем и отпечатком пальца

```
$AuthForReport          = @{
    'CF189AF5-01C5-469D-A859-A8F2F41ED153' = 'Пароль'
    'A0EF00AD-1EEB-4D48-8BCF-06E19CD5585F' = 'Отпечаток пальца'
}
```

2. В переменной `ApplicationId` указывается наименование модуля интеграции Indeed. Список модулей можно найти в разделе Идентификаторы приложений.

   Пример настройки для приложения Windows Logon

   ```
   $ApplicationId="Windows Logon"
   ```

3. Вы можете указать, в каком формате будет выгружаться отчет. Поддерживаются форматы CSV и HTML. Можно выгружать отчет в двух форматах одновременно. Если обе переменные не определены, это приведет к ошибке выгрузки.

   Чтобы отчет выгружался в CSV, задайте переменной `CsvReport` значение *true*.

   ```
   $CsvReport = 'true'
   ```

   Чтобы отчет выгружался в HTML задайте переменной `HtmlReport` значение *true*.

   ```
   $HtmlReport = 'true'
   ```

4. В переменной `pathReportLogonsByProvider` указывается путь до папки, где будет сохранен отчет. По умолчанию используется корень папки со скриптом.

   ```
   $pathReportLogonsByProvider="$ScriptDirectory\Reports\LogonsByProvider"
   ```

Пример работы

1. Для начала работы со скриптом откройте оснастку PowerShell, перейдите в папку со скриптом и запустите файл *Start.ps1* через команду `.\Start.ps1`.

2. При необходимости настройте фильтры скрипта и нажмите кнопку Report of number of logins by providers.

3. После завершения работы скрипта будет сформирована таблица формата HTML по указанному при настройке пути.

Имя пользователя	Приложение	Дата и время последнего входа	Палец	Пароль
who_i@indeed.local	Windows Logon	22.09.2022 14:11:03	0	0
Ivan_I@indeed.local	Windows Logon	22.09.2022 14:13:06	0	0
vf-adm@indeed.local	Windows Logon	28.09.2022 11:21:16	2	1
ii@indeed.local	Windows Logon	The user:ii@indeed.local is not logged in to any application	0	0
vf@indeed.local	Windows Logon	The user:vf@indeed.local is not logged in to any application	0	0
rdp@indeed.local	Windows Logon	06.05.2022 14:31:41	0	0
Admin-Indeed@indeed.local	Windows Logon	28.09.2022 11:09:44	1	1
Number of users: 7 Number of logons by 'Палец': 3 Number of logons by 'Пароль': 2				

Сбор статистики по обученным аутентификаторам пользователей

> **ИНФОРМАЦИЯ**
>
> Скрипт для сбора статистики вы можете скачать по этой ссылке.

Предварительные требования

- Установленный модуль Active Directory для PowerShell в Windows Server.
- Работоспособный сервер Indeed AM.
- Пользователь, от имени которого будет запускаться скрипт, должен обладать минимальными глобальными правами *Инспектор* в системе Indeed AM.

Как работает скрипт

Работа скрипта состоит из нескольких этапов:

1. Скрипт перебирает идентификаторы политик из массива конфигурационного файла *Config.ps1*.
2. С помощью метода `/api/v6/policy/get` запрашивается информация о политике.
3. Из свойства области действия запрашивается информация по настроенным объектам с помощью метода `/api/v6/userCatalog/getObjects`.
4. Из полученных объектов запрашиваются пользователи:
   - С помощью командлета PowerShell `Get-ADGroup` в функции `getUsersCN` файла *Base/AdditionalFunctions/GetUsers.ps1* для группы Active Directory.
   - С помощью командлета PowerShell `Get-ADUser` в функции `getUsersOU` файла *Base/AdditionalFunctions/GetUsers.ps1* для подразделения Active Directory.
5. По полученным пользователям составляется отчет по состоянию аутентификаторов, которые указаны в переменной `AuthForReport` файла *Config.ps1*.
   - С помощью метода `/api/v6/authenticator/findByUserIds` запрашивается информация со всеми внутренними GUID аутентификаторов пользователя.
   - С помощью метода `/api/v6/authenticator/getUserAuth` запрашивается информация по конкретному GUID.
6. С помощью функции `addDataToCSV` файла *Base/AdditionalFunctions/CsvReport.ps1* собирается таблица в формате CSV.

Настройка

Для работы скрипта необходимо сконфигурировать файл *Config.ps1*, который находится в корне папки со скриптом.

В файле:

- `$serverUrl` — URL сервера Indeed AM. Обязательный параметр.
- `$logsOnFile` — включение\отключение логирования в файл. Обязательный параметр. По умолчанию включено.
- `$logsOnConsole` — включение\отключение логирования в консоль. Обязательный параметр. По умолчанию отключено.
- `$apiVersion` — версия API, используемая в скрипте. Обязательный параметр. Значение по умолчанию: *v6*.
- `$policyIds` — идентификаторы политик, из области действия которых запрашиваются пользователи.
- `$AuthForReport` — в переменной указываются GUID аутентификаторов Indeed и их название для отчета. Название может быть произвольным. Значения указываются в следующем формате: `'GUID' = "Наименование"`.

  Пример настройки для Indeed Key и Passcode

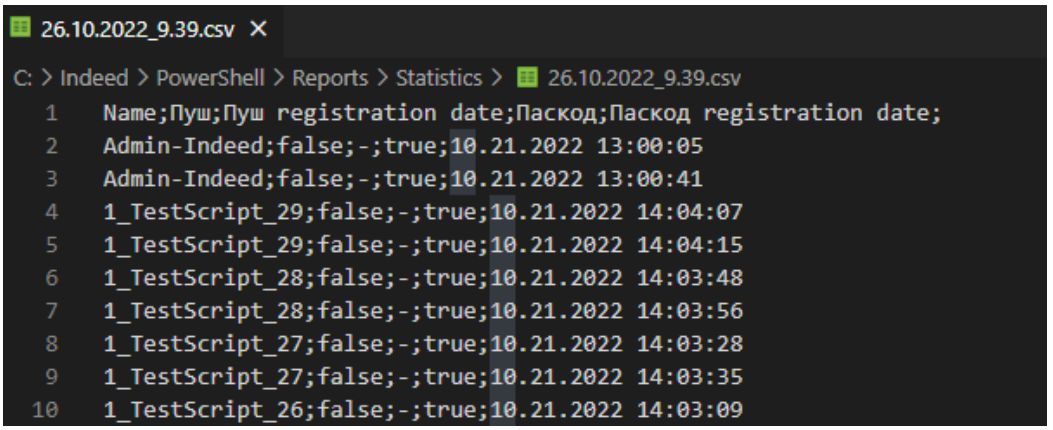
  ```
  $AuthForReport      = @{
      'F696F05D-5466-42b4-BF52-21BEE1CB9529' = 'Passcode'
      'DEEF0CB8-AD2F-4B89-964A-B6C7ECA80C68' = 'Push-уведомление в Indeed Key'
  }
  ```

- `$csvPathToReport` — путь до CSV-файла отчета. По умолчанию файл создается в папке скрипта по пути *Reports\Statistics*.

Пример работы

1. Для запуска скрипта запустите файл *main.ps1*.
2. В процессе работы скрипта по пути из переменной `$csvPathToReport` будет создан файл формата CSV.

> **ПРИМЕЧАНИЕ**
>
> Пользователи добавляются в отчет последовательно.


26.10.2022_9.39.csv
C: > Indeed > PowerShell > Reports > Statistics > 26.10.2022_9.39.csv
1 Name;Пуш;Пуш registration date;Паскод;Паскод registration date;
2 Admin-Indeed;false;-;true;10.21.2022 13:00:05
3 Admin-Indeed;false;-;true;10.21.2022 13:00:41
4 1_TestScript_29;false;-;true;10.21.2022 14:04:07
5 1_TestScript_29;false;-;true;10.21.2022 14:04:15
6 1_TestScript_28;false;-;true;10.21.2022 14:03:48
7 1_TestScript_28;false;-;true;10.21.2022 14:03:56
8 1_TestScript_27;false;-;true;10.21.2022 14:03:28
9 1_TestScript_27;false;-;true;10.21.2022 14:03:35
10 1_TestScript_26;false;-;true;10.21.2022 14:03:09

Получение списка пользователей с лицензиями

> **ИНФОРМАЦИЯ**
>
> Скрипт для получения списка пользователей вы можете скачать по этой ссылке.

Предварительные требования

- Установленный модуль Active Directory для PowerShell в Windows Server.
- Работоспособный сервер Indeed AM.
- Пользователь, от имени которого будет запускаться скрипт, должен обладать минимальными глобальными правами *Инспектор* в системе Indeed AM.

Как работает скрипт

Скрипт формирует таблицу формата CSV со следующими столбцами:

- <UserName>,
- <true>,
- <false>,

где *true\false* — это столбцы с соответствующим названием лицензии.

Массив лицензий, наличие которых проверяется у пользователя, — это список всех зарегистрированных лицензий.

Работа скрипта состоит из нескольких этапов:

1. Формируется массив загруженных в систему лицензий с помощью метода `/license/getAllLicenses`.
2. С помощью метода `/api/v6/policy/get` запрашивается информация о политике.
3. Из свойства области действия запрашивается информация по настроенным объектам с помощью метода `/api/v6/userCatalog/getObjects`.
4. Из полученных объектов запрашиваются пользователи:
   - С помощью командлета PowersShell `Get-ADGroup` в функции `getUsersCN` файла *Base/AdditionalFunctions/GetUsers.ps1* для группы Active Directory.
   - С помощью командлета PowersShell `Get-ADUser` в функции `getUsersOU` файла *Base/AdditionalFunctions/GetUsers.ps1* для подразделения Active Directory.
5. С помощью метода `license/getCatalogObjectLicenses` запрашивается наличие лицензий пользователя и сопоставляется с общим массивом лицензий.

6. С помощью функции `addDataToCSV` файла *Base/AdditionalFunctions/CsvReport.ps1* собирается таблица в формате CSV.

Настройка

Для работы скрипта необходимо сконфигурировать файл *Config.ps1*, который находится в корне папки со скриптом.

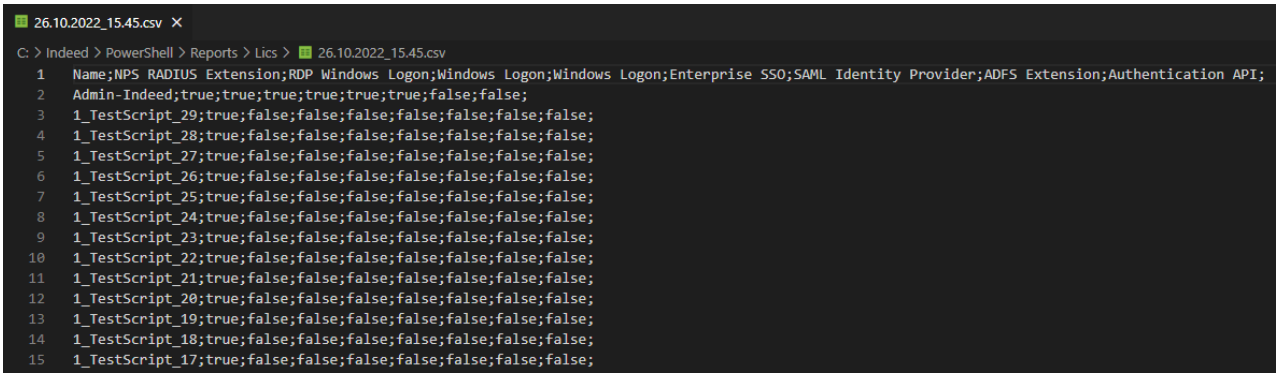
В файле:

- `$serverUrl` — URL сервера Indeed AM. Обязательный параметр.
- `$logsOnFile` — включение\отключение логирования в файл. Обязательный параметр. По умолчанию включено.
- `$logsOnConsole` — включение\отключение логирования в консоль. Обязательный параметр. По умолчанию отключено.
- `$apiVersion` — версия API, используемая в скрипте. Обязательный параметр. Значение по умолчанию: *v5*.
- `$policyIds` — идентификаторы политик, из области действия которых запрашиваются пользователи.
- `$csvPathToReport` — путь до CSV-файла отчета. По умолчанию файл создается в папке скрипта по пути *Reports\Statistics*.

Пример работы

1. Для запуска скрипта запустите файл *main.ps1*.

2. В процессе работы скрипта по пути из переменной `$csvPathToReport` будет создан файл формата CSV.



Двухфакторная аутентификация в API

> **ИНФОРМАЦИЯ**
>
> Скрипт для выполнения двухфакторной аутентификации через API вы можете скачать по этой ссылке.

Как работает скрипт

Скрипт выполняет аутентификацию через стандартное API Core Server. В качестве провайдеров аутентификации поддерживаются провайдеры с одноразовым паролем, Passcode, Windows Password.

Чтобы выполнить аутентификацию через API, выполните следующее:

1. Вызовите метод `/api/v6/templateSession/openVerifySession`. При успешном выполнении метода вернется идентификатор сессии — переменная `$SessionId` в скрипте.

   > **ПРИМЕЧАНИЕ**
   >
   > В качестве примера в скрипте используется формат имени *PrincipalName*.

2. Следующие шаги отличаются в зависимости от используемого провайдера аутентификации:

Если одноразовый код известен

Если одноразовый код известен и его не нужно отправлять, то аутентификация выполняется по следующему алгоритму (функция `SimpleLogon` в скрипте):

1. Запрашивается ввод одноразового кода.
2. Подготовка шаблона аутентификации — вызывается метод `/api/v6/templateSession/prepareTemplateData`.

В качестве `Data` строкой передается одноразовый код (строка №12 в скрипте). Если подготовка прошла успешно, то создается шаблон, вызывается метод `/api/v6/templateSession/createTemplate`.

Завершающий шаг — это аутентификация пользователя с помощью метода `/api/v6/logon/authenticate`.

При успешной аутентификации возвращается токен в формате JSON.

Если одноразовый код не известен

Если одноразовый код не известен, то сначала нужно инициировать его отправку с помощью функции `LogonByOtp` в скрипте.

1. Вызовите метод `/api/v6/templateSession/prepareTemplateData`. Первоначально в качестве `Data` передается значение *Null*.

   Первый вызов необходим для того, чтобы сервер выполнил отправку одноразового кода, например отправку СМС. Также при первоначальном запросе значение параметра `EnoughData` будет содержать *false*.

2. Запрашивается ввод одноразового кода.

3. Подготовка шаблона аутентификации — вызывается метод `/api/v6/templateSession/prepareTemplateData`.

В качестве `Data` строкой передается одноразовый код (строка №12 в скрипте). Запрос вернет объект, где значение параметра `EnoughData` будет содержать *true*. Если подготовка прошла успешно, то создается шаблон, вызывается метод `/api/v6/templateSession/createTemplate`.

Завершающий шаг — это аутентификация пользователя с помощью метода `/api/v6/logon/authenticate`. При успешной аутентификации возвращается токен в формате JSON.

Предварительные требования

- работоспособный сервер Indeed AM,
- наличие лицензии *Authentication API*.

Настройка

Для работы скрипта необходимо сконфигурировать *файл Config.ps1*, который находится в корне папки со скриптом.

`$serverUrl` — URL сервера Indeed AM. Обязательный параметр. `$logsOnFile` — включение\отключение логирования в файл. Обязательный параметр. По умолчанию включено. `$logsOnConsole` — включение\отключение логирования в консоль. Обязательный параметр. По умолчанию отключено. `$apiVersion` — версия API, используемая в скрипте. Обязательный параметр. Значение по умолчанию — *v6*.

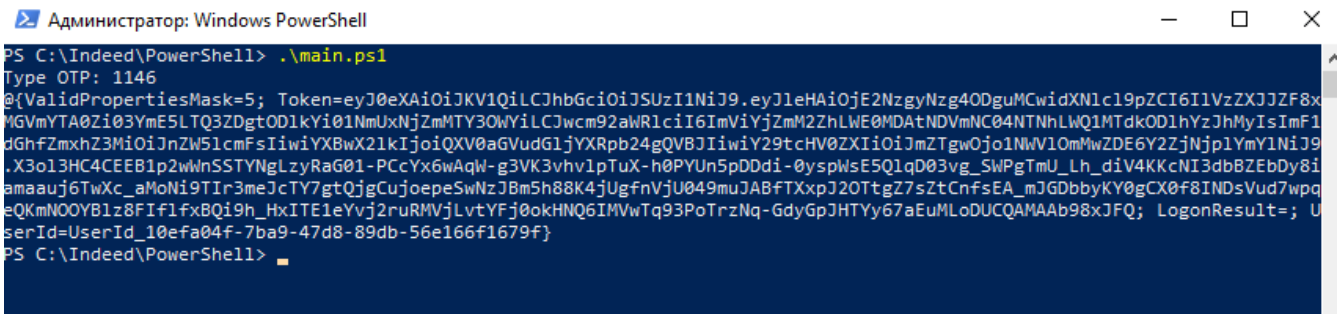
В основном файле *main.ps1* выполните следующее:

1. В параметре `$ProviderGuid` укажите GUID провайдера аутентификации, который будет использоваться в скрипте.

   В качестве примера в скрипте используется идентификатор провайдера Indeed AM SMS OTP Provider — {EBB6F3FA-A400-45F4-853A-D517D89AC2A3}.

2. В параметре `$UserName` укажите имя пользователя в формате UPN.

Пример работы



Удаление пользователей из политики

> **ИНФОРМАЦИЯ**
>
> Скрипт для сбора статистики вы можете скачать по этой ссылке.

Предварительные требования

- Работоспособный сервер Indeed AM.
- Наличие лицензии Authentication API.

Как работает скрипт

Скрипт удаляет пользователя из указанной политики, используя стандартное API Indeed AM Core.

Настройка

Параметр	За что отвечает	Требование	Настройки по умолчанию
$serverUrl	Содержит URL сервера Indeed AM	Обязательный параметр	Отсутствуют
$logsOnFile	Включение\отключение логирования в файл	Обязательный параметр	По умолчанию включено
$logsOnConsole	Включение\отключение логирования в консоль	Обязательный параметр	По умолчанию отключено
$apiVersion	Версия API, используемая в скрипте	Обязательный параметр	Значение по умолчанию — v6

Пример работы

1. Запустите скрипт *main.ps1*.
2. Введите имя пользователя в формате *UPN*. Сформируется список номеров всех политик, в которые входит пользователь.
3. Введите номера политик, из которых вы хотите удалить пользователя, через запятую (или укажите только одну политику).

Пример

```
Enter UPN: Admin-Indeed@indeed.local
User is in scope of the following policies:
0. Radius
1. Main
2. WL + ESSO
Choose policies to remove user from (e.g. 0,1,2): 0,2
User successfully removed from Radius
User successfully removed from WL + ESSO
```

Получение списка пользователей из политики

> **ИНФОРМАЦИЯ**
>
> Скрипт для получения списка пользователей из политики Indeed вы можете скачать по этой ссылке.

Предварительные требования

- Установленный модуль Active Directory для PowerShell в Windows Server.
- Работоспособный сервер Indeed AM.
- Пользователь, от имени которого будет запускаться скрипт, должен обладать минимальными глобальными правами *Инспектор*.

Как работает скрипт

Скрипт выгружает список пользователей из указанной политики в формате CSV. Выгружаются атрибуты пользователя *UserPrincipalName* и *displayName*.

1. Скрипт перебирает идентификаторы политик из массива конфигурационного файла *Config.ps1*.
2. С помощью метода `/api/v6/policy/get` запрашивается информация о политике.
3. Из свойства области действия запрашивается информация по настроенным объектам с помощью метода `/api/v6/userCatalog/getObjects`.
4. Из полученных объектов запрашиваются пользователи:
   - С помощью командлета `Get-ADGroup` в функции `getUsersCN` файла *Base/AdditionalFunctions/GetUsers.ps1* для группы Active Directory.
   - С помощью командлета `Get-ADUser` в функции `getUsersOU` файла *Base/AdditionalFunctions/GetUsers.ps1* для подразделения Active Directory.
   - С помощью командлета `Get-ADUser` в функции `getADUser` файла *Base/AdditionalFunctions/GetUsers.ps1* для пользователя Active Directory.
5. С помощью функции `addDataForUserInPolicyReportCsv` файла *Scenarios/Reports/CsvReport.ps1* собирается таблица в формате CSV.

Настройка

1. В файле *Config.ps1* в переменной `$serverUrl` укажите адрес Indeed AM сервера в формате `https://indeedam.indeed.local/`.
2. В переменной `$logServerUrl` укажите адрес Log Server в формате `https://indeedam.indeed.local/`.

3. В переменной `$policyIds` укажите идентификатор целевой политики в формате *@('2fc7eeec-5adf-4a50-bad3-ba04585c76cd')*. Можно указать несколько через запятую *@('2fc7eeec-5adf-4a50-bad3-ba04585c76cd','7436daa7-abf7-437b-991f-0e89cc9f1b9b')*.

> **СОВЕТ**
>
> Вы можете найти идентификатор политики в Management Console. Откройте нужную политику, идентификатор содержится в адресной строке браузера в переменной `policyId`.

Файл с выгруженными пользователями сохраняется в каталоге *$ScriptDirectory\Reports\UserInPolicyReport*. Если вы хотите сохранить файл в другом месте, укажите путь в переменной `$pathReportUserInPolicyReport` в файле *Config.ps1*.

Чтобы запустить скрипт, выполните файл *Start.ps1* с помощью PowerShell.

Миграция с Indeed AM 8.2.x на Indeed AM 9.x

Миграция с Microsoft SQL на PostgreSQL

Утилита для переноса данных компонента Log Server

Подключение базы данных Core Server на Windows Server к Linux

Подключение данных компонента Core Server

Валидация Passcode

Утилита для валидации Passcode

Особенности миграции

Известные проблемы при миграции

Миграция с Microsoft SQL на PostgreSQL

Миграция базы данных Log Server

Чтобы перенести данные компонента Log Server, выполните следующие действия:

1. Остановите работу Log Server.
2. Создайте эталонную схему базы данных в PostgreSQL.
3. Перенесите данные с помощью утилиты *pgLoader*.
4. Задайте значение последовательности после переноса данных.
5. Установите и запустите новую версию LogServer.

Остановка работы Log Server

1. Откройте Консоль управления IIS с помощью комбинации клавиш Win+R и ввода *inetmgr*.
2. В разделе Подключения выберите Пулы приложений.
3. Нажмите Indeed.LS и выберите Остановить.

> **ПРИМЕЧАНИЕ**
>
> Прежде чем продолжить, рекомендуется сделать резервные копии *C:\inetpub\wwwroot\ls\clientApps.config* и *C:\inetpub\wwwroot\ls\targetConfigs*.

Эталонная схема базы данных

1. Подключитесь к базе данных PostgreSQL и создайте пустую базу данных с необходимыми правами доступа.
2. Создайте схему базы данных с помощью скрипта *LogService_9.5.0_pg_int_db.sql*.

Миграция данных

Чтобы перенести данные, используйте *pgLoader* — инструмент загрузки данных для PostgreSQL.

1. Загрузите *pgLoader* с помощью Docker:

```
docker pull ghcr.io/<user>/pgloader:latest
```

2. Подготовьте конфигурационный файл с расширением *migrate.pgloader* со следующим содержимым.

Пример migrate.pgloader

```
load database
   from mssql://user:password@localhost:1433/LogDB
   into postgresql://user:password@localhost:5432/am_logs

excluding table names like '__MigrationHistory' in schema 'dbo'

set mssql parameters textsize to '104857600'

alter schema 'dbo' rename to 'public'

with prefetch rows = 1000, include no drop, data only, quote identifiers

set work_mem to '16MB', maintenance_work_mem to '512 MB', timezone to 'UTC';
```

Параметр	Описание
`load database from ... into ...`	Команда для копирования данных из одной базы данных в другую.
`excluding table names like '__MigrationHistory' in schema 'dbo'`	Параметр исключает копирование таблицы с миграциями.
`set mssql parameters textsize to`	Увеличение максимальной длины переносимых строк с 2048 до максимального значения.
`alter schema 'dbo' rename to 'public'`	Переименование схемы, так как в Microsoft SQL схема по умолчанию — dbo, а в PostgreSQL — public.
`prefetch rows`	Ограничение количества строк, которые выгружаются в память для последующей обработки. Значение по умолчанию `100000`.
`include no drop, data only`	Копирование только данных, без изменения схемы в целевой базе данных.
`quote identifiers`	Имена идентификаторов заключаются в кавычки (имена таблиц и столбцов).

`work_mem`	Объем оперативной памяти, выделяемой для выполнения операций сортировки и хеширования в запросах.
`maintenance_work_mem`	Объем памяти, выделяемой для операций обслуживания, таких как создание индексов, клонирование таблиц, миграция больших объемов данных.
`timezone to 'UTC'`	Формат времени. Рекомендуется использовать значение по умолчанию — `UTC`.

3. Запустите процесс копирования с помощью утилиты *pgloader* для Linux или Windows.

Linux

1. Создайте каталог *pgloader* и добавьте в него файл *docker-compose.yml* со следующим содержимым:

```
version: "3.8"

services:
  pgloader:
    container_name: pgloader_container
    image: ghcr.io/dimitri/pgloader:latest
    entrypoint: "pgloader /etc/pgloader/migrate.pgloader"
    network_mode: "host"
    volumes:
      - ./config:/etc/pgloader
```

2. Создайте каталог *pgloader/config* и перенесите в него конфигурационный файл *migrate.pgloader*.

Структура файлов

```
pgloader/
  config/
    migrate.pgloader
  docker-compose.yml
```

3. Из каталога *pgloader* выполните команду `docker-compose up`.

Windows

Выполните команду:

```
docker run --rm --network="host" -v "C:\pgloader:/data"
ghcr.io/dimitri/pgloader:latest pgloader /data/migrate.pgloader --dynamic-
space-size 2048
```

Где:

- `"C:\pgloader:/data"` — том Docker, в котором хранится конфигурационный файл *migrate.pgloader*.
- `/data/migrate.pgloader` — название конфигурационного файла *migrate.pgloader*.
- `--dynamic-space-size 2048` — параметр, задающий максимальный размер оперативной памяти в мегабайтах (Мб). Значение по умолчанию 1024. Этот параметр работает в комбинации с параметром `prefetch rows` и другими параметрами обработки пакетов. Чтобы утилита `pgLoader` успевала очищать память при переносе данных, необходимо уменьшить размер пакета и увеличить максимальный лимит.

Обновление последовательностей

После переноса данных необходимо задать значение последовательности `EventAttributeEntities_Id_seq`. Эта последовательность отвечает за заполнение первичного ключа в таблице `EventAttributeEntities`. По умолчанию значение последовательности равно `1`.

Установите максимальное значение на основе текущих данных, чтобы избежать конфликтов. Выполните следующий запрос `Update_seq.sql`:

```
select setval(quote_ident('EventAttributeEntities_Id_seq'), (select max("Id") from
"EventAttributeEntities"));
```

Результат: функция установит и выведет текущее значение, которое должно быть больше или равно количеству записей в таблице `EventAttributeEntities`.

Установка и запуск новой версии Log Server

1. После успешной миграции установите актуальную версию Log Server.
2. В конфигурационном файле *am/ls/targets/DbTargetSqlAM.config* укажите настройки подключения к базе данных PostgreSQL.
3. Выполните запуск контейнера ls с помощью команды `docker-compose up`.

4. Выполните POST-запрос на чтение данных:

```
curl -X 'POST' \
  'https://localhost/ls/api/ReadLogs' \
  -H 'accept: text/plain' \
  -H 'Content-Type: application/json' \
  -d '{
  "applicationName": "ea",
  "request": {
    "filters": [
    ],
    "startFrom": 0,
    "take": 1,
    "sortBy": "Name",
    "sortDesc": false
  }
}'
```

Результат: получен ответ с кодом 200 и первой записью из таблицы логов.

Миграция базы данных Core Server

Чтобы перенести данные компонента Core Server, выполните следующие действия:

1. Создайте эталонную базу данных в PostgreSQL.
2. Перенесите данные с помощью утилиты *psql*.

Для миграции используйте утилиту *psql* для Linux или *psql.exe* для Windows. Утилита поставляется с дистрибутивами PostgreSQL или pgAdmin.

Эталонная схема базы данных

1. Подключитесь к базе данных PostgreSQL и создайте новую базу данных:

```
psql -h <host_address> -U postgres -W
create database <db_name>;
```

Где `<host_address>` — это адрес хоста с PostgreSQL.

Чтобы выйти из *psql*, используйте команду:

```
\q
```

2. Запустите скрипт для установки схемы базы данных *sql/schema_v.0.0_clean.sql*:

```
psql -h <host_address> -U postgres -d <db_name> -f sql/schema_v.0.0_clean.sql
```

> **ПРИМЕЧАНИЕ**
>
> Имя пользователя по умолчанию — *postgres*. Если имя пользователя в вашей системе отличается, после выполнения скрипта откройте файл *sql/schema_v.0.0_clean.sql* и найдите строку `/set DatabaseOwner 'user_name'`. В параметре `user_name` укажите корректное имя пользователя.

Миграция данных

Чтобы перенести данные, используйте *pgLoader* — инструмент загрузки данных для PostgreSQL.

1. Загрузите *pgLoader* с помощью Docker:

```
docker pull ghcr.io/<user>/pgloader:latest
```

2. В файле *config/ms.load* укажите строки подключения для Microsoft SQL и PostgreSQL:

```
load database
  from mssql://{user}:{password}@{host}:{port}/{database}
  into pgsql://{user}:{password}@{host}:{port}/{database}
```

> **Пример config/ms.load**
>
> ```
> load database
>    from mssql://user:password@localhost:1433/Core_DB
>    into postgresql://user:password@localhost:5432/am_logs
> ```

3. Чтобы выполнить миграцию данных, запустите утилиту *pgloader* в Docker:

```
docker-compose up
```

4. Запустите скрипт для применения изменений:

```
psql -h <host_address> -U postgres -d <db_name> -f sql/datafix.sql
```

Подключение базы данных Core Server на Windows Server к Linux

Чтобы подключить базу данных Core Server из AM 8 к AM 9, выполните следующие действия:

1. Обновите Access Manager до версии 8.2.8.
2. Подготовьте целевой хост: установите и запустите компоненты Access Manager 9.
3. Выполните валидацию Passcode, если в версии Access Manager 8.2.8 используется Windows Logon или RDP Windows Logon.

Подготовка целевого хоста

> **ПРИМЕЧАНИЕ**
>
> Прежде чем продолжить, рекомендуется сделать резервные копии базы данных Core Server.

Подготовьте целевой хост:

1. Установите и настройте Docker. Системные требования
2. Настройте сетевое взаимодействие с базой данных.
3. Установите Access Manager 9 на новом хосте.

   > **ПРИМЕЧАНИЕ**
   >
   > При настройке Core Server в конфигурационном файле *am/core/app-settings.json* укажите параметры базы данных из AM 8.2.8.

4. Запустите компоненты Access Manager 9 на подготовленном хосте:

   ```
   sudo docker-compose up -d
   ```

   База данных автоматически обновит структуру и будет готова к работе.

Валидация Passcode

Перед началом процедуры миграции с Access Manager 8.2.x на Access Manager 9.x рекомендуется выполнить валидацию Passcode, если в версии Access Manager 8.2.x используется Windows Logon или RDP Windows Logon. Процесс валидации Passcode обеспечивает корректность и целостность данных и позволяет избежать ошибок преобразования данных из бинарного формата.

Чтобы обеспечить консистентность данных и гарантировать успешное функционирование аутентификации с помощью провайдера Passcode в Access Manager 9.2, используйте утилиту *AccessManager.Tools.Passcode.Services.Console.exe*.

Настройки на стороне Access Manager 9.2

Перед использованием утилиты *AccessManager.Tools.Passcode.Services.Console.exe* необходимо выполнить следующее:

1. Выполните установку и настройку серверных компонентов Access Manager 9.2.

   > ⚠ **ВАЖНО**
   >
   > При настройке компонента Core Server, укажите строку подключения к базе данных от Access Manager 8.2.x.

2. Для компонента Core Server включите логирование с уровнем `Error`.

3. Откройте файл *am/core/app-settings.json* и убедитесь, что следующий параметр задан корректно:

   ```
   "PlatformCompatibility": {
     "Registry": {
       "Source": "PlatformOrFile",
       "File": "server-registry.json"
     }
     }
   ```

   Где файл *server-registry.json* — эмулятор реестра в Access Manager 9.2.

4. Внесите изменения в файл *am/core/server-registry.json*:

   - `LogPasscodeDeserializationError` — включает и выключает логирование ошибочных данных (pickle) для Passcode. Возможные значения: `"1"` и `"0"`.
   - `LogPasscodeEncryptionPublicKey` — публичный ключ шифрования ошибочных данных (pickle) для Passcode. Не изменяйте этот параметр.

- `NativePasscodeValidationEnabled` — включает и выключает режим валидации нативных данных (pickle) для Passcode. Возможные значения: `"1"` и `"0"`.
- `NativePasscodeValidationSecret` — секрет, который передается утилитой валидации. Сгенерируйте его в виде случайного набора латинских букв и цифр длиной от 1 до 30 символов без использования специальных символов. Этот секрет нужен для дополнительной защиты режима валидации Passcode.
- `NativePasscodeValidationCoreApiUrl` — URL-адрес компонента Core Server версии Access Manager 8.2.x.

Пример

```
{
 "KeyName": "HKEY_LOCAL_MACHINE\\SOFTWARE\\Policies\\Indeed-Id\\BSPs\\Passcode",
 "ValueName": "LogPasscodeDeserializationError",
 "StringValue": "1"
},
{
 "KeyName": "HKEY_LOCAL_MACHINE\\SOFTWARE\\Policies\\Indeed-Id\\BSPs\\Passcode",
 "ValueName": "LogPasscodeEncryptionPublicKey",
 "StringValue": "<RSAKeyValue>
<Modulus>ySDCRwBj5NbWGtZ8YgNbWzjTZfFB9UeSXAKHz2qwk4Q/iJJJ5FYB622s5MAZH5BI7s+npm272
</Modulus><Exponent>AQAB</Exponent></RSAKeyValue>"
},
{
 "KeyName": "HKEY_LOCAL_MACHINE\\SOFTWARE\\Policies\\Indeed-Id\\BSPs\\Passcode",
 "ValueName": "NativePasscodeValidationEnabled",
 "StringValue": "1"
},
{
 "KeyName": "HKEY_LOCAL_MACHINE\\SOFTWARE\\Policies\\Indeed-Id\\BSPs\\Passcode",
 "ValueName": "NativePasscodeValidationSecret",
 "StringValue": "somesecretindid"
},
{
 "KeyName": "HKEY_LOCAL_MACHINE\\SOFTWARE\\Policies\\Indeed-Id\\BSPs\\Passcode",
 "ValueName": "NativePasscodeValidationCoreApiUrl",
 "StringValue": "http(s)://app8.ind.my/am/core"
}
```

Запуск утилиты валидации Passcode

Чтобы выполнить валидацию Passcode, необходимо на стороне Access Manager 8.2.x открыть терминал и запустить утилиту валидации *AccessManager.Tools.Passcode.Services.Console.exe* со следующими командами и параметрами.

Шаг 1. `export-users` — определяет список пользователей, для которых требуется валидация Passcode.

Шаг 2. `validate-users-passcode` — производит валидацию Passcode на основании списка пользователей.

Глобальные параметры

В следующей таблице приведены глобальные параметры, которые можно задать при выполнении команд `export-users` и `validate-users-passcode`. У пользователя должно быть достаточно прав для изменения необходимых файлов.

• `--server-url` • `--url`	Обязательный параметр. URL-адрес Core Server версии Access Manager 9.2. Пример: http(s)://access-manager-server-url/am/core.
• `--client-certificate` • `--certificate` • `--cert`	Отпечаток клиентского сертификата. Если параметр не задан, используется встроенный сертификат. Пример: `"client-certificate-thumbprint"`.
• `--client-certificate-location` • `--certificate-location` • `--cert-location`	Расположение хранилища клиентских сертификатов. Значение по умолчанию: `CurrentUser`.
• `--log-level` • `--log`	Уровень логирования. Возможные значения: `Trace`, `Debug`, `Info` (по умолчанию), `Warn`, `Error`, `Fatal`, `Off`.

Экспорт пользователей

Чтобы выполнить экспорт пользователей, для которых необходимо выполнить валидацию, запустите утилиту *AccessManager.Tools.Passcode.Services.Console.exe* с командой `export-users` и необходимыми параметрами. Все параметры приведены в следующей таблице. Также можно добавить любые глобальные параметры.

> **ПРИМЕЧАНИЕ**
>
> Список пользователей формируется на основе привязанных к ним лицензий для указанных приложений (параметр `--application` или `--app`). Можно указать несколько приложений.

Пример команды для экспорта пользователей

```
AccessManager.Tools.Passcode.Services.Console.exe export-users --out
c:\path\to\file.txt --overwrite true --app "Windows Logon" --u domain\\globaladmin -
-limit 10000 --url http://<AM_CORE_URL>/am/core --log Trace
```

Параметры для команды `export-users`

• `--output` • `--out` • `--o`	Обязательный параметр. Имя файла, в который будет записан результат экспорта. Можно указать полный путь файла, относительный путь файла или имя файла. Имя файла можно указать без расширения.
• `--allow-overwrite-output` • `--allow-overwrite` • `--overwrite`	Позволяет перезаписывать файл. Значение по умолчанию `false`.
• `--application` • `--app`	Обязательный параметр. Приложение, на основе которого осуществляется выгрузка. Можно указать несколько приложений, например `--app "Windows Logon"` `--app "Enterprise SSO"`.
• `--user` • `--u`	Логин глобального администратора Access Manager, который осуществляет выгрузку. Если логин не указан, то в среде Windows будет использоваться аутентификация Windows (если настроена). Если логин указан, то будет запрошен Windows-пароль. Логин можно указывать в формате `PrincipalName` (*user@domain.local*) или `SamCompatibleName` (*domain\user*).
• `--limit`	Ограничение количества выгружаемых пользователей. Применяется, если задано значение больше нуля. Значение по умолчанию `0` (безлимитно).

Валидация Passcode

Чтобы начать валидацию Passcode на основе списка экспортированных пользователей, запустите утилиту с командой `validate-users-passcode` и задайте один из следующих параметров. Также можно добавить любые глобальные параметры.

Пример команды для валидации Passcode

```
AccessManager.Tools.Passcode.Services.Console.exe validate-users-passcode --from
c:\path\to\export.txt --url http://<AM_CORE_URL>/am/core --log Trace
```

Параметры для команды `validate-users-passcode`

• `--import-location` • `--from`	Путь, по которому находится файл с ранее экспортированными пользователями. Файл можно редактировать.

После запуска валидации запрашивается значение параметра *NativePasscodeValidationSecret*, которое вы задали ранее в файле *server-registry.json* на стороне Access Manager 9.2.

При успешной валидации Passcode на стороне Access Manager 8.2.x в Log Server записываются события об успешной аутентификации по Passcode, а на стороне Access Manager 9.2 записываются ошибки входа.

Сбор логов

На стороне Access Manager 9.2 результат валидации хранится в файле *NativePasscodeValidator.<guid>.txt*, который находится в логах компонента Core Server. При наличии ошибок в файле *NativePasscodeValidator.<guid>.txt* обратитесь в службу технической поддержки support@indeed-id.com.

Пример ошибки

```
2025-02-26 16:18:46.7999|0HNAM9VAJ2LCI:00000002|0|ERROR|,4e68816e-e33b-4281-
8719-4c0b774b4c53,ActiveDirectory_d5d11f1b-a87f-4ca0-bab1-4c3bcf5743b0,unknown
type: System.Byte[],error_pickle_parsing,Error message: Pickle can't be parsed:
unmatched: range N0(0, 44), @0, 1!=3,  hr -2147024883,...
```

Пример валидации без ошибок

```
2025-02-28 09:50:28.5360|0HNANOJULLERO:00000002|0|ERROR|,188fef22-eb79-4105-
a2e1-4fb9b3c19471,a406f_186dc38a-403f-4054-9aca-
731f3216d6f0,string_passcode,skipped,,
2025-02-28 09:50:28.9423|0HNANOJULLERO:00000002|0|ERROR|,188fef22-eb79-4105-
a2e1-4fb9b3c19471,a406f_186dc38a-403f-4054-9aca-
731f3216d6f0,bin_sha1_passcode,success,(null),(null)
2025-02-28 09:50:28.9423|0HNANOJULLERO:00000002|0|ERROR|,188fef22-eb79-4105-
a2e1-4fb9b3c19471,a406f_186dc38a-403f-4054-9aca-
731f3216d6f0,string_passcode,skipped,,
2025-02-28 09:50:29.2444|0HNANOJULLERO:00000002|0|ERROR|,188fef22-eb79-4105-
a2e1-4fb9b3c19471,a406f_186dc38a-403f-4054-9aca-
731f3216d6f0,bin_passcode,success,(null),(null)
2025-02-28 09:50:29.8941|0HNANOJULLERT:00000002|0|ERROR|,188fef22-eb79-4105-
a2e1-4fb9b3c19471,a406f_f688dd25-349f-42c5-afd5-
9f2e50b15f0f,bin_passcode,success,(null),(null)
```

Особенности миграции

После миграции с Indeed AM 8.2.x на Indeed AM 9.x могут наблюдаться следующие ограничения::

- При выгрузке логов отдельным архивом с помощью утилиты `GetLog` без указания альтернативного пути может возникнуть ошибка.

  Чтобы этого избежать, добавьте параметр `--o`, `--output` или `--path` с указанием директории, куда нужно сохранить архив.

  Пример

  ```
  GetLog --archive --output ~/Downloads/
  ```

- При импорте собственного клиентского сертификата *am/tools/certName.pfx*, сгенерированного через скрипт *tool_gen_client_cert.sh*, может возникнуть ошибка пароля в мастере импорта сертификатов на Windows Server 2016.

  Импорт работает без ошибок с Window Server 2019 и выше.

- Модуль FreeRADIUS поддерживает работу только по протоколу Password Authentication Protocol (PAP).

Решение проблем

Сбор программных логов

Логи ADFS Extension, RDP Windows Logon и Windows Logon

Сбор логов компонентов Access Manager

Логи серверных и модульных компонентов

Настройка событий Syslog

Настройка записи атрибутов событий Syslog

База знаний

Часто задаваемые вопросы и их решения

Техническая поддержка

Как создать обращение в поддержку

Сбор программных логов

Приложение Indeed AM GetLog предназначено для локального и удаленного сбора программных логов следующих компонентов:

- RDP Windows Logon,
- Windows Logon.

Подключение к компьютеру

Чтобы подключиться к компьютеру, логи которого нужно получить:

1. Запустите утилиту GetLog от имени локального администратора. Файл запуска расположен в *Indeed AM <номер версии>\logging\IndeedAM.GetLog.exe*.
2. В поле Computer введите имя или IP-адрес удаленного компьютера. Чтобы подключиться к локальному компьютеру, введите *localhost* или *127.0.0.1*.
3. Нажмите Connect. После установки соединения станут доступны:

- кнопка включения/отключения логов Enable Log/Disable Log;
- кнопка получения логов Get Log;
- кнопка перехода к дополнительным настройкам Advanced Settings;
- кнопка отключения Disconnect.

> **ПОДСКАЗКА**
>
> Чтобы подключиться к удаленному компьютеру под управлением Windows 7 и выше, убедитесь в том, что на удаленном компьютере запущена и не заблокирована служба Инструментарий управления Windows (WMI) (Windows Management Instrumentation).

Основные действия

Работа с утилитой

Чтобы включить или отключить логирование и получить логи:

1. Подключитесь к компьютеру.
2. Для включения записи логов нажмите Enable Log.
3. Если сбор логов требуется для выявления причин проблемной ситуации, выполните действия для воспроизведения проблемы.
4. Для отключения записи логов нажмите Disable Log.
5. Для получения логов нажмите Get Log....

6. Укажите каталог для сохранения ZIP-архива и нажмите Сохранить.
7. Для отключения от компьютера нажмите Disconnect и закройте приложение.

Работа с реестром

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, чтобы отключить логирование;
- 1, чтобы включить логирование.

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.

Дополнительные настройки

Настройки в утилите

Чтобы перейти к дополнительным настройкам, нажмите Advanced Settings в главном окне Indeed AM GetLog. В окне Advanced Settings доступны следующие 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 компонентов Access Manager

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

Trace	Наиболее подробный уровень. Логи с уровнем Trace содержат всю информацию о процессах работы компонента, включая детали о вызовах методов API.
Debug	При этом уровне логирования записи содержат подробности о ходе работы компонента, значимые переменные и другие данные, которые могут быть полезными при обнаружении и исправлении ошибок.
Info	При этом уровне логирования записываются информационные сообщения, которые уведомляют о нормальном функционировании компонента. Они могут включать такие события, как запуск или завершение процессов, отправка почты, редактирование профиля пользователя и другие.
Warn	Логирование этого уровня используется, чтобы записывать предупреждения и уведомления о потенциальных ошибках и внештатных ситуациях. События не являются критическими, но требуют внимания. При этом компонент может продолжать работу.
Error	Уровень логирования, используемый для записи ошибок, повлекших за собой некорректную работу компонента или возникновение серьезных проблем. Логи с уровнем Error указывают на проблемы, которые требуют вмешательства и исправления.
Fatal	Наименее подробный уровень логирования. Если задан этот уровень, будут записываться только самые критические ошибки и проблемы, которые приводят к немедленному завершению работы компонента или другим серьезным последствиям. Логи с уровнем Fatal обычно означают серьезные сбои, которые требуют немедленного вмешательства и исправления.

Core Server

Включение логирования

1. Откройте с правами администратора файл *am/core/nlog.config*.
2. Для тегов `logger` в параметре `minlevel` установите значение `Trace`, в параметре `enabled` установите `true`.

   Пример

```
<rules>
  <logger name="*" writeTo="defaultFile" minlevel="Warn" enabled="true">
    <filters defaultAction="Log">
      <when condition="equals('${logger}','metricTime')" action="Ignore" />
      <when condition="equals('${logger}','metricInfo')" action="Ignore" />
    </filters>
  </logger>
  <logger name="Microsoft.Hosting.Lifetime" writeTo="lifetimeConsole"
final="false" />
  <logger name="metricTime" writeTo="metricsTimeFile" minlevel="Trace"
enabled="false" />
  <logger name="metricInfo" writeTo="metricsInfoFile" minlevel="Trace"
enabled="false" />
</rules>
```

3. Сохраните файл и перезапустите контейнер с приложением.

Сбор логов

1. Очистите существующие логи сервера Indeed AM в каталоге *am/core/Logs/<текущая_дата>*.
2. Воспроизведите проблему.
3. Соберите архив с логами и отправьте в поддержку с подробным описанием действий пользователя и указанием точного времени воспроизведения проблемы.

Log Server

Включение логирования

1. Откройте с правами администратора файл *am/ls/app-settings.json*.
2. Для тега `NLog` в параметрах `minLevel` и `dbMinLevel` установите значение `Trace`. В параметре `enabled` установите значение `true`.

   Пример

```
"NLog": {
"variables": {
  "minLevel": "Trace",
  "dbMinLevel": "Trace"
},
"rules": {
  "20_Errors": {
    "logger": "*",
    "minLevel": "Error",
    "writeTo": "errorsFile",
    "enabled":  true
  },
  "47_Db": {
    "logger": "Microsoft.EntityFrameworkCore*",
    "minLevel": "${dbMinLevel}",
    "writeTo": "dbFile",
    "enabled":  true
  },
  "52_Full": {
    "logger": "*",
    "minLevel": "${minLevel}",
    "writeTo": "fullFile",
    "enabled":  true
  }
}
```

- `20_Errors` — запись ошибок в файл *errors.log*;
- `47_Db` — запись событий, относящихся к базе данных (например соединение), в соответствии с уровнем логирования в параметре `"variables":"minLevel"`;
- `52_Full` — запись всех событий в соответствии с уровнем логирования в параметре `"variables":"minLevel"`.

3. Сохраните файл и перезапустите контейнер с приложением.

Сбор логов

1. Очистите существующие логи Indeed AM Log Server в каталоге *am/ls/Logs/<текущая_дата>*.
2. Воспроизведите проблему.
3. Соберите архив с логами и отправьте в поддержку с подробным описанием действий пользователя и указанием точного времени воспроизведения проблемы.

Management Console

Включение логирования

1. Откройте с правами администратора файл *am/mc/nlog.config*.
2. Для тега `logger` в параметре `minlevel` установите значение `Trace`, в параметре `enabled` установите `true`.

   Пример

   ```
   <rules>
     <logger name="*" writeTo="defaultFile" minlevel="Trace" enabled="true"/>
   </rules>
   ```

3. Сохраните файл и перезапустите контейнер с приложением.

Сбор логов

1. Очистите существующие логи Indeed AM Management Console в каталоге *am/mc/Logs/<текущая_дата>*.
2. Воспроизведите проблему.
3. Соберите архив с логами и отправьте в поддержку с подробным описанием действий пользователя и указанием точного времени воспроизведения проблемы.

User Console

Включение логирования

1. Откройте с правами администратора файл *am/uc/nlog.config*.
2. Для тега `logger` в параметре `minlevel` установите значение `Trace`, в параметре `enabled` установите `true`.

   Пример

   ```
   <rules>
     <logger name="*" writeTo="defaultFile" minlevel="Trace" enabled="true"/>
   </rules>
   ```

3. Сохраните файл и перезапустите контейнер с приложением.

Сбор логов

1. Очистите существующие логи Indeed AM User Console в каталоге *am/uc/Logs/<текущая_дата>*.

2. Воспроизведите проблему.
3. Соберите архив с логами и отправьте в поддержку с подробным описанием действий пользователя и указанием точного времени воспроизведения проблемы.

Identity Provider

Включение логирования

1. Откройте с правами администратора файл *am/idp/nlog.config*.
2. Для тега `logger` в параметре `minlevel` установите значение `Trace`, в параметре `enabled` установите `true`.

   Пример

   ```
   <rules>
      <logger name="*" writeTo="defaultFile" minlevel="Trace" enabled="true" />
   </rules>
   ```

3. Сохраните файл и перезапустите контейнер с приложением.

Сбор логов

1. Очистите существующие логи Indeed AM Identity Provider в каталоге *am/idp/Logs/<текущая_дата>*.
2. Воспроизведите проблему.
3. Соберите архив с логами и отправьте в поддержку с подробным описанием действий пользователя и указанием точного времени воспроизведения проблемы.

Key Server

Включение логирования

1. Откройте с правами администратора файл *am/indeed-key/nlog.config*.
2. Для тега `logger` в параметре `minlevel` установите значение `Trace`, в параметре `enabled` установите `true`.

   Пример

```
<rules>
  <logger name="*" writeTo="defaultFile" minlevel="Trace" enabled="true">
    <filters defaultAction="Log">
      <when condition="equals('${logger}','metricTime')" action="Ignore" />
      <when condition="equals('${logger}','metricInfo')" action="Ignore" />
    </filters>
  </logger>
  <logger name="Microsoft.Hosting.Lifetime" writeTo="lifetimeConsole"
final="false" />
  <logger name="metricTime" writeTo="metricsTimeFile" minlevel="Trace"
enabled="true" />
  <logger name="metricInfo" writeTo="metricsInfoFile" minlevel="Trace"
enabled="true" />
</rules>
```

3. Сохраните файл и перезапустите контейнер с приложением.

Сбор логов

1. Очистите существующие логи сервера Indeed Key в каталоге *am/indeed-key/Logs/<текущая_дата>*.
2. Воспроизведите проблему.
3. Соберите архив с логами и отправьте в поддержку с подробным описанием действий пользователя и указанием точного времени воспроизведения проблемы.

LDAP Proxy

Включение логирования

1. Откройте с правами администратора файл *am/ldap-proxy/configs/nlog.config*.
2. Для тега `logger` в параметре `minlevel` установите значение `Trace`, в параметре `enabled` установите `true`.

Пример

```
<rules>
   <logger name="*" writeTo="defaultFile" minlevel="Trace" enabled="true" />
</rules>
```

3. Сохраните файл и перезапустите контейнер с приложением.

Сбор логов

1. Очистите существующие логи LDAP Proxy в каталоге *am/ldap-proxy/Logs/<текущая_дата>*.
2. Воспроизведите проблему.
3. Соберите архив с логами и отправьте в поддержку с подробным описанием действий пользователя и указанием точного времени воспроизведения проблемы.

SMS Proxy

Включение логирования

1. Откройте с правами администратора файл *am/sms-proxy/nlog.config*.
2. Для тега `logger` в параметре `minlevel` установите значение `Trace`, в параметре `enabled` установите `true`.

   Пример

   ```
   <rules>
      <logger name="*" writeTo="defaultFile" minlevel="Trace" enabled="true" />
   </rules>
   ```

3. Сохраните файл и перезапустите контейнер с приложением.

Сбор логов

1. Очистите существующие логи SMS Proxy в каталоге *am/sms-proxy/Logs/<текущая_дата>*.
2. Воспроизведите проблему.
3. Соберите архив с логами и отправьте в поддержку с подробным описанием действий пользователя и указанием точного времени воспроизведения проблемы.

Telegram Service

Включение логирования

1. Откройте с правами администратора файл *am/telegram-service/Logs/<текущая_дата>*.
2. Для тега `logger` в параметре `minlevel` установите значение `Trace`, в параметре `enabled` установите `true`.

   Пример

   ```
   <rules>
      <logger name="*" writeTo="defaultFile" minlevel="Trace" enabled="false"/>
   </rules>
   ```

3. Сохраните файл и перезапустите контейнер с приложением.

Сбор логов

1. Очистите существующие логи Telegram Service в каталоге *am/telegram-service/Logs/<текущая_дата>*
2. Воспроизведите проблему.
3. Соберите архив с логами и отправьте в поддержку с подробным описанием действий пользователя и указанием точного времени воспроизведения проблемы.

Настройка событий Syslog

По умолчанию Log Server в Syslog записывает только уникальный идентификатор события — атрибут `reason`. Чтобы записывать дополнительные атрибуты, укажите имена этих атрибутов в файле схемы для соответствующего события.

1. Чтобы найти необходимый файл с событиями Syslog, откройте *am/ls/clientApps.config* и в блоке `Applications` найдите значение параметра `SchemaId`.

   Пример

   ```
   <ApplicationsConfiguration>
     <Applications>
       <Application Id="ea" SchemaId="eaSchema">
       ...
     <Applications>
   ```

2. Откройте для редактирования файл с событиями, например *am/ls/eaSchema.config*, где *eaSchema* — значение параметра `SchemaId`.

3. Найдите необходимое событие и в блоке `Attributes` добавьте значения для атрибутов, которые хотите отображать в событии. Для этого в строке с соответствующим атрибутом добавьте один из следующих параметров с любым значением:

   - для формата CEF — `CefName=""`
   - для формата LEEF — `LeefName=""`

В следующем примере событие `LogonByAuthenticatorSucceeded` записывается с атрибутами: `reason` (по умолчанию), `requestApplication` и `requestComputer`.

Пример для формата CEF

```
    <Event Name="LogonByAuthenticatorSucceeded" Severity="info"
Text="LogonByAuthenticatorSucceededText" Code="1000">
      <Attributes>
        <Attribute Name="requestApplication" Type="string"
CefName="requestApplication"/>
        <Attribute Name="requestUser" Type="string" />
        <Attribute Name="requestComputer" Type="string" CefName="requestComputer"/>
        <Attribute Name="authMode" Type="string" />
        <Attribute Name="authComment" Type="string"/>
        <Attribute Name="businessApplication" Type="string" DefaultValue=""/>
      </Attributes>
    </Event>
```

Пример события по заданным параметрам

```
<134>Nov 7 06:41:58 31f8d1a0234e ea[1]:
CEF:0|Indeed|server|unknown|1000|LogonByAuthenticatorSucceeded|4|reason=164fca53-
8ae9-45f9-ab7e-8f89a4b528c9 requestApplication=RDP Windows Logon
requestComputer=**** businessApplication=
```

База знаний

В базе знаний вы можете найти ответы на часто задаваемые вопросы, познакомиться с примерами внедрения Access Manager с бизнес-приложениями, оставить запрос на доработку, отправить заявку в службу поддержки.

Главы базы знаний разделены по версиям продукта Access Manager:

- Access Manager 9,
- Access Manager 8,
- Access Manager 7,
- Access Manager 6.

Техническая поддержка

Если вы не нашли ответ на ваш вопрос в документации или базе знаний, вы можете обратиться за помощью в службу поддержки.

Если вы обращаетесь в поддержку для решения проблемы, предоставьте как можно больше информации, включая файлы, скриншоты, логи. Это поможет решить проблему оперативно.

Чтобы отправить обращение в поддержку, выполните следующее:

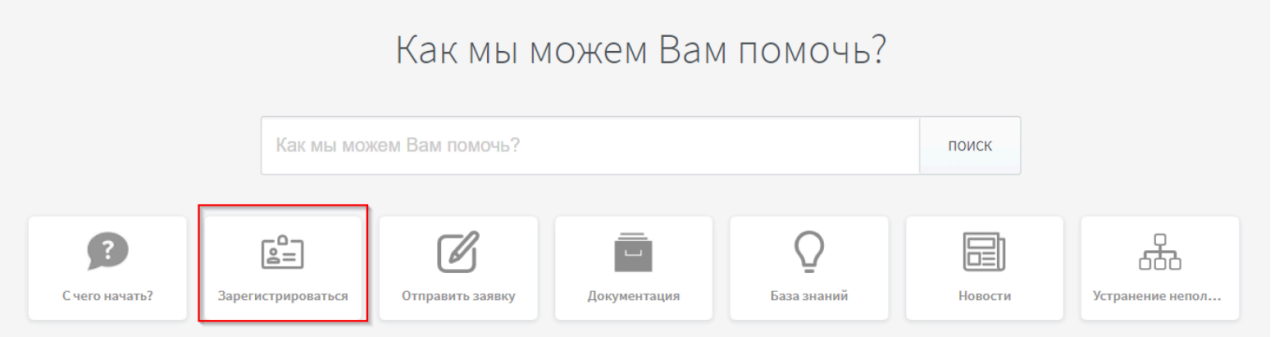
1. Откройте портал технической поддержки.
2. Введите ваш электронный адрес и пароль и нажмите Вход.

Если у вас нет логина и пароля

Вы можете зарегистрироваться на портале поддержки самостоятельно или отправить заявку на регистрацию.

Чтобы зарегистрироваться самостоятельно:

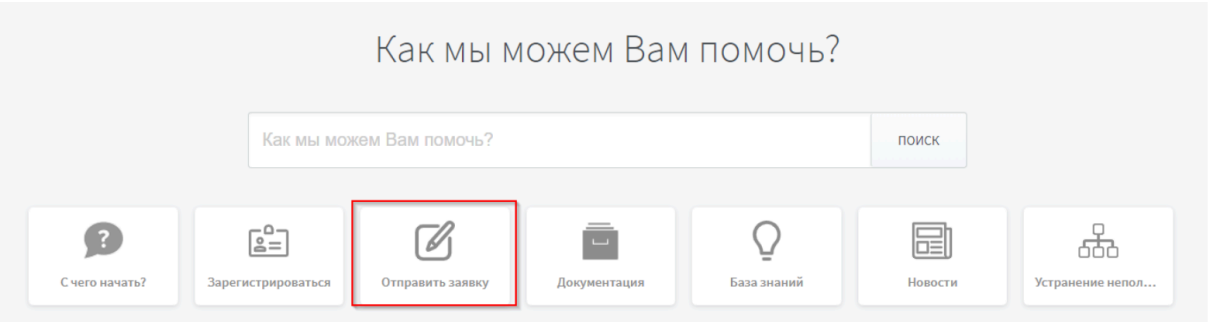
1. Нажмите Зарегистрироваться.



2. Откроется форма регистрации.Заполните поля и нажмите Зарегистрироваться.
3. На указанный электронный адрес вы получите письмо со ссылкой для активации аккаунта. Пройдите по ссылке.

Чтобы отправить заявку на регистрацию

1. Нажмите Отправить заявку.



2. Откроется форма заявки. Укажите, что это заявка на создание учетной записи.
3. На указанный электронный адрес вы получите письмо со ссылкой для активации аккаунта. Пройдите по ссылке.

3. Нажмите Отправить заявку.
4. Выберите департамент и нажмите Вперед.
5. Заполните форму заявки и нажмите Отправить.

Также вы можете связаться с командой поддержки по следующим телефонам:

- 8 800 333 09-06,

- +7 (495) 640 06-09,
- +7 (812) 640 06-09.

История версий

В этом разделе содержится краткое описание изменений и улучшений в продукте Indeed Access Manager по версиям.

9.3.1

- В Indeed Key Server исправлена ошибка при попытке отправить push-уведомление, если push-сервис недоступен.
- Исправлена ошибка входа через LDAP Proxy по имени пользователя в формате Distinguished Name, если в имени пробел.
- После установки Access Manager с помощью мастера конфигурации в конфигурационные файлы Haproxy добавлены отсутствовавшие настройки LDAP Proxy.
- Устранена неисправность, препятствовавшая использованию SSH-порта, заданного не по умолчанию.
- В мастере конфигурации исправлена ссылка на документацию Indeed Access Manager.
- Устранена ошибка, возникавшая при автоматической установке с помощью мастера конфигурации.
- Скорректированы настройки томов Docker, вызывавшие ошибку при старте Docker-контейнера Core Server на РЕД ОС.

9.3

- Реализована автоматическая установка AM через мастер конфигурации.
- Добавлен новый модуль интеграции Linux Logon — альтернатива Windows Logon для развертывания в системе под управлением Linux OS.
- Добавлен новый модуль интеграции LDAP Proxy для двухфакторной аутентификации в приложениях, которые работают по LDAP-протоколу.
- Реализована поддержка каталога FreeIPA — альтернатива Active Directory для Linux OS.
- Добавлена поддержка провайдера аутентификации Telegram Provider на сервере под управлением Linux OS.
- Добавлена возможность настройки времени ожидания для LDAP-соединения.
- Поддержана возможность запрета метода аутентификации для выбранного пользователя.
- Добавлены новые возможности для модуля FreeRADIUS: настройка способа проверки доменного пароля, конфигурация всех доступных переменных, добавление доменных и NetBIOS-имен при использовании нескольких LDAP-серверов.
- В Identity Provider (IDP) добавлена поддержка упрощенного метода аутентификации по стандарту OAuth 2.0 (Implicit Flow).
- Добавлена возможность регистрации нескольких аутентификаторов Secured TOTP на разных устройствах для одного пользователя.
- Исправлена логика при завершении сессии в Management Console: после повторной аутентификации пользователь возвращается на последнюю посещенную страницу.

- Добавлена возможность автоматической выдачи первичных прав администратора.
- Добавлены значения по умолчанию для идентификаторов пользователя и группы в файле переменных окружения.

9.2.1

- Добавлена возможность ограничивать доступ в Phone Management Server для групп пользователей.
- В конфигурационном файле утилиты валидации Passcode добавлены настройки по умолчанию.
- Добавлена настройка, позволяющая успешно запустить FreeRADIUS, даже если один из LDAP-серверов недоступен.
- Устранены ошибки при работе Log Server с базой Microsoft SQL.

9.2

- Реализована поддержка Linux OS для серверных компонентов Indeed AM.
- Добавлен новый модуль интеграции — FreeRADIUS Extension, альтернатива NPS RADIUS Extension для развертывания на сервере под управлением Linux OS.
- Добавлена поддержка следующих модулей интеграции на сервере под управлением Linux OS: Indeed ADFS Extension, Indeed RDP Windows Logon, Indeed Windows Logon и Indeed Identity Provider.
- Оптимизирована работа с несколькими каталогами пользователей.
- Создана утилита для миграции баз данных из Microsoft SQL в PostgreSQL.
- Добавлены новые возможности Management Console: настройка формата отображения имени пользователя, поиск по адресу электронной почты, единый формат времени и даты для локалей RU и EN, уменьшен интервал поиска событий до минуты.
- Большинство настроек провайдеров аутентификации перенесены в Management Console.
- Реализована возможность отключения сервиса освобождения лицензий.
- Добавлена возможность настраивать срок действия токена при доступе в модули интеграции через API.
- Добавлена возможность запретить или разрешить пользователям, которые не включены ни в одну политику доступа Indeed AM, аутентифицироваться в User Console.
- Добавлены события выхода пользователя из Management Console и User Console.
- Адреса клиентских машин теперь передаются через User Console и Management Console на сервер Indeed AM, а также отображаются в заголовках запросов к серверу.
- Реализована защита доступа к API с помощью клиентского сертификата.
- Осуществлена миграция основных компонентов Indeed AM в более актуальный фреймворк – ASP.NET Core.
- Добавлена возможность кастомизации интерфейса Management Console и User Console.
- В API добавлен новый метод, позволяющий получить подробную информацию о параметрах используемых методов аутентификации.

Справочник

Журнал событий

Список событий Indeed Core Server и Indeed Key Server

Роли

Права доступа администратора, оператора и инспектора

Журнал событий

Данный раздел содержит списки событий Indeed Core Server и Indeed Key Server.

События Indeed Core Server

В Indeed AM ведется учет событий следующих типов:

- информация (информационное сообщение, нет проблем или ошибок),
- ошибка (проблемы или ошибки, которые требуют вмешательства пользователя),
- предупреждение (возможны проблемы или ошибки).

Информация

Код	Текст сообщения	Атрибуты события
1000	Пользователь был аутентифицирован по предоставленному аутентификатору.	Модуль интеграции, Инициатор, Компьютер, Способ аутентификации, Комментарий аутентификатора, Приложение.
1001	Сервер Indeed-Id был запущен.	Компьютер.
1002	Сервер Indeed-Id был остановлен.	Компьютер.
1003	Пользователь был идентифицирован по предоставленному способу аутентификации.	Приложение, Инициатор, Компьютер, Способ аутентификации.
1004	Аутентификатор для целевого пользователя был зарегистрирован администратором.	Приложение, Целевой пользователь, Инициатор, Компьютер, Способ аутентификации, Комментарий аутентификатора.
1005	Настройка 'Максимальное количество аутентификаторов' для целевого пользователя была изменена администратором.	Инициатор, Компьютер, Целевой пользователь, Старое значение, Новое значение.
1006	Настройка 'Право на регистрацию аутентификатора' для целевого пользователя была изменена администратором.	Инициатор, Компьютер, Целевой пользователь, Старое значение, Новое значение.

Код	Текст сообщения	Атрибуты события
1007	Настройка 'Право на изменение аутентификатора' для целевого пользователя была изменена администратором.	Инициатор, Компьютер, Целевой пользователь, Старое значение, Новое значение.
1008	Настройка 'Право на удаление аутентификатора' для целевого пользователя была изменена администратором.	Инициатор, Компьютер, Целевой пользователь, Старое значение, Новое значение.
1009	Настройка 'Право на изменение комментария аутентификатора при регистрации' для целевого пользователя была изменена администратором.	Инициатор, Компьютер, Целевой пользователь, Старое значение, Новое значение.
1010	Настройка 'Право на изменение комментария аутентификатора' для целевого пользователя была изменена администратором	Инициатор, Компьютер, Целевой пользователь, Старое значение, Новое значение.
1011	Настройка 'Кэширование данных начиная с' для целевого пользователя была изменена администратором.	Инициатор, Компьютер, Целевой пользователь, Старое значение, Новое значение.
1012	Настройка 'Кэширование данных вплоть до' для целевого пользователя была изменена администратором.	Инициатор, Компьютер, Целевой пользователь, Старое значение, Новое значение.
1014	Настройка 'Кэширование данных в период' для целевого пользователя была изменена администратором.	Инициатор, Компьютер, Целевой пользователь, Старое значение, Новое значение.
1015	Настройка 'Начальная дата замещения пользователя' для целевого пользователя была изменена администратором.	Администратор, Инициатор, Компьютер, Целевой пользователь, Старое значение, Новое значение.
1016	Настройка 'Конечная дата замещения пользователя' для целевого пользователя была изменена администратором.	Администратор, Инициатор, Компьютер, Целевой пользователь, Старое значение, Новое значение.

Код	Текст сообщения	Атрибуты события
1017	Настройка 'Список заместителей' для целевого пользователя была изменена администратором.	Инициатор, Компьютер, Целевой пользователь, Старое значение, Новое значение.
1018	Настройка 'Разрешить кэширование' для целевого пользователя была изменена администратором.	Инициатор, Компьютер, Целевой пользователь, Старое значение, Новое значение.
1019	Настройка 'Разрешить замещение' для целевого пользователя была изменена администратором.	Инициатор, Компьютер, Целевой пользователь, Старое значение, Новое значение.
1020	Лицензия была выдана целевому объекту каталога администратором.	Компьютер, Инициатор, Идентификатор приложения, Целевой объект каталога.
1021	Лицензия была добавлена	Идентификатор лицензии, Дата начала, Дата окончания, Количество, Описание, Инициатор, Компьютер
1022	Лицензия была удалена	Идентификатор лицензии, Дата начала, Дата окончания, Количество, Описание, Инициатор, Компьютер.
1023	Лицензия целевого объекта каталога была удалена администратором.	Идентификатор лицензии, Компьютер, Инициатор, Идентификатор приложения, Целевой объект каталога, Тип лицензии.
1024	Аутентификатор целевого пользователя был изменен администратором.	Приложение, Целевой пользователь, Инициатор, Компьютер, Способ аутентификации, Комментарий аутентификатора.
1025	Комментарий аутентификатора целевого пользователя был изменен администратором.	Приложение, Целевой пользователь, Инициатор, Компьютер, Способ аутентификации, Старый комментарий аутентификатора, Новый комментарий аутентификатора.
1026	Аутентификатор целевого пользователя был удален администратором.	Приложение, Целевой пользователь, Инициатор, Компьютер, Способ аутентификации, Комментарий аутентификатора.
1027	Лицензия целевого пользователя была удалена сервером.	Идентификатор лицензии, Идентификатор приложения, Целевой пользователь.

Код	Текст сообщения	Атрибуты события
1028	Администратор назначил роль целевому объекту каталога	Приложение, Инициатор, Компьютер, Целевое приложение, Целевой объект каталога, Политика, Роль, Область действия.
1029	Администратор удалил роль у целевого объекта каталога	Приложение, Инициатор, Компьютер, Целевое приложение, Целевой объект каталога, Политика, Роль, Область действия.
1030	Устройство было добавлено пользователем.	Приложение, Инициатор, Компьютер, Устройство, Комментарий, Серийный номер.
1031	Устройство было удалено пользователем.	Приложение, Инициатор, Компьютер, Устройство, Комментарий, Серийный номер, Идентификатор устройства.
1032	Способ аутентификации для целевого пользователя был запрещен администратором.	Приложение, Инициатор, Компьютер, Целевой пользователь, Способ аутентификации.
1033	Способ аутентификации для целевого пользователя был разрешен администратором.	Приложение, Инициатор, Компьютер, Целевой пользователь, Способ аутентификации.
1034	Аутентификатор целевого пользователя был заблокирован администратором.	Приложение, Инициатор, Компьютер, Целевой пользователь, Способ аутентификации, Комментарий аутентификатора.
1035	Аутентификатор целевого пользователя был разблокирован администратором.	Приложение, Инициатор, Компьютер, Целевой пользователь, Способ аутентификации, Комментарий аутентификатора.
1036	Способ аутентификации пользователя заблокирован из-за превышения числа попыток аутентификации	Приложение, Инициатор, Компьютер, Способ аутентификации.
1037	Способ аутентификации для целевого пользователя был разблокирован администратором.	Приложение, Инициатор, Компьютер, Целевой пользователь, Способ аутентификации.

Код	Текст сообщения	Атрибуты события
1038	SMS-сообщение отправлено пользователю	Модуль интеграции, Инициатор, Компьютер, Способ аутентификации, Телефон, Источник телефона, Время отправки, Параметры отправки, Идентификатор сообщения, Приложение.
1039	Email-сообщение отправлено пользователю	Модуль интеграции, Инициатор, Компьютер, Способ аутентификации, Email, Приложение.
1040	Часть каталогов сервера недоступна.	Компьютер, Описание ошибки.
1041	Аутентификатор был изменен пользователем.	Приложение, Инициатор, Компьютер, Способ аутентификации, Комментарий аутентификатора.
1042	Аутентификатор был зарегистрирован пользователем.	Приложение, Инициатор, Компьютер, Способ аутентификации, Комментарий аутентификатора.
1043	Комментарий аутентификатора был изменен пользователем.	Приложение, Инициатор, Компьютер, Способ аутентификации, Старый комментарий аутентификатора, Новый комментарий аутентификатора.
1044	Аутентификатор был удален пользователем.	Приложение, Инициатор, Компьютер, Способ аутентификации, Комментарий аутентификатора.
1045	Аутентификатор целевого пользователя был отключен администратором.	Приложение, Инициатор, Компьютер, Целевой пользователь, Способ аутентификации, Комментарий аутентификатора.
1046	Аутентификатор целевого пользователя был включен администратором.	Приложение, Инициатор, Компьютер, Целевой пользователь, Способ аутентификации, Комментарий аутентификатора.
1047	Лицензия целевого объекта каталога была удалена администратором.	Компьютер, Инициатор, Идентификатор приложения, Целевой объект каталога.
1048	Лицензия была добавлена	Идентификатор лицензии, Дата начала, Дата окончания, Количество, Описание, Инициатор, Компьютер, Идентификатор приложения.
1049	Лицензия была удалена	Идентификатор лицензии, Дата начала, Дата окончания, Количество, Описание, Инициатор, Компьютер, Идентификатор приложения.

Код	Текст сообщения	Атрибуты события
1050	Лицензия целевого пользователя была удалена сервером.	Идентификатор приложения, Целевой пользователь.
1051	Политика успешно создана.	Идентификатор, Имя, Описание, Приоритет, Новые объекты каталога, Новые приложения, Приложение, Инициатор, Компьютер.
1052	Политика удалена.	Идентификатор, Имя, Описание, Приоритет, Удаленные объекты каталога, Удаленные приложения, Приложение, Инициатор, Компьютер.
1053	Политика изменена.	Идентификатор, Имя, Описание, Приоритет, Новые объекты каталога, Новые приложения, Удаленные объекты каталога, Удаленные приложения, Приложение, Инициатор, Компьютер, Доступные лицензии.
1054	Пароль пользователя был успешно синхронизирован.	Инициатор, Адрес клиента, Имя пользователя, Компьютер.
1055	Инициатор, Компьютер, Имя пользователя, Компьютер.	Инициатор, Компьютер, Клиентский пользователь, Клиентский компьютер.
1056	Пользователь успешно выполнил вход по кэшированному аутентификатору.	Инициатор, Способ входа, Комментарий аутентификатора, Адрес клиента, Имя пользователя, Компьютер.
1057	Пользователь успешно выполнил вход по предоставленному аутентификатору.	Инициатор, Способ входа, Комментарий аутентификатора, Адрес клиента, Имя пользователя, Компьютер.
1058	Пользователь убрал устройство входа. Сессия завершена.	Инициатор, Комментарий аутентификатора, Адрес клиента, Имя пользователя, Компьютер.
1059	Пользователь вышел из системы.	Инициатор, Комментарий аутентификатора, Адрес клиента, Имя пользователя, Компьютер.
1060	Пользователь убрал устройство входа. Компьютер заблокирован.	Инициатор, Комментарий аутентификатора, Компьютер, Имя пользователя, Компьютер.
1061	Пользователь заблокировал компьютер.	Инициатор, Комментарий аутентификатора, Адрес клиента, Имя пользователя, Компьютер.

Код	Текст сообщения	Атрибуты события
1062	Пользователь разблокировал компьютер по предоставленному паролю.	Инициатор, Адрес клиента, Имя пользователя, Компьютер.
1063	Пользователь разблокировал компьютер по кэшированному аутентификатору.	Инициатор, Способ входа, Комментарий аутентификатора, Адрес клиента, Имя пользователя, Компьютер.
1064	Пользователь разблокировал компьютер по предоставленному аутентификатору.	Инициатор, Способ входа, Комментарий аутентификатора, Адрес клиента, Имя пользователя, Компьютер.
1065	Пользователь снова подключился к своему терминальному сеансу.	Инициатор, Комментарий аутентификатора, Адрес клиента, Имя пользователя, Компьютер.
1066	Пользователь отключился от терминального сеанса.	Инициатор, Комментарий аутентификатора, Адрес клиента, Имя пользователя, Компьютер.
1067	Пароль пользователя был успешно сменен автоматически.	Инициатор, Адрес клиента, Имя пользователя, Компьютер.
1068	Пароль пользователя был успешно сменен.	Инициатор, Адрес клиента, Имя пользователя, Компьютер.
1069	Пароль пользователя рассинхронизирован.	Инициатор, Адрес клиента, Имя пользователя, Компьютер.
1070	Пользователь был аутентифицирован для целевого приложения.	Модуль интеграции, Приложение, Инициатор, Компьютер, Целевой пользователь.
1073	Изменение настроек метода аутентификации:	Приложение, Инициатор, Компьютер, Провайдер, Настройки.
1076	Настройки доступных действий пользователей над своими аутентификаторами были изменены	Политика, Пользователь, Обучение, Переобучение, Удаление, Изменение комментария только при обучении, Изменение комментария, Приложение, Инициатор, Компьютер.

Код	Текст сообщения	Атрибуты события
1077	Создана учетная запись	Политика, Целевой пользователь, Связанная учетная запись, Приложение, Имя, Пароль задан, Пароль случайный, Учетная запись выключена, Требовать аутентификацию при входе, Использовать учетные данные ОС, Формат преобразования имени, Описание, Приложение, Инициатор, Компьютер.
1078	Удалена учетная запись	Политика, Целевой пользователь, Связанная учетная запись, Приложение, Имя, Пароль задан, Пароль случайный, Учетная запись выключена, Требовать аутентификацию при входе, Использовать учетные данные ОС, Формат преобразования имени, Описание, Приложение, Инициатор, Компьютер.
1079	Изменены настройки учетной записи	Политика, Целевой пользователь, Связанная учетная запись, Приложение, Имя, Пароль задан, Пароль случайный, Учетная запись выключена, Требовать аутентификацию при входе, Использовать учетные данные ОС, Формат преобразования имени, Описание, Приложение, Инициатор, Компьютер.
1082	Изменение настроек метода аутентификации для пользователя:	Целевой пользователь, Провайдер, Приложение, Инициатор, Компьютер, Настройки.
1085	Изменение настроек метода аутентификации для приложения	Модуль, Провайдер, Политика, Id политики, Приложение, Инициатор, Компьютер, Настройки.
1086	Настройки кэширования данных пользователя были успешно изменены:	Целевое приложение, Целевой пользователь, Старые значения, Новые значения, Приложение, Инициатор, Компьютер.
1087	Настройки кэширования данных пользователя в политике были успешно изменены:	Целевое приложение, Политика, Старые значения, Новые значения, Приложение, Инициатор, Компьютер.
1088	Телефонный номер успешно зарегистрирован.	Пользователь, Инициатор, Пользователь API, Телефон.
1089	Телефонный номер успешно изменен.	Пользователь, Инициатор, Пользователь API, Телефон.
1090	Телефонный номер успешно удален.	Пользователь, Инициатор, Пользователь API.

Код	Текст сообщения	Атрибуты события
1091	Пароль пользователя был успешно сменен автоматически.	Целевой пользователь, Приложение, Инициатор, Компьютер.
1092	Пароль пользователя был успешно сменен.	Целевой пользователь, Приложение, Инициатор, Компьютер.
1093	Изменение политики метода аутентификации:	Провайдер, Политика, Id политики, Приложение, Инициатор, Компьютер, Настройки.
1094	Сервис отзыва лицензий завершил работу	Завершен отзыв лицензий в связи с удалением пользователя, политики, приложения политики или исключением пользователя из политики в которой была выдана лицензия, Отозвано лицензий, Не удалось отозвать.
1095	Лицензия целевого пользователя была удалена сервером в связи с превышением периода неактивности пользователя.	Идентификатор приложения, Целевой пользователь.
1096	Сервис отзыва лицензий завершил работу	Завершен отзыв лицензий в связи с неактивностью пользователей, Отозвано лицензий, Не удалось отозвать.
1097	ESSO Agent успешно инициализировался и начал работу	Инициатор, Адрес клиента, Идентификатор процесса, Компьютер.
1098	ESSO Agent завершает работу	Инициатор, Адрес клиента, Идентификатор процесса, Компьютер.
1099	Приложение было принудительно завершено	ИИнициатор, Адрес клиента, Приложение, Путь исполняемого файла приложения, Компьютер, Командная строка.
1100	Форма приложения была принудительно закрыта	Инициатор, Адрес клиента, Приложение, Путь исполняемого файла приложения, Тип формы, Компьютер, Командная строка.
1101	Пользователь аутентифицировался в ESSO	Инициатор, Адрес клиента, Имя пользователя, Компьютер.
1102	Пользователь реаутентифицировался в ESSO	Инициатор, Адрес клиента, Имя пользователя, Компьютер.

Код	Текст сообщения	Атрибуты события
1103	Пользователь выполнил вход в приложение.	Инициатор, Адрес клиента, Приложение, Путь исполняемого файла приложения, Имя пользователя, Имя учетной записи пользователя в приложении, Компьютер, Описание учетной записи ESSO, Командная строка.
1104	Пароль пользователя был успешно сменен.	Инициатор, Адрес клиента, Приложение, Путь исполняемого файла приложения, Имя пользователя, Имя учетной записи пользователя в приложении, Компьютер, Описание учетной записи ESSO, Командная строка.
1105	Добавлено сетевое подключение для пользователя ESSO	Инициатор, Компьютер, Имя пользователя, Диск подключения, Путь подключения, Компьютер.
1106	Удалено сетевое подключение для пользователя ESSO	Инициатор, Компьютер, Имя пользователя, Диск подключения, Компьютер.
1107	Ошибка при удалении сетевого подключения для пользователя ESSO	Инициатор, Компьютер, Имя пользователя, Диск подключения, Компьютер.
1108	Пользователь успешно разблокировал приложение.	Инициатор, Адрес клиента, Приложение, Путь исполняемого файла приложения, Имя пользователя, Имя учетной записи пользователя в приложении, Компьютер, Описание учетной записи ESSO, Командная строка.
1109	Замещающий пользователь аутентифицировался в ESSO	Инициатор, Компьютер, Имя пользователя, Замещающий пользователь, Компьютер.
1110	Замещающий пользователь реаутентифицировался в ESSO	Инициатор, Компьютер, Имя пользователя, Замещающий пользователь, Компьютер.
1111	Пароль пользователя был успешно сгенерирован и сменен автоматически.	Инициатор, Адрес клиента, Приложение, Путь исполняемого файла приложения, Имя пользователя, Имя учетной записи пользователя в приложении, Компьютер, Описание учетной записи ESSO, Командная строка.
1112	Добавлено новое приложение.	Название приложения, Описание, Модуль интеграции, Модуль, Инициатор, Компьютер.
1113	Приложение удалено.	Название приложения, Описание, Модуль интеграции, Модуль, Инициатор, Компьютер.

Код	Текст сообщения	Атрибуты события
1114	Параметры приложения изменены.	Название приложения, Описание, Список изменений, Модуль, Инициатор, Компьютер.
1115	Сообщение Telegram отправлено пользователю.	Модуль интеграции, Инициатор, Компьютер, Способ аутентификации, Приложение.
1116	Контакт Telegram успешно зарегистрирован.	Пользователь, Инициатор, Телефон.
1117	Пользователь был аутентифицирован в целях формирования ПЭП.	Ключ проверки ПЭП, Имя бизнес-приложения, Идентификатор устройства, Пользователь API, Пользователь.
1118	Отправка сообщений пользователям возобновлена.	Компьютер, Способ аутентификации.
1119	Пользователь был аутентифицирован на устройстве.	Предъявленный идентификатор, Ключ операции, Имя бизнес-приложения, Идентификатор устройства, Метод аутентификации, Пользователь API.
1120	Пользователь был аутентифицирован для подписания ЭД.	Предъявленный идентификатор, Ключ проверки ПЭП, Имя бизнес-приложения, Идентификатор ЭД, Метод аутентификации, Пользователь API.
1121	Инициирован процесс регистрации аутентификатора.	Приложение, Инициатор, Компьютер, Способ аутентификации.
1122	Инициирована аутентификация пользователя.	Модуль интеграции, Инициатор, Компьютер, Способ аутентификации, Приложение.
1123	Пользователь успешно вывел мобильное устройство из карантина Exchange.	Инициатор, Идентификатор устройства.
1124	Пользователь вышел из целевого приложения	Модуль интеграции, Приложение, Инициатор, Компьютер.
1125	Администратор перевел аутентификатор целевого пользователя в статус Готов	Приложение, Инициатор, Компьютер, Целевой пользователь, Способ аутентификации, Комментарий аутентификатора.

Код	Текст сообщения	Атрибуты события
1126	Администратор перевел аутентификатор целевого пользователя в статус Не готов	Приложение, Инициатор, Компьютер, Целевой пользователь, Способ аутентификации, Комментарий аутентификатора.
1127	Администратор перевел аутентификатор целевого пользователя в статус Ошибка	Приложение, Инициатор, Компьютер, Целевой пользователь, Способ аутентификации, Комментарий аутентификатора.
1128	Системное изменение настроек метода аутентификации:	Провайдер, Настройки.

Ошибка

Код	Текст сообщения	Атрибуты события	Причины возникновения
2000	Ошибка при попытке аутентифицировать пользователя по предоставленному способу аутентификации.	Модуль интеграции, Инициатор, Компьютер, Способ аутентификации, Описание ошибки, Приложение.	Неверный аутентификатор. Аутентификатор считается неверным, если: Аутентификатор указанного типа не обучен для пользователя. Аутентификатор не найден в списке аутентификаторов пользователя. Хранилище данных повреждено.
2001	Ошибка при попытке запустить сервер Indeed-Id	Компьютер, Описание ошибки.	Неуспешная попытка запуска Indeed Core Server вручную. Возможные причины: Ошибка в конфигурационном файле сервера. Сервер уже запущен. Повреждено хранилище данных. Ошибка IIS.
2002	Ошибка при попытке остановить сервер Indeed-Id	Компьютер, Описание ошибки.	Неуспешная попытка остановки Indeed Core Server вручную. Возможные причины: Недостаточно прав для выполнения операции. Indeed Core Server уже остановлен.

Код	Текст сообщения	Атрибуты события	Причины возникновения
2003	Ошибка при попытке идентифицировать пользователя по предоставленному способу аутентификации.	Приложение, Компьютер, Способ аутентификации, Описание ошибки.	Неуспешная попытка идентификации пользователя по выбранному способу аутентификации. Возможные причины: Пользователю отключен/ заблокирован выбранный способ аутентификации. Аутентификатор не найден в списке аутентификаторов пользователя. Хранилище данных повреждено.
2004	Ошибка при попытке администратора зарегистрировать аутентификатор для целевого пользователя.	Приложение, Целевой пользователь, Инициатор, Компьютер, Способ аутентификации, Комментарий аутентификатора, Описание ошибки.	Неуспешная попытка регистрации аутентификатора администратором. Возможные причины: Провайдер аутентификатора удален. Повреждено хранилище данных. Нет прав на управление аутентификаторами.
2005	Ошибка при попытке администратора изменить аутентификатор целевого пользователя.	Приложение, Целевой пользователь, Инициатор, Компьютер, Способ аутентификации, Старый комментарий аутентификатора, Новый комментарий аутентификатора, Описание ошибки.	Неуспешная попытка изменения аутентификатора администратором. Возможные причины: Провайдер аутентификатора удален. Повреждено хранилище данных. Нет прав на изменение аутентификатора.
2006	Ошибка при попытке администратора удалить аутентификатор целевого пользователя.	Приложение, Целевой пользователь, Инициатор, Компьютер, Способ аутентификации, Комментарий аутентификатора, Описание ошибки.	Неуспешная попытка администратора системы Indeed AM удалить аутентификатор пользователя. Возможные причины: Аутентификатор уже удален. Повреждено хранилище данных.

Код	Текст сообщения	Атрибуты события	Причины возникновения
2007	Ошибка при попытке администратора выдать лицензию для целевого объекта каталога.	Компьютер, Инициатор, Идентификатор приложения, Целевой объект каталога, Описание ошибки.	Неуспешная попытка администратора системы Indeed AM выдать лицензию для целевого объекта каталога. Возможные причины: Ошибка в файле лицензии. Сервер Indeed AM неактивен. Повреждено хранилище данных.
2008	Ошибка при попытке администратора удалить лицензию целевого объекта каталога.	Компьютер, Инициатор, Идентификатор приложения, Целевой объект каталога, Описание ошибки.	Неуспешная попытка администратора системы Indeed AM удалить лицензию целевого объекта каталога. Возможные причины: Лицензия уже удалена. Сервер Indeed AM неактивен. Повреждено хранилище данных.
2009	Ошибка при попытке удалить лицензию.	Идентификатор лицензии, Инициатор, Компьютер, Описание ошибки.	Неуспешная попытка пользователя системы Indeed AM удалить лицензию. Возможные причины: Лицензия уже удалена. Недостаточно прав. Сервер Indeed AM неактивен. Повреждено хранилище данных.
2010	Ошибка при попытке добавить лицензию.	Идентификатор лицензии, Инициатор, Компьютер, Описание ошибки.	Неуспешная попытка пользователя системы Indeed AM добавить лицензию. Возможные причины: Ошибка в файле лицензии. Недостаточно прав. Сервер Indeed AM неактивен. Повреждено хранилище данных.
2011	Ошибка при попытке сервера удалить лицензию целевого пользователя.	Идентификатор лицензии, Идентификатор приложения, Целевой пользователь, Описание ошибки.	Неуспешная попытка сервера удалить лицензию целевого пользователя. Возможные причины: Лицензия уже удалена. Повреждено хранилище данных.

Код	Текст сообщения	Атрибуты события	Причины возникновения
2012	Ошибка при попытке администратора изменить настройку 'Максимальное количество аутентификаторов' для целевого пользователя.	Инициатор, Компьютер, Целевой пользователь, Старое значение, Новое значение, Описание ошибки.	Неуспешная попытка смены параметра "Максимальное количество аутентификаторов" для пользователя администратором системы. Возможные причины: Недостаточно прав. Сервер Indeed AM неактивен. Повреждено хранилище данных.
2013	Ошибка при попытке администратора изменить настройку 'Право на регистрацию аутентификатора' для целевого пользователя.	Инициатор, Компьютер, Целевой пользователь, Старое значение, Новое значение, Описание ошибки.	Неуспешная попытка смены параметра "Право на регистрацию аутентификатора" для пользователя администратором системы. Возможные причины: Недостаточно прав. Сервер Indeed AM неактивен. Повреждено хранилище данных.
2014	Ошибка при попытке администратора изменить настройку 'Право на изменение аутентификатора' для целевого пользователя.	Инициатор, Компьютер, Целевой пользователь, Старое значение, Новое значение, Описание ошибки.	Неуспешная попытка смены параметра "Право на изменение аутентификатора" для пользователя администратором системы. Возможные причины: Недостаточно прав. Сервер Indeed AM неактивен. Повреждено хранилище данных.
2015	Ошибка при попытке администратора изменить настройку 'Право на удаление аутентификатора' для целевого пользователя.	Инициатор, Компьютер, Целевой пользователь, Старое значение, Новое значение, Описание ошибки.	Неуспешная попытка смены параметра "Право на удаление аутентификатора" для пользователя администратором системы. Возможные причины: Недостаточно прав. Сервер Indeed AM неактивен. Повреждено хранилище данных.
2016	Ошибка при попытке администратора изменить настройку 'Право на изменение комментария аутентификатора при регистрации' для целевого пользователя.	Инициатор, Компьютер, Целевой пользователь, Старое значение, Новое значение, Описание ошибки.	Неуспешная попытка смены параметра "Право на изменение комментария аутентификатора при регистрации" для пользователя администратором системы. Возможные причины: Недостаточно прав. Сервер Indeed AM неактивен. Повреждено хранилище данных.

Код	Текст сообщения	Атрибуты события	Причины возникновения
2017	Ошибка при попытке администратора изменить настройку 'Право на изменение комментария аутентификатора' для целевого пользователя.	Инициатор, Компьютер, Целевой пользователь, Старое значение, Новое значение, Описание ошибки.	Неуспешная попытка смены параметра "Право на изменение комментария аутентификатора" для пользователя администратором системы. Возможные причины: Недостаточно прав. Сервер Indeed AM неактивен. Повреждено хранилище данных.
2018	Ошибка при попытке администратора изменить настройку 'Кэширование данных начиная с' для целевого пользователя.	Инициатор, Компьютер, Целевой пользователь, Старое значение, Новое значение, Описание ошибки.	Неуспешная попытка смены параметра "Кэширование данных начиная с" для пользователя администратором системы. Возможные причины: Недостаточно прав. Сервер Indeed AM неактивен. Повреждено хранилище данных.
2019	Ошибка при попытке администратора изменить настройку 'Кэширование данных вплоть до' для целевого пользователя.	Инициатор, Компьютер, Целевой пользователь, Старое значение, Новое значение, Описание ошибки.	Неуспешная попытка смены параметра "Кэширование данных вплоть до" для пользователя администратором системы. Возможные причины: Недостаточно прав. Сервер Indeed AM неактивен. Повреждено хранилище данных.
2020	Ошибка при попытке администратора изменить настройку 'Кэширование данных в период' для целевого пользователя.	Инициатор, Компьютер, Целевой пользователь, Старое значение, Новое значение, Описание ошибки.	Неуспешная попытка смены параметра "Кэширование данных в период" для пользователя администратором системы. Возможные причины: Недостаточно прав. Сервер Indeed AM неактивен. Повреждено хранилище данных.
2021	Ошибка при попытке администратора изменить настройку 'Начальная дата замещения пользователя' для целевого пользователя.	Инициатор, Компьютер, Целевой пользователь, Старое значение, Новое значение, Описание ошибки.	Неуспешная попытка смены параметра "Начальная дата замещения пользователя" для пользователя администратором системы. Возможные причины: Недостаточно прав. Сервер Indeed AM неактивен. Повреждено хранилище данных.

Код	Текст сообщения	Атрибуты события	Причины возникновения
2022	Ошибка при попытке администратора изменить настройку 'Конечная дата замещения пользователя' для целевого пользователя.	Инициатор, Компьютер, Целевой пользователь, Старое значение, Новое значение, Описание ошибки.	Неуспешная попытка смены параметра "Конечная дата замещения пользователя" для пользователя администратором системы. Возможные причины: Недостаточно прав. Сервер Indeed AM неактивен. Повреждено хранилище данных.
2023	Ошибка при попытке администратора изменить настройку 'Список заместителей' для целевого пользователя.	Инициатор, Компьютер, Целевой пользователь, Старое значение, Новое значение, Описание ошибки.	Неуспешная попытка смены параметра "Список заместителей" для пользователя администратором системы. Возможные причины: Недостаточно прав. Сервер Indeed AM неактивен. Повреждено хранилище данных.
2024	Ошибка при попытке администратора изменить настройку 'Разрешить кэширование' для целевого пользователя.	Инициатор, Компьютер, Целевой пользователь, Старое значение, Новое значение, Описание ошибки.	Неуспешная попытка смены параметра "Разрешить кэширование" для пользователя администратором системы. Возможные причины: Недостаточно прав. Сервер Indeed AM неактивен. Повреждено хранилище данных.
2025	Ошибка при попытке администратора изменить настройку 'Разрешить замещение' для целевого пользователя.	Инициатор, Компьютер, Целевой пользователь, Старое значение, Новое значение, Описание ошибки.	Неуспешная попытка смены параметра "Разрешить замещение" для пользователя администратором системы. Возможные причины: Недостаточно прав. Сервер Indeed AM неактивен. Повреждено хранилище данных.
2026	Ошибка при попытке администратора назначить роль целевому объекту	Приложение, Инициатор, Компьютер, Целевое приложение, Целевой объект каталога, Политика, Роль, Область действия, Описание ошибки.	Неуспешная попытка добавления целевого объекта каталога в группу доступа для целевого приложения. Возможные причины: Недостаточно прав. Сервер Indeed AM неактивен. Повреждено хранилище данных.

Код	Текст сообщения	Атрибуты события	Причины возникновения
2027	Ошибка при попытке администратора удалить роль у целевого объекта каталога	Приложение, Инициатор, Компьютер, Целевое приложение, Целевой объект каталога, Политика, Роль, Область действия, Описание ошибки.	Неуспешная попытка удаления целевого объекта каталога из группы доступа для целевого приложения. Возможные причины: Недостаточно прав. Сервер Indeed AM неактивен. Повреждено хранилище данных.
2028	Ошибка при попытке пользователя добавить устройство.	Приложение, Инициатор, Компьютер, Устройство, Комментарий, Серийный номер, Описание ошибки.	Неуспешная попытка при добавлении устройства пользователем системы. Возможные причины: Недостаточно прав. Сервер Indeed AM неактивен. Повреждено хранилище данных.
2029	Ошибка при попытке пользователя удалить устройство.	Приложение, Инициатор, Компьютер, Устройство, Комментарий, Серийный номер, Идентификатор устройства, Описание ошибки.	Неуспешная попытка при удалении устройства пользователем системы. Возможные причины: Устройство уже удалено. Недостаточно прав. Сервер Indeed AM неактивен. Повреждено хранилище данных.
2030	Ошибка при попытке администратора запретить способ аутентификации для целевого пользователя.	Приложение, Инициатор, Компьютер, Целевой пользователь, Способ аутентификации, Описание ошибки.	Неуспешная попытка при запрете способа аутентификации для целевого пользователя администратором системы. Возможные причины: Данный способ уже запрещен. Недостаточно прав. Сервер Indeed AM неактивен. Повреждено хранилище данных.
2031	Ошибка при попытке администратора разрешить способ аутентификации для целевого пользователя.	Приложение, Инициатор, Компьютер, Целевой пользователь, Способ аутентификации, Описание ошибки.	Неуспешная попытка при разрешении способа аутентификации для целевого пользователя администратором системы. Возможные причины: Недостаточно прав. Сервер Indeed AM неактивен. Повреждено хранилище данных.

Код	Текст сообщения	Атрибуты события	Причины возникновения
2032	Ошибка при попытке администратора заблокировать аутентификатор целевого пользователя.	Приложение, Инициатор, Компьютер, Целевой объект каталога, Способ аутентификации, Комментарий аутентификатора, Описание ошибки.	Неуспешная попытка при блокировке аутентификатора целевого пользователя администратором системы. Возможные причины: Аутентификатор уже заблокирован. Недостаточно прав. Сервер Indeed AM неактивен. Повреждено хранилище данных.
2033	Ошибка при попытке администратора разблокировать аутентификатор целевого пользователя.	Приложение, Инициатор, Компьютер, Целевой пользователь, Способ аутентификации, Комментарий аутентификатора, Описание ошибки.	Неуспешная попытка при разблокировке аутентификатора целевого пользователя администратором системы. Возможные причины: Аутентификатор уже заблокирован. Недостаточно прав. Сервер Indeed AM неактивен. Повреждено хранилище данных.
2034	Ошибка при попытке заблокировать способ аутентификации пользователю	Приложение, Инициатор, Компьютер, Способ аутентификации, Описание ошибки.	Неуспешная попытка при блокировке способа аутентификации пользователем. Возможные причины: Способ аутентификации уже заблокирован. Недостаточно прав. Сервер Indeed AM неактивен. Повреждено хранилище данных.
2035	Ошибка при попытке администратора разблокировать способ аутентификации для целевого пользователя.	Приложение, Инициатор, Компьютер, Целевой пользователь, Способ аутентификации, Описание ошибки.	Неуспешная попытка при разблокировке способа аутентификации пользователем. Возможные причины: Способ аутентификации уже разблокирован. Недостаточно прав. Сервер Indeed AM неактивен. Повреждено хранилище данных.

Код	Текст сообщения	Атрибуты события	Причины возникновения
2036	Ошибка при попытке отправить SMS-сообщение.	Модуль интеграции, Инициатор, Компьютер, Способ аутентификации, Телефон, Источник телефона, Описание ошибки, Время отправки, Параметры отправки, Идентификатор сообщения, Приложение.	Неуспешная попытка при отправке SMS. Возможные причины: Ошибка при подключении к SMPP серверу. Не задан номер телефона.
2037	Ошибка при попытке отправить Email-сообщение	Модуль интеграции, Инициатор, Компьютер, Способ аутентификации, Email, Приложение.	Неуспешная попытка при отправке Email-сообщения. Возможные причины: Ошибка при подключении к SMTP серверу. Не задан email пользователя.
2038	Хранилище сервера недоступно.	Компьютер, Описание ошибки.	Неуспешная попытка при соединении с сервером Indeed. Возможные причины: Сервер Indeed AM неактивен. Повреждено хранилище данных.
2039	Каталоги сервера недоступны.	Компьютер, Описание ошибки.	
2040	Сервер не был запущен.	Компьютер, Описание ошибки.	Неуспешная попытка при запуске сервера indeed. Возможные причины: Сервер Indeed AM уже запущен. Ошибка в конфигурационном файле. Повреждено хранилище данных.
2041	Ошибка при попытке пользователя изменить аутентификатор.	Приложение, Инициатор, Компьютер, Способ аутентификации, Старый комментарий аутентификатора, Новый комментарий аутентификатора, Описание ошибки.	Неуспешная попытка при изменении аутентификатора пользователем. Возможные причины: Недостаточно прав. Сервер Indeed AM неактивен. Повреждено хранилище данных.

Код	Текст сообщения	Атрибуты события	Причины возникновения
2042	Ошибка при попытке пользователя зарегистрировать аутентификатор.	Приложение, Инициатор, Компьютер, Способ аутентификации, Комментарий аутентификатора, Описание ошибки.	Неуспешная попытка при регистрации аутентификатора пользователем. Возможные причины: Недостаточно прав. Сервер Indeed AM неактивен. Повреждено хранилище данных.
2043	Ошибка при попытке пользователя удалить аутентификатор.	Приложение, Инициатор, Компьютер, Способ аутентификации, Комментарий аутентификатора, Описание ошибки.	Неуспешная попытка при удалении аутентификатора пользователем. Возможные причины: Аутентификатор уже удален. Недостаточно прав. Сервер Indeed AM неактивен. Повреждено хранилище данных.
2044	Ошибка при попытке администратора отключить аутентификатор целевого пользователя.	Приложение, Инициатор, Компьютер, Целевой объект каталога, Способ аутентификации, Комментарий аутентификатора, Описание ошибки.	Неуспешная попытка при отключении аутентификатора целевого пользователя администратором системы. Возможные причины: Аутентификатор уже отключен. Недостаточно прав. Сервер Indeed AM неактивен. Повреждено хранилище данных.
2045	Ошибка при попытке администратора включить аутентификатор целевого пользователя.	Приложение, Инициатор, Компьютер, Целевой пользователь, Способ аутентификации, Комментарий аутентификатора, Описание ошибки.	Неуспешная попытка при включении аутентификатора целевого пользователя администратором системы. Возможные причины: Аутентификатор уже включен. Недостаточно прав. Сервер Indeed AM неактивен. Повреждено хранилище данных.
2046	Ошибка при попытке добавить лицензию	Идентификатор лицензии, Инициатор, Компьютер, Идентификатор приложения, Описание ошибки.	Неуспешная попытка при добавлении лицензии пользователем. Возможные причины: Недостаточно прав. Сервер Indeed AM неактивен. Повреждено хранилище данных. Ошибка в файле лицензии.

Код	Текст сообщения	Атрибуты события	Причины возникновения
2047	Ошибка при попытке удалить лицензию	Идентификатор лицензии, Инициатор, Компьютер, Идентификатор приложения, Описание ошибки.	Неуспешная попытка при удалении лицензии пользователем. Возможные причины: Недостаточно прав. Сервер Indeed AM неактивен. Повреждено хранилище данных.
2048	Ошибка при попытке сервера удалить лицензию целевого пользователя.	Идентификатор приложения, Целевой пользователь, Описание ошибки.	Неуспешная попытка при удалении лицензии сервером.
2049	Ошибка при создании политики.	Идентификатор, Имя, Описание, Приоритет, Новые объекты каталога, Новые приложения, Ошибка, Приложение, Инициатор, Компьютер.	Неуспешное создание политики.
2050	Ошибка при удалении политики.	Идентификатор, Имя, Описание, Приоритет, Удаленные объекты каталога, Удаленные приложения, Ошибка, Приложение, Инициатор, Компьютер.	Неуспешное удаление политики.
2051	Ошибка при изменении политики.	Идентификатор, Имя, Описание, Приоритет, Новые объекты каталога, Новые приложения, Удаленные объекты каталога, Удаленные приложения, Ошибка, Приложение, Инициатор, Компьютер.	Неуспешное изменение политики.
2052	Сервер Indeed-Id не найден.	Компьютер, Описание ошибки, Код ошибки.	Ошибка при попытке подключения к серверу Indeed AM. Указан неверный URL. Проблема в DNS.

Код	Текст сообщения	Атрибуты события	Причины возникновения
2053	Не удалось сменить пароль пользователя.	Инициатор, Адрес клиента, Имя пользователя, Компьютер, Описание ошибки, Код ошибки, Идентификатор события, Исходная ошибка.	Неуспешная смена пароля пользователя.
2054	Не удалось сменить пароль пользователя автоматически.	Инициатор, Адрес клиента, Имя пользователя, Компьютер, Описание ошибки, Код ошибки, Идентификатор события, Исходная ошибка.	Неуспешная смена пароля пользователя автоматически.
2055	Не удалось синхронизировать пароль пользователя.	Инициатор, Компьютер, Имя пользователя, Компьютер, Описание ошибки, Код ошибки, Идентификатор события, Исходная ошибка.	Ошибка синхронизации доменного пароля пользователя с паролем в хранилище Indeed. Возможные причины: Сервер Indeed недоступен. Повреждено хранилище данных.
2058	Изменение настроек метода аутентификации:	Приложение, Инициатор, Компьютер, Провайдер, Настройки, Описание ошибки.	Неуспешное изменение настроек метода аутентификации.
2061	Ошибка при попытке изменить настройки доступных действий пользователей над своими аутентификаторами	Политика, Пользователь, Обучение, Переобучение, Удаление, Изменение комментария только при обучении, Изменение комментария, Приложение, Инициатор, Компьютер, Ошибка.	Неуспешное изменение настройки прав аутентификатора.

Код	Текст сообщения	Атрибуты события	Причины возникновения
2062	Ошибка при попытке создать учетную запись	Политика, Целевой пользователь, Связанная учетная запись, Приложение, Имя, Пароль задан, Пароль случайный, Учетная запись выключена, Требовать аутентификацию при входе, Использовать учетные данные ОС, Формат преобразования имени, Описание, Приложение, Инициатор, Компьютер, Ошибка.	Неуспешное создание настройки учетной записи
2063	Ошибка при попытке удалить учетную запись	Политика, Целевой пользователь, Связанная учетная запись, Приложение, Имя, Пароль задан, Пароль случайный, Учетная запись выключена, Требовать аутентификацию при входе, Использовать учетные данные ОС, Формат преобразования имени, Описание, Приложение, Инициатор, Компьютер, Ошибка.	

Код	Текст сообщения	Атрибуты события	Причины возникновения
2064	Ошибка при попытке изменить настройки учетной записи	Политика, Целевой пользователь, Связанная учетная запись, Приложение, Имя, Пароль задан, Пароль случайный, Учетная запись выключена, Требовать аутентификацию при входе, Использовать учетные данные ОС, Формат преобразования имени, Описание, Приложение, Инициатор, Компьютер, Ошибка.	
2067	Изменение настроек метода аутентификации для пользователя:	Целевой пользователь, Провайдер, Приложение, Инициатор, Компьютер, Настройки, Описание ошибки.	Неуспешное изменение настроек метода аутентификации для пользователя.
2070	Ошибка при попытке изменить настройки метода аутентификации для приложения	Модуль, Провайдер, Политика, Id политики, Приложение, Инициатор, Компьютер, Настройки, Описание ошибки.	Неуспешное изменение настроек метода аутентификации для модуля
2071	Ошибка при попытке изменить настройки кэширования данных пользователя:	Целевое приложение, Целевой пользователь, Старые значения, Новые значения, Приложение, Инициатор, Компьютер, Описание ошибки.	Неуспешная попытка изменить настройки кэширования данных пользователя. Возможные причины: Недостаточно прав для выполнения операции. Повреждено хранилище данных.
2072	Ошибка при попытке изменить настройки кэширования данных пользователя в политике:	Целевое приложение, Политика, Старые значения, Новые значения, Приложение, Инициатор, Компьютер, Описание ошибки.	Неуспешная попытка изменить настройки кэширования данных пользователя в политике. Возможные причины: Недостаточно прав для выполнения операции. Повреждено хранилище данных.

Код	Текст сообщения	Атрибуты события	Причины возникновения
2073	Ошибка регистрации телефонного номера.	Пользователь, Инициатор, Пользователь API, Описание ошибки, Инициатор ошибки, Телефон.	Неуспешная попытка регистрации телефонного номера. Возможные причины: Недостаточно прав для выполнения операции. Не доступен компонент EAPhoneServer. Указан несуществующий пользователь. Повреждено хранилище данных.
2074	Ошибка изменения телефонного номера.	Пользователь, Инициатор, Пользователь API, Описание ошибки, Инициатор ошибки, Телефон.	Неуспешная попытка изменения телефонного номера. Возможные причины: Недостаточно прав для выполнения операции. Не доступен компонент EAPhoneServer. Указан несуществующий пользователь. Повреждено хранилище данных.
2075	Ошибка удаления телефонного номера.	Пользователь, Инициатор, Пользователь API, Описание ошибки, Инициатор ошибки.	Неуспешная попытка удаления телефонного номера. Возможные причины: Недостаточно прав для выполнения операции. Не доступен компонент EAPhoneServer. Указан несуществующий пользователь. Повреждено хранилище данных.
2076	Не удалось сменить пароль пользователя автоматически.	Целевой пользователь, Приложение, Инициатор, Компьютер, Описание ошибки.	Неуспешная попытка смены пароля на случайный. Возможные причины: Недостаточно прав для выполнения операции. Повреждена инсталляция Indeed-Id Server. Запрос на смену пароля блокирован политиками безопасности.
2077	Не удалось сменить пароль пользователя.	Целевой пользователь, Приложение, Инициатор, Компьютер, Описание ошибки.	Неуспешная попытка смены пароля пользователем вручную (при первом входе, в окне «Безопасность Windows» после нажатия комбинации клавиш [Ctrl]+[Alt]+[Del]).

Код	Текст сообщения	Атрибуты события	Причины возникновения
2078	Ошибка изменения политики метода аутентификации:	Провайдер, Политика, Id политики, Приложение, Инициатор, Компьютер, Настройки, Описание ошибки.	Неуспешное изменение политики метода аутентификации.
2079	Ошибка при сохранении пароля пользователя в базе данных ESSO	Инициатор, Компьютер, Описание приложения, Путь исполняемого файла приложения, Имя пользователя, Имя учетной записи пользователя в приложении, Компьютер, Описание ошибки, Код ошибки, Командная строка.	Отсутствует связь с сервером Indeed или контроллером домена.
2080	Ошибка при загрузке данных ESSO для аутентифицировавшегося пользователя	Инициатор, Адрес клиента, Имя пользователя, Компьютер, Описание ошибки, Код ошибки.	Повреждены данные пользователя Indeed Enterprise Single Sign-On в Active Directory. Не удалось принудительно завершить форму приложения.
2081	Обнаружен сбой в ESSO Agent	Инициатор, Адрес клиента, Компьютер, Описание ошибки, Код ошибки.	Не удалось завершить процесс приложения.
2082	Ошибка при добавлении сетевого подключения для пользователя	Инициатор, Компьютер, Имя пользователя, Диск подключения, Путь подключения, Компьютер, Описание ошибки, Код ошибки.	Сетевой диск заполнен. Отсутствует связь с сервером Indeed.
2083	Ошибка при добавлении нового приложения.	Название приложения, Описание, Модуль интеграции, Модуль, Инициатор, Компьютер, Описание ошибки.	Неуспешная попытка добавления нового приложения: Недостаточно прав для выполнения операции. Отсутствует связь с сервером Indeed AM.

Код	Текст сообщения	Атрибуты события	Причины возникновения
2084	Ошибка при удалении приложения.	Название приложения, Описание, Модуль интеграции, Модуль, Инициатор, Компьютер, Описание ошибки.	Неуспешная попытка удаления приложения: Недостаточно прав для выполнения операции. Отсутствует связь с сервером Indeed AM.
2085	Ошибка при изменении параметров приложения.	Название приложения, Описание, Список изменений, Модуль, Инициатор, Компьютер, Описание ошибки.	Неуспешная попытка изменения параметров приложения: Недостаточно прав для выполнения операции. Отсутствует связь с сервером Indeed AM.
2086	Не удалось доставить сообщение на центральный лог-сервер.	Приложение, Инициатор, Компьютер, Тип, Категория, ID сообщения, Описание.	Неуспешная попытка отправки сообщения на центральный лог-сервер: Отсутствует связь с лог сервером Indeed AM.
2087	Ошибка при попытке отправить сообщение Telegram.	Модуль интеграции, Инициатор, Компьютер, Способ аутентификации, Описание ошибки, Приложение.	Произошла одна или несколько ошибок. Произошла ошибка при отправке запроса: нет доступа / связи с сервера AM core до api.telegram.org.
2088	Ошибка регистрации контакта Telegram.	Пользователь, Инициатор, Описание ошибки, Инициатор ошибки, Телефон.	Доступ запрещен. Пользователь не может быть авторизован. Произошла одна или несколько ошибок. У пользователя нет следующих прав: ReadUserAuthenticators для приложения Authenticator Management: сервисная УЗ Telegram не добавлена в глобальные администраторы Management Console.
2089	Ошибка при попытке аутентифицировать пользователя в целях формирования ПЭП.	Описание ошибки, Имя бизнес-приложения, Пользователь API, Идентификатор устройства.	Произошла ошибка аутентификации пользователя при формировании простой электронной подписи.

Код	Текст сообщения	Атрибуты события	Причины возникновения
2090	Обнаружена потенциальная спам-атака. Отправка сообщений приостановлена.	Компьютер, Способ аутентификации, Начало временного интервала, Конец временного интервала, Кол-во отправок, Кол-во успешных входов, Процент успешных входов.	Неуспешная попытка отправки сообщения из-за обнаружения подозрительной активности при данном способе аутентификации.
2091	Ошибка при попытке аутентифицировать пользователя на устройстве.	Описание ошибки, Предъявленный идентификатор, Ключ операции, Имя бизнес-приложения, Идентификатор устройства, Метод аутентификации, Пользователь API.	Неуспешный ввод кода на устройстве.
2092	Ошибка при попытке аутентифицировать пользователя для подписания ЭД.	Описание ошибки, Предъявленный идентификатор, Ключ проверки ПЭП, Имя бизнес-приложения, Идентификатор ЭД, Метод аутентификации, Пользователь API.	Неуспешная попытка входа. Возможные причины: Неверный логин. Неверный пароль.
2093	Пользователь ввел OTP, длина которого не совпадает с настройками провайдера аутентификации.	Способ аутентификации, Целевой пользователь, Значение при регистрации, Текущее значение.	Несоответствие фактической длины введенного OTP и заданной длины OTP провайдера.
2094	Период обновления OTP в аутентификаторе пользователя не совпадает с настройками провайдера аутентификации.	Способ аутентификации, Целевой пользователь, Значение при регистрации, Текущее значение.	Несоответствие фактического периода обновления OTP с заданным периодом обновления.

Код	Текст сообщения	Атрибуты события	Причины возникновения
2095	Алгоритм OTP в аутентификаторе пользователя не совпадает с настройками провайдера аутентификации.	Способ аутентификации, Целевой пользователь, Значение при регистрации, Текущее значение.	Неуспешная попытка вывести устройство из карантина.
2096	Не удалось вывести мобильное устройство из карантина Exchange.	Инициатор, Идентификатор устройства.	Несоответствие фактического алгоритма OTP с заданным алгоритмом.
2097	Не удалось заблокировать мобильное устройство на сервере Exchange.	Инициатор, Идентификатор устройства.	Неуспешная попытка заблокировать мобильное устройство.
2098	Вход в приложение запрещен политикой доступа.	Приложение, Модуль интеграции, Инициатор, Компьютер.	Неуспешная попытка входа в RADIUS, если пользователь не добавлен в политику.
2099	Ошибка при попытке перевести аутентификатор целевого пользователя в статус Готов.	Приложение, Инициатор, Компьютер, Целевой пользователь, Способ аутентификации, Комментарий аутентификатора, Описание ошибки	Неуспешная попытка обновления статуса аутентификатора в хранилище данных. Возможные причины: У учетной записи, используемой для подключения к БД, отсутствуют необходимые права на изменение записей. Хранилище данных повреждено.
2100	Ошибка при попытке перевести аутентификатор целевого пользователя в статус Не готов.	Приложение, Инициатор, Компьютер, Целевой пользователь, Способ аутентификации, Комментарий аутентификатора, Описание ошибки	Неуспешная попытка обновления статуса аутентификатора в хранилище данных. Возможные причины: У учетной записи, используемой для подключения к БД, отсутствуют необходимые права на изменение записей. Хранилище данных повреждено.

Код	Текст сообщения	Атрибуты события	Причины возникновения
2101	Ошибка при попытке перевести аутентификатор целевого пользователя в статус Ошибка.	Приложение, Инициатор, Компьютер, Целевой пользователь, Способ аутентификации, Комментарий аутентификатора, Описание ошибки	Неуспешная попытка обновления статуса аутентификатора в хранилище данных. Возможные причины: У учетной записи, используемой для подключения к БД, отсутствуют необходимые права на изменение записей. Хранилище данных повреждено.
2102	Ошибка при попытке системного изменения настроек метода аутентификации:	Провайдер, Настройки, Описание ошибки	Неуспешная попытка обновления настроек метода аутентификации. Возможные причины: У учетной записи, используемой для подключения к БД, отсутствуют необходимые права на изменение записей. Хранилище данных повреждено.
2103	Ошибка при попытке отправить push-уведомление Indeed Key.	Модуль интеграции, Инициатор, Компьютер, Способ аутентификации, Описание ошибки, Приложение	Неуспешная попытка отправки push-уведомления пользователю. Возможные причины: Целевой пользователь еще не зарегистрировал аутентификатор , либо для провайдера сработала автоматическая защита от спама. Сервер Indeed Key (IKS) недоступен. В конфигурации указан невалидный или неразрешимый адрес подключения к IKS. Пользователь не зарегистрировал аутентификатор. Различается значение Trusted Id в конфигурации провайдера Indeed Key и в конфигурации IKS. В IKS для строки подключения к БД указаны неверные логин или пароль.

Предупреждение

Код	Текст сообщения	Атрибуты события	Причины возникновения
3000	Окно сравнения OTP в аутентификаторе пользователя не совпадает с настройками провайдера аутентификации.	Способ аутентификации, Целевой пользователь, Значение при регистрации, Текущее значение.	Несоответствие фактического окна сравнения OTP с заданным окном сравнения.
3001	Окно синхронизации OTP в аутентификаторе пользователя не совпадает с настройками провайдера аутентификации.	Способ аутентификации, Целевой пользователь, Значение при регистрации, Текущее значение.	Несоответствие фактического окна синхронизации OTP с заданным окном синхронизации.
3002	Пользователь заблокировал мобильное устройство на сервере Exchange.	Инициатор, Идентификатор устройства.	Успешная попытка заблокировать устройство.

События Indeed Key Server

> **ИНФОРМАЦИЯ**
>
> Просмотр журнала событий возможен через просмотр EventLog Windows (при использовании хранилища Windows) или сторонними средствами через SQL (при использовании хранилища SQL).

Код	Категория	Сервис	Текст сообщения
1000	Информация	Indeed Key	Запрос на аутентификацию пользователя {userLogin} отправлен. Приложение: {appId}
1001	Информация	Indeed Key	Запрос на регистрацию пользователя {userLogin} отправлен. Приложение: {appId}
1002	Информация	Indeed Key	Обработан ответ пользователя {userLogin} на запрос аутентификации. Приложение: {appId}. Результат: {state}. Сообщение: {message}
1003	Информация	Indeed Key	Запрос на установку сертификата пользователю {userLogin} отправлен. Приложение: {appId}
1004	Информация	Indeed Key	Регистрация пользователя {userLogin} успешно завершена. Приложение: {appId}

Код	Категория	Сервис	Текст сообщения
1005	Информация	Indeed Key	Удаление пользователя {userLogin} успешно завершено. Приложение: {appId}
2000	Ошибка	Indeed Key	Ошибка при отправке запроса на аутентификацию пользователя {userLogin}. Приложение: {appId}. Ошибка:
2001	Ошибка	Indeed Key	Ошибка при отправке запроса на регистрацию пользователя {userLogin}. Приложение: {appId}. Ошибка:
2002	Ошибка	Indeed Key	Ошибка при отправке запроса на установку сертификата пользователю {userLogin}. Приложение: {appId}. Ошибка:
2003	Ошибка	Indeed Key	Ошибка при регистрации пользователя {userLogin}. Приложение: {appId}. Ошибка:
2004	Ошибка	Indeed Key	Ошибка при удалении пользователя {userLogin}. Приложение: {appId}. Ошибка:

Роли

Данный раздел содержит таблицы ролей и прав следующих пользователей:

- Администратор — полный доступ ко всем функциям и настройкам системы,
- Оператор — права только на изменение настроек пользователей и устройств аутентификации,
- Инспектор — доступ на чтение всех данных и настроек системы.

Политики

Операция	Администратор	Оператор	Инспектор
Просмотр политики	✓	✓	✓
Создание политики	✓	✗	✗
Удаление политики	✓	✗	✗
Редактирование политики	✓	✗	✗
Копирование политики	✓	✗	✗
Информация			
Доступ к разделу Информация	✓	✓	✓
Просмотр информации о политике	✓	✓	✓
Просмотр количества приложений	✓	✓	✓
Приложения			
Доступ к разделу Приложения	✓	✓	✓
Просмотр всех приложений	✓	✓	✓
Добавление приложения	✓	✗	✗
Удаление приложения	✓	✗	✗

Операция	Администратор	Оператор	Инспектор
Управление приложением в политике			
Просмотр информации о приложении	✓	✓	✓
Изменение информации о приложении	✓	✓	✗
Добавление приложения	✓	✗	✗
Удаление приложения	✓	✗	✗
Управление кешированием приложения			
Просмотр настроек кеширования	✓	✓	✓
Включение/выключение кеширования	✓	✓	✗
Изменение настроек кеширования	✓	✗	✗
Управление методами аутентификации приложения			
Просмотр доступных методов аутентификации	✓	✓	✓
Изменение доступных методов аутентификации	✓	✓	✗
Область действия			
Доступ к разделу Область действия	✓	✓	✓
Добавление пользователя	✓	✗	✗
Удаление пользователя	✓	✗	✗
Администраторы			
Доступ к разделу Администраторы	✓	✗	✓
Добавление администратора	✓	✗	✗

Операция	Администратор	Оператор	Инспектор
Удаление администратора	✓	✗	✗
Лицензии			
Доступ к разделу Лицензии	✓	✗	✓
Просмотр используемых лицензий	✓	✗	✓
Изменение количества доступных лицензий	✓	✗	✗
Управление приоритетом политики			
Просмотр приоритета политики	✓	✓	✓
Изменение приоритета политики	✓	✗	✗