



Indeed Access Manager

Руководство по администрированию

Оглавление

1. Indeed Access Manager 8.1 Documentation	5
1.1 С чего начать?	6
1.2 Общее описание	7
1.3 Схема и состав решения	8
1.3.1 Основные элементы решения	9
1.3.2 Размещение компонентов	11
1.3.3 Список реализуемых сценариев	13
1.4 Установка системы	16
1.4.1 Системные требования	17
1.4.1.1 Системные требования серверных компонентов	18
1.4.1.1.1 Требования Indeed AM Log Server	19
1.4.1.1.2 Требования Indeed Access Manager Server	21
1.4.1.1.3 Требования Indeed AM Management Console	23
1.4.1.1.4 Требования Indeed AM User Console	25
1.4.1.1.5 Требования Indeed Key Server	27
1.4.1.1.6 Требования Indeed AM Phone Management Server	30
1.4.1.2 Системные требования модулей интеграции	32
1.4.1.3 Системные требования клиентских компонентов	37
1.4.1.4 Сетевое взаимодействие	40
1.4.2 Подготовка	42
1.4.2.1 Установка компонентов Internet Information Services	43
1.4.2.2 Создание и настройка хранилища данных	44
1.4.2.2.1 Хранилище данных Microsoft SQL	45
1.4.2.2.2 Хранилище данных PostgreSQL	54
1.4.2.3 Каталог пользователей	59
1.4.2.4 Установка клиентского сертификата	64
1.4.3 Порядок установки	66
1.4.4 Установка и настройка	67
1.4.4.1 Indeed AM Log Server	69
1.4.4.1.1 Установка и настройка Indeed AM Log Server с резервным хранилищем	72
1.4.4.1.2 Установка и настройка Indeed AM Log Server с хранилищем в SysLog	78
1.4.4.1.3 Установка и настройка Indeed AM Log Server с хранилищем в БД ..	86
1.4.4.1.4 Установка и настройка Indeed AM Log Server с хранилищем в EventLog	93
1.4.4.2 Indeed Access Manager Server	96
1.4.4.2.1 Indeed Access Manager Server с хранилищем данных в MS SQL	98
1.4.4.2.2 Indeed Access Manager Server с хранилищем данных в PostgreSQL	118
1.4.4.3 Indeed AM Management Console	138
1.4.4.4 Indeed AM User Console	153
1.4.4.5 Indeed Key Server	171
1.4.4.6 Indeed AM Phone Management Server	181
1.4.4.7 Indeed AM Reset Password	196
1.4.4.8 Установка и настройка провайдеров	203
1.4.4.8.1 Indeed AM Windows Password Provider	204
1.4.4.8.2 Indeed AM Smart Card Provider	205
1.4.4.8.3 Indeed AM IronLogic Z2USB Provider	213
1.4.4.8.4 Indeed AM OMNIKEY Provider	221

1.4.4.8.5 Indeed AM Futronic Provider	228
1.4.4.8.6 Indeed AM Passcode Provider	235
1.4.4.8.7 Indeed AM Email OTP Provider	238
1.4.4.8.8 Indeed AM Hardware TOTP Provider	244
1.4.4.8.9 Indeed AM HOTP Provider	253
1.4.4.8.10 Indeed AM Storage SMS OTP Provider	261
1.4.4.8.11 Indeed AM Telegram OTP Provider	271
1.4.4.8.12 Indeed AM SMS OTP Provider	284
1.4.4.8.13 Indeed AM Software OTP Provider	306
1.4.4.8.14 Indeed Key Provider	311
1.4.4.8.15 Indeed AM MFA Provider	329
1.4.4.9 Модули интеграции	338
1.4.4.9.1 Indeed AM Identity Provider	339
1.4.4.9.2 Indeed AM ADFS Extension	353
1.4.4.9.3 Indeed AM ESSO Agent	374
1.4.4.9.4 Indeed AM IIS Extension	397
1.4.4.9.5 Indeed AM NPS RADIUS Extension	409
1.4.4.9.6 Indeed AM RDP Windows Logon	438
1.4.4.9.7 Indeed AM Windows Logon	446
1.4.4.9.8 Indeed AM SAML IDP	466
1.4.5 Сбор логов	479
1.4.5.1 Indeed AM GetLog	480
1.4.5.2 Сбор логов серверных компонентов	484
1.4.6 Миграция с Indeed AM 7.x на Indeed AM 8.1	490
1.4.6.1 Подготовка к миграции	491
1.4.6.2 Миграция MS SQL	493
1.4.6.3 Миграция хранилища Active Directory	508
1.5 Администрирование системы	519
1.5.1 API	521
1.5.1.1 Общая информация	522
1.5.1.2 Быстрый старт	526
1.5.1.3 Описание методов API	528
1.5.1.3.1 Authenticator	529
1.5.1.3.2 License	532
1.5.1.3.3 Logon	535
1.5.1.3.4 Policy	540
1.5.1.3.5 TemplateSession	542
1.5.1.3.6 User	546
1.5.1.3.7 UserCatalog	547
1.5.1.3.8 UserProfile	555
1.5.1.4 Сценарии использования	556
1.5.1.4.1 2FA аутентификация в API	557
1.5.1.4.2 Получение списка лицензий с их общим количеством и количеством используемых	560
1.5.1.4.3 Получение списка пользователей с лицензиями	562
1.5.1.4.4 Сбор статистики по обученным аутентификаторам пользователей .	5
64	
1.5.1.4.5 Создание отчетов	567
1.5.2 Консоль администратора	575
1.5.2.1 Получение и регистрация лицензий	576
1.5.2.2 Создание и настройка политик	580

1.5.2.3	Добавление и настройка приложений	588
1.5.2.4	Кеширование данных пользователя	596
1.5.2.5	Управление аутентификаторами	599
1.5.2.6	Поиск пользователей	604
1.5.2.7	Карточка пользователя	605
1.5.2.8	Журнал событий	608
1.5.2.9	Конфигурация	671
1.5.3	Консоль управления аутентификаторами пользователя	678
1.5.3.1	Локализация (User Console)	679
1.5.3.2	Управление аутентификаторами (User Console)	680
1.5.3.3	Карточка пользователя (User Console)	689
1.5.4	Утилита управления аутентификаторами	690
1.5.4.1	Удаление аутентификатора	692
1.5.4.2	Проверка аутентификатора	694
1.5.4.3	Редактирование аутентификатора	696
1.5.4.4	Добавление аутентификатора	700
1.6	Предыдущие версии	703

Indeed Access Manager 8.1 Documentation

Indeed Access Manager 8.1

Предыдущие версии

- [Indeed Access Manager 8.0](#)
- [Indeed Access Manager 7.2](#)
- [Indeed Access Manager 7.1](#)
- [Indeed Access Manager 7.0](#)

С чего начать?

Добро пожаловать в электронное руководство по продукту Indeed Access Manager.

Введение в Indeed AM

- [Общее описание](#)

Описание компонентов Indeed AM

- [Основные элементы решения](#)
- [Список реализуемых сценариев](#)

Подготовка, установка и настройка Indeed AM

- [Системные требования](#)
- [Подготовка](#)
- [Порядок установки](#)
- [Установка и настройка](#)
- [Установка и настройка расширений](#)

Администрирование Indeed AM

- [Консоль администратора](#)

Общее описание

Система **Indeed Access Manager 8.1** позволяет реализовать строгую аутентификацию в следующих компонентах:

- Windows Logon
- Enterprise Single Sign-On
- NPS RADIUS Extension
- Identity Provider
- ADFS Extension
- IIS Extension
- RDP Windows Logon

Ниже представлены ссылки на описание решаемых задач системой Indeed AM

- [Защита опубликованных корпоративных приложений](#)
- [Выполнение требований стандарта PCI DSS в части аутентификации пользователей](#)
- [Замена паролей на биометрическую аутентификацию сотрудников](#)
- [Организация единой точки доступа в информационные системы компании](#)
- [Использование RFID-карт для доступа в информационные системы](#)
- [Корпоративное удостоверение сотрудника](#)

Схема и состав решения

Информация

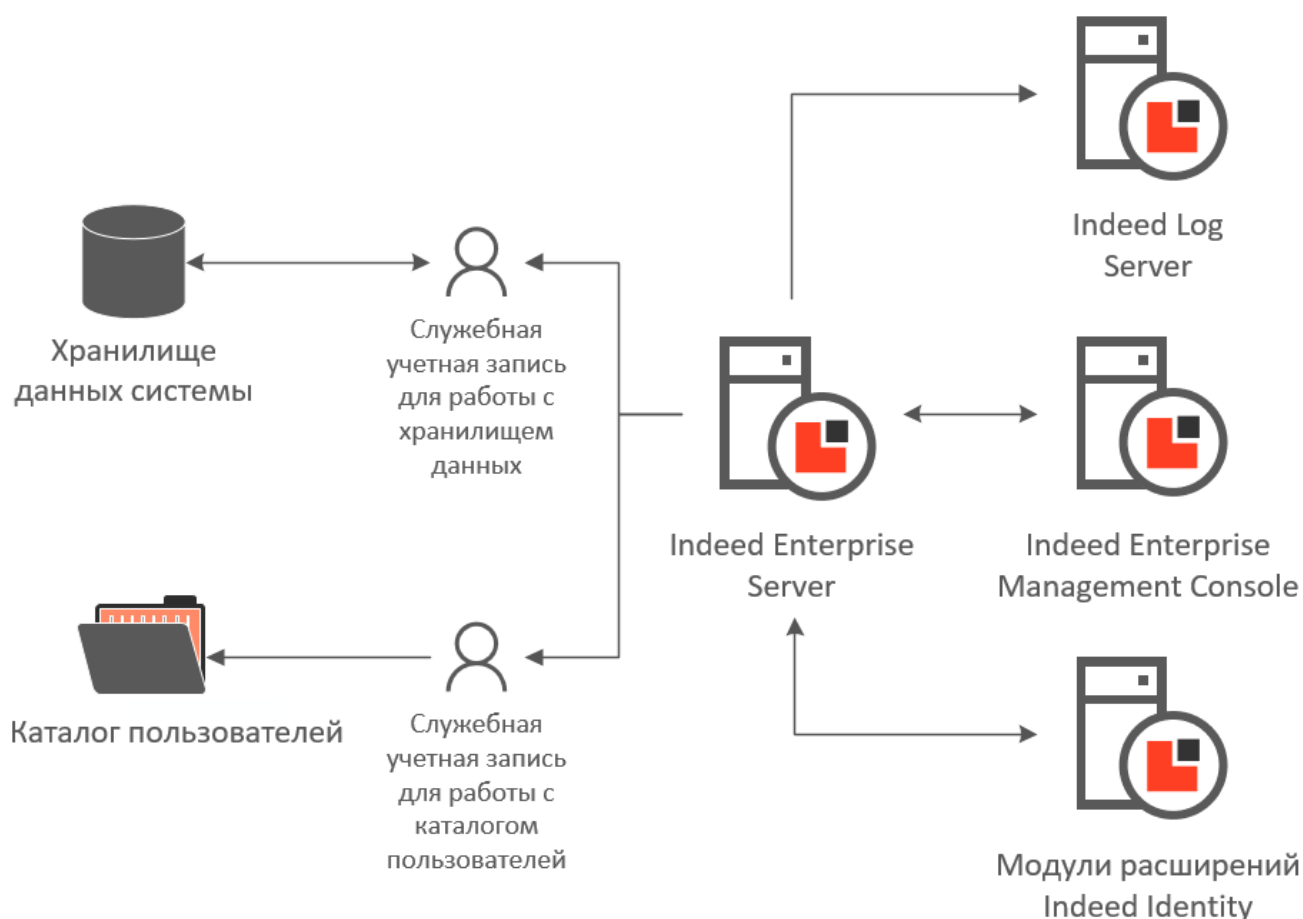
Страница дополняется.

В разделе описаны элементы, использующиеся в системе Indeed Access Manager 8.1, приведена схема компонентов и сценарии использования системы.

1. [Основные элементы решения](#)
2. [Список реализуемых сценариев](#)

Основные элементы решения

1. **Indeed Access Manager Server** — основной модуль системы Indeed AM.
2. **Indeed AM Log Server** — централизованный сбор и аудит событий системы Indeed AM.
3. **Indeed AM Management Console** — консоль администратора системы Indeed AM.
4. **Модули интеграции** — дополнительные компоненты, позволяющие системе Indeed Access Manager участвовать в процессе аутентификации пользователей.
5. **Хранилище данных** — базы данных для компонентов Indeed AM Server, Indeed AM Log Server и Indeed AM AirKey Server.
6. **Служебная учетная запись для работы с хранилищем данных** — учетная запись, у которой есть доступ на чтение и запись информации.
7. **Каталог пользователей** — каталог Active Directory, в котором хранятся данные о пользователях Indeed AM.
8. **Служебная учетная запись для работы с каталогом пользователя** — учетная запись, у которой есть доступ на чтение информации.



Размещение компонентов

Размещение 1

Наименование сервера	Требование	Компоненты Indeed AM	Описание
Indeed AM Server PC	Обязательный компонент.	Indeed AM Log Server	Данное размещение рекомендуется использовать при пилотных внедрениях, для ознакомления с системой и проведения демонстраций.
		Indeed AM Server	
		Indeed AM Management Console	
	Опциональный компонент.	Indeed AM Identity Provider	Все компоненты системы, требуемые провайдеры и модули интеграции устанавливаются на одной машине.
	Обязательный компонент. Тип метода аутентификации зависит от конечного сценария.	Indeed AM Providers	Модули интеграции Indeed могут быть развернуты на отдельных машинах.
	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	
	Опциональный компонент.	Indeed AM User Console	

Системные требования

Наименование сервера	CPU	RAM	HDD	Network
Indeed AM Server PC	4 cores	8 Gb	200Gb	100 Mb/s
Indeed AM External PC	4 cores	8 Gb	100Gb	100 Mb/s

Размещение 2

Наименование сервера	Требование	Компоненты Indeed AM
Indeed AM Server\Indeed AM Log Server	Обязательный компонент.	Indeed AM Server, Indeed AM Log
Indeed AM Server\Indeed AM Management Console\Indeed AM Identity Provider	Обязательный компонент. <i>Indeed AM Identity Provider обязателен только для сценариев, где требуется выполнять обучение аутентификаторов внешним пользователям.</i>	Indeed AM Server, Indeed AM Management Console, Indeed AM Identity Provider

Indeed AM Indeed Key Server\Indeed AM User Console	Опциональный компонент. <i>Indeed Key Server требуется только для сценариев с использованием Push аутентификации.</i> <i>Indeed AM User Console требуется для обучения аутентификаторов внешним пользователям системы.</i>	Indeed AM Indeed Key User Console
Indeed AM Indeed Key Server\Indeed AM User Console	Опциональный компонент. <i>Только для сценариев с использованием Push аутентификации.</i>	Indeed AM Indeed Key User Console
Indeed AM Extensions	Обязательный компонент. <i>Тип модуля интеграции зависит от конечного сценария.</i>	Модули интеграции
Балансировщик нагрузки	Системные требования зависят от выбранного балансировщика.	Балансировка осуществляется сторонними компонентами
Балансировщик нагрузки		

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 Gb	200Gb	100 Mb/s
Indeed AM Server\Indeed AM Management Console\Indeed AM Identity Provider	8 cores	8 Gb	200Gb	100 Mb/s
Indeed AM Indeed Key Server\Indeed AM User Console	8 cores	8 Gb	150Gb	100 Mb/s
Indeed AM Indeed Key Server\Indeed AM User Console	8 cores	8 Gb	150Gb	100 Mb/s
Indeed AM Extensions	Системные требования зависят от выбранного модуля интеграции			
ПК с БД Indeed и событиями Indeed 1	8 cores	8 Gb	500Gb	100 Mb/s
ПК с БД Indeed и событиями Indeed 2	8 cores	8 Gb	500Gb	100 Mb/s

Список реализуемых сценариев

Информация

На данной странице приведен список возможных сценариев с компонентами Indeed AM. Для поддержки различных сценариев системы требуется установка различных клиентских компонентов. Серверные компоненты Indeed Access Manager Server, Management Console, Log Server всегда устанавливаются независимо от сценария.

Строгая аутентификация на доменный ПК внутри корпоративной сети

Для поддержки данного сценария используется компонент [Indeed AM Windows Logon](#). Данный компонент позволяет реализовать строгую аутентификацию сотрудников в систему с использованием различных методов аутентификации: биометрические способы аутентификации, бесконтактные RFID карты, USB-ключи, контактные смарт-карты, одноразовые пароли, push-уведомления в мобильном приложении.

Все поддерживаемые методы аутентификации перечислены в разделе [Установка и настройка провайдеров](#).

Строгая аутентификация в целевых Web\Win приложениях

Для поддержки данного сценария используется компонент [Indeed AM ESSO Agent](#). Данный компонент реализует технологию единого доступа Single Sign On в информационные системы организации: централизованно хранит пароли приложений пользователя и выполняет автоматическую подстановку пароля в скрытом виде при необходимости доступа в приложение или выполнения других действий, требующих аутентификации с использованием различных методов аутентификации: биометрические способы аутентификации, бесконтактные RFID карты, USB-ключи, контактные смарт-карты, одноразовые пароли, push-уведомления в мобильном приложении.

Все поддерживаемые методы аутентификации перечислены в разделе [Установка и настройка провайдеров](#).

Двухфакторная\Однофакторная аутентификация в VPN

Для реализации сценариев поддержки VPN-клиентов используется компонент [Indeed AM NPS RADIUS Extension](#), который позволяет реализовать технологию двухфакторной\однофакторной аутентификации для RADIUS-совместимых сервисов и приложений. Поддерживаются различные методы аутентификации: одноразовые пароли, отправленные по SMS, email; одноразовые пароли, генерируемые на специальных устройствах; push-уведомления.

Примеры внедрения расширения

1. [Настройка Cisco ASA для аутентификации через Indeed NPS RADIUS Extension](#)
2. [Настройка FortiGate VM для двухфакторной аутентификации через Indeed NPS Radius Extension](#)
3. [Установка и настройка аутентификации по OTP в Citrix Netscaler](#)

Двухфакторная аутентификация в RDP-подключении

Для реализации сценария 2FA в RDP-подключении используется компонент [Indeed AM RDP Windows Logon](#).

В качестве второго фактора могут выступать мастер-пароль (**провайдер Passcode**), одноразовый пароль, сгенерированный мобильным приложением (**провайдер Software OTP**) или устройством, одноразовый пароль, отправленный по SMS или email или push-уведомления.

Двухфакторная аутентификация для приложений с поддержкой ADFS

Для реализации данного сценария используется компонент [Indeed AM ADFS Extension](#). Компонент **ADFS Extension** реализует провайдер мультифакторной аутентификации для сервера **Microsoft ADFS**, добавляя в процесс получения доступа второй фактор.

В качестве второго фактора могут выступать мастер-пароль (**провайдер Passcode**), одноразовый пароль, сгенерированный мобильным приложением (**провайдер Software OTP**) или устройством, одноразовый пароль, отправленный по SMS или email или push-уведомления.

Примеры внедрения расширения

1. [Настройка двухфакторной аутентификации для приложений опубликованных в WAP](#)
2. [Настройка двухфакторной аутентификации в AD FS для интеграции с Exchange Server 2016](#)
3. [Настройка двухфакторной аутентификации в Microsoft Office 365 при помощи Indeed AM ADFS Extension](#)

Двухфакторная аутентификация для приложений с поддержкой SAML

Для реализации данного сценария используется компонент [Indeed AM Identity Provider](#).

В качестве второго фактора могут выступать мастер-пароль (**провайдер Passcode**), одноразовый пароль, сгенерированный мобильным приложением (**провайдер Software OTP**) или устройством, одноразовый пароль, отправленный по SMS или email или push-уведомления.

Установка системы

В разделе описаны подготовка к установке, установка и настройка компонентов Indeed Access Manager

- [Системные требования](#)
- [Подготовка](#)
- [Порядок установки](#)
- [Установка и настройка](#)

Системные требования

В разделе описаны программно-аппаратные требования к компонентам Indeed Access Manager, требующим взаимодействия.

- [Системные требования серверных компонентов](#)
- [Системные требования модулей интеграции](#)
- [Системные требования клиентских компонентов](#)
- [Сетевое взаимодействие](#)

Системные требования серверных компонентов

- [Требования Indeed AM Log Server](#)
- [Требования Indeed Access Manager Server](#)
- [Требования Indeed AM Management Console](#)
- [Требования Indeed AM User Console](#)
- [Требования Indeed Key Server](#)
- [Требования Indeed AM Phone Management Server](#)

Требования Indeed AM Log Server

Программные требования

Операционная система:

- Windows Server 2012 R2 или выше

Internet Information Services 7.0 и выше со следующими модулями:



Информация

Для автоматической установки всех необходимых компонентов сервера IIS воспользуйтесь скриптом PowerShell, включенным в состав дистрибутива.

- Статическое содержимое (Static Content)
- Перенаправление HTTP (HTTP Redirection)
- ASP.NET
- Расширяемость .NET (.NET Extensibility)
- Расширения ISAPI (ISAPI Extensions)
- Фильтры ISAPI (ISAPI Filters)
- Обычная проверка подлинности (Basic Authentication)
- Windows-проверка подлинности (Windows Authentication)
- Консоль управления службами IIS (IIS Management Console)

Компоненты Microsoft:

- Microsoft .NET Framework 4.6.1

Microsoft SQL Server:

- Microsoft SQL Server 2012 всех редакций и более новые версии (При использовании хранилища в SQL)

PostgreSQL:

- PostgreSQL и PostgreSQL Pro версии 10 и выше.

Аппаратные требования

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

Требования Indeed Access Manager Server

Программные требования

Домен:

- Active Directory

Операционная система:

- Windows Server 2012 R2 или выше

Internet Information Services 7.0 и выше со следующими модулями:



Информация

Для автоматической установки всех необходимых компонентов сервера IIS воспользуйтесь скриптом PowerShell, включенным в состав дистрибутива.

- Статическое содержимое (Static Content)
- Перенаправление HTTP (HTTP Redirection)
- ASP.NET
- Расширяемость .NET (.NET Extensibility)
- Расширения ISAPI (ISAPI Extensions)
- Фильтры ISAPI (ISAPI Filters)
- Обычная проверка подлинности (Basic Authentication)
- Windows-проверка подлинности (Windows Authentication)
- Консоль управления службами IIS (IIS Management Console)

Компоненты Microsoft:

- Microsoft .NET Framework 4.5.2

Microsoft SQL Server:

- Microsoft SQL Server 2012 всех редакций и более новые версии

PostgreSQL:

- PostgreSQL, PostgreSQL Pro

Аппаратные требования

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

Требования Indeed AM Management Console

Программные требования

Информация

Если для входа в Management Console используется Windows Authentication, то машина должна находиться в домене.

Операционная система:

- Windows Server 2012 R2 или выше

Internet Information Services 7.0 и выше со следующими модулями:

Информация

Для автоматической установки всех необходимых компонентов сервера IIS воспользуйтесь скриптом PowerShell, включенным в состав дистрибутива.

- Статическое содержимое (Static Content)
- Перенаправление HTTP (HTTP Redirection)
- ASP.NET
- Расширяемость .NET (.NET Extensibility)
- Расширения ISAPI (ISAPI Extensions)
- Фильтры ISAPI (ISAPI Filters)
- Обычная проверка подлинности (Basic Authentication)
- Windows-проверка подлинности (Windows Authentication)
- Консоль управления службами IIS (IIS Management Console)

Компоненты Microsoft:

- Microsoft .NET Framework 4.8 и выше.

Web-браузер актуальной версии:

- Chrome
- Firefox
- MS Edge
- IE

Аппаратные требования

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

Требования Indeed AM User Console

Программные требования

Информация

Если для входа в User Console используется Windows Authentication, то машина должна находиться в домене.

Операционная система:

- Windows Server 2012 R2 или выше

Internet Information Services 7.0 и выше со следующими модулями:

Информация

Для автоматической установки всех необходимых компонентов сервера IIS воспользуйтесь скриптом PowerShell, включенным в состав дистрибутива.

- Статическое содержимое (Static Content)
- Перенаправление HTTP (HTTP Redirection)
- ASP.NET
- Расширяемость .NET (.NET Extensibility)
- Расширения ISAPI (ISAPI Extensions)
- Фильтры ISAPI (ISAPI Filters)
- Обычная проверка подлинности (Basic Authentication)
- Windows-проверка подлинности (Windows Authentication)
- Консоль управления службами IIS (IIS Management Console)

Компоненты Microsoft:

- Microsoft .NET Framework 4.5.2

Web-браузер актуальной версии:

- Chrome
- Firefox
- MS Edge
- IE

Аппаратные требования

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

Требования Indeed Key Server

Информация

Сервер поддерживает работу вне домена.

Программные требования

Операционная система:

- Windows Server 2012 R2 или выше

Internet Information Services 7.0 и выше со следующими модулями:

- Статическое содержимое (Static Content)
- Перенаправление HTTP (HTTP Redirection)
- ASP.NET 4.6
- Расширяемость .NET (.NET Extensibility)
- Расширения ISAPI (ISAPI Extensions)
- Фильтры ISAPI (ISAPI Filters)
- Windows-проверка подлинности (Windows Authentication)
- Консоль управления службами IIS (IIS Management Console)

Информация

Для автоматической установки всех необходимых компонентов сервера IIS воспользуйтесь скриптом PowerShell, включенным в состав дистрибутива.

Компоненты Microsoft:

- Microsoft .NET Framework 4.5.2

Microsoft SQL Server:

- 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

Для взаимодействия с мобильным приложением Indeed Key:

- Для отправки push-уведомлений серверу Indeed Key требуется внешний доступ к интернету (для доступа к [fcm.googleapis.com:443](https://fcm.googleapis.com)).
- Сервер Indeed Key должен быть доступен по указанному в настройках **dns имени** и **порту** (данные параметры задаются при настройке Indeed Key Server) из внешней сети.
- На сервере Indeed Key должен быть включён TLS 1.2 или TLS 1.3.
- DNS-имя 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

Аппаратные требования

- Не менее 8 ГБ оперативной памяти
- Не менее 200 ГБ свободного дискового пространства
- Аппаратные требования совпадают с требованиями, предъявляемыми к операционным системам, на которых функционирует ПО

Требование к сертификатам для iOS устройств



Информация

Сертификат должен быть на устройстве, и должно быть доверие со стороны смартфона.



Информация

Требования 4 и 5 появились осенью 2019 года для сертификатов, выпущенных после 1 июля 2019. Сертификаты, выпущенные ранее, принимаются устройствами iOS без указания идентификатора объекта и сроком действия.

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

Требования Indeed AM Phone Management Server

Операционная система:

- Windows Server 2012 R2 или выше

Internet Information Services 7.0 и выше со следующими модулями:



Информация

Для автоматической установки всех необходимых компонентов сервера IIS воспользуйтесь скриптом PowerShell, включенным в состав дистрибутива.

- Статическое содержимое (Static Content)
- Перенаправление HTTP (HTTP Redirection)
- ASP.NET
- Расширяемость .NET (.NET Extensibility)
- Расширения ISAPI (ISAPI Extensions)
- Фильтры ISAPI (ISAPI Filters)
- Обычная проверка подлинности (Basic Authentication)
- Консоль управления службами IIS (IIS Management Console)
- Авторизация URL-адреса (URL Authorization) — установка данного компонента не входит в скрипт Powershell с автоматической установкой компонентов IIS.

Компоненты Microsoft:

- Microsoft .NET Framework 4.5.2
- Web Deploy Package (<https://go.microsoft.com/?linkid=9278654>)

Аппаратные требования

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

Системные требования модулей интеграции

Программные требования

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



Не рекомендуется на одном сервере устанавливать **только один** из следующих компонентов:

- ADFS Extension,
- IIS Extension,
- RDP Windows Logon,
- NPS Radius Extension.

Одновременное размещение этих компонентов приведет к ошибке.

Требования для Indeed AM ADFS Extension

- Операционная система:
 - Windows Server 2012 R2 или выше
- Установленная роль **Active Directory Federation Services**

Требования для Indeed AM NPS RADIUS Extension

- Операционная система:
 - Windows Server 2012 R2 или выше
- Установленная роль **Network Policy Server**

Требования для Indeed AM IIS Extension

- Операционная система:
 - Windows Server 2012 R2 или выше

- Установленный сервер Internet Information Services

Требования для Indeed AM RDP Windows Logon

- Операционная система:
 - Windows Server 2012 R2 или выше
 - Windows 7 32/64bit
 - Windows 8.1 32/64bit
 - Windows 10 32/64bit

Требования для Indeed AM Identity Provider

- Операционная система:
 - Windows Server 2012 R2 или выше



Информация

Для автоматической установки всех необходимых компонентов сервера IIS воспользуйтесь скриптом PowerShell, включенным в состав дистрибутива

- **Internet Information Services 7.5** и выше со следующими модулями:
 - Статическое содержимое (Static Content)
 - Стандартный документ (Default Document)
 - Обзор каталогов (Directory Browsing)
 - Ошибки HTTP (HTTP Errors)
 - Перенаправление HTTP (HTTP Redirection)
 - Веб-публикация DAV (WebDAV Publishing)
 - ASP.NET
 - Расширяемость .NET (.NET Extensibility)
 - ASP
 - CGI
 - Расширения ISAPI (ISAPI Extensions)
 - Фильтры ISAPI (ISAPI Filters)
 - Включения на стороне сервера (SSI) (Server Side Includes)
 - Ведение журнала HTTP (HTTP Logging)
 - Средства ведения журналов (Logging Tools)
 - Монитор запросов (Request Monitor)
 - Слежение (Tracing)
 - Обычная проверка подлинности (Basic Authentication)
 - Windows-проверка подлинности (Windows Authentication)
 - Дайджест-проверка подлинности (Digest Authentication)
 - Проверка подлинности с сопоставлением сертификата клиента (Client Certificate Mapping Authentication)
 - Проверка подлинности с сопоставлением сертификата клиента IIS (IIS Client Certificate Mapping Authentication)
 - Авторизация URL-адресов (URL Authorization) и Фильтрация запросов (Request Filtering)
 - Ограничения по IP-адресам и доменам (IP and Domain Restrictions)
 - Сжатие статического содержимого (Static Content Compression)
 - Сжатие динамического содержимого (Dynamic Content Compression)
 - Консоль управления IIS (IIS Management Console)
 - Сценарии и средства управления IIS (IIS Management Scripts and Tools)
 - Служба управления (Management Service)
- Компоненты Microsoft:
 - Microsoft .NET 4.8
 - Для Windows Server 2012 R2 необходимо включить компоненты:
 - Активация по HTTP (HTTP Activation)
 - Активация по MSMQ (Message Queuing Activation)
 - Активация по TCP (TCP Activation)
 - Совместное использование портов TCP (TCP Port Sharing)

- 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

Требования Indeed AM Windows® Logon

Аппаратные требования к рабочим станциям пользователей

- Не менее 50 МБ свободного дискового пространства
- 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 Server 2012 R2 или выше

Требования Indeed AM ESSO Агент

Аппаратные требования к рабочим станциям пользователей

- Не менее 50 МБ свободного дискового пространства
- Наличие .net framework версии 4.5 и выше
- **Веб-браузеры**
 - Internet Explorer 8 и выше
 - Mozilla Firefox 52.6 и выше
 - Google Chrome 49.0 и выше
- USB-порт для подключения устройства аутентификации

Поддерживаемые операционные системы

- Windows Server 2012 R2 или выше
- Windows 7 SP1 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

Системные требования клиентских компонентов

Требования Indeed AM Windows® Logon

Аппаратные требования к рабочим станциям пользователей

- Не менее 50 МБ свободного дискового пространства
- 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 Server 2012/2012 R2
- Windows Server 2016
- Windows Server 2019

Требования к окружению

Для корректной работы Indeed AM Windows® Logon необходимо следующее окружение:

- **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 AM Windows® Logon требуются права **Локального Администратора** (Administrator).

Настройки межсетевого экрана

Для корректной работы системы Indeed AM необходимо изменить следующие настройки межсетевого экрана на Indeed AM Server и на рабочих станциях, на которых установлен компонент Indeed AM Windows® Logon:

1. **Открыть порт 53 (DNS) (TCP и UDP)** для всех процессов в обоих направлениях. Этот порт используется системой Indeed AM для определения наличия сети.
2. **Открыть порт 135 (RPC)** для всех процессов в обоих направлениях. Этот порт используется системой для коммуникации между рабочими станциями пользователей и Indeed AM Server.
3. **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 Indeed AM Server).

Требования Indeed AM ESSO Агент

Аппаратные требования к рабочим станциям пользователей

- Не менее 50 МБ свободного дискового пространства
- Наличие .net framework версии 4.5 и выше
- **Веб-браузеры**
 - Internet Explorer 8 и выше
 - Mozilla Firefox 52.6 и выше
 - Google Chrome 49.0 и выше
- USB-порт для подключения устройства аутентификации

Поддерживаемые операционные системы

- Windows Server 2012/2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows 7 SP1 32/64bit
- Windows 8.1 32/64bit
- Windows 10 32/64bit

Настройки межсетевого экрана

Задайте следующие настройки межсетевого экрана на сервере Indeed ESSO и на рабочих станциях с установленным Indeed AM ESSO Агент:

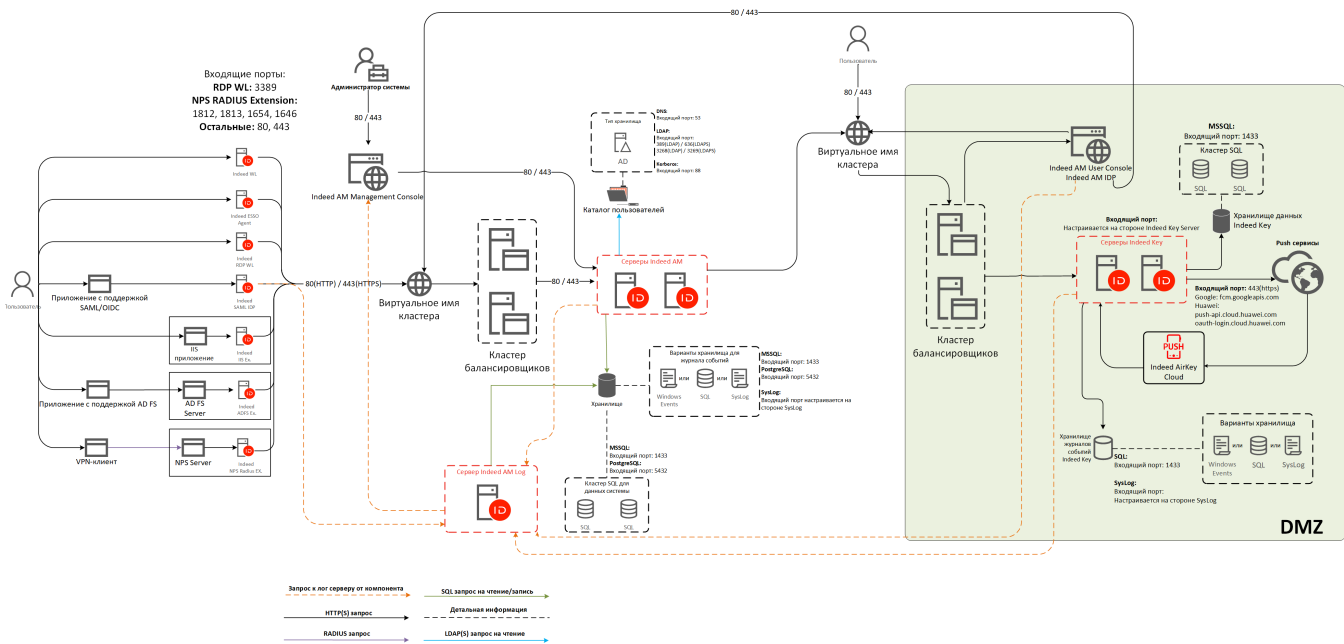
1. **Откройте порт 53 DNS (TCP и UDP)** для всех процессов в обоих направлениях. Этот порт используется для определения наличия сети.
2. **Открыть порт 135 (RPC)** для всех процессов в обоих направлениях. Этот порт используется для обмена данными между рабочими станциями пользователей и Indeed AM Enterprise Server.
3. **Открыть порт 389 (LDAP)** для всех процессов в обоих направлениях. Этот порт используется для получения доступа в Active Directory (в том числе при поиске Indeed AM Enterprise Server).

Сетевое взаимодействие

Информация

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

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



Информация

Взаимодействие между основными компонентами Indeed AM в сетевой инфраструктуре осуществляется через http\https протоколы.

Наименование	Протокол	Входящий порт	Исходящий порт
Indeed Access Manager 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 (MS SQL)	TCP/UDP	1433	49152- 65535
Indeed AM Log Сервер (PostgreSQL)	TCP/UDP	5432	49152- 65535
MS SQL База Данных Indeed AM	TCP/UDP	1433	49152- 65535
PostgreSQL База Данных Indeed AM	TCP/UDP	5432	49152- 65535
Active Directory	DNS	53	49152- 65535
	LDAP	389 (LDAP) / 636 (LDAPS) 3268 (LDAP) / 3269 (LDAPS)	49152- 65535
	Kerberos	88	49152- 65535
Indeed AM Indeed Key Server	TCP/UDP	Настраивается на стороне сервера АК	49152- 65535
MS SQL База Данных Indeed AM Indeed Key Server	TCP/UDP	1433	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 IIS Extension	TCP/UDP	80(http) 443(https)	49152- 65535
Indeed AM NPS RADIUS 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

Подготовка

Перед установкой Indeed Access Manager вы должны выполнить следующие действия:

- [Установите компоненты Internet Information Services](#). Компоненты нужны для корректной работы всей системы Indeed Access Manager.
- [Создайте базы данных для компонентов Indeed AM Server и Indeed AM Log Server](#). Если вы планируете использовать пуш-нотификации, создайте отдельную базу данных для компонента Indeed AM AirKey Server.
- [Определите каталог пользователей в Active Directory](#). В нем будут храниться данные о конечных пользователях Indeed Access Manager.
- [Добавьте клиентский сертификат в доверенное хранилище сертификатов](#). Сертификат проверяет запросы от модулей интеграции к серверу.



Информация

Для установки и настройки основных компонентов системы выделите учетную запись с правами локального администратора.

Установка компонентов Internet Information Services

Перед установкой любого модуля Indeed Access Manager вы должны установить необходимые компоненты Internet Information Services.

Вы можете установить компоненты Internet Information Services с помощью скрипта Powershell, который вы найдете в составе дистрибутива Indeed Access Manager, либо вручную. Список необходимых компонентов Internet Information Services вы можете найти в [системных требованиях](#) к модулям.



Примечание

Запустите Powershell от имени администратора.

Чтобы найти скрипт, откройте папку с дистрибутивом Indeed Access Manager, перейдите в папку *Misc\IISScripts*.

Запустите скрипт *Indeed.Main.IIS.Install.MSServer.ps1* в Powershell.

Дистрибутив Indeed Access Manager распространяется с двумя версиями скриптов Powershell для Windows Server 2008 и Windows Server 2012 и более поздних версий.

Чтобы найти скрипты, откройте папку с дистрибутивом Indeed Access Manager, перейдите в папку *Misc*.

В папке *Server 2008* вы найдете скрипт *Indeed.AdminConsole.IIS.Install.MSServer2008.ps1* для установки всех компонентов Internet Information Services.

В папке *Server 2012* вы найдете следующие скрипты:

- *Indeed.AdminConsole.IIS.Install.MSServer2012.ps1* — скрипт для установки компонентов IIS для модуля Indeed AM Management Console.
- *Indeed.SAML.IIS.Install.MSServer2012.ps1* — скрипт для установки компонентов IIS для модуля Indeed AM SAML IDP.
- *Indeed.SelfService.IIS.Install.MSServer2012.ps1* — скрипт для установки компонентов IIS для модуля Indeed AM User Console.

Создание и настройка хранилища данных

Для работы Indeed Access Manager нужны две базы данных. В одной из баз данных хранится информация для компонента [Indeed AM Server](#). В другой — для компонента [Indeed AM Log Server](#).

Если вы планируете использовать пуш-нотификации, вам необходима отдельная база данных для [Indeed AM AirKey Server](#).

Также необходимо создать сервисного пользователя, от имени которого будут выполняться запросы на чтение и запись информации.

Indeed Access Manager поддерживает Microsoft SQL для следующих компонентов:

- Indeed AM Server
- Indeed AM Log Server
- Indeed AM AirKey Server

PostgreSQL подходит для следующих компонентов:

- Indeed AM Server
- Indeed AM Log Server

В этом разделе

- [Хранилище данных Microsoft SQL](#)
- [Хранилище данных PostgreSQL](#)

Хранилище данных Microsoft SQL

На сервере с установленным Microsoft SQL Server создайте две базы данных — одну для Indeed AM Server, другую для Indeed AM Log Server — и сервисную учетную запись.

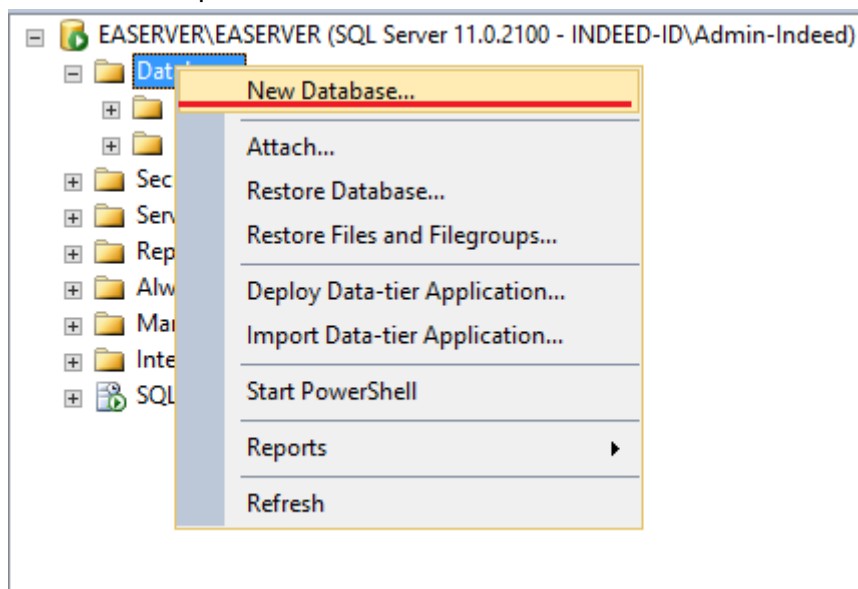
⚠ Важно!

Если вы планируете использовать пуш-нотификации, вам нужна еще одна база данных для Indeed AM AirKey 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 и нажмите **ОК**.

Database name: EA_Server_7.0

Owner: <default>

☒ Use full-text indexing

Database files:

Logical Name	File Type	Filegroup	Initial Size (MB)	Autogrowth / Maxsize
EA_Server_...	Rows ...	PRIMARY	5	By 1 MB, Unlimited
EA_Server_...	Log	Not Applicable	1	By 10 percent, Unlimited

Buttons: Add, Remove, OK, Cancel

Создание сервисной учетной записи

Indeed Access Manager поддерживает сервисные учетные записи с режимом проверки подлинности Windows и с режимом проверки подлинности SQL Server.



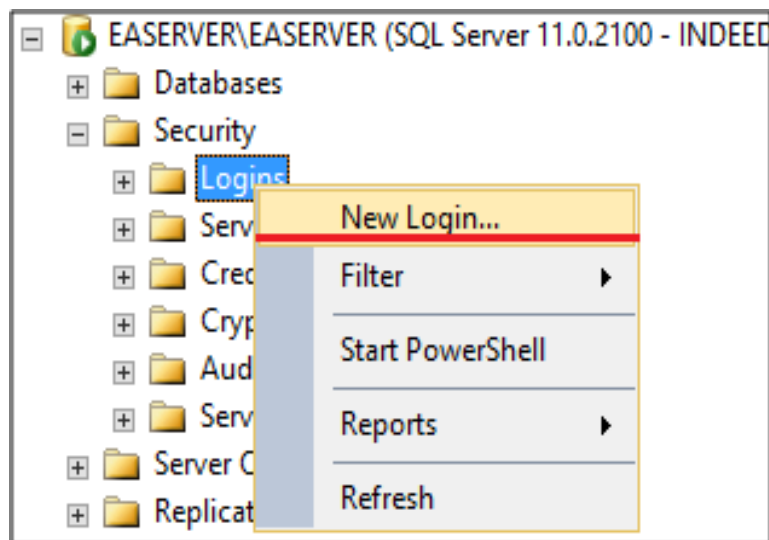
Важно!

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 сбой в работе.

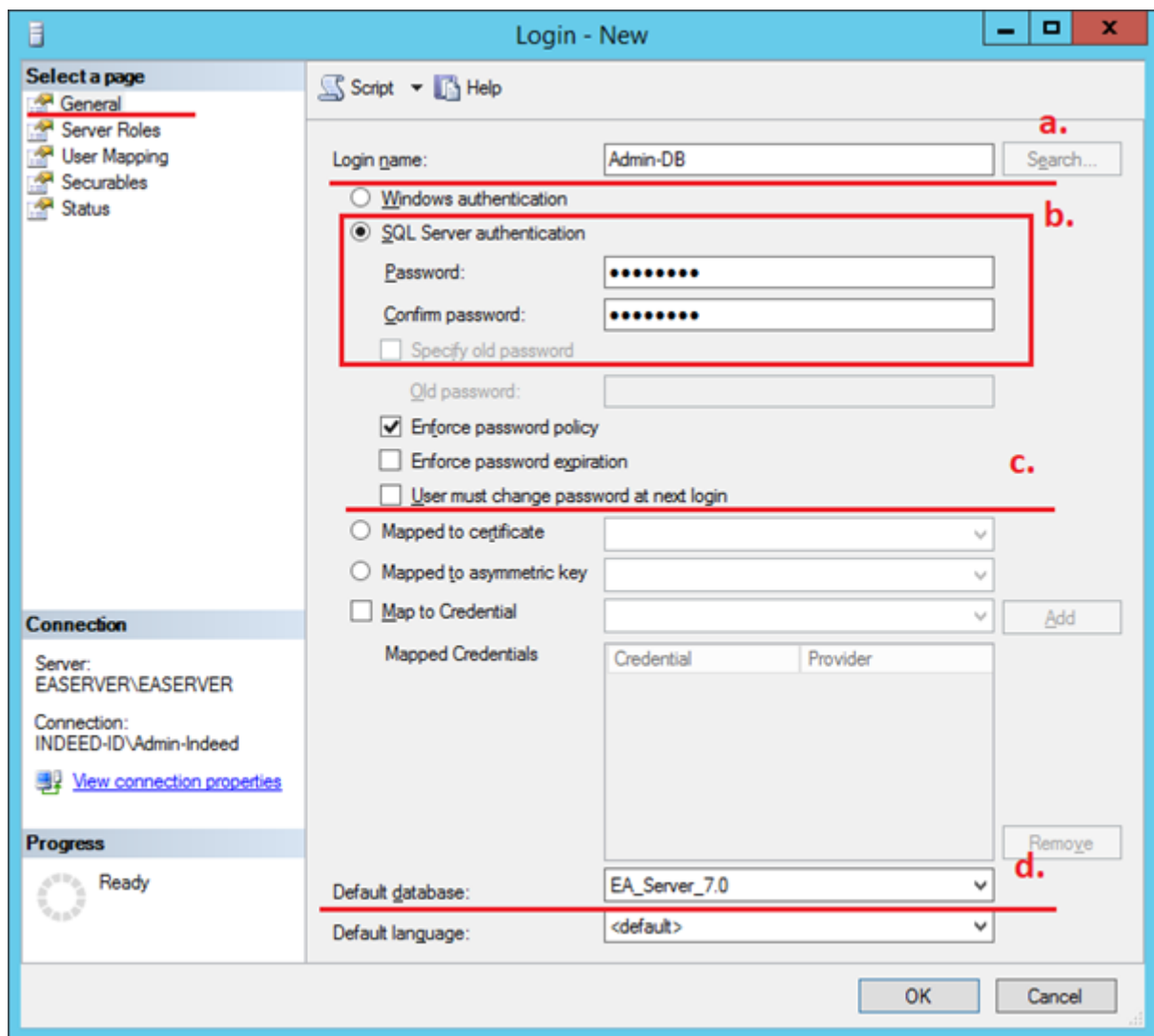
Создание сервисной учетной записи с режимом проверки подлинности SQL Server

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:
 - a. Введите имя пользователя.
 - b. Выберите опцию **SQL Server authentication**.
 - c. Отключите опцию **Enable password policy**.
 - d. В меню слева выберите **User Mapping**.
 - e. Выберите ранее созданные базы.
 - f. Для каждой базы выберите роль **db_owner** и нажмите **OK**.



Создание сервисной учетной записи с режимом проверки подлинности Windows

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

1. Создайте доменную учетную запись.
2. Откройте SQL Server Management Studio и подключитесь к серверу.
3. Раскройте узел **Security**.
4. Правой кнопкой мыши нажмите узел **Logins**.
5. В появившемся окне выберите **New Login**.

6. В окне **Login - New** выполните следующие действия:
 - a. Найдите ранее созданного пользователя.
 - b. В меню слева выберите **User Mapping**.
 - c. Выберите ранее созданные базы.
 - d. Для каждой базы выберите роль **db_owner** и нажмите **OK**.

7. Откройте в текстовом редакторе конфигурационный файл компонента, для которого вы создаете базу:
 - a. Файл для компонента Indeed AM Server хранится в *C:\inetpub\wwwroot\am\core\Web.config*.
 - b. Файл для компонента Indeed AM Log Server хранится в *C:\inetpub\wwwroot\ls\targetConfigs\sampleDb.config*.
8. В теге *connectionString* укажите значение *Integrated Security=SSPI*.

Пример для Indeed AM Server

```
<mssqlDbContexts>
  <mssqlDbContext connectionString="Data Source=SERVER\SQLEXPRESS;Initial
  Catalog=am8;Integrated Security=SSPI" id="mssql" />
</mssqlDbContexts>
```

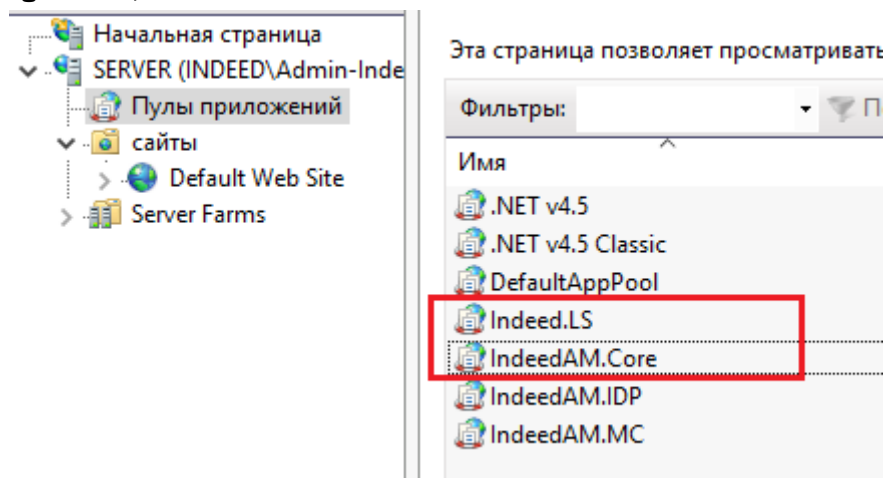
Пример для Indeed AM Log Server

```
<Settings>
  <ConnectionString>Data Source=SERVER\SQLEXPRESS;Initial Catalog=Log81;Integrated
  Security=SSPI</ConnectionString>
</Settings>
```

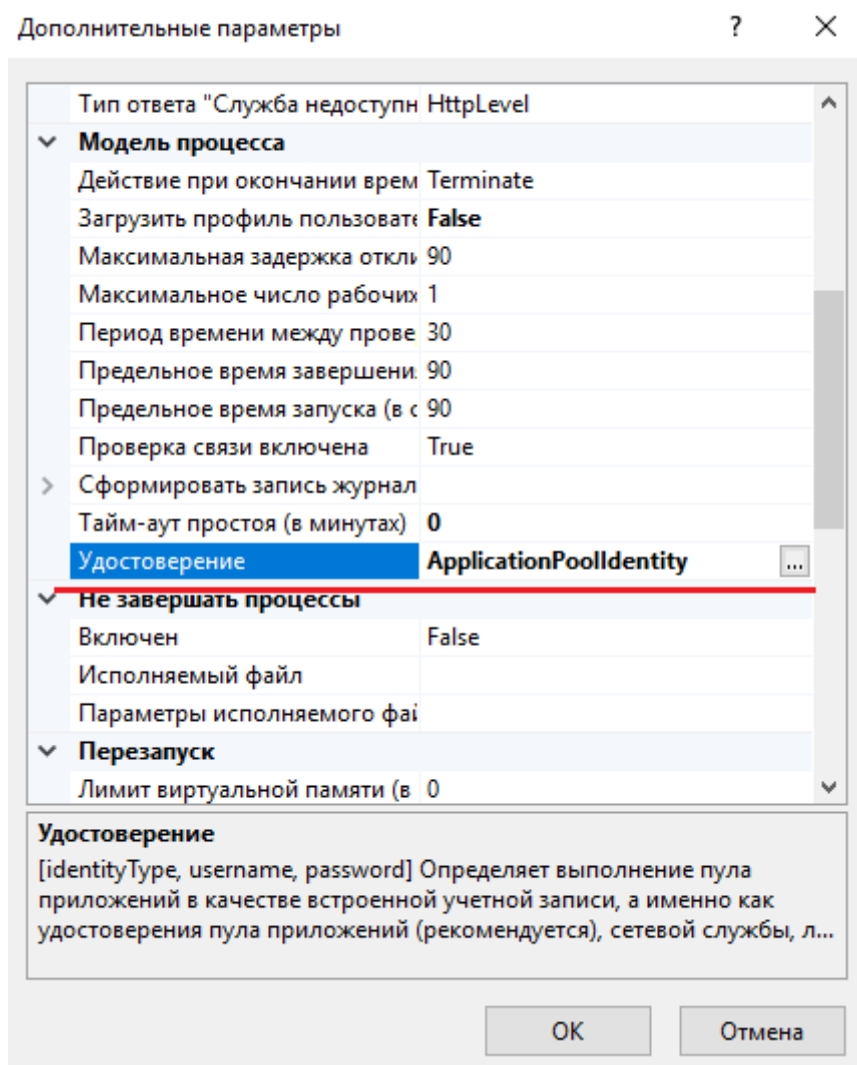
9. Сохраните конфигурационный файл.

Далее настройте пулы приложений в Internet Information Services.

1. Запустите Диспетчер служб IIS.
2. Выберите **Пулы приложений** **IndeedAM.Core** (для Indeed AM Server)**Indeed.LS** (для Indeed AM Log Server).

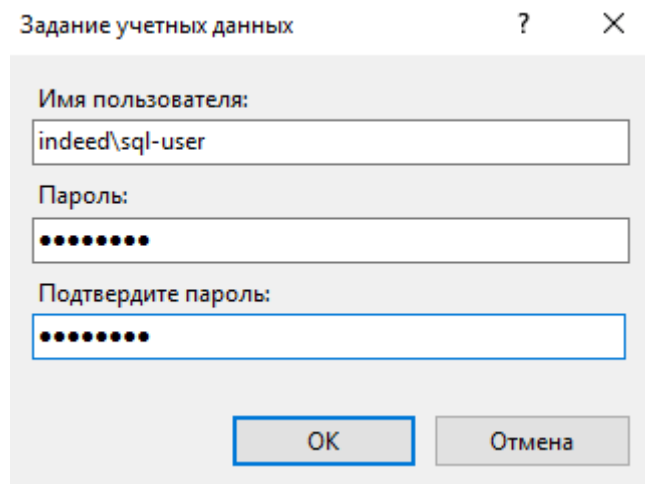


3. В разделе **Действия** выберите **Дополнительные параметры**.
4. В окне **Дополнительные параметры** найдите параметр **Удостоверение** и нажмите кнопку справа.



5. В окне **Удостоверение пула приложений** выберите **Особая учетная запись** и нажмите **Установить...**

6. Задайте учетную запись с указанием домена и нажмите **ОК**.



Задание учетных данных

Имя пользователя:
indeed\sql-user

Пароль:
●●●●●●

Подтвердите пароль:
●●●●●●

ОК Отмена

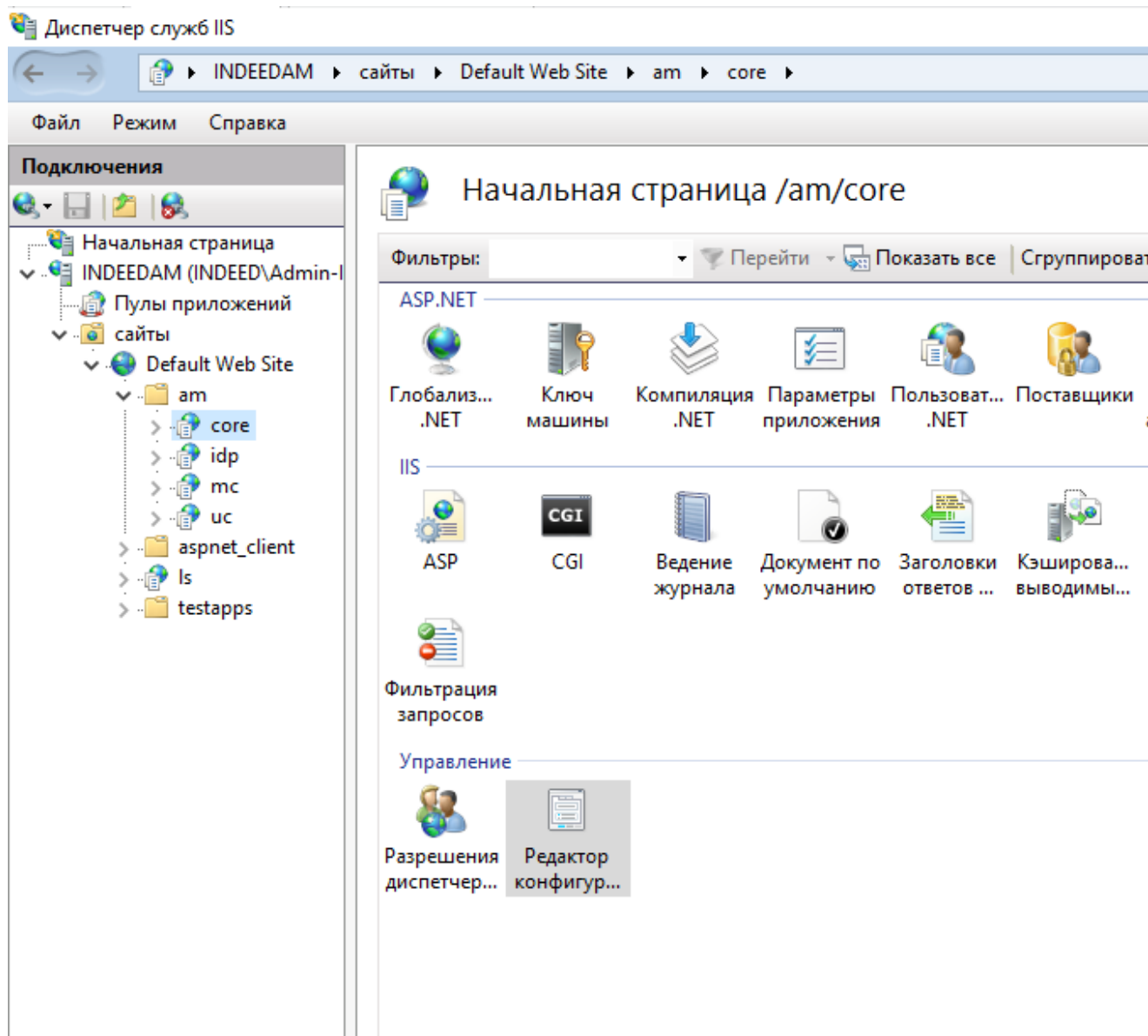
7. В разделе **Действия** перезапустите пул приложения, для которого выполнялась настройка, и откройте начальную страницу приложения в IIS.
8. Выберите настраиваемый серверный компонент Indeed в IIS.

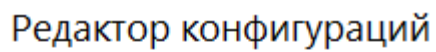


Информация

Если настройка выполняется и для IndeedAM.Core, и для Indeed.LS, то действия необходимо выполнить для каждого компонента

9. В разделе **Управление** выберите **Редактор конфигурации** и откройте *system.webServer/security/authentication/windowsAuthentication*.
10. Для параметра *useAppPoolCredentials* установите значение **True** и нажмите **Применить** в блоке **Действия**.
11. Перезапустите сервер IIS.





▼ Οτ: Applicationt

e/am/core

Хранилище данных PostgreSQL

Это хранилище данных подходит только для Indeed AM Server и Indeed AM Log Server. Если вы планируете создать базу данных для Indeed AM AirKey Server, создайте [хранилище Microsoft SQL](#).

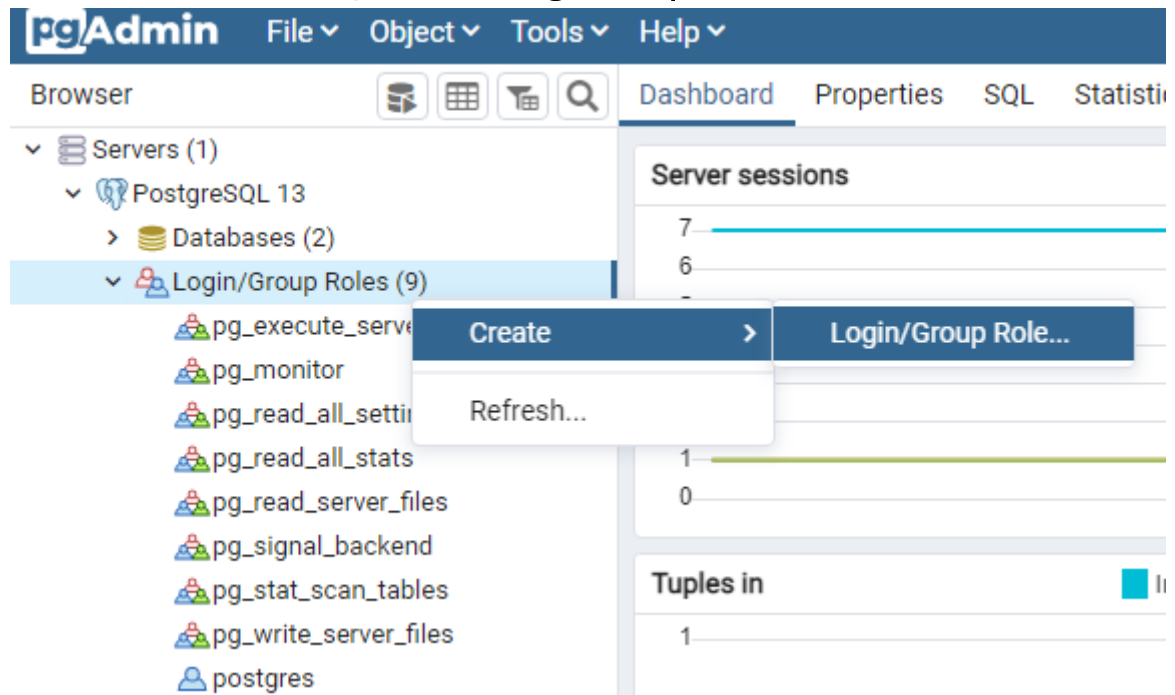
Создайте две базы данных и сервисную учетную запись.

Если базы данных и сервер Indeed AM находятся на разных машинах, вы должны настроить удаленное подключение к базе данных.

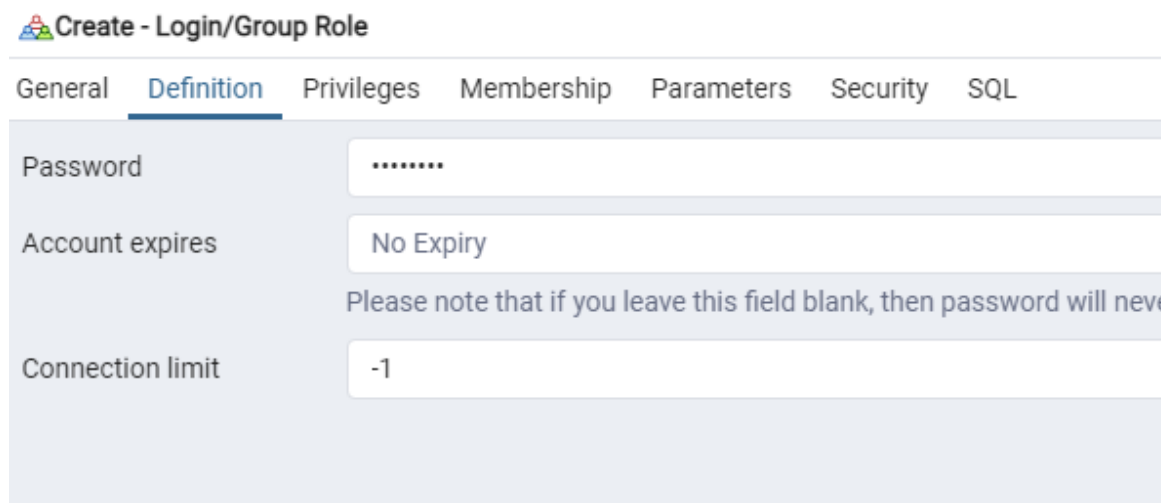
Создание сервисной учетной записи

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 **CreateLogin/Group Role...**



4. В окне **Create-Login/Group Role** выполните следующие действия:
 - а. На вкладке **General** в поле **Name** введите имя пользователя.
 - б. На вкладке **Definition** в поле **Password** введите пароль. В поле **Account Expires** укажите значение **No expiry**.



- с. На вкладке **Privileges** включите опцию **Can login?** и нажмите **Save**.

Create - Login/Group Role

General

Definition

Privileges

Membership

Parameters

Security

SQL

Can login?

Yes

Superuser?

No

Create roles?

No

Create databases?

No

Update catalog?

No

Inherit rights from the parent roles?

Yes

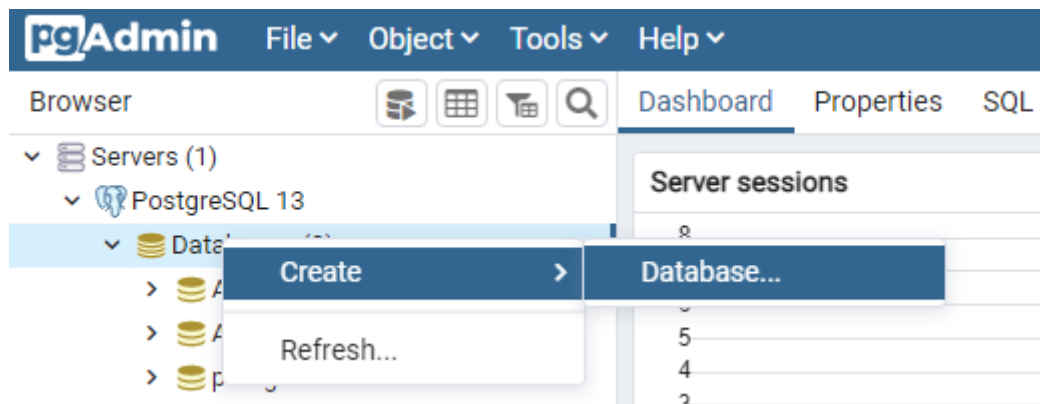
Can initiate streaming replication and backups?

No

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 **CreateDatabase...**



5. В окне **Create-Database** выполните следующие действия:
 - а. В поле **Database** введите имя базы данных.
 - б. В поле **Owner** из списка выберите ранее созданного пользователя и нажмите **Save**.

 The screenshot shows the 'Create - Database' dialog box. It has tabs for 'General', 'Definition', 'Security', 'Parameters', 'Advanced', and 'SQL'. The 'General' tab is active. It contains three fields: 'Database' with the value 'AMdatabase', 'Owner' with a dropdown menu showing 'IndeedDB' selected, and a large empty text area for 'Comment'.

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 md5
```

- i. *host* — тип подключения. Если вы не указываете тип подключения, по умолчанию используется подключение по TCP/IP.
- ii. *databaseName* — имя базы данных, для которой вы настраиваете подключение.
- iii. *UserName* — имя пользователя, который будет подключаться к этой базе данных.
- iv. *HostIP* — IP-адрес машины, на которой установлен компонент Indeed AM. Укажите значение с маской.
- v. *md5* — метод аутентификации пользователя.

Пример

```
host all all 192.168.1.0/24 md5
```

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

Indeed Access Manager использует данные о конечных пользователях из Active Directory. Это те пользователи, которые будут проходить процедуру аутентификации с помощью Indeed Access Manager.

Чтобы данные о пользователях появились в Indeed Access Manager, вы должны подготовить в Active Directory объект с конечными пользователями и создать сервисную учетную запись, от имени которой будут читаться данные.

Вы можете настроить отдельное подразделение пользователей, либо использовать домен пользователей целиком.



Важно!

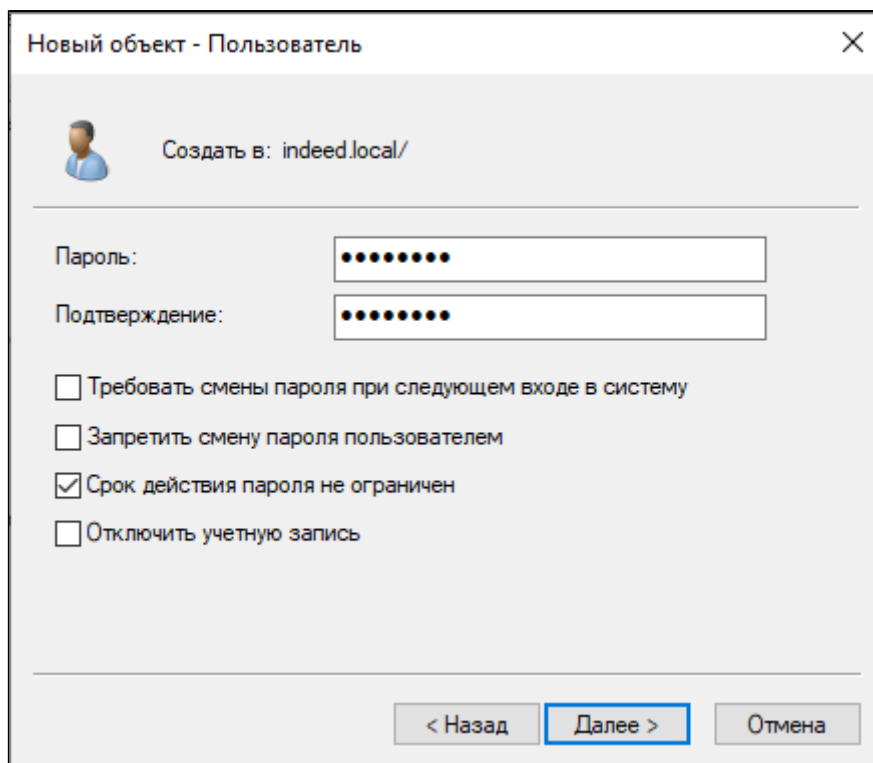
Если вы планируете использовать отдельное подразделение, то все необходимые объекты — группы, администраторы, конечные пользователи — должны находиться внутри этого подразделения.

Indeed Access Manager только читает данные из Active Directory, новые данные не записываются.

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**.



Новый объект - Пользователь

Создать в: indeed.local/

Пароль:

Подтверждение:

☐ Требовать смены пароля при следующем входе в систему

☐ Запретить смену пароля пользователем

☒ Срок действия пароля не ограничен

☐ Отключить учетную запись

< Назад **Далее >** Отмена

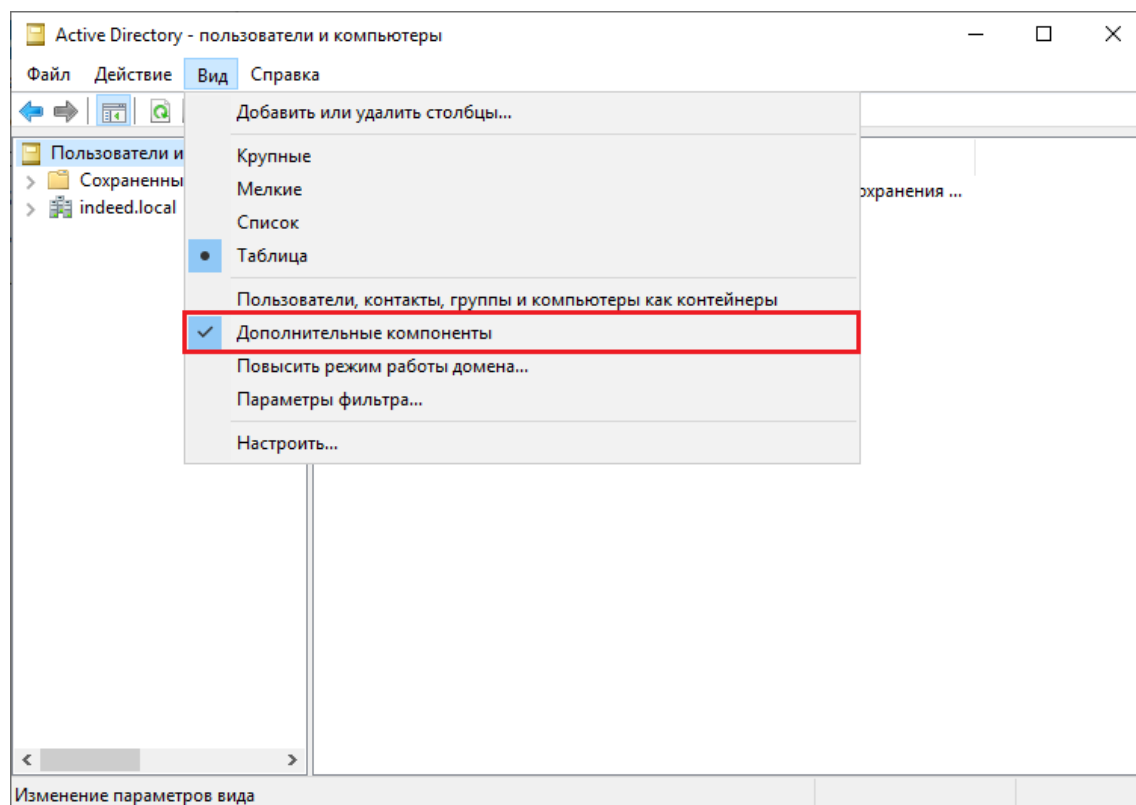
Предоставление прав на чтение данных

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:

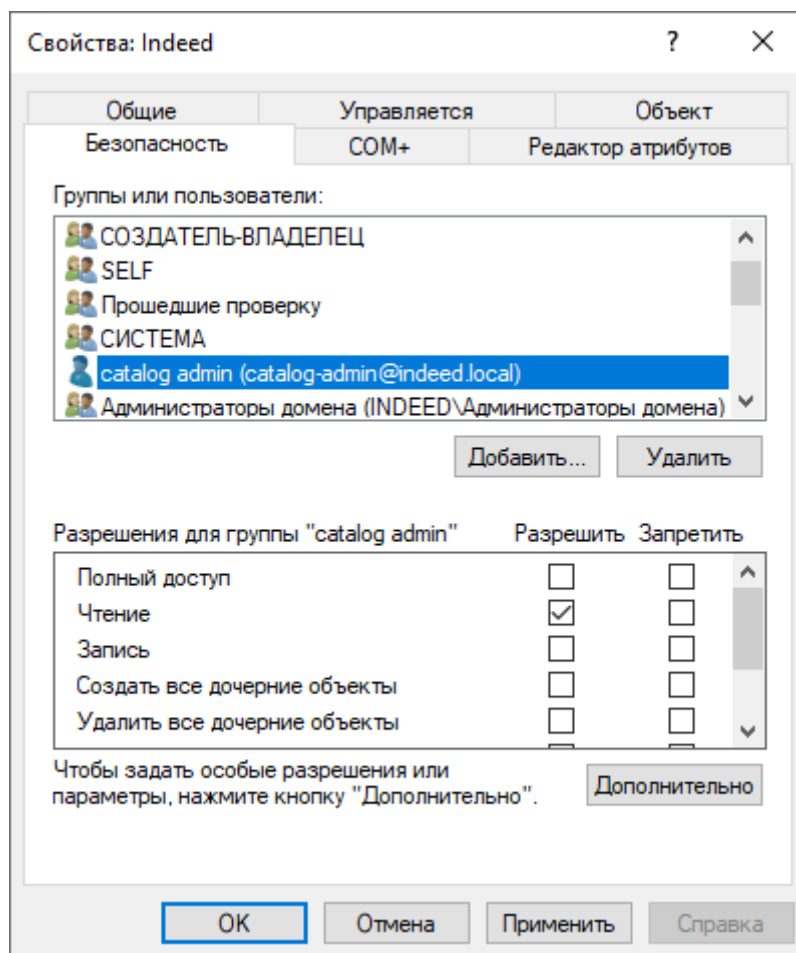
1. Откройте Active Directory Users and Computers.

2. Во вкладке **View** включите опцию **Advanced Features**.

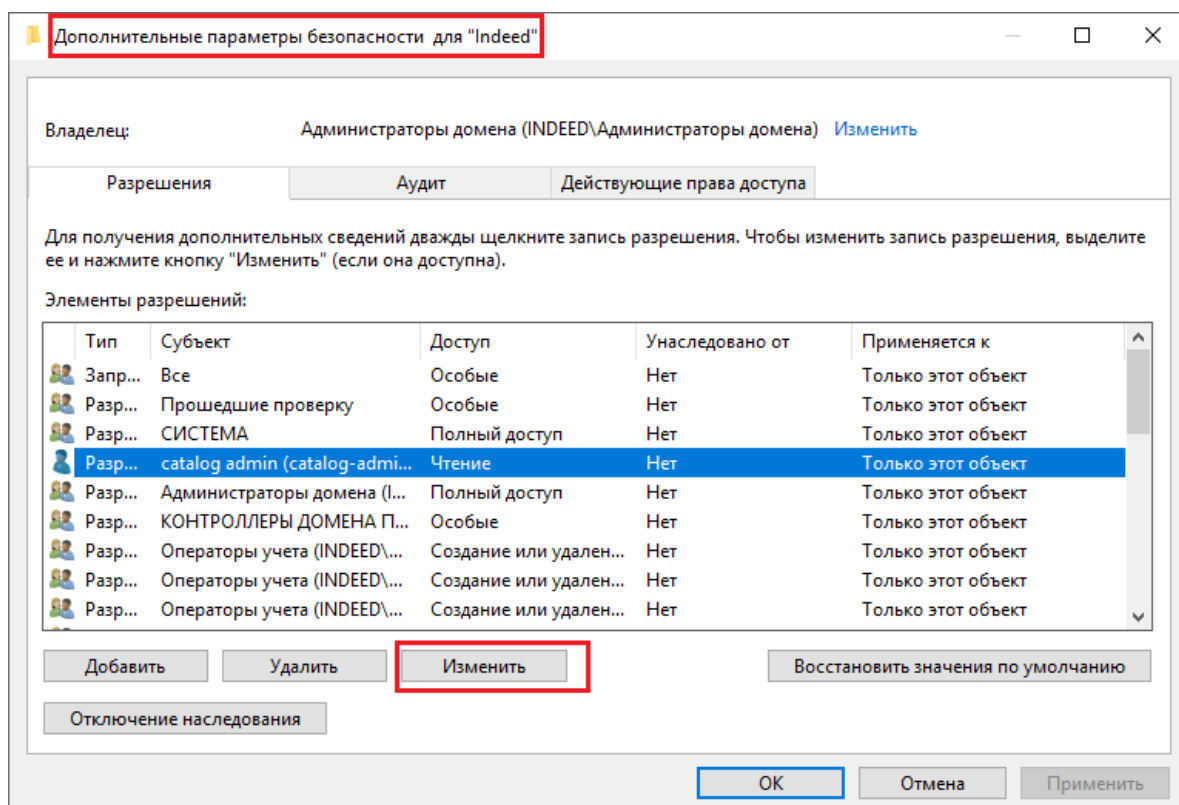


3. Правой кнопкой мыши нажмите объект с пользователями и выберите **Properties**.

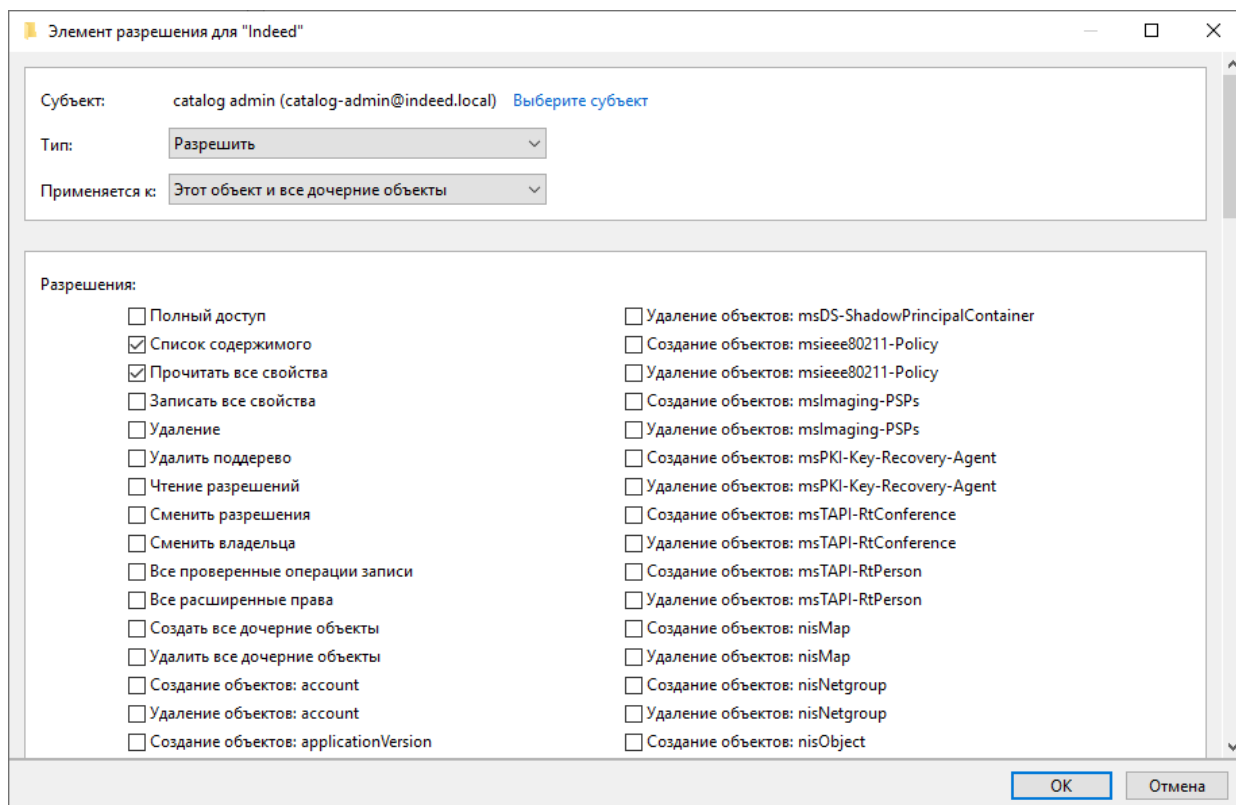
4. В окне **Properties** выполните следующие действия:
- a. Откройте вкладку **Security**.
 - b. В разделе **Group or user names** добавьте созданную ранее сервисную учетную запись.
 - c. В разделе **Permissions for** выберите опцию **Read** и нажмите кнопку **Advanced**.



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**.



Установка клиентского сертификата

Клиентский сертификат проверяет запросы от модулей интеграции к серверу Indeed Access Manager.

Установка сертификата обязательна только при прямых запросах от модулей к серверу. Если вы используете балансировщик нагрузки, установка сертификата необязательна, однако сертификат может потребоваться для тех случаев, когда запросы нужно отправить в обход балансировщика.

Сертификат *SourceCode_EA.Server_Certificates_ClientCertificate_eaclient* расположен в папке *Indeed AM номер_версии\Indeed Access Manager Server\номер_версии\Misc*.

Установите сертификат из дистрибутива Indeed Access Manager на компьютер, где вы развернули сервер Indeed.

Для этого выполните следующие действия:

1. Двойным щелчком откройте файл сертификата.
2. В окне **Сертификат** нажмите кнопку **Установить сертификат**.
3. В окне **Мастер импорта сертификатов** выберите **Локальный компьютер** и нажмите **Далее**.
4. Разрешите внесение изменений.
5. В окне **Мастер импорта сертификатов** выберите опцию **Поместить все сертификаты в следующее хранилище** и нажмите кнопку **Обзор**.
6. В окне **Выбор хранилища сертификата** выберите **Доверенные корневые центры сертификации** и нажмите **ОК**.
7. В окне **Мастер импорта сертификатов** нажмите **ДалееГотово**.

Убедитесь, что вы разрешили серверу Indeed Access Manager принимать клиентский сертификат. Для этого выполните следующие действия:

1. Откройте Диспетчер служб IIS.
2. Выберите **Indeed AMСайтыDefault Web Siteamcore**.
3. Нажмите **Параметры SSL**.
4. Выберите опцию **Принимать клиентские сертификаты**.

Порядок установки

Все компоненты входят в состав дистрибутива, для установки потребуется запустить установочный файл нужного приложения и последовать указаниям мастера.



Информация

Обновление компонентов Indeed Access Manager осуществляется вручную без использования сервисов внешней сети.

1. [Установить Indeed AM Log Server](#)
 - a. [Системные требования](#)
 - b. [Подготовка](#)
 - c. [Установка и настройка](#)
2. [Установить сервер Indeed Access Manager](#)
 - a. [Системные требования](#)
 - b. [Подготовка](#)
 - c. [Установка и настройка](#)
3. [Установить Indeed AM Admin Console](#)
 - a. [Системные требования](#)
 - b. [Подготовка](#)
 - c. [Установка и настройка](#)
4. [Установить необходимый набор провайдеров](#)
5. [Установить необходимые расширения](#)
 - a. [Системные требования](#)

Установка и настройка

- [Indeed AM Log Server](#)
 - [Установка и настройка Indeed AM Log Server с резервным хранилищем](#)
 - [Установка и настройка Indeed AM Log Server с хранилищем в SysLog](#)
 - [Установка и настройка Indeed AM Log Server с хранилищем в БД](#)
 - [Установка и настройка Indeed AM Log Server с хранилищем в EventLog](#)
- [Indeed Access Manager Server](#)
 - [Indeed Access Manager Server с хранилищем данных в MS SQL](#)
 - [Indeed Access Manager Server с хранилищем данных в PostgreSQL](#)
- [Indeed AM Management Console](#)
- [Indeed AM User Console](#)
- [Indeed Key Server](#)
- [Indeed AM Phone Management Server](#)
- [Indeed AM Reset Password](#)
- [Установка и настройка провайдеров](#)
 - [Indeed AM Windows Password Provider](#)
 - [Indeed AM Smart Card Provider](#)
 - [Indeed AM IronLogic Z2USB Provider](#)
 - [Indeed AM OMNIKEY Provider](#)
 - [Indeed AM Futronic Provider](#)
 - [Indeed AM Passcode Provider](#)
 - [Indeed AM Email OTP Provider](#)
 - [Indeed AM Hardware TOTP Provider](#)
 - [Indeed AM HOTP Provider](#)
 - [Indeed AM Storage SMS OTP Provider](#)
 - [Indeed AM Telegram OTP Provider](#)
 - [Indeed AM SMS OTP Provider](#)
 - [Indeed AM Software OTP Provider](#)
 - [Indeed Key Provider](#)
 - [Indeed AM MFA Provider](#)

- Модули интеграции
 - Indeed AM Identity Provider
 - Интеграция с приложениями по протоколам OpenID Connect и OAuth 2.0
 - Интеграция с приложениями по протоколу SAML
 - Аутентификация по имени пользователя без указания домена
 - Включение защиты от перебора
 - Indeed AM ADFS Extension
 - Indeed AM ADFS Extension (2012)
 - Indeed AM ADFS Extension (2016)
 - Indeed AM ESSO Agent
 - Indeed AM IIS Extension
 - Indeed AM NPS RADIUS Extension
 - Indeed AM RDP Windows Logon
 - Indeed AM Windows Logon
 - Indeed AM SAML IDP

Indeed AM Log Server

Indeed AM Log Server — это web-приложение, которое работает на базе IIS. Данный модуль отвечает за централизованный сбор и аудит событий системы.

Информация

Отказоустойчивость

Если LogServer не доступен, события кэшируются в локальную папку на сервере Indeed AM.



Информация о недоступности LogServer отображается в событиях Windows во вкладке "Приложение".

Код события: 500

Текст: Log server client fluentSchedulerBackgroundLoaderTask. Iteration WEB exception: Время ожидания операции истекло

Путь к папке для хранения событий задается в конфигурационном файле сервера **Indeed Web.config** в теге "**logServerClient**" в параметре "**EventCacheDirectory**" (По умолчанию: `./EventCache`). Время отправки логов, после возобновления работы LogServer, задается в теге "**logServerClient**" в параметре "**EventCacheSendingIntervalSec**" (По умолчанию: 600 секунд)



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, данный параметр задается в конфигурационном файле схемы.

Пример

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

Схема

Схема событий Indeed создается автоматически при установке компонента **IndeedAM.Server.EventLog** и находится в `C:\ProgramData\Indeed\LogServer\Schemes`

Настройка системы:

- [Установка и настройка Indeed AM Log Server с хранилищем в EventLog](#)
- [Установка и настройка Indeed AM Log Server с хранилищем в БД](#)
- [Установка и настройка Indeed AM Log Server с хранилищем в SysLog](#)
- [Установка и настройка Indeed AM Log Server с резервным хранилищем](#)

Установка и настройка Indeed AM Log Server с резервным хранилищем

Информация

Файлы для **Indeed AM Log Server** расположены в папке *Indeed AM Log Server*.

- **Indeed.LogServer-<номер версии>.x64.ru-ru.msi** — пакет для установки Indeed Log Server.
- **IndeedAM.Server.EventLog-<номер версии>.x64.ru-ru.msi** — пакет для создания необходимой структуры журнала в Windows EvetLog.

Установка

1. Выполнить установку Indeed AM Log Server через запуск инсталлятора **Indeed.LogServer-<номер версии>.x64.ru-ru.msi**.
2. Выполнить установку Indeed EventLog на машине с Log Server через запуск инсталлятора **IndeedAM.Server.EventLog-<номер версии>.x64.ru-ru.msi**.
3. Добавить привязку **https** в настройках **Default Web Site** в IIS Manager.

Информация

Indeed Log Server является Web приложением, которое работает на базе IIS, в процессе установки для него по умолчанию включается обязательно требование SSL в настройках, что в свою очередь требует включенной привязки https.

Если вы не намерены использовать протокол https, необходимо отключить требование SSL в настройках IIS для logserver.

- a. Запустите **IIS Manager** и раскройте пункт **Сайты (Sites)**.
- b. Выберите сайт **Default Web Site** и нажмите **Привязки (Bindings)** в разделе **Действия (Actions)**.
- c. Нажмите **Добавить (Add)**:
 - i. **Тип (Type)** - https.
 - ii. **Порт (Port)** - 443.
 - iii. Выберите **SSL-сертификат (SSL Certificate)**.
- d. Сохраните привязку.

Редактирование конфигурационного файла.

Настройка с несколькими хранилищами разного типа

Информация

В качестве примера выполнена настройка, при которой чтение событий осуществляется с событий Windows, запись осуществляется в события Windows и базу SQL.

1. Откройте конфигурационный файл сервера **clientApps.config** (C:\inetpub\wwwroot\ls\clientApps.config).
2. Для блока с "Application Id="ea"" в тегах **ReadTargetId** указать **sampleEventLog** или **sampleDb**.

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>...</Targets>**, конфигурационные файлы для каждого типа находятся в папке **targetConfigs** с соответствующим именем.

3. В блоке **WriteTargets** укажите **<TargetId>sampleEventLog</TargetId>** и **<TargetId>sampleDb</TargetId>**.
4. Откройте конфигурационный файл **sampleDb.config** (C:\inetpub\wwwroot\ls\targetConfigs\sampleDb.config).

5. Укажите данные для подключения к базе данных в теге **connectionString**.

- a. **Data Source** — задает экземпляр сервера. Это свойство является обязательным для всех соединений. Допустимые значения — сетевое имя или IP-адрес сервера, local или localhost для локальных соединений.
- b. **Database** — определяет имя базы данных.
- c. **User Id** — имя пользователя для подключения к базе данных.
- d. **Password** — пароль пользователя для подключения к базе данных.

Пример

```
<Settings>
  <ConnectionString>Data Source=localhost;Database=LogServ;User Id=log;
  Password=Q1q2E3e4</ConnectionString>
</Settings>
```



Информация

При такой конфигурации чтение событий системы будет осуществляться из событий Windows, запись событий будет осуществляться в базу данных SQL.

Пример

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

Настройка с резервным хранилищем в базе данных

1. Откройте конфигурационный файл сервера **clientApps.config** (C:\inetpub\wwwroot\ls\clientApps.config).

2. В блоке **<Targets>** скопируйте тег **Target** с **Id="sampleDb"** и измените id на произвольное значение, например **sampleDbBackup**.

Пример

```
<Targets>
  <Target Id="sampleEventLog" Type="eventlog"/>
  <Target Id="sampleDb" Type="mssql"/>
  <Target Id="sampleDbBackup" Type="mssql"/>
  <Target Id="akcSqlTarget" Type="mssql"/>
  <Target Id="akcEventLogTarget" Type="eventlog"/>
  <Target Id="sampleSyslog" Type="syslog"/>
</Targets>
```

3. Для блока с "Application Id="ea"" в тегах **ReadTargetId** указать **sampleDb**.

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>...</Targets>**, конфигурационные файлы для каждого типа находятся в папке **targetConfigs** с соответствующим именем.

4. В блоке **WriteTargets** укажите `<TargetId>sampleDb</TargetId>` и `<TargetId>sampleDbBackup</TargetId>`.

 Информация

При такой конфигурации чтение событий будет осуществляться с базы данных, указанной в конфигурационном файле: `ls\targetConfigs\sampleDb.config`. Запись будет осуществляться в базы данных указанные в файлах:

- `ls\targetConfigs\sampleDb.config`
- `ls\targetConfigs\sampleDbBackup.config`

Пример

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

5. Откройте конфигурационный файл **sampleDb.config** (C:\inetpub\wwwroot\ls\targetConfigs\sampleDb.config).
6. Укажите данные для подключения к базе данных в теге **connectionString**.

 Информация

Укажите данные для подключения к основной базе данных.

- Data Source** — задает экземпляр сервера. Это свойство является обязательным для всех соединений. Допустимые значения — сетевое имя или IP-адрес сервера, `local` или `localhost` для локальных соединений.
- Database** — определяет имя базы данных.
- User Id** — имя пользователя для подключения к базе данных.
- Password** — пароль пользователя для подключения к базе данных.

Пример

```
<Settings>
  <ConnectionString>Data Source=localhost;Database=LogServ;User Id=log;
  Password=Q1q2E3e4</ConnectionString>
</Settings>
```


7. Создайте файл **sampleDbBackup** с расширением **config**.



Информация

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

8. Укажите данные для подключения к базе данных в теге **connectionString**.



Информация

Укажите данные для подключения к резервной базе данных.

- a. **Data Source** — задает экземпляр сервера. Это свойство является обязательным для всех соединений. Допустимые значения — сетевое имя или IP-адрес сервера, **local** или **localhost** для локальных соединений.
- b. **Database** — определяет имя базы данных.
- c. **User Id** — имя пользователя для подключения к базе данных.
- d. **Password** — пароль пользователя для подключения к базе данных.

Пример

```
<Settings>  
  <ConnectionString>Data Source=localhost;Database=LogServBackup;User Id=log;  
  Password=Q1q2E3e4</ConnectionString>  
</Settings>
```

Установка и настройка Indeed AM Log Server с хранилищем в SysLog

Информация

Файлы для **Indeed AM Log Server** расположены в папке *Indeed AM Log Server*.

- **Indeed.LogServer-<номер версии>.x64.ru-ru.msi** — пакет для установки Indeed Log Server.
- **IndeedAM.Server.EventLog-<номер версии>.x64.ru-ru.msi** — пакет для создания схемы событий Indeed AM и необходимой структуры журнала в Windows EvetLog.

Информация

Indeed AM Admin Console не позволяет читать события из sysLog сервера. Для отображения журнала в Admin Console необходимо наличие своей БД (SQL-сервер или EventLog) для хранения событий Indeed AM LogServer.

Мы поддерживаем форматы Plain, CEF, LEEF. По умолчанию используется Plain.

Установка

1. Выполнить установку Indeed AM Log Server через запуск соответствующего пакета.
2. Выполнить установку Indeed EventLog на машине с Log Server через запуск инсталлятора **IndeedAM.Server.EventLog-<номер версии>.x64.ru-ru.msi**.
3. Добавить привязку **https** в настройка **Default Web Site** в IIS Manager.

Информация

Indeed Log Server является Web приложением, которое работает на базе IIS, в процессе установки для него по умолчанию включается обязательно требование SSL в настройках, что в свою очередь требует включенной привязки https.

Если вы не намерены использовать протокол https, необходимо отключить требование SSL в настройках IIS для logserver.

- a. Запустите **IIS Manager** и раскройте пункт **Сайты (Sites)**.
- b. Выберите сайт **Default Web Site** и нажмите **Привязки (Bindings)** в разделе **Действия (Actions)**.
- c. Нажмите **Добавить (Add)**:
 - i. **Тип (Type)** — https.
 - ii. **Порт (Port)** — 443.
 - iii. Выберите **SSL-сертификат (SSL Certificate)**.
- d. Сохраните привязку.

Установка sysLog сервера

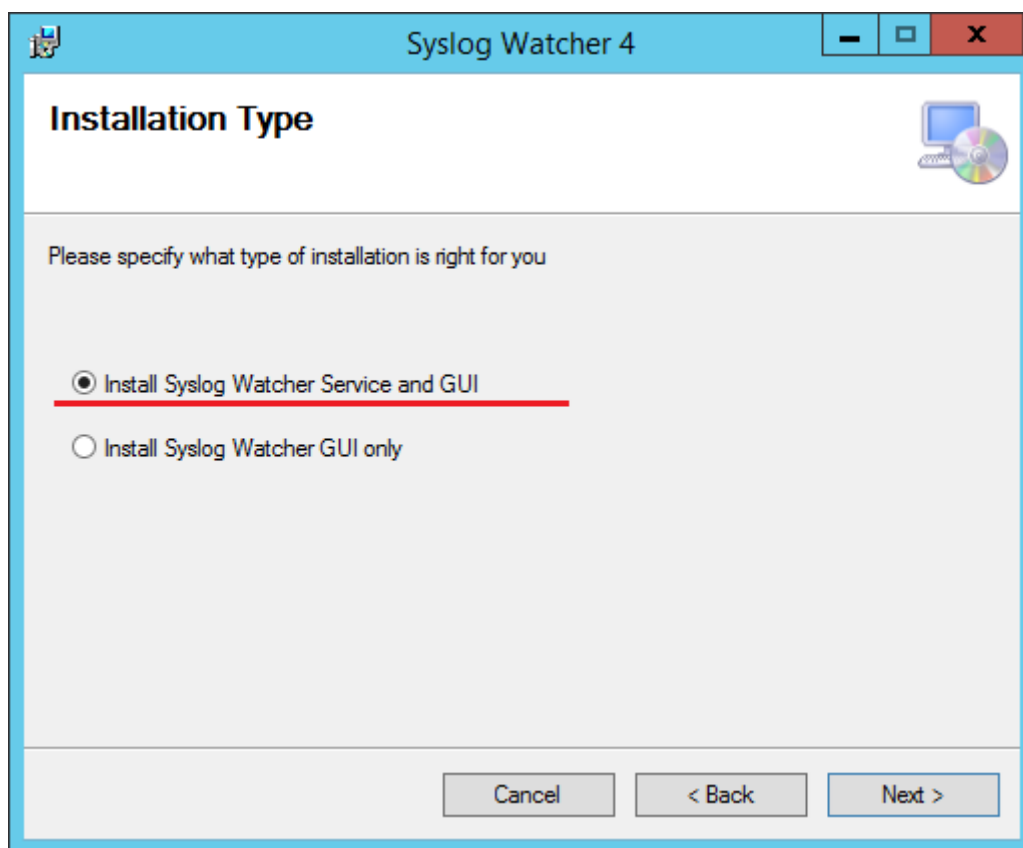
Информация

Indeed AM Log Server поддерживает формат sys-log, вы можете использовать любой сервер, работающий с данным форматом. В качестве примера далее рассмотрена настройка sys-log сервера **Syslog Watcher v4.8.6**.

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

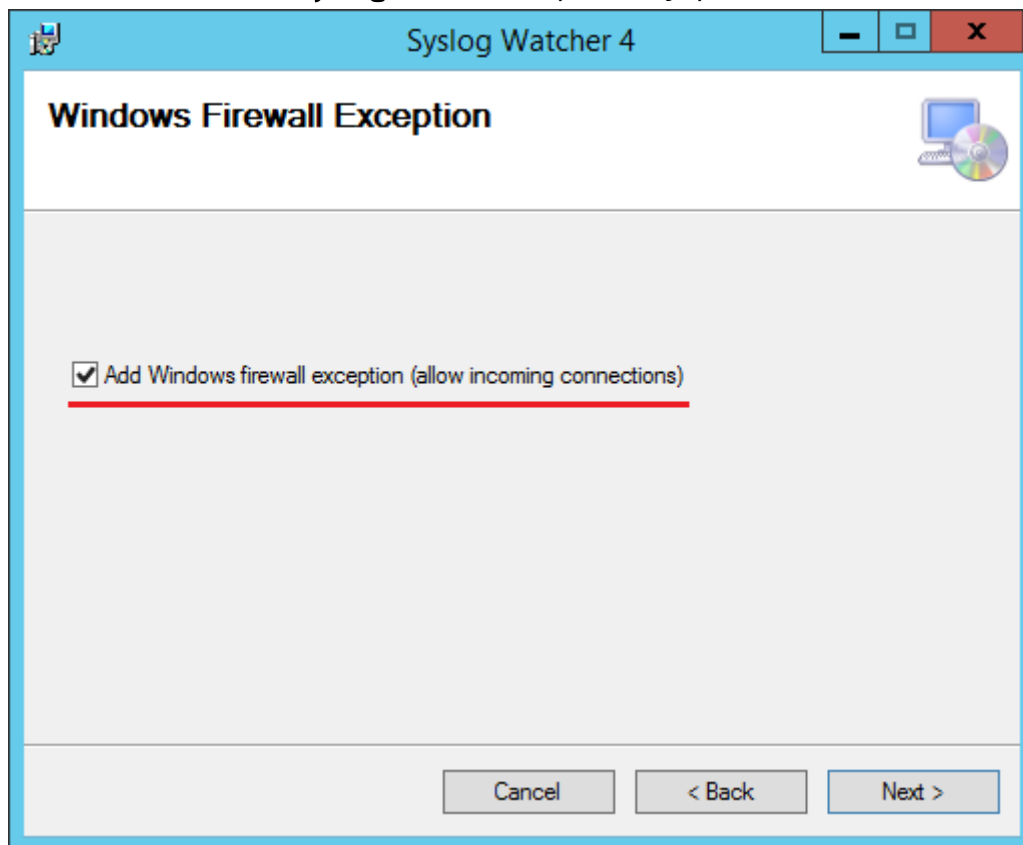
1. Запустите установочный файл **SyslogWatcherSetup-*. *-win32.msi**.
2. В окне "**License Agreement**" примите лицензионное соглашение.

3. В окне "Installation Type" выбрать тип установки "Install Syslog Watcher Service and GUI".



4. В окне "Select installation Folder" выбрать путь установки для **sys-log** сервера.

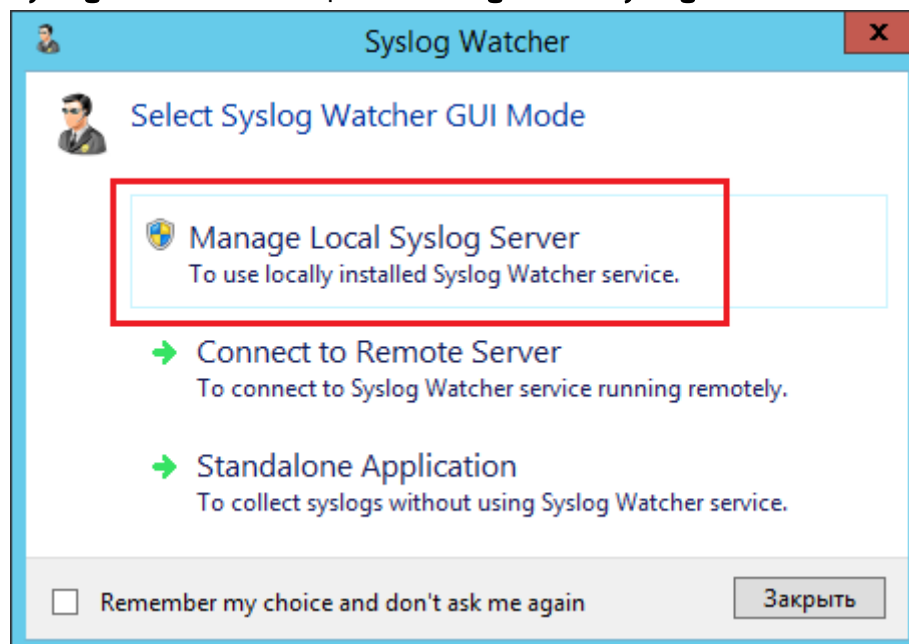
5. В окне **"Windows Firewall Exception"** разрешить добавление правила на все входящие соединения для **Syslog Watcher** в брандмауэр **Windows**.



6. В окне **"Confirm Installation"** нажать **"Next"** для подтверждения установки.
7. Дождаться завершения установки сервера.

Настройка sysLog сервера

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



2. Нажмите "**Settings**" в верхнем меню программы.
- Выберите пункт "**Network Interfaces**".
 - Проверьте что выбрано использование протокола udp и указан порт.

The screenshot shows the 'Syslog Watcher Settings' dialog box with the 'Network Interfaces' tab selected in the left sidebar. The 'Internet Protocol' section has the following settings: 'Bind to local IPv4 interfaces' is checked with a link to 'Show Local Interfaces'; 'Bind to specified IPv4 address' is selected with the value '192.168.1.4'; 'Bind to local IPv6 interfaces' is checked; 'Bind to all local IPv6 addresses (:::)' is selected. The 'Transport Layer' section has 'Receive syslogs over UDP on port: 514' checked and underlined in red, with a link to 'Show Used Ports', and 'Receive syslogs over TCP on port: 1468' is unchecked. The 'OK', 'Cancel', and 'Apply' buttons are at the bottom right.

- Выберите пункт "**Processing**". Выберите кодировку **UTF-8**.

The screenshot shows the 'Syslog Watcher Settings' dialog box with the 'Processing' tab selected in the left sidebar. The 'Processing' section has the following settings: 'Default severity: Debug' and 'Default facility: local 0' are set in dropdown menus; 'Remove trailing CR/LF (Carriage Return / Line Feed)' is checked; 'Replace non-printable ASCII characters (codes 0-31) with:' is checked, with 'Hexadecimal ACSII code of the character' selected; 'Force codepage: 65001 (UTF-8)' is checked and underlined in red; 'Insert domain name after IP address within message body' is checked. The 'OK', 'Cancel', and 'Apply' buttons are at the bottom right.

Редактирование конфигурационного файла

1. Откройте конфигурационный файл **sampleSyslog.config** (C:\inetpub\wwwroot\ls\targetConfigs\sampleSyslog.config).
2. Для тега **"Settings"** укажите данные для подключения к **sys-log**.

Пример настройки для Syslog Watcher

```
<Settings HostName="localhost" Port="514" Protocol="udp" />
```

3. Откройте конфигурационный файл **clientApps.config** (C:\inetpub\wwwroot\ls\clientApps.config).
4. Для блока с **"Application Id="ea"** в тегах **TargetId** и **ReadTargetId** указать **sampleSyslog**.

Информация

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

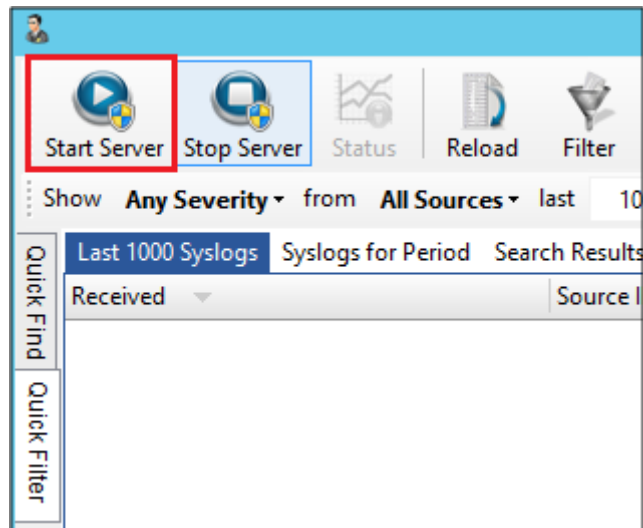
В блоке **WriteTargets**, в тегах **TargetId**, указывается идентификатор хранилища куда будет осуществляться запись событий.

Идентификаторы заданы в теге **<Targets>...</Targets>**, конфигурационные файлы для каждого типа находится в папке **targetConfigs** с соответствующим именем.

Пример

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

5. Нажмите "**Start Server**" в верхнем левом углу программы **Syslog Watcher**.



Пример отображения

- Пример отображения в Syslog Watcher.

The screenshot displays the Syslog Watcher - Local Syslog Server application. The interface includes a top toolbar with buttons for Start Server, Stop Server, Status, Reload, Filter, Find, Search, Import, Export, Delete, Reports, Storage, and Settings. Below the toolbar are Vendor Pack, Help, and Info buttons. A status bar shows 'Show Any Severity from LOG last 1000 messages | Update every 10 seconds | Updated at 26.11.2018 12:01:26'. The main area is divided into a 'Quick Find' sidebar and a 'Message View' section. The 'Quick Find' sidebar contains a table with columns: Received, Source IP, Source, Facility, Severity, Timestamp, Tag, Ori..., and Message. The table lists several log entries from 26.11.2018 10:52:00 to 26.11.2018 12:00:00, all from source '1' and facility 'local 7', with severity 'Info'. The 'Message View' section shows a detailed view of a selected message, including the timestamp '26 ноября 2018 г. 11:00:31.963' and the message content: 'server LogonByAuthenticatorSucceeded [indeed@32473 requestApplication="Enterprise Management Console" requestUser="Admin Indeed" requestComputer="192.168.1.3" logonMode="Windows Token" authComment=""] Пользователь был успешно аутентифицирован по предоставленному аутентификатору. Приложение: Enterprise Management Console. Пользователь: Admin Indeed. Компьютер: 192.168.1.3. Способ входа: Windows Token. Комментарий аутентификатора: .

Received	Source IP	Source	Facility	Severity	Timestamp	Tag	Ori...	Message
26.11.2018 10:52:...	::1	LOG	local 7	Info	2018-11-2...	ea	unk...	server LogonByAuthenticatorSucceeded [inde
26.11.2018 11:00:...	::1	LOG	local 7	Info	2018-11-2...	ea	unk...	server LogonByAuthenticatorSucceeded [inde
26.11.2018 12:00:...	::1	LOG	local 7	Info	2018-11-2...	ea	unk...	server AcquirePersonalLicense [indeed@32473
26.11.2018 12:00:...	::1	LOG	local 7	Info	2018-11-2...	ea	unk...	server ReleasePersonalLicense [indeed@32473
26.11.2018 12:00:...	::1	LOG	local 7	Info	2018-11-2...	ea	unk...	server ReleasePersonalLicense [indeed@32473
26.11.2018 12:00:...	::1	LOG	local 7	Info	2018-11-2...	ea	unk...	server AcquirePersonalLicense [indeed@32473
26.11.2018 12:00:...	::1	LOG	local 7	Info	2018-11-2...	ea	unk...	server AcquirePersonalLicense [indeed@32473
26.11.2018 12:00:...	::1	LOG	local 7	Info	2018-11-2...	ea	unk...	server ReleasePersonalLicense [indeed@32473
26.11.2018 12:00:...	::1	LOG	local 7	Info	2018-11-2...	ea	unk...	server ReleasePersonalLicense [indeed@32473
26.11.2018 12:00:...	::1	LOG	local 7	Info	2018-11-2...	ea	unk...	server AcquirePersonalLicense [indeed@32473

Message View

Info / local 7 LOG (::1) 26 ноября 2018 г. 11:00:31.963

server LogonByAuthenticatorSucceeded [indeed@32473
requestApplication="Enterprise Management Console" requestUser="Admin Indeed" requestComputer="192.168.1.3"
logonMode="Windows Token" authComment=""] Пользователь был успешно аутентифицирован по предоставленному
аутентификатору. Приложение: Enterprise Management Console. Пользователь: Admin Indeed. Компьютер:
192.168.1.3. Способ входа: Windows Token. Комментарий аутентификатора: .

For Help, press F1 Service: Started (4.8.6) Tot: 10 Dsn: 10 Flt: 0 Sel: 1 UDP: 514 TCP: 1468

Установка и настройка Indeed AM Log Server с хранилищем в БД

Информация

Файлы для **Indeed AM Log Server** расположены в папке *Indeed AM Log Server*.

- **Indeed.LogServer-<номер версии>.x64.ru-ru.msi** — пакет для установки Indeed Log Server.
- **IndeedAM.Server.EventLog-<номер версии>.x64.ru-ru.msi** — пакет для создания схемы событий Indeed AM и необходимой структуры журнала в Windows EventLog.
- **Indeed.LogServer.Config.Encryptor.zip** — утилита для шифрования конфигурационного файла.

Установка компонентов

1. Выполнить установку Indeed AM Log Server через запуск соответствующего пакета.
2. Выполнить установку Indeed EventLog на машине с Log Server через запуск инсталлятора **IndeedAM.Server.EventLog-<номер версии>.x64.ru-ru.msi**.
3. Добавить привязку **https** в настройках **Default Web Site** в IIS Manager.

Информация

Indeed AM Log Server является Web приложением, которое работает на базе IIS, в процессе установки для него по умолчанию включается обязательно требование SSL в настройках, что в свою очередь требует включенной привязки https.

Если вы не намерены использовать протокол https, необходимо отключить требование SSL в настройках IIS для logserver.

- a. Запустите **IIS Manager** и раскройте пункт **Сайты (Sites)**.
- b. Выберите сайт **Default Web Site** и нажмите **Привязки (Bindings)** в разделе **Действия (Actions)**.
- c. Нажмите **Добавить (Add)**:
 - i. **Тип (Type)** — https.
 - ii. **Порт (Port)** — 443.
 - iii. Выберите **SSL-сертификат (SSL Certificate)**.
- d. Сохраните привязку.

Создание базы данных для хранения событий

1. Для создание базы данных в MSSQL можно воспользоваться [этой инструкцией](#).
2. Для создание базы данных в PostgreSQL можно воспользоваться [этой инструкцией](#).

Редактирование конфигурационного файла

База данных MSSQL

1. Откройте конфигурационный файл **sampleDb.config** (C:\inetpub\wwwroot\ls\targetConfigs\sampleDb.config).
2. Укажите данные для подключения к базе данных в теге **connectionString**.
 - a. **Data Source** — задает экземпляр сервера. Это свойство является обязательным для всех соединений. Допустимые значения — сетевое имя или IP-адрес сервера, local или localhost для локальных соединений.
 - b. **Database** — определяет имя базы данных.
 - c. **User Id** — имя пользователя для подключения к базе данных.
 - d. **Password** — пароль пользователя для подключения к базе данных.

Пример

```
<Settings>
  <ConnectionString>Data Source=localhost;Database=LogServ;User Id=log;
  Password=Q1q2E3e4</ConnectionString>
</Settings>
```

3. Откройте конфигурационный файл сервера **clientApps.config** (C:\inetpub\wwwroot\ls\clientApps.config).

4. Раскомментируйте блок с "**Application Id="ea"** в тегах **TargetId** и **ReadTargetId** указать **sampleDb**.

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>...</Targets>**, конфигурационные файлы для каждого типа находятся в папке **targetConfigs** с соответствующим именем.

Пример

```
<Application Id="ea" Schemald="eaSchema">
<ReadTargetId>sampleDb</ReadTargetId>
<WriteTargets>
  <TargetId>sampleDb</TargetId>
</WriteTargets>
<AccessControl>
  <!--<CertificateAccessControl CertificateThumbprint="001122...AA11" Rights="Read" />-->
</AccessControl>
</Application>
```

База данных PostgreSQL

1. Перейдите в папку **targetConfigs** (C:\inetpub\wwwroot\ls\targetConfigs).
2. Создайте файл с произвольным именем и расширением **".config"**, например **postgresDb.config**.
3. Добавьте в файл следующие:

Пример

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

4. В строке "**ConnectionString**" укажите следующие данные:

- a. **Server** — DNS\IP адрес сервера с БД PostgreSQL.
- b. **Database** — имя базы данных.
- c. **Integrated Security** — False.



Информация

Встроенная аутентификация не поддерживается

- d. **User ID** — имя пользователя, который имеет полные права для базы данных "Database".
- e. **Password** — пароль пользователя.

Пример

```
Server=192.200.1.2;Database=AM8Log;Integrated Security=False;User ID=IndeedDB;  
Password=auqOVg
```

5. Откройте конфигурационный файл сервера **clientApps.config** (C:\inetpub\wwwroot\ls\clientApps.config).

6. Раскомментируйте блок с "**Application Id="ea"** в тегах **TargetId** и **ReadTargetId** указать **postgresDb**.

 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>...</Targets>**, конфигурационные файлы для каждого типа находятся в папке **targetConfigs** с соответствующим именем.

Пример

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

7. Далее в этом же файле в секции **Targets** добавьте новый элемент:

Пример

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

Пример отображения

- Отображения журнала в **Indeed AM Management Console**.

События

 Экспортировать

Пользователь или инициатор Не задано  Выбрать	Приложение Не задано 	Начальная дата 2020/09/05 00:00 	Конечная дата 2020/09/09 00:00
Тип аутентификатора Не задано 	Модуль Не задано 	Описание содержит 	Тип события Не задано
Код события Выбрать			

Применить **Сбросить**

СОБЫТИЕ	ДАТА	МОДУЛЬ	ИНИЦИАТОР
 Пользователь был аутентифицирован по предоставленному аутентификатору.	2020.09.08 14:29:12	Enterprise Management Console	Admin-Indeed
 Сервис отзыва лицензий завершил работу.	2020.09.08 14:26:39	None	None
 Пользователь был аутентифицирован по предоставленному аутентификатору.	2020.09.08 14:26:29	Enterprise Management Console	Admin-Indeed
 Сервис отзыва лицензий завершил работу.	2020.09.08 13:21:15	None	None
 Сервис отзыва лицензий завершил работу.	2020.09.08 13:16:41	None	None
 Сервис отзыва лицензий завершил работу.	2020.09.08 13:06:41	None	None
 Сервис отзыва лицензий завершил работу.	2020.09.08 12:56:41	None	None
 Сервис отзыва лицензий завершил работу.	2020.09.08 12:46:41	None	None

Шифрование/Расшифрование конфигурационного файла

- Запустите командную строку от имени **"Администратора"**.
- В командной строке перейдите в папку с утилитой для шифрования (**Indeed. LogServer.Config.Encryptor**).

- Шифрование конфигурационного файла

Для шифрования требуется запустить утилиту со следующими параметрами:

Пример

```
protect -f C:\inetpub\wwwroot\ls\targetConfigs\sampleDb.config -t Sql
```

-f, --file Путь к конфигурационному файлу, обязательный параметр
-t, --type Тип target'a конфигурационного файла. Опциональный параметр, по умолчанию равен Sql

- Расшифровка конфигурационного файла

Для расшифровки требуется запустить утилиту со следующими параметрами:

Пример

```
unprotect -f C:\inetpub\wwwroot\ls\targetConfigs\sampleDb.config -t Sql
```

-f, --file Путь к конфигурационному файлу, обязательный параметр

-t, --type Тип target'a конфигурационного файла. Опциональный параметр, по умолчанию равен Sql

Установка и настройка Indeed AM Log Server с хранилищем в EventLog

Информация

Файлы для **Indeed AM Log Server** расположены в папке *Indeed AM Log Server*.

- **Indeed.LogServer-<номер версии>.x64.ru-ru.msi** — пакет для установки Indeed Log Server.
- **IndeedAM.Server.EventLog-<номер версии>.x64.ru-ru.msi** — пакет для создания необходимой структуры журнала в Windows EventLog.

Установка

1. Выполнить установку Indeed AM Log Server через запуск соответствующего пакета.
2. Выполнить установку Indeed EventLog на машине с Log Server через запуск инсталлятора **IndeedAM.Server.EventLog-<номер версии>.x64.ru-ru.msi**.
3. Добавить привязку **https** в настройках **Default Web Site** в IIS Manager.

Информация

Indeed Log Server является Web приложением, которое работает на базе IIS, в процессе установки для него по умолчанию включается обязательно требование SSL в настройках, что в свою очередь требует включенной привязки https.

Если вы не намерены использовать протокол https, необходимо отключить требование SSL в настройках IIS для logserver.

- a. Запустите **IIS Manager** и раскройте пункт **Сайты** (Sites).
- b. Выберите сайт **Default Web Site** и нажмите **Привязки** (Bindings) в разделе **Действия** (Actions).
- c. Нажмите **Добавить** (Add):
 - i. **Тип** (Type) — https.
 - ii. **Порт** (Port) — 443.
 - iii. Выберите **SSL-сертификат** (SSL Certificate).
- d. Сохраните привязку.

Редактирование конфигурационного файла

1. Откройте конфигурационный файл сервера **clientApps.config** (C:\inetpub\wwwroot\ls\clientApps.config).
2. Раскомментируйте блок с "**Application Id**="ea"" в тегах **TargetId** и **ReadTargetId** указать **sampleEventLog**.

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>...</Targets>**, конфигурационные файлы для каждого типа находится в папке **targetConfigs** с соответствующим именем.

Пример

```
<Application Id="ea" Schemald="eaSchema">
  <ReadTargetId>sampleEventLog</ReadTargetId>
  <WriteTargets>
    <TargetId>sampleEventLog</TargetId>
  </WriteTargets>
  <AccessControl>
    <!--<CertificateAccessControl CertificateThumbprint="001122...AA11" Rights="Read" />-->
  </AccessControl>
</Application>
```

Пример отображения

- Отображения журнала в Indeed AM Admin Console.

События

Экспортировать

Пользователь или инициатор

Не задано

Выбрать

Приложение

Не задано

▼

Начальная дата

2020/09/05 00:00

📅

Конечная дата

2020/09/09 00:00

📅

Тип аутентификатора

Не задано

▼

Модуль

Не задано

▼

Описание содержит

Тип события

Не задано

▼

Код события

Выбрать

Применить

Сбросить

СОБЫТИЕ	ДАТА	МОДУЛЬ	ИНИЦИАТОР	КОД
▶ Пользователь был аутентифицирован по предоставленному аутентификатору.	2020.09.08 14:29:12	Enterprise Management Console	Admin-Indeed	1000
▶ Сервис отзыва лицензий завершил работу.	2020.09.08 14:26:39	None	None	1094
▶ Пользователь был аутентифицирован по предоставленному аутентификатору.	2020.09.08 14:26:29	Enterprise Management Console	Admin-Indeed	1000
▶ Сервис отзыва лицензий завершил работу.	2020.09.08 13:21:15	None	None	1094
▶ Сервис отзыва лицензий завершил работу.	2020.09.08 13:16:41	None	None	1094
▶ Сервис отзыва лицензий завершил работу.	2020.09.08 13:06:41	None	None	1094
▶ Сервис отзыва лицензий завершил работу.	2020.09.08 12:56:41	None	None	1094
▶ Сервис отзыва лицензий завершил работу.	2020.09.08 12:46:41	None	None	1094

- Отображения журнала в событиях Windows.

Просмотр событий (Локальный)

Настраиваемые представления

Журналы Windows

Журналы приложений и служб

Indeed EA

Operational

Microsoft

ThinPrint Diagnostics

Windows PowerShell

Служба управления ключами

События оборудования

Подписки

Operational Событий: 27

Уровень	Дата и время	Источник	Код события	Категория задачи
Сведения	05.10.2018 11:32:34	Indeed EA	1000	EA Сервер
Сведения	05.10.2018 11:32:34	Indeed EA	1000	EA Сервер
Сведения	05.10.2018 11:32:34	Indeed EA	1000	EA Сервер
Сведения	05.10.2018 11:10:48	Indeed EA	1033	EA Сервер
Сведения	05.10.2018 11:10:34	Indeed EA	1033	EA Сервер
Сведения	05.10.2018 11:10:34	Indeed EA	1028	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1000	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1028	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1028	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1000	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1028	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1020	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1021	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1005	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1028	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1028	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1028	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1008	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1007	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1000	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1000	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1032	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1000	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1032	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1000	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1000	EA Сервер
Сведения	05.10.2018 11:10:33	Indeed EA	1000	EA Сервер

Indeed Access Manager Server

Indeed AM 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

Кэширование пользовательских запросов

Indeed AM Server кэширует данные при получении пользователя, группы, контейнера, сценариев авторизации и бизнес логики. Основные запросы в каталог - получение пользователя, группы, контейнера по ID - отдаются из кэша. Все остальные запросы - по имени, по телефону, email и т.п. - только обновляют кэш данными из каталога. Первый запрос пользователя по ID также обновляет кэш, последующие берутся из кэша. Время жизни объекта в кэше - 10 минут.

Проверка состояния сервера

Чтобы проверить состояние сервера, в браузере введите адрес core сервера в формате

https://полное_dns_имя_сервера/am/core/.

Автоматически вы будете перенаправлены на

https://полное_dns_имя_сервера/am/core/api/v5/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
- список ошибок при наличии



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

В этом разделе

- [Indeed Access Manager Server с хранилищем данных в MS SQL](#)
- [Indeed Access Manager Server с хранилищем данных в PostgreSQL](#)

Indeed Access Manager Server с хранилищем данных в MS SQL

Информация

Файлы для Indeed AM Server расположены в *Indeed Access Manager Server/⟨номер версии⟩*.

- **IndeedAM.Server-⟨номер версии⟩.x64.ru-ru.msi** — пакет для установки Indeed AM Server.
- **/Misc/EA.KeyGen.exe** — утилита для генерации ключей шифрования.
- **/Misc/AccessControllInitialConfig/EA.Server.AccessControllInitialConfig.exe** — утилита первичной конфигурации.
- **/Misc/AccessControllInitialConfig/EA.Server.AccessControllInitialConfig.exe.config** — файл для настройки утилиты конфигурации.
- **/Misc/EA.Config.Encryptor/EA.Config.Encryptor.exe** — утилита для шифрования конфигурационного файла.
- **/Misc/EA.Config.Encryptor/encryptConfigs.bat** — скрипт для шифрования всех секций конфигурационного файла.
- **/Misc/EA.Config.Encryptor/decryptConfigs.bat** — скрипт для расшифровки всех секций конфигурационного файла.

Установка

1. Выполнить установку Indeed AM Server через запуск соответствующего пакета.

2. Добавить привязку **https** в настройках **Default Web Site** в IIS Manager.



Информация

Indeed Access Manager Server является Web приложением, которое работает на базе IIS, в процессе установки для него по умолчанию включается обязательно требование SSL в настройках, что в свою очередь требует включенной привязки https.

Если вы не намерены использовать протокол https, необходимо отключить требование SSL в настройках IIS для core и в конфигурационном файле сервера (C:\inetpub\wwwroot\am\core\Web.config) изменить значение параметра "requireHttps" на "false".

```
<appSettings>  
<add key="requireHttps" value="false" />  
</appSettings>
```

- a. Запустите **IIS Manager** и раскройте пункт **Сайты (Sites)**.
- b. Выберите сайт **Default Web Site** и нажмите **Привязки (Bindings)** в разделе **Действия (Actions)**.
- c. Нажмите **Добавить (Add)**:
 - i. **Тип (Type)** - https.
 - ii. **Порт (Port)** - 443.
 - iii. Выберите **SSL-сертификат (SSL Certificate)**.
- d. Сохраните привязку.

Настройка с помощью мастера конфигурации



Информация

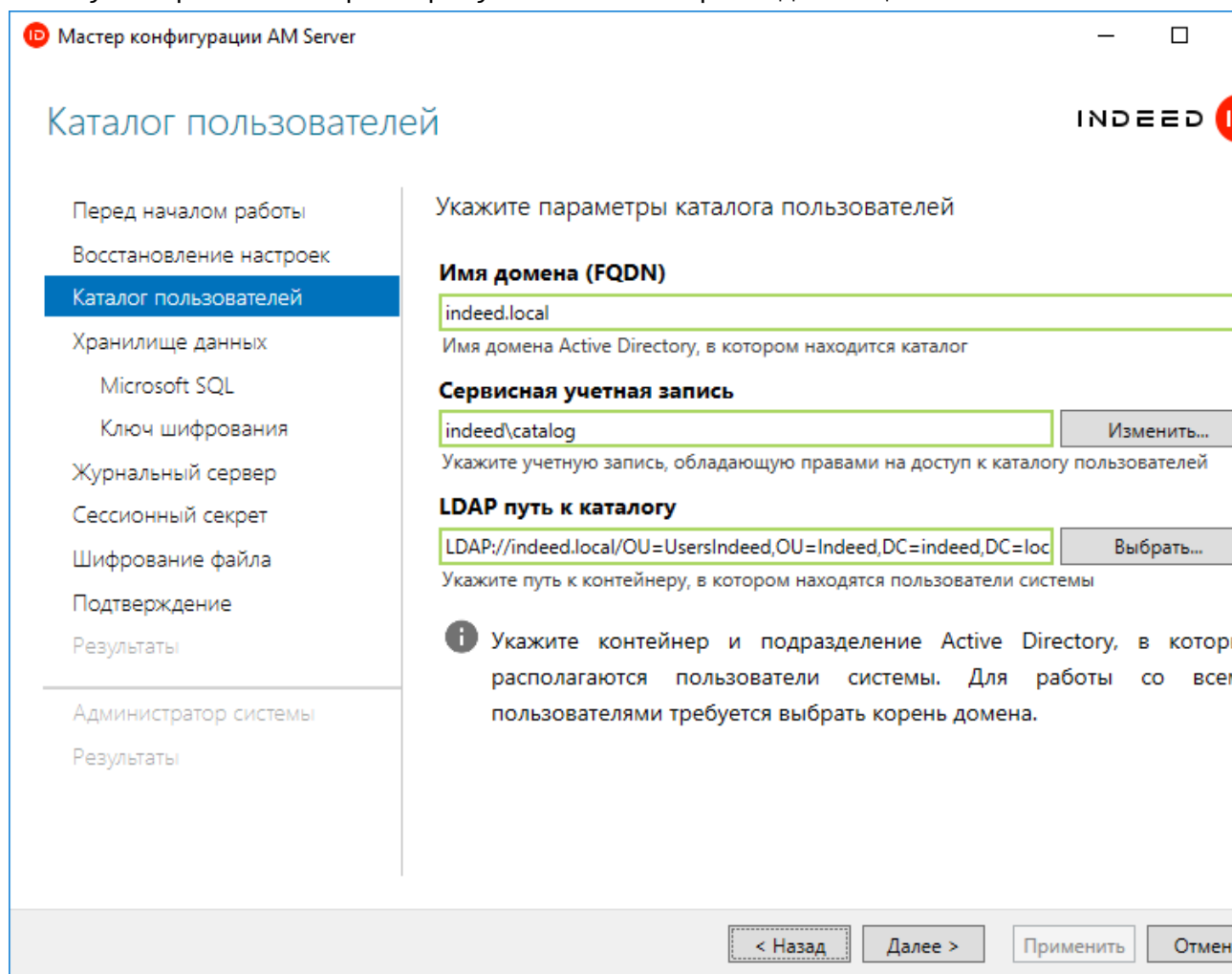
Мастер конфигурации по умолчанию запускается автоматически после установки Indeed AM Server, если запуск не был отключен пользователем.

Для запуска мастера вручную откройте файл: C:\Program Files\Indeed AM\Wizard\EA.Server.Wizard.exe

Информация

В мастер включена автоматическая проверка введенных данных, в случае успешного ввода - поля будут подсвечены зеленым цветом, и вы сможете перейти к следующему шагу, если данные введены некорректно, то поля будут подсвечены красным, и вы не сможете перейти к следующему шагу пока не укажете корректные данные.

1. На шаге "**Перед началом работы**" нажмите "Далее".
2. На шаге "**Восстановление настроек**" нажмите "Далее".
3. На шаге "**Каталог пользователей**" укажите следующие параметры:
 - a. **Имя домена (FQDN)** - Укажите полное имя домена, например: *domain.local*.
 - b. **Сервисная учетная запись** - Укажите сервисную учетную запись, обладающую правами доступа к пользовательскому каталогу. Нажмите кнопку "**Изменить**" и укажите требуемые данные учетной записи.
 - c. **LDAP путь к каталогу** - Укажите путь к каталогу с пользователями. Нажмите кнопку "**Выбрать**" и выберите требуемый контейнер или домен целиком.



The screenshot shows the 'Master Configuration of AM Server' window with the 'User Catalog' step selected in the left sidebar. The main area contains three configuration sections: 'Domain Name (FQDN)' with the value 'indeed.local', 'Service Account' with the value 'indeed\catalog', and 'LDAP Path to Catalog' with the value 'LDAP://indeed.local/OU=UsersIndeed,OU=Indeed,DC=indeed,DC=loc'. Each section has a corresponding button ('Изменить...' or 'Выбрать...'). An information icon and text at the bottom of the main area provide additional instructions. The bottom of the window features navigation buttons: '< Назад', 'Далее >', 'Применить', and 'Отменить'.

Мастер конфигурации AM Server

Каталог пользователей

Укажите параметры каталога пользователей

Имя домена (FQDN)
indeed.local
Имя домена Active Directory, в котором находится каталог

Сервисная учетная запись
indeed\catalog
Укажите учетную запись, обладающую правами на доступ к каталогу пользователей

LDAP путь к каталогу
LDAP://indeed.local/OU=UsersIndeed,OU=Indeed,DC=indeed,DC=loc
Укажите путь к контейнеру, в котором находятся пользователи системы

 Укажите контейнер и подразделение Active Directory, в котором располагаются пользователи системы. Для работы со всеми пользователями требуется выбрать корень домена.

< Назад Далее > Применить Отменить

4. На шаге "**Хранилище данных**" выберете тип хранилища Microsoft SQL.

5. **Строка подключения к базе данных** - Нажмите "**Изменить**", чтобы задать данные для подключения к базе данных, которая будет использоваться в качестве хранилища данных Indeed AM.

- a. Server name - Имя сервера БД.
- b. Выберите способ аутентификации SQL "**Use SQL Server Authentication**" и укажите данные сервисного пользователя, с полными правами для базы данных.
- c. В пункте "**Select or enter a database name**" выберите или укажите базу данных, которая будет использоваться в качестве хранилища Indeed AM.
- d. После выполнения настройки нажмите "**Test Connection**". При корректной конфигурации отобразится окно с "**Test connection succeeded**".
- e. Нажмите "**Ок**" во всех окнах.

The screenshot shows the 'Connection Properties' dialog box. It has several sections: 'Data source' with a dropdown set to 'Microsoft SQL Server (SqlClient)' and a 'Change...' button; 'Server name' with a dropdown set to 'SERVER\SQLEXPRESS' and a 'Refresh' button; 'Log on to the server' with two radio buttons, 'Use Windows Authentication' and 'Use SQL Server Authentication' (which is selected), followed by 'User name' (Indeed) and 'Password' (masked with dots), and a 'Save my password' checkbox; 'Connect to a database' with two radio buttons, 'Select or enter a database name' (selected) and 'Attach a database file', followed by a dropdown set to 'Indeed8DB', a 'Browse...' button, and a 'Logical name' field; and an 'Advanced...' button. At the bottom, there are 'Test Connection', 'OK', and 'Cancel' buttons. The 'Test Connection' button is highlighted with a blue border.

6. Шаг "**Ключ шифрования**". Выберите алгоритм шифрования, нажмите "**Сгенерировать**" и нажмите "**Далее**".



Информация

Настоятельно рекомендуется выполнить резервную копию ключа шифрования и сохранить в защищенном месте.

7. На шаге "**Журнальный сервер**" укажите следующие данные:



Информация

Чтобы при тестировании соединения не возникало ошибок, требуется полностью настроенный лог-сервер, с настроенной базой данных или установленным компонентом EventLog. Если журнальный сервер не готов к работе, вы можете пропустить этот шаг.

- a. **Адрес журнального сервера** - URL для подключения к серверу в формате http(s)://полное_dns_имя_сервера/ls/ , например: http://logserver.demo.local/ls/
- b. **Сертификат** - Сертификат для настройки двухстороннего TLS соединения между сервером Indeed AM и Indeed AM Log Server.

И **Информация**

Данную настройку не требуется указывать. В текущей версии системы Indeed AM не поддерживается работа 2-х стороннего TLS соединения.

- c. **Журналируемое поле объекта каталога** - Укажите формат в котором будет осуществляться логирование имени пользователя.
- d. **Журналируемое поле компьютера** - Укажите формат в котором будет осуществляться логирование поля "Компьютер".

И **Информация**

Для логирования в формате DNS потребуется дополнительная настройка. [Подробнее по настройке логирования в формате DNS.](#)

Master configuration AM Server

Журнальный сервер

Перед началом работы

Восстановление настроек

Каталог пользователей

Хранилище данных

Microsoft SQL

Ключ шифрования

Журнальный сервер

Сессионный секрет

Шифрование файла

Подтверждение

Результаты

Администратор системы

Результаты

Укажите параметры журнального сервера

Адрес журнального сервера

URL для подключения к серверу в формате http(s)://полное_dns_имя_сервера/имя_веб_приложения_по_умолчанию)

Сертификат

Журналируемое поле объекта каталога

Журналируемое поле компьютера

И

Если используется несколько серверов, укажите адрес бал нагрузки.

< Назад

Далее >

Примени

8. Шаг "**Сессионный секрет**". Сгенерируйте секрет для подписи токена, для этого нажмите "**Сгенерировать**". После генерации нажмите "**Далее**".
9. Шаг "**Шифрование файла**". Вы можете выполнить шифрование настроек конфигурационного файла.



Информация

В целях повышения безопасности рекомендуется выполнить шифрование конфигурационного файла.

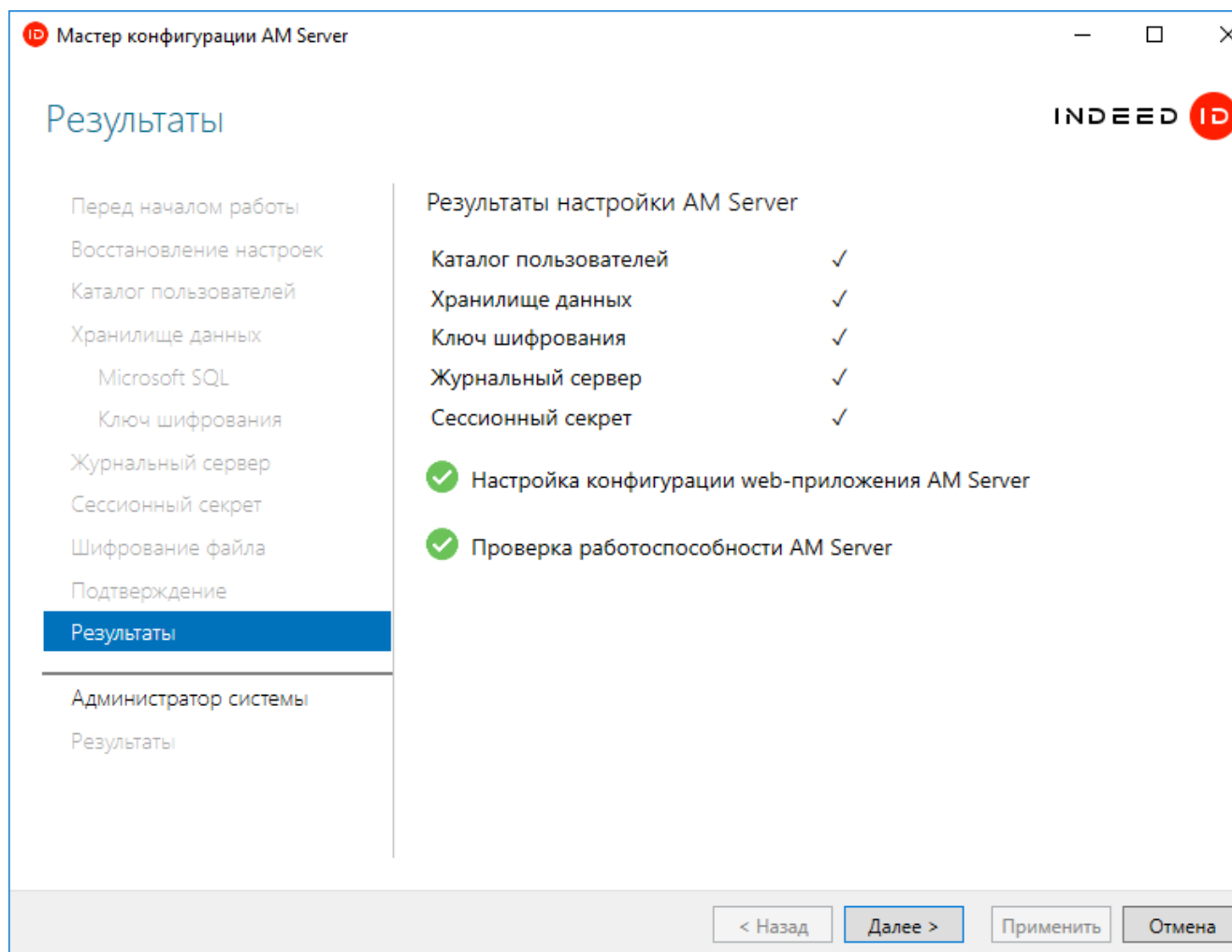
10. Шаг "**Подтверждение**". Убедитесь в корректности указанных данных и нажмите "**Применить**".



Информация

Рекомендуется сделать резервную копию конфигурационного файла, по умолчанию параметр "**Сохранить резервную копию параметров конфигурации**" активен.

11. Шаг "**Результаты**". Осуществляется проверка настроек и тестирование подключения к Indeed AM Server.



Настройка администратора системы



Информация

Пользователь, который указывается в качестве администратора системы, должен находиться в пользовательском каталоге.

1. На шаге "**Администратор системы**" задайте учетную запись администратора Indeed. Указанной учетной записи будут выданы первичные права администратора системы.

 Информация

Для настройки администратора требуется установленный Indeed AM Windows Password (***indeed AM<номер версии>\Indeed AM Providers\Indeed AM Windows Password Provider\<номер версии>***), так как при выдаче первичных прав указанному пользователю, осуществляется аутентификация на сервере Indeed AM

2. На шаге "**Результаты**" отображается статус настройки конфигурационного файла и статус настройки администратора системы.

Ручная настройка системы

Редактирование конфигурационного файла

 Информация

Для сохранения изменений в конфигурационном файле приложения, требуется запустить редактор с правами администратора.

Ошибки, возникшие при развертывании сервера AM (Например ошибка в конфигурационном файле), будут логироваться исходя из настроек LogServer.

Для генерации ключей шифрования рекомендуется использовать утилиту **EA.KeyGen.exe**, выбрав необходимый алгоритм из предложенного списка.

Информация

Если в пароле для сервисных пользователей используются следующие символы: **&**, **"**, **;**, **<**, **пробел**, то пароль следует указывать так:

Символ амперсанд (&) - При указании пароля для пользователя из AD или SQL символ требуется заменить на: **&**; Пример(AD\SQL): **password="Q1q2E3e4&"\Password=Q1q2E3e4&;**

Символ двойные кавычки (") - При указании пароля для пользователя из AD или SQL символ требуется заменить на: **"**; Для пользователя из SQL дополнительно требуется указать пароль в одинарных кавычках. Пример(AD\SQL): **password="Q1q2E3e4""\Password='Q1q2E3e4";**

Символ точка с запятой (;) - При указании пароля для пользователя из AD не требуется дополнительных действий, для пользователя из SQL требуется указать пароль в одинарных кавычках. Пример(AD\SQL): **password="Q1q2E3e4;"\Password='Q1q2E3e4;;**

Символ "меньше" (<) - При указании пароля для пользователя из AD или SQL символ требуется заменить на: **<**; Пример(AD\SQL): **password="Q1q2E3e4<"\Password=Q1q2E3e4<;**

Символ "Пробел" - При указании пароля для пользователя из AD не требуется дополнительных действий, для пользователя из SQL требуется указать пароль в одинарных кавычках. Пример(AD\SQL): **password="Q1q2E3e4 "\Password='Q1q2E3e4 ';**

Символ "Одинарной кавычки" (') - При указании пароля для пользователя из AD не требуется дополнительных действий, для пользователя из SQL требуется указать пароль в **"**, символ кавычки указать в обычном виде. Пример(AD\SQL): **password="Q1q2E3e4'"\Password="Q1q2E3e4'";**

1. Откройте конфигурационный файл сервера **Web.config** (C:\inetpub\wwwroot\am\core\Web.config).

2. Добавить секретный ключ для подписи токена для параметра "**secretKey**" тега "**logonSettings**". Параметр "**secretKey**" используется для создания токена пользователя в формате "**jwt**".

Пример

```
<logonSettings secretKey="67d7e6caec61d61239dc0b05f86063ed899931b581fa1ed8140d7843b320fe02"/>
```

3. Задать каталог пользователя системы, для этого необходимо отредактировать параметры в теге **adUserCatalogProvider**:
- a. **id** - произвольный уникальный идентификатор каталога.
 - b. **serverName** - имя домена Active Directory, в котором находится каталог.
 - c. **containerPath** - путь к контейнеру в виде Distinguished Name или весь домен, если для хранения пользователей используется весь домен.
 - d. **userName** - имя сервисной учетной записи для подключения к каталогу пользователей.
 - e. **password** - пароль сервисной учетной записи каталога пользователей в AD.

Пример

```
<adUserCatalogProviders>
  <adUserCatalogProvider id="UserId" serverName="indeed-id.local" containerPath="DC=demo,DC=local" userName="IndeedCatalogUser" password="Q1q2E3e4"/>
</adUserCatalogProviders>
```

4. Указать корневой идентификатор провайдера работы с каталогом, необходимо отредактировать атрибут **rootUserCatalogProviderId** в теге **userCatalogProviderSettings**.
- a. **rootUserCatalogProviderId** - задать значение, которое уже было задано в тэге **adUserCatalogProvider** в атрибуте **id**.

Пример

```
<userCatalogProviderSettings rootUserCatalogProviderId="UserId">
```


5. Задать хранилище данных системы. Для хранилища данных в SQL Server редактируем тег **dbContextSettings** и создаем тег **mssqlDbContext** с параметрами **id** и **connectionString**.
- rootDbContextId** - задать произвольно уникальное значение идентификатора хранилища.
 - id** - задать значение, которое уже было задано в тэге **rootDbContextId**.
 - Добавить параметр **connectionString**, со встроенными параметрами:
 - Data Source** - Задаёт экземпляр сервера. Это свойство является обязательным для всех соединений. Допустимые значения — сетевое имя или IP-адрес сервера, local или localhost для локальных соединений.
 - Initial Catalog** - Определяет имя базы данных.
 - User Id** - Имя пользователя для подключения к базе данных.
 - Password** - Пароль пользователя для подключения к базе данных.

Пример

```
<dbContextSettings rootDbContextId="mssql"> <mssqlDbContexts> <mssqlDbContext id="mssql" connectionString="Data Source=EASERVER\EASERVER;Initial Catalog=AM_Server_7; User Id=Admin-DB;Password=Q1q2E3e4;" /> </mssqlDbContexts> </dbContextSettings>
```

6. Задать ключ шифрования данных системы. Редактируем параметры в тэге **encryptionSettings**.
- cryptoAlgName** - указать использованный алгоритм шифрования.
 - cryptoKey** - значения ключа, сгенерированного утилитой.
 - certificateThumbprint** - Thumbprint сертификата, которым зашифрован ключ (чтобы не учитывать - нужно удалить атрибут).

Пример

```
<encryptionSettings cryptoAlgName="Aes" cryptoKey="90ce7dbc3ff94a7867abc6672c23c2c3717d38af42f04293130cb68a34ecc2" />
```

7. Задать администратора системы. Редактируем параметр **userId** тега **accessControlAdminSettings**.

- а. **userId** - идентификатор пользователя в формате: "<**Идентификатор каталога**><**нижнее подчеркивание**><**GUID Администратора Системы**>".

 Примечание

Пользователь должен находиться внутри каталога пользователей.

При использовании нескольких пользовательских контейнеров для <**Идентификатор каталога**> указывается **id** контейнера в котором находится администратор системы.

Пример

```
<accessControlAdminSettings userId="UserId_84e9ccd9-73a2-43c7-abc6-604a16902037"/>
```

 Информация

Получить GUID можно с помощью команды **PowerShell**. Предварительно необходимо установить компонент **Remote Server Administration Tools**:

Пример

```
Get-ADUser YouUserName -Properties * | Select ObjectGUID
```

8. Задаем url для подключения к лог серверу. Редактируем тег **logServer**.

- а. **URL** - url для подключения к log серверу в формате **http(s)://имя сервера/ls/api**.

 Примечание

Если используется несколько серверов, указываем адрес балансировщика нагрузки.

- б. **CertificateThumbprint** - если закрытый ключ в реестре, а сертификат в хранилище компьютера.
- в. **CertificateFilePath** - если ключевая пара в pfx.
- г. **CertificateFilePassword** - пароль от pfx.

Пример

```
<logServer Url="http://log.indeed-id.local/l5/api/" CertificateThumbprint=""  
CertificateFilePath="" CertificateFilePassword=""/>
```

Шифрование/Расшифрование конфигурационного файла

- а. Запустите командную строку от имени **"Администратора"**.
- б. В командной строке перейдите в папку с утилитой для шифрования.



Информация

Утилита шифрует секции: **logServer, logonSettings, userCatalogProviderSettings, encryptionSettings, dbContextSettings**.
Рекомендуется зашифровать все секции.

- i. Шифрование/Расшифрование отдельных секций.

Для **шифрования отдельной секции** необходимо выполнить команду вида: EA.Config.Encryptor /encrypt "Путь к конфигурационному файлу сервера" "Имя секции"

Пример

```
EA.Config.Encryptor /encrypt "C:\inetpub\wwwroot\am\core\Web.config"  
"logServer"
```

Для **расшифровки отдельной секции** необходимо выполнить команду вида: EA.Config.Encryptor /decrypt "Путь к конфигурационному файлу сервера" "Имя секции"

Пример

```
EA.Config.Encryptor /decrypt "C:\inetpub\wwwroot\am\core\Web.config"  
"logServer"
```

ii. Шифрование/Расшифрование всех секций.

Для **шифрования всех секций** необходимо запустить скрипт **encryptConfigs.bat**.

```
C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>encryptConfigs.bat

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>rem logServer

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>EA.Config.Encryptor /encrypt "C:\inetpub\wwwroot\ease
rver\Web.config" "logServer"
Configuration section has been encrypted successfully.

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>rem logonSettings

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>EA.Config.Encryptor /encrypt "C:\inetpub\wwwroot\ease
rver\Web.config" "logonSettings"
Configuration section has been encrypted successfully.

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>rem userCatalogProviderSettings

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>EA.Config.Encryptor /encrypt "C:\inetpub\wwwroot\ease
rver\Web.config" "userCatalogProviderSettings"
Configuration section has been encrypted successfully.

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>rem encryptionSettings

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>EA.Config.Encryptor /encrypt "C:\inetpub\wwwroot\ease
rver\Web.config" "encryptionSettings"
Configuration section has been encrypted successfully.

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>rem dbContextSettings

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>EA.Config.Encryptor /encrypt "C:\inetpub\wwwroot\ease
rver\Web.config" "dbContextSettings"
Configuration section has been encrypted successfully.

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>pause
Для продолжения нажмите любую клавишу . . .
```

Для **расшифровки всех секций** необходимо выполнить скрипт **decryptConfigs.bat**

```
C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>decryptConfigs.bat

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>rem logServer

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>EA.Config.Encryptor /decrypt "C:\inetpub\wwwroot\ease
rver\Web.config" "logServer"
Configuration section has been decrypted successfully.

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>rem logonSettings

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>EA.Config.Encryptor /decrypt "C:\inetpub\wwwroot\ease
rver\Web.config" "logonSettings"
Configuration section has been decrypted successfully.

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>rem userCatalogProviderSettings

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>EA.Config.Encryptor /decrypt "C:\inetpub\wwwroot\ease
rver\Web.config" "userCatalogProviderSettings"
Configuration section has been decrypted successfully.

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>rem encryptionSettings

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>EA.Config.Encryptor /decrypt "C:\inetpub\wwwroot\ease
rver\Web.config" "encryptionSettings"
Configuration section has been decrypted successfully.

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>rem dbContextSettings

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>EA.Config.Encryptor /decrypt "C:\inetpub\wwwroot\ease
rver\Web.config" "dbContextSettings"
Configuration section has been decrypted successfully.

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>pause
Для продолжения нажмите любую клавишу . . .
```

Защита от перебора

Для того, чтобы включить защиту от перебора UserId, необходимо на сервере Indeed AM, в файле **C:\inetpub\wwwroot\am\core\Web.config**, указать список приложений разделенных запятыми:

Пример

```
<appSettings>
  <add key="bruteForceProtectionApps" value="SAML Identity Provider, Windows Logon, IIS
Extension" />
  ...
</appSettings>
```

Настройка нескольких пользовательских каталогов



Информация

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 **"accessControlAdminSettings"**, 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**.



Информация

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

1. Добавьте внутри тега **adUserCatalogProviders** строки для подключения к контейнерам.

Пример

```
<userCatalogProviderSettings rootUserCatalogProviderId="user">
  <userCatalogProviders>
    <sqlUserCatalogProviders></sqlUserCatalogProviders>
    <adUserCatalogProviders>
      <adUserCatalogProvider id="Ad1" serverName="demo.local" containerPath="OU=Indeed_Users,
DC=demo,DC=local" userName="demo\ind-user" password="Q1q2E3e4" />
      <adUserCatalogProvider id="Ad2" serverName="demo.local" containerPath="
OU=inDomainUsers,DC=demo,DC=local" userName="demo\ind-user" password="Q1q2E3e4" />
      <adUserCatalogProvider id="Ad3" serverName="inforest.demo.local" containerPath="
OU=UsersInForest,DC=inforest,DC=demo,DC=local" userName="inforest\cataloguser1" password="
Q1q2E3e4" />
      <adUserCatalogProvider id="Ad4" serverName="newforest.local" containerPath="
OU=Usersoutforest,DC=newforest,DC=local" userName="newforest\cataloguser2" password="
Q1q2E3e4" />
    </adUserCatalogProviders>
  </userCatalogProviders>
</userCatalogProviderSettings>
```

2. Добавьте внутри тега **orUserCatalogProviders** тег **orUserCatalogProvider** с параметром **id**.



Информация

Значение параметра **id** должно соответствовать значению заданному в параметре **rootUserCatalogProviderId**

3. Добавьте внутри тега **orUserCatalogProvider** тег **userCatalogProviders**. Внутри тега **userCatalogProviders** добавьте теги **userCatalogProvider** 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

Данные теги могут отсутствовать в конфигурационном файле, если ранее было выполнено шифрование конфигурационного файла с не заданными параметрами. Если теги отсутствуют, то добавьте их вручную. Полная структура файла представлена ниже.

Пример

```
<orUserCatalogProviders>
  <orUserCatalogProvider id="user">
    <userCatalogProviders>
      <userCatalogProvider id="Ad1" ignoreExceptions="true" />
      <userCatalogProvider id="Ad2" ignoreExceptions="true" />
      <userCatalogProvider id="Ad3" ignoreExceptions="true" />
      <userCatalogProvider id="Ad4" ignoreExceptions="true" />
    </userCatalogProviders>
  </orUserCatalogProvider>
</orUserCatalogProviders>
```

Пример структуры файла

Пример

```
<accessControlAdminSettings userId="UserId_891f2b6c-9a55-4e1a-b69b-b4d6418f4c4c"/>
<logonSettings secretKey="*****"/>
<userCatalogProviderSettings rootUserCatalogProviderId="user">
  <userCatalogProviders>
    <sqlUserCatalogProviders>
    </sqlUserCatalogProviders>
    <adUserCatalogProviders>
      <adUserCatalogProvider id="UserId" serverName="new.loc" containerPath="DC=new,
DC=loc"
        userName="indeed-users" password="Q1q2E3e4" />
      <adUserCatalogProvider id="UserId1" serverName="test.new.loc" containerPath="
DC=test,DC=loc"
        userName="indeed-users" password="Q1q2E3e4" />
    </adUserCatalogProviders>
  </userCatalogProviders>
  <combineRules>
    <orUserCatalogProviders>
      <orUserCatalogProvider id="user">
        <userCatalogProviders>
          <userCatalogProvider id="UserId" ignoreExceptions="true" />
          <userCatalogProvider id="UserId1" ignoreExceptions="true" />
        </userCatalogProviders>
      </orUserCatalogProvider>
    </orUserCatalogProviders>
    <andUserCatalogProviders>
    </andUserCatalogProviders>
  </combineRules>
</userCatalogProviderSettings>
```

LDAP-фильтр при поиске пользователей и групп в Active Directory

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

Для этого нужно:

1. На сервере Indeed AM открыть файл конфигурации сервера **C:\inetpub\wwwroot\am\core\Web.config**
2. Найти секцию **"adUserCatalogProvider"** и в задать в ней атрибуты **catalogFilter** и **dnFilter** для фильтрации элементов пользовательского каталога:
 - a. **catalogFilter** - строка LDAP-запрос для фильтрации элементов на этапе выполнения запроса к AD. Не поддерживает фильтрацию по частичному совпадению атрибутов distinguishedName и canonicalName (для этих целей добавлен dnFilter);
 - b. **dnFilter** (distinguishedName фильтр) - содержит регулярное выражение для фильтрации результатов после выполнения LDAP-запроса к AD.

Примеры использования фильтров

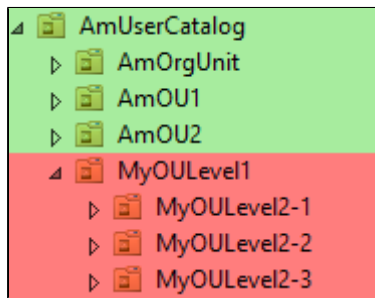
catalogFilter:

- Исключение определенных пользователей
& (! (name=AmUser1)) (! (name=AmUser2) (! (name=AmUser3)))
- Исключение всех дочерних элементов 1 уровня указанной OU
!(msDS-parentdistinguishedname=OU=AmOrgUnit, OU=AmUserCatalog, DC=dom, DC=local)
- Исключение всех членов группы
!(memberof=CN=AmGroup, OU=AmUserCatalog, DC=dom, DC=local)

dnFilter:

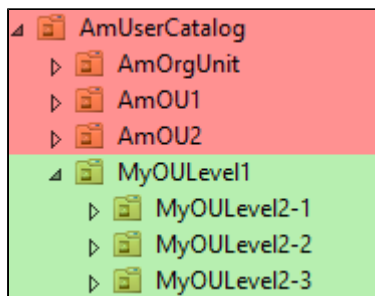
- Исключение OU и всех дочерних элементов:

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



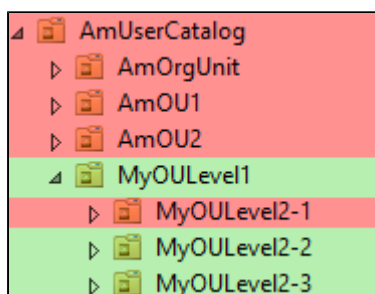
- Использование только указанной OU:

(^.*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\$)



Indeed Access Manager Server с хранилищем данных в PostgreSQL

Информация

Файлы для Indeed AM Server расположены в *Indeed Access Manager Server/<номер версии>*.

- **IndeedAM.Server-<номер версии>.x64.ru-ru.msi** — пакет для установки Indeed AM Server.
- **/Misc/EA.KeyGen.exe** — утилита для генерации ключей шифрования.
- **/Misc/AccessControlInitialConfig/EA.Server.AccessControlInitialConfig.exe** — утилита первичной конфигурации.
- **/Misc/AccessControlInitialConfig/EA.Server.AccessControlInitialConfig.exe.config** — файл для настройки утилиты конфигурации.
- **/Misc/EA.Config.Encryptor/EA.Config.Encryptor.exe** — утилита для шифрования конфигурационного файла.
- **/Misc/EA.Config.Encryptor/encryptConfigs.bat** — скрипт для шифрования всех секций конфигурационного файла.
- **/Misc/EA.Config.Encryptor/decryptConfigs.bat** — скрипт для расшифровки всех секций конфигурационного файла.

Установка

1. Выполнить установку Indeed AM Server через запуск соответствующего пакета.

2. Добавить привязку **https** в настройках **Default Web Site** в IIS Manager.



Информация

Indeed Access Manager Server является Web приложением, которое работает на базе IIS, в процессе установки для него по умолчанию включается обязательно требование SSL в настройках, что в свою очередь требует включенной привязки https.

Если вы не намерены использовать протокол https, необходимо отключить требование SSL в настройках IIS для core и в конфигурационном файле сервера (C:\inetpub\wwwroot\am\core\Web.config) изменить значение параметра "requireHttps" на "false".

```
<appSettings>  
<add key="requireHttps" value="false" />  
</appSettings>
```

- a. Запустите **IIS Manager** и раскройте пункт **Сайты (Sites)**.
- b. Выберите сайт **Default Web Site** и нажмите **Привязки (Bindings)** в разделе **Действия (Actions)**.
- c. Нажмите **Добавить (Add)**:
 - i. **Тип (Type)** - https.
 - ii. **Порт (Port)** - 443.
 - iii. Выберите **SSL-сертификат (SSL Certificate)**.
- d. Сохраните привязку.

Настройка с помощью мастера конфигурации



Информация

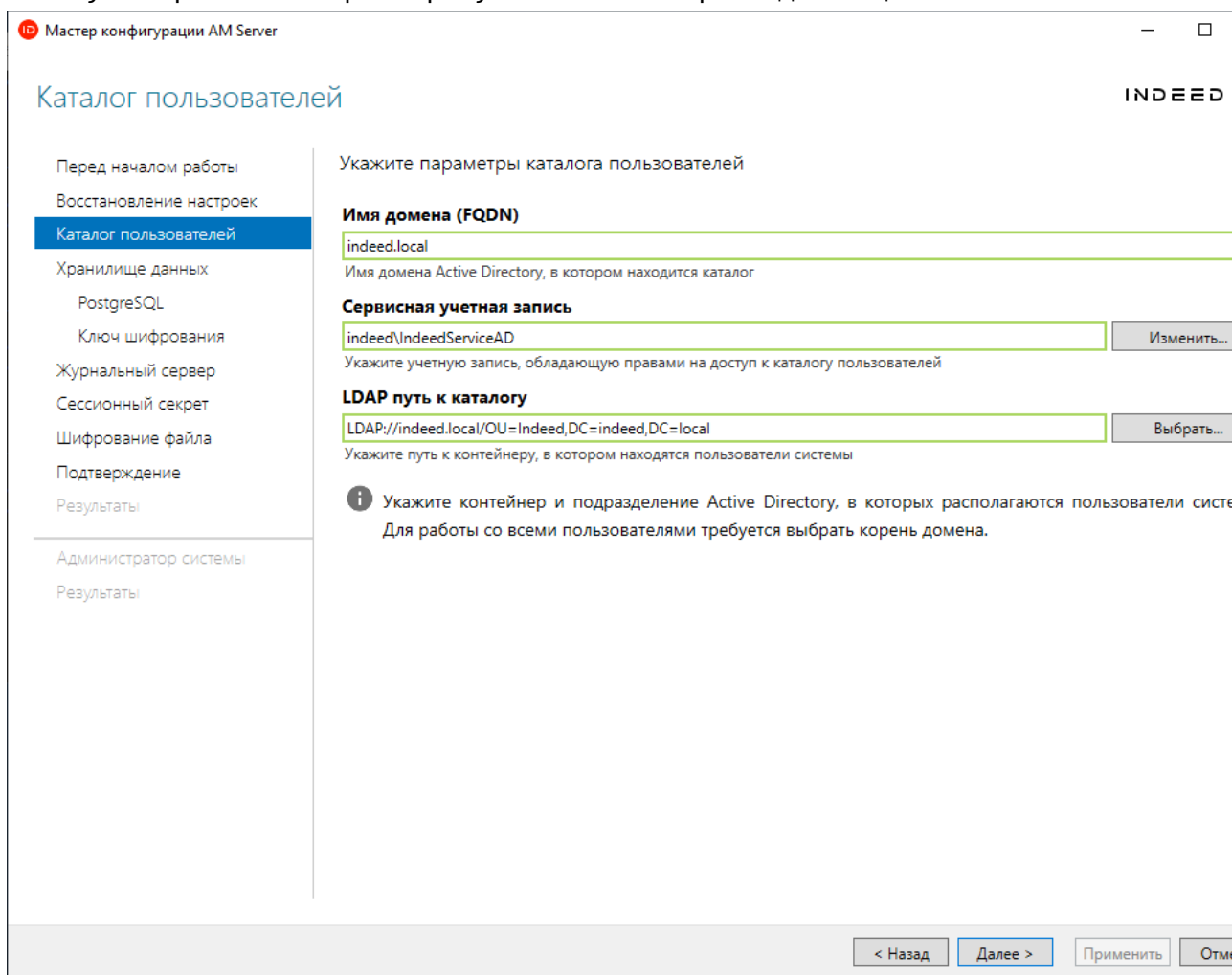
Мастер конфигурации по умолчанию запускается автоматически после установки Indeed AM Server, если запуск не был отключен пользователем.

Для запуска мастера вручную откройте файл: C:\Program Files\Indeed AM\Wizard\EA.Server.Wizard.exe

Информация

В мастер включена автоматическая проверка введенных данных, в случае успешного ввода - поля будут подсвечены зеленым цветом, и вы сможете перейти к следующему шагу, если данные введены некорректно, то поля будут подсвечены красным, и вы не сможете перейти к следующему шагу пока не укажете корректные данные.

1. На шаге **"Перед началом работы"** нажмите **"Далее"**.
2. На шаге **"Восстановление настроек"** нажмите **"Далее"**.
3. На шаге **"Каталог пользователей"** укажите следующие параметры:
 - a. **Имя домена (FQDN)** - Укажите полное имя домена, например: *domain.local*.
 - b. **Сервисная учетная запись** - Укажите сервисную учетную запись, обладающую правами доступа к пользовательскому каталогу. Нажмите кнопку **"Изменить"** и укажите требуемые данные учетной записи.
 - c. **LDAP путь к каталогу** - Укажите путь к каталогу с пользователями. Нажмите кнопку **"Выбрать"** и выберите требуемый контейнер или домен целиком.



4. На шаге **"Хранилище данных"** выберите тип хранилища PostgreSQL.

5. В строке подключения к базе данных указываем:

- a. **server** - ip адрес сервера базы данных.
- b. **port** - Используемый порт. По умолчанию - 5432.
- c. **user id** - Имя пользователя, который имеет полные права для базы данных.
- d. **password** - пароль пользователя.
- e. **database** - база данных, содержащая данные об Indeed AM Server.

Нажмите "**Тест**", чтобы проверить подключение к базе данных.

Master configuration of AM Server

PostgreSQL

Укажите параметры подключения к хранилищу данных Indeed AM в среде PostgreSQL

Строка подключения к базе данных

server=192.168.1.2;port=5432;user id=postgres;password=!QAZ2wsx;database=indeedamcore

Тест

Строка подключения к PostgreSQL серверу в формате:
server=server_dns_name;port=5432;user id=account_name;password=account_password;database=database_name
(5432 - порт подключения по умолчанию)

< Назад Далее > Применить

6. Шаг "**Ключ шифрования**". Выберите алгоритм шифрования, нажмите "**Сгенерировать**" и нажмите "**Далее**".



Информация

Настоятельно рекомендуется выполнить резервную копию ключа шифрования и сохранить в защищенном месте.

7. На шаге "**Журнальный сервер**" укажите следующие данные:

 Информация

Чтобы при тестировании соединения не возникало ошибок, требуется полностью настроенный лог-сервер, с настроенной базой данных или установленным компонентом EventLog. Если журнальный сервер не готов к работе, вы можете пропустить этот шаг.

- a. **Адрес журнального сервера** - URL для подключения к серверу в формате http(s)://полное_dns_имя_сервера/ls/ , например: <http://logserver.demo.local/ls/>
- b. **Сертификат** - Сертификат для настройки двухстороннего TLS соединения между сервером Indeed AM и Indeed AM Log Server.

И Информация

Данную настройку не требуется указывать. В текущей версии системы Indeed AM не поддерживается работа 2-х стороннего TLS соединения.

- c. **Журналируемое поле объекта каталога** - Укажите формат в котором будет осуществляться логирование имени пользователя.
- d. **Журналируемое поле компьютера** - Укажите формат в котором будет осуществляться логирование поля "Компьютер".

И Информация

Для логирования в формате DNS потребуется дополнительная настройка

Master configuration of AM Server

Журнальный сервер

Перед началом работы

Восстановление настроек

Каталог пользователей

Хранилище данных

Microsoft SQL

Ключ шифрования

Журнальный сервер

Сессионный секрет

Шифрование файла

Подтверждение

Результаты

Администратор системы

Результаты

Укажите параметры журнального сервера

Адрес журнального сервера

URL для подключения к серверу в формате http(s)://полное_dns_имя_сервера/имя_веб_приложения_по_умолчанию)

Сертификат

Журналируемое поле объекта каталога

Журналируемое поле компьютера

И

Если используется несколько серверов, укажите адрес балансировки.

< Назад

Далее >

Применить

8. Шаг "**Сессионный секрет**". Сгенерируйте секрет для подписи токена, для этого нажмите "**Сгенерировать**". После генерации нажмите "**Далее**".
9. Шаг "**Шифрование файла**". Вы можете выполнить шифрование настроек конфигурационного файла.



Информация

В целях повышения безопасности рекомендуется выполнить шифрование конфигурационного файла.

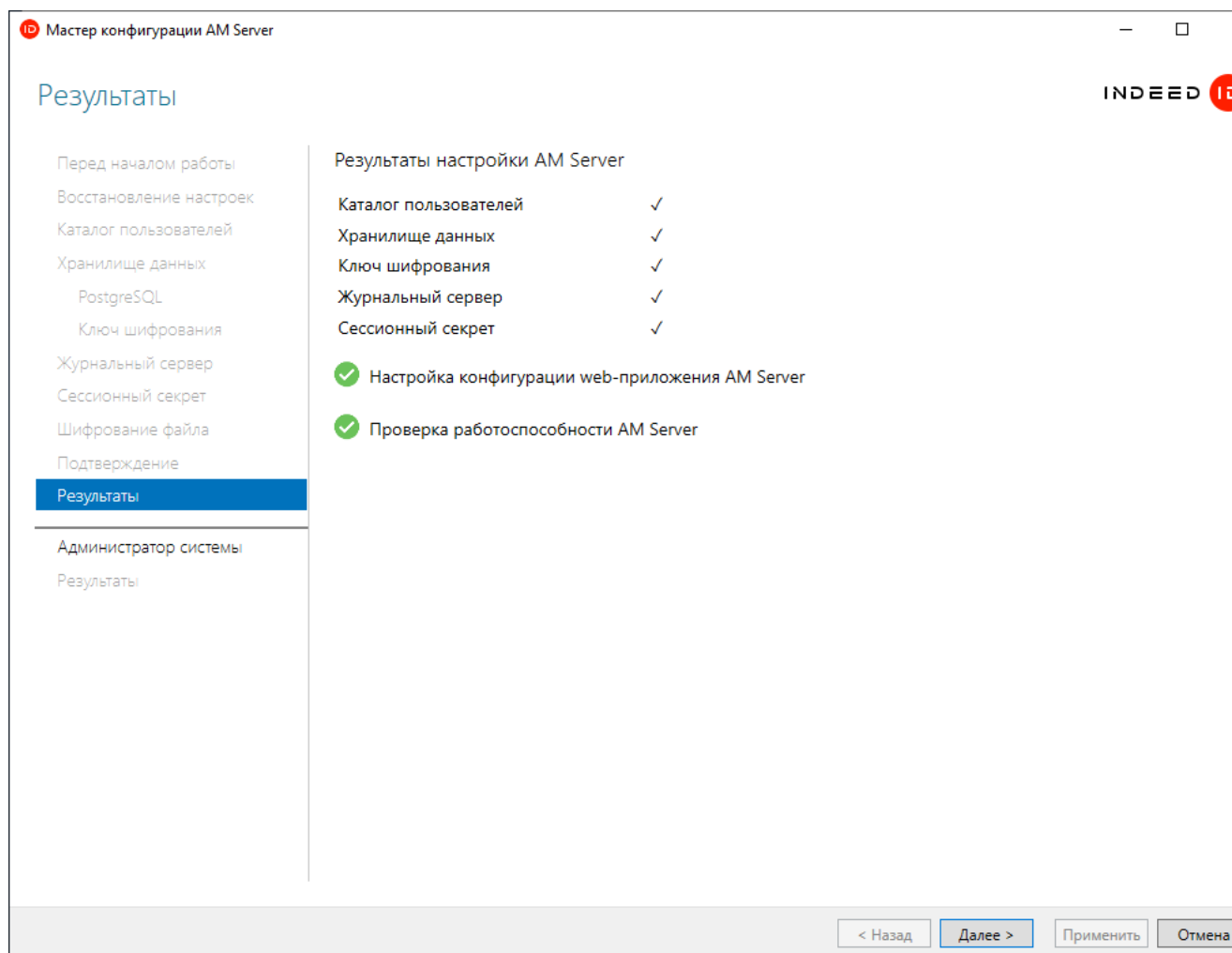
10. Шаг "**Подтверждение**". Убедитесь в корректности указанных данных и нажмите "**Применить**".



Информация

Рекомендуется сделать резервную копию конфигурационного файла, по умолчанию параметр "**Сохранить резервную копию параметров конфигурации**" активен.

11. Шаг "**Результаты**". Осуществляется проверка настроек и тестирование подключения к Indeed AM Server.



Настройка администратора системы



Информация

Пользователь, который указывается в качестве администратора системы, должен находиться в пользовательском каталоге.

1. На шаге "**Администратор системы**" задайте учетную запись администратора Indeed. Указанной учетной записи будут выданы первичные права администратора системы.

 Информация

Для настройки администратора требуется установленный Indeed AM Windows Password, так как при выдаче первичных прав указанному пользователю, осуществляется аутентификация на сервере Indeed AM

2. На шаге "**Результаты**" отображается статус настройки конфигурационного файла и статус настройки администратора системы.

Ручная настройка системы

Редактирование конфигурационного файла

 Информация

Для сохранения изменений в конфигурационном файле приложения, требуется запустить редактор с правами администратора.

Ошибки, возникшие при развертывании сервера AM (Например ошибка в конфигурационном файле), будут логироваться исходя из настроек LogServer.

Для генерации ключей шифрования рекомендуется использовать утилиту **EA.KeyGen.exe**, выбрав необходимый алгоритм из предложенного списка.

Информация

Если в пароле для сервисных пользователей используются следующие символы: **&**, **"**, **;**, **<**, **пробел** , то пароль следует указывать так:

Символ амперсанд (&) - При указании пароля для пользователя из AD или SQL символ требуется заменить на: **&** Пример(AD\SQL): **password="Q1q2E3e4&"\Password=Q1q2E3e4&;**

Символ двойные кавычки (") - При указании пароля для пользователя из AD или SQL символ требуется заменить на: **"** Для пользователя из SQL дополнительно требуется указать пароль в одинарных кавычках. Пример(AD\SQL): **password="Q1q2E3e4""\Password='Q1q2E3e4";**

Символ точка с запятой (;) - При указании пароля для пользователя из AD не требуется дополнительных действий, для пользователя из SQL требуется указать пароль в одинарных кавычках. Пример(AD\SQL): **password="Q1q2E3e4;"\Password='Q1q2E3e4;;**

Символ "меньше" (<) - При указании пароля для пользователя из AD или SQL символ требуется заменить на: **<** Пример(AD\SQL): **password="Q1q2E3e4<"\Password=Q1q2E3e4<;**

Символ "Пробел" - При указании пароля для пользователя из AD не требуется дополнительных действий, для пользователя из SQL требуется указать пароль в одинарных кавычках. Пример(AD\SQL): **password="Q1q2E3e4 "\Password='Q1q2E3e4 ';**

Символ "Одинарной кавычки" (') - При указании пароля для пользователя из AD не требуется дополнительных действий, для пользователя из SQL требуется указать пароль в **"** , символ кавычки указать в обычном виде . Пример(AD\SQL): **password="Q1q2E3e4'"'\Password="Q1q2E3e4'";**

1. Откройте конфигурационный файл сервера **Web.config** (C:\inetpub\wwwroot\am\core\Web.config).

2. Добавить секретный ключ для подписи токена для параметра "**secretKey**" тега "**loginSettings**". Параметр "**secretKey**" используется для создания токена пользователя в формате "**jwt**".

Пример

```
<loginSettings secretKey="67d7e6caec61d61239dc0b05f86063ed899931b581fa1ed8140d7843b320fe02"/>
```

3. Задать каталог пользователя системы, для этого необходимо отредактировать параметры в теге **adUserCatalogProvider**:
- a. **id** - произвольный уникальный идентификатор каталога.
 - b. **serverName** - имя домена Active Directory, в котором находится каталог.
 - c. **containerPath** - путь к контейнеру в виде Distinguished Name или весь домен, если для хранения пользователей используется весь домен.
 - d. **userName** - имя сервисной учетной записи для подключения к каталогу пользователей.
 - e. **password** - пароль сервисной учетной записи каталога пользователей в AD.

Пример

```
<adUserCatalogProviders>
  <adUserCatalogProvider id="UserId" serverName="indeed-id.local" containerPath="DC=demo,DC=local" userName="IndeedCatalogUser" password="Q1q2E3e4"/>
</adUserCatalogProviders>
```

4. Указать корневой идентификатор провайдера работы с каталогом, необходимо отредактировать атрибут **rootUserCatalogProviderId** в теге **userCatalogProviderSettings**.
- a. **rootUserCatalogProviderId** - задать значение, которое уже было задано в тэге **adUserCatalogProvider** в атрибуте **id**.

Пример

```
<userCatalogProviderSettings rootUserCatalogProviderId="UserId">
```

5. Задать хранилище данных системы. Для хранилища данных в PostgreSQL Server редактируем тег **dbContextSettings** и создаем тег **postgresqlDbContexts** с параметрами **id** и **connectionString**.

- a. **rootDbContextId** - задать произвольно уникальное значение идентификатора хранилища.
- b. **id** - задать значение, которое уже было задано в тэге **rootDbContextId**.
- c. Добавить параметр **connectionString**, со встроенными параметрами:
 - **Server** - DNS\IP адрес сервера с БД PostgreSQL.
 - **Database** - Определяет имя базы данных.
 - **Integrated Security** - Включает встроенную аутентификацию.



Информация

Встроенная аутентификация не поддерживается.

- **User ID** - Имя пользователя для подключения к базе данных.
- **Password** - Пароль пользователя для подключения к базе данных.

Пример

```
<dbContextSettings rootDbContextId="postgreSql">
  <postgresqlDbContexts>
    <postgresqlDbContext connectionString="server=192.168.1.2;port=5432;user id=postgres;
password=!QAZZwsx;database=indeedamcore"
    id="postgreSql" />
  </postgresqlDbContexts>
</dbContextSettings>
```

6. Задать ключ шифрования данных системы. Редактируем параметры в тэге **encryptionSettings**.

- a. **cryptoAlgName** - указать использованный алгоритм шифрования.
- b. **cryptoKey** - значения ключа, сгенерированного утилитой.
- c. **certificateThumbprint** - Thumbprint сертификата, которым зашифрован ключ (чтобы не учитывать - нужно удалить атрибут).

Пример

```
<encryptionSettings cryptoAlgName="Aes" cryptoKey="
90ce7dbc3ff94a7867abc6672c23cce2c3717d38af42f04293130cb68a34ecc2"/>
```

7. Задать администратора системы. Редактируем параметр **userId** тега **accessControlAdminSettings**.

- а. **userId** - идентификатор пользователя в формате: "<**Идентификатор каталога**><нижнее подчеркивание><GUID Администратора Системы>".

 Примечание

Пользователь должен находиться внутри каталога пользователей.

При использовании нескольких пользовательских контейнеров для <**Идентификатор каталога**> указывается **id** контейнера в котором находится администратор системы.

Пример

```
<accessControlAdminSettings userId="UserId_84e9ccd9-73a2-43c7-abc6-604a16902037"/>
```

 Информация

Получить GUID можно с помощью команды **PowerShell**. Предварительно необходимо установить компонент **Remote Server Administration Tools**:

Пример

```
Get-ADUser YouUserName -Properties * | Select ObjectGUID
```

8. Задаем url для подключения к лог серверу. Редактируем тег **logServer**.

- а. **URL** - url для подключения к лог серверу в формате **http(s)://имя сервера/ls/api**.

 Примечание

Если используется несколько серверов, указываем адрес балансировщика нагрузки.

- б. **CertificateThumbprint** - если закрытый ключ в реестре, а сертификат в хранилище компьютера.
- в. **CertificateFilePath** - если ключевая пара в pfx.
- г. **CertificateFilePassword** - пароль от pfx.

Пример

```
<logServer Url="http://log.indeed-id.local/l5/api/" CertificateThumbprint=""  
CertificateFilePath="" CertificateFilePassword=""/>
```

Шифрование/Расшифрование конфигурационного файла

- а. Запустите командную строку от имени **"Администратора"**.
- б. В командной строке перейдите в папку с утилитой для шифрования.



Информация

Утилита шифрует секции: **logServer, logonSettings, userCatalogProviderSettings, encryptionSettings, dbContextSettings**.
Рекомендуется зашифровать все секции.

- i. Шифрование/Расшифрование отдельных секций.

Для **шифрования отдельной секции** необходимо выполнить команду вида: EA.Config.Encryptor /encrypt "Путь к конфигурационному файлу сервера" "Имя секции"

Пример

```
EA.Config.Encryptor /encrypt "C:\inetpub\wwwroot\am\core\Web.config"  
"logServer"
```

Для **расшифровки отдельной секции** необходимо выполнить команду вида: EA.Config.Encryptor /decrypt "Путь к конфигурационному файлу сервера" "Имя секции"

Пример

```
EA.Config.Encryptor /decrypt "C:\inetpub\wwwroot\am\core\Web.config"  
"logServer"
```

ii. Шифрование/Расшифрование всех секций.

Для **шифрования всех секций** необходимо запустить скрипт **encryptConfigs.bat**.

```
C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>encryptConfigs.bat

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>rem logServer

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>EA.Config.Encryptor /encrypt "C:\inetpub\wwwroot\ease
rver\Web.config" "logServer"
Configuration section has been encrypted successfully.

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>rem logonSettings

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>EA.Config.Encryptor /encrypt "C:\inetpub\wwwroot\ease
rver\Web.config" "logonSettings"
Configuration section has been encrypted successfully.

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>rem userCatalogProviderSettings

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>EA.Config.Encryptor /encrypt "C:\inetpub\wwwroot\ease
rver\Web.config" "userCatalogProviderSettings"
Configuration section has been encrypted successfully.

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>rem encryptionSettings

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>EA.Config.Encryptor /encrypt "C:\inetpub\wwwroot\ease
rver\Web.config" "encryptionSettings"
Configuration section has been encrypted successfully.

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>rem dbContextSettings

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>EA.Config.Encryptor /encrypt "C:\inetpub\wwwroot\ease
rver\Web.config" "dbContextSettings"
Configuration section has been encrypted successfully.

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>pause
Для продолжения нажмите любую клавишу . . .
```

Для **расшифровки всех секций** необходимо выполнить скрипт **decryptConfigs.bat**

```
C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>decryptConfigs.bat

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>rem logServer

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>EA.Config.Encryptor /decrypt "C:\inetpub\wwwroot\ease
rver\Web.config" "logServer"
Configuration section has been decrypted successfully.

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>rem logonSettings

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>EA.Config.Encryptor /decrypt "C:\inetpub\wwwroot\ease
rver\Web.config" "logonSettings"
Configuration section has been decrypted successfully.

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>rem userCatalogProviderSettings

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>EA.Config.Encryptor /decrypt "C:\inetpub\wwwroot\ease
rver\Web.config" "userCatalogProviderSettings"
Configuration section has been decrypted successfully.

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>rem encryptionSettings

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>EA.Config.Encryptor /decrypt "C:\inetpub\wwwroot\ease
rver\Web.config" "encryptionSettings"
Configuration section has been decrypted successfully.

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>rem dbContextSettings

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>EA.Config.Encryptor /decrypt "C:\inetpub\wwwroot\ease
rver\Web.config" "dbContextSettings"
Configuration section has been decrypted successfully.

C:\Users\Admin-Indeed\Desktop\EA.Config.Encryptor>pause
Для продолжения нажмите любую клавишу . . .
```


Защита от перебора

Для того, чтобы включить защиту от перебора UserId, необходимо на сервере Indeed AM, в файле **C:\inetpub\wwwroot\am\core\Web.config**, указать список приложений разделенных запятыми:

Пример

```
<appSettings>
  <add key="bruteForceProtectionApps" value="SAML Identity Provider, Windows Logon, IIS Extension" />
  ...
</appSettings>
```

Настройка нескольких пользовательских каталогов



Информация

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 **"accessControlAdminSettings"**, 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**.



Информация

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

1. Добавьте внутри тега **adUserCatalogProviders** строки для подключения к контейнерам.

Пример

```
<userCatalogProviderSettings rootUserCatalogProviderId="user">
  <userCatalogProviders>
    <sqlUserCatalogProviders></sqlUserCatalogProviders>
    <adUserCatalogProviders>
      <adUserCatalogProvider id="Ad1" serverName="demo.local" containerPath="OU=Indeed_Users,
DC=demo,DC=local" userName="demo\ind-user" password="Q1q2E3e4" />
      <adUserCatalogProvider id="Ad2" serverName="demo.local" containerPath="
OU=inDomainUsers,DC=demo,DC=local" userName="demo\ind-user" password="Q1q2E3e4" />
      <adUserCatalogProvider id="Ad3" serverName="inforest.demo.local" containerPath="
OU=UsersInForest,DC=inforest,DC=demo,DC=local" userName="inforest\cataloguser1" password="
Q1q2E3e4" />
      <adUserCatalogProvider id="Ad4" serverName="newforest.local" containerPath="
OU=Usersoutforest,DC=newforest,DC=local" userName="newforest\cataloguser2" password="
Q1q2E3e4" />
    </adUserCatalogProviders>
  </userCatalogProviders>
</userCatalogProviderSettings>
```

2. Добавьте внутри тега **orUserCatalogProviders** тег **orUserCatalogProvider** с параметром **id**.



Информация

Значение параметра **id** должно соответствовать значению заданному в параметре **rootUserCatalogProviderId**

3. Добавьте внутри тега **orUserCatalogProvider** тег **userCatalogProviders**. Внутри тега **userCatalogProviders** добавьте теги **userCatalogProvider** 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

Данные теги могут отсутствовать в конфигурационном файле, если ранее было выполнено шифрование конфигурационного файла с не заданными параметрами. Если теги отсутствуют, то добавьте их вручную. Полная структура файла представлена ниже.

Пример

```
<orUserCatalogProviders>
  <orUserCatalogProvider id="user">
    <userCatalogProviders>
      <userCatalogProvider id="Ad1" ignoreExceptions="true" />
      <userCatalogProvider id="Ad2" ignoreExceptions="true" />
      <userCatalogProvider id="Ad3" ignoreExceptions="true" />
      <userCatalogProvider id="Ad4" ignoreExceptions="true" />
    </userCatalogProviders>
  </orUserCatalogProvider>
</orUserCatalogProviders>
```

Пример структуры файла

Пример

```
<accessControlAdminSettings userId="UserId_891f2b6c-9a55-4e1a-b69b-b4d6418f4c4c"/>
<logonSettings secretKey="*****"/>
<userCatalogProviderSettings rootUserCatalogProviderId="user">
  <userCatalogProviders>
    <sqlUserCatalogProviders>
    </sqlUserCatalogProviders>
    <adUserCatalogProviders>
      <adUserCatalogProvider id="UserId" serverName="new.loc" containerPath="DC=new,
DC=loc"
        userName="indeed-users" password="Q1q2E3e4" />
      <adUserCatalogProvider id="UserId1" serverName="test.new.loc" containerPath="
DC=test,DC=loc"
        userName="indeed-users" password="Q1q2E3e4" />
    </adUserCatalogProviders>
  </userCatalogProviders>
  <combineRules>
    <orUserCatalogProviders>
      <orUserCatalogProvider id="user">
        <userCatalogProviders>
          <userCatalogProvider id="UserId" ignoreExceptions="true" />
          <userCatalogProvider id="UserId1" ignoreExceptions="true" />
        </userCatalogProviders>
      </orUserCatalogProvider>
    </orUserCatalogProviders>
    <andUserCatalogProviders>
    </andUserCatalogProviders>
  </combineRules>
</userCatalogProviderSettings>
```

LDAP-фильтр при поиске пользователей и групп в Active Directory

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

Для этого нужно:

1. На сервере Indeed AM открыть файл конфигурации сервера **C:\inetpub\wwwroot\am\core\Web.config**
2. Найти секцию **"adUserCatalogProvider"** и в задать в ней атрибуты **catalogFilter** и **dnFilter** для фильтрации элементов пользовательского каталога:
 - a. **catalogFilter** - строка LDAP-запрос для фильтрации элементов на этапе выполнения запроса к AD. Не поддерживает фильтрацию по частичному совпадению атрибутов distinguishedName и canonicalName (для этих целей добавлен dnFilter);
 - b. **dnFilter** (distinguishedName фильтр) - содержит регулярное выражение для фильтрации результатов после выполнения LDAP-запроса к AD.

Примеры использования фильтров

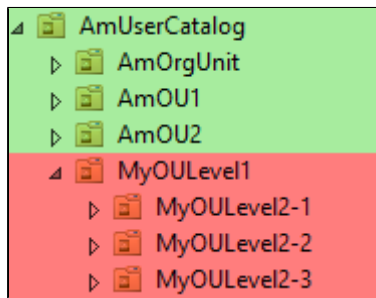
catalogFilter:

- Исключение определенных пользователей
& (! (name=AmUser1)) (! (name=AmUser2) (! (name=AmUser3)))
- Исключение всех дочерних элементов 1 уровня указанной OU
!(msDS-parentdistinguishedname=OU=AmOrgUnit, OU=AmUserCatalog, DC=dom, DC=local)
- Исключение всех членов группы
!(memberof=CN=AmGroup, OU=AmUserCatalog, DC=dom, DC=local)

dnFilter:

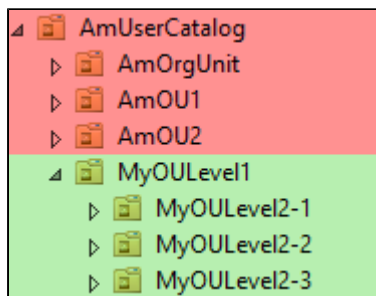
- Исключение OU и всех дочерних элементов:

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



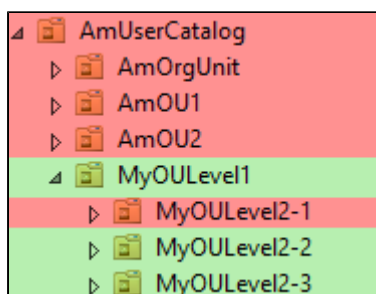
- Использование только указанной OU:

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



Indeed AM Management Console

Indeed AM Management Console — это Web-приложение, которое работает на базе IIS. В данном модуле осуществляется администрирование системы, через которую производятся все настройки системы и пользователей.

Информация

Файлы для Management Console расположены: ***indeed AM <номер версии>/Indeed AM Management Console/<номер версии>***.

- **IndeedAM.ManagementConsole-<номер версии>.x64.ru-ru.msi** — пакет для установки Management Console.

Дополнительные файлы для установки Management Console расположены: ***indeed AM <номер версии>/Misc***.

- **Server2008/Indeed.AdminConsole.IIS.Install.MSServer2008.ps1** — скрипт для установки необходимых компонентов IIS сервера для Windows Server 2008.
- **Server2008/NDP452-KB2901907-x86-x64-AllOS-ENU.exe** — пакет с обновлением Microsoft .NET Framework 4.5.2 для Windows Server 2008.
- **Server2012/Indeed.AdminConsole.IIS.Install.MSServer2012.ps1** — скрипт для установки необходимых компонентов IIS сервера для Windows Server 2012.

Информация

Путь к Management Console в браузере: ***http(s)://<днс_сервера>/am/mc***

Путь к Management Console в IIS: ***<имя_машины>\сайты\Default Web Site\am\mc***

Установка

Информация

Для работы **Indeed AM Management Console** требуется установленный **.NET Framework 4.8**

1. Выполнить установку Indeed AM Management Console через запуск соответствующего пакета.



Информация

Оptionальная настройка. Генерация сертификата необходима при аутентификации в консоль администратора [с использованием Indeed AM Identity Provider](#).

Данный сертификат не предназначен для организации SSL соединения.

Если данный сертификат был сгенерирован ранее, то необходимо убрать флажок.

По завершении установки будет предложено сгенерировать новый IDP сертификат. Если флажок будет выставлен, то сгенерируется и установится в хранилище сертификатов (*Local Machine -> Personal*) новый самоподписанный сертификат. Сертификат используется для шифрования данных, передаваемых между сервером аутентификации и клиентским приложением.

Программа установки Indeed Enterprise Management Con... — □ ×



Установка программы Indeed Enterprise Management Console x64 завершена

Нажмите 'Готово', чтобы завершить работу программы установки.

Для шифрования данных, передаваемых между сервером аутентификации и клиентским приложением требуется сертификат. Данный сертификат не предназначен для организации SSL соединения.

☒ Создать и установить новый сертификат IDP клиента

< Назад

Готово

Отмена

2. Добавить привязку **https** в настройках **Default Web Site** в IIS Manager.



Информация

Indeed AM Management Console является Web приложением, которое работает на базе IIS, в процессе установки для него по умолчанию включается обязательно требование SSL в настройках, что в свою очередь требует включенной привязки https.

Если вы не намерены использовать протокол https, необходимо отключить требование SSL в настройках IIS для Management Console.

Также в этом случае необходимо в конфигурационном файле **MC (C:\inetpub\wwwroot\am\mc\Web.config)** изменить значение параметра **requireSSL** на **false**:

Пример

```
<httpCookies httpOnlyCookies="true" requireSSL="false" />
```

- a. Запустите **IIS Manager** и раскройте пункт **Сайты (Sites)**.
- b. Выберите сайт **Default Web Site** и нажмите **Привязки (Bindings)** в разделе **Действия (Actions)**.
- c. Нажмите **Добавить (Add)**:
 - i. **Тип (Type)** - https.
 - ii. **Порт (Port)** - 443.
 - iii. Выберите **SSL-сертификат (SSL Certificate)**.
- d. Сохраните привязку.

Редактирование конфигурационного файла

1. Откройте конфигурационный файл консоли **Web.config** (C:\inetpub\wwwroot\am\mc\Web.config).

Информация

Для сохранения изменений в конфигурационном файле приложения, требуется запустить редактор с правами администратора.

2. Укажите **URL** для подключения к серверу **Indeed AM** для параметра **Url** в тэге **amAuthServer**.

- а. Параметр **Url** - url адрес сервера Indeed в формате **http(s)://**
полное_dns_имя_сервера/am/core/

Информация

Для игнорирования ошибок сертификата сервера необходимо изменить параметр **"isIgnoreCertErrors"** на значение **"true"** в файле **"applicationSettings.config"** (am\mc\Config).

Пример

```
<amAuthServer Url="https://amserv.indeed-id.local/am/core/" />
```

3. Задайте url для подключения к лог серверу. Редактируем тег **logServer**.

- а. **URL** - url для подключения к лог серверу в формате **http(s)://полное_dns_имя_сервера/ls/api**.

 Примечание

Если используется несколько серверов, указываем адрес балансировщика нагрузки.

 Информация

Настройки связанные с сертификатом необходимы для настройки двухстороннего TLS соединения между сервером Indeed MC и Indeed AM Log Server.

 Информация

Данную настройку не требуется указывать. В текущей версии системы Indeed AM не поддерживается работа 2-х стороннего TLS соединения.

- б. **CertificateThumbprint** - если закрытый ключ в реестре, а сертификат в хранилище компьютера.
- с. **CertificateFilePath** - если ключевая пара в pfx.
- д. **CertificateFilePassword** - пароль от pfx.

Пример

```
<logServer Url="http://log.indeed-id.local/ls/api/" CertificateThumbprint=""  
CertificateFilePath="" CertificateFilePassword=""/>
```

4. После редактирования конфигурационных файлов перезапустите IIS сервер. Management Console будет доступен по адресу: "**http(s)://полное_dns_имя_сервера/am/mc/**"

Настройка срока жизни сессии

 Информация

Данная настройка не является обязательной

Для увеличения или уменьшения срока жизни сессии в Management Console выполните следующие действия

1. Откройте конфигурационный файл Indeed Management Console **applicationSettings.config**: C:\inetpub\wwwroot\am\mc\Config\applicationSettings.config
2. Для параметра "**sessionExpirationTimeInMinutes**" установите необходимое значение. Значение по умолчанию 30(минут).

Пример

```
<amApplicationSettings
  findUsersMaxResultCount="200"
  isIgnoreCertErrors="false"
  sessionExpirationTimeInMinutes="60"
  allowOverrideRandomPasswordGeneration="false"
/>
```

3. Сохраните изменения.

Аутентификация с помощью Indeed AM Identity Provider

Вы можете настроить аутентификацию в Management Console через модуль Indeed AM Identity Provider.

Настройка зависит от версии Indeed Access Manager:

Вы можете настроить защищенный вход в Management Console с использованием Identity Provider.

Редактирование конфигурационного файла Management Console



Важно

Перед редактированием конфигурационного файла, выполните следующие действия:

1. Запустите Диспетчер служб IIS,
2. Выберите <имя сервера>**SitesDefault Web Site**ammc.
3. Выберите **Проверка подлинности** и включите опции **Анонимная проверка подлинности** и **Проверка подлинности с помощью форм**.

1. Откройте конфигурационный файл *web.config* из *C:\inetpub\wwwroot\am\mc\Web.config*.
2. В параметре *amAuthentication* выполните следующие действия:
 - a. В строке *mode* укажите значение *Saml*
 - b. В строке *loginUrl* укажите адрес Identity Provider в формате *http(s)://полное_dns_имя_сервера/am/idp/*

Пример

```
<amAuthentication mode="Saml" loginUrl="https://server.test.local/am/idp/>
```

- c. В строке *identityProviderCertificateThumbprint* укажите отпечаток сертификата Identity Provider.

Информация

Если Identity Provider и Management Console были установлены на разные серверы, экспортируйте сертификат без закрытого ключа с сервера с модулем Identity Provider на сервер с Management Console. Сертификат необходимо добавить в хранилище сертификатов в *Local MachinePersonal*.

Чтобы получить отпечаток сертификата с помощью запроса PowerShell:

```
Get-Childitem Cert:\LocalMachine\My\ | Where-Object {$_.Subject -eq "CN=idp"}
```

- d. В строке *serviceProviderCertificateThumbprint* укажите отпечаток сертификата Management Console, который был сгенерирован [при установке пакета](#).

Информация

Сертификат устанавливается в хранилище сертификатов *Local MachinePersonal* с общим именем *mcsp*.

Чтобы получить отпечаток сертификата с помощью запроса PowerShell:

```
Get-Childitem Cert:\LocalMachine\My\ | Where-Object {$_.Subject -eq "CN=mcsp"}
```

3. Сохраните изменения и перезапустите IIS.

Редактирование конфигурационного файла Identity Provider

Важно

Перед редактированием конфигурационного файла, выполните следующие действия:

1. Запустите Диспетчер служб IIS,
2. Выберите <имя сервера> **SitesDefault Web Site** *am\idp*.
3. Выберите **Проверка подлинности** и отключите опцию **Проверка подлинности Windows**.

1. Откройте конфигурационный файл *app-settings.json* из *C:\inetpub\wwwroot\am\idp*.
2. В параметре *PartnerServiceProviderConfigurations* выполните следующие действия:
 - a. В строке *SingleLogoutServiceUrl* укажите адрес сервера с компонентом Indeed AM Management Console в формате *http(s)://полное_dns_имя_сервера/am/mc/Account/SLOService*
 - b. В строке *Thumbprint* укажите отпечаток сертификата Indeed AM Management Console.

Информация

Если Identity Provider и management console были установлены на разные серверы, экспортируйте сертификат без закрытого ключа с сервера с management console на сервер с модулем Identity Provider. Сертификат необходимо добавить в хранилище сертификатов в *Local MachinePersonal*.

Чтобы получить с помощью запроса PowerShell:

```
Get-Childitem Cert:\LocalMachine\My\ | Where-Object {$_.Subject -eq "CN=mcsp"}
```

Пример

```
"PartnerServiceProviderConfigurations":
{
  "Name": "urn:indeedid:emc",
  "SingleLogoutServiceUrl": "https://server.indeed.local/am/mc/Account
/SLOService",
  "PartnerCertificates": [
    {
      "Thumbprint": "C77EDF29EA05B468BDAF553DE3D804DA4B139C1E"
```

3. Сохраните изменения и перезапустите IIS.

Настройка выхода из Management Console с использованием Identity Provider

1. Откройте конфигурационный файл консоли *web.config* из *C:\inetpub\wwwroot\am\mc\Web.config*.
2. В параметр *amAuthentication* добавьте параметр *enableLogout* со значением *true* (по умолчанию установлено значение *false*).

Пример

```
<amAuthentication mode="Saml" loginUrl="https://server.test.local/am/idp/"
enableLogout="true"/>
```

3. Откройте конфигурационный файл Identity Provider *app-settings.json* из *C:\inetpub\wwwroot\am\idp*.
4. Измените параметр *PartnerServiceProviderConfigurations*. В строке *SingleLogoutServiceUrl* укажите адрес сервера с компонентом Indeed AM Management Console в формате *http(s)://полное_dns_имя_сервера/am/mc/Account/SLOService*

Пример

```
"PartnerServiceProviderConfigurations": [
  {
    ...
    "SingleLogoutServiceUrl": "https://server01.test.local/am/mc/Account/SLOService",
    ...
  }
]
```

5. Сохраните изменения и перезапустите IIS.

Чтобы настроить защищенный вход в Management Console, выполните следующие действия:



Информация

Данная настройка не является обязательной

1. Откройте **IIS Manager**, выберите **"Default Web Site -> am"** и откройте приложение **"mc"**.

2. Откройте "Проверка подлинности" и включите следующие методы:
- a. Анонимная проверка подлинности.
 - b. Проверка подлинности с помощью форм.



Проверка подлинности

Сгруппировать по: Без группирования ▾		
Имя	Состояние	Тип ответа
Анонимная проверка подлинности	Включен	
Обычная проверка подлинности	Отключен	Вызов HTTP 401
Олицетворение ASP.NET	Отключен	
Проверка подлинности Windows	Отключен	Вызов HTTP 401
Проверка подлинности с помощью форм	Включен	Вход-перенаправлени...

3. Откройте конфигурационный файл консоли **Web.config** (C:\inetpub\wwwroot\am\mc\Web.config).

4. В теге **amAuthentication** выполните следующие:

- a. В параметре **mode** укажите значение **Saml**.
- b. В параметре **loginUrl** кажите **URL** в формате http (s)://полное_dns_имя_сервера/am/idp/ для подключения к серверу **Indeed SAML**.

```
<amAuthentication mode="Saml" loginUrl="http://saml.demo.local/am/idp/" />
```

- c. В параметре **identityProviderCertificateThumbprint** укажите отпечаток сертификата Indeed AM Saml Idp. Сертификат необходимо экспортировать без закрытого ключа с сервера SAML на сервер с Indeed AM Management Console. Сертификат необходимо добавить в хранилище сертификатов, в Local Machine -> Personal.

Получение отпечатка сертификата Saml Idp через PS

```
Get-Childitem Cert:\LocalMachine\My\ | Where-Object {$_.Subject -eq "CN=idp"}
```

- d. В параметре **serviceProviderCertificateThumbprint** укажите отпечаток сертификата IDP клиента Indeed AM Management Console, который был сгенерирован при установке.

Информация

Сертификат устанавливается в хранилище сертификатов (*Local Machine* -> *Personal*) с общим именем "**mcsp**".

Получить его отпечаток можно с помощью PowerShell запроса:

```
Get-Childitem Cert:\LocalMachine\My\ | Where-Object {$_.Subject -eq "CN=mcsp"}
```

5. Сохраните изменения в конфигурационном файле.

Информация

Для отключения запроса доменных логина и пароля необходимо отключить "**Проверку подлинности Windows**" в IIS для приложения **idp** на сервере **SAML**.

6. Откройте конфигурационный файл Indeed AM Saml Idp **Web.config** (C:\inetpub\wwwroot\am\idp\Web.config).

7. В теге **amPartnerServiceProviderSettings** укажите следующие:

- a. В параметре **EmcServiceUrl** укажите URL сервера с компонентом Indeed AM Management Console в формате `http(s)://полное_dns_имя_сервера/mc/`
- b. В параметре **EmcCertificateThumbprint** укажите отпечаток сертификата Indeed AM Management Console. Сертификат необходимо экспортировать без закрытого ключа с сервера Indeed AM Management Console на сервер с Indeed AM Saml Idp. Сертификат необходимо добавить в хранилище сертификатов, в Local Machine -> Personal.

Получение отпечатка сертификата Management Console через PS

```
Get-Childitem Cert:\LocalMachine\My\ | Where-Object {$_.Subject -eq "CN=mcsp"}
```

Пример

```
<amPartnerServiceProviderSettings SelfServiceUrl="SELF_SERVICE_URL" EmcServiceUrl="https://server.indeed.local/am/mc/" SelfServiceCertificateThumbprint="" EmcCertificateThumbprint="C77EDF29EA05B468BDAF553DE3D804DA4B139C1E"/>
```

Чтобы настроить защищенный выход из Management Console, выполните следующие действия:

1. Откройте конфигурационный файл консоли **Web.config** (C:\inetpub\wwwroot\am\mc\Web.config).
2. Для тега **amAuthentication** добавьте параметр **enableLogout** со значение **true** (По умолчанию false).

Пример

```
<amAuthentication mode="Saml" loginUrl="http://saml.demo.local/am/idp/" enableLogout="true"/>
```

3. Откройте конфигурационный файл **SAML Web.config** (C:\inetpub\wwwroot\am\idp\Web.config).
4. Для параметра **EmcServiceUrl** в теге **amPartnerServiceProviderSettings** укажите URL адрес сервера **Management Console**.

Пример

```
<amPartnerServiceProviderSettings SelfServiceUrl="http://dc.demo.local/am/uc/" EmcServiceUrl="http://dc.demo.local/am/mc/" />
```

Настройка поиска по пользователям

Вы можете настроить поиск пользователей в Management Console по следующим запросам:

- по имени
- по фамилии
- по логину
- по имени пользователя в каталоге Active Directory
- по имени и фамилии

Для настройки используйте файл *userSearchSettings.config* из папки *C:\inetpub\wwwroot\am\mc\Config*.

searchTemplate — в параметре задается шаблон поиска. Примеры допустимых шаблонов: *{0}*, *{0}**, **{0}**.

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 name. Значение по умолчанию *true*.

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.
*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 <i>searchTemplate</i> . Если шаблон <i>searchTemplate</i> не указан, то к запросу будут добавлены * с обеих сторон.
** * * **иван ** иван**	Примеры неправильных запросов. Не возвращают результат поиска.

Отключение отображения информации о платформе и версии

Для того, чтобы не добавлять заголовки, содержащие информацию о платформе и версии, на которой разрабатывалось приложение, в response, нужно:

1. Открыть конфигурационный файл Management Console C:
\\inetpub\\wwwroot\\am\\mc\\Web.config;
2. В зависимости от версии IIS:
 - а. Для IIS 10 перенести комментарий в секции "security" со 2 на 3 строчку:

Пример

```
<security>
  <!--<requestFiltering removeServerHeader="true" >-->
  <requestFiltering>
    <requestLimits maxAllowedContentLength="104857600" />
  </requestFiltering>
</security>
```

- б. IIS старше 10:
 - Установить URL Rewrite
 - В секцию <system.webServer> добавить:

Пример

```
<rewrite>
  <outboundRules>
    <rule name="replace server header" patternSyntax="Wildcard" lockItem="false">
      <match serverVariable="RESPONSE_SERVER" pattern="*" />
      <action type="Rewrite" value="MyServer" />
    </rule>
  </outboundRules>
</rewrite>
```

Indeed AM User Console

Indeed AM User Console - это Web-приложение, которое работает на базе IIS. В данном модуле пользователь может осуществлять управление своими аутентификаторами.

Информация

Файлы для indeed AM User Console расположены: ***indeed AM <номер версии>/Indeed AM User Console/<номер версии>***.

IndeedAM.UserConsole-<номер версии>.x64.ru-ru.msi — пакет для установки Indeed AM User Console.

Информация

Путь к User Console в браузере: ***http(s)://<днс_сервера>/am/uc***

Путь к User Console в IIS: ***<имя_машины>\сайты\Default Web Site\am\uc***

Установка

1. Выполнить установку **Indeed AM User Console** через запуск соответствующего пакета.



Информация

Опциональная настройка. Генерация сертификата необходима при аутентификации в Indeed AM User Console [с использованием Indeed AM Identity Provider](#).

Данный сертификат не предназначен для организации SSL соединения.

Если данный сертификат был сгенерирован ранее, то необходимо убрать флажок.

По завершении установки будет предложено сгенерировать новый IDP сертификат. Если флажок будет выставлен, то сгенерируется и установится в хранилище сертификатов (*Local Machine -> Personal*) новый самоподписанный сертификат. Сертификат используется для шифрования данных, передаваемых между сервером аутентификации и клиентским приложением.



Программа установки Indeed Self Service x64



Установка программы Indeed Self Service x64 завершена

Нажмите 'Готово', чтобы завершить работу программы установки.

Для шифрования данных, передаваемых между сервером аутентификации и клиентским приложением требуется сертификат. Данный сертификат не предназначен для организации SSL соединения.

☒ Создать и установить новый сертификат IDP клиента

< Назад

Готово

Отмена

2. Добавить привязку **https** в настройках **Default Web Site** в IIS Manager.

Информация

User Console является Web приложением, которое работает на базе IIS, в процессе установки для него по умолчанию включается обязательно требование SSL в настройках, что в свою очередь требует включенной привязки https.

Если вы не намерены использовать протокол https, необходимо отключить требование SSL в настройках IIS для User Console.

Также в этом случае необходимо в конфигурационном файле **UC (C:\inetpub\wwwroot\am\uc\Web.config)** изменить значение параметра **requireSSL** на **false**:

Пример

```
<httpCookies httpOnlyCookies="true" requireSSL="false" />
```

- a. Запустите **IIS Manager** и раскройте пункт **Сайты (Sites)**.
- b. Выберите сайт **Default Web Site** и нажмите **Привязки (Bindings)** в разделе **Действия (Actions)**.
- c. Нажмите **Добавить (Add)**:
 - i. **Тип (Type)** - https.
 - ii. **Порт (Port)** - 443.
 - iii. Выберите **SSL-сертификат (SSL Certificate)**.
- d. Сохраните привязку.

Настройка

Информация

Для сохранения изменений в конфигурационном файле приложения, требуется запустить редактор с правами администратора.

По умолчанию компонент **Indeed AM User Console** настроен на использование SAML аутентификации, при необходимости можно настроить прозрачную Windows аутентификацию.

Аутентификация с Windows Authentication

1. Откройте конфигурационный файл User Console **Web.config** (C:\inetpub\wwwroot\am\uc\Web.config).
2. Укажите **URL** для подключения к серверу **Indeed** для параметра **Url** в тэге **amAuthServer**.
 - а. Параметр **Url** - url адрес сервера Indeed в формате **http(s)://**
полное_dns_имя_сервера/am/core/

И **н** **ф** **о** **р** **м** **а** **ц** **и** **я**

Для игнорирования ошибок сертификата сервера необходимо изменить параметр "isIgnoreCertErrors" на значение "true" в файле "applicationSettings.config" (am\uc\Config).

П **р** **и** **м** **е** **р**

```
<amAuthServer Url="https://amserv.indeed-id.local/am/core/" />
```

3. Запустите **IIS Manager**, выберите "**Default Web Site -> am**" и откройте приложение "**uc**".
4. Откройте "**Проверка подлинности**" и включите следующие методы:
 - а. Олицетворение ASP.NET.
 - б. Проверка подлинности Windows.



П **р** **о** **в** **e** **р** **к** **а** **п** **о** **д** **л** **и** **н** **н** **о** **с** **т** **и**

Сгруппировать по: Без группирования ▾		
Имя	Состояние	Тип ответа
Анонимная проверка подлинности	Отключен	
Обычная проверка подлинности	Отключен	Вызов HTTP 401
Олицетворение ASP.NET	Включен	
Проверка подлинности Windows	Включен	Вызов HTTP 401
Проверка подлинности с помощью форм	Отключен	Вход-перенаправлени...

5. Отключите все остальные методы.
6. Откройте конфигурационный файл User Console **Web.config** (C:\inetpub\wwwroot\am\uc\Web.config).

7. Для тега **"amAuthentication"** в параметре **"mode"** укажите **"Windows"**.

 Информация

Параметр **"loginUrl"** оставьте без изменений, при использовании Windows аутентификации данный параметр не учитывается.

Пример

```
<amAuthentication mode="Windows" loginUrl="" identityProviderCertificateThumbprint=""
serviceProviderCertificateThumbprint="" enableLogout="true"/>
```

8. Перезапустите IIS сервер. User Console будет доступен по адресу: **"http(s)://
полное_dns_имя_сервера/am/uc/"**.

Аутентификация с помощью Indeed AM Identity Provider

Вы можете настроить аутентификацию в User Console через модуль Indeed AM Identity Provider.

Настройка зависит от версии Indeed Access Manager:

Вы можете настроить защищенный вход в User Console с использованием Identity Provider.

Редактирование конфигурационного файла User Console

 Важно

Перед редактированием конфигурационного файла, выполните следующие действия:

1. Запустите Диспетчер служб IIS,
2. Выберите **<имя сервера>SitesDefault Web Siteamuc**.
3. Выберите **Проверка подлинности** и включите опции **Анонимная проверка подлинности** и **Проверка подлинности с помощью форм**.

1. Откройте конфигурационный файл *web.config* из *C:\inetpub\wwwroot\am\uc\Web.config*.

2. В параметре *amAuthServer Url* укажите адрес сервера Indeed в формате *http(s)://полное_dns_имя_сервера/am/core/*

Пример

```
<amAuthServer Url="https://amserv.indeed-id.local/am/core/" />
```

3. В параметре *amAuthentication* выполните следующие действия:
- a. В строке *mode* укажите значение *Saml*.
 - b. В строке *loginUrl* укажите адрес Identity Provider в формате *http(s)://полное_dns_имя_сервера/am/idp/*

Пример

```
<amAuthentication mode="Saml" loginUrl="https://server.test.local/am/idp/>
```

- c. В строке *identityProviderCertificateThumbprint* укажите отпечаток сертификата Identity Provider.

И **н** **ф** **о** **р** **м** **а** **ц** **и** **я**

Если Identity Provider и User Console были установлены на разные серверы, экспортируйте сертификат без закрытого ключа с сервера с модулем Identity Provider на сервер с User Console. Сертификат необходимо добавить в хранилище сертификатов в *Local MachinePersonal*.

Чтобы получить отпечаток сертификата с помощью запроса PowerShell:

```
Get-Childitem Cert:\LocalMachine\My\ | Where-Object {$_.Subject -eq "CN=idp"}
```

- d. В строке *serviceProviderCertificateThumbprint* укажите отпечаток сертификата User Console, который был сгенерирован [при установке пакета](#).

И **н** **ф** **о** **р** **м** **а** **ц** **и** **я**

Сертификат устанавливается в хранилище сертификатов *Local MachinePersonal* с общим именем *ucsp*.

Чтобы получить отпечаток сертификата с помощью запроса PowerShell:

```
Get-Childitem Cert:\LocalMachine\My\ | Where-Object {$_.Subject -eq "CN=ucsp"}
```

4. Сохраните изменения и перезапустите IIS.

Редактирование конфигурационного файла Identity Provider

Важно

Перед редактированием конфигурационного файла, выполните следующие действия:

1. Запустите Диспетчер служб IIS,
2. Выберите <имя сервера>**SitesDefault Web Site** и **idp**.
3. Выберите **Проверка подлинности** и отключите опцию **Проверка подлинности Windows**.

1. Откройте конфигурационный файл *app-settings.json* из *C:\inetpub\wwwroot\am\idp*.
2. В параметре *PartnerServiceProviderConfigurations* выполните следующие действия:
 - a. В строке *SingleLogoutServiceUrl* укажите адрес сервера, где вы развернули User Console, в формате *http(s)://полное_dns_имя_сервера/am/uc/Account/SLOService*
 - b. В строке *Thumbprint* укажите отпечаток сертификата User Console.

Информация

Если Identity Provider и User Console были установлены на разные серверы, экспортируйте сертификат без закрытого ключа с сервера развернутым User Console на сервер с модулем Identity Provider. Сертификат необходимо добавить в хранилище сертификатов в *Local MachinePersonal*.

Чтобы получить с помощью запроса PowerShell:

```
Get-Childitem Cert:\LocalMachine\My\ | Where-Object {$_.Subject -eq "CN=ucsp"}
```

Пример

```
"PartnerServiceProviderConfigurations":  
  {  
    "Name": "urn:indeedid:selfservice",  
    "SingleLogoutServiceUrl": "https://server.indeed.local/am/uc/Account  
/SLOService",  
    "PartnerCertificates": [  
      {  
        "Thumbprint": "C77EDF29EA05B468BDAF553DE3D804DA4B139C1E"      }  
    ]  
  }
```

3. Сохраните изменения и перезапустите IIS.

Настройка выхода из User Console с использованием Identity Provider

1. Откройте конфигурационный файл консоли *web.config* из *C:*
\inetpub\wwwroot\am\uc\Web.config.
2. В параметр *amAuthentication* добавьте параметр *enableLogout* со значением *true* (по умолчанию установлено значение *false*).

Пример

```
<amAuthentication mode="Saml" loginUrl="https://server.test.local/am/idp/"  
enableLogout="true"/>
```

3. Откройте конфигурационный файл Identity Provider *app-settings.json* из *C:*
\inetpub\wwwroot\am\idp.
4. Измените параметр *PartnerServiceProviderConfigurations*. В строке *SingleLogoutServiceUrl* укажите адрес сервера с компонентом Indeed AM User Console в формате *http(s)://полное_dns_имя_сервера/am/uc/Account/SLOService*

Пример

```
"PartnerServiceProviderConfigurations": [  
  {  
    ...  
    "SingleLogoutServiceUrl": "https://server01.test.local/am/uc/Account/SLOService",  
    ...  
  }  
]
```

5. Сохраните изменения и перезапустите IIS.

1. Откройте конфигурационный файл User Console **Web.config** (*C:*
\inetpub\wwwroot\am\uc\Web.config).
2. Укажите **URL** для подключения к серверу **Indeed** для параметра **Url** в тэге **amAuthServer**.

- а. Параметр **Url** - url адрес сервера Indeed в формате **http(s)://полное_dns_имя_сервера/am/core/**

Информация

Для игнорирования ошибок сертификата сервера необходимо изменить параметр **"isIgnoreCertErrors"** на значение **"true"** в файле **"applicationSettings.config"** (**am\uc\Config**).

Пример

```
<amAuthServer Url="https://amserv.indeed-id.local/am/core/" />
```

3. Запустите **IIS Manager**, выберите **"Default Web Site -> am"** и откройте приложение **"uc"**.
4. Откройте **"Проверка подлинности"** и включите следующие методы:
- а. Анонимная проверка подлинности.
 - б. Проверка подлинности с помощью форм.



Проверка подлинности

Сгруппировать по: Без группирования ▾		
Имя	Состояние	Тип ответа
Анонимная проверка подлинности	Включен	
Дайджест-проверка подлинности	Отключен	Вызов HTTP 401
Обычная проверка подлинности	Отключен	Вызов HTTP 401
Олицетворение ASP.NET	Отключен	
Проверка подлинности Windows	Отключен	Вызов HTTP 401
Проверка подлинности с помощью форм	Включен	Вход-перенаправлени...

5. Отключите все остальные методы.
6. Откройте конфигурационный файл User Console **Web.config** (C:\inetpub\wwwroot\am\uc\Web.config).

7. В теге **amAuthentication** выполните следующие:

- a. В параметре **mode** укажите значение **Saml**.
- b. В параметре **loginUrl** кажите **URL** в формате http (s)://полное_dns_имя_сервера/am/idp/ для подключения к серверу **Indeed SAML**.

```
<amAuthentication mode="Saml" loginUrl="http://saml.demo.local/am/idp/" />
```

- c. В параметре **identityProviderCertificateThumbprint** укажите отпечаток сертификата Indeed AM Saml Idp. Сертификат необходимо экспортировать без закрытого ключа с сервера SAML на сервер с Indeed AM User Console. Сертификат необходимо добавить в хранилище сертификатов, в Local Machine -> Personal.

Получение отпечатка сертификата Saml Idp через PS

```
Get-Childitem Cert:\LocalMachine\My\ | Where-Object {$_.Subject -eq "CN=idp"}
```

- d. В параметре **serviceProviderCertificateThumbprint** укажите отпечаток сертификата IDP клиента Indeed AM User Console, который был сгенерирован при установке.

Информация

Сертификат устанавливается в хранилище сертификатов (*Local Machine -> Personal*) с общим именем "**ucsp**".

Получить его отпечаток можно с помощью PowerShell запроса:

```
Get-Childitem Cert:\LocalMachine\My\ | Where-Object {$_.Subject -eq "CN=ucsp"}
```

- e. Параметр **enableLogout** (Не обязательный) - включает возможность выполнять выход из User Console.

Пример

```
<amAuthentication mode="Saml" loginUrl="https://logserver.indeed.local/am/idp/"
identityProviderCertificateThumbprint="C72DF64AE6E039445C8ED53FD83F75A9A2BA3
7E9" serviceProviderCertificateThumbprint="3A1663D905E543782DD84B50391DEBC517
8269D7" enableLogout="true" />
```


8. Откройте конфигурационный файл Indeed AM Saml Idp **Web.config** (C:

\inetpub\wwwroot\am\idp\Web.config).

а. В теге **amPartnerServiceProviderSettings** укажите следующие:

- i. В параметре **SelfServiceUrl** укажите URL сервера с компонентом Indeed AM User Console в формате http(s)://полное_dns_имя_сервера/am/uc/
- ii. В параметре **SelfServiceCertificateThumbprint** укажите отпечаток сертификата Indeed AM User Console. Сертификат необходимо экспортировать без закрытого ключа с сервера Indeed AM User Console на сервер с Indeed AM Saml Idp. Сертификат необходимо добавить в хранилище сертификатов, в Local Machine -> Personal.

Получение отпечатка сертификата User Console через PS

```
Get-Childitem Cert:\LocalMachine\My\ | Where-Object {$_.Subject -eq "CN=u  
csp"}
```

Пример

```
<amPartnerServiceProviderSettings SelfServiceUrl="https://server.indeed.local/am  
/uc/" EmcServiceUrl="" SelfServiceCertificateThumbprint="3A1663D905E543782DD84B5039  
1DEBC5178269D7" EmcCertificateThumbprint=""/>
```

9. Сохраните изменения в конфигурационных файлах и перезапустите IIS сервера с Indeed AM Saml и с Indeed AM User Console.

Включение защиты от перебора

Сервер Indeed AM поддерживает включение защиты от подбора УЗ пользователей для компонента Indeed AM Identity Provider. По умолчанию данная настройка отключена.

При включенной настройке злоумышленник не сможет определить валидные УЗ в домене по возвращаемой от компонента ошибке.

Настройка зависит от версии Indeed AM Access Manager:

1. Откройте конфигурационный файл сервера Indeed AM *Web.config* из *C:\inetpub\wwwroot\am\core*.
2. В параметре *appSettings* в строке *bruteForceProtectionApps* укажите значения *Self Service* и *Identity Provider*.

Пример

```
<appSettings>
...
<add key="bruteForceProtectionApps" value="Self Service, Identity Provider" />
</appSettings>
```

3. Сохраните изменения и перезапустите IIS сервер.

1. Откройте конфигурационный файл сервера Indeed AM: *C:\inetpub\wwwroot\am\core\Web.config*
2. В теге "appSettings", для параметра "**bruteForceProtectionApps**", задайте значения "**Self Service**" и "**SAML Identity Provider**".

Пример

```
<appSettings>
...
<add key="bruteForceProtectionApps" value="Self Service, SAML Identity Provider" />
</appSettings>
```

3. Сохраните изменения и перезапустите IIS сервер.

Настройка срока жизни сессии

Информация

Данная настройка не является обязательной

Для увеличения или уменьшения срока жизни сессии в Admin Console выполните следующие действия

1. Откройте конфигурационный файл Indeed Admin Console **applicationSettings.config**: C:\inetpub\wwwroot\am\uc\Config\applicationSettings.config
2. Для параметра "**sessionExpirationTimeInMinutes**" установите необходимое значение. Значение по умолчанию 30(минут).

Пример

```
<?xml version="1.0"?>
<amApplicationSettings isIgnoreCertErrors="false" sessionExpirationTimeInMinutes="30"/>
```

3. Сохраните изменения.

Вход в User Console с использованием Indeed AM Identity Provider

1. Откройте в браузере Web интерфейс консоли User Console.
2. В появившемся окне аутентификации нажмите "**Back**" для выбора способа аутентификации, по умолчанию используется последний используемый способ.





DEMO\Admin-Indeed

Enter the windows password

Back

Next

3. Выберите способ аутентификации и нажмите **"Select"**.

 Информация

Если у пользователя нет обученного аутентификатора, то выберите **"Windows Password"**.

 Информация

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.

INDEED 



DEMO\Admin-Indeed

Choose an authentication method you want to use

- ☐ Passcode
- ☒ Windows Password + Passcode
- ☐ Hardware OTP + Passcode
- ☐ Hardware TOTP

Select

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



Admin Indeed

Имя учетной записи Admin-Indeed@demo.local
Путь demo.local/Users/Admin Indeed
E-mail Admin-Indeed@demo.local
Телефон

История входов

Аутентификаторы **2**

Модуль	Время входа	Способ входа
Self Service	16.05.2019 15:44:54	Passcode
Enterprise Management Console	16.05.2019 14:53:39	Windows Token
SAML Identity Provider	16.05.2019 13:15:48	Passcode
RDP Windows Logon	16.05.2019 11:35:45	Passcode

5. Для выхода из User Console выполните:



Информация

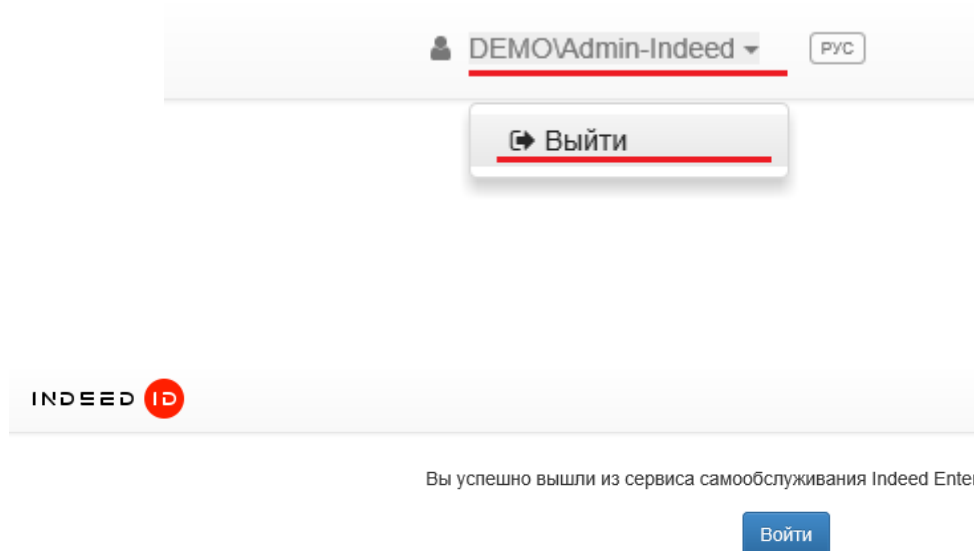
Данная опция будет активна если в пункте 3.b раздела "**Установка**", был настроен параметр **enableLogout**. По умолчанию отключена.

- a. Нажмите на имя пользователя в верхней части окна.
- b. Выберите "**Выйти**" из выпадающего списка.



Информация

При выходе из User Console происходит автоматический выход из Identity Provider.



Отключение отображения информации о платформе и версии

Для того, чтобы не добавлять заголовки, содержащие информацию о платформе и версии, на которой разрабатывалось приложение, в response, нужно:

1. Открыть конфигурационный файл User Console **C:\inetpub\wwwroot\am\uc\Web.config**;
2. В зависимости от версии IIS:
 - a. Для IIS 10 убрать комментарии со следующих строк:

Пример

```
<security>
  <requestFiltering removeServerHeader="true" />
</security>
```

- b. IIS старше 10:

- Установить URL Rewrite
- В секцию `<system.webServer>` добавить:

Пример

```
<rewrite>
  <outboundRules>
    <rule name="replace server header" patternSyntax="Wildcard" lockItem="false">
      <match serverVariable="RESPONSE_SERVER" pattern="*" />
      <action type="Rewrite" value="MyServer" />
    </rule>
  </outboundRules>
</rewrite>
```

Indeed Key Server

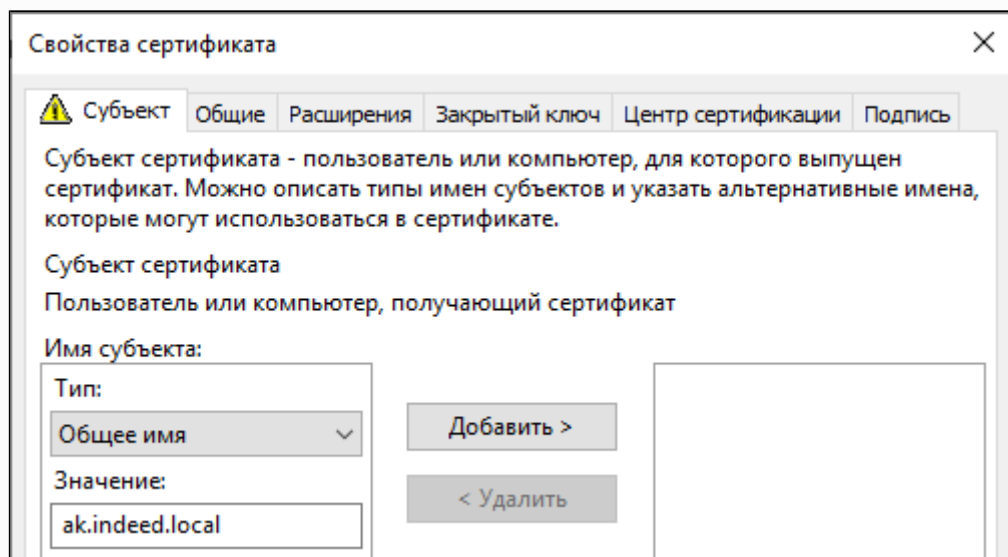
Информация

Файлы для Indeed Key Server расположены: ***indeed AM <номер версии>/Indeed AM Indeed Key Server/<Номер версии>***.

- **Indeed.AirKey.CloudServer-<номер версии>.x64.ru.ru.msi** — пакет для установки Indeed Key Server.
- **Indeed.AirKey.EventLog.Setup-<номер версии>.x64.ru.ru.msi** — пакет для создания необходимой структуры журнала в Windows EvetLog.

Информация

При использовании SSL-соединения необходим корневой сертификат и сертификат проверки подлинности веб сервера. При создании сертификата для Indeed Key Server в Common Name должно быть имя или IP сервера, к которому настроен доступ для приложения Indeed Key в теге ServerUrl конфигурационного файла сервера Indeed Key Server. Если в CN указан IP-адрес, то он должен быть без протокола и порта.



Установка

Создание базы данных и пользователя

1. Откройте SQL Manager Studio.
2. Создайте пользователя. На вкладке "**General**" укажите:
 - a. Имя пользователя.
 - b. Выберите способ аутентификации "**SQL Server authentication**" и укажите пароль для пользователя.
 - c. Отключите обязательную смену пароля при следующем входе и срок действия пароля.

Login name:

☐ Windows authentication

☒ **SQL Server authentication**

Password:

Confirm password:

☐ Specify old password

Old password:

☒ Enforce password policy

☐ Enforce password expiration

☐ **User must change password at next login**

3. Выдайте пользователю права на создание базы данных.

 Информация

После создания базы данных АК(после первого запроса) можно уменьшить права для пользователя. Достаточно права "**db_owner**" для созданной БД.

4. Нажмите "Ок".

Установки и настройка компонента

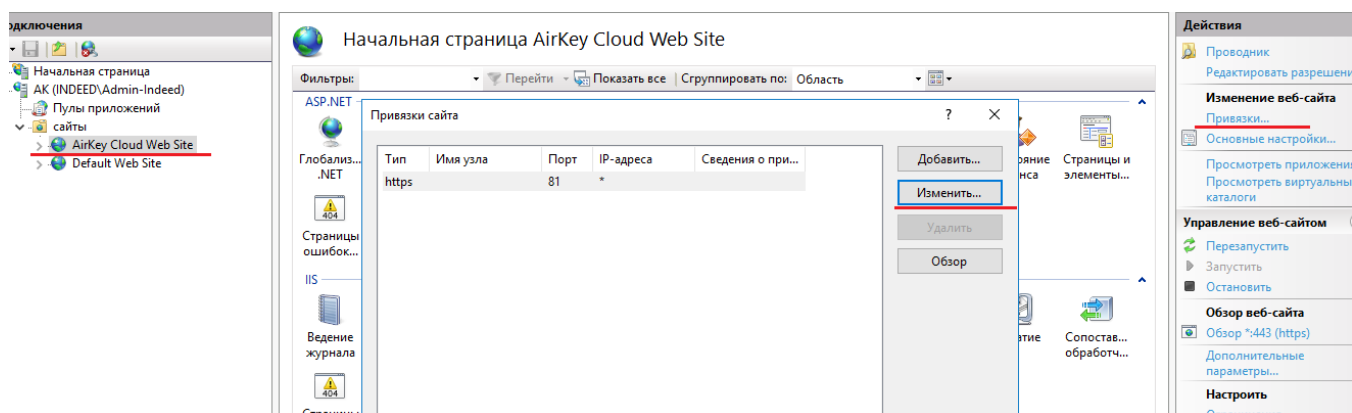
 Информация

Indeed Key Server является Web приложением, которое работает на базе IIS, в процессе установки для него по умолчанию включается обязательно требование SSL в настройках, что в свою очередь требует включенной привязки https.

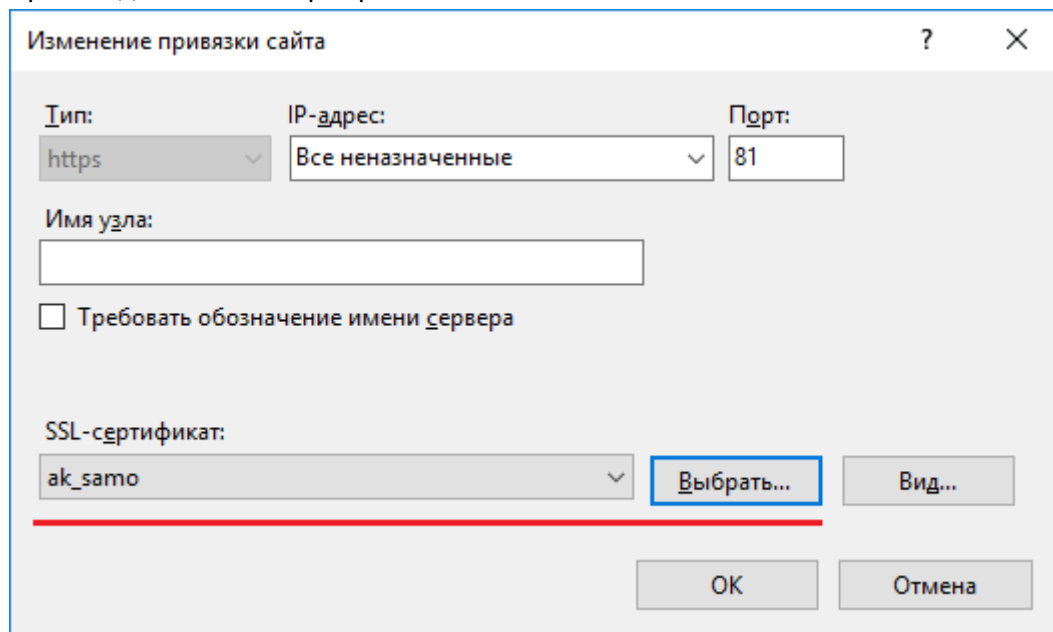
 Информация

На Indeed Key Server должен быть установлен ASP.NET 4.7 для корректной работы.

1. Выполните установку **Indeed Key Server** через запуск пакета для установки.
2. Откройте **IIS Manager**.
3. Выберите **AirKey Cloud Web Site**. В окне "**Действия**" выберите "**Привязки...**" и нажмите "**Изменить...**"



4. В окне "Изменение привязки сайта" выберите SSL сертификат с назначением "Проверка подлинности сервера" и нажмите "Ок".



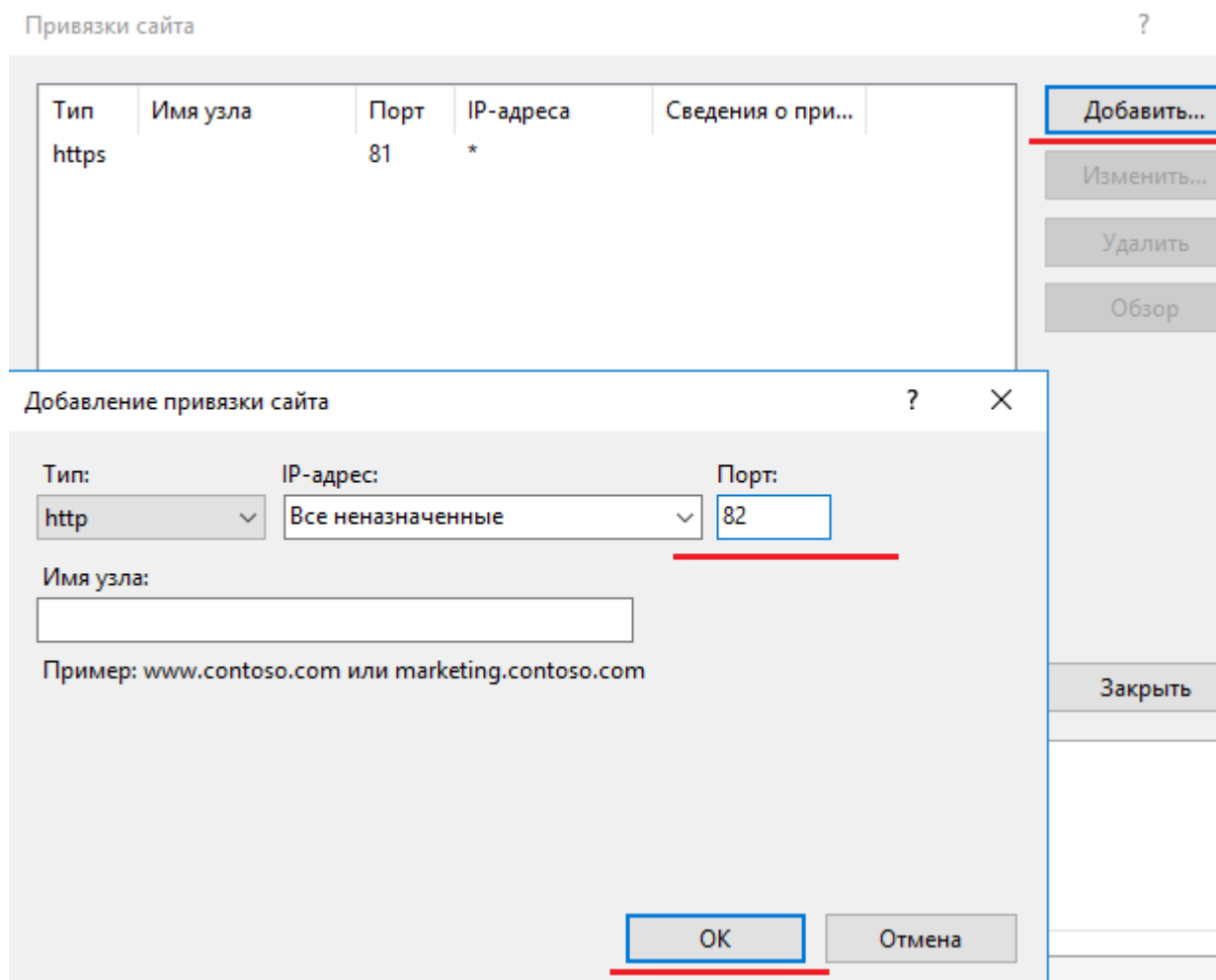
Информация

Для сохранения изменений в конфигурационном файле приложения требуется запустить редактор с правами администратора.

5. При использовании http добавьте привязку с произвольным доступным портом и нажмите "Ок". В конфигурационном файле Web.config (C:\inetpub\wwwroot\airkeycloud) отключите требование https. Для этого измените значение с true на false для ключа requireHttps.

Пример

```
<add key="requireHttps" value="false" />
```



6. Откройте конфигурационный файл **Web.config** (C:\inetpub\wwwroot\airkeycloud).

7. Задайте значение для подключения к SQL Server. Для параметра "**connectionString**" в теге "**connectionStrings**" укажите строку подключения к созданной базе данных.

 Информация

В данной версии не поддерживается Windows аутентификация.

Пример

```
<connectionStrings> <add name="AkDbContext" connectionString="Data Source=AK;
Database=ak_cloud;User Id=ak_cloud_user;Password=Q1q2E3e4" providerName="System.
Data.SqlClient" /> </connectionStrings>
```

8. Для параметра "**value**" с ключом "**ServerUrl**" укажите URL для подключения к Indeed Key Server.

 Информация

По умолчанию используется защищенное соединение (Порт по умолчанию - 81).

При использовании http соединения укажите порт отличный от 80 (Порт 80 используется как порт по умолчанию для http соединений IIS сервера).

 Информация

Indeed Key Server должен быть доступен с мобильного телефона.

Пример

```
<add key="ServerUrl" value="https://airkeycloud.indeed.local:81" /> при использовании
http <add key="ServerUrl" value="http://airkeycloud.indeed.local:82" />
```

9. Укажите URL для подключения к Log серверу Indeed в параметра Url тега logServer.

И **Информация**

Настройки связанные с сертификатом необходимы для настройки двухстороннего TLS соединения между сервером Indeed Key Server и Indeed AM Log Server.

И **Информация**

Данную настройку не требуется указывать. В текущей версии системы Indeed AM не поддерживается работа 2-х стороннего TLS соединения.

Пример

```
<logServer Url="http://logserver.indeed.local/ls/api" CertificateThumbprint=""  
CertificateFilePath="" CertificateFilePassword="" />
```

10. Сохраните изменения и выполните перезагрузку IIS сервера.

Настройка событий сервера

Важно!

В текущей версии системы Indeed AM просмотр событий **Indeed Key Server** со стороны консоли администратора невозможен.

Информация

Установка и настройка осуществляется на Log-сервере Indeed.

В качестве хранилища можно использовать все способы хранения, которые поддерживает Indeed AM Log Server. Мониторить альтернативными способами:

- При хранении в событиях Windows - Через Windows Events.
- При хранении в БД - Сторонними средствами мониторинга или используя SQL запросы.
- При использовании Syslog - Сторонними средствами мониторинга, поддерживающих Syslog.

1. На Log сервере выполните установку пакета "**Indeed.AirKey.EventLog.Setup**".
2. Откройте каталог C:\inetpub\wwwroot\ls.
3. Откройте файл clientApps.config.

4. Для параметра "**Schemald**" со значением "**akcSchema**" задайте место хранения лог-файлов. В теге "**ReadTargetId**" и вложенным тегом "**TargetId**" тега "**WriteTargets**" установите необходимый параметр:

 Информация

По умолчанию задано **akcEventLogTarget** - чтение и запись производится с отдельного журнала событий Windows.

- a. **akcEventLogTarget** - чтение и запись событий из журнала событий Windows.

 Информация

Просмотр событий осуществляется в журнале событий Windows на Log-сервере Indeed. Панель управления Администрирование Просмотр событий Журналы приложений и служб Indeed AirKey Operational

- b. **akcSqlTarget** - чтение и запись событий из базы данных SQL.

 Информация

События доступны в таблице EventEntities через SQL запрос, либо с использование API Indeed AM.

Пример

```
<Application Id="akc" Schemald="akcSchema">
  <ReadTargetId>akcSqlTarget</ReadTargetId>
  <WriteTargets>
    <TargetId>akcSqlTarget</TargetId>
  </WriteTargets>
  <AccessControl> <!--<CertificateAccessControl CertificateThumbprint="001122...
AA11" Rights="Read" />--> </AccessControl> </Application>
```

- c. При использовании в качестве хранилища событий СУБД выполните настройку подключения к БД в файле: C:\inetpub\wwwroot\ls\targetConfigs\akcSqlTarget.config.

 Информация

Для событий **Indeed Key Server** необходимо использовать отдельную от Log Server БД.

Сервис очистки старых данных

В `C:\inetpub\wwwroot\airkeycloud\Web.config` можно задать параметры сервиса очистки старых данных из таблицы `AkDatas`:

Пример

```
<jobSettings>
  <cleanAkDatas enabled="true" firstRunTime="00:00" intervalSec="86400" akDataLifeTimeSec="86400" />
</jobSettings>
```

Описание атрибутов:

Имя атрибута	Описание	Значение	Значение по умолчанию	Минимально допустимое значение
enabled	Флаг включения сервиса	true \ false	true	-
firstRunTime	Время первого запуска сервиса	Строка в формате времени hh:mm	00:00 (полночь)	-
intervalSec	Интервал запуска сервиса	Число секунд	86400 (24 ч)	600
akDataLifeTimeSec	Время жизни данных	Число секунд	86400 (24 ч)	600

Проверка состояния сервера

В [Indeed Key Server](#) существует метод API для проверки состояния сервера: `/api/HealthCheck`. Сервер в фоновой задаче осуществляет проверку состояния хранилища. Интервал выполнения фоновой задачи задается в конфигурационном файле `C:\inetpub\wwwroot\airkeycloud\Web.config` в секции `<jobSettings>`:

Пример

```
<jobSettings>
  <storageHealthCheck intervalSec="60" />
</jobSettings>
```

Шифрование/Расшифрование конфигурационного файла

Запустите командную строку от имени **"Администратора"**.

Для **шифрования конфигурационного файла** необходимо выполнить команду вида:

Пример

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -pe "connectionStrings" -app "/airkeycloud" -prov "DataProtectionConfigurationProvider"
```

Для **расшифровки конфигурационного файла** необходимо выполнить команду вида:

Пример

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -pd "connectionStrings" -app "/airkeycloud"
```


Indeed AM Phone Management Server



Информация

Для работы с приложением требуется установить компонент "Обычная проверка подлинности (Basic Authentication)" для IIS сервера.

Indeed AM Phone Management Server - это Web-приложение, которое работает на базе IIS. Данный компонент предоставляет облегченное API для регистрации, изменения и удаления номеров в базе данных SQL.



Информация

Для регистрации, изменения и удаления номеров в базе данных SQL требуется установка Indeed AM Storage SMS OTP Provider.



Информация

Файлы для Indeed AM Phone Management Server расположены: ***indeed AM <номер версии>/Indeed AM Phone Management Server/Distrib.***

- **Distrib\EA.PhoneManagementServer.deploy.cmd** - Cmd файл необходимый для установки компонента.
- **Scripts <номер версии>** - Power Shell скрипты с примером вызова каждого метода API.
- **WebDeploy_amd64_en-US.msi** - Пакет для установки компонента WebDeploy 3.6 версии 10.0.1973

Установка компонента



Информация

Для установки компонента требуется установить WebDeploy версии 10.0.1973 и выше.

1. Откройте командную строку с правами администратора.
2. Перейдите в папку **Distrib** компонента **EAPhoneServer**.
3. Запустите установку компонента через вызов команды:

```
EA.PhoneManagementServer.deploy.cmd /Y
```

4. После успешной установки в IIS Manager отобразится отдельное Web приложение EAPhoneServer.

```
Администратор: Командная строка
Сведения: Добавляется файл (Default Web Site/EAPhoneServer\bin\roslyn\Microsoft.DiaSymReader.Native.amd64.dll).
Сведения: Добавляется файл (Default Web Site/EAPhoneServer\bin\roslyn\Microsoft.DiaSymReader.Native.x86.dll).
Сведения: Добавляется файл (Default Web Site/EAPhoneServer\bin\roslyn\Microsoft.VisualBasic.Core.targets).
Сведения: Добавляется файл (Default Web Site/EAPhoneServer\bin\roslyn\System.AppContext.dll).
Сведения: Добавляется файл (Default Web Site/EAPhoneServer\bin\roslyn\System.Collections.Immutable.dll).
Сведения: Добавляется файл (Default Web Site/EAPhoneServer\bin\roslyn\System.Diagnostics.StackTrace.dll).
Сведения: Добавляется файл (Default Web Site/EAPhoneServer\bin\roslyn\System.IO.FileSystem.dll).
Сведения: Добавляется файл (Default Web Site/EAPhoneServer\bin\roslyn\System.IO.FileSystem.Primitives.dll).
Сведения: Добавляется файл (Default Web Site/EAPhoneServer\bin\roslyn\System.Reflection.Metadata.dll).
Сведения: Добавляется файл (Default Web Site/EAPhoneServer\bin\roslyn\vbc.exe).
Сведения: Добавляется файл (Default Web Site/EAPhoneServer\bin\roslyn\vbc.exe.config).
Сведения: Добавляется файл (Default Web Site/EAPhoneServer\bin\roslyn\vbc.rsp).
Сведения: Добавляется файл (Default Web Site/EAPhoneServer\bin\roslyn\VBCSCompiler.exe).
Сведения: Добавляется файл (Default Web Site/EAPhoneServer\bin\roslyn\VBCSCompiler.exe.config).
Сведения: Добавляется каталог (Default Web Site/EAPhoneServer\bin\ru).
Сведения: Добавляется файл (Default Web Site/EAPhoneServer\bin\ru\EA.Core.resources.dll).
Сведения: Добавляется файл (Default Web Site/EAPhoneServer\bin\Swashbuckle.Core.dll).
Сведения: Добавляется файл (Default Web Site/EAPhoneServer\bin\System.Net.Http.Formatting.dll).
Сведения: Добавляется файл (Default Web Site/EAPhoneServer\bin\System.Runtime.CompilerServices.Unsafe.dll).
Сведения: Добавляется файл (Default Web Site/EAPhoneServer\bin\System.Threading.Tasks.Extensions.dll).
Сведения: Добавляется файл (Default Web Site/EAPhoneServer\bin\System.Web.Http.dll).
Сведения: Добавляется файл (Default Web Site/EAPhoneServer\bin\System.Web.Http.WebHost.dll).
Сведения: Добавляется файл (Default Web Site/EAPhoneServer\bin\Unity.Abstractions.dll).
Сведения: Добавляется файл (Default Web Site/EAPhoneServer\bin\Unity.Abstractions.pdb).
Сведения: Добавляется файл (Default Web Site/EAPhoneServer\bin\Unity.AspNet.WebApi.dll).
Сведения: Добавляется файл (Default Web Site/EAPhoneServer\bin\Unity.AspNet.WebApi.pdb).
Сведения: Добавляется файл (Default Web Site/EAPhoneServer\bin\Unity.Container.dll).
Сведения: Добавляется файл (Default Web Site/EAPhoneServer\bin\Unity.Container.pdb).
Сведения: Добавляется файл (Default Web Site/EAPhoneServer\bin\WebActivatorEx.dll).
Сведения: Добавляется файл (Default Web Site/EAPhoneServer\Global.asax).
Сведения: Добавляется файл (Default Web Site/EAPhoneServer\Web.config).
Сведения: Adding ACLs for path (Default Web Site/EAPhoneServer)
Сведения: Adding ACLs for path (Default Web Site/EAPhoneServer)
Сводка по изменениям: 74 (добавлено: 73, удалено: 0, обновлено: 1, параметров изменено: 0, скопировано байт: 21672941)

C:\Users\Admin-Indeed\Desktop\EAPhoneServer_v.1.4\distrib>
```

Удаление компонента EAPhoneServer

1. Остановите IIS сервер с компонентом EaPhone Server.
2. Откройте папку **C:\inetpub\wwwroot**.
3. Удалите папку **"EAPhoneServer"** со всем содержимым.
4. Удалите приложение **"EAPhoneServer"** в IIS Manager.
5. Возобновите работу IIS.

Настройка компонента

1. Откройте компонент **EAPhoneServer** в IIS Manager.
2. Откройте "**Проверка подлинности**" и включите параметр "**Обычная проверка подлинности**". Все остальные методы проверки подлинности требуется отключить.
3. Откройте "**Правила авторизации**". Измените существующее правило или добавьте новое. В настройках укажите пользователя или группу пользователей, которым будет доступен вызов методов API.



Информация

Данную настройку рекомендуется выполнить в целях обеспечения безопасного доступа к компоненту EAPhoneServer.



Информация

При указании группы пользователей указывается значение атрибута **name** данной группы.

При указании пользователя указывается значение атрибута **sAMAccountName** или **userPrincipalName**.

Настройка политики



Информация

Политику необходимо настроить для предоставления сервисному пользователю необходимого набора прав для работы.

1. Откройте Admin Console и основную политику системы, которая распространяется на целевых пользователей системы.
2. Перейдите на вкладку "**Администраторы**" и добавьте сервисного пользователя для компонента Indeed AM EAPhone Server в роль "**Администратор**".

Main - Администраторы

Информация	+ Добавить Удалить		
Приложения			
Область действия			
Администраторы			
Аутентификаторы			
	ИМЯ	ГРУППА БЕЗОПАСНОСТИ	ТИП ОБЪЕКТА
	Администратор		
	☐ AdminsIndeed	Администратор	Группа
	☐ eapphone	Администратор	Пользователь

Настройка конфигурационного файла

Информация

Для сохранения изменений в конфигурационном файле приложения, требуется запустить редактор с правами администратора.

1. Откройте конфигурационный файл компонента **Web.config** (C:\inetpub\wwwroot\EAPhoneServer\Web.config).
2. В теге **appSettings** выполните следующие настройки:

Информация

От имени указанного пользователя будут выполняться запросы к API.

- а. В строке с параметром **key**, со значением **username**, задайте значение для параметра **value**. В значении укажите имя пользователя в формате **UPN**, созданного для работы с компонентом.

Пример

```
<add key="username" value="eaphone@indeed.local" />
```

- б. В строке с параметром **key**, со значением **password**, задайте значение для параметра **value**. В значении укажите пароль пользователя.

Пример

```
<add key="password" value="Q1q2E3e4" />
```

- в. В строке с параметром **key**, со значением **lognames**, задайте формат логирования имен пользователей. Поддерживаемые форматы :



Информация

Если необходимо указать несколько форматов, то требуется указать значения через запятую.

- **Id** - Идентификатор пользователя в системе Indeed AM в формате **rootUserCatalogProviderId_Guid**.
- **Name** - Значение атрибута **name** из Active Directory.
- **CanonicalName** - Имя пользователя в формате **Canonical-Name** (myserver.demo.local/users/UserName).
- **PrincipalName** - Значение атрибута **userPrincipalName** из Active Directory.
- **SamCompatibleName** - Имя пользователя в формате **domainName\UserName**.
- **DistinguishedName** - Значение атрибута **distinguishedName** из Active Directory.
- **Sid** - Значение атрибута **objectSid** из Active Directory.
- **Email** - Значение атрибута **mail** из Active Directory или значение указанное в конфигурационном файле сервера.
- **Phone** - Значение атрибута **telephoneNumber** из Active Directory или значение указанное в конфигурационном файле сервера.

Пример

```
<add key="lognames" value="PrincipalName,Sid" />
```

3. Задайте **url** для подключения к лог серверу. Редактируем тег **logServer**.
- a. **URL** - url для подключения к лог серверу в формате http (s)://полное_dns_имя_сервера/ls/api.
 - b. **CertificateThumbprint** - если закрытый ключ в реестре, а сертификат в хранилище компьютера.
 - c. **CertificateFilePath** - если ключевая пара в pfx.
 - d. **CertificateFilePassword** - пароль от pfx.

Пример

```
<logServer Url="http://dc2.new.loc/ls/api/" CertificateThumbprint=""  
CertificateFilePath="" CertificateFilePassword="" />
```

4. Создайте папку для хранения локального кэша событий. По умолчанию задан путь: *D:\Temp\IndeedIdServerEventLog\EaPhoneEventCache*. Создайте указанную по умолчанию папку, либо укажите любой другой локальный путь. Выдайте полный доступ для пользователя **IIS_IUSRS** на конечную папку.

Пример

```
<logServerClient AppId="ea" Component="server" EventCacheDirectory="C:  
\inetpub\wwwroot\EAPhoneServer\EventCache" LogServerTargetConfigFile="" />
```

5. Для значения параметра **connectionString** укажите полный URL доступного сервера Indeed AM или балансировщика в формате:

```
http/https://<Полное DNS имя сервера Indeed AM или балансировщика>/am/core/
```

Пример

```
<add name="EAPhoneAPIURL" connectionString="http://dc2.new.loc/am/core/" />
```

Шифрование и дешифрование конфигурационного файла



Информация

Настройка рекомендована в целях обеспечения безопасности.

1. Для шифрования выполните следующую команду в командной строке с правами администратора:

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -pe "appSettings" -app "/EAPhoneServer" -prov "DataProtectionConfigurationProvider"
```

```
C:\Windows\system32>C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -pe "appSettings" -app "/EAPhoneServer" -prov "DataProtectionConfigurationProvider"
Microsoft (R) ASP.NET RegIIS версии 4.0.30319.0
Административная программа для установки и удаления ASP.NET на локальном компьютере.
(C) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.
Шифрование раздела конфигурации...
Выполнено!
```

2. Для расшифровки выполните следующую команду в командной строке с правами администратора:

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -pd "appSettings" -app "/EAPhoneServer"
```

```
C:\Windows\system32>C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -pd "appSettings" -app "/EAPhoneServer"
Microsoft (R) ASP.NET RegIIS версии 4.0.30319.0
Административная программа для установки и удаления ASP.NET на локальном компьютере.
(C) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.
Расшифровка раздела конфигурации...
Выполнено!
```

Доступ к UI API

Для доступа к UI компонента выполните следующее:

1. Откройте URL: *http(s)://<Полное DNS имя сервера с компонентом EAPhoneServer>/EAPhoneServer/swagger*
2. Выполните авторизацию под пользователем который входит в группу, настроенную в "Правила авторизации". Для входа укажите имя пользователя в формате UPN.

Описание методов API компонента

Информация

Входные данные передаются в формате JSON. Для вызова метода API используется URL в формате:

```
http/https://<Полное DNS имя сервера с компонентом EAPhoneServer>/EAPhoneServer  
/<метод API>
```

Регистрация

Информация

Скрипт по работе с данным методом API доступен по ссылке.

Для регистрации номера телефона используется POST запрос к методу API: **/api/IID/CreatePhone**

1. Входные данные:
 - a. **Username** - Имя пользователя в формате UPN для которого следует зарегистрировать номер телефона.
 - b. **Phone** - Номер телефона пользователя, который следует зарегистрировать в системе.
2. Выходные данные: HTTP ответ с кодом состояния HTTP.
3. Пример запроса:
 - a. **URL** - `http://AmIndeed.demo.local/EAPhoneServer/api/IID/CreatePhone`
 - b. **Данные** - `{ "Username": "User@demo.local", "Phone": "123456" }`

Генерируемые события

Информация

В качестве примера используется формат имени: **PrincipalName, Sid**

Успешная регистрация

При успешной регистрации провайдера генерируется событие с уникальным Id - **1088**.
Тело события содержит:

- **Описание:** Телефонный номер успешно зарегистрирован.
- **Пользователь** - В данном параметре указывается пользователь, для которого была выполнена регистрация. Формат имени пользователя задается в конфигурационном файле, в параметре **lognames**.
- **Инициатор** - В данном параметре указывается пользователь, который указан в качестве администратора компонента EAPhoneServer в конфигурационном файле. Формат имени пользователя задается в конфигурационном файле, в параметре **lognames**.
- **Пользователь API** - В данном параметре указывается пользователь, который был аутентифицирован по Basic аутентификации перед использованием метода API. Имя отображается в формате, который был указан при вводе в форму аутентификации.
- **Телефон** - В данном параметре отображается номер телефона пользователя, который будет зарегистрирован.

СОБЫТИЕ	ДАТА	МОДУЛЬ	ИНИЦИАТОР	КОД
▼ ⓘ Телефонный номер успешно зарегистрирован.	2020.09.10 10:44:04	None	eaphone@indeed.local, S-1-5-21-3872528378-1805565572-380156938-1109	1088

Телефонный номер успешно зарегистрирован.
 Пользователь: Admin-Indeed@indeed.local, S-1-5-21-3872528378-1805565572-380156938-1104
 Инициатор: eaphone@indeed.local, S-1-5-21-3872528378-1805565572-380156938-1109
 Пользователь API: INDEED\Admin-Indeed
 Телефон: 8952485654

Ошибка при регистрации

При возникновении ошибки, во время регистрации провайдера, генерируется событие с уникальным Id - **2073**. Тело события содержит:

- **Описание:** Ошибка регистрации телефонного номера.
- **Пользователь** - В данном параметре указывается пользователь, для которого была выполнена регистрация. Формат имени пользователя задается в конфигурационном файле, в параметре **lognames**.
- **Инициатор** - В данном параметре указывается пользователь, который указан в качестве администратора компонента EAPhoneServer в конфигурационном файле. Формат имени пользователя задается в конфигурационном файле, в параметре **lognames**.
- **Пользователь API** - В данном параметре указывается пользователь, который был аутентифицирован по Basic аутентификации перед использованием метода API. Имя отображается в формате, который был указан при вводе в форму аутентификации.
- **Описание ошибки** - В данном параметре указывается более подробное описание возникшей ошибки.
- **Инициатор ошибки** - В данном параметре указывается пользователь, по причине которого возникла ошибка.
- **Телефон** - В данном параметре отображается номер телефона пользователя, который будет зарегистрирован.



Информация

В случае возникновения **ошибки при логоне в систему** или **возникновения ошибки доступа(403)**, в данном параметре будут отображаться данные **Сервисного пользователя**.

СОБЫТИЕ	ДАТА	МОДУЛЬ	ИНИЦИАТОР	К
▼ Ошибка регистрации телефонного номера.	2020.09.10 10:45:58	None	eapphone@indeed.local, S-1-5-21-3872528378- 1805565572- 380156938-1109	21

Ошибка регистрации телефонного номера.
Пользователь: Admi-Indeed@indeed.local
Инициатор: eapphone@indeed.local, S-1-5-21-3872528378-1805565572-380156938-1109
Пользователь API: INDEED\Admin-Indeed
Описание ошибки: Данные не найдены. Пользователь не найден.
Инициатор ошибки: Admi-Indeed@indeed.local
Телефон: 8952485654

Изменение



Информация

Скрипт по работе с данным методом API доступен по ссылке.

Для изменения номера телефона используется POST запрос к методу API: **/api/IID/UpdatePhone**

1. Входные данные :
 - a. **Phone** - Номер телефона пользователя, который следует зарегистрировать в системе.
 - b. **Username** - Имя пользователя в формате UPN для которого следует изменить номер телефона.
2. Выходные данные: HTTP ответ с кодом состояния HTTP.
3. Пример запроса:
 - a. **URL** - `http://AmIndeed.demo.local/EAPhoneServer/api/IID/UpdatePhone`
 - b. **Данные** - `{ "Username": "User@demo.local", "Phone": "654321" }` Пример запроса:

Генерируемые события



Информация

В качестве примера используется формат имени: **Id, Name, PrincipalName**.

Успешное изменение

При успешном изменении провайдера генерируется событие с уникальным Id - **1089**. Тело события содержит:

- **Описание:** Телефонный номер успешно изменен.
- **Пользователь** - В данном параметре указывается пользователь, для которого была выполнена регистрация. Формат имени пользователя задается в конфигурационном файле, в параметре `lognames`.
- **Инициатор** - В данном параметре указывается пользователь, который указан в качестве администратора компонента EAPhoneServer в конфигурационном файле. Формат имени пользователя задается в конфигурационном файле, в параметре `lognames`.
- **Пользователь API** - В данном параметре указывается пользователь, который был аутентифицирован по Basic аутентификации перед использованием метода API. Имя отображается в формате, который был указан при вводе в форму аутентификации.
- **Телефон** - В данном параметре отображается измененный номер телефона пользователя.

СОБЫТИЕ	ДАТА	МОДУЛЬ	ИНИЦИАТОР	К
▼ ⓘ Телефонный номер успешно изменен.	2020.09.10 10:50:46	None	Userid_969f39ac-1e2b-4784-8d5c-3836adc1ac5c, eaphone, eaphone@indeed.local	10

Телефонный номер успешно изменен.
 Пользователь: Userid_3273c290-bcdc-469b-a281-18fe83b4d00e, Admin-Indeed, Admin-Indeed@indeed.local
 Инициатор: Userid_969f39ac-1e2b-4784-8d5c-3836adc1ac5c, eaphone, eaphone@indeed.local
 Пользователь API: INDEED\Admin-Indeed
 Телефон: 12345678910

Ошибка при изменении

При возникновении ошибки, во время изменения провайдера, генерируется событие с уникальным Id - **2074**. Тело события содержит:

- **Описание:** Ошибка изменения телефонного номера.
- **Пользователь** - В данном параметре указывается пользователь, для которого была выполнена регистрация. Формат имени пользователя задается в конфигурационном файле, в параметре **lognames**.
- **Инициатор** - В данном параметре указывается пользователь, который указан в качестве администратора компонента EAPhoneServer в конфигурационном файле. Формат имени пользователя задается в конфигурационном файле, в параметре **lognames**.
- **Пользователь API** - В данном параметре указывается пользователь, который был аутентифицирован по Basic аутентификации перед использованием метода API. Имя отображается в формате, который был указан при вводе в форму аутентификации.
- **Описание ошибки** - В данном параметре указывается более подробное описание возникшей ошибки.
- **Инициатор ошибки** - В данном параметре указывается пользователь, по причине которого возникла ошибка.
- **Телефон** - В данном параметре отображается измененный номер телефона пользователя.



Информация

В случае возникновения **ошибки при логоне в систему** или **возникновения ошибки доступа(403)**, в данном параметре будут отображаться данные **Сервисного пользователя**.

СОБЫТИЕ	ДАТА	МОДУЛЬ	ИНИЦИАТОР	КОД
❗ Ошибка изменения телефонного номера.	2020.09.10 10:54:16	None	Userid_969f39ac-1e2b-4784-8d5c-3836adc1ac5c, eaphone, eaphone@indeed.local	2074

Ошибка изменения телефонного номера.
 Пользователь: Admi-Indeed@indeed.local
 Инициатор: Userid_969f39ac-1e2b-4784-8d5c-3836adc1ac5c, eaphone, eaphone@indeed.local
 Пользователь API: INDEED\Admin-Indeed
 Описание ошибки: Данные не найдены. Пользователь не найден.
 Инициатор ошибки: Admi-Indeed@indeed.local
 Телефон: 12345678910

Удаление

Информация

Скрипт по работе с данным методом API доступен по ссылке.

Для удаления номера телефона используется POST запрос к методу API: **/api/IID/DeletePhone**

- Входные данные:
 - Username** - Имя пользователя в формате UPN для которого следует удалить номер телефона.
- Выходные данные: HTTP ответ с кодом состояния HTTP.
- Пример запроса:
 - URL** - `http://AmIndeed.demo.local/EAPhoneServer/api/IID/DeletePhone`
 - Данные** - `{ "Username": "User@demo.local" }`

Генерируемые события

Информация

В качестве примера используется формат имени: **DistinguishedName**, **SamCompatibleName**.

Успешное удаление

При успешном удалении провайдера генерируется событие с уникальным Id - **1090**. Тело события содержит:

- **Описание:** Телефонный номер успешно удален.
- **Пользователь** - В данном параметре указывается пользователь, для которого была выполнена регистрация. Формат имени пользователя задается в конфигурационном файле, в параметре `lognames`.
- **Инициатор** - В данном параметре указывается пользователь, который указан в качестве администратора компонента EAPhoneServer в конфигурационном файле. Формат имени пользователя задается в конфигурационном файле, в параметре `lognames`.
- **Пользователь API** - В данном параметре указывается пользователь, который был аутентифицирован по Basic аутентификации перед использованием метода API. Имя отображается в формате, который был указан при вводе в форму аутентификации.

СОБЫТИЕ	ДАТА	МОДУЛЬ	ИНИЦИАТОР
Телефонный номер успешно удален.	2020.09.10 10:56:02	None	CN=eaphone,OU=ServiceUsers,OU=UsersIndeed,OU=Indeed,DC=indeed,DC=local, INDEED\eaphone
Телефонный номер успешно удален. Пользователь: CN=Admin-Indeed,OU=UsersIndeed,OU=Indeed,DC=indeed,DC=local, INDEED\Admin-Indeed Инициатор: CN=eaphone,OU=ServiceUsers,OU=UsersIndeed,OU=Indeed,DC=indeed,DC=local, INDEED\eaphone Пользователь API: INDEED\Admin-Indeed			

Ошибка при удалении

При возникновении ошибки, во время удаления провайдера, генерируется событие с уникальным Id - **2075**. Тело события содержит:

- **Описание:** Ошибка удаления телефонного номера.
- **Пользователь** - В данном параметре указывается пользователь, для которого была выполнена регистрация. Формат имени пользователя задается в конфигурационном файле, в параметре **lognames**.
- **Инициатор** - В данном параметре указывается пользователь, который указан в качестве администратора компонента EAPhoneServer в конфигурационном файле. Формат имени пользователя задается в конфигурационном файле, в параметре **lognames**.
- **Пользователь API** - В данном параметре указывается пользователь, который был аутентифицирован по Basic аутентификации перед использованием метода API. Имя отображается в формате, который был указан при вводе в форму аутентификации.
- **Описание ошибки** - В данном параметре указывается более подробное описание возникшей ошибки.
- **Инициатор ошибки** - В данном параметре указывается пользователь, по причине которого возникла ошибка.



Информация

В случае возникновения **ошибки при логоне в систему** или **возникновения ошибки доступа(403)**, в данном параметре будут отображаться данные **Сервисного пользователя**.

СОБЫТИЕ	ДАТА	МОДУЛЬ	ИНИЦИАТОР	КОД
▼ ⓘ Ошибка удаления телефонного номера.	2020.09.10 10:56:53	None	CN=eaphone,OU=ServiceUsers,OU=UsersIndeed,OU=Indeed,DC=indeed,DC=local, INDEED\eaphone	2075

Ошибка удаления телефонного номера.
 Пользователь: Admin-Indeed@indeed.local
 Инициатор: CN=eaphone,OU=ServiceUsers,OU=UsersIndeed,OU=Indeed,DC=indeed,DC=local, INDEED\eaphone
 Пользователь API: INDEED\Admin-Indeed
 Описание ошибки: Данные не найдены. Пользователь не найден.
 Инициатор ошибки: Admin-Indeed@indeed.local

Indeed AM Reset Password

Indeed AM Reset Password - Утилита предназначенная для сброса пароля пользователю в Active Directory с автоматической синхронизацией в системе Indeed AM.

При сбросе пароля через данную утилиту пароль будет сгенерирован утилитой автоматически, сложность генерируемого пароля задаётся администратором системы при настройке утилиты. Генерируемый пароль отправляется пользователю посредством Email или SMS.

Утилита выполняет сброс пароля пользователя в Active Directory, поэтому для пользователя, от имени которого выполняется запуск утилиты, необходимо выдать права администратора в домене. Достаточно добавить пользователя в доменную группу "**Администраторы**".

Также пользователю необходимо выдать права глобального администратора в системе Indeed AM.

Важно!

Для отправки пароля пользователю через Email или SMS на сервере Indeed AM должен быть установлен и настроен соответствующий провайдер Indeed.

Информация

Файлы для установки утилиты расположены в дистрибутиве системы по пути:
Indeed AM <номер версии>\Indeed AM Reset Password.

- **IndeedAM.EA.ResetPassword -<номер версии>.x64.ru-ru.msi** - Пакет для установки утилиты Indeed AM Reset Password
- **Misc** - Папка с шаблонами групповых политик.

Установка и настройка

Установка

Информация

Установка утилиты выполняется на рабочую станцию\сервер, где в дальнейшем будет выполняться запуск утилиты.

1. Выполнить установку утилиты через запуск пакета для установки утилиты Indeed AM Reset Password.

Настройка

Настройка через групповые политики

1. Выполните загрузку шаблонов GPO Indeed из дистрибутива в локальное хранилище машины, где установлена утилита.



Информация

Локальное хранилище GPO находится по пути: C:\Windows\PolicyDefinitions

2. Откройте редактор локальной групповой политики и перейдите в раздел:
Конфигурация компьютера Административные шаблоны Indeed ID Reset Password
3. Выберите и настройте политику "**Настройка утилиты сброса пароля**". Для настройки задайте следующие значения:
 - a. **Server URL** - URL адрес сервера Indeed AM в формате: **http(s)://<DNS имя Indeed AM сервера>/am/core/**
 - b. **Тип провайдера** - Выбирается способ получения сгенерированного пароля для пользователя. Доступно использования SMS или Email.
 - c. **Текст темы сообщения** - Указывается тема сообщения, которая будет указана в письме.



Важно!

Обязательный параметр при использовании Email для получения пароля.

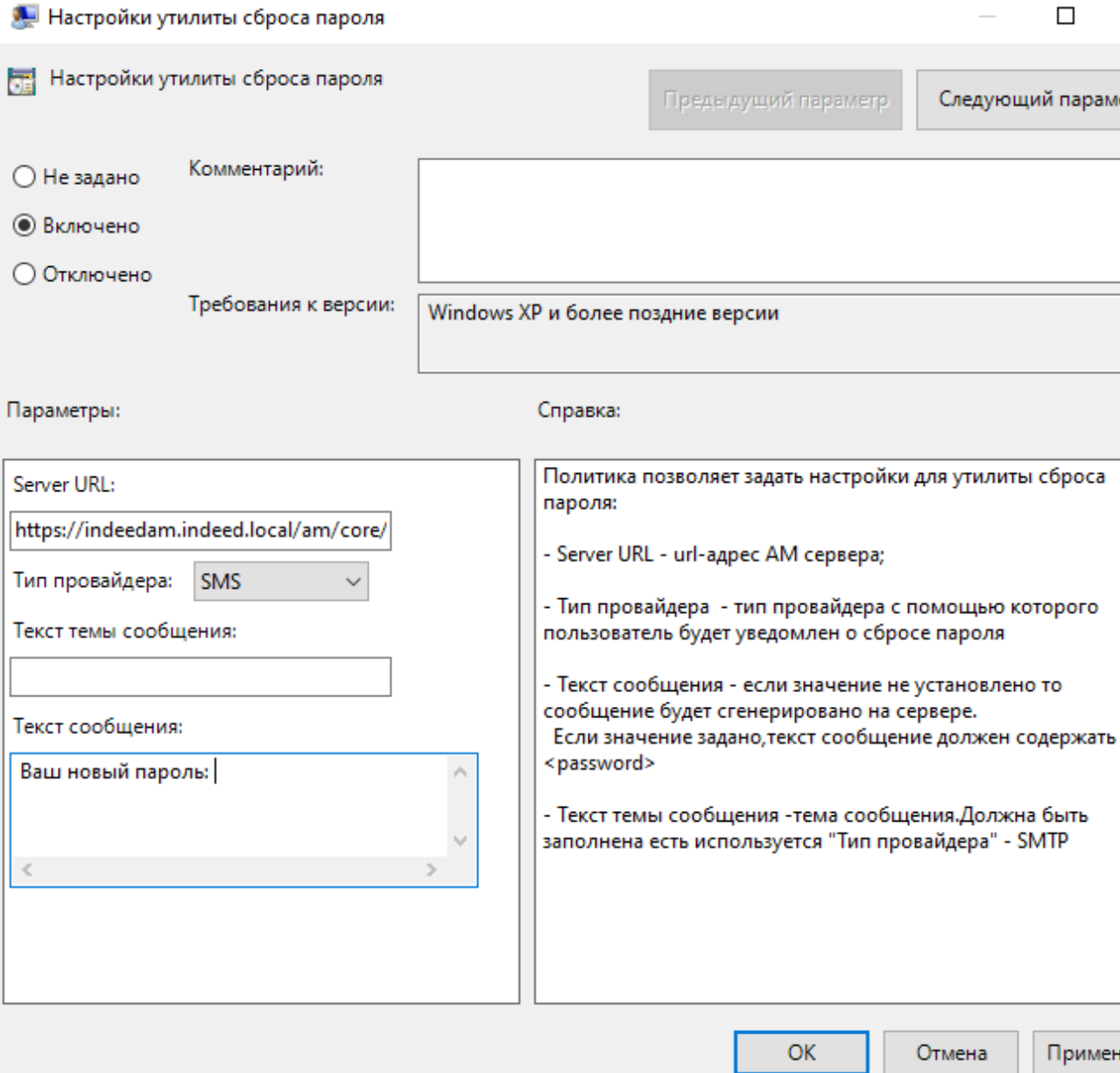
d. **Текст сообщения** - Указывается текст сообщения.

 Информация

Опциональный параметр.

Если значение не установлено, то в качестве текста будет указан пароль.

Если задано значение, то поле должно содержать текст: <password>



Настройки утилиты сброса пароля

Настройки утилиты сброса пароля

Предыдущий параметр Следующий параметр

☐ Не задано ☒ Включено ☐ Отключено

Комментарий:

Требования к версии: Windows XP и более поздние версии

Параметры:

Server URL: https://indeedam.indeed.local/am/core/

Тип провайдера: SMS

Текст темы сообщения:

Текст сообщения: Ваш новый пароль:

Справка:

Политика позволяет задать настройки для утилиты сброса пароля:

- Server URL - url-адрес AM сервера;
- Тип провайдера - тип провайдера с помощью которого пользователь будет уведомлен о сбросе пароля
- Текст сообщения - если значение не установлено то сообщение будет сгенерировано на сервере. Если значение задано, текст сообщения должен содержать <password>
- Текст темы сообщения - тема сообщения. Должна быть заполнена если используется "Тип провайдера" - SMTP

ОК Отмена Применить

4. Выберите и настройте политику "**Настройки генерации пароля**". В политике укажите необходимые критерии для генерации пароля.

Настройки генерации пароля

Предыдущий параметр Следующий параметр

☐ Не задано Комментарий:

☒ Включено

☐ Отключено

Требования к версии: Windows XP и более поздние версии

Параметры: Справка:

Длина пароля 12

Вхождение групп символов:

☒ Цифры

☒ Строчные латинские буквы

☒ Прописные латинские буквы

☒ Специальные символы

Политика позволяет задать длину и вхождение групп символов при генерации пароля.

Группы символов:
Цифры - "0-9";
Строчные латинские буквы - "a-z";
Прописные латинские буквы - "A-Z";
Специальные символы - ".,<>/?[]{}=+-_\\!@#\$%^&*0"

Если политика не определена или выключена, то пароль будет состоять из цифр, латинских букв, специальных символов и иметь длину 8 знаков.

OK Отмена Применить

Пример использования

1. Запустите утилиту "**Reset Password**" из меню "**Пуск**" Windows или через запуск исполняемого файла "**C:\Program Files\Indeed AM\Reset Password\EA.ResetPassword.exe**" от имени пользователя, у которого есть права для сброса пароля в AD.

2. В основном окне утилиты нажмите на кнопку **"Login"**.



Информация

Вход в утилиту выполняется под пользователем в чьей сессии выполняется запуск. При необходимости можно выполнить запуск утилиты от имени другого пользователя в активной сессии.

3. Выполните поиск пользователя, которому необходимо сбросить пароль, и выберите его в результатах поиска.



ResetPassword

Пользователи

Имя

Имя	Имя учетной записи
Иван Иванов	ii@indeed.local

4. На странице с пользователем нажмите на кнопку "Сбросить пароль AD" и подтвердите действие.



Информация

При сбросе пароля обратите внимание на поля "Номер телефона" и "Email". Для отправки пароля в смс в поле "Номер телефона" должен быть указан номер телефона пользователя, а при отправке по почте в поле "Email" адрес электронной почты.



ResetPassword

INDEED\ii - Общая информация

Учетная запись

INDEED\ii

Имя

Иван

Фамилия

Иванов

Номер телефона

88889992233

Email

ii@demo.local

Путь в каталоге

indeed.local/Indeed/Users/Иван Иванов

Сбросить пароль AD

Назад

5. При успешном сбросе пароля будет выведено сообщение, что пароль был успешно сброшен и сообщение отправлено.

Сброс пароля



Пароль был успешно сброшен. Сообщение отправлено пользователю.

ОК

Установка и настройка провайдеров



Информация

Файлы шаблонов политик для провайдеров расположены: *indeed AM <номер версии>\Misc\ADMX Templates..*

Необходимые файлы шаблонов для локальной групповой политики нужно скопировать на целевой машине в *C:\Windows\PolicyDefinitions.*

Необходимые файлы шаблонов для доменной групповой политики нужно скопировать на контроллере домена в *C:\Windows\SYSVOL\sysvol\<Имя домена>\Policies\PolicyDefinitions*

В этом разделе содержится описание настраиваемых параметров работы Indeed AM Provider и способах их изменения. Изменение параметров работы провайдера осуществляется через механизм групповых политик Active Directory.

- [Indeed AM Windows Password Provider](#)
- [Indeed AM Smart Card Provider](#)
- [Indeed AM IronLogic Z2USB Provider](#)
- [Indeed AM OMNIKEY Provider](#)
- [Indeed AM Futronic Provider](#)
- [Indeed AM Passcode Provider](#)
- [Indeed AM Email OTP Provider](#)
- [Indeed AM Hardware TOTP Provider](#)
- [Indeed AM HOTP Provider](#)
- [Indeed AM Storage SMS OTP Provider](#)
- [Indeed AM Telegram OTP Provider](#)
- [Indeed AM SMS OTP Provider](#)
- [Indeed AM Software OTP Provider](#)
- [Indeed Key Provider](#)
- [Indeed AM MFA Provider](#)

Indeed AM Windows Password Provider

ID Провайдера

{CF189AF5-01C5-469D-A859-A8F2F41ED153}

Информация

Файлы для Indeed AM Windows Password Provider расположены: ***indeed AM <номер версии>/Indeed AM Providers/Indeed AM Windows Password Provider/<Номер версии>***.

- **IndeedAM.AuthProviders.AMWP-<номер версии>.x64.ru-ru.msi** - Пакет для установки Indeed AM Windows Password Provider на 64-х битных ОС.
- **IndeedAM.AuthProviders.AMWP-<номер версии>.x86.ru-ru.msi** - Пакет для установки Indeed AM Windows Password Provider на 32-х битных ОС.

1. Выполнить установку Indeed AM Windows Password Provider через запуск соответствующего пакета.
2. После завершения установки может потребоваться перезагрузка системы. Если программа установки предлагает выполнить перезагрузку, подтвердите данное действие.
3. Удаление/Восстановление продукта осуществляется стандартным для поддерживаемых ОС способом, через меню Панель управления.

Indeed AM Smart Card Provider

ID Провайдера

Smartcard: {0AF65AD8-DB77-4B64-B489-958D9B36E28C}

Smartcard + PIN: {42456525-8EC1-4AB1-97B8-45AF8635D10F}

Информация

Файлы для Indeed AM SmartCard Provider расположены: ***indeed AM <номер версии> /Indeed AM Providers/Indeed AM SmartCard Provider/<номер версии>***

- **IndeedID.Smartcard.Provider.msi** - Пакет для установки **Indeed AM Smart Card Provider**.
- **IndeedID.Smartcard.PIN.Provider.msi** - Пакет для установки **Indeed AM Smart Card Provider + PIN**.

Файлы шаблонов политик расположены: ***indeed AM <номер версии>\Misc\ADMX Templates***.

О компоненте Indeed AM Smart Card Provider

Компонент Indeed AM Smart Card Provider предназначен для аутентификации пользователей по персональным устройствам (смарт-картам, USB-ключам) и совместного использования с продуктами Indeed Windows Logon и Indeed Enterprise Single Sign-On.

Возможны варианты использования одного и того же устройства аутентификации как с запросом PIN-кода, так и без него. В случае использования Indeed AM Smart Card Provider для аутентификации пользователю потребуется приложить карту к считывателю, PIN-код запрашиваться не будет. При использовании Indeed AM Smart Card Provider with PIN ввод PIN-кода потребуется при каждой аутентификации пользователя.

Информация

Indeed AM Smart Card Provider with PIN не позволяет задавать, изменять или удалять PIN-коды устройств аутентификации. Для изменения или удаления PIN кодов используйте специализированное программное обеспечение от производителей устройств аутентификации.

Установка



Примечание

Для работы провайдера требуется установка Indeed AM Bsp Broker на сервере Indeed AM.

Файлы для Indeed AM Bsp Broker расположены: ***indeed AM <номер версии>/Indeed Providers/Indeed AM Bsp Broker/<Номер версии>***.

- **IndeedAM.AuthProviders.BspBroker-<номер версии>.x64.ru-ru.msi** - Пакет для установки Indeed Bsp Broker на 64-х битных ОС.
- **IndeedAM.AuthProviders.BspBroker-<номер версии>.x86.ru-ru.msi** - Пакет для установки Indeed Bsp Broker на 32-х битных ОС.

1. Выполните установку провайдера Indeed AM Smart Card Provider на сервере Indeed AM и на клиентской машине через запуск соответствующего пакета из дистрибутива.



Информация

Если в инфраструктуре используется несколько серверов Indeed AM, то установку провайдера необходимо выполнить на всех серверах инфраструктуры.

2. После завершения установки может потребоваться перезагрузка системы. Если программа установки предлагает выполнить перезагрузку, подтвердите данное действие.
3. Удаление/Восстановление продукта осуществляется стандартным для поддерживаемых ОС способом, через меню Панель управления.

Настройка параметров аутентификации



Информация

Перед настройкой групповой политики необходимо добавить в список административных шаблонов шаблоны политик Indeed AM. Файлы шаблонов политик входят в состав дистрибутива провайдера и расположены в каталоге Misc.

Таймаут выполнения действия при извлечении смарткарты



Административный файл шаблона политики **IndeedID.Client.admx** входит в состав дистрибутива и расположен в каталоге Misc

Политика раздела Windows Logon определяет продолжительность стандартного и сервисного таймута после извлечения устройства аутентификации.

Политика задает интервал времени в секундах между извлечением смарт-карты и действием, выполняемым согласно политике Windows Интерактивный вход: поведение при извлечении смарткарты (Interactive logon: Smart-card enhanced removal behavior).

Наличие стандартного таймута предотвращает автоматическую блокировку компьютера при случайном извлечении устройства аутентификации.

Наличие сервисного таймута предотвращает автоматическую блокировку компьютера в случаях, когда извлечение используемого устройства аутентификации необходимо (зарегистрировать дополнительный аутентификатор, получить доступ в операционную систему или приложение под другой учетной записью и аутентификатором). Для активации сервисного таймута перед извлечением устройства нажмите и удерживайте комбинацию клавиш [Ctrl]+[L].

Если политика не задана или отключена, то таймаут перед автоматической блокировкой рабочей станции не предоставляется.

Таймаут выполнения действия при извлечении смарт-карты

Таймаут выполнения действия при извлечении смарт-карты

☐ Не задано
 ☒ Включено
 ☐ Отключено

Комментарий:

Требования к версии: Windows XP и более поздние версии

Параметры: Таймаут (сек): 1
 Сервисный таймаут (сек): 1

Справка:

Политика задает интервал времени в секундах между извлечением смарт-карты и действием, выполняемым согласно политике Windows "Интерактивный вход: поведение при извлечении смарт-карты".

Если в момент снятия смарт-карты с устройства удерживать комбинацию клавиш <Ctrl+L>, в качестве таймаута будет использоваться значение поля "Сервисный таймаут".

Использовать дополнительные данные

- Административный файл шаблона политики **IndeedID.Smartcard.Provider.admx** входит в состав дистрибутива и расположен в каталоге Misc

Политика раздела позволяет настроить режим повышенной безопасности с возможностью записи дополнительных данных на устройство и чтения этих данных. Режим использования дополнительных данных предотвращает повторную инициализацию устройства и последующее несанкционированное использование аутентификатора от имени учетной записи настоящего владельца.

Дополнительные данные – последовательность из 64 случайных байт, которая записывается на смарт-карту (usb-ключ) и включается в состав аутентификатора вместе с серийным номером средства аутентификации. Дополнительные данные считываются с устройства и проходят проверку одновременно с серийным номером при аутентификации пользователя. Режим использования дополнительных данных включен, если настройка политики установлена в значение Включен (Enabled) или Не задан (Not Configured). Разрешить работу без дополнительных данных – разрешение работы провайдера без использования дополнительных данных (при включенной политике). Опция может использоваться для работы с устройствами, зарегистрированными в старых версиях Indeed AM Smart Card Provider (без поддержки дополнительных данных).

Ожидание смарт-карты после входа в терминальную сессии

Политика позволяет задать время в секундах, в течение которого будет происходить ожидание смарт-карты после входа в терминальную сессию в случаях некорректной работы PKCS смарт-карты.

The screenshot shows a Windows-style dialog box titled "Ожидание смарт-карты после входа в терминальную сессию". It contains several sections: "Настройка" (Configuration) with radio buttons for "Не задано", "Включено" (selected), and "Отключено", and a "Комментарий" (Comment) text area; "Требования к версии" (Version requirements) with a dropdown menu showing "Windows XP и более поздние версии"; "Параметры" (Parameters) with a label "Ожидание смарт-карты после входа в терминальную сессию в секундах:" and a numeric spinner set to "10"; and "Справка" (Help) with a text area containing the policy description. At the bottom are "ОК", "Отмена", and "Применить" buttons.

Ожидание смарт-карты после входа в терминальную сессию

Ожидание смарт-карты после входа в терминальную сессию

Предыдущий параметр Следующий параметр

☐ Не задано ☒ Включено ☐ Отключено

Комментарий:

Требования к версии: Windows XP и более поздние версии

Параметры: Справка:

Ожидание смарт-карты после входа в терминальную сессию в секундах: 10

Политика позволяет задать время в секундах, в течение которого будет происходить ожидание смарт-карты после входа в терминальную сессию в случаях некорректной работы PKCS смарт-карты.

ОК Отмена Применить

Аутентификация при помощи Indeed AM Smart Card Provider

1. При первом входе в систему или приложение с использованием технологии аутентификации Indeed AM необходимо выбрать способ входа. Для этого нажмите "**Сменить способ входа**" окне "**Вход в Windows**" (окно Аутентификация для Enterprise SSO). Выберите способ входа "**Смарт-карта или USB-ключ**" или "**Смарт-карта или USB-ключ + PIN**".

Вход в Windows



Владислав Фомичёв (INDEED\vladislav.fomichev)

- [Одноразовый пароль](#) (Aladdin eToken PASS)
- [Одноразовый пароль](#) (SMS OTP)
- [Палец](#) (Futronic)
- [Пароль](#)
- [Смарт-карта или USB-ключ](#)
- [Пароль Windows](#)

[RU](#) [Отмена](#)

2. Подключите USB-ключ или смарт-карту к компьютеру. Если используется Indeed AM Smart Card Providerwith PIN, введите PIN-код и нажмите Вход.

Вход в Windows



Владислав Фомичёв (INDEED\vladislav.fomichev)



Выберите смарт-карту или токен

Token: 0641367757

Ok

[→ Сменить способ входа](#)

[RU](#) [Отмена](#)

3. После обработки данных с карты будет выполнена аутентификация. В случае успешного входа по аутентификатору, способ входа "**Смарт-карта или USB-ключ (Смарт-карта или USB-ключ + PIN)**" запоминается, как предпочтительный и будет автоматически предложен пользователю при следующем входе в систему или приложение.

Indeed AM IronLogic Z2USB Provider

ID Провайдера

Z2USB: {CB5109DA-B575-422C-8805-524FE12B02F5}

Z2USB + PIN: {1EDFD6E1-FD66-4A5B-971A-CBA0C611BA9B}

Информация

Файлы для Indeed AM IronLogic Z2USB Provider расположены: ***indeed AM\Indeed AM Providers\Indeed AM IronLogic Z2USB Provider\<Номер версии>***

- **IndeedID.IronLogic.Z2USB.Provider.x64.msi** - Пакет для установки Indeed AM IronLogic Z2USB Provider x64 версии.
- **IndeedID.IronLogic.Z2USB.Provider.msi** - Пакет для установки Indeed AM IronLogic Z2USB Provider x86 версии.

Файлы шаблонов политик расположены: ***indeed AM <номер версии>\Misc\ADMX Templates***.

О компоненте Indeed AM IronLogic Z2USB Provider

Indeed AM IronLogic Z2USB Provider предназначен для совместного использования с продуктами Indeed AM Windows Logon и Indeed AM Enterprise SSO. Подробную информацию о считывателях и метках IronLogic Вы можете получить на сайте компании-производителя.

Информация

Для корректной работы провайдера требуется специализированная версия считывателя IronLogic Z-2 USB (мод. Indeed). Работа других версий Z-2 USB с ПО Indeed ID не гарантирована.

Установка



Примечание

Для работы провайдера требуется установка Indeed AM Bsp Broker на сервере Indeed AM.

Файлы для Indeed Bsp Broker расположены: ***indeed AM <Номер версии>\Indeed Providers\Indeed AM Bsp Broker\<Номер версии>***

- **IndeedEA.AuthProviders.BspBroker-<номер версии>.x64.ru-ru.msi** - Пакет для установки Indeed Bsp Broker на 64-х битных ОС.
- **IndeedEA.AuthProviders.BspBroker-<номер версии>.x86.ru-ru.msi** - Пакет для установки Indeed Bsp Broker на 32-х битных ОС.

1. Выполните установку провайдера IronLogic Z2USB Provider на сервере Indeed AM и на клиентской машине через запуск соответствующего пакета из дистрибутива.



Информация

Если в инфраструктуре используется несколько серверов Indeed AM, то установку провайдера необходимо выполнить на всех серверах инфраструктуры.

2. После завершения установки может потребоваться перезагрузка системы. Если программа установки предлагает выполнить перезагрузку, подтвердите данное действие.
3. Удаление/Восстановление продукта осуществляется стандартным для поддерживаемых ОС способом, через меню Панель управления.

Настройка параметров аутентификации



Информация

Перед настройкой групповой политики необходимо добавить в список административных шаблонов шаблоны политик Indeed AM. Файлы шаблонов политик входят в состав дистрибутива провайдера и расположены в каталоге Misc.



Информация

Настройка политик необходима для повышения уровня безопасности. Однако полноценная работа Indeed AM IronLogic Z2USB Provider возможна и со значениями политик, определенными по умолчанию

Таймаут выполнения действия при извлечении смарт-карты

Политика раздела Windows Logon® определяет продолжительность стандартного и сервисного таймаута после извлечения устройства аутентификации. Политика задает интервал времени в секундах между извлечением смарт-карты и действием, выполняемым согласно политике Windows Интерактивный вход: поведение при извлечении смарт-карты (Interactive logon: Smart-card enhanced removal behavior).

Наличие **стандартного таймаута** позволяет предотвратить автоматическую блокировку компьютера при случайном извлечении устройства аутентификации.

Наличие **сервисного таймаута** позволяет предотвратить автоматическую блокировку компьютера в случаях, когда извлечение используемого устройства аутентификации необходимо (обучение дополнительного аутентификатора, получение доступа в систему от имени другой учетной записи по другому аутентификатору и т. п.). Для активации сервисного таймаута перед извлечением устройства необходимо нажать и удерживать комбинацию клавиш **[Ctrl]+[L]**.

Если политика не задана или отключена, то таймаут перед автоматической блокировкой рабочей станции не предоставляется.

Таймаут выполнения действия при извлечении смарт-карты

Предыдущий параметр Следующий параметр

☐ Не задано Комментарий:

☒ Включено

☐ Отключено

Требования к версии: Windows XP и более поздние версии

Параметры:

Таймаут (сек): 5

Сервисный таймаут (сек): 10

Справка:

Политика задает интервал времени в секундах между извлечением смарт-карты и действием, выполняемым согласно политике Windows "Интерактивный вход: поведение при извлечении смарт-карты".

Если в момент снятия смарт-карты с устройства удерживать комбинацию клавиш <Ctrl+L>, в качестве таймаута будет использоваться значение поля "Сервисный таймаут".

ОК Отмена Применить

Использование ID бесконтактных карт в формате СКУД

Политика определяет формат хранения идентификаторов карт в базе данных Indeed AM. Это дает возможность обеспечить совместимость с форматом хранения идентификаторов СКУД. По умолчанию хранится полная информация о картах: тип, производитель, номер партии и идентификатор карты.

Использовать ID бесконтактных карт в формате SKUD

Использовать ID бесконтактных карт в формате SKUD

Предыдущий параметр

Следующий параметр

☐ Не задано
 ☒ Включено
 ☐ Отключено

Комментарий:

Требования к версии:

Windows XP и более поздние версии

Параметры:

Программное обеспечение SKUD:

Perco/Gate

Справка:

Политика определяет формат хранения идентификаторов карт в базе данных Indeed EA. Это дает возможность обеспечить совместимость с форматом хранения идентификаторов SKUD. По умолчанию хранится полная информация о картах: тип, производитель, номер партии и идентификатор карты.

Пример для карт EM-Marine и SKUD Perco/Gate
 ID карты в формате SKUD: 159/2518.
 ID карты в формате Indeed EA: EM-Marine[3D00]159,2518.
 После включения политики, новые карты будут регистрироваться в базе Indeed EA в формате SKUD Perco/Gate, что даст возможность импортировать идентификаторы карт из базы SKUD в Indeed EA.

OK

Отмена

Применить

Аутентификация при помощи Indeed AM IronLogic Z2USB Provider

1. При первом входе в систему или приложение с использованием технологии аутентификации Indeed AM необходимо выбрать способ входа. Для этого нажмите "**Сменить способ**" входа в окне "**Вход в Windows**". Выберите способ аутентификации "**Карта(Z2 USB Card Reader)**".

Вход в Windows



Владислав Фомичёв (INDEED\vladislav.fomichev)

→ [AirKey](#)

→ [Карта](#) (HID OMNIKEY Smart Card Reader)

→ [Карта](#) (Z2 USB Card Reader)

→ [Карта + PIN](#) (HID OMNIKEY Smart Card Reader)

→ [Многофакторная аутентификация](#)

→ [Однофакторный пароль](#) (Google Authenticator)

RU

[Отмена](#)

2. Подключите считыватель карт Z2 USB и положите на него зарегистрированную карту.

Вход в Windows



Владислав Фомичёв (INDEED\vladislav.fomichev)



Пожалуйста, положите карту на считыватель Z2-USB для аутентификации

→ [Сменить способ входа](#)

RU [Отмена](#)

3. После обработки данных с карты будет выполнена аутентификация. В случае успешного входа по аутентификатору, способ входа "**Карта**" запоминается, как предпочтительный и будет автоматически предложен пользователю при следующем входе в систему или приложение.

Вход в Windows

INDEED 

Владислав Фомичёв (INDEED\vladislav.fomichev)



Идентификационные данные получены. Идет обработка...

→ [Сменить способ входа](#)

RU [Отмена](#)

Indeed AM OMNIKEY Provider

ID Провайдера

OMNIKEY: {4B15AF52-A795-4CA6-B7CD-CDB8ABF2D2C2}

OMNIKEY + PIN: {199B8FA8-FA9D-4ED8-941D-F86A5C681E0C}

Информация

Файлы для Indeed AM OMNIKEY Provider расположены: ***indeed AM <Номер версии>\Indeed AM Providers\Indeed AM OMNIKEY Provider\<Номер версии>***

- **IndeedID.OMNIKEY.Provider.x64.msi** - Пакет для установки Indeed AM OMNIKEY Provider x64 версии.
- **IndeedID.OMNIKEY.Provider.msi** - Пакет для установки Indeed AM OMNIKEY Provider x86 версии.

О компоненте Indeed AM OMNIKEY Provider

Indeed AM OMNIKEY Provider предназначен для совместного использования с продуктами Indeed AM Windows Logon и Indeed AM Enterprise SSO. Компонент обеспечивает работу считывателей смарткарт HID OMNIKEY с модулями программного комплекса Indeed AM Access Management. Подробную информацию о считывателях и картах OMNIKEY Вы можете получить на сайте компании производителя.

На данный момент поддерживаются следующие модели сканеров HID OMNIKEY:

- OMNIKEY 5325
- OMNIKEY 6321
- OMNIKEY 5321 CLi
- OMNIKEY 6321 CLi
- OMNIKEY 5427 СК
- OMNIKEY 5421
- OMNIKEY 5022
- OMNIKEY 5025

Установка



Примечание

Для работы провайдера требуется установка Indeed AM Bsp Broker на сервере Indeed AM.

Файлы для Indeed Bsp Broker расположены: *indeed AM <Номер версии>\Indeed Providers\Indeed AM Bsp Broker\<Номер версии>*

- **IndeedEA.AuthProviders.BspBroker-<номер версии>.x64.ru-ru.msi** - Пакет для установки Indeed Bsp Broker на 64-х битных ОС.
- **IndeedEA.AuthProviders.BspBroker-<номер версии>.x86.ru-ru.msi** - Пакет для установки Indeed Bsp Broker на 32-х битных ОС.

1. Выполните установку провайдера **OMNIKEY Provider** на сервере Indeed AM и на клиентской машине через запуск соответствующего пакета из дистрибутива.



Информация

Если в инфраструктуре используется несколько серверов Indeed AM, то установку провайдера необходимо выполнить на всех серверах инфраструктуры.

2. После завершения установки может потребоваться перезагрузка системы. Если программа установки предлагает выполнить перезагрузку, подтвердите данное действие.
3. Удаление/Восстановление продукта осуществляется стандартным для поддерживаемых ОС способом, через меню Панель управления.

Настройка параметров аутентификации



Информация

Перед настройкой групповой политики необходимо добавить в список административных шаблонов шаблоны политик Indeed AM. Файлы шаблонов политик входят в состав дистрибутива провайдера и расположены в каталоге Misc.

Таймаут выполнения действия при извлечении смарт-карты

Политика раздела Windows Logon® определяет продолжительность стандартного и сервисного таймаута после извлечения устройства аутентификации.

Политика задает интервал времени в секундах между извлечением смарт-карты и действием, выполняемым согласно политике Windows Интерактивный вход: поведение при извлечении смарт-карты (Interactive logon: Smart-card enhanced removal behavior).

Наличие стандартного таймаута позволяет предотвратить автоматическую блокировку компьютера при случайном извлечении устройства аутентификации.

Наличие сервисного таймаута позволяет предотвратить автоматическую блокировку компьютера в случаях, когда извлечение используемого устройства аутентификации необходимо (обучение дополнительного аутентификатора, получение доступа в систему от имени другой учетной записи по другому аутентификатору и т. п.). Для активации сервисного таймаута перед извлечением устройства необходимо нажать и удерживать комбинацию клавиш [Ctrl]+[L].

Если политика не задана или отключена, то таймаут перед автоматической блокировкой рабочей станции не предоставляется.

Таймаут выполнения действия при извлечении смарт-карты

Таймаут выполнения действия при извлечении смарт-карты

☐ Не задано
 ☒ Включено
 ☐ Отключено

Комментарий:

Требования к версии: Windows XP и более поздние версии

Параметры: Таймаут (сек): 5
 Сервисный таймаут (сек): 10

Справка:

Политика задает интервал времени в секундах между извлечением смарт-карты и действием, выполняемым согласно политике Windows "Интерактивный вход: поведение при извлечении смарт-карты".

Если в момент снятия смарт-карты с устройства удерживать комбинацию клавиш <Ctrl+L>, в качестве таймаута будет использоваться значение поля "Сервисный таймаут".

Использовать данные PACS

 Политика применяется к рабочим станциям пользователя

При включении, данная политика позволяет использовать данные PACS вместо идентификатора карты. Не требует настройки.

Аутентификация при помощи Indeed AM OMNIKEY Provider

1. При первом входе в систему или приложение с использованием технологии аутентификации Indeed AM необходимо выбрать способ входа. Для этого нажмите "**Сменить способ входа**" окне "**Вход в Windows**" (окно Аутентификация для Enterprise SSO). Выберите способ входа "**Карта(HID OMNIKEY)**".

Вход в Windows

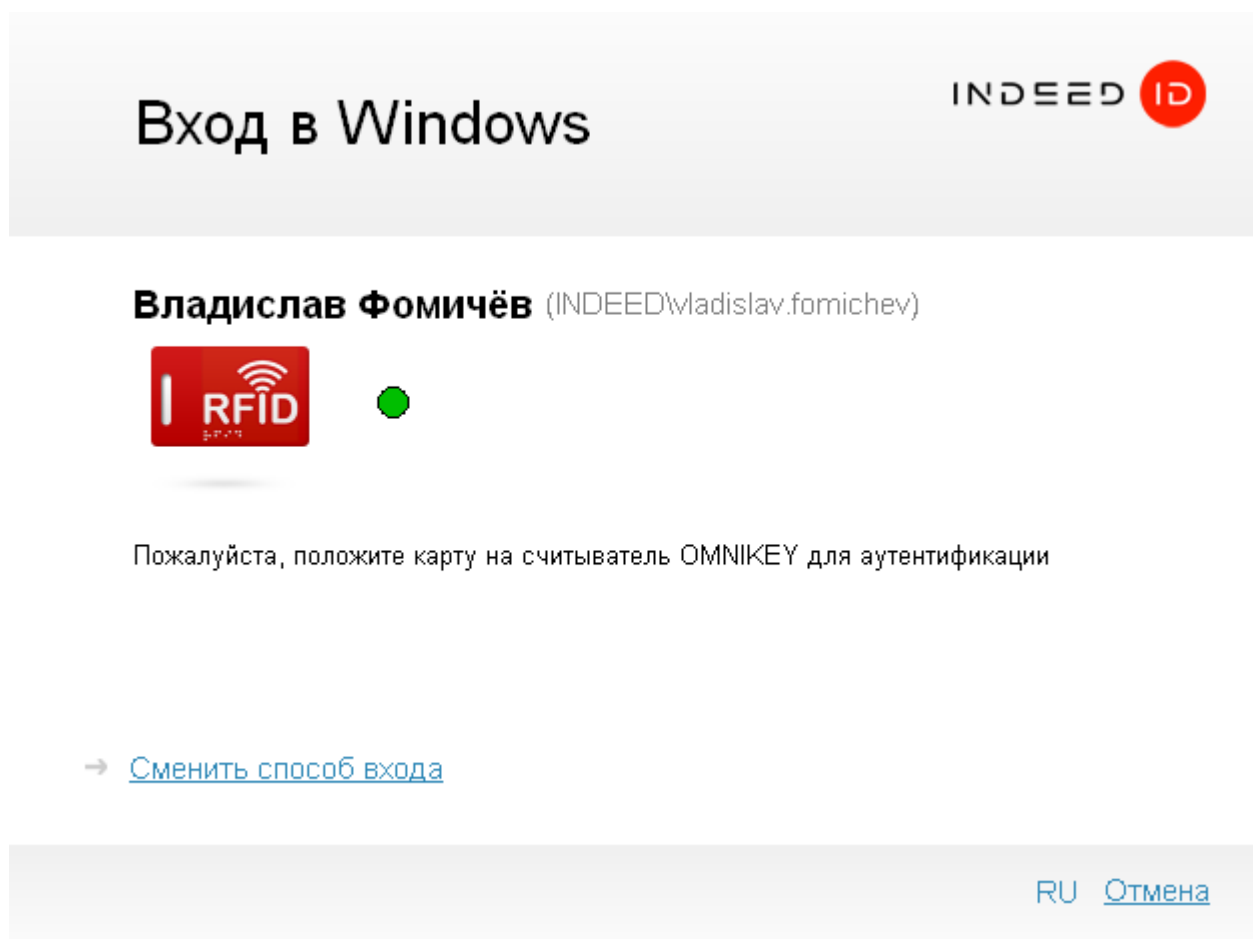


Владислав Фомичёв (INDEED\vladislav.fomichev)

- [AirKey](#)
- [Карта](#) (HID OMNIKEY Smart Card Reader)
- [Карта](#) (Z2 USB Card Reader)
- [Карта + PIN](#) (HID OMNIKEY Smart Card Reader)
- [Многофакторная аутентификация](#)
- [Однофакторный пароль](#) (Google Authenticator)

[RU](#) [Отмена](#)

2. Подключите считыватель карт HID OMNIKEY и положите на него зарегистрированную карту.



3. После обработки данных с карты будет выполнена аутентификация. В случае успешного входа по аутентификатору, способ входа "**Карта**". запоминается, как предпочтительный и будет автоматически предложен пользователю при следующем входе в систему или приложение.

Indeed AM Futronic Provider

ID Провайдера

{A0EF00AD-1EEB-4D48-8BCF-06E19CD5585F}

Информация

Файлы для Indeed AM Futronic Provider расположены: ***indeed AM <Номер версии>\Indeed AM Providers\Indeed AM Futronic Provider\<Номер версии>***

- **IndeedID.Futronic.Provider.x64.msi** - Пакет для установки Indeed AM Futronic Provider x64 версии.
- **IndeedID.Futronic.Provider.msi** - Пакет для установки Indeed AM Futronic Provider x86 версии.

Файлы шаблонов политик расположены: ***indeed AM <номер версии>\Misc\ADMX Templates.***

О компоненте Indeed AM Futronic Provider

Indeed AM Futronic Provider предназначен для совместного использования с продуктами Indeed AM Windows Logon и Indeed AM Enterprise SSO. Компонент Indeed AM Futronic Provider необходим для аутентификации пользователей с применением биометрического сканера Futronic FS80. Получить подробную информацию об устройствах Futronic вы можете на официальном сайте компании Futronic Technologies.

Установка



Примечание

Для работы провайдера требуется установка Indeed AM Bsp Broker на сервере Indeed AM.

Файлы для Indeed Bsp Broker расположены: *indeed AM <Номер версии>\Indeed Providers\Indeed AM Bsp Broker\<Номер версии>*

- **IndeedEA.AuthProviders.BspBroker-<номер версии>.x64.ru-ru.msi** - Пакет для установки Indeed Bsp Broker на 64-х битных ОС.
- **IndeedEA.AuthProviders.BspBroker-<номер версии>.x86.ru-ru.msi** - Пакет для установки Indeed Bsp Broker на 32-х битных ОС.

1. Выполните установку провайдера **Futronic** на сервере Indeed AM и на клиентской машине через запуск соответствующего пакета из дистрибутива.
2. После завершения установки может потребоваться перезагрузка системы. Если программа установки предлагает выполнить перезагрузку, подтвердите данное действие.
3. Удаление/Восстановление продукта осуществляется стандартным для поддерживаемых ОС способом, через меню Панель управления.

Настройка параметров аутентификации



Информация

Перед настройкой групповой политики необходимо добавить в список административных шаблонов шаблоны политик Indeed AM. Файлы шаблонов политик входят в состав дистрибутива провайдера и расположены в каталоге Misc.

Минимально допустимое качество шаблона при обучении



Информация

Политика должна быть определена на рабочих станциях пользователей, на которых установлены клиентские компоненты системы. Если политика не определена, по умолчанию используется значение **3**.

Политика определяет, каким должно быть минимально приемлемое качество шаблона отпечатка пальца при обучении. Качество шаблона задается целым числом от 1 до 10, где 10 соответствует максимально возможному качеству шаблона.

Для достижения максимального качества шаблона при обучении необходимо прикладывать палец к сканеру аккуратно и не меняя положения пальца относительно сканера.

Минимально допустимое качество шаблона при обучении

Минимально допустимое качество шаблона при обучении

Предыдущий параметр Следующий параметр

☐ Не задано Комментарий:

☒ Включено

☐ Отключено

Требования к версии: Windows XP и более поздние версии

Параметры: Справка:

Минимальное качество шаблона

5

Политика определяет, каким должно быть минимально приемлемое качество шаблона отпечатка пальца при обучении. Качество шаблона задается целым числом от 1 до 10, где 10 соответствует максимально возможному качеству шаблона. Для достижения максимального качества шаблона при обучении необходимо прикладывать палец к сканеру аккуратно и не меняя положения пальца относительно сканера.

Политика применяется к рабочим станциям пользователей, на которых происходит обучение аутентификаторов.

Если политика не определена, в качестве значения по умолчанию используется 3

OK Отмена Применить

Максимально допустимый FAR

Информация

Политика должна быть определена на всех серверах Indeed AM. Если политика не определена, значением по умолчанию является 250.

Политика определяет максимально допустимое значение FAR (False Acceptance Rate) при сравнении шаблонов отпечатков. Задается целым числом от 1 до 1000. Значение 1 соответствует самому «мягкому» сравнению, когда вероятность сравнить разные шаблоны и получить положительный результат максимальна. Значение 1000 соответствует самому «жесткому» сравнению, когда такая вероятность минимальна. Если задано слишком большое значение параметра, это может привести к частым ошибкам, связанным с отказом легитимным пользователям.

Настройка индикации работы сканера

Политика задает параметры работы светодиодов сканера. По умолчанию мигание светодиодов сканера отсутствуют в обоих режимах.

Настройки индикации работы сканера

Настройки индикации работы сканера

Предыдущий параметр Следующий параметр

☐ Не задано Комментарий:

☒ Включено

☐ Отключено

Требования к версии: Windows XP и более поздние версии

Параметры:

Справка:

Цвет светодиода в режиме ожидания отпечатка:
Красный

Цвет светодиода в режиме сканирования:
Зеленый

Политика задает параметры работы светодиодов сканера. По умолчанию мигание светодиодов сканера отсутствуют в обоих режимах.

OK Отмена Применить

Аутентификация при помощи Indeed AM Futronic Provider

1. При первом входе в систему или приложение с использованием технологии аутентификации Indeed AM необходимо выбрать способ входа. Для этого нажмите "**Сменить способ**" входа в окне "**Вход в Windows**". Выберите способ аутентификации "**Палец**".

Вход в Windows

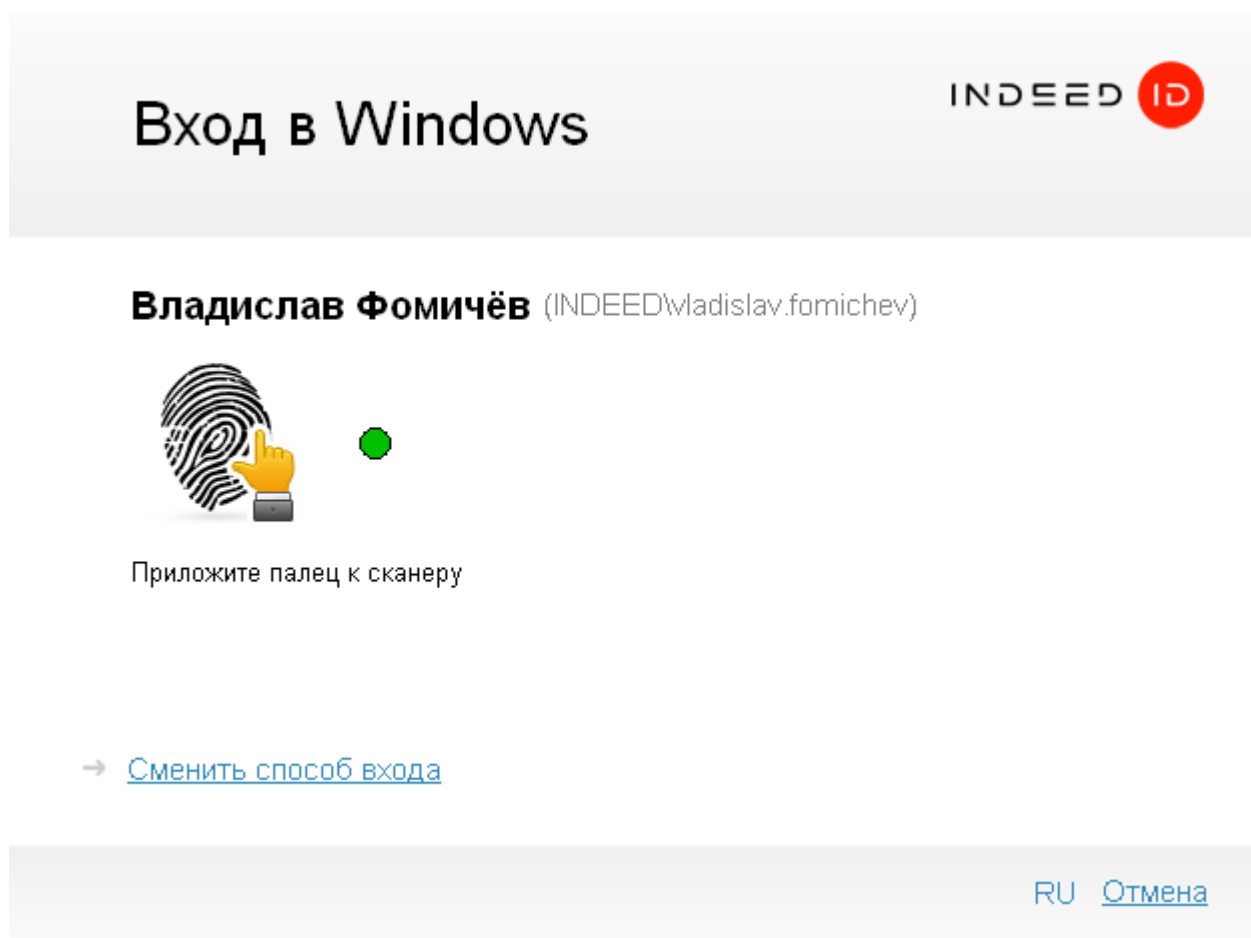


Владислав Фомичёв (INDEED\vladislav.fomichev)

- [Одноразовый пароль](#) (Google Authenticator + PIN)
- [Одноразовый пароль](#) (Aladdin eToken PASS)
- [Одноразовый пароль](#) (SMS OTP)
- [Палец](#)
- [Пароль](#)
- [Пароль Windows](#)

RU [Отмена](#)

2. Подключите биометрический сканер к компьютеру и приложите к нему палец.



3. В случае успешного входа по аутентификатору, способ входа "**Палец**" запоминается, как предпочтительный и будет автоматически предложен пользователю при следующем входе в систему или приложение.

Indeed AM Passcode Provider

ID Провайдера

{F696F05D-5466-42b4-BF52-21BEE1CB9529}

Информация

Файлы для Indeed Passcode Provider расположены: ***indeed AM <Номер версии>\Indeed AM Providers\Indeed AM Passcode Provider\<Номер версии>***

- **IndeedID.Passcode.Provider-<номер версии>.x86.ru-ru.msi** - Пакет для установки Indeed Passcode Provider на x64 и x86 битных ОС.

Файлы шаблонов политик расположены: ***indeed AM <номер версии>\Misc\ADMX Templates.***

О компоненте Indeed AM Passcode Provider

Indeed AM Passcode Provider предназначен для аутентификации пользователей по самостоятельно заданному паролю и совместного использования с продуктами Indeed AM.

Примечание

Для работы провайдера требуется установка Indeed AM Bsp Broker на сервере Indeed AM.

Файлы для Indeed Bsp Broker расположены: ***indeed AM <Номер версии>\Indeed Providers\Indeed AM Bsp Broker\<Номер версии>***

- **IndeedEA.AuthProviders.BspBroker-<номер версии>.x64.ru-ru.msi** - Пакет для установки Indeed Bsp Broker на 64-х битных ОС.
- **IndeedEA.AuthProviders.BspBroker-<номер версии>.x86.ru-ru.msi** - Пакет для установки Indeed Bsp Broker на 32-х битных ОС.

Установка

1. Выполнить установку Indeed AM Passcode Provider через запуск соответствующего пакета из дистрибутива.

Информация

Если в инфраструктуре используется несколько серверов Indeed AM, то установку провайдера необходимо выполнить на всех серверах инфраструктуры.

2. После завершения установки может потребоваться перезагрузка системы. Если программа установки предлагает выполнить перезагрузку, подтвердите это действие.
3. Удаление/Восстановление продукта осуществляется стандартным для поддерживаемых ОС способом через меню Панель управления.

Настройка параметров аутентификации

Информация

Перед настройкой групповой политики необходимо добавить в список административных шаблонов шаблоны политик Indeed AM. Файлы шаблонов политик входят в состав дистрибутива провайдера и расположены в каталоге Misc.

Настройки хранения пароля

Политика включает хранение sha1 хэша пароля Passcode вместо его значения. Если политика не определена или выключена, то пароль будет сохранен в оригинальном виде.

Настройки требований к паролю

Примечание

Для того чтобы изменения в настройках политик вступили в силу, необходимо выполнить обновление групповой политики. Для немедленного обновления групповой политики используйте команду **gpupdate /force**

Политика позволяет 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, для отсутствия ограничения.

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 политика не определена или выключена, то пароль может состоять только из цифр, строчных латинских букв и иметь длину не менее 6 символов.

Indeed AM Email OTP Provider

ID Провайдера

{093F612B-727E-44E7-9C95-095F07CBB94B}

Информация

Файлы для Indeed AM Email OTP Provider расположены: ***indeed AM <Номер версии>\Indeed AM Providers\Indeed AM Email OTP Provider\Server\<Номер версии>***

- **IndeedAM.AuthProviders.AMSMTP-<номер версии>.x64.ru-ru.msi** - Пакет для установки Indeed Email OTP Provider на 64-х битных ОС.
- **IndeedAM.AuthProviders.AMSMTP-<номер версии>.x86.ru-ru.msi** - Пакет для установки Indeed Email OTP Provider на 32-х битных ОС.

Файлы шаблонов политик расположены: ***indeed AM <номер версии>\Misc\ADMX Templates.***

О компоненте Indeed AM Email OTP Provider

Примечание

Для использования **Indeed AM 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 Email-адрес в атрибуте "**mail**", иначе аутентификатор будет не доступен для использования.

Обучение для аутентификатора не требуется.

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 (англ. Simple Mail Transfer Protocol).

Установка

1. Выполнить установку Indeed Email OTP Provider через запуск соответствующего пакета для установки.
2. После завершения установки может потребоваться перезагрузка системы. Если программа установки предлагает выполнить перезагрузку, подтвердите данное действие.
3. Удаление/Восстановление продукта осуществляется стандартным для поддерживаемых ОС способом, через меню Панель управления.

Настройка атрибута с электронной почтой

Для смены атрибута по умолчанию необходимо добавить параметры в конфигурационный файл сервера (C:\inetpub\wwwroot\am\core\Web.config).

- Добавить тег **"userMapRules"** в теге **"adUserCatalogProvider"**.
Добавить тег **"adObjectMapRule"** в теге **"userMapRules"** с параметрами:
 - **"attribute="Email"** - Указывает на изменяемый параметр.
 - **"adAttribute="otherMailbox"** - Указывает с какого атрибута AD брать значение.
- Добавить тег **"objectTypeSettings"**.
- Добавить тег **"objectSetting"** с параметрами **"category="person" class="user"**

Пример

```
<adUserCatalogProvider id="userId" serverName="ind.loc" containerPath="DC=ind,DC=loc"
userName="userAdmin" password="Q1q2E3e4">
  <userMapRules>
    <adObjectMapRule attribute="Email" adAttribute="otherMailbox"/>
  </userMapRules>
  <objectTypeSettings>
    <objectSetting category="person" class="user"></objectSetting>
  </objectTypeSettings>
</adUserCatalogProvider>
```

Настройка параметров аутентификации

Информация

Перед настройкой групповой политики необходимо добавить в список административных шаблонов шаблоны политик Indeed. Файлы шаблонов политик входят в состав дистрибутива провайдера и расположены в каталоге Misc.

Настройки SMTP-сервера

Политика применяется к серверам Indeed AM и позволяет задать следующие настройки для работы с SMTP-сервером:

- **Сервер (DNS-имя, IP-адрес)** – адрес подключения к серверу;
- **Порт** – порт подключения к серверу;
- **Таймаут сервера** – время ожидания ответа от сервера в секундах;
- **Тип соединения** – незащищенное, TLS или SSL;
- **Логин** – имя учетной записи для подключения к серверу;
- **Пароль** – пароль учетной записи для подключения к серверу;
- **Одноразовый пароль в теме письма** – если опция включена, то одноразовый пароль будет подставлен в тему письма, в противном случае в сам текст письма.
- **Текст письма** – имя и почта отправителя, тема и текст письма.

Информация

В тексте письма необходимо указать место вставки одноразового пароля с помощью тега .

Например:

Ваш одноразовый пароль: **<otp>** .

Если выставлена опция **Одноразовый пароль в теме письма**, то аналогичное место подстановки одноразового пароля необходимо указать в теме письма.

Не задан (Not Configured) или Отключен (Disabled)

Если политика не определена или отключена, то Email OTP Provider не будет использоваться для аутентификации пользователя.

Включен (Enabled)

При включении политики Email OTP Provider будет работать используя определенные в политике параметры.

Настройки генерации одноразового пароля

Политика применяется к серверам Indeed AM и позволяет задать длину и вхождение групп символов при генерации одноразового пароля.

Не задан (Not Configured) или Отключен (Disabled)

Если политика не задана или отключена, то пароль будет состоять из цифр и иметь длину 6 символов.

Включен (Enabled)

Одноразовый пароль будет генерироваться согласно заданным в политике правилам. Если политика включена, но не определена ни одна группа символов, то пароль будет состоять только из цифр (длина пароля по умолчанию – 6 символов).

Настройки генерации одноразового пароля

Предыдущий параметр Следующий параметр

☐ Не задано
☒ Включено
☐ Отключено

Комментарий:

Требования к версии: Windows XP и более поздние версии

Параметры:

Длина одноразового пароля: 6

Вхождение групп символов:

☒ Цифры
☐ Строчные латинские буквы
☒ Прописные латинские буквы
☐ Специальные символы

Справка:

Данная политика позволяет задать длину и вхождение групп символов при генерации одноразового пароля.

Группы символов:

Цифры - "0-9";
 Строчные латинские буквы - "a-z";
 Прописные латинские буквы - "A-Z";
 Специальные символы - ".<>/?[]+=+~_!@#%&*'"

Если политика не определена или выключена, то пароль будет состоять из цифр и иметь длину 6 символов.

OK Отмена Применить

Настройка защиты от спама



Описание работы

Осуществляется оценка процента успешных входов относительно всех отправленных сообщений за указанный интервал времени (оценка осуществляется только если кол-во отправленных сообщений превышает "Окно оценки").

При обнаружении атаки блокируется дальнейшая отправка сообщений, при попытке входа возникает ошибка: Potential spam attack detected.

Отправка возобновится спустя некоторое время когда будет превышен необходимый порог успешных входов за указанный интервал времени. Максимальное время блокировки равно временному интервалу оценки.

Чтобы настроить защиту от спама:

1. Откройте **редактор реестра**;
2. Создайте раздел **Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-Id\BSPs\SMTP\SpamProtection**;
3. Создайте необходимые параметры:
 - a. **SpamProtectionEnabled**: Флаг включения защиты от спама (DWORD). Значение по умолчанию: 0
 - b. **TimeSpanSec**: Интервал времени (сек), по которому осуществляются расчеты (DWORD). Значение по умолчанию: 600
 - c. **EvaluationWindow**: Окно оценки (DWORD). Значение по умолчанию: 10
 - d. **MinSuccessfulLogonPercent**: Минимальный процент успешных входов относительно всех отправленных сообщений (DWORD). Значение по умолчанию: 20



События лог-сервера

2090: Обнаружена потенциальная спам-атака. Отправка сообщений приостановлена.

1118: Отправка сообщений пользователям возобновлена.

Indeed AM Hardware TOTP Provider

ID Провайдера

{CEB3FEAF-86ED-4A5A-BD3F-6A7B6E60CA05}

Важно

Не поддерживается в [Indeed AM Windows Logon](#) и в [Indeed AM ESSO Agent](#)

Информация

Файлы для Indeed AM Hardware TOTP Provider расположены: *indeed AM <Номер версии>\Indeed AM Providers\Indeed AM Hardware TOTP Provider\<Номер версии>*

- *IndeedAM.AuthProviders.HardwareTOTP-<номер версии>.x64.ru-ru.msi* - Пакет для установки Indeed AM Hardware TOTP Provider на 64-х битные ОС.
- *IndeedAM.AuthProviders.HardwareTOTP-<номер версии>.x86.ru-ru.msi* - Пакет для установки Indeed AM Hardware TOTP Provider на 32-х битные ОС.

Файлы шаблонов политик расположены: *indeed AM <номер версии>\Misc\ADMX Templates*.

О компоненте Indeed AM Hardware TOTP Provider

Информация

Подробную информацию об устройстве **eToken PASS** Вы можете получить на официальном сайте компании Aladdin: <http://www.aladdin-rd.ru>.

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. В **eToken PASS** реализован алгоритм генерации одноразовых паролей (One-Time Password – OTP). Главное отличие TOTP от HOTP это генерация пароля на основе времени, то есть время является параметром. При этом обычно используется не точное указание времени, а текущий интервал с установленными заранее границами (например, 30 секунд).

Установка провайдера.

1. Выполнить установку **Hardware TOTP Provider** через запуск соответствующего пакета для установки.
2. После завершения установки может потребоваться перезагрузка системы. Если программа установки предлагает выполнить перезагрузку, подтвердите данное действие.
3. Удаление/Восстановление продукта осуществляется стандартным для поддерживаемых ОС способом, через меню Панель управления.

Добавления устройства



Информация

Одно устройство может быть зарегистрировано только для одного пользователя

Для добавления устройства необходимо выполнить следующие действия:

1. Открыть консоль управления **Management Console**.
2. Перейти на вкладку "Устройства".
3. Нажать "**Добавить устройство**".

Поиск устройства

Провайдер аутентификации

Серийный номер

Hardware TOTP

AP578201

Комментарий

Добавить/удалить устройство ▾

Из файла

Вручную

Тип устройства

Файл устройств

eToken PASS (TOTP)

Выбрать файл

Добавить

Удалить



Примечание

Вы можете добавить устройство выбрав файл с параметрами устройства (Вкладка "Из файла"), либо указать параметры вручную (Вкладка "Вручную").

а. Добавление из файла.

- На вкладке **"Из файла"** нажать **"Выбрать файл"**.
- Выбрать файл формата XML с параметрами устройства.

Пример конфигурации устройства

```
<?xml version="1.0" encoding="utf-8" ?>
<Tokens>
  <Token serial="AP578201">
    <CaseModel>5</CaseModel>
    <Model>517</Model>
    <ProductionDate>03/25/2016</ProductionDate>
    <ProductName>eTPass 6.20</ProductName>
    <Applications>
      <Application ConnectorID="{a61c4073-2fc8-4170-99d1-9f5b70a2cec6}">
        <Seed>964e94a69eaf67a103ffb81d2f8c5229c1d5956e2cff7c44d427b5e1d4b1c05a</Seed>
        <MovingFactor>1</MovingFactor>
      </Application>
    </Applications>
  </Token>
</Tokens>
```

- Нажать **"Добавить"**

[Добавить/удалить устройство](#) ▾

Из файла Вручную

Тип устройства: eToken PASS (TOTP)

Файл устройства: eToken+PASS.XML

Выбрать файл

Добавить Удалить

б. Добавление вручную

- Выбрать вкладку **"Вручную"**.
- В поле **"Серийный номер"** укажите серийный номер устройства.
- В поле **"Секретный ключ"** укажите секретный ключ сгенерированный устройством.
- Поле **"Комментарий"** не обязательный параметр.
- Нажмите **"Добавить"**.

Из файла Вручную

Модель: eToken PASS (TOTP): eTPass 6.20

Серийный номер: AP578201

Секретный ключ: 964e94a69eaf67a103ffb81d2f8c5229c1d5956e2cff7c44d427b5e1d4b1c05a

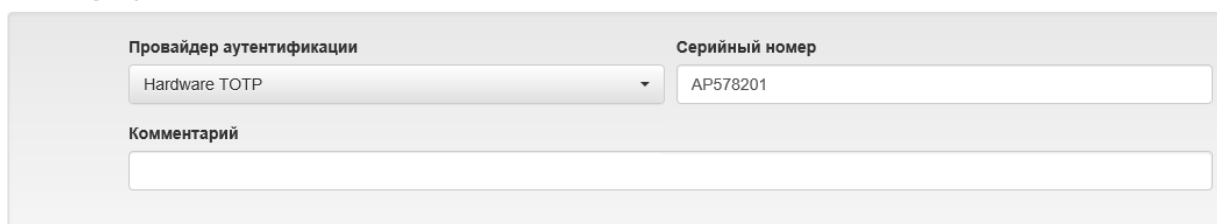
Комментарий: eToken Pass TOTP

Добавить

Редактирование устройства.

Для удаления устройства необходимо выполнить следующие действия:

1. Открыть консоль управления **Management Console**.
2. Перейти на вкладку "**Устройства**".
3. В поле "**Провайдер аутентификации**" выбрать "**Hardware OTP**", в поле "Серийный номер", если известно, укажите серийный номер необходимого устройства и выполните поиск.
Поиск устройства

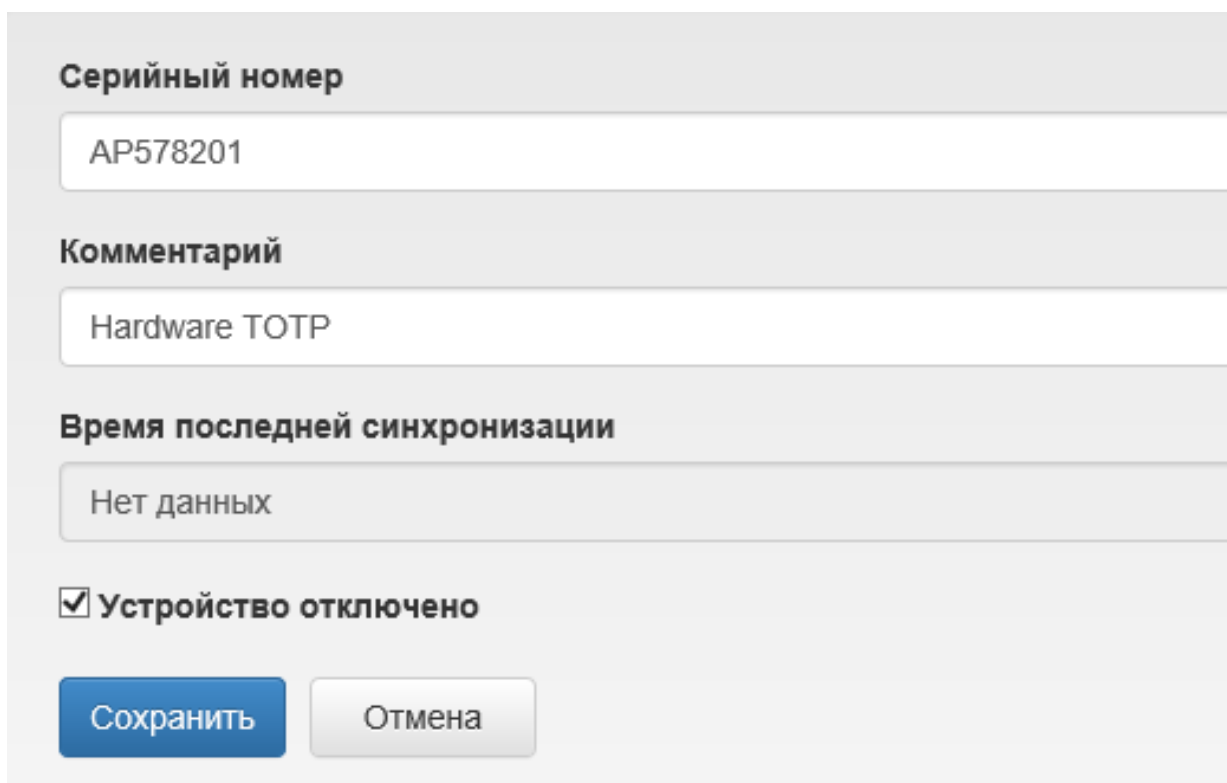


4. Выберите найденное устройство и нажмите на значок редактирования.

Устройства					Удалить
☒	Серийный номер	Провайдер	Модель	Комментарий	Пользователь
☒	AP578201	Hardware TOTP	eTPass 6.20		


Редактировать

5. В окне редактирования можно изменить серийный номер устройства, комментарий или отключить устройство. После внесения изменений нажать "**Сохранить**".

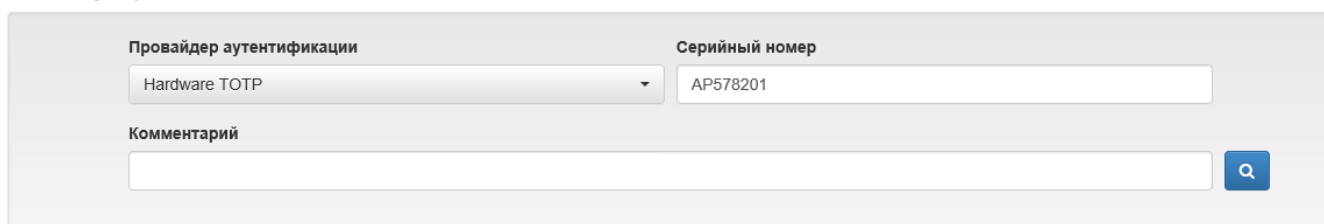


Удаление устройства.

Для удаления устройства необходимо выполнить следующие действия:

1. Открыть консоль управления **Management Console**.
2. Перейти на вкладку "**Устройства**".
3. В поле "**Провайдер аутентификации**" выбрать "**Hardware OTP**", в поле "Серийный номер", если известно, укажите серийный номер необходимого устройства и выполните поиск.

Поиск устройства



Провайдер аутентификации: Hardware TOTP

Серийный номер: AP578201

Комментарий:

Поиск

4. Выберите найденное устройство и нажмите "**Удалить устройство**".

Устройства

[✕ Удалить устройства](#)

☒	Серийный номер	Провайдер	Модель	Комментарий	Пользователь
☒	AP578201	Hardware TOTP	eTPass 6.20		

5. В сплывающем окне подтвердите удаление.

Удаление устройств



Вы уверены, что хотите удалить выделенные устройства?

Внимание: вместе с устройствами будут удалены все зарегистрированные аутентификаторы

Отмена

Удалить

Синхронизация устройства.

Для синхронизации устройства необходимо выполнить следующие действия:

1. Открыть консоль управления **Management Console**.
2. Открыть карточку пользователя с зарегистрированным устройством.
3. Нажать "**Настройки**" для устройства и выбрать "**Синхронизировать**".

Дата регистрации	Комментарий	Серийный номер
29.03.2019 14:48:42	TOTP	AP578201

4. В поле "**Одноразовый пароль 1**" и "**Одноразовый пароль 2**" укажите пароли с устройства и нажмите "**Синхронизировать**".

INDEED ID

Синхронизация TOTP устройства

Для синхронизации устройства с системой необходимо ввести его серийный номер и два последовательно сгенерированных на нём одноразовых пароля в соответствующие поля ввода ниже

AP578201

623920

623966

Синхронизировать

Отмена

5. После успешной синхронизации вы будете возвращены на страницу пользователя.

Политика "Настройки синхронизации и проверки одноразового пароля"

Задаёт интервал значений счетчика при синхронизации и при проверке одноразового пароля.

Значение по умолчанию:

- "Окно синхронизации" - 100
- "Окно проверки одноразового пароля" - 1

Настройки синхронизации и проверки одноразового пароля

Предыдущий параметр Следующий параметр

☐ Не задано ☒ Включено ☐ Отключено

Комментарий:

Требования к версии: Windows XP и более поздние версии

Параметры:

Окно синхронизации: 100

Окно проверки одноразового пароля: 1

Справка:

Задаёт интервал значений счетчика при синхронизации и при проверке одноразового пароля.

- Окно синхронизации - количество перебираемых OTP при синхронизации;
- Окно проверки - количество проверяемых OTP при аутентификации.

Например, если окно проверки равно '1', то валидными считаем как одноразовый пароль, соответствующий текущему времени на сервере, так и одноразовые пароли следующие за ним и после него.

ОК Отмена Применить

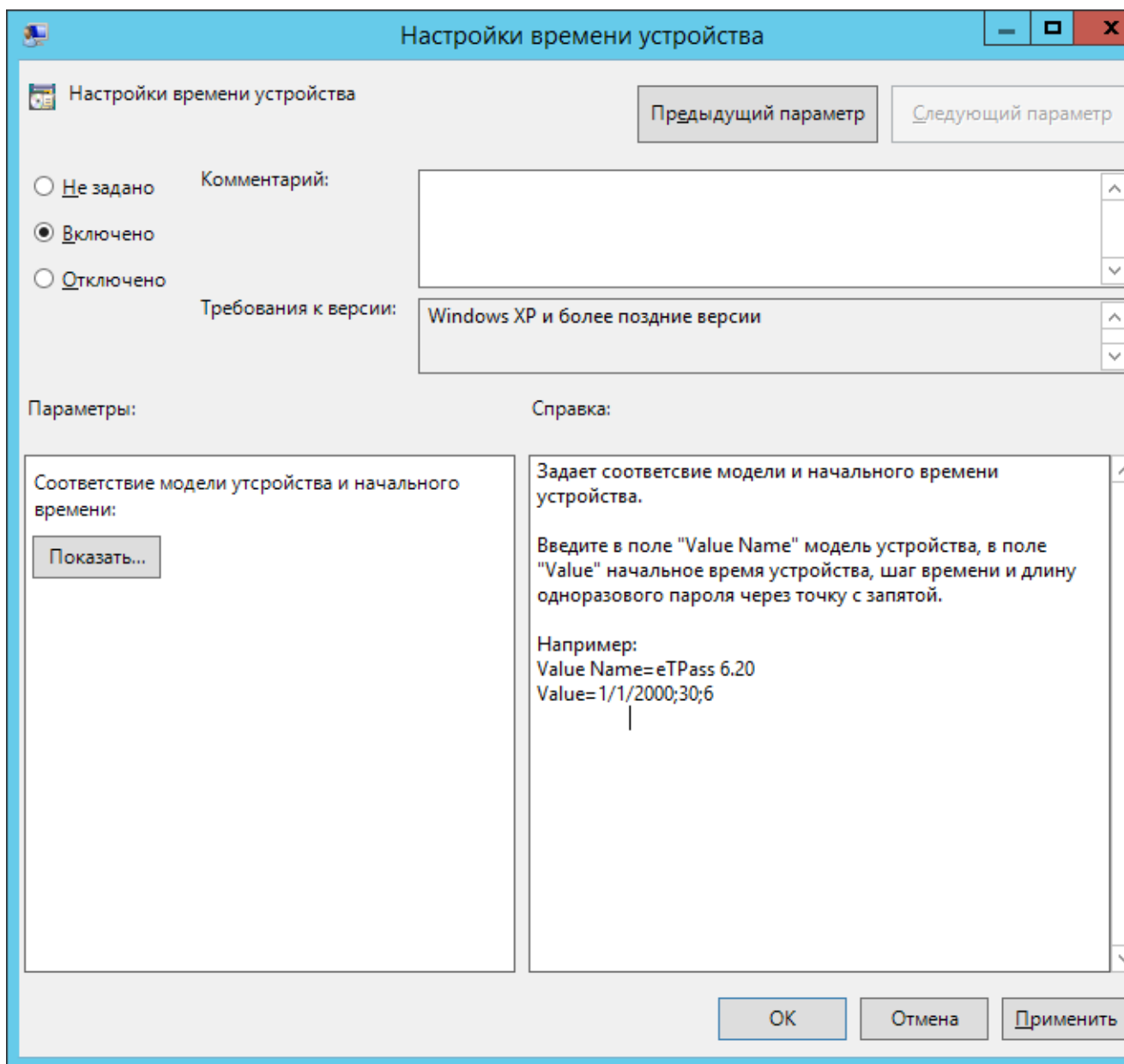
Политика "Настройка времени вручную"

Задаёт соответствие модели и начального времени устройства.

Информация

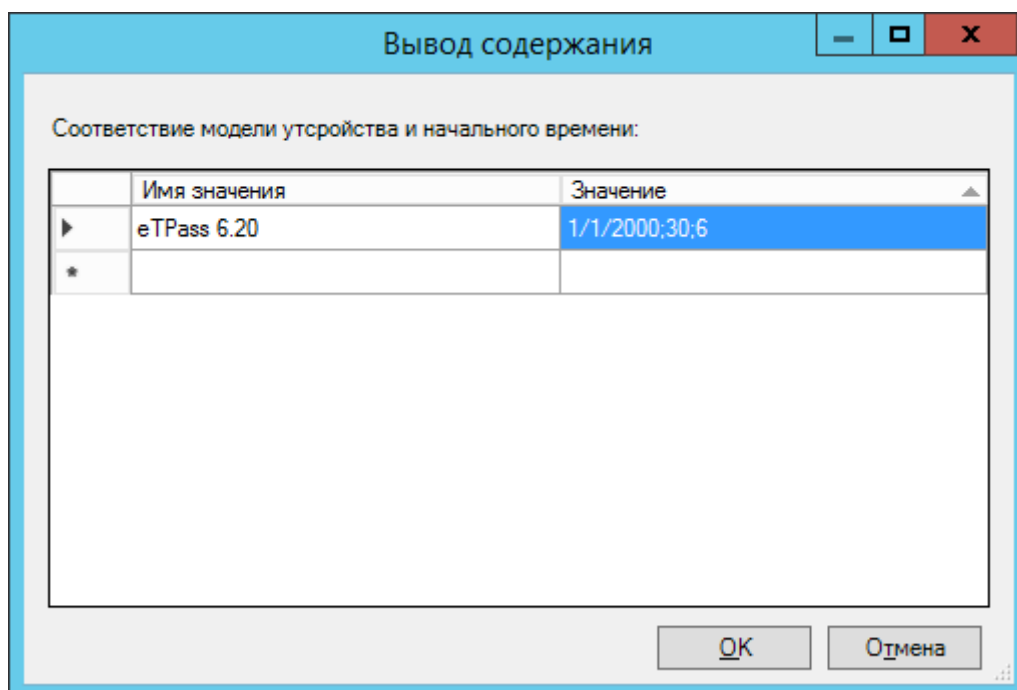
Для модели "eTPass 6.20" по умолчанию(если политика не задана) считаем шаг времени: 30 сек., начальное время: 1/1/2000.

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*



Indeed AM HOTP Provider

ID Провайдера

{631F1011-2DEE-47C5-95D8-75B9CAED7DC7}

Информация

Файлы для Indeed AM HOTP Provider расположены: ***indeed AM <Номер версии>\Indeed AM Providers\Indeed AM HOTP Provider\Server\<Номер версии>***

- **IndeedAM.AuthProviders.HOTP-<номер версии>.x64.ru-ru.msi** - Пакет для установки Indeed AM HOTP Provider на 64-х битных ОС.
- **IndeedAM.AuthProviders.HOTP-<номер версии>.x86.ru-ru.msi** - Пакет для установки Indeed AM HOTP Provider на 32-х битных ОС.

Файлы шаблонов политик расположены: ***indeed AM <номер версии>\Misc\ADMX Templates.***

О компоненте Indeed AM HOTP Provider

Информация

Подробную информацию об устройстве **eToken PASS** Вы можете получить на официальном сайте компании Aladdin: **<http://www.aladdin-rd.ru>**.

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. В **eToken PASS** реализован алгоритм генерации одноразовых паролей (One-Time Password – OTP). Этот алгоритм основан на алгоритме **HMAC** и хэшфункции **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.

Установка провайдера

1. Выполнить установку **Indeed HOTP Provider** через запуск соответствующего пакета для установки.
2. После завершения установки может потребоваться перезагрузка системы. Если программа установки предлагает выполнить перезагрузку, подтвердите данное действие.
3. Удаление/Восстановление продукта осуществляется стандартным для поддерживаемых ОС способом, через меню Панель управления.

Добавления устройства

Информация

Одно устройство может быть зарегистрировано только для одного пользователя

Для добавления устройства необходимо выполнить следующие действия:

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**").

Устройства

 Добавить  Добавить из файла  Удалить  Удалить из файла  Заблокировать  Разбл

Модель	Серийный номер	Комментарий	Провайдер аутентификации
Не выбрана ▾			Не выбран ▾
Поиск		Сбросить	

Нет информации о зарегистрированных устройствах

а. Добавление из файла.

- Нажмите **"Добавить из файла"**.
- Выберите файл формата XML с параметрами устройства.

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 OTP v1.0</ProductName>
    <Applications>
      <Application ConnectorID="{a61c4073-2fc8-4170-99d1-9f5b70a2cec6}">
        <Seed>884f20ce4b2c406e0b6199338990bb6cc3fabac403eaa7f8<
/Seed>
        <MovingFactor>1</MovingFactor>
      </Application>
    </Applications>
  </Token>
</Tokens>
```

- Нажмите **"Добавить"**.

Устройство

+ Добавить

Добавить устройство

Тип устройства

eToken PASS (HOTP)

Файл устройств

etoken.xml

Выбрать файл

Отмена

Добавить

в. Добавление вручную

- Нажмите **"Добавить"**.
- В поле **"Серийный номер"** укажите серийный номер устройства.
- В поле **"Секретный ключ"** укажите seed устройства.
- Поле **"Комментарий"** не обязательный параметр.
- Нажмите **"Добавить"**.

Добавить устройство

Модель

eToken PASS (HOTP): Aladdin OTPD v1.0

Серийный номер

000200071927

Секретный ключ

884f20ce4b2c406e0b6199338990bb6cc3fabac403eaa7f8

Комментарий

eToken 000200071927

Отл

Редактирование устройства.

Для редактирования устройства необходимо выполнить следующие действия:

1. Откройте консоль управления **Management Console**.
2. Перейдите на вкладку "Устройства".
3. Нажмите на серийный номер устройства.

Информация

При необходимости можно выполнить поиск используя фильтры в верхней части страницы.

Устройства

 Добавить  Добавить из файла  Удалить  Удалить из файла  Заблокировать  Разблокировать

Модель

Серийный номер

Комментарий

Провайдер аутентификации

Не выбрана

Не выбран

Поиск

Сбросить

МОДЕЛЬ	СЕРИЙНЫЙ НОМЕР	ПРОВАЙДЕР АУТЕНТИФИКАЦИИ	ПОЛЬЗОВАТЕЛЬ	КОММЕНТАРИЙ
☐ Aladdin OTP v1.0	<u>000200071927</u>	Hardware HOTP		eToken 000200071927

4. В окне редактирования можно изменить комментарий, заблокировать устройство или синхронизировать.
5. После внесения изменений нажать "Сохранить".

Aladdin OTP v1.0, 000200071927

 Сохранить  Отмена  Синхронизировать OTP  Заблокировать  Разблокировать  Удалить

Модель

Серийный номер

Провайдер аутентификации

Aladdin OTP v1.0

000200071927

Hardware HOTP

Комментарий

Статус

eToken 000200071927

Активно

Удаление устройства.

Для удаления устройства необходимо выполнить следующие действия:

1. Откройте консоль управления **Management Console**.
2. Перейдите на вкладку **"Устройства"**.
3. Выберите необходимое устройство и нажмите **"Удалить"**.



Информация

При необходимости можно выполнить поиск используя фильтры в верхней части страницы.

Устройства

+ Добавить
↑ Добавить из файла
 Удалить
↑ Удалить из файла
🔒 Заблокировать
🔓 Разблокировать

Модель
 Не выбрана

Серийный номер

Комментарий

Провайдер аутентификации
 Не выбран

Поиск
Сбросить

МОДЕЛЬ	СЕРИЙНЫЙ НОМЕР	ПРОВАЙДЕР АУТЕНТИФИКАЦИИ	ПОЛЬЗОВАТЕЛЬ	КОММЕНТАРИЙ
☒ Aladdin OTP v1.0	000200071927	Hardware HOTP		eToken 000:

- а. Для удаления устройства по информации из файла нажмите **"Удалить из файла"**.
- б. Выберите файл конфигурации устройства.
- в. Нажмите **"Удалить"**.

Удалить устройство

Тип устройства

eToken PASS (HOTP)

Файл устройств

etoken.xml

Выбрать

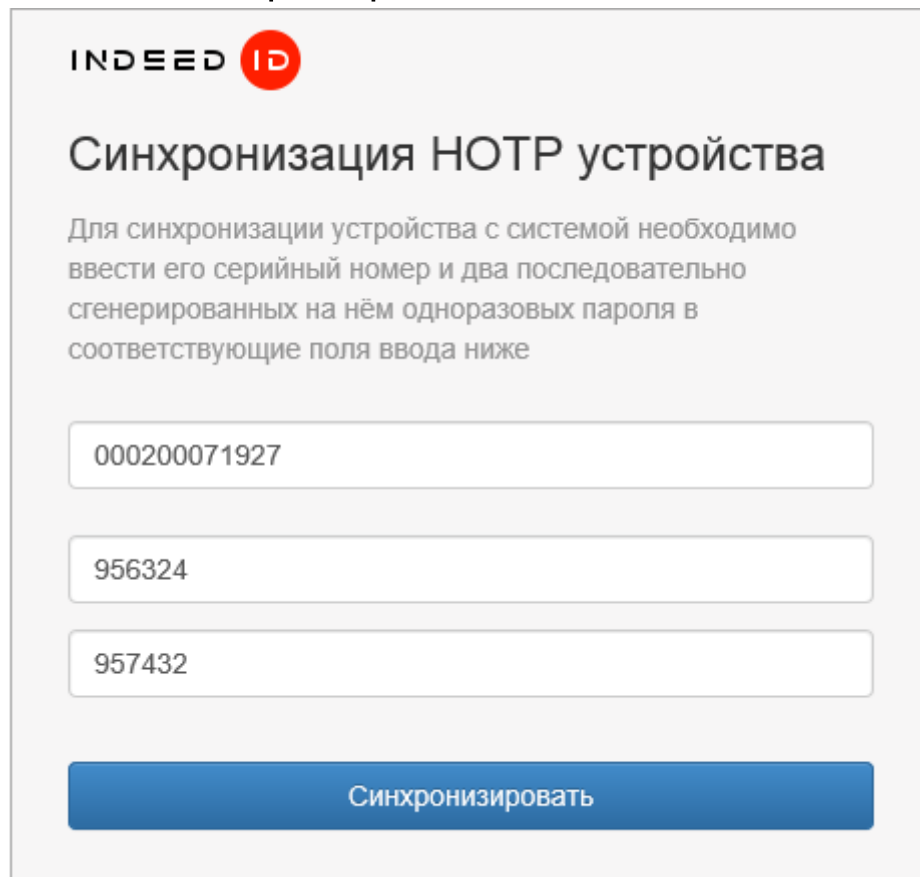
Отмена

Уд

Синхронизация устройства.

Для синхронизации устройства необходимо выполнить следующие действия:

1. Откройте консоль управления **Management Console**.
2. Перейдите на вкладку "**Устройства**".
3. Нажмите на 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

Политика "Настройки синхронизации и проверки одноразового пароля"

Задаёт интервал значений счетчика при синхронизации и при проверке одноразового пароля.

Значение по умолчанию:

- "Окно синхронизации" - 2000
- "Окно проверки одноразового пароля" - 5

Настройки синхронизации и проверки одноразового пароля

Настройки синхронизации и проверки одноразового пароля

Предыдущий параметр

Следующий параметр

☐ Не задано

☒ Включено

☐ Отключено

Комментарий:

Требования к версии:

Windows XP и более поздние версии

Параметры:

Справка:

Окно синхронизации: 1000

Окно проверки одноразового пароля: 50

Задаёт интервал значений счетчика при синхронизации и при проверке одноразового пароля.

OK

Отмена

Применить

Indeed AM Storage SMS OTP Provider

ID Провайдера

{3F2C1156-B5AF-4643-BFCB-9816012F3F34}

Информация

Файлы для Indeed AM Storage SMS Provider расположены: ***indeed AM <Номер версии>\Indeed AM Providers\Indeed AM Storage SMS OTP Provider***

- **Server\<Номер версии>\IndeedAM.AuthProviders.StorageSmsOTP-<номер версии>.x64.ru-ru.msi** - Пакет для установки Indeed Storage SMS OTP Provider на 64-х битных ОС.
- **Server\<Номер версии>\IndeedAM.AuthProviders.StorageSmsOTP-<номер версии>.x86.ru-ru.msi** - Пакет для установки Indeed Storage SMS OTP Provider на 32-х битных ОС.
- **Client\<Номер версии>\IndeedID.SMSOTP.Provider.msi** - Пакет для установки Indeed Storage SMS OTP Provider на клиентские машины.

Файлы шаблонов политик расположены: ***indeed AM <номер версии>\Misc\ADMX Templates.***

О компоненте Indeed AM Storage SMS Provider

Информация

Данный провайдер поддерживается только в сценариях с компонентами Indeed AM Radius Extension и Indeed AM ADFS Extension.

При использовании в качестве хранилища данных системы Indeed AM базу данных SQL, вы можете использовать провайдер Indeed AM Storage SMS OTP Provider, который предоставляет возможность хранения, получения и обновления телефонных номеров пользователей системы indeed AM в базе данных SQL. Номера телефонов хранятся в зашифрованном виде.



Примечание

Для использования Indeed AM Storage SMS OTP Provider необходимо наличие смс шлюза. Данный шлюз должен быть доступен с каждого сервера Indeed AM, на котором предполагается установка Indeed AM Storage SMS OTP Provider.

Провайдер Indeed AM Storage SMS OTP Provider позволяет хранить и использовать номера телефонов пользователей в базе данных SQL. Номера телефонов хранятся в зашифрованном виде.

Для использования провайдера необходима его регистрация.

Установка

1. Выполнить установку Storage SMS OTP Provider через запуск соответствующего пакета.



Примечание

При использовании провайдера в клиентских сценариях с Indeed AM Windowsl Logon и ESSO Agent, необходимо выполнить установку провайдера из папки **Client** на клиентские машины.

2. После завершения установки может потребоваться перезагрузка системы. Если программа установки предлагает выполнить перезагрузку, подтвердите данное действие.
3. Удаление/Восстановление продукта осуществляется стандартным для поддерживаемых ОС способом, через меню Панель управления.

Регистрация провайдера

Регистрация провайдера рекомендуется осуществляется через облегченную версию API компонента Indeed AM EAPhoneServer, предназначенную специально для работы с Storage SMS OTP Provider, также возможно использование основного API системы Indeed.

Настройка провайдера

Информация

Перед настройкой групповой политики необходимо добавить в список административных шаблонов шаблоны политик Indeed AM. Файлы шаблонов политик входят в состав дистрибутива провайдера и расположены в каталоге Misc.

Сервис отправки SMS

Политика применяется к серверам Indeed AM и определяет следующие настройки для сервера отправки SMS:

- **Use tls** - Использование шифрования.
- **URL(IP-адрес)** - Адрес подключения к серверу.
- **Порт** - Порт подключения к серверу.
- **SystemId (Логин)** - Имя учетной записи для подключения к серверу.
- **Пароль** - Пароль учетной записи для подключения к серверу.

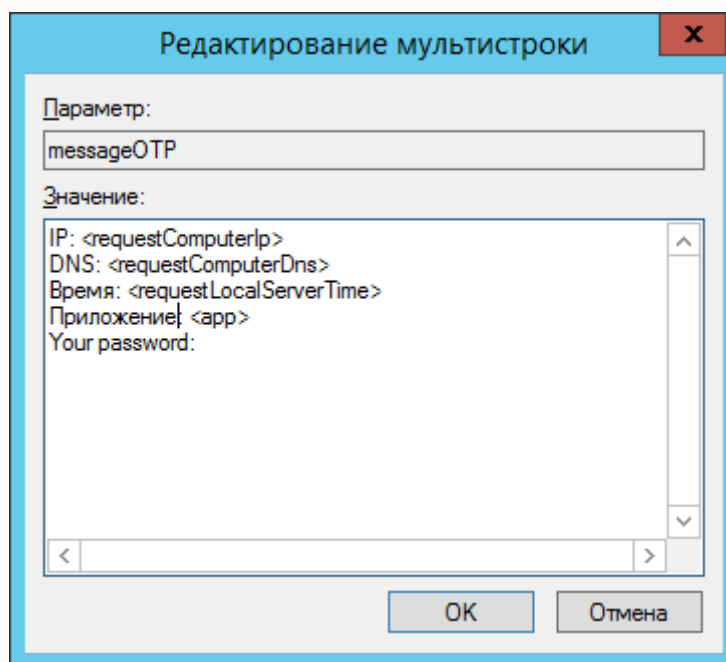
- **SystemType** - Поле PDU операции BIND_TRANSCEIVER протокола SMPP.
- **Отправитель** - Имя отправителя, которое будет отображаться при получении SMS.

- **Дополнительный текст перед OTP** - Произвольный текст сообщения, предшествующий одноразовому паролю. По умолчанию отправляется только OTP, для дополнительной настройки параметров используйте следующие параметры:
 - **<app>** - Имя приложения, отправившего запрос на авторизацию.
 - **<requestLocalServerTime>** - Локальное серверное время получения запроса.
 - **<requestComputerDns>** - DNS имя компьютера отправившего запрос.
 - **<requestComputerIp>** - IP адрес компьютера отправившего запрос.

Информация

Отображение OTP кода не настраивается, OTP всегда отображается в конце сообщения.

Для переноса строк отправляемого сообщения необходимо внести изменения в реестр **HKLM/SOFTWARE/Policies/Indeed-ID/BSPs/SMSOTP**. Измените значение для старого параметра **"messageOTP"** с типом **"REG_SZ"**, на **"messageOTP"** с типом **"REG_MULTI_SZ"**.



- **Время ожидания статуса SMS** - Время ожидания получения статуса отправленного SMS с сервера.
- **PDU со статусом SMS** - PDU, в котором сервер присылает статус отправленного сообщения.
- **source_addr_ton** - Тип Номера (Type of Number) для исходного адреса.

- **source_addr_npi** - Индикатор Схемы Присвоения Номеров (Numbering Plan Indicator) для исходного адреса.
- **dest_addr_ton** - Тип Номера (Type of Number) для адресата.
- **dest_addr_npi** - Индикатор Схемы Присвоения Номеров (Numbering Plan Indicator) для адресата.
- **esm_class** - Указывает Message Mode & Message Type.
- **registered_delivery** - Индикатор для того, чтобы обозначить, что запрашивается расписка о получении SMSC или подтверждение SME.

- **data_coding** - Определяет схему кодировки пользовательских данных короткого сообщения.

Сервис отправки SMS

Предыдущий параметр

Следующий параметр

☐ Не задано
 ☒ Включено
 ☐ Отключено

Комментарий:

Требования к версии:

Windows XP и более поздние версии

Параметры:

☒ Use tls

URL(IP-адрес):

Порт:

SystemId(Логин):

Пароль:

SystemType:

Отправитель:

Дополнительный текст перед OTP:

Время ожидания статуса SMS:

PDU со статусом SMS:

Подключаться как:

Параметры SMPP:

source_addr_ton

source_addr_npi

dest_addr_ton

dest_addr_npi

esm_class

registered_delivery

data_coding

Настройка формата сообщения

Политика позволяет задать настройки формата отображения даты. Примеры форматов можно посмотреть по ссылке <https://docs.microsoft.com/ru-ru/dotnet/standard/base-types/standard-date-and-time-format-strings>

Включен (Enabled)

Дата будет отображаться согласно заданному в политике формату.

☐ Не задано	Комментарий:	
☒ Включено		
☐ Отключено	Требования к версии:	Windows XP и более поздние версии
Параметры:		
Формат даты:	d	

Настройки генерации одноразового пароля

Политика применяется к серверам Indeed AM и позволяет задать длину и вхождение групп символов при генерации одноразового пароля.

Не задан (Not Configured) или Отключен (Disabled)

Если политика не задана или отключена, то пароль будет состоять из цифр и иметь длину 4 символов.

Включен (Enabled)

Одноразовый пароль будет генерироваться согласно заданным в политике правилам. Если политика не определена или выключена, то пароль будет состоять из цифр, строчных латинских букв и иметь длину 6 символов.

☐ Не задано	Комментарий:	
☒ Включено		
☐ Отключено	Требования к версии:	Windows XP и более поздние версии
Параметры:		
Длина одноразового пароля	10	
Вхождение групп символов:		
☒ Цифры		
☒ Строчные латинские буквы		
☒ Прописные латинские буквы		
☒ Специальные символы		

Настройки одновременного подключения к серверу SMPP

Политика применяется к серверам Indeed AM и определяет порядок обработки запросов к серверу SMPP. Включение политики может быть необходимо, в случае если сервер SMPP не поддерживает несколько подключений от одного пользователя (учетной записи, указанной в политике Сервис отправки SMS) одновременно.

Не задан (Not Configured) или Отключен (Disabled)

Подключение к серверу SMPP и запросы на отправку сообщений будут происходить параллельно.

Включен (Enabled)

Подключение к серверу SMPP и запросы на отправку сообщений будут происходить последовательно.

Настройка защиты от спама



Описание работы

Осуществляется оценка процента успешных входов относительно всех отправленных сообщений за указанный интервал времени (оценка осуществляется только если кол-во отправленных сообщений превышает "Окно оценки").

При обнаружении атаки блокируется дальнейшая отправка сообщений, при попытке входа возникает ошибка: `Potential spam attack detected`.

Отправка возобновится спустя некоторое время когда будет превышен необходимый порог успешных входов за указанный интервал времени. Максимальное время блокировки равно временному интервалу оценки.

Чтобы настроить защиту от спама:

1. Откройте **редактор реестра**;
2. Создайте раздел **Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-Id\BSPs\SMSOTP\SpamProtection**;
3. Создайте необходимые параметры:
 - a. **SpamProtectionEnabled**: Флаг включения защиты от спама (DWORD). Значение по умолчанию: 0
 - b. **TimeSpanSec**: Интервал времени (сек), по которому осуществляются расчеты (DWORD). Значение по умолчанию: 600
 - c. **EvaluationWindow**: Окно оценки (DWORD). Значение по умолчанию: 10
 - d. **MinSuccessfulLogonPercent**: Минимальный процент успешных входов относительно всех отправленных сообщений (DWORD). Значение по умолчанию: 20



События лог-сервера

2090: Обнаружена потенциальная спам-атака. Отправка сообщений приостановлена.

1118: Отправка сообщений пользователям возобновлена.

Indeed AM Telegram OTP Provider

ID Провайдера

{CA4645CC-5896-485E-A6CA-011FCC20DF1D}

Информация

Файлы для Indeed Telegram OTP Provider расположены: ***indeed AM <Номер версии>\Indeed AM Providers\Indeed AM Telegram OTP Provider***

- ***<Номер версии>\IndeedAM.AuthProviders.TelegramOTP-<номер версии>.x64.ru-ru.msi*** - Пакет для установки Indeed AM Telegram OTP Provider x64 версии.
- ***<Номер версии>\IndeedAM.AuthProviders.TelegramOTP-<номер версии>.x86.ru-ru.msi*** - Пакет для установки Indeed AM Telegram OTP Provider x86 версии.
- ***IndeedId.Telegram.Service-<номер версии>.x86.ru-ru.msi*** - Пакет для установки службы для работы с ботом.
- ***Misc\Reg*** - Файл настройки сервиса отправки через реестр.

Файлы шаблонов политик расположены: ***indeed AM <номер версии>\Misc\ADMX Templates***.

О компоненте Indeed AM Telegram OTP Provider

Информация

Для работы компонента требуется доступ к серверам Telegram для сервисной службы.

Информация

В данной версии системы Indeed провайдер Telegram OTP поддерживается в сценариях с Indeed NPS Radius, Identity Provider, IIS Extension.

Компонент Indeed AM Telegram Provider предназначен для аутентификации пользователей с применением технологии одноразовых паролей, доставляемых пользователям через созданного бота в мессенджере Telegram.

Одноразовый пароль представляет собой набор случайных символов (цифр, специальных символов и латинских букв). Генерация пароля происходит на сервере Indeed AM, затем пароль передается на серверы Telegram и отображается в чате с ботом.

Установка

Установка сервисной службы

1. Выполнить установку службы **AM Telegram Service** через запуск соответствующего пакета.
2. После завершения установки может потребоваться перезагрузка системы. Если программа установки предлагает выполнить перезагрузку, подтвердите данное действие.
3. Удаление/Восстановление продукта осуществляется стандартным для поддерживаемых ОС способом, через меню Панель управления.

Установка провайдера

1. Выполнить установку провайдера **Telegram OTP** через запуск соответствующего пакета.

Информация

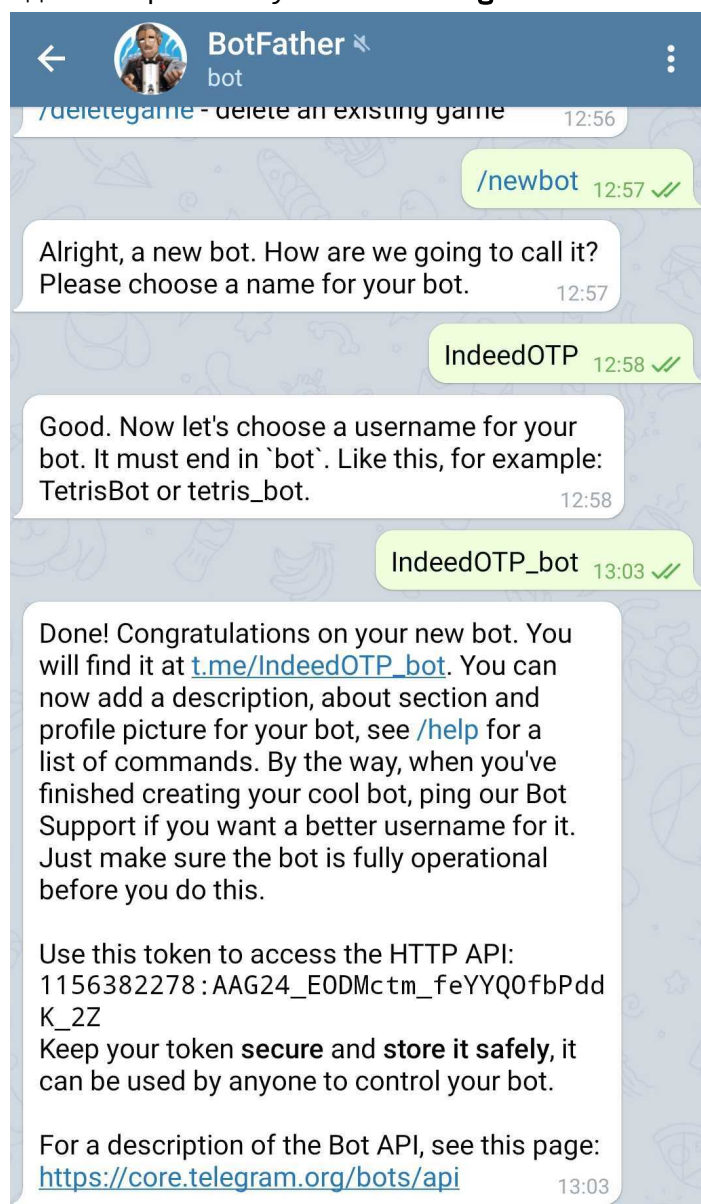
Если в инфраструктуре используется несколько серверов Indeed AM, то установку провайдера необходимо выполнить на всех серверах инфраструктуры.

2. После завершения установки может потребоваться перезагрузка системы. Если программа установки предлагает выполнить перезагрузку, подтвердите данное действие.
3. Удаление/Восстановление продукта осуществляется стандартным для поддерживаемых ОС способом, через меню Панель управления.

Настройка

Создание бота

1. Откройте приложение Telegram, найдите специального бота "**@botfather**" и откройте диалог с данным ботом.
2. Нажмите "**Start**" и введите команду "**/newbot**".
3. Необходимо указать имя создаваемого бота, данное название будет отображаться в окне диалога с ботом. Введите любое имя, например, **IndeedOTP**.
4. Необходимо указать имя пользователя для аккаунта с ботом с 'bot' в конце, данное имя пользователя используется для ссылок на него. Введите любое имя, например, **IndeedOTP_bot**.
5. В случае успешной регистрации будет отображен токен для доступа к API. Данный токен потребуется для настройки службы "**AM Telegram Service**".



Настройка службы

1. Откройте конфигурационный файл службы **AM.Telegram.Service.exe.config** (C:\Program Files (x86)\Indeed-Id\Indeed-Id Telegram Service).



Информация

Для сохранения изменений в конфигурационном файле приложения, требуется запустить редактор с правами администратора.

2. В атрибутах **value** для соответствующих атрибутов **key** укажите необходимые значения

- a. **culture** - Язык локализации, поддерживается русский и английский. Значение по умолчанию: **ru-RU**.
- b. **EAWebAPIURL** - URL адрес сервер Indeed AM.
- c. **username** - Имя сервисного пользователя от имени которого будет осуществляться регистрация аутентификаторов.
- d. **password** - Пароль сервисного пользователя.
- e. **lognames** - Формат логирования имен пользователей. Значение по умолчанию: **Name**. Поддерживаемые форматы:
 - **Id** - Идентификатор пользователя в системе Indeed AM в формате **rootUserCatalogProviderId_Guid**.
 - **Name** - Значение атрибута **name** из Active Directory.
 - **CanonicalName** - Имя пользователя в формате **Canonical-Name** (myserver.demo.local/users/UserName).
 - **PrincipalName** - Значение атрибута **userPrincipalName** из Active Directory.
 - **SamCompatibleName** - Имя пользователя в формате **domainName\UserName**.
 - **DistinguishedName** - Значение атрибута **distinguishedName** из Active Directory.
 - **Sid** - Значение атрибута **objectSid** из Active Directory.
 - **Email** - Значение атрибута **mail** из Active Directory или значение указанное в конфигурационном файле сервера.
 - **Phone** - Значение атрибута **telephoneNumber** из Active Directory или значение указанное в конфигурационном файле сервера.

Пример

```
<add key="lognames" value="PrincipalName,Sid" />
```

- f. **botId** - Идентификатор бота(токен), получаемый при его регистрации в Telegram.

Пример

```
<appSettings>
  <add key="culture" value="ru-RU" />
  <add key="EAWebAPIURL" value="https://server.indeed.local/am/core/" />
  <add key="username" value="telegram@indeed.local" />
  <add key="password" value="Q1q2E3e4" />
  <add key="lognames" value="Name" />
  <add key="botId" value="1156320278:AAG24_EODMotm_feYYQOfbPddK_2Z_JDiKQ" />
</appSettings>
```

3. Задайте **url** для подключения к лог серверу. Редактируем тег **logServer**.
 - a. **URL** - url для подключения к log серверу в формате http (s)://полное_dns_имя_сервера/ls/api.
 - b. **CertificateThumbprint** - если закрытый ключ в реестре, а сертификат в хранилище компьютера.
 - c. **CertificateFilePath** - если ключевая пара в pfx.
 - d. **CertificateFilePassword**- пароль от pfx.

```
<logServer Url="https://logserver.indeed.local/ls/api/" CertificateThumbprint=""
CertificateFilePath="" CertificateFilePassword="" />
```

4. Запустите службу "**AM Telegram Service**".

Имя	Описание	Состояние	Тип запуска	Вход от имени
 AM Telegram Service	AM Telegram Bot Service	Выполняется	Автоматиче...	Локальная сис...
 ASP.NET State Service	Provides support for out...		Вручную	Сетевая служба
 CDPUserSvc_148370	< Не удается прочитать...	Выполняется	Автоматиче...	Локальная сис...
 CoreMessaging	Manages communicatio...	Выполняется	Автоматиче...	Локальная слу...
 DataCollectionPublishingSe...	The DCP (Data Collectio...		Вручную (ак...	Локальная сис...

Настройка сервиса отправки

Настройка через групповые политики

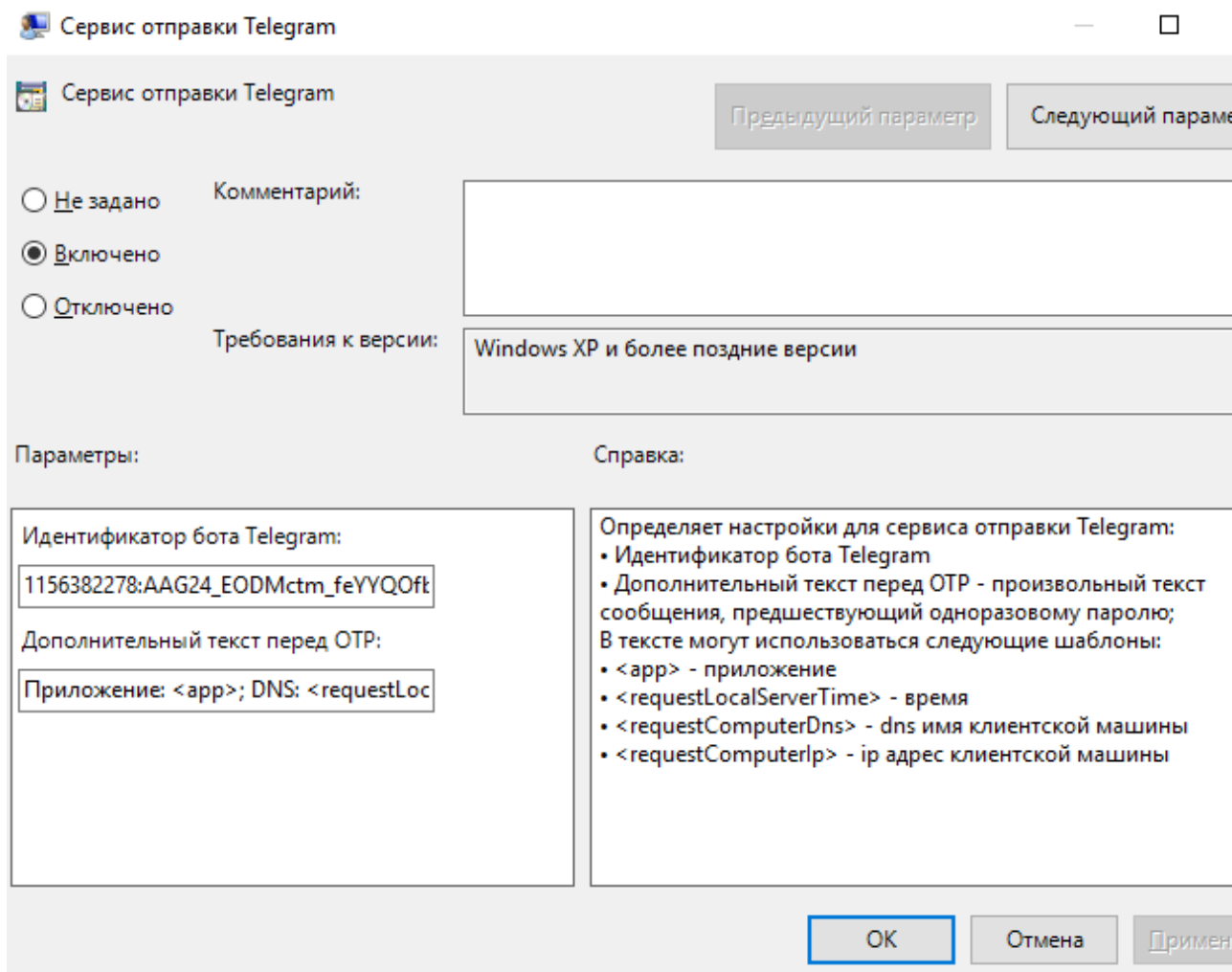
Информация

Перед настройкой групповой политики необходимо добавить в список административных шаблонов шаблоны политик Indeed AM. Файлы шаблонов политик входят в состав дистрибутива провайдера и расположены в каталоге Misc.

1. Откройте политику "Сервис отправки Telegram".
2. В поле "Идентификатор бота Telegram" Укажите идентификатор(токен) созданного бота.
3. В поле "Дополнительный текст перед OTP" можно задать дополнительную информацию:

 Необязательный параметр

- **<app>** - Приложение
- **<requestLocalServerTime>** - Время
- **<requestComputerDns>** - dns имя клиентской машины
- **<requestComputerIp>** - ip адрес клиентской машины



Сервис отправки Telegram

Предыдущий параметр

Следующий параметр

☐ Не задано Комментарий:

☒ Включено

☐ Отключено

Требования к версии: Windows XP и более поздние версии

Параметры:

Идентификатор бота Telegram:
1156382278:AAG24_EODMctm_feYYQOfk

Дополнительный текст перед OTP:
Приложение: <app>; DNS: <requestLoc

Справка:

Определяет настройки для сервиса отправки Telegram:

- Идентификатор бота Telegram
- Дополнительный текст перед OTP - произвольный текст сообщения, предшествующий одноразовому паролю; В тексте могут использоваться следующие шаблоны:
- <app> - приложение
- <requestLocalServerTime> - время
- <requestComputerDns> - dns имя клиентской машины
- <requestComputerIp> - ip адрес клиентской машины

OK Отмена Примен

Настройка через реестр

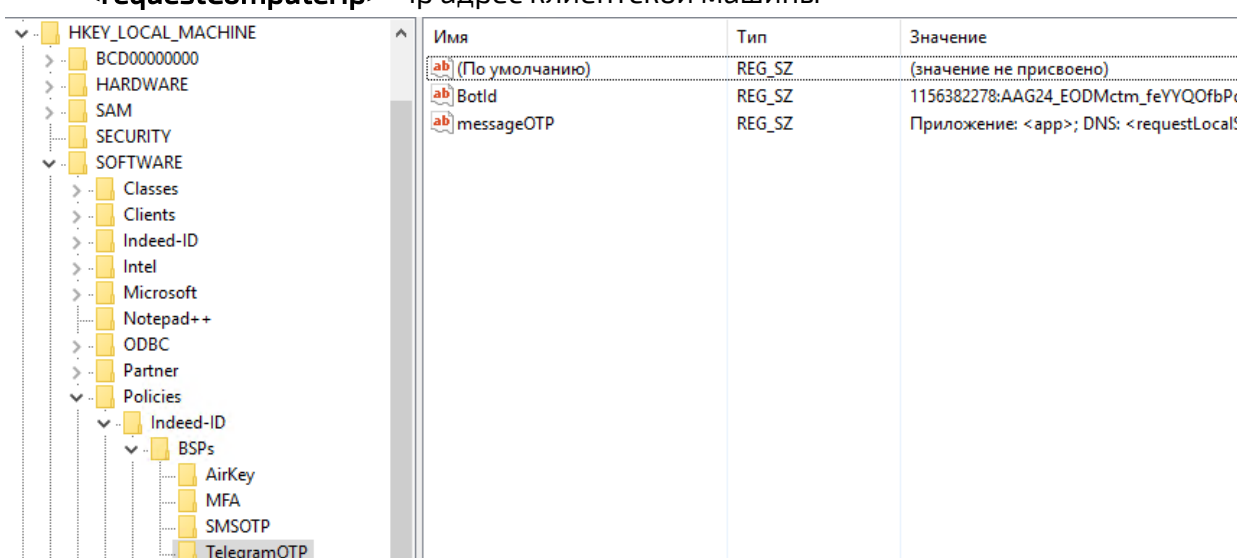
Информация

В /Misc/Reg провайдера расположен .reg файл с примером настройки.

1. В разделе **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\BSPs** создайте раздел **"TelegramOTP"**.
2. В разделе **"TelegramOTP"** создайте параметр типа **REG_SZ** с именем **"BotId"** и укажите идентификатор (токен) бота.
3. В разделе **"TelegramOTP"** создайте параметр типа **REG_SZ** с именем **"messageOTP"** и укажите дополнительную информацию, которую будет отображать перед OTP:

i Необязательный параметр

- **<app>** - Приложение
- **<requestLocalServerTime>** - Время
- **<requestComputerDns>** - dns имя клиентской машины
- **<requestComputerIp>** - ip адрес клиентской машины



The image shows the Windows Registry Editor with the following structure:

- HKEY_LOCAL_MACHINE
 - BCD00000000
 - HARDWARE
 - SAM
 - SECURITY
 - SOFTWARE
 - Classes
 - Clients
 - Indeed-ID
 - Intel
 - Microsoft
 - Notepad++
 - ODBC
 - Partner
 - Policies
 - Indeed-ID
 - BSPs
 - AirKey
 - MFA
 - SMSOTP
 - TelegramOTP

The right pane displays the following registry values:

Имя	Тип	Значение
(По умолчанию)	REG_SZ	(значение не присвоено)
BotId	REG_SZ	1156382278:AAG24_EODMctm_feYYQOfbP
messageOTP	REG_SZ	Приложение: <app>; DNS: <requestLocal!

Настройка параметров аутентификации

i Информация

Перед настройкой групповой политики необходимо добавить в список административных шаблонов шаблоны политик Indeed AM. Файлы шаблонов политик входят в состав дистрибутива провайдера и расположены в каталоге Misc.

Настройка генерации одноразового пароля

Политика позволяет задать длину и вхождение групп символов при генерации одноразового пароля.

Группы символов:

- Цифры - "0-9";
- Строчные латинские буквы - "a-z";
- Прописные латинские буквы - "A-Z";
- Специальные символы - ",.<>/?[]{}=+-_\\!@#\$\$%^&*()"

Если политика не определена или выключена, то пароль будет состоять из цифр, строчных латинских букв и иметь длину 6 символов.

Настройки генерации одноразового пароля

Настройки генерации одноразового пароля

Предыдущий параметр Следующий параметр

☐ Не задано Комментарий:

☒ Включено

☐ Отключено

Требования к версии: Windows XP и более поздние версии

Параметры:

Длина одноразового пароля: 6

Вхождение групп символов:

☒ Цифры

☐ Строчные латинские буквы

☐ Прописные латинские буквы

Справка:

Политика позволяет задать длину и вхождение групп символов при генерации одноразового пароля.

Группы символов:

Цифры - "0-9";

Строчные латинские буквы - "a-z";

Прописные латинские буквы - "A-Z";

Специальные символы - ",.<>/?[]{}=+-_\\!@#\$\$%^&*()"

Если политика не определена или выключена, то пароль будет состоять из цифр, строчных латинских букв и иметь длину 6 символов.

ОК Отмена Применить

Регистрация аутентификатора



Информация

При регистрации провайдера будет запрошен номер телефона из аккаунта Telegram, необходимо чтобы у пользователя в AD номер телефона полностью соответствовал и был одного формата. Поддерживаемы форматы: +7xxxxxxxxxx или 8xxxxxxxxxx

1. Откройте чат с созданным ботом и нажмите "Start".
2. Введите команду **"/register"**. После ввода команды необходимо предоставить номер телефона аккаунта Telegram боту.

Share your phone number?

The bot will know your phone number. This can be useful for integration with other services.

CANCEL

SHARE CONTACT

3. При успешной регистрации аутентификатора отобразится сообщение "Вы были успешно зарегистрированы".

Описание работы

Осуществляется оценка процента успешных входов относительно всех отправленных сообщений за указанный интервал времени (оценка осуществляется только если кол-во отправленных сообщений превышает "Окно оценки").

При обнаружении атаки блокируется дальнейшая отправка сообщений, при попытке входа возникает ошибка: `Potential spam attack detected`.

Отправка возобновится спустя некоторое время когда будет превышен необходимый порог успешных входов за указанный интервал времени. Максимальное время блокировки равно временному интервалу оценки.

Чтобы настроить защиту от спама:

1. Откройте **редактор реестра**;
2. Создайте раздел **Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-Id\BSPs\TelegramOTP\SpamProtection**;
3. Создайте необходимые параметры:
 - a. **SpamProtectionEnabled**: Флаг включения защиты от спама (DWORD). Значение по умолчанию: 0
 - b. **TimeSpanSec**: Интервал времени (сек), по которому осуществляются расчеты (DWORD). Значение по умолчанию: 600
 - c. **EvaluationWindow**: Окно оценки (DWORD). Значение по умолчанию: 10
 - d. **MinSuccessfulLogonPercent**: Минимальный процент успешных входов относительно всех отправленных сообщений (DWORD). Значение по умолчанию: 20

События лог-сервера

2090: Обнаружена потенциальная спам-атака. Отправка сообщений приостановлена.

1118: Отправка сообщений пользователям возобновлена.

Настройка прокси

Чтобы настроить работу Telegram OTP Provider через прокси, выполните следующие действия:

1. Откройте конфигурационный файл *AM.Telegram.Service.exe.config* из *C:\Program Files (x86)\Indeed-Id\Indeed-Id Telegram Service* и измените следующие параметры:
 - а. в параметре *useProхy* укажите значение *true* (по умолчанию *false*)
 - б. в параметре *proхyAddress* укажите адрес прокси-сервера
2. Откройте редактор реестра. В созданном ранее [разделе Telegram OTP](#) создайте два параметра:
 - а. параметр типа REG_SZ с именем *proхyAddress* с адресом прокси-сервера
 - б. параметр типа REG_DWORD с именем *useProхy* со значением *1*

Indeed AM SMS OTP Provider

ID Провайдера

{EBB6F3FA-A400-45F4-853A-D517D89AC2A3}

Информация

Файлы для Indeed SMS OTP Provider расположены: *indeed AM <Номер версии> \Indeed AM Providers\Indeed AM SMS OTP Provider*

- **Server\<Номер версии>\IndeedAM.AuthProviders.SmsOTP-<номер версии>.x64.ru-ru.msi** - Пакет для установки Indeed SMS OTP Provider на сервер Indeed AM на 64-х битной ОС.
- **Server\<Номер версии>\IndeedAM.AuthProviders.SmsOTP-<номер версии>.x86.ru-ru.msi** - Пакет для установки Indeed SMS OTP Provider на сервер Indeed AM на 32-х битной ОС.
- **Client\<Номер версии>\IndeedID.SMSOTP.Provider.msi** - Пакет для установки Indeed SMS OTP Provider на клиентские машины.

Файлы шаблонов политик расположены: *indeed AM <номер версии>\Misc\ADMX Templates.*

О компоненте Indeed AM SMS OTP Provider

Примечание

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 Indeed AM 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 не доступен для использования.

Обучение для аутентификатора не требуется.

Компонент Indeed AM SMS OTP Provider предназначен для аутентификации пользователей с применением технологии одноразовых паролей, доставляемых пользователям по SMS.

Одноразовый пароль представляет собой набор случайных символов (цифр, специальных символов и латинских букв). Генерация пароля происходит на сервере Indeed AM, затем пароль передается на SMS шлюз, имеющийся в инфраструктуре клиента, после OTP отправляется на номер телефона пользователя. Передача данных происходит по протоколу SMPP (англ. Short Message Peer-to-Peer).

Установка

1. Выполнить установку SMS OTP Provider через запуск соответствующего пакета.



Информация

Если в инфраструктуре используется несколько серверов Indeed AM, то установку провайдера необходимо выполнить на всех серверах инфраструктуры.

При использовании провайдера в клиентских сценариях с Indeed AM Windowsl Logon и ESSO Agent, необходимо выполнить установку провайдера из папки **Client** на клиентские машины.

2. После завершения установки может потребоваться перезагрузка системы. Если программа установки предлагает выполнить перезагрузку, подтвердите данное действие.
3. Удаление/Восстановление продукта осуществляется стандартным для поддерживаемых ОС способом, через меню Панель управления.

Настройка параметров аутентификации



Информация

Перед настройкой групповой политики необходимо добавить в список административных шаблонов шаблоны политик Indeed AM. Файлы шаблонов политик входят в состав дистрибутива провайдера и расположены в каталоге Misc.

Настройка атрибута с номером телефона

Для смены атрибута по умолчанию необходимо добавить параметры в конфигурационный файл сервера (C:\inetpub\wwwroot\am\core\Web.config).

- Добавить тег "userMapRules" в теге "adUserCatalogProvider".
Добавить тег "adObjectMapRule" в теге "userMapRules" с параметрами:
 - "attribute="Phone"" - Указывает на изменяемый параметр.
 - "adAttribute="mobile"" - Указывает с какого атрибута AD брать значение.
- Добавить тег "objectTypeSettings".
- Добавить тег "objectSetting" с параметрами "category="person" class="user"

Пример

```
<adUserCatalogProvider id="userId" serverName="ind.loc" containerPath="DC=ind,DC=loc"
userName="userAdmin" password="Q1q2E3e4">
  <userMapRules>
    <adObjectMapRule attribute="Phone" adAttribute="mobile"/>
  </userMapRules>
  <objectTypeSettings>
    <objectSetting category="person" class="user"></objectSetting>
  </objectTypeSettings>
</adUserCatalogProvider>
```

Настройка провайдера

Выбор типа подключения для провайдера (Choosing the connection type for the provider)

Настройка через GPO

Политика применяется к серверам Indeed AM и предназначена для выбора Sender провайдера SMSOTP.

Не задан (Not Configured) или Отключен (Disabled)

Будет использоваться подключение по SMPP

Включен (Enabled)

Будет использоваться подключение по заданному провайдеру.

Выбор типа подключения для провайдера

Предыдущий параметр Следующий параметр

☐ Не задано ☒ Включено ☐ Отключено

Комментарий:

Требования к версии: Windows XP и более поздние версии

Параметры:

Провайдер: Megafon
Megafon
OneGate
Smpp

Настройка через реестр

1. Откройте редактор реестра на сервере Indeed AM;
2. Откройте раздел "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\BSPs\SMSOTP";
3. Создайте следующий DWORD параметр **SmsSenderType**, со значением: 0 - Smpp; 1 - Megafon; 2 - OneGate.

Настройка сервиса SMPP (Service Configurations SMPP)

Настройка через GPO

Политика применяется к серверам Indeed AM и определяет следующие настройки для сервиса SMPP:

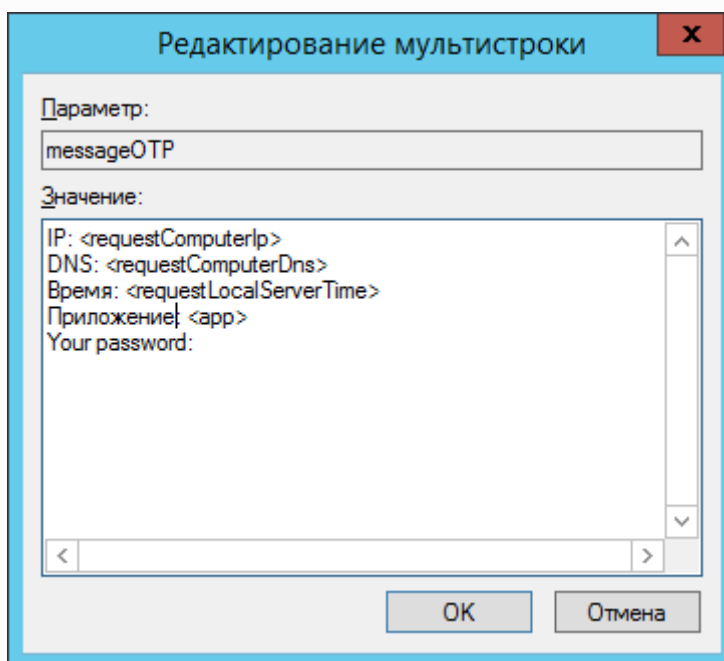
- **Use tls** - Использование шифрования.
- **URL(IP-адрес)** - Адрес подключения к серверу.
- **Порт** - Порт подключения к серверу.
- **SystemId (Логин)** - Имя учетной записи для подключения к серверу.
- **Пароль** - Пароль учетной записи для подключения к серверу.
- **SystemType** - Поле PDU операции BIND_TRANSCEIVER протокола SMPP.
- **Отправитель** - Имя отправителя, которое будет отображаться при получении SMS.
- **Дополнительный текст перед OTP** - Произвольный текст сообщения, предшествующий одноразовому паролю. По умолчанию отправляется только OTP, для дополнительной настройки параметров используйте следующие параметры:

- **<app>** - Имя приложения, отправившего запрос на авторизацию.
- **<requestLocalServerTime>** - Локальное серверное время получения запроса.
- **<requestComputerDns>** - DNS имя компьютера отправившего запрос.
- **<requestComputerIp>** - IP адрес компьютера отправившего запрос.

Информация

Отображение OTP кода не настраивается, OTP всегда отображается в конце сообщения.

Для переноса строк отправляемого сообщения необходимо внести изменения в реестр **HKLM/SOFTWARE/Policies/Indeed-ID/BSPs/SMSOTP**. Измените значение для старого параметра **"messageOTP"** с типом **"REG_SZ"**, на **"messageOTP"** с типом **"REG_MULTI_SZ"**.



- **Время ожидания статуса SMS** - Время ожидания получения статуса отправленного SMS с сервера.
- **PDU со статусом SMS** - PDU, в котором сервер присылает статус отправленного сообщения.
- **Подключаться как: Transmitter** - отправка пакета BIND_TRANSMITTER при подключении, **Transceiver** - отправка пакета BIND_TRANSCEIVER при подключении. В случае подключения как Transmitter сервер присылает статус отправленного SMS сообщения только в пакете SUBMIT_SM_RESP.
- **source_addr_ton** - Тип Номера (Type of Number) для исходного адреса.
- **source_addr_npi** - Индикатор Схемы Присвоения Номеров (Numbering Plan Indicator) для исходного адреса.

- **dest_addr_ton** - Тип Номера (Type of Number) для адресата.
- **dest_addr_npi** - Индикатор Схемы Присвоения Номеров (Numbering Plan Indicator) для адресата.
- **esm_class** - Указывает Message Mode & Message Type.
- **registered_delivery** - Индикатор для того, чтобы обозначить, что запрашивается расписка о получении SMSC или подтверждение SME.
- **data_coding** - Определяет схему кодировки пользовательских данных короткого сообщения.


Настройка сервиса SMPP

[Предыдущий параметр](#)
[Следующий параметр](#)

☐ Не задано
 ☒ Включено
 ☐ Отключено

Комментарий:

Требования к версии:

Windows XP и более поздние версии

Параметры:

☒ Use tls

URL(IP-адрес):

Порт:

SystemId(Логин):

Пароль:

SystemType:

Отправитель:

Дополнительный текст перед OTP:

Время ожидания статуса SMS:

PDU со статусом SMS:

Подключаться как:

Параметры SMPP:

source_addr_ton

source_addr_npi

dest_addr_ton

dest_addr_npi

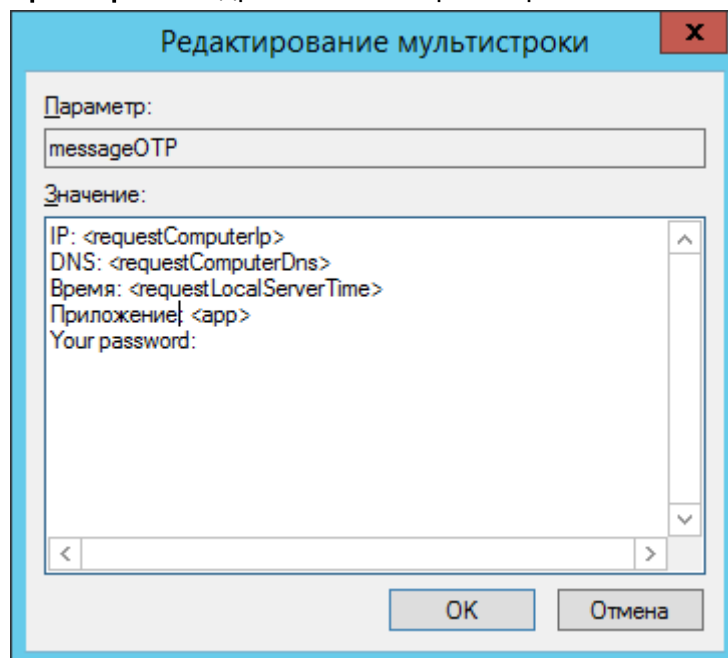
esm_class

registered_delivery

data_coding

Настройка через реестр

1. Откройте редактор реестра на сервере Indeed AM;
2. Откройте раздел "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\BSPs\SMSOTP";
3. Создайте следующие параметры:
 - a. **enableTls** (DWORD) - Использование шифрования (1 или 0).
 - b. **srvAddr** (строковый параметр) - Адрес подключения к серверу.
 - c. **srvPort** (DWORD) - Порт подключения к серверу.
 - d. **srvSystemId** (REG_SZ)- Имя учетной записи для подключения к серверу.
 - e. **srvPassword** (REG_SZ) - Пароль учетной записи для подключения к серверу.
 - f. **srvSysType** (REG_SZ) - Поле PDU операции BIND_TRANSCEIVER протокола SMPP.
 - g. **senderName** (REG_SZ) - Имя отправителя, которое будет отображаться при получении SMS.
 - h. **messageOTP** (REG_MULTI_SZ) - Произвольный текст сообщения, предшествующий одноразовому паролю. По умолчанию отправляется только OTP, для дополнительной настройки параметров используйте следующие параметры:
 - **<app>** - Имя приложения, отправившего запрос на авторизацию.
 - **<requestLocalServerTime>** - Локальное серверное время получения запроса.
 - **<requestComputerDns>** - DNS имя компьютера отправившего запрос.
 - **<requestComputerIp>** - IP адрес компьютера отправившего запрос.



- i. **SMPPServerTimeoutSec** (DWORD)- Время ожидания получения статуса отправленного SMS с сервера.
- j. **MessageStatusPDU** (DWORD) - PDU, в котором сервер присылает статус отправленного сообщения. 0 - SUBMIT_SM_RESP; 1 - DELIVER_SM.

- k. **BindTransmitter** (DWORD). 1 - **Transmitter** - отправка пакета BIND_TRANSMITTER при подключении; 0 - **Transceiver** - отправка пакета BIND_TRANSCEIVER при подключении. В случае подключения как Transmitter сервер присылает статус отправленного SMS сообщения только в пакете SUBMIT_SM_RESP.
- l. **sourceAddrTon** (DWORD) - Тип Номера (Type of Number) для исходного адреса.
- m. **sourceAddrNpi** (DWORD)- Индикатор Схемы Присвоения Номеров (Numbering Plan Indicator) для исходного адреса.
- n. **destAddrTon** (DWORD) - Тип Номера (Type of Number) для адресата.
- o. **destAddrNpi** (DWORD)- Индикатор Схемы Присвоения Номеров (Numbering Plan Indicator) для адресата.
- p. **esmClass** - Указывает Message Mode & Message Type.
- q. **registeredDelivery** - Индикатор для того, чтобы обозначить, что запрашивается расписка о получении SMSC или подтверждение SME.
- r. **dataCoding** - Определяет схему кодировки пользовательских данных короткого сообщения.

Настройка резервного сервиса SMPP

В политике «Настройка сервиса SMPP (резервный)» вы можете настроить резервный сервис SMPP, через который будут отправляться СМС, если основной сервис недоступен.

При отправке СМС core сервер проверяет доступность основного сервиса SMPP. Если основной сервис доступен, СМС отправляется через основной шлюз. Если основной сервис недоступен, СМС отправляется через резервный шлюз.

Сервис считается недоступным, если core сервер получает следующие ошибки:

- SMS sending service address unavailable
- SMPP Error Bind
- SMPP Error SubmitS

Политика резервного сервиса SMPP настраивается аналогично [основной политики SMPP](#).

При наличии настроенного резервного сервиса переход к нему при недоступности основного сервиса происходит автоматически.

Настройки сервиса Megafon (Service Configurations Megafon)

Настройка через GPO

Политика применяется к серверам Indeed AM и определяет настройки для Megafon сервиса отправки SMS:

- **URL** - Адрес подключения к серверу;
- **Логин** - Имя учетной записи для подключения к серверу;
- **Пароль** - Пароль учетной записи для подключения к серверу;
- **Отправитель** - Имя отправителя, которое будет отображаться при получении SMS;
- **Дополнительный текст перед OTP** - Произвольный текст сообщения, предшествующий одноразовому паролю.

 Настройки сервиса MegaFon

 Настройки сервиса MegaFon

Предыдущий параметр Следующий параметр

☐ Не задано Комментарий:

☒ Включено

☐ Отключено

Требования к версии: Windows XP и более поздние версии

Параметры:

URL:

Логин:

Пароль:

Отправитель:

Дополнительный текст перед отправкой OTP:

Настройка через реестр

1. Откройте редактор реестра на сервере Indeed AM;
2. Откройте раздел "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\BSPs\SMSOTP\Megafon";
3. Создайте следующие параметры:
 - a. **ServerUrl** (REG_SZ) - Адрес подключения к серверу;
 - b. **Login** (REG_SZ) - Имя учетной записи для подключения к серверу;
 - c. **Password** (REG_SZ) - Пароль учетной записи для подключения к серверу;
 - d. **From** (REG_SZ) - Имя отправителя, которое будет отображаться при получении SMS;
 - e. **messageOTP** (REG_SZ) - Произвольный текст сообщения, предшествующий одноразовому паролю.

Настройки сервиса OneGate (Service Configurations OneGate)

Настройка через GPO

Политика применяется к серверам Indeed AM и определяет настройки для OneGate сервиса отправки SMS:

- **URL** - адрес подключения к серверу;
- **Логин** - имя учетной записи для подключения к серверу;
- **Пароль** - пароль учетной записи для подключения к серверу;
- **Имя отправителя** - Отображается как имя отправителя в устройстве получателя;
- **Имя системы отправителя** - Сочетание "Имя системы отправителя" и "Имя отправителя" определяет логин под которым обращаемся в сепаратор;
- **Дополнительный текст перед OTP** - произвольный текст сообщения, предшествующий одноразовому паролю.

Настройки сервиса OneGate

Настройки сервиса OneGate

☒ Не задано Комментарий:

☐ Включено

☐ Отключено

Требования к версии: Windows XP и более поздние версии

Параметры:

URL:

Логин:

Пароль:

Имя отправителя:

Имя системы-отправителя:

Дополнительный текст перед отправкой OTP:

Настройка через реестр

1. Откройте редактор реестра на сервере Indeed AM;
2. Откройте раздел "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\BSPs\SMSOTP\OneGate";
3. Создайте следующие параметры:
 - a. **ServerUrl** (REG_SZ) - Адрес подключения к серверу;
 - b. **Login** (REG_SZ) - Имя учетной записи для подключения к серверу;
 - c. **Password** (REG_SZ) - Пароль учетной записи для подключения к серверу;
 - d. **NameSender** (REG_SZ) - Отображается как имя отправителя в устройстве получателя;
 - e. **NameSystem** (REG_SZ) - Сочетание "Имя системы отправителя" и "Имя отправителя" определяет логин, под которым обращаемся в сепаратор;
 - f. **messageOTP** (REG_SZ) - Произвольный текст сообщения, предшествующий одноразовому паролю.

Настройки сервиса MFMSolution (Service Configurations MFMSolution)

Настройка через GPO

Политика применяется к серверам Indeed AM и определяет настройки для MFMSolution сервиса отправки SMS:

- **URL** - адрес подключения к серверу;
- **Логин** - имя учетной записи для подключения к серверу;
- **Пароль** - пароль учетной записи для подключения к серверу;
- **Имя отправителя** - отображается как имя отправителя в устройстве получателя;
- **Дополнительный текст перед OTP** - произвольный текст сообщения, предшествующий одноразовому паролю.

Настройки сервиса MFMSolution

Предыдущий параметр Следующий параметр

☐ Не задано
 ☒ Включено
 ☐ Отключено

Комментарий:

Требования к версии: Windows XP и более поздние версии

Параметры:

URL:

Логин:

Пароль:

Отправитель:

Дополнительный текст перед отправкой OTP:

Справка:

Определяет настройки для MFMSolution сервиса отправки SMS:

- URL - адрес подключения к серверу;
- SystemId (Логин) - имя учетной записи для подключения к серверу;
- Пароль - пароль учетной записи для подключения к серверу;
- Отправитель - имя отправителя, которое будет отображаться при получении SMS
- Дополнительный текст перед OTP - произвольный текст сообщения, предшествующий одноразовому паролю.

ОК Отмена Применить

Настройка через реестр

1. Откройте редактор реестра на сервере Indeed AM;
2. Откройте раздел **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\BSPs\SMSOTP\MFM**;
3. Создайте следующие параметры:
 - a. **ServerUrl** (REG_SZ) - Адрес подключения к серверу;
 - b. **Login** (REG_SZ) - Имя учетной записи для подключения к серверу;
 - c. **Password** (REG_SZ) - Пароль учетной записи для подключения к серверу;
 - d. **From** (REG_SZ) - Отображается как имя отправителя в устройстве получателя;
 - e. **MessageOTP** (REG_SZ) - Произвольный текст сообщения, предшествующий одноразовому паролю.

Настройки сервиса Apache Kafka

Настройка через GPO

Политика применяется к серверам Indeed AM и определяет настройки для Apache Kafka сервиса отправки SMS:

- **URL** - адрес подключения к серверу;
- **Таймаут сервера** - время ожидания локального сообщения. Это значение применяется только локально и ограничивает время, в течение которого создаваемое сообщение ожидает успешную доставку. Если вы укажете значение 0 сек, то время ожидания будет бесконечным;
- **Включить сериализацию сообщения** - флаг включает или отключает сериализацию сообщения;
- **Schema registry URL** - адрес подключения к Schema Registry;
- **Путь к схеме сериализации** - путь к файлу json со схемой сериализации;
- **Протокол безопасности** - протокол, используемый для связи с брокерами;
- **SASL механизм** - механизм SASL для аутентификации;
- **Имя темы** - имя темы, в которую будут публиковаться сообщения;
- **Формат даты сообщения** - формат даты в полях сообщения;
- **Дополнительный текст перед OTP** - произвольный текст сообщения, предшествующий одноразовому паролю;

- **Путь к формату сообщения** - путь к файлу json с форматом сообщения.

Настройки сервиса Kafka

Настройки сервиса Kafka

Предыдущий параметр

Следующий параметр

Не задано

Комментарий:

Включено

Требования к версии:

Отключено

Windows XP and later versions

Параметры:

Справка:

URL:

Таймаут сервера (сек): 0

Включить сериализацию сообщения

Schema registry URL:

Путь к схеме сериализации:

Протокол безопасности:

SASL механизм:

Имя темы:

Формат даты сообщения:

Дополнительный текст перед OTP:

Путь к формату сообщения:

Определяет настройки для Kafka сервиса отправки SMS:

- URL - адрес подключения к серверу;
- Таймаут сервера - время ожидания локального сообщения. Это значение применяется только локально и ограничивает время, в течение которого создаваемое сообщение ожидает успешной доставки. Время 0 бесконечно;
- Путь к схеме сериализации - путь к json-файлу со схемой сериализации;
- Дополнительный текст перед OTP - произвольный текст сообщения, предшествующий одноразовому паролю;
- Путь к формату сообщения - путь к json-файлу с форматом сообщения.

OK

Отмена

Применить

Настройка через реестр

Indeed Access Manager Documentation

Страница 15 из 22

1. Откройте редактор реестра на сервере Indeed AM;
2. Откройте раздел **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\BSPs\SMSOTP** создайте следующие параметры:
 - a. **SmsSenderType** (DWORD) - тип отправителя СМС (для Apache Kafka установите значение 3);
 - b. **ParsePhone** (DWORD) - включение парсинга телефонного номера;
 - c. **PhonePrefix** (REG_SZ) - префикс номера телефона (если вы включили парсинг телефонного номера);
 - d. **PhoneLength** (DWORD) - длина номера телефона (если вы включили парсинг телефонного номера);
3. В разделе **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\BSPs\SMSOTP\Kafka** создайте следующие параметры:
 - a. **messageOTP** (REG_SZ) - произвольный текст сообщения, предшествующий одноразовому паролю;
 - b. **MessageFormatPath** (REG_SZ) - путь к файлу json с форматом сообщения;
 - c. **MessageDateFormat** (REG_SZ) - формат даты в полях сообщения;
 - d. **ServerUrl** (REG_SZ) - адрес сервера Apache Kafka;
 - e. **MessageTimeoutSec** (REG_DWORD) - время ожидания локального сообщения. Это значение применяется только локально и ограничивает время, в течение которого создаваемое сообщение ожидает успешную доставку. Если вы укажете значение 0 сек, то время ожидания будет бесконечным;
 - f. **TopicName** (REG_SZ) - имя темы Apache Kafka, в которую будут публиковаться сообщения;
 - g. **UseSerialization** (REG_DWORD) - включение или отключение сериализации;
 - h. **SchemaRegistryUrl** - адрес подключения к schema registry;
 - i. **RecordSchemaPath** (REG_SZ) - путь к файлу json со схемой сериализации;

Если вы используете авторизацию в Apache Kafka, добавьте следующие параметры;

 - j. **SecurityProtocol** (REG_SZ) - протокол, используемый для связи с брокерами;
 - k. **SaslMechanism** (REG_SZ) - механизм SASL для аутентификации;

Настройка формата сообщения (Date time format)

Настройка через GPO

Политика позволяет задать настройки формата отображения даты. Примеры форматов можно посмотреть по ссылке <https://docs.microsoft.com/ru-ru/dotnet/standard/base-types/standard-date-and-time-format-strings>

Включен (Enabled)

Дата будет отображаться согласно заданному в политике формату.

☐ Не задано Комментарий:

☒ Включено

☐ Отключено

Требования к версии: Windows XP и более поздние версии

Параметры:

Формат даты:

Настройка через реестр

1. Откройте редактор реестра на сервере Indeed AM;
2. Откройте раздел "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\BSPs\SMSOTP";
3. Создайте следующие параметры:
 - a. **SMSOTP** (DWORD) со значением 1.
 - b. **dateFormat** (REG_SZ) - Позволяет задать настройки формата отображения даты. Примеры форматов можно посмотреть по ссылке [Строки стандартных форматов даты и времени](#).

Настройки генерации одноразового пароля (One-time password generation settings)

Настройка через GPO

Политика применяется к серверам Indeed AM и позволяет задать длину и вхождение групп символов при генерации одноразового пароля.

Не задан (Not Configured) или Отключен (Disabled)

Если политика не задана или отключена, то пароль будет состоять из цифр и иметь длину 4 символов.

Включен (Enabled)

Одноразовый пароль будет генерироваться согласно заданным в политике правилам. Если политика не определена или выключена, то пароль будет состоять из цифр, строчных латинских букв и иметь длину 6 символов.

☐ Не задано	Комментарий:	
☒ Включено		
☐ Отключено		
Требования к версии:		Windows XP и более поздние версии
Параметры:		
Длина одноразового пароля		10
Вхождение групп символов:		
☒ Цифры		
☒ Строчные латинские буквы		
☒ Прописные латинские буквы		
☒ Специальные символы		

Настройка через реестр

1. Откройте редактор реестра на сервере Indeed AM;
2. Откройте раздел "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\BSPs\SMSOTP";
3. Создайте следующие параметры:
 - a. **OTPGeerator** (DWORD) - Включает данную настройку;
 - b. **OneTimePasswordLength** (DWORD) - Длина одноразового пароля;
 - c. **AllowDigitsChGr** (DWORD) - Использовать цифры в OTP;
 - d. **AllowLatinsLowerChGr** (DWORD) - Использовать строчные латинские буквы в OTP;
 - e. **AllowLatinsUpperChGr** (DWORD) - Использовать прописные латинские буквы в OTP;
 - f. **AllowSpecialChGr** (DWORD) - Использовать специальные символы в OTP.

Настройки формата телефонного номера (Settings phone number)

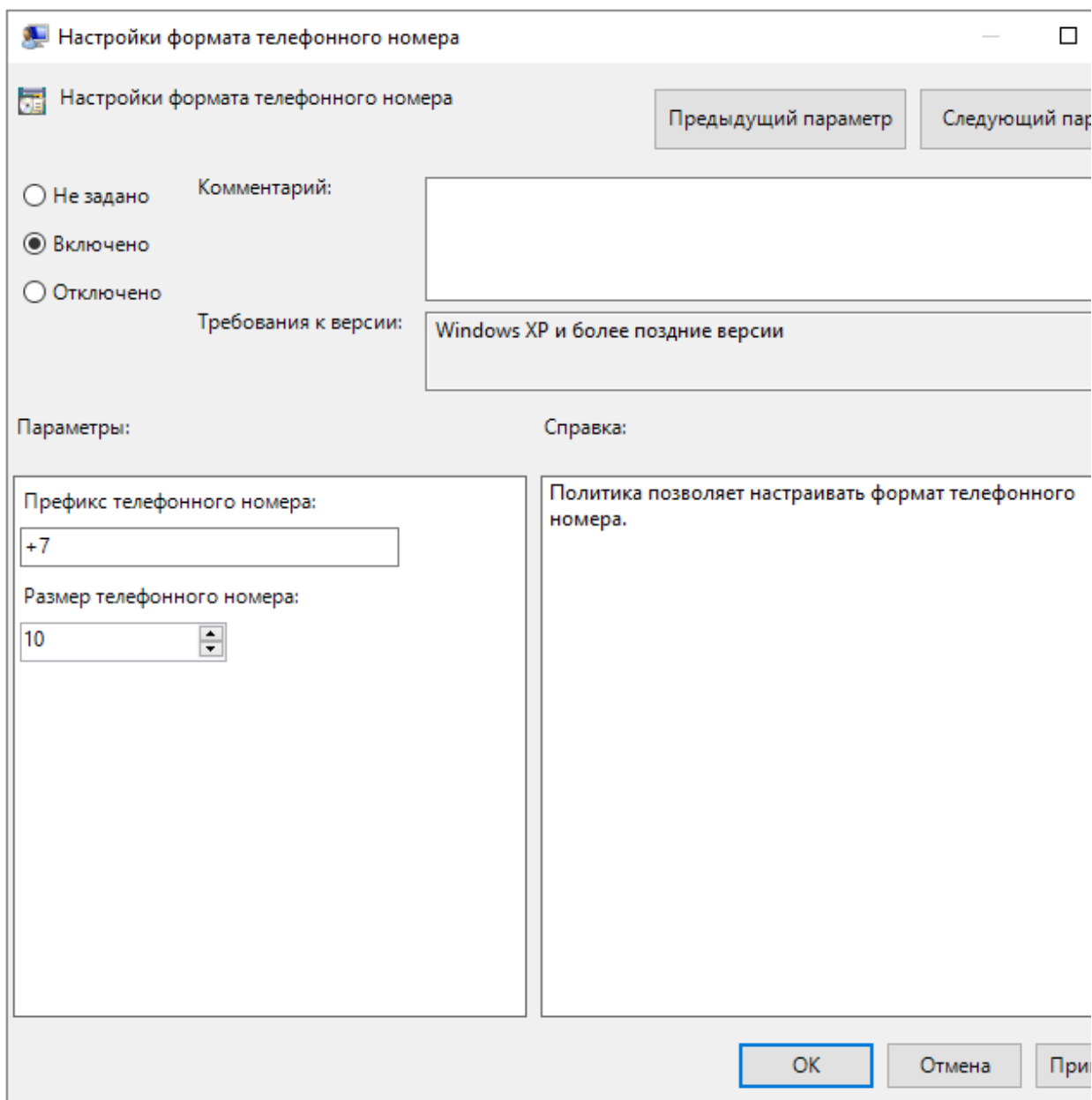
Настройка через GPO

Политика применяется к серверам Indeed AM и позволяет настраивать формат телефонного номера. При включении данной политики, включается нормализация телефонного номера. Это означает, что:

1. Пробелы, табуляцию, скобочки, дефисы будут удаляться.
2. Если в строке записаны несколько номеров и разделены запятой или точкой с запятой, будет браться первый номер в строке до разделителя.
3. 8 будет заменяться на +7.
4. Если в номере не хватает +7 или 8 в начале строки, то будет добавляться +7 перед номером.
5. В номерах могут быть символы O вместо цифры 0, они будут заменяться обратно на цифры.

Информация

Мегафон — по требованию формата REST запроса номер телефона должен иметь тип long. При нормализации "+" не учитывается.



Настройка через реестр

1. Откройте редактор реестра на сервере Indeed AM;
2. Откройте раздел "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\BSPs\SMSOTP";
3. Создайте следующие параметры:
 - a. **ParsePhone** (DWORD) - Включает парсинг телефонного номера;
 - b. **PhoneLength** (DWORD) - Размер телефонного номера;
 - c. **PhonePrefix** (DWORD) - Префикс телефонного номера.

Настройки одновременного подключения к серверу SMPP

Политика применяется к серверам Indeed AM и определяет порядок обработки запросов к серверу SMPP. Включение политики может быть необходимо, в случае если сервер SMPP не поддерживает несколько подключений от одного пользователя (учетной записи, указанной в политике Настройка сервиса SMPP) одновременно.

Не задан (Not Configured) или Отключен (Disabled)

Подключение к серверу SMPP и запросы на отправку сообщений будут происходить параллельно.

Включен (Enabled)

Подключение к серверу SMPP и запросы на отправку сообщений будут происходить последовательно.

Настройка защиты от спама



Описание работы

Осуществляется оценка процента успешных входов относительно всех отправленных сообщений за указанный интервал времени (оценка осуществляется только если кол-во отправленных сообщений превышает "Окно оценки").

При обнаружении атаки блокируется дальнейшая отправка сообщений, при попытке входа возникает ошибка: `Potential spam attack detected`.

Отправка возобновится спустя некоторое время когда будет превышен необходимый порог успешных входов за указанный интервал времени. Максимальное время блокировки равно временному интервалу оценки.

Чтобы настроить защиту от спама:

1. Откройте **редактор реестра**;
2. Создайте раздел **Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-Id\BSPs\SMSOTP\SpamProtection**;
3. Создайте необходимые параметры:
 - a. **SpamProtectionEnabled**: Флаг включения защиты от спама (DWORD). Значение по умолчанию: 0
 - b. **TimeSpanSec**: Интервал времени (сек), по которому осуществляются расчеты (DWORD). Значение по умолчанию: 600
 - c. **EvaluationWindow**: Окно оценки (DWORD). Значение по умолчанию: 10
 - d. **MinSuccessfulLogonPercent**: Минимальный процент успешных входов относительно всех отправленных сообщений (DWORD). Значение по умолчанию: 20

События лог-сервера

2090: Обнаружена потенциальная спам-атака. Отправка сообщений приостановлена.

1118: Отправка сообщений пользователям возобновлена.

Indeed AM Software OTP Provider

ID Провайдера

{0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0}

Для Indeed AM NPS RADIUS Extension

{B772829C-4076-482B-B9BD-53B55EA1A302}

Информация

Файлы для Indeed AM Software OTP Provider расположены: ***indeed AM <Номер версии>\Indeed AM Providers\Indeed AM Software OTP Provider\<Номер версии>***

- **IndeedId.SoftwareTOTP.Provider-<номер версии>.x86.ru-ru.msi** - Пакет для установки Indeed Software OTP Provider на x32 и x64 битных ОС.

Файлы шаблонов политик расположены: ***indeed AM <номер версии>\Misc\ADM Templates***.

О компоненте Indeed AM Software OTP Provider

Software OTP Provider – это двухфакторная аутентификация, основанная 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. 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).

Установка



Примечание

Для работы провайдера требуется установка Indeed AM Bsp Broker на сервере Indeed AM.

Файлы для Indeed Bsp Broker расположены: ***indeed AM <Номер версии>\Indeed Providers\Indeed AM Bsp Broker\<Номер версии>***

- **IndeedEA.AuthProviders.BspBroker-<номер версии>.x64.ru-ru.msi** - Пакет для установки Indeed Bsp Broker на 64-х битных ОС.
- **IndeedEA.AuthProviders.BspBroker-<номер версии>.x86.ru-ru.msi** - Пакет для установки Indeed Bsp Broker на 32-х битных ОС.

1. Выполнить установку Software OTP Provider через запуск соответствующего пакета.



Информация

Если в инфраструктуре используется несколько серверов Indeed AM, то установку провайдера необходимо выполнить на всех серверах инфраструктуры.

2. После завершения установки может потребоваться перезагрузка системы. Если программа установки предлагает выполнить перезагрузку, подтвердите данное действие.
3. Удаление/Восстановление продукта осуществляется стандартным для поддерживаемых ОС способом, через меню Панель управления.

Настройка параметров аутентификации

Информация

Перед настройкой групповой политики необходимо добавить в список административных шаблонов шаблоны политик Indeed AM. Файлы шаблонов политик входят в состав дистрибутива провайдера и расположены в каталоге Misc.

Примечание

Настройка политик необходима для повышения уровня безопасности. Однако полноценная работа Software OTP Provider возможна и со значениями политик, определенными по умолчанию

- **Время действия одноразового пароля**

Политика определяет, каким должен быть минимальный период действия одноразового пароля при обучении. Период задается целым числом от 3 до 18, где 3 соответствует временному промежутку в 30 секунд (+/- 15 секунд). Если политика не определена, по умолчанию используется значение 6.

- **Минимальная длина PIN-кода**

Политика позволяет задать минимальное количество символов, из которых должен состоять PIN-код. Допустимый диапазон от 4 до 25 символов.

- **Формат имени**

Информация

Политика применяется к серверам с установленной **Management Console консолью**. Если политика не была применена, в качестве имени OTP аккаунта будет использоваться имя пользователя.

Политика позволяет задать параметр пользователя в качестве имени OTP-аккаунта, который будет передаваться в QR-коде. Возможные параметры:

- **CanonicalName**
- **CN**
- **DistiguatedName**
- **FullName**
- **Mail**
- **PrincipalName**
- **SamCompatibleName**

Формат имени

Формат имени

Предыдущий параметр Следующий параметр

☐ Не задано Комментарий:

☒ Включено

☐ Отключено

Требования к версии: Windows XP и более поздние версии

Параметры: Справка:

Формат имени: CanonicalName
CanonicalName
CN
DistinguishedName
FullName
Mail
PrincipalName
SamCompatibleName

Формат имени. Возможные значения:

- CanonicalName,
- PrincipalName,
- SamCompatibleName,
- DistinguishedName,
- FullName,
- CN,
- Mail.

OK Отмена Применить

Google Authenticator



751 821

DistinguishedName

Indeed-Id:CN=Admin Adminov,OU=IndeedCatalog,DC=indeed-test,DC=com

141 593

CanonicalName

Indeed-Id:indeed-test.com/IndeedCatalog/Admin Adminov



Indeed Key Provider

ID Провайдера

{DEEF0CB8-AD2F-4B89-964A-B6C7ECA80C68}

Информация

Файлы для Indeed AM AirKey Provider расположены: ***indeed AM <Номер версии>\Indeed AM Providers\Indeed AM AirKey Provider***

- **Server\<Номер версии>\IndeedAM.AuthProviders.AirKey-<номер версии>.x64.ru-ru.msi** - Пакет для установки Indeed AM AirKey Provider на сервере Indeed AM на 64-битных ОС.
- **Server\<Номер версии>\IndeedAM.AuthProviders.AirKey-<номер версии>.x86.ru-ru.msi** - Пакет для установки Indeed AM AirKey Provider на сервере Indeed AM на 32-битных ОС.
- **Client\<Номер версии>\IndeedID.AirKey.Provider.msi** - Пакет для установки Indeed AM AirKey Provider на клиентской машине.

Файлы шаблонов политик расположены: ***indeed AM <номер версии>\Misc\ADMX Templates.***

О компоненте Indeed AM AirKey Provider

Информация

Для осуществления аутентификации с помощью Push-уведомлений есть следующие требования:

В сетевой инфраструктуре:

- Установка сервера Indeed Indeed Key Server. Данный сервер выполняет отправку уведомлений на смартфон пользователя используя API сервисы Google.
- Установка провайдера аутентификации Indeed AirKey. 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 Indeed Key Server, Indeed AirKey Provider и приложения Indeed Key, аутентификация с помощью Push-уведомлений невозможна.

Установка провайдера

1. Выполнить установку **AirKey Provider** на сервере Indeed AM и на клиенте через запуск соответствующего пакета для установки.



Информация

Если в инфраструктуре используется несколько серверов Indeed AM, то установку провайдера необходимо выполнить на всех серверах инфраструктуры.

При использовании провайдера в клиентских сценариях с Indeed AM Windowsl Logon и ESSO Agent, необходимо выполнить установку провайдера из папки **Client** на клиентские машины.

2. После завершения установки может потребоваться перезагрузка системы. Если программа установки предлагает выполнить перезагрузку, подтвердите данное действие.
3. Удаление/Восстановление продукта осуществляется стандартным для поддерживаемых ОС способом, через меню Панель управления.

Настройка провайдера

1. Откройте **Консоль администрирования**
2. Пройдите в раздел **Конфигурация**
3. В разделе **Конфигурация** выберите пункт **Push-аутентификация**

Укажите следующие данные:

1. **URL-адрес Indeed Key Server** - Указывается URL по которому **Indeed AirKey** сервер доступен с машины **Indeed AM**
2. **Отображаемое имя сервера** - Указывается название сервера **Indeed AM Indeed Key Server**, отображаемое в мобильном приложении
3. **Доверенный ID Indeed Key Server** - Укажите произвольный уникальный идентификатор. Необходим для подтверждения запроса удаления аутентификатора. Значение идентификатора должно совпадать с тем, что введено в конфигурационном файле **Indeed Key Server** ([ter trustedClients](#))
4. **Режим работы AirKey** - по умолчанию выбран **Push**. В случае выбора режима **OTP**, вместо подтверждения входа на телефоне, пользователю потребуется ввести **6-тизначный код** в соответствующее окно ввода.
5. **Способ подтверждения Push** - принудительный запрос у пользователя подтверждения:
 - a. **Подтверждение не требуется** - для подтверждения входа, у пользователя не будет запрашиваться доп. аутентификация на устройстве
 - b. **Подтверждение биометрическими средствами** - для подтверждения входа, у пользователя будет запрашиваться доп. аутентификация на устройстве, с помощью биометрии
 - c. **Подтверждение любыми средствами, доступными на устройстве** - для подтверждения входа, у пользователя будет запрашиваться доп. аутентификация на устройстве, с помощью любого доступного на устройстве метода
6. **Способ подтверждения для отображения OTP** - принудительный запрос у пользователя подтверждения:
 - a. **Подтверждение не требуется** - для подтверждения входа, у пользователя не будет запрашиваться доп. аутентификация на устройстве
 - b. **Подтверждение биометрическими средствами** - для подтверждения входа, у пользователя будет запрашиваться доп. аутентификация на устройстве, с помощью биометрии
 - c. **Подтверждение любыми средствами, доступными на устройстве** - для подтверждения входа, у пользователя будет запрашиваться доп. аутентификация на устройстве, с помощью любого доступного на устройстве метода
7. **Время отображения OTP** - количество секунд, которое актуален OTP.

INDEED ID

Пользователи

Политики

Аудит

События

Настройки

Приложения

Конфигурация

Устройства

Лицензии

Помощь и поддержка

МС / Конфигурация / Аутентификаторы

Конфигурация - Push-аутентификация

СохранитьОтмена

Права доступа

Роли

Глобальные администраторы

Аутентификаторы

Push-аутентификация

Пароль Windows

Блокировать способ аутентификации в случае серии неудачных попыток

ДаНет

Количество попыток аутентификации до блокировки

5

Сброс счетчика блокировки через (минут)

5

Таймаут до разблокировки способа входа (минут)

5

URL-адрес AirKey Cloud Server

https://am.indeed.local:82/

Отображаемое имя сервера

airkey

Доверенный ID AirKey Cloud Server

1

Режим работы AirKey

PushОТР

Способ подтверждения Push

Подтверждение не тре

Способ подтверждения для отображения ОТР

Подтверждение не тре

Время отображения ОТР

30

Настройка доверенного идентификатора для Indeed Key Server

Информация

По умолчанию при удалении аутентификатора в User Console, утилите управления аутентификаторами или в консоли администратора, аутентификатор будет удален из системы без уведомлений и останется отображаться в приложении. Для настройки push уведомления с информацией об удалении аутентификатора и удалением в приложении необходимо выполнить дополнительные настройки.

Indeed Access Manager Documentation

Страница 5 из 18

1. Откройте конфигурационный файл Indeed Key Server **Web.config** (C:\inetpub\wwwroot\airkeycloud).
2. Добавьте в файл следующие теги после блока **"appSettings"**:

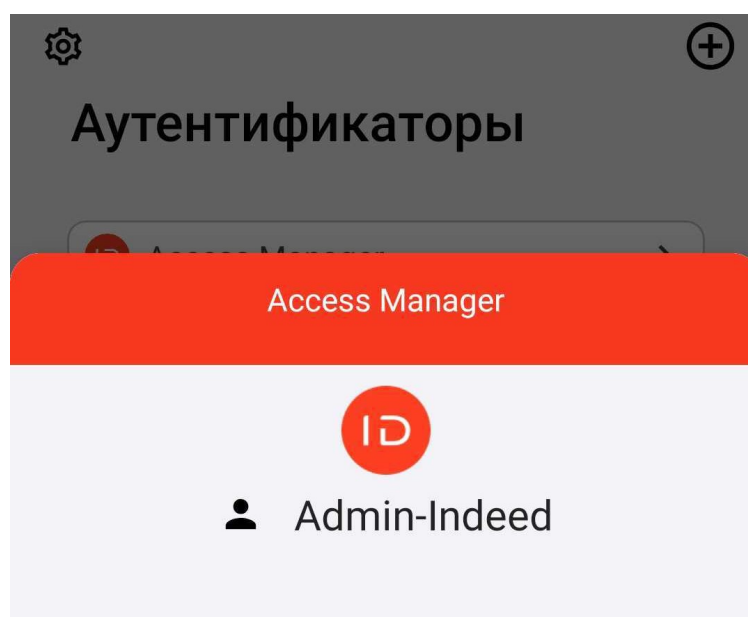
 Информация

В параметре **id** тега **add** укажите уникальный идентификатор, указанный в пункте **Доверенный ID Indeed Key Server**, в консоли администрирования.

Пример

```
<trustedClientsSettings>
  <trustedClients>
    <add id="1" />
  </trustedClients>
</trustedClientsSettings>
```


3. После применения параметров пользователь будет получать уведомления об удалении ключа.



Удаление аутентификатора

Дата и время

08 июля 2022, 09:27

Сообщение

Аутентификатор был удалён на сервере
Access Manager

Настройка приложения на смартфоне

Установка сертификата УЦ

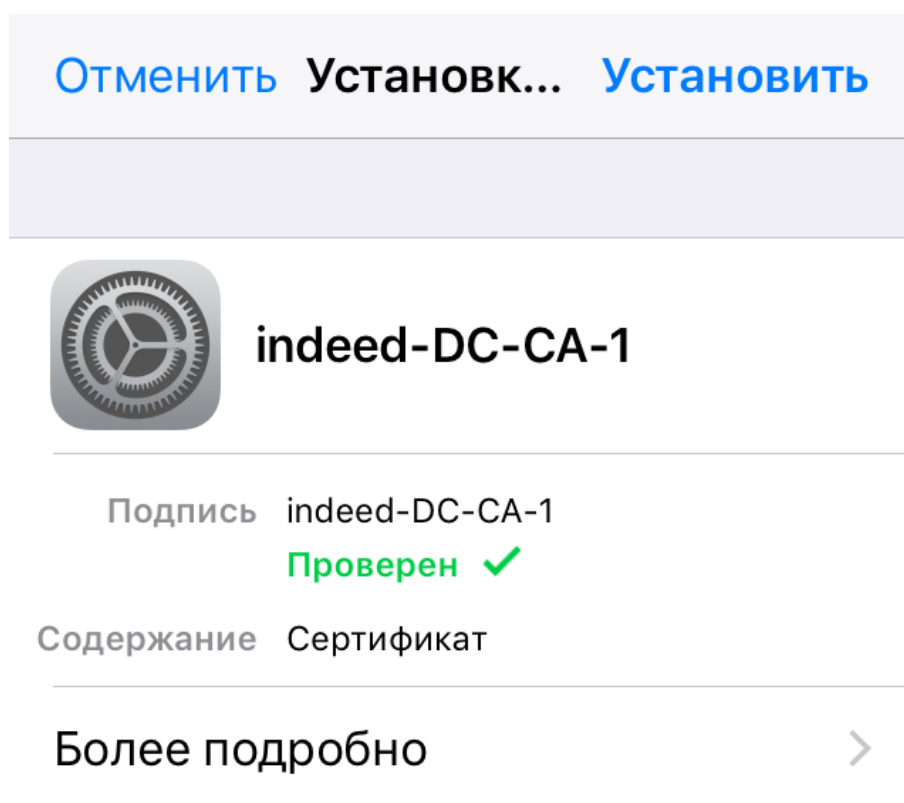
Информация

Установка сертификата УЦ необходима, только если для сервера AirKey используется доменный сертификат. При использовании сертификата общедоступного УЦ выполнять настройку не требуется.

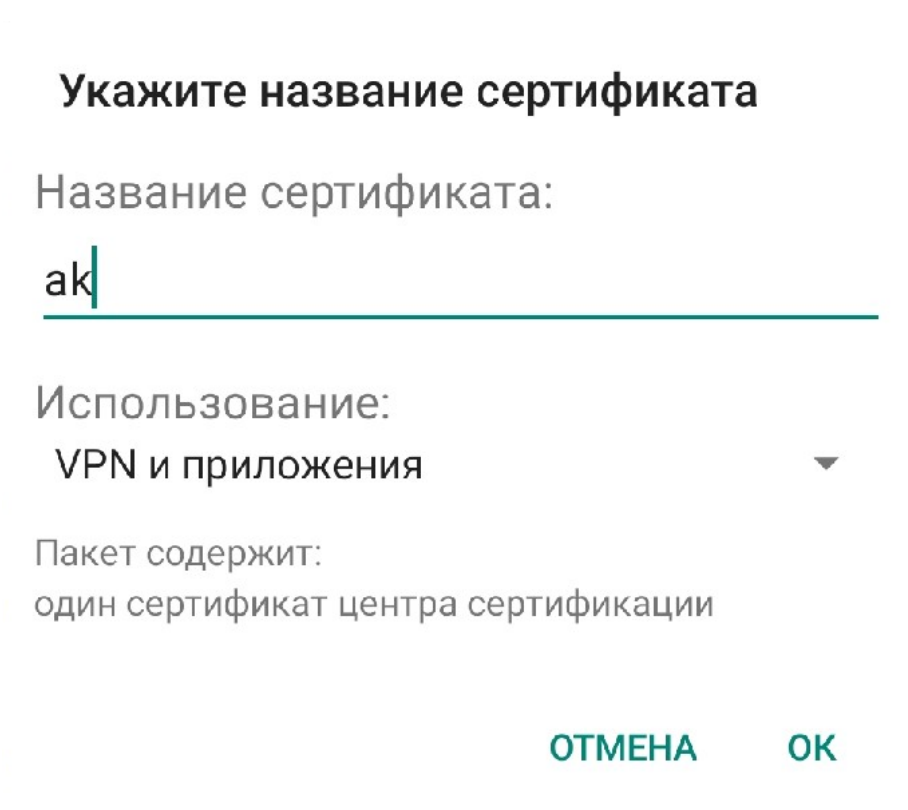
1. Экспортируйте корневой сертификат в формате **cer/crt**, **pfx/p12** не распознается как корневой сертификат.

2. Отправьте сертификат на смартфон и установите его.

а. Пример запроса на установку сертификата на IOS устройствах.

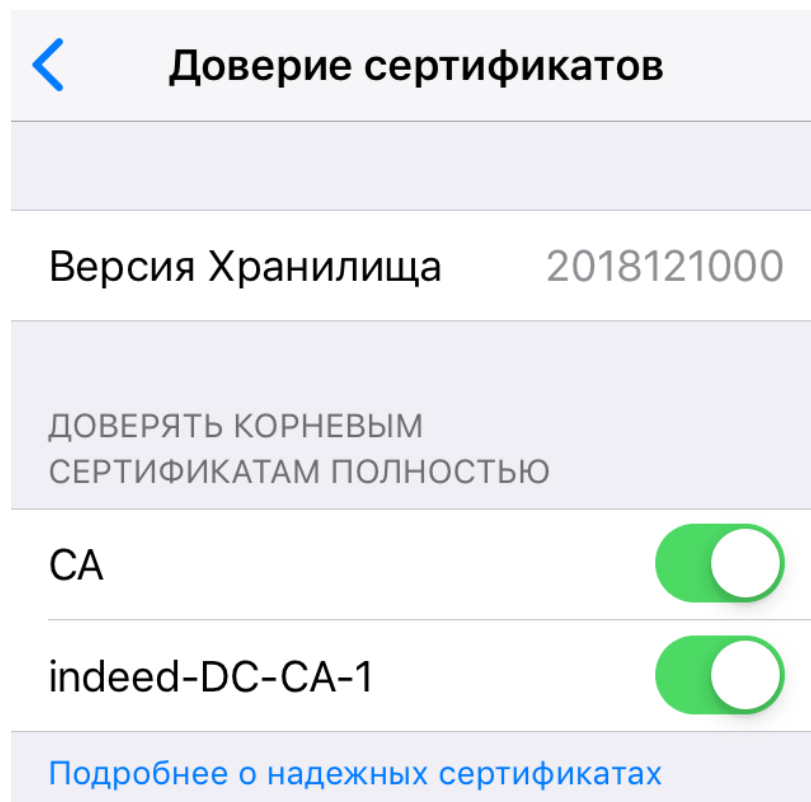


б. Пример запроса на установку сертификата на Android устройствах. Для установки укажите произвольное название сертификата и в пункте "Использование" выберите: "VPN и приложения".



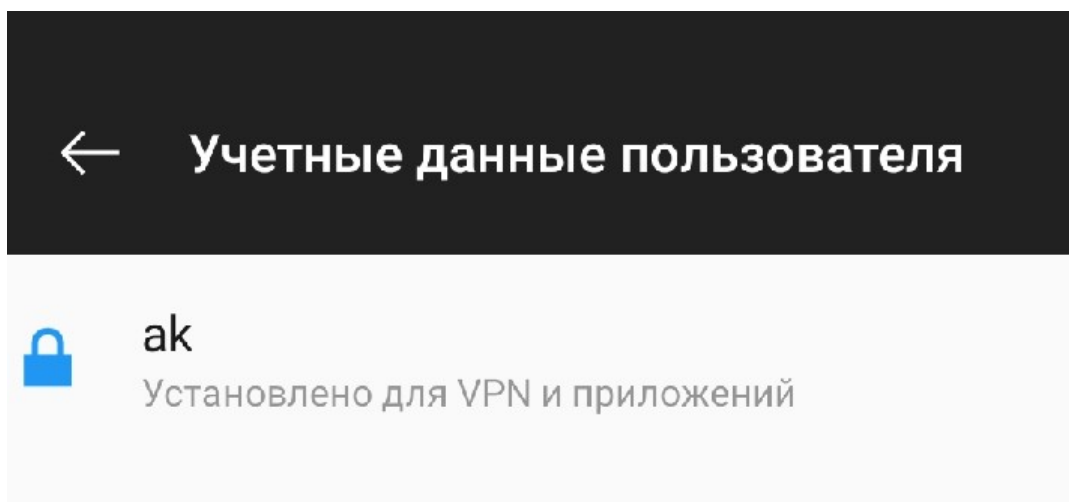
3. Добавить сертификат в доверенные.

- а. Для IOS устройств откройте: **Настройки Основные Об этом устройстве Доверие сертификатов**. В группе "Доверять корневым сертификатам полностью" включите доверие к установленному сертификату.

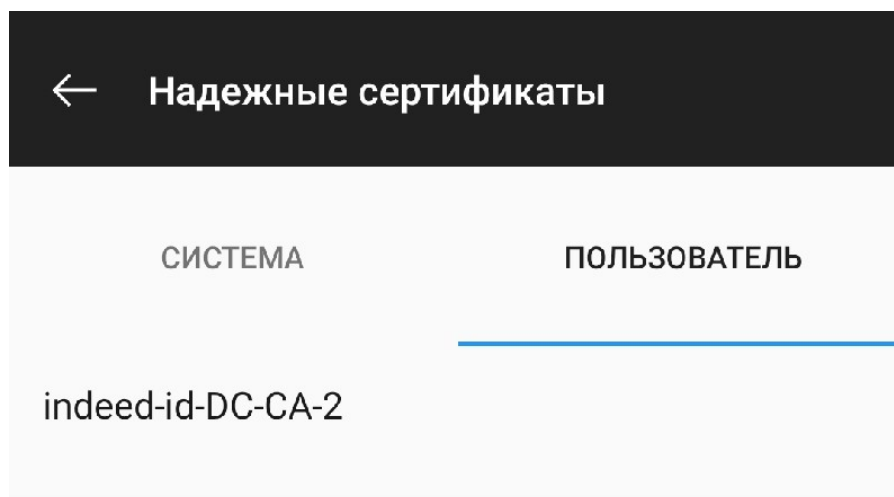


б. Для Android устройств откройте: **Настройки** **Безопасность и блокировка экрана** **Шифрование и учетные данные**

- Убедитесь что в радел "Учетные данные пользователя" успешно добавлен сертификат.



- Убедитесь что в раздел "Надежные сертификаты Пользователь" успешно добавлен сертификат.



Установка приложения

Приложение Indeed Key доступно для смартфонов с iOS 13.0 и выше, Android 7.0 и выше.

Для того, чтобы скачать приложение, воспользуйтесь следующими ссылками:

- App Store — <https://apps.apple.com/us/app/indeed-key/id1541323258>
- Google Play — <https://play.google.com/store/apps/details?id=com.indeedid.key>
- Huawei AppGallery — <https://appgallery.huawei.com/app/C106522471>

❗ Корректная работа приложения Indeed Key гарантируется только в том случае, если оно скачано из официальных магазинов приложений.



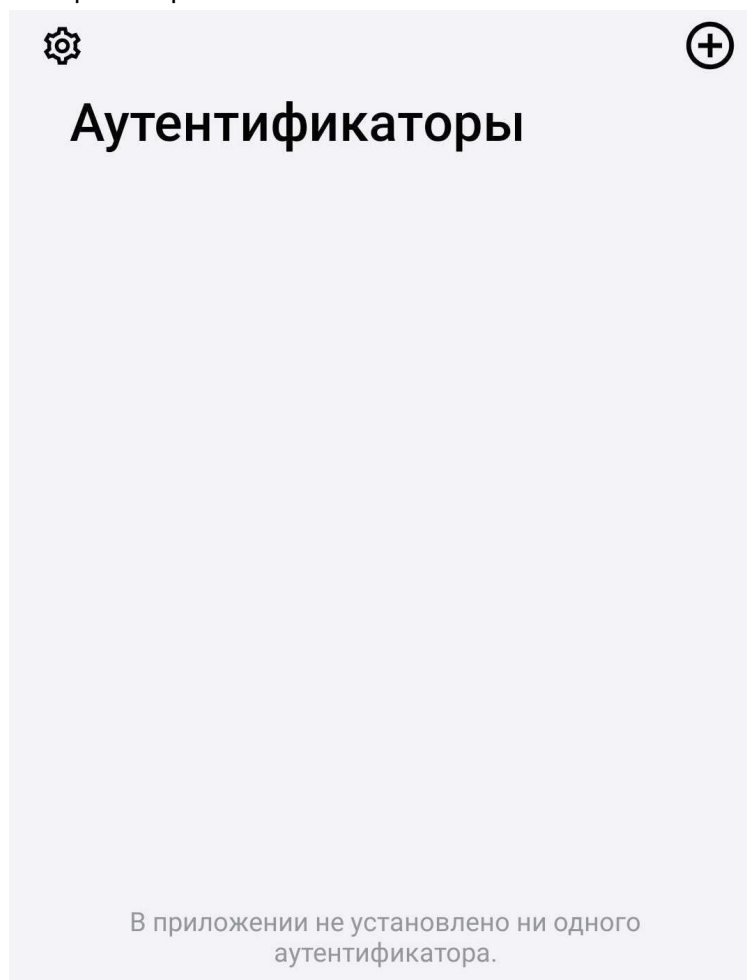
Информация

Для корректной работы Push уведомлений на Android устройствах убедитесь, что выполнены следующие обязательные требования:

1. Вы разрешили приложению отправку уведомлений
2. Для версии Android 9 и выше необходимо отключить режим энергосбережения.

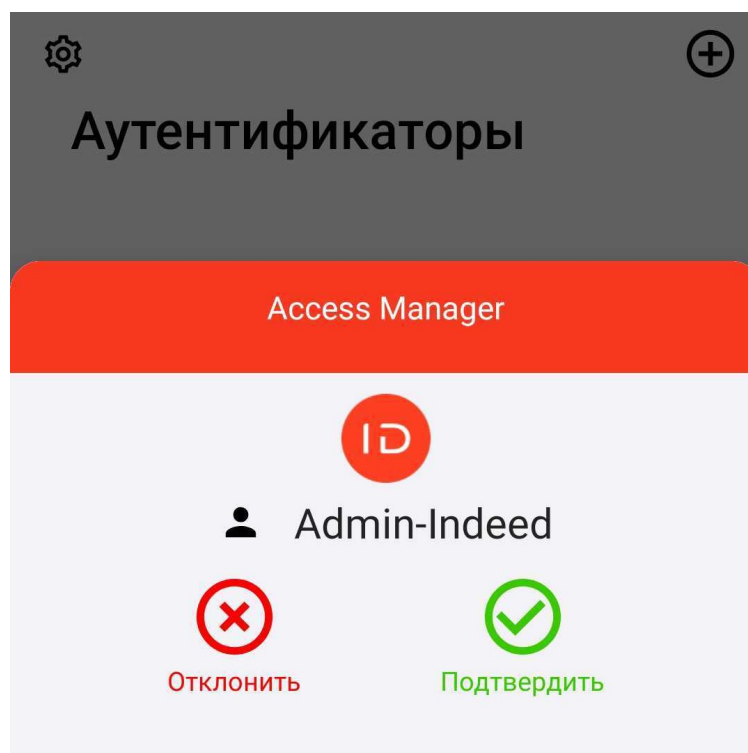
Примечание: корректная работа Push-уведомлений возможна не на всех модификациях Android.

1. Откройте приложение. В панели "**Аутентификаторы**" нажмите на значок "+" для добавления аутентификатора.



2. Разрешите приложению доступ к камере и отсканируйте QR код.

3. Подтвердите регистрацию аутентификатора нажав кнопку "Принять".



Регистрация аутентификатора

Дата и время

08 июля 2022, 09:28

Сообщение

Подтвердите создание аутентификатора

4. После успешной регистрации аутентификатор будет отображаться на главном окне программы.



Аутентификаторы



Access Manager

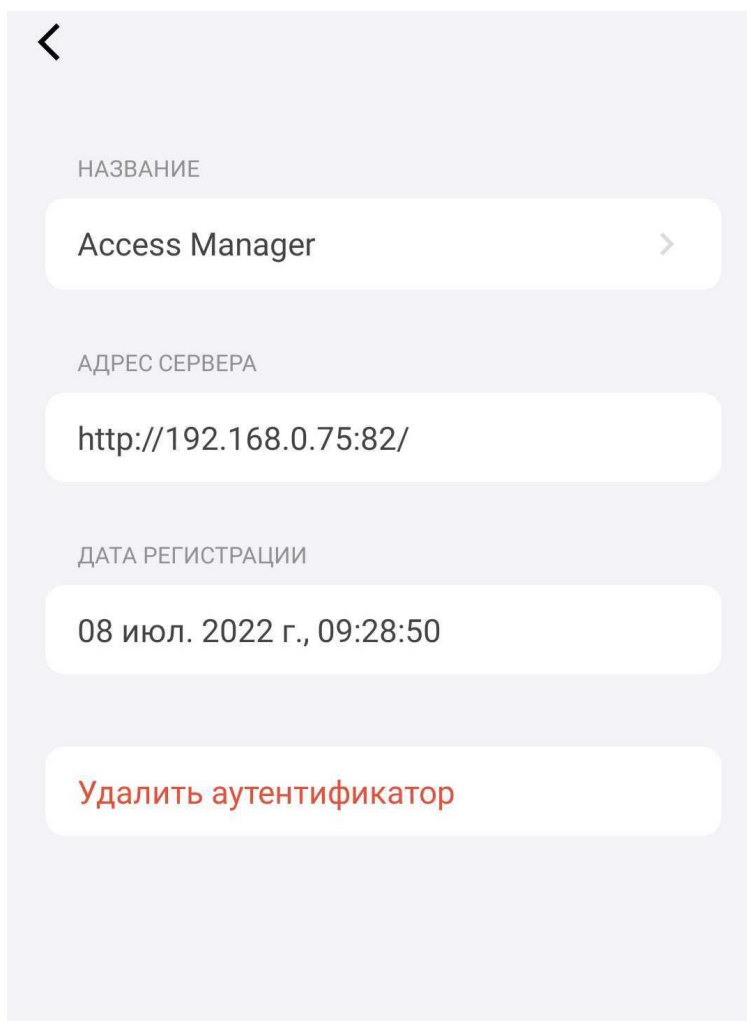


Admin-Indeed



Коснитесь, чтобы увидеть одноразовый
пароль

- а. Для удаления нажмите на необходимый аутентификатор и выберите **"Удалить аутентификатор"**.



Настройка параметров аутентификации

Информация

Перед настройкой групповой политики необходимо добавить в список административных шаблонов шаблоны политик Indeed AM. Файлы шаблонов политик входят в состав дистрибутива провайдера и расположены в каталоге Misc.

Информация

Политики распространяются на машины с установленными компонентами Indeed AM Windows Logon и Indeed AM ESSO Agent.

Таймаут операции для приложения AirKey

Политика определяет время ожидания операции для приложения AirKey.

Таймаут операции для приложения AirKey

Предыдущий параметр Следующий параметр

☐ Не задано ☒ Включено ☐ Отключено

Комментарий:

Требования к версии: Windows 8.1\10 (x64)

Параметры:

Таймаут операции (в секундах): 60

Справка:

Политика определяет время ожидания операции для приложения AirKey.

ОК Отмена Применить

Требовать команды от пользователя

Политика указывает ждать команды от пользователя для активации процедуры входа.

Требовать команды от пользователя

Требовать команды от пользователя

Предыдущий параметр Следующий параметр

☐ Не задано Комментарий:

☒ Включено

☐ Отключено

Требования к версии: Windows 8.1\10 (x64)

Параметры:

Справка:

Политика указывает ждать команды от пользователя для активации процедуры входа.

OK Отмена Применить

Аутентификация



Admin-Indeed (INDEED\Admin-Indeed)



Ожидание подтверждения

Вход

- [Выбрать другого пользователя](#)
- [Сменить способ входа](#)

EN [Отмена](#)

Настройка защиты от спама



Описание работы

Осуществляется оценка процента успешных входов относительно всех отправленных сообщений за указанный интервал времени (оценка осуществляется только если кол-во отправленных сообщений превышает "Окно оценки").

При обнаружении атаки блокируется дальнейшая отправка сообщений, при попытке входа возникает ошибка: `Potential spam attack detected`.

Отправка возобновится спустя некоторое время когда будет превышен необходимый порог успешных входов за указанный интервал времени. Максимальное время блокировки равно временному интервалу оценки.

Чтобы настроить защиту от спама:

1. Откройте **редактор реестра**;
2. Создайте раздел **Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-Id\BSPs\AirKey\SpamProtection**;
3. Создайте необходимые параметры:
 - a. **SpamProtectionEnabled**: Флаг включения защиты от спама (DWORD). Значение по умолчанию: 0
 - b. **TimeSpanSec**: Интервал времени (сек), по которому осуществляются расчеты (DWORD). Значение по умолчанию: 600
 - c. **EvaluationWindow**: Окно оценки (DWORD). Значение по умолчанию: 10
 - d. **MinSuccessfulLogonPercent**: Минимальный процент успешных входов относительно всех отправленных сообщений (DWORD). Значение по умолчанию: 20



События лог-сервера

2090: Обнаружена потенциальная спам-атака. Отправка сообщений приостановлена.

1118: Отправка сообщений пользователям возобновлена.

Indeed AM MFA Provider

ID провайдера

{070719BA-EB57-4EA8-BB4D-D15A33E7363D}

Информация

Файлы для провайдера Indeed AM MFA Provider расположены: ***indeed AM <Номер версии>\Indeed AM Providers\Indeed AM MFA Provider***

- **Server\<Номер версии>\IndeedAM.AuthProviders.MFA-<номер версии>.x64.ru-ru.msi**- Пакет для установки Indeed AM MFA Provider на сервер Indeed AM на 64-х битных ОС.
- **Server\<Номер версии>\IndeedAM.AuthProviders.MFA-<номер версии>.x86.ru-ru.msi**- Пакет для установки Indeed AM MFA Provider на сервер Indeed AM на 86-х битных ОС.
- **Client\<Номер версии>\IndeedID.MFA.Provider.msi** - Пакет для установки Indeed AM MFA Provider на клиентские машины.

Файлы шаблонов политик расположены: ***indeed AM <номер версии>\Misc\ADMX Templates***.

Indeed AM MFA Provider

Данный провайдер позволяет задать последовательность методов аутентификации в цепочке многофакторной аутентификации в компонентах Indeed AM Windows Logon и Indeed AM ESSO Agent.

Важно

Каждый идентификатор в параметре **Цепочка многофакторной аутентификации** обязательно указывайте в фигурных скобках и с новой строки.

Подробнее в разделе [Настройка параметров аутентификации](#).

Установка

1. Выполнить установку MFA Provider и провайдеров, которые будут использованы в цепочке, на сервере Indeed AM и на клиентской машине через запуск соответствующих пакетов из дистрибутива.



Информация

Если в инфраструктуре используется несколько серверов Indeed AM, то установку провайдера необходимо выполнить на всех серверах инфраструктуры.

2. После завершения установки может потребоваться перезагрузка системы. Если программа установки предлагает выполнить перезагрузку, подтвердите данное действие.
3. Удаление/Восстановление продукта осуществляется стандартным для поддерживаемых ОС способом, через меню Панель управления.

Настройка параметров аутентификации

Перед настройкой групповой политики необходимо добавить в список административных шаблонов шаблоны политик Indeed AM. Файлы шаблонов политик входят в состав дистрибутива провайдера и расположены в каталоге Misc.



Политика должна быть применена **на все серверы Indeed AM и на все клиентские машины**.

Настройка через GPO

1. Откройте политику **"Настройки цепочки многофакторной аутентификации"**. Политика располагается по пути: Административные шаблоны Indeed-ID Id Providers MFA
2. Установите значение политики в **"Включено"**.

3. В параметре "Цепочка многофакторной аутентификации" укажите ID провайдеров аутентификации, которые будут использоваться в цепочке. Каждый идентификатор указывайте в фигурных скобках и с новой строки без пробелов и других символов.



Информация

Запрещённый для использования провайдер может быть использован в цепочке провайдера MFA.



Пример

Пример цепочки Indeed AM Passcode + Indeed AM SMS OTP:

{F696F05D-5466-42b4-BF52-21BEE1CB9529}

{EBB6F3FA-A400-45F4-853A-D517D89AC2A3}



Информация

Список ID поддерживаемых провайдеров:

{EBB6F3FA-A400-45F4-853A-D517D89AC2A3} - **SMS OTP**

{F696F05D-5466-42b4-BF52-21BEE1CB9529} - **Passcode**

{0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0} - **Software OTP**

{CF189AF5-01C5-469D-A859-A8F2F41ED153} - **Windows Password**

{CB5109DA-B575-422C-8805-524FE12B02F5} - **Z2 USB**

{A0EF00AD-1EEB-4D48-8BCF-06E19CD5585F} - **Futronic**

{0AF65AD8-DB77-4B64-B489-958D9B36E28C} - **Смарт-карта или USB-ключ**

{4B15AF52-A795-4CA6-B7CD-CDB8ABF2D2C2} - **HID OMNIKEY**

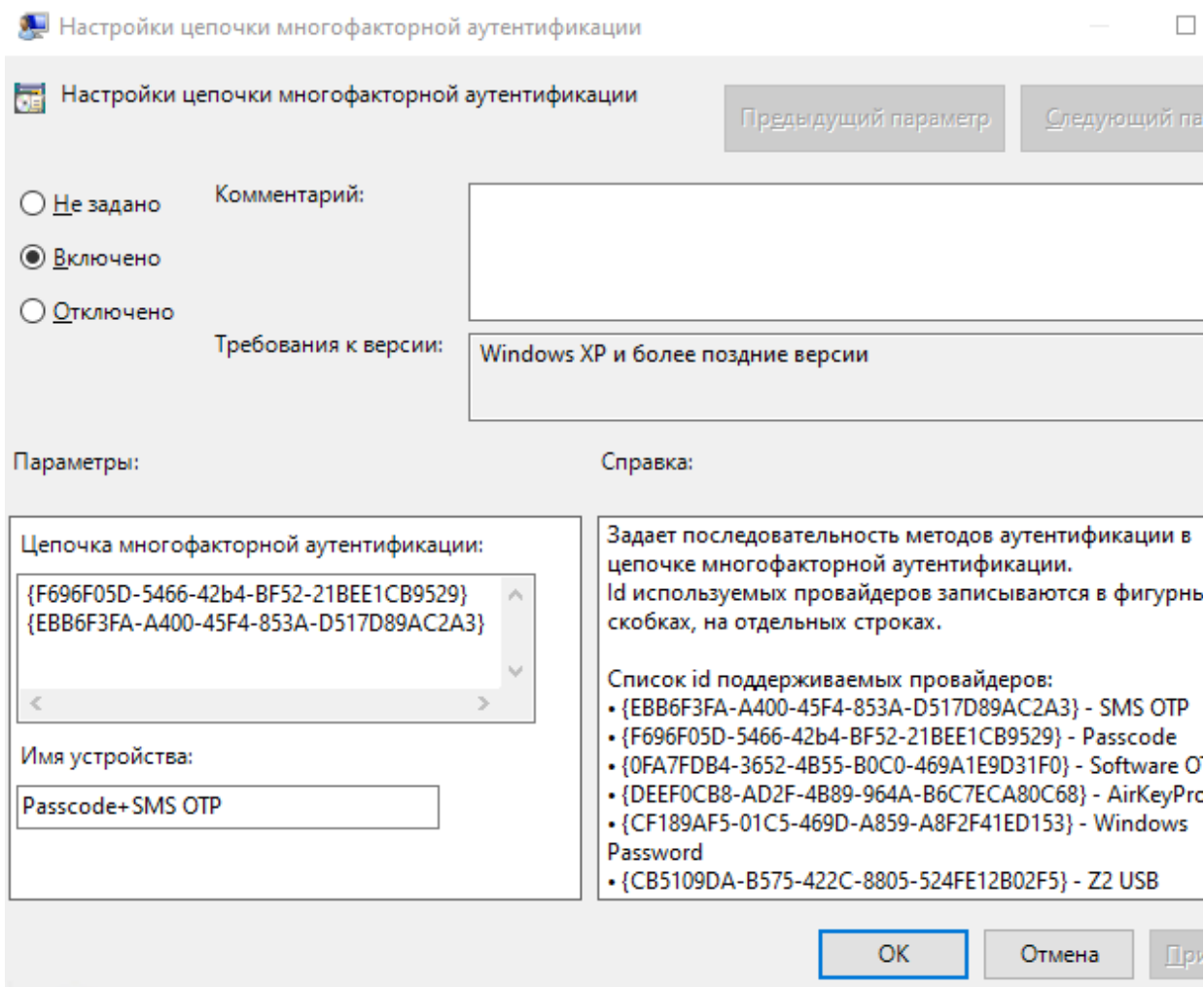
{DEEF0CB8-AD2F-4B89-964A-B6C7ECA80C68} - **Indeed Key**

{AD3FBA95-AE99-4773-93A3-6530A29C7556} - **Hardware HOTP**

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.



Настройки цепочки многофакторной аутентификации

Предыдущий параметр Следующий параметр

☐ Не задано Комментарий:

☒ Включено

☐ Отключено Требования к версии: Windows XP и более поздние версии

Параметры: Справка:

Цепочка многофакторной аутентификации:

{F696F05D-5466-42b4-BF52-21BEE1CB9529}

{EBB6F3FA-A400-45F4-853A-D517D89AC2A3}

Имя устройства: Passcode+SMS OTP

Задаёт последовательность методов аутентификации в цепочке многофакторной аутентификации. Id используемых провайдеров записываются в фигурные скобки, на отдельных строках.

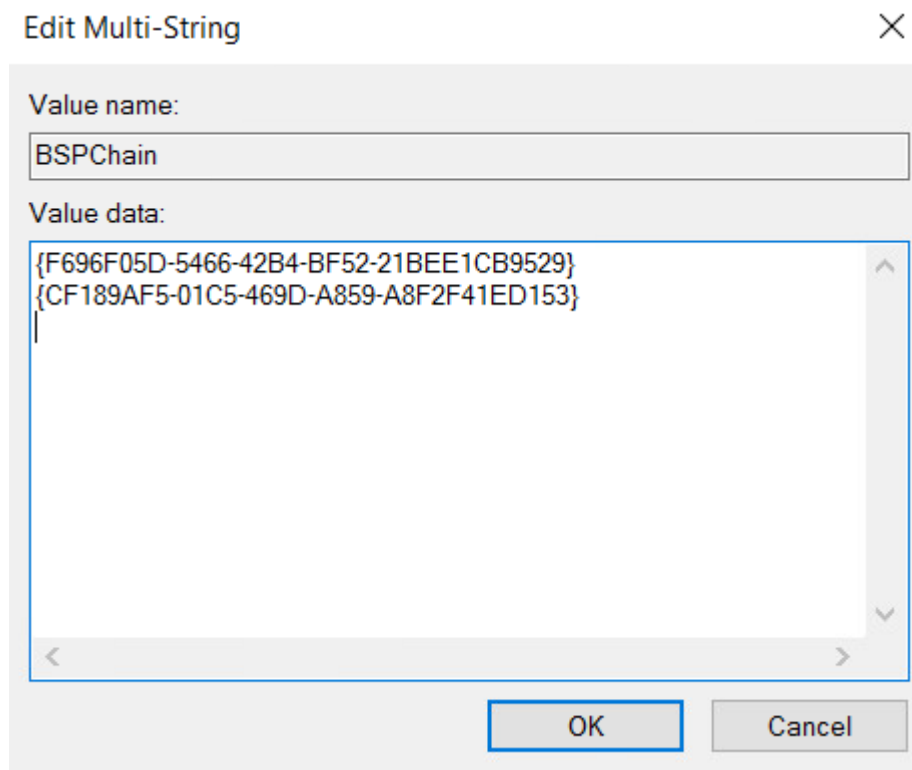
Список id поддерживаемых провайдеров:

- {EBB6F3FA-A400-45F4-853A-D517D89AC2A3} - SMS OTP
- {F696F05D-5466-42b4-BF52-21BEE1CB9529} - Passcode
- {0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0} - Software O
- {DEEF0CB8-AD2F-4B89-964A-B6C7ECA80C68} - AirKeyPrc
- {CF189AF5-01C5-469D-A859-A8F2F41ED153} - Windows Password
- {CB5109DA-B575-422C-8805-524FE12B02F5} - Z2 USB

OK Отмена При

Настройка через реестр

1. Откройте редактор реестра на сервере Indeed AM.
2. Откройте раздел **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\BSPs\MFA**.
3. Создайте параметр **BSPChain** типа **REG_MULTI_SZ** и укажите ID провайдеров аутентификации, которые будут использоваться в цепочке. Каждый идентификатор указывайте в фигурных скобках и с новой строки без пробелов и других символов.



4. Создайте параметр **MFADeviceName** типа **REG_SZ** и укажите имя для созданной цепочки.

Indeed-ID

Intel

Microsoft

Mozilla

Notepad++

ODBC

Partner

pgAdmin 4

Policies

Google

Indeed-Id

BSPs

AirKey

EncryptedSoftwareTOTP

GoogleOTP

HardwareTOTP

HOTP

MFA

Passcode

SMSOTP

SMTP

SoftwareHOTP

TelegramOTP

Name	Type	Data
(Default)	REG_SZ	(value not set)
BSPChain	REG_MULTI_SZ	{F696F05D-5466-42B4-BF52-21BEE1CB...
MFADeviceName	REG_SZ	MFA

Аутентификация при помощи Indeed AM MFA



Информация

В данном примере используется компонент Indeed AM Windows Logon и цепочка провайдеров Indeed AM Passcode + Indeed AM SMS OTP.

1. Выберите провайдер аутентификации "**Многофакторная аутентификация**".

Вход в Windows



Admin-Indeed (INDEED\Admin-Indeed)

- [AirKey](#)
- [Многофакторная аутентификация](#)
- [Одноразовый пароль](#) (Google Authenticator)
- [Одноразовый пароль](#) (Google Authenticator + PIN)
- [Одноразовый пароль](#) (SMS OTP)
- [Панель](#)

RU [Отмена](#)

2. Введите данные для первого провайдера в цепочке.

Вход в Windows



Admin-Indeed (INDEED\Admin-Indeed)

Введите пароль Passcode



••••••••

Вход

[→ Сменить способ входа](#)

EN [Отмена](#)

3. Введите данные для второго провайдера в цепочке.

Вход в Windows



Admin-Indeed (INDEED\Admin-Indeed)

Введите одноразовый пароль, полученный в SMS



[→ Сменить способ входа](#)

[EN](#) [Отмена](#)

4. Выполните вход.

Модули интеграции



Информация

Для использования модулей интеграции требуются соответствующие лицензии.



Информация

Файлы шаблонов политик для модулей интеграции расположены: ***indeed AM <Номер версии>\ADMX Templates***

Необходимые файлы шаблонов для локальной групповой политики нужно скопировать на целевой машине в ***C:\Windows\PolicyDefinitions***

Необходимые файлы шаблонов для доменной групповой политики нужно скопировать на контроллере домена в ***C:\Windows\SYSVOL\sysvol\<Имя домена>\Policies\PolicyDefinitions***

Модули интеграции системы Indeed AM 8.1:

- [Indeed AM Identity Provider](#)
 - [Интеграция с приложениями по протоколам OpenID Connect и OAuth 2.0](#)
 - [Интеграция с приложениями по протоколу SAML](#)
 - [Аутентификация по имени пользователя без указания домена](#)
 - [Включение защиты от перебора](#)
- [Indeed AM ADFS Extension](#)
 - [Indeed AM ADFS Extension \(2012\)](#)
 - [Indeed AM ADFS Extension \(2016\)](#)
- [Indeed AM ESSO Agent](#)
- [Indeed AM IIS Extension](#)
- [Indeed AM NPS RADIUS Extension](#)
- [Indeed AM RDP Windows Logon](#)
- [Indeed AM Windows Logon](#)
- [Indeed AM SAML IDP](#)

Indeed AM Identity Provider

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

Начиная с версии Indeed AM Access Manager 8.1.5, модуль Indeed AM Identity Provider поддерживает следующие протоколы:

- [OpenID Connect](#) и [OAuth 2.0](#)
- [SAML](#)



Важно

Если вы пользуетесь Indeed AM Access Manager 8.1.4 и ниже, необходимую информацию об установке и настройке модуля вы найдете на странице [Indeed AM SAML IDP](#).

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.

Identity Provider поддерживает следующие технологии аутентификации пользователей в любых сочетаниях:

- доменный пароль
- одноразовые пароли OATH, TOTP и HOTP
- одноразовые коды через SMS и email
- мобильное приложение Indeed Key

Подготовка к установке

Перед установкой Identity Provider убедитесь, что на сервере установлен .NET 6 и необходимые компоненты Internet Information Services.



Примечание

Корректная работа Identity Provider гарантируется только при использовании .NET 6.

Для установки .NET запустите утилиту *dotnet-hosting-6.0.10-win.exe* из *Indeed AM <номер версии>/Indeed AM Idp*.

Для установки компонентов Internet Information Services запустите скрипт *Indeed.SAML.IIS.Install.MSSserver.ps1* из *Indeed AM <номер версии>/Misc/IISScripts*.

В папке *Indeed AM <номер версии>/Indeed AM Idp* расположены следующие файлы:

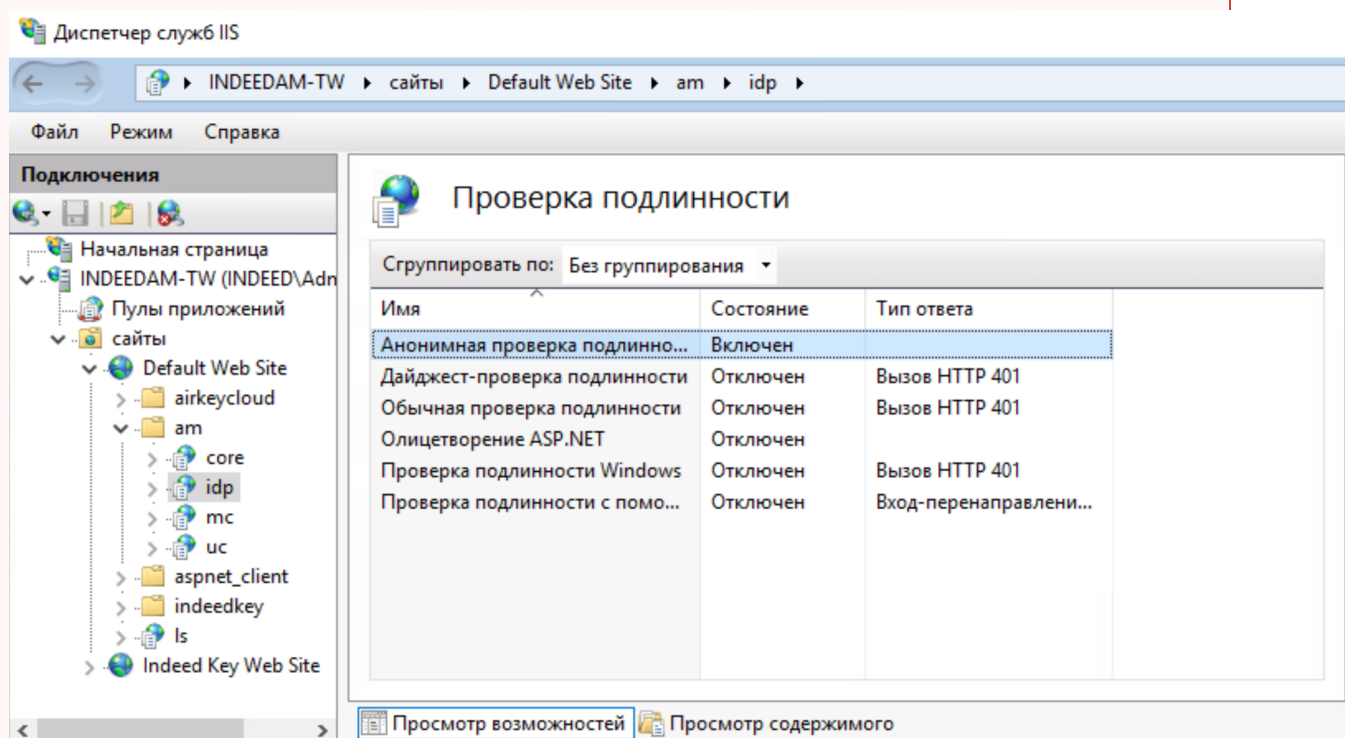
- *IndeedAM.IDP-v8.1.5.x64.ru-ru.msi* — пакет для установки Identity Provider.
- *AccessManager.Tools.Importer.Services.Console.x64.exe* — утилита для обновления Indeed AM SAML IDP до Identity Provider.
- *dotnet-hosting-6.0.10-win.exe* — утилита для установки .NET.

❗ Информация

По умолчанию Identity Provider использует аутентификацию Windows. Для внедоменных сценариев включите анонимную аутентификацию.

Для этого выполните следующие действия:

1. В Диспетчере служб IIS в меню слева выберите **Indeed AM сайты Default Web Siteamidp** и нажмите значок **Проверка подлинности**.
2. Включите опцию **Анонимная проверка подлинности**, остальные опции оставьте выключенными.



Установка пакета

Чтобы установить и настроить Identity Provider, выполните следующие действия:

1. Установите пакет IndeedAM.IDP-v8.1.5.x64.ru-ru.msi.

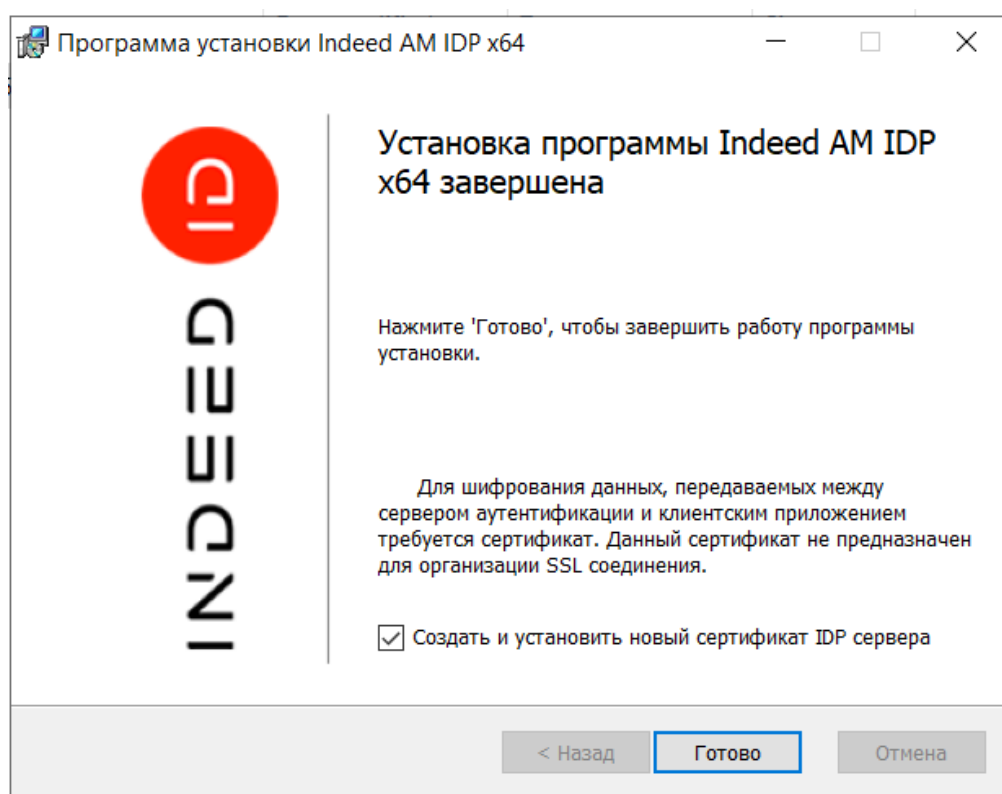


Информация

По умолчанию после установки пакета создается и устанавливается новый сертификат сервера IDP. Сертификат шифрует данные, передаваемые между сервером Indeed AM Access Manager и конечными приложениями, например консолью администратора.

Сертификат не предназначен для организации соединения по протоколу SSL.

Если сертификат был сгенерирован ранее, уберите флажок **Создать и установить новый сертификат IDP сервера**.



2. Добавьте привязку в настройках IIS.

- a. Запустите Диспетчер служб IIS и выберите **Сайты** (Sites).
- b. Выберите **Default Web Site** и нажмите **Привязки** (Bindings) в разделе **Действия** (Actions).
- c. Нажмите **Добавить** (Add):
 - i. **Тип** (Type) — https.
 - ii. **Порт** (Port) — 443.
 - iii. Выберите **SSL-сертификат** (SSL Certificate).
- d. Сохраните привязку.

Информация

Identity Provider — это веб-приложение, которое работает на базе IIS. По требованиям безопасности Identity Provider работает только по протоколу HTTPS. Не меняйте протокол, это снижает безопасность соединения.

Если вы планируете использовать соединение по протоколу HTTP, измените настройки в файле *Web.config* из *C:\inetpub\wwwroot\am\idp*.

В теге *aspNetCore* добавьте следующее:

```
<environmentVariables>
  <environmentVariable name="ASPNETCORE_ENVIRONMENT" value="Development" />
</environmentVariables>
```

Должно получиться следующее:

```
<aspNetCore processPath="dotnet" arguments=".\\AM.IDP.dll" stdoutLogEnabled="false"
stdoutLogFile=".\logs\stdout" hostingModel="inprocess">
  <environmentVariables>
    <environmentVariable name="ASPNETCORE_ENVIRONMENT" value="Development" />
  </environmentVariables>
</aspNetCore>
```

Редактирование конфигурационного файла

В конфигурационном файле *app-settings.json* выполните следующие действия:

1. Откройте конфигурационный файл *app-settings.json* из *C:\inetpub\wwwroot\am\idp*.

2. Измените параметр *AuthenticationServer*. В строке *Url* укажите адрес сервера в формате *http(s)://полное_dns_имя_сервера/am/core/*.

```
"AuthenticationServer": {  
  "Url": "AUTH_SERVER_URL",  
  "IsIgnoreCertErrors": false  
}
```

Пример адреса сервера

`https://server.test.local/am/core/`



Информация

Если вы используете соединение по протоколу HTTPS, вам необходимо установить клиентский сертификат на каждый сервер Indeed AM.

Чтобы ошибки сертификата сервера игнорировались, измените значение параметра *IsIgnoreCertErrors* на значение *true*.

3. Измените параметр *Server*. В строке *Url* укажите адрес для подключения к Indeed AM Log Server в формате *http(s)://полное_dns_имя_сервера/ls/api*.

```
"Server": {  
  "Url": "LOG_SERVER_URL"  
}
```

Пример адреса сервера Indeed AM Log Server

`https://server.test.local/ls/api/`

4. Измените параметр *LocalIdentityProviderConfiguration*:

- а. В строке *SingleSignOnServiceUrl* укажите адрес Identity Provider в формате *http(s)://полное_dns_имя_сервера/am/idp/Account/SsoService*.

```
"LocalIdentityProviderConfiguration": {  
  "Name": "urn:indeedid:saml_idp",  
  "SingleSignOnServiceUrl": "IDENTITY_PROVIDER_URL/Account/SsoService"
```

Пример адреса сервера SSO

`https://server.test.local/am/idp/Account/SsoService`

- б. В строке *Thumbprint* укажите отпечаток сертификата Identity Provider, который был сгенерирован при установке.

```
"LocalIdentityProviderConfiguration": {  
  "LocalCertificates": [  
    {  
      "Thumbprint": ""  
    }  
  ]  
}
```

 Информация

Вы можете найти сертификат в хранилище *Local MachinePersonalCertificates* (сертификат с именем *idp*), либо получить с помощью запроса PowerShell:

```
Get-Childitem Cert:\LocalMachine\My\ | Where-Object {$_.Subject -eq  
"CN=idp"}
```

5. 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* — идентификатор используемого провайдера.

Доступные идентификаторы для Identity Provider

Identity Provider поддерживает следующие провайдеры:

- 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
- HOTP Provider — AD3FBA95-AE99-4773-93A3-6530A29C7556
- TOTP Provider — CEB3FEAF-86ED-4A5A-BD3F-6A7B6E60CA05
- AirKeyProvider — DEEF0CB8-AD2F-4B89-964A-B6C7ECA80C68
- Windows Password — CF189AF5-01C5-469D-A859-A8F2F41ED153
- Telegram OTP — CA4645CC-5896-485E-A6CA-011FCC20DF1D

- а. Если для аутентификации используется один провайдер:

Пример использования одного провайдера

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

- б. Если для аутентификации используются несколько провайдеров:

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.

6. Сохраните конфигурационный файл и перезапустите IIS.

В этом разделе

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

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 конфигурационный файл *app-settings.json*:

- *CertificateThumbprint* — указывается отпечаток сертификата Identity Provider. Сертификат загружен на компьютер, где установлен Indeed AM Identity Provider.
- *Clients* — содержит свойства клиентских приложений.
- *ClientId* — указывается идентификатор клиентского приложения.
- *ClientSecret* — указывается секрет клиентского приложения. **Важно:** в зависимости от приложения может быть захешировано или зашифровано по соображениям безопасности.
- *Permissions* — содержит разрешения приложения.
- *PostLogoutRedirectUri* — содержит допустимые URL-адреса, на которые перенаправляется пользователь после завершения сессии клиентского приложения.
- *RedirectUri* — содержит допустимые URL-адреса, на которые перенаправляется пользователь после завершения сессии клиентского приложения.
- *Requirements* — содержит дополнительные требования приложения.

Подробнее о настройке интеграции с приложениями по протоколам OpenID Connect и OAuth 2.0 вы можете прочитать в статье [Настройка OIDC на примере Keycloak](#).

Интеграция с приложениями по протоколу SAML

1. Identity Provider Login URL — *http(s)://<полное_DNS_имя_сервера_Identity_Provider>/am/idp/AssertionConsumerService*
2. Identity Provider Logout URL — *http(s)://<полное_DNS_имя_сервера_Identity_Provider>/am/idp/Logout*
3. Identity Provider Name — *urn:indeedid:saml_idp*

Для интеграции Identity Provider с приложениями по протоколу SAML используйте следующие параметры файла *app-settings.json*:

- *SingleSignOnServiceUrl* — содержит URL-адрес Single SignOn Service, который получает сообщения SAML от приложения.
- *LocalCertificates* — указывается сертификат Identity Provider. Сертификат загружается в хранилище сертификатов развернут Indeed AM Identity Provider. Сертификат указывается в параметре *Thumbprint*.
- *SingleLogoutServiceUrl* — содержит URL-адрес Single Logout, который получает сообщения SAML от 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 подписан. 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*.
- *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, отправляемые клиентскому приложению, на выход из клиентского приложения. Рекомендуемое значение: *true*.
- *WantLogoutResponseSigned* — параметр указывает, должны ли быть подписаны ответы SAML, отправляемые клиентскому приложению, на выход из клиентского приложения. Рекомендуемое значение: *true*.
- *AssertionConsumerServiceUrl* — параметр содержит URL-адрес Assertion Consumer Service клиентского приложения, который получает запросы SAML.

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 *app-settings.json* из *C:\inetpub\wwwroot\am\idp*.
2. Измените параметр *AuthenticationSettings*. В строке *Domains* укажите значения необходимых доменов.

```
"AuthenticationSettings": {  
  "SessionExpirationTimeInMinutes": 30,  
  "Domains": [  
    ""  
  ]  
}
```

Пример

```
"AuthenticationSettings": {  
  "SessionExpirationTimeInMinutes": 30,  
  "Domains": [  
    "test.local",  
    "demo.local",  
    "indeed.local"  
  ]  
}
```

3. Сохраните файл и перезапустите IIS.

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 отображает способы аутентификации, запрашивая пароль. Если введен существующий пользователь через Identity Provider: отображает способы аутентификации, запрашивая пароль. Если введен существующий пользователь через Identity Provider: 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 *утренняя 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 *web.config* из *C:\inetpub\wwwroot\am\config*.
2. Измените параметр *appSettings*. В строке *bruteForceProtectionApps* укажите значение *Identity Provider*.

Пример

```
<appSettings>
  <add key="bruteForceProtectionApps" value="Identity Provider" />
  ...
</appSettings>
```

3. Сохраните изменения и перезапустите IIS.

Indeed AM ADFS Extension

- [Indeed AM ADFS Extension \(2012\)](#)
- [Indeed AM ADFS Extension \(2016\)](#)

Indeed AM ADFS Extension (2012)

Компонент **ADFS Extension** реализует провайдер мультифакторной аутентификации для сервера **Microsoft ADFS**, добавляя в процесс получения доступа второй фактор.

Информация

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

- **IndeedId.ADFS.Extension-<номер версии>.x64.ru-ru.msi** - Пакет для установки Indeed ADFS Extension.

Установка и настройка ADFS Extension

1. Выполните установку ADFS Extension через запуск соответствующего пакета из дистрибутива.

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

EANetServerURL - адрес AM Server.

ModelId - идентификатор используемого метода аутентификации.



Информация

ModelId может иметь разные **ID** провайдеров:

{EBB6F3FA-A400-45F4-853A-D517D89AC2A3} - **SMS OTP**

{093F612B-727E-44E7-9C95-095F07CBB94B} - **EMAIL OTP**

{F696F05D-5466-42b4-BF52-21BEE1CB9529} - **Passcode**

{0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0} - **Software OTP**

{AD3FBA95-AE99-4773-93A3-6530A29C7556} - **HOTP Provider**

{CEB3FEAF-86ED-4A5A-BD3F-6A7B6E60CA05} - **TOTP Provider**

{DEEF0CB8-AD2F-4B89-964A-B6C7ECA80C68} - **AirKey Provider**

Пример

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



Информация

При использовании https соединения требуется выполнить [установку клиентского сертификата](#) на каждый сервер Indeed AM.

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

 Информация

YourPath\MFAAdapter.json - укажите свой полный путь к конфигурационному файлу созданному ранее.

 Важно!

При регистрации, изменении или удалении адаптера необходимо выполнить перезапуск службы ADFS на каждом сервере ADFS.

 Информация

В переменной **\$typeName**, в параметре **Version** указывается номер версии используемого **ADFS Extension**.

Пример

```
$typeName = "IndeedId.ADFS.MFAAdapter.MFAAdapter, IndeedId.ADFS.MFAAdapter,
Version=1.0.6.0, Culture=neutral, PublicKeyToken=1ebb0d9282100d91"
Register-AdfsAuthenticationProvider -TypeName $typeName -Name "Indeed Id MFA
Adapter" -ConfigurationFilePath 'YourPath\MFAAdapter.json'
```

- а. Для регистрации нескольких провайдеров измените имя провайдера в параметре **"Name"**

Пример

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

- б. Изменить отображаемое имя провайдера. Для параметра **"Name"** указать значение из предыдущего шага, для параметра **"DisplayName"** задать имя, которое будет отображаться при выполнении аутентификации через ADFS:

Пример

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


4. Для удаления адаптера необходимо выполнить следующую команду:

Пример

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

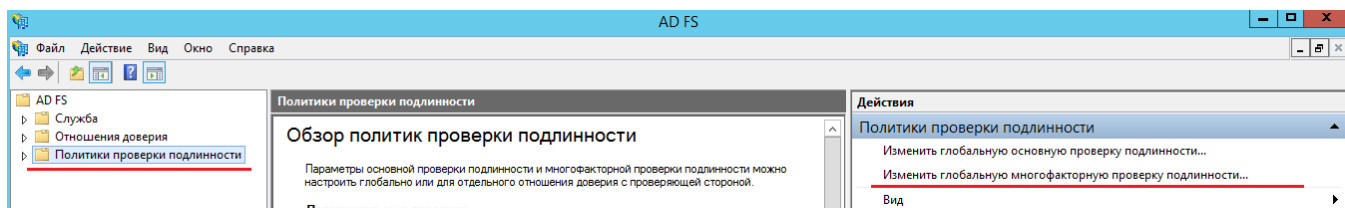
5. Для обновления конфигурации необходимо выполнить следующую команду:

Пример

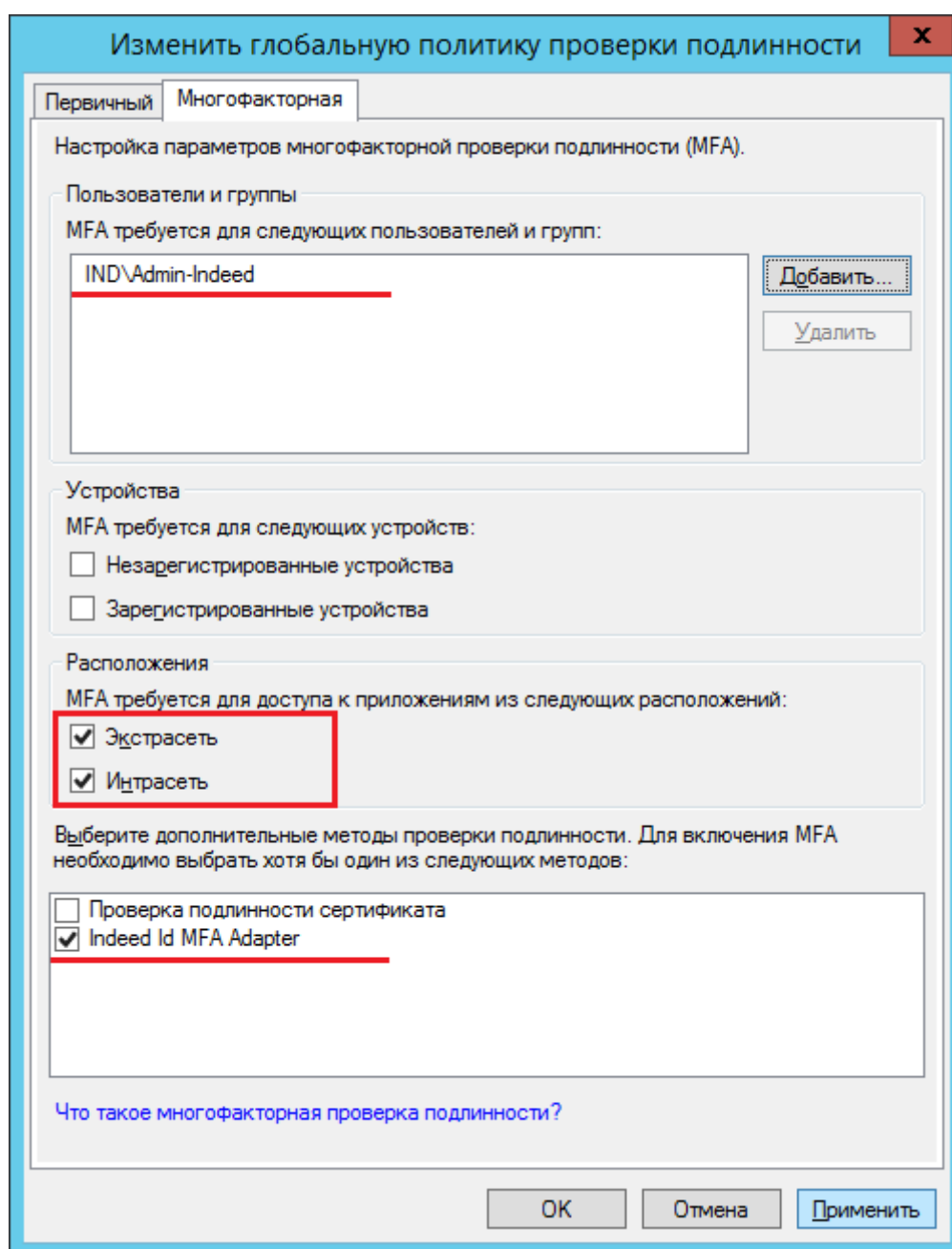
```
Import-AdfsAuthenticationProviderConfigurationData -Name "Indeed Id MFA Adapter" -  
FilePath 'YourPath\MFAAdapter.json'
```

Включение многофакторной аутентификации для ADFS

1. Откройте консоль управления AD FS.
2. Выберите "Политики проверки подлинности", в окне "Действия" выберите "Изменить глобальную многофакторную проверку подлинности..."



3. Добавьте пользователя/группу и включите следующие параметры:
 - a. В пункте "Расположение" выберите "Экстрасеть" и "Интрасеть".
 - b. Выберите использование провайдера "Indeed Id MFA Adapter".



4. Для применения изменений перезапустите службу AD FS.

Пример работы расширения

Пример работы расширения на idpinitiatedsignon странице ADFS

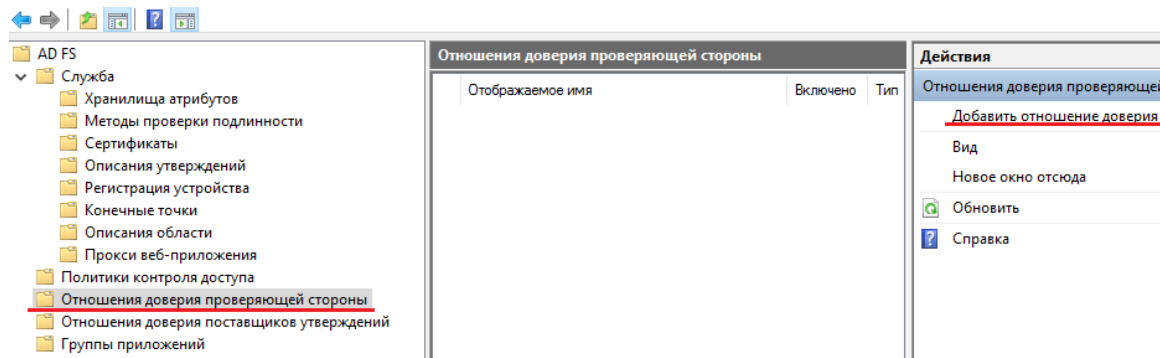


Информация

Пример работы расширения показан на странице ADFS **idpinitiatedsignon.htm**. По умолчанию данная страница не настроена (Настройка данной страницы не обязательна).

1. Настройка тестовой страницы

- а. Выберите "**Отношение доверия проверяющей стороны**" и нажмите "**Добавить отношение доверия проверяющей стороны...**".



- б. На вкладке "**Добро пожаловать!**" выберите "**Поддерживающие утверждения**" и нажмите "**Запустить**".

- с. На вкладке "**Выбор источника данных**" укажите URL адрес вашего приложения и нажмите "**Далее**".

Информация

В качестве примера работы расширения используется стандартная страница ADFS `idpinitiatedsignon.htm`. Адрес метаданных используется для данной страницы.

The screenshot shows the 'Master of adding trust relationships for the relying party' wizard. The title bar reads 'Мастер добавления отношений доверия проверяющей стороны'. The main title is 'Выбор источника данных'. On the left, a 'Шаги' (Steps) pane lists: 'Добро пожаловать!', 'Выбор источника данных' (highlighted with a red underline), 'Выбор политики управления доступом', 'Готовность для добавления отношения доверия', and 'Готово'. The main area has the instruction 'Выберите способ, используемый мастером для получения данных об этой проверяющей стороне'. There are three radio button options: 1. 'Импорт данных о проверяющей стороне, опубликованных в Интернете или локальной сети' (selected). It includes a text box for 'Адрес метаданных федерации (имя узла или URL-адрес):' containing 'https://adfsnew.indeed.local/federationmetadata/2007-06/federationmetadata.xml', and a 'Пример:' line showing 'fs.contoso.com' and 'https://www.contoso.com/app'. 2. 'Импорт данных о проверяющей стороне из файла'. It includes a text box for 'Местоположение файлов метаданных федерации:' and an 'Обзор...' button. 3. 'Ввод данных о проверяющей стороне вручную'. At the bottom right, there are three buttons: '< Назад', 'Далее >' (highlighted with a red rectangle), and 'Отмена'.

- d. На вкладке "**Указание отображаемого имени**" введите имя и описание для вашего отношения доверия и нажмите "**Далее**".

- е. 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.

The screenshot shows the 'Master of Trust Relationships' wizard in the 'Select Access Policy' step. On the left, a 'Steps' pane lists: 'Welcome!', 'Select data source', 'Specify display name', 'Select access policy' (highlighted with a red bar), 'Ready to add trust relationship', and 'Ready'. The main area is titled 'Select an access policy:' and contains a table with two columns: 'Name' and 'Description'. The first row, 'Allow for everyone and request MFA', is highlighted in blue. Below the table, a 'Policy' section shows the selected policy: 'Allow users and requires multifactor authentication'. At the bottom, there is a checkbox 'Do not configure access policies in this step. No user will have access to this application.' and two buttons: '< Back' and 'Next >', with the 'Next >' button highlighted by a red rectangle.

Имя	Описание
Разрешение для каждого и запрос MFA	Предоставьте досту
Разрешение для каждого и запрос MFA для внешних польз...	Предоставление до
Разрешение для каждого и запрос MFA для определенной г...	Предоставление до
Разрешение для каждого и запрос MFA с непроверенных у...	Предоставьте досту
Разрешение для каждого.	Предоставление до
Разрешение для определенной группы	Предоставление до
Разрешение доступа через интрасеть для каждого	Предоставьте досту
Разрешить всем и требовать MFA, разрешить автоматичес	Предоставить досту

Политика

Разрешение пользователям
и требуется многофакторная проверка подлинности

☐ Не настраивать политики управления доступом в этот раз. Ни один пользователь
доступ к этому приложению.

< Назад Далее >

- f. Остальные параметры оставьте по умолчанию.
- g. Для применения изменений перезапустите службу AD FS.

Работа расширения

- a. Откройте тестовую страницу ADFS: <https://YourDomainName/adfs/ls/idpinitiatedsignon.htm>
- b. Выполните вход.

с. После ввода доменного логин/пароля укажите данные для второго фактора.

ADFS

Добро пожаловать IND\Admin-Indeed

В целях безопасности необходимо указать
дополнительные данные для проверки учетной
записи

Indeed Id Enterprise Authentication
One Time Password

•••••

Submit

d. После корректного ввода данных будет выполнен вход.

ADFS

Вы выполнили вход.

Выход

Примеры внедрения расширения

1. [Настройка двухфакторной аутентификации для приложений опубликованных в WAP](#)
2. [Настройка двухфакторной аутентификации в AD FS для интеграции с Exchange Server 2016](#)
3. [Настройка двухфакторной аутентификации в Microsoft Office 365 при помощи Indeed AM ADFS Extension](#)

Indeed AM ADFS Extension (2016)

Компонент **ADFS Extension** реализует провайдер мультифакторной аутентификации для сервера **Microsoft ADFS**, добавляя в процесс получения доступа второй фактор.

Информация

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

- **IndeedId.ADFS.Extension-<номер версии>.x64.ru-ru.msi** - Пакет для установки Indeed ADFS Extension.

Установка и настройка ADFS Extension

1. Выполните установку ADFS Extension через запуск соответствующего пакета из дистрибутива.

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

EANetServerURL - адрес AM Server.

Modeld - идентификатор используемого метода аутентификации.



Информация

Modeld может иметь разные **ID** провайдеров:

{EBB6F3FA-A400-45F4-853A-D517D89AC2A3} - **SMS OTP**

{093F612B-727E-44E7-9C95-095F07CBB94B} - **EMAIL OTP**

{F696F05D-5466-42b4-BF52-21BEE1CB9529} - **Passcode**

{0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0} - **Software OTP**

{AD3FBA95-AE99-4773-93A3-6530A29C7556} - **HOTP Provider**

{CEB3FEAF-86ED-4A5A-BD3F-6A7B6E60CA05} - **TOTP Provider**

{DEEF0CB8-AD2F-4B89-964A-B6C7ECA80C68} - **AirKey Provider**

Пример

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



Информация

При использовании https соединения требуется выполнить [установку клиентского сертификата](#) на каждый сервер Indeed AM.

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

 Информация

YourPath\MFAAdapter.json - укажите свой полный путь к конфигурационному файлу созданному ранее.

 Важно!

При регистрации, изменении или удалении адаптера необходимо выполнить перезапуск службы ADFS на каждом сервере ADFS.

 Информация

В переменной **\$typeName**, в параметре **Version** указывается номер версии используемого **Indeed ADFS Extension**.

Пример

```
$typeName = "IndeedId.ADFS.MFAAdapter.MFAAdapter, IndeedId.ADFS.MFAAdapter,
Version=1.0.12.0, Culture=neutral, PublicKeyToken=1ebb0d9282100d91"
Register-AdfsAuthenticationProvider -TypeName $typeName -Name "Indeed Id MFA
Adapter" -ConfigurationFilePath 'YourPath\MFAAdapter.json'
```

- а. Для регистрации нескольких провайдеров измените имя провайдера в параметре **"Name"**

Пример

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

- б. Изменить отображаемое имя провайдера. Для параметра **"Name"** указать значение из предыдущего шага, для параметра **"DisplayName"** задать имя, которое будет отображаться при выполнении аутентификации через ADFS:

Пример

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

4. Для удаления адаптера необходимо выполнить следующую команду:

Пример

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

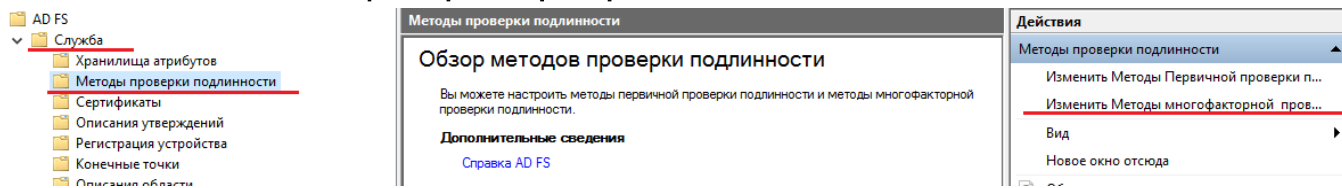
5. Для обновления конфигурации необходимо выполнить следующую команду:

Пример

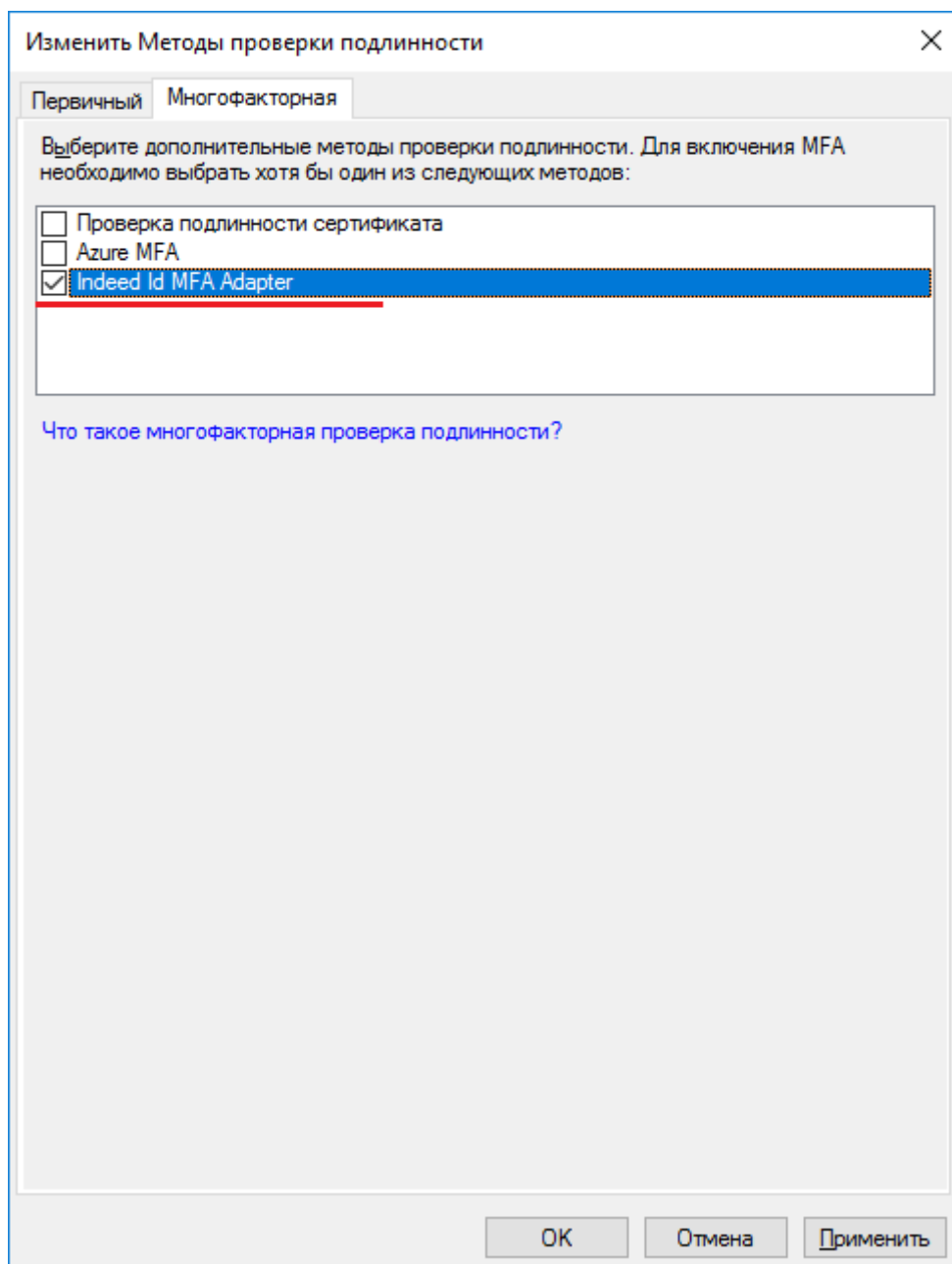
```
Import-AdfsAuthenticationProviderConfigurationData -Name "Indeed Id MFA Adapter" -  
FilePath 'YourPath\MFAAdapter.json'
```

Включение многофакторной аутентификации для ADFS

1. Откройте консоль управления AD FS.
2. Выберите "Служба Методы проверки подлинности", в окне "Действия" выберите "Изменить Методы многофакторной проверки..."



3. В вкладке "Многофакторная" выберите созданный ранее провайдер и нажмите "Применить".



4. Для применения изменений перезапустите службу AD FS.

Пример работы расширения

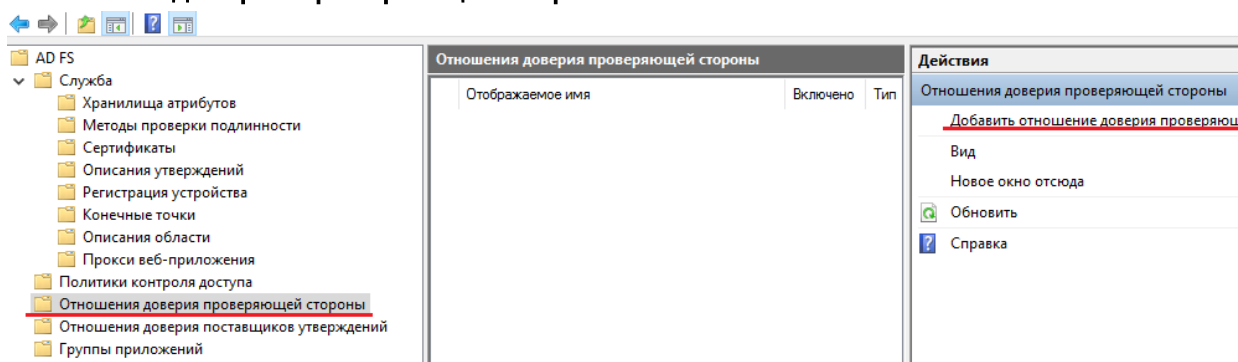
Пример работы расширения на idpinitiatedsignon странице ADFS

Информация

Пример работы расширения показан на странице ADFS `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 "Поддерживаемые утверждения" и нажмите "Запустить".

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

Информация

В качестве примера работы расширения используется стандартная страница ADFS `idpinitiatedsignon.htm`. Адрес метаданных используется для данной страницы.

The screenshot shows the 'Master of adding trust relationships' (Мастер добавления отношений доверия проверяющей стороны) wizard. The current step is 'Select data source' (Выбор источника данных). On the left, a 'Steps' (Шаги) pane shows the progress: 'Welcome' (Добро пожаловать!), 'Select data source' (Выбор источника данных), 'Select policy' (Выбор политики управления доступом), 'Ready to add' (Готовность для добавления отношения доверия), and 'Finish' (Готово). The main area has the title 'Select the method the master uses to obtain data about this relying party:' (Выберите способ, используемый мастером для получения данных об этой проверяющей стороне:). There are three radio button options: 1. 'Import data from the relying party, published in the Internet or local network' (Импорт данных о проверяющей стороне, опубликованных в Интернете или локальной сети). This option is selected. Below it, a text box for 'Federation metadata address (name or URL address):' (Адрес метаданных федерации (имя узла или URL-адрес):) contains the URL 'https://adfsnew.indeed.local/federationmetadata/2007-06/federationmetadata.xml'. A red underline is under the URL. Below the text box is an example: 'Example: fs.contoso.com or https://www.contoso.com/app'. 2. 'Import data from the relying party from a file' (Импорт данных о проверяющей стороне из файла). Below it, a text box for 'Location of federation metadata files' (Местоположение файлов метаданных федерации) is empty. To the right of this text box is a button labeled 'Browse...' (Обзор...). 3. 'Enter data from the relying party manually' (Ввод данных о проверяющей стороне вручную). Below it, a text box for 'Select the parameter to enter the required data about the relying party manually' (Выберите данный параметр, чтобы ввести требуемые данные об организации проверяющей стороны вручную) is empty. At the bottom right, there are three buttons: '< Back' (Назад), 'Next >' (Далее), and 'Cancel' (Отмена). The 'Next >' button is highlighted with a red rectangle.

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.

Мастер добавления отношений доверия проверяющей стороны

Выбрать политику управления доступом

Шаги

- Добро пожаловать!
- Выбор источника данных
- Указание отображаемого имени
- Выбрать политику управления доступом**
- Готовность для добавления отношения доверия
- Готово

Выберите политику управления доступом:

Имя	Описание
Разрешение для каждого и запрос MFA	Предоставьте доступ всем и
Разрешение для каждого и запрос MFA для внешних польз...	Предоставление доступа по...
Разрешение для каждого и запрос MFA для определенной г...	Предоставление доступа ка:
Разрешение для каждого и запрос MFA с непроверенных у...	Предоставьте доступ всем и
Разрешение для каждого.	Предоставление доступа ка:
Разрешение для определенной группы	Предоставление доступа по...
Разрешение доступа через интрасеть для каждого	Предоставьте доступ пользк
Разрешить всем и требовать MFA, разрешить автоматическ	Предоставить доступ всем и

Политика

Разрешение пользователям
и требуется многофакторная проверка подлинности

☐ Не настраивать политики управления доступом в этот раз. Ни один пользователь не пол
доступ к этому приложению.

< Назад **Далее >** От

6. Остальные параметры оставьте по умолчанию.
7. Для применения изменений перезапустите службу AD FS.

Работа расширения

Информация

По умолчанию страница **idpinitiatedsignon.htm** отключена в AD FS 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 логин/пароля укажите данные для второго фактора.

ADFS

Добро пожаловать IND\Admin-Indeed

В целях безопасности необходимо указать
дополнительные данные для проверки учетной
записи

Indeed Id Enterprise Authentication
One Time Password

••••••••

Submit

4. После корректного ввода данных будет выполнен вход.

ADFS

Вы выполнили вход.

Выход

Примеры внедрения расширения

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

Indeed AM ESSO Agent

Описание

Indeed Enterprise Single Sign-On реализует технологию единого доступа Single Sign On в информационные системы организации: централизованно хранит пароли приложений пользователя и выполняет автоматическую подстановку пароля в скрытом виде при необходимости доступа в приложение или выполнения других действий, требующих аутентификации. Indeed AM ESSO Агент упрощает процедуру аутентификации в приложениях исключая необходимость ручного ввода пароля и периодической смены пароля пользователем.

Поддерживаемые приложения

Технология доступа Indeed Enterprise Single Sign-On применяется для windows и web приложений и настраивается без программного вмешательства в серверную или клиентскую часть целевого приложения. Поддержка нового приложения подразумевает создание специального шаблона в формате .xml. В шаблоне указывается, какие формы приложения будут контролироваться. Контроль доступа выражается в повторном запросе аутентификации, заполнении полей регистрационными данными (имя пользователя и пароль), активации нужных элементов управления (нажатие кнопки «Вход»), запись события в журнал и т.п.

Поддерживаемые технологии аутентификации

В дополнение к стандартной технологии аутентификации, реализованной в большинстве продуктов Single Sign-On, - универсальному паролю мастер-паролю, Indeed AM Enterprise SSO поддерживает альтернативные технологии аутентификации.

Установка



Информация

Установка компонента выполняется на рабочих местах пользователей. Для установки компонента требуются права Локального администратора.

Информация

Для развертывания Indeed AM SSO Агент на рабочих станциях пользователей в автоматическом режиме удобно использовать механизм групповых политик (Microsoft Group Policy). Или любой другой инструмент, позволяющий массово распространять и устанавливать msi-пакеты на рабочие станции пользователей (например, Microsoft System Center Configuration Manager). Подробнее со способами распространения компонентов системы Indeed AM в автоматическом режиме можно ознакомиться в документе [Indeed-Id Руководство по развертыванию системы.pdf](#).

1. Запустите программу установки **IndeedID.Enterprise SSO.Agent.msi** и следуйте указаниям Мастера установки.
2. После завершения установки компонента потребуется перезагрузка системы. Нажмите **Да**, чтобы выполнить перезагрузку сразу, или **Нет**, чтобы сделать это позднее вручную.

Информация

Файлы для **Indeed AM SSO Агент** расположены: *indeed AM <Номер версии>\Indeed AM Enterprise SSO\<Номер версии>*

- **IndeedID.ESSO.Agent.msi** - Пакет для установки **Indeed AM SSO Агент** на 32-битных ОС.
- **IndeedID.ESSO.Agent.x64.msi** - Пакет для установки **Indeed AM SSO Агент** на 64-битных ОС.

Файлы шаблонов политик расположены: *indeed AM <номер версии>\Misc\ADMX Templates*.

Настройка подключения к AM серверу

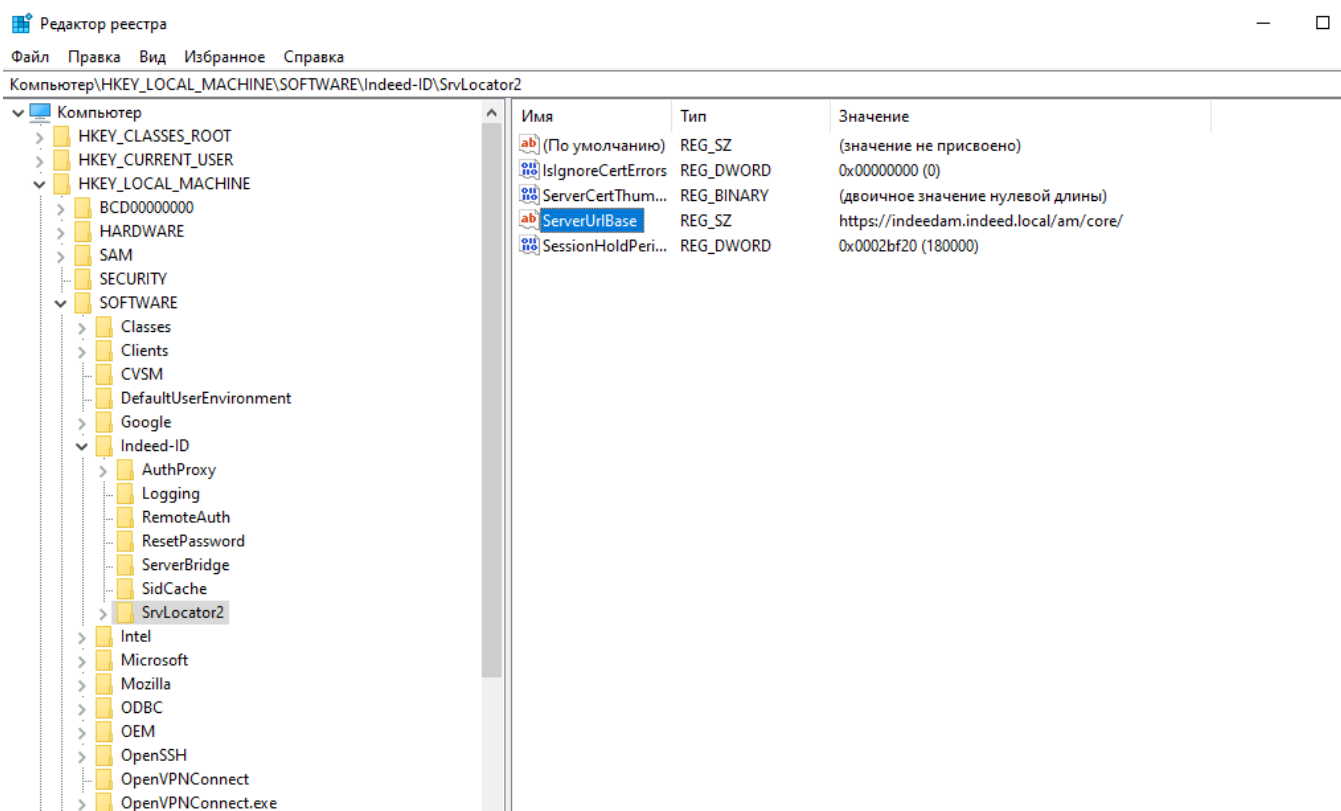
Настройка через реестр

1. Откройте редактор реестра **Windows**.
2. Перейдите в раздел **HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\SrvLocator2**.
3. Измените строковый параметр **ServerUrlBase** и укажите значение URL вашего **Indeed Access Manager Server** (например `http(s)://dc.indeed-id.local/am/core/`).



Информация

При использовании `https` соединения требуется выполнить [установку клиентского сертификата](#) на каждый сервер Indeed AM.



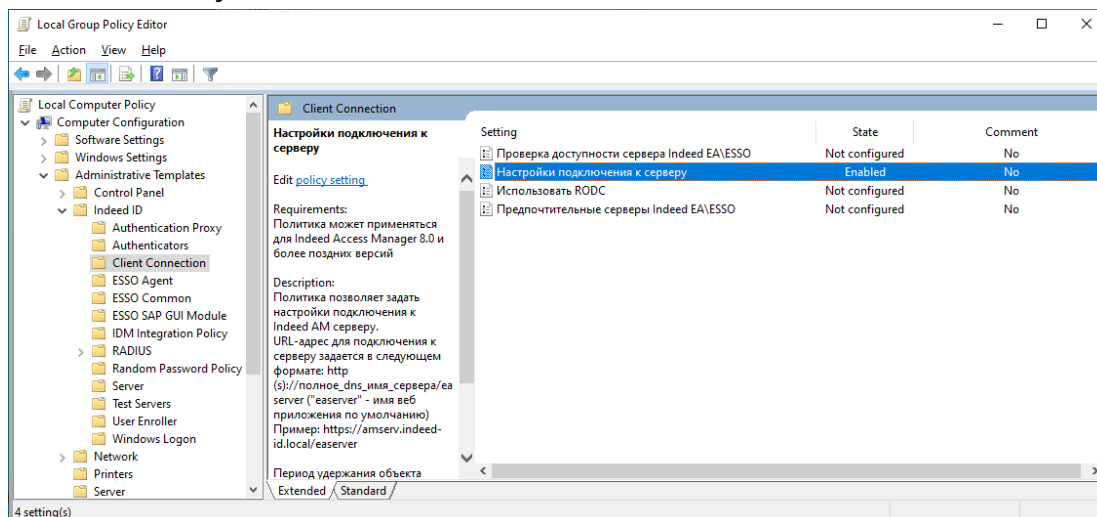
Настройка через GPO



Информация

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 ESSO Agent**.
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 значение URL вашего **Indeed Access Manager Server** (например ***http(s)://dc.indeed-id.local/am/core/***).

Настройки подключения к серверу

Настройки подключения к серверу

☐ Не задано
 ☒ Включено
 ☐ Отключено

Комментарий:

Требования к версии:

Политика может применяться для Indeed Access Manager 8.0 и более поздних версий

Параметры:

URL-адрес AM сервера:

`https://indeedam.indeed.local/am/core`

☐ Игнорировать ошибки сертификата:

Период удержания объекта сессии (мс):

180000

Справка:

Политика позволяет задать настройки подключения к Indeed AM серверу.
 URL-адрес для подключения к серверу задается в следующем формате: `http(s)://полное_dns_имя_сервера/easerver`
 ("easerver" - имя веб приложения по умолчанию)
 Пример: `https://amserv.indeed-id.local/easerver`

Период удержания объекта сессии - период удержания объекта сессии для повторного использования при кратковременных разрывах подключения.

OK
 Отмена
 Применить

Настройка web-плаги́на Indeed ESSO

При работе с web-приложениями Indeed AM ESSO Агент использует web-плагин для браузеров Internet Explorer, Mozilla Firefox и Google Chrome.

Internet Explorer

Надстройка Indeed AM SSO Helper для Internet Explorer устанавливается вместе с IndeedId ESSO Агент. Для работы расширения включите его в браузере. Если после установки Indeed AM ESSO Агент надстройка не появилась в браузере выполните следующие действия:

- Перейдите в **Свойства браузера (Internet options)** -> **Дополнительно (Advanced)** -> раздел **Обзор (Browsing)** и включите опцию **Разрешение сторонних расширений обозревателя (Enable third-party browser extensions)**.

Надстройка Indeed-Id Enterprise SSO Helper издателя INDID, ООО готова к использованию.

Включить

Не включать



Информация

На серверных операционных системах в дополнение перейдите в **Диспетчер серверов (Server manager)** -> **Локальный сервер (Local server)** и отключите **Конфигурацию усиленной безопасности Internet Explorer (IE ESC)**.

Для массовой настройки параметров работы с надстройками в Internet Explorer используйте групповые политики Windows.

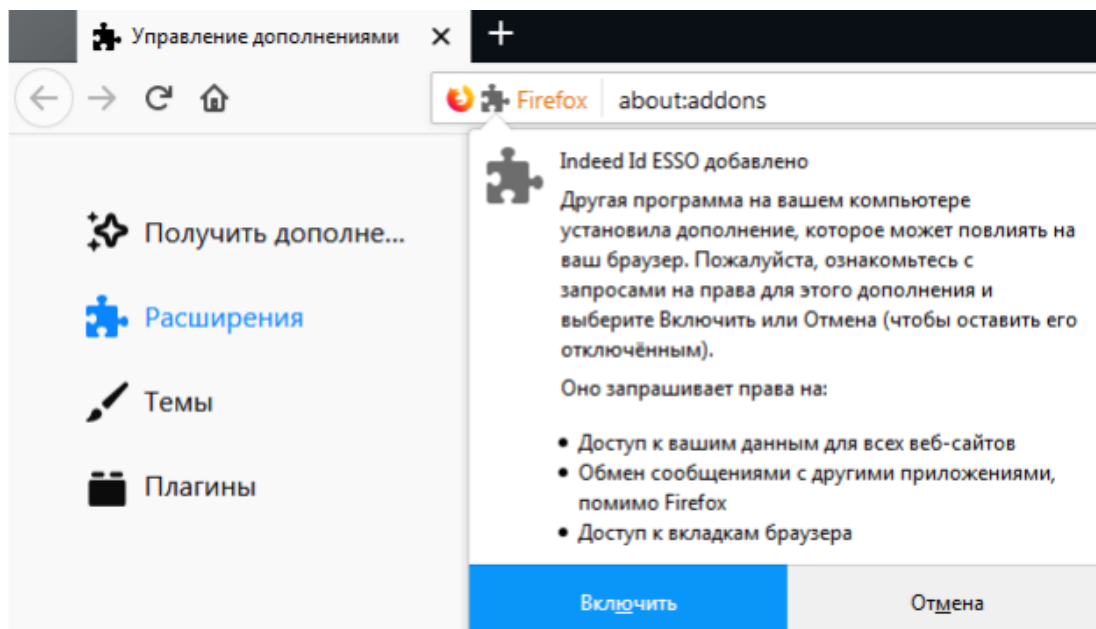
Политики располагаются в **Редакторе локальной групповой политики (Local Group Policy Editor, gpedit.msc)** в разделе **Конфигурация пользователя (User Configuration)** \

Административные шаблоны (Administrative Templates) \ **Компоненты Windows (Windows Components)** \ **Internet Explorer**.

1. Включите политику **Автоматически активировать новые установленные надстройки (Automatically activate newly installed add-ons)** для автоматического включения web-плагина.
2. Для запрета выключения надстроек пользователями включите политику **Не разрешать пользователям включать и отключать надстройки (Do not allow users to enable or disable addons)**.

Mozilla Firefox

Расширение Indeed Id ESSO устанавливается вместе с Indeed-Id ESSO Агент. Для работы расширения включите его в браузере.

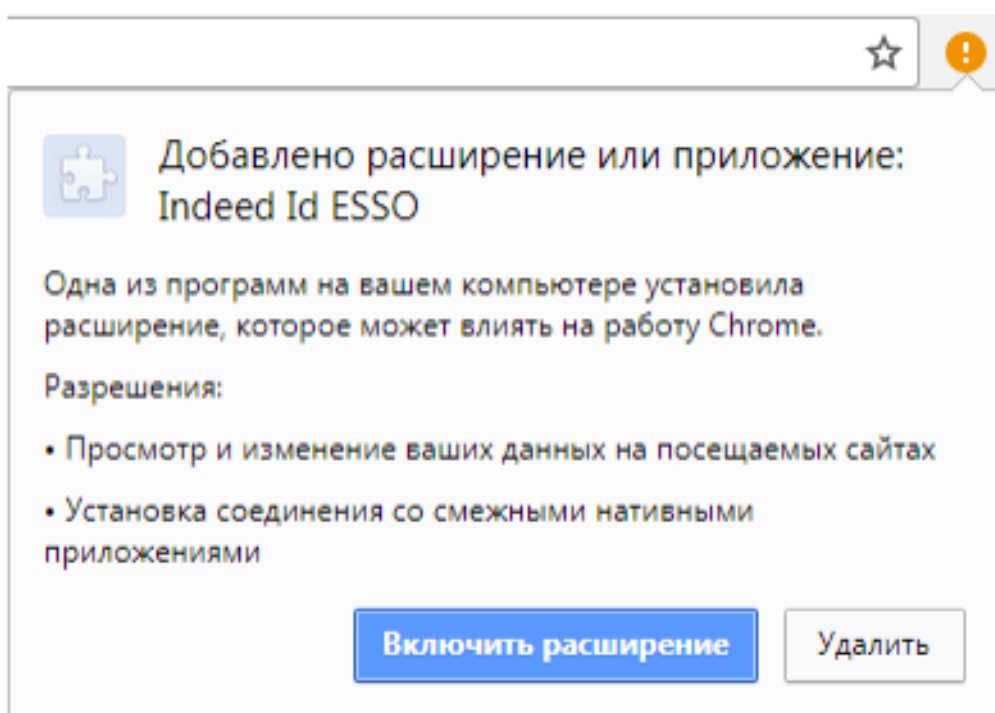


Google Chrome

Расширение Indeed AM ESSO устанавливается в ручном или автоматическом режиме, через механизм групповых политик Microsoft Windows.

Установка из Интернет-магазина Chrome:

1. Установите Indeed AM ESSO Агент на рабочую станцию, обладающей доступом в Интернет.
2. Запустите Google Chrome. Загрузка расширения произойдет автоматически в течение 1 минуты. После загрузки расширения доступ к интернету не требуется. Для работы расширения включите его в браузере.





Информация

Загрузку и включение расширения потребуется производить для каждой сессии пользователя в Windows. Если расширение было удалено из браузера вручную, то для повторной установки загрузите его из Интернет-магазина Chrome.

Доступно по ссылке <https://chrome.google.com/webstore/detail/indeed-id-esso/lcjenjmcehnkfkghcflkfialplejjkdj>

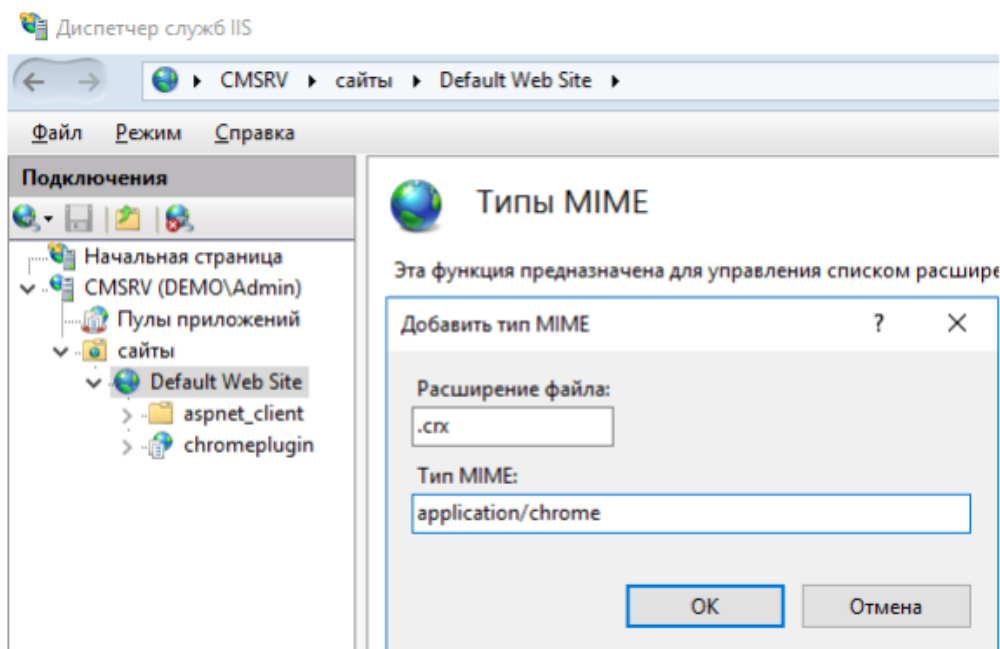
Установка через механизм групповых политик:

Расширение Indeed AM ESSO, распространяемое групповыми политиками, устанавливается для всех пользователей рабочей станции. Для установки не требуется доступ в Интернет.

Для настройки групповой политики на установку расширения Indeed AM ESSO выполните следующие действия:

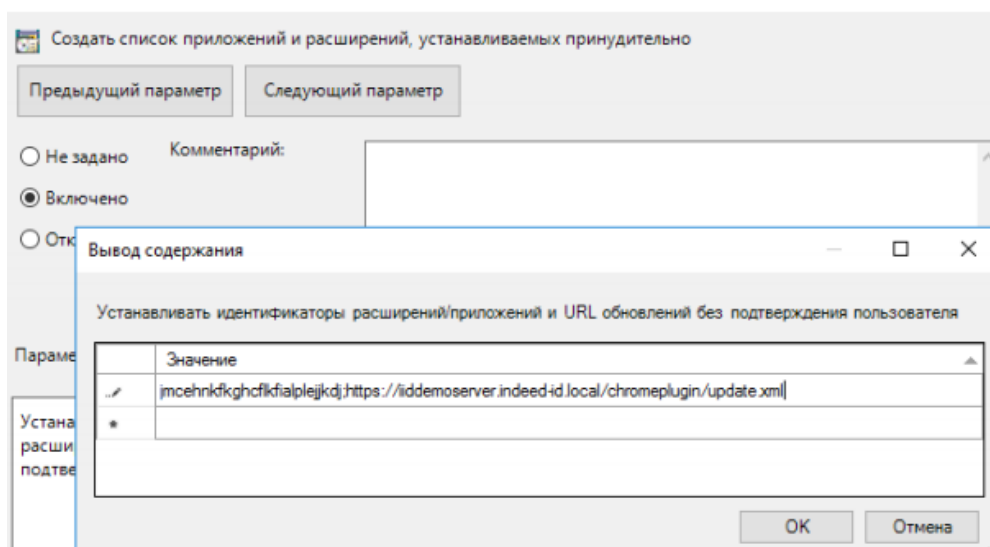
1. Создайте в **Диспетчере служб IIS (IIS Manager)** web-приложение с произвольным именем, например **chromeplugin**, определите для него пул приложений **DefaultAppPool** и **Анонимную проверку подлинности (Anonymous Authentication)**.
2. В каталог приложения поместите файлы **lcjenjmcehnkfkghcflkfialplejjkdj.crx** и **update.xml** (располагаются в дистрибутиве Indeed AM Single Sign-On\<версия>\Misc\ChromePlugin).

3. В разделе **Типы MIME (MIME Types)** веб-сайта, в котором находится приложение **chromeplugin**, добавьте новый тип с расширением **.crx** и описанием **application/chrome**.

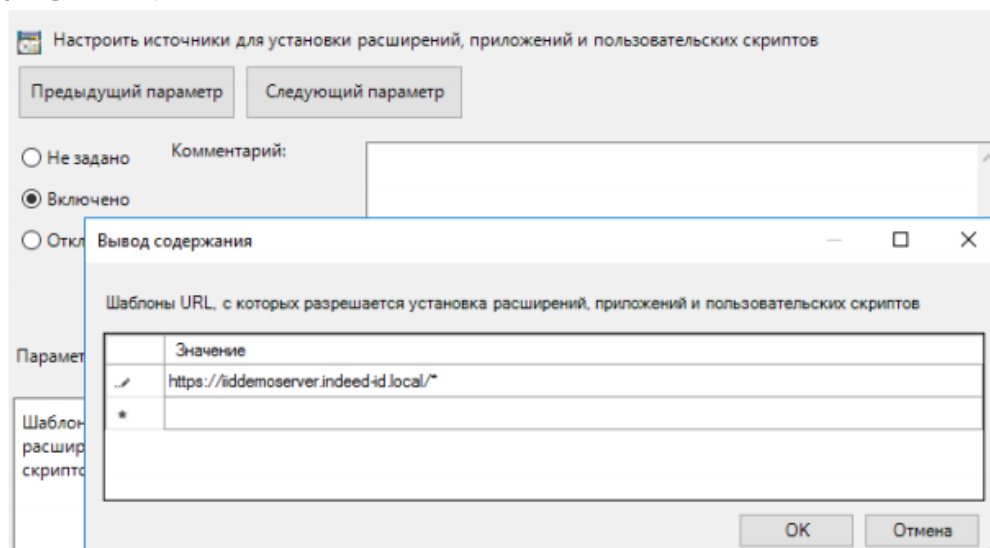


4. Настройте безопасное https соединение для приложения **chromeplugin** и убедитесь что к нему можно обратиться с рабочих станций пользователей.
5. Добавьте шаблоны adm/admx в локальное/центральное хранилище административных шаблонов контроллера домена и создайте новый объект групповой политики в оснастке **Управление групповой политикой (Group Policy Management)** с произвольным именем.
6. Откройте для редактирования созданный объект групповой политики и перейдите в раздел **Конфигурация компьютера (Computer Configuration)** -> **Административные шаблоны (Administrative Templates)** -> **Google** -> **Google Chrome** -> **Расширения (Extensions)**.

7. Включите политику **Создать список приложений и расширений, устанавливаемых принудительно** (Configure the list of force-installed apps and extensions) и укажите идентификатор расширения (указан в имени файла **.crx**) и путь к **.xml** файлу в каталоге созданного в п.2 web-приложения **chromeplugin**. Сохраните внесенные изменения.

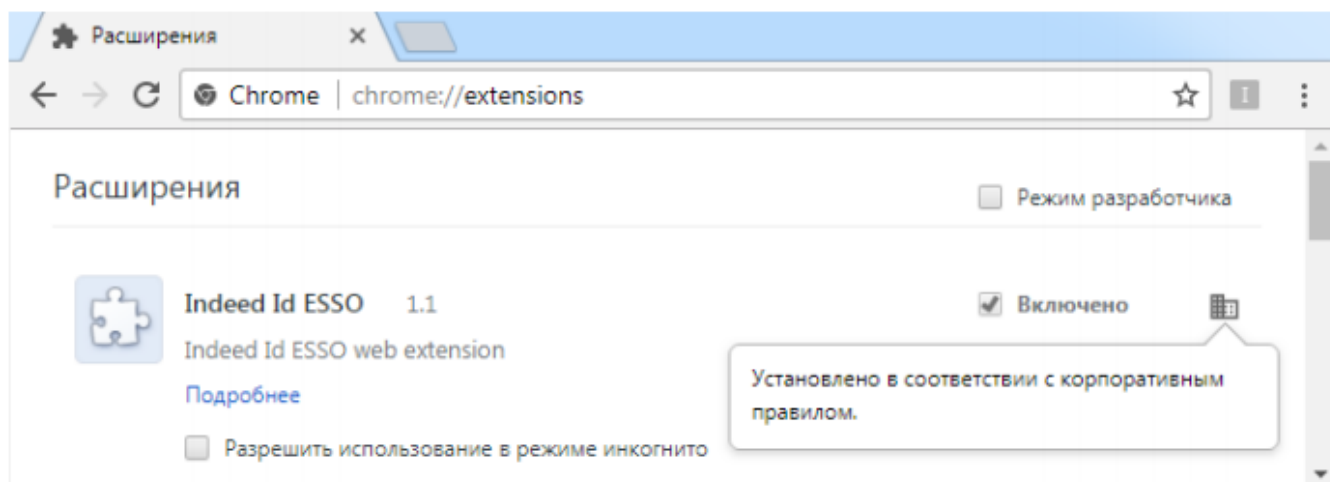


8. Включите политику **Настроить источники для установки расширений, приложений и пользовательских скриптов** (Configure extension, app, and user script install sources) и укажите адрес сервера, на котором развернуто созданное в п.2 web-приложение **chromeplugin**. Сохраните изменения.



9. Распространите действие объекта групповой политики на рабочие станции пользователей с установленным **Indeed AM ESSO Агент**.

10. Расширение автоматически загрузится и установится после применения групповой политики к рабочей станции. Может потребоваться до нескольких минут для того, чтобы оно отобразилось в списке установленных в браузере. Установленное через групповые политики расширение отмечено соответствующим символом.



Работа Indeed AM Single Sign-On

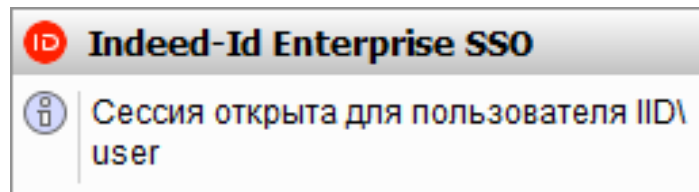
Работа Indeed AM Single Sign-On заключается в отслеживании запуска приложений и автоматическом заполнении полей и форм данными, необходимыми для получения доступа в приложение:

имя пользователя, пароль и т.п. Автоматическое заполнение полей данными происходит только после подтверждения личности пользователя с применением поддерживаемой технологии аутентификации. Таким образом, Indeed AM Single Sign-On избавляет пользователей от необходимости запоминания, записи, хранения, ручного ввода паролей для выполнения входа в приложение. Благодаря централизованному хранению SSO-профилей пользователи получают доступ в приложения с любой рабочей станции, где установлен компонент Indeed AM ESSO Агент. Поддержка в Indeed AM ESSO Агент технологий аутентификации, специально адаптированных для использования в терминальной среде и не требующих установки дополнительного оборудования, дает возможность работать на «неподготовленном» компьютере и использовать тонкие клиенты на базе Windows CE, Linux, Wyse и т.п.

Единый доступ в приложения по технологии аутентификации Indeed

Доступ в приложения с использованием аутентификатора становится возможен после настройки учетной записи приложения, профиля пользователя и регистрации аутентификатора. Для получения доступа в приложение с использованием технологии аутентификации Indeed AM выполните следующие действия:

1. Выполните вход на рабочую станцию. В панели задач отобразится всплывающее сообщение об открытии SSO-сессии.

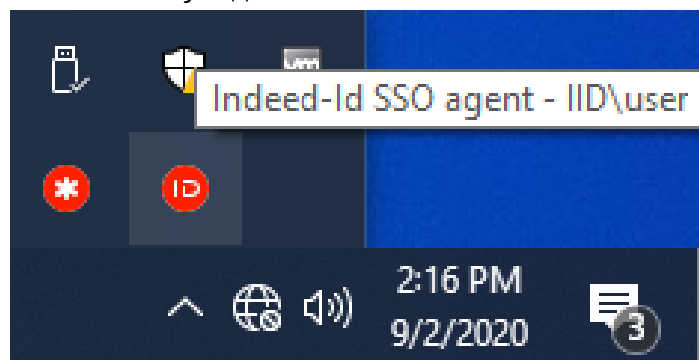


2. **Indeed AM ESSO Агент** запускается автоматически при входе в операционную систему. Для запуска вручную выберите пункт **Indeed AM > AM SSO > AM SSO - Агент** в меню **Программы**.

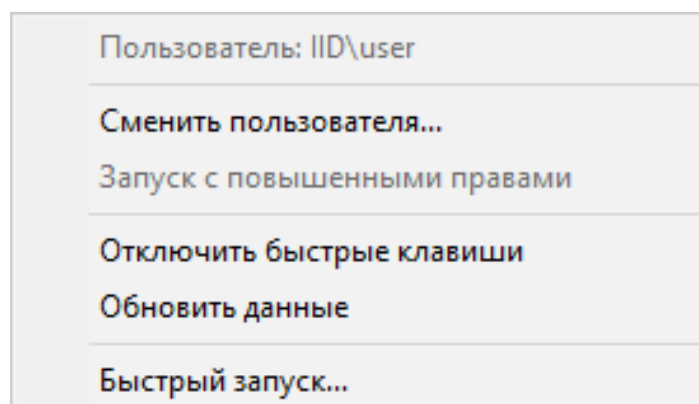
Выбор целевого приложения

Для выбора целевого приложения выполните одно из следующих действий:

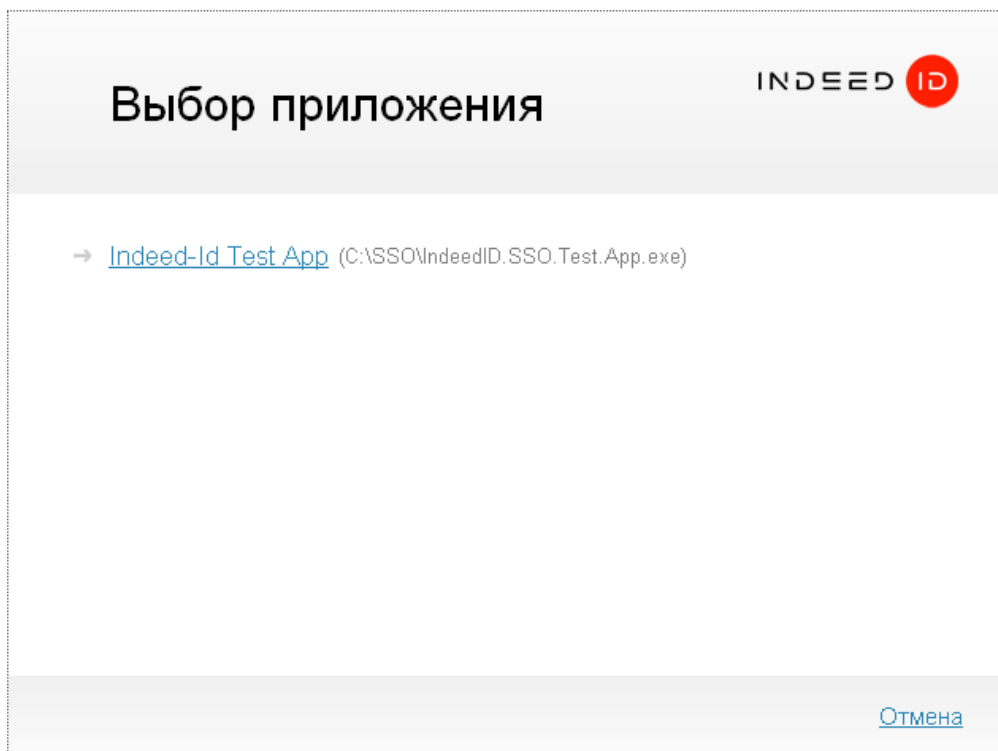
1. Нажмите **[Ctrl]+[Alt]+[Q]** или откройте приложение **Indeed AM SSO Агент** двойным щелчком по иконке в области уведомлений Windows.



2. Нажатием правой кнопки мыши на иконку в области уведомлений Windows вызовите контекстное меню приложения Indeed-Id ESSO Агент и выберите пункт **Быстрый запуск**.



В окне **Выбор приложения** доступны приложения, разрешенные для запуска с помощью **Indeed AM ESSO Агент**. Вид окна **Выбор приложения** определяется настройками ESSO-приложений. На рисунке ниже, представлена ситуация, когда у целевого приложения один исполняемый файл.



Информация

Если для одного целевого приложения настроено несколько учетных записей SSO, то после выбора приложения потребуется выбрать учетную запись.

Если приложение содержит в себе несколько компонентов (например, приложение «1С Предприятие» может содержать в себе приложения «1С:Бухгалтерия», «1С:Управление Торговлей» и т.д.), то исполняемые файлы каждого компонента группируются для удобства выбора в панели быстрого запуска под одним именем. На Рисунке ниже приведен пример группировки нескольких компонентов 1С под одним именем 1С: Предприятие.

Выбор приложения

INDEED 

1С Предприятие 8.0

- [1С: Бухгалтерия](#)
- [1С: Зарплата и управление персоналом](#)
- [1С: Управление Торговлей](#)
- [1С: Управление производственным предприятием](#)

[Отмена](#)

После выбора приложения потребуется выбрать учетную запись, если их несколько для выбранного приложения.

Выбор учетной записи

INDEED 

1С Предприятие 8.2 (русская версия)

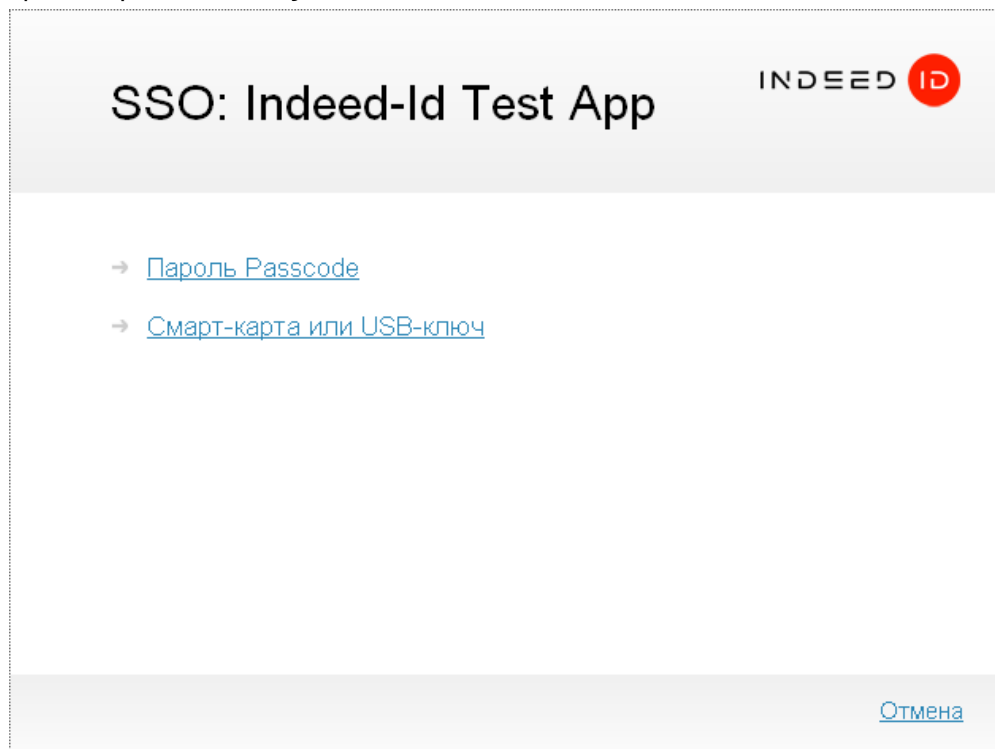
- [Администратор](#) (Администратор)
- [Евгений Белов](#) (Пользователь)

[Отмена](#)

Аутентификация

Для аутентификации в приложении выполните следующие действия:

1. Выберите имя пользователя и способ входа. По умолчанию операционная система предлагает последний использованный способ. Следуйте подсказкам на экране и предоставьте обученный аутентификатор. При наличии нескольких обученных аутентификаторов используйте любой из них.



SSO: Indeed-Id Test App

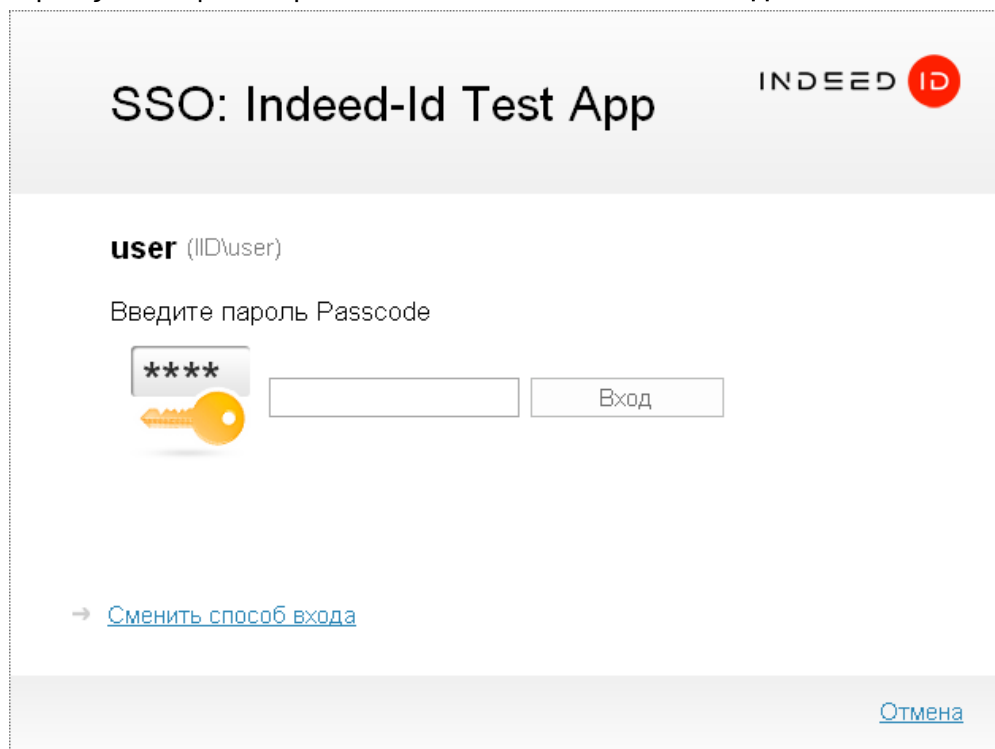
INDEED ID

→ [Пароль Passcode](#)

→ [Смарт-карта или USB-ключ](#)

[Отмена](#)

2. Для выбора аутентификатора нажмите **Сменить способ входа**



SSO: Indeed-Id Test App

INDEED ID

user (IID\user)

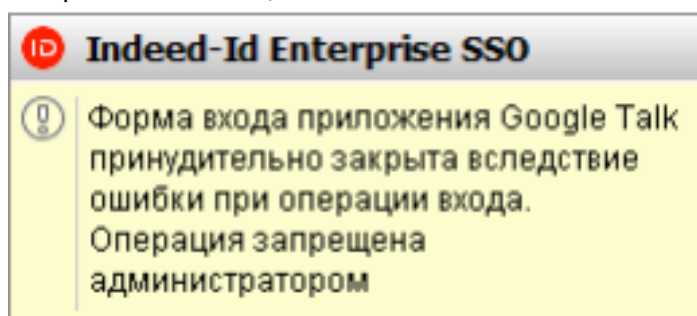
Введите пароль Passcode



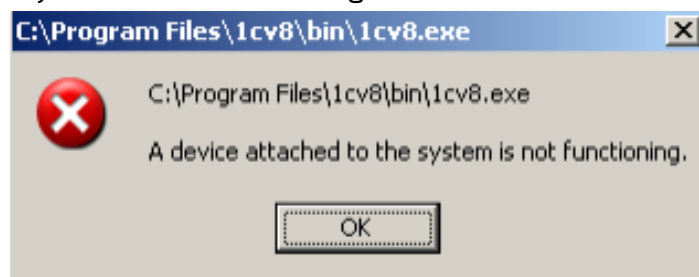
→ [Сменить способ входа](#)

[Отмена](#)

3. После аутентификации отображается окно входа в целевое приложение. В поля «Имя пользователя» и «Пароль» автоматически подставляются данные, указанные при создании учетной записи SSO, и выполняется вход в приложение. Помимо автоматической подстановки учетных данных в форму входа приложения поддерживается и ручной ввод логина и пароля. Указанные при первом входе в приложение логин и пароль запоминаются и будут автоматически подставлены при следующем входе. При отмене аутентификации вход в приложение не будет выполнен: текущая форма приложения или само приложение будет закрыто.
4. Если в настройках запуска приложения администратором определен параметр запуска приложения только при помощи Indeed AM ESSO Агент и настроено требование аутентификации при входе в приложение, то в случае отмены аутентификации отобразится сообщение об ошибке.



Доступ к целевым приложениям регулируется административными настройками. Некоторые приложения могут быть запрещены для запуска администратором ESSO. Запрещенные приложения недоступны в окне **Выбор приложения** Indeed AM ESSO Агент. При попытке запуска запрещенного приложения отображается сообщение об ошибке «A device attached to the system is not functioning».

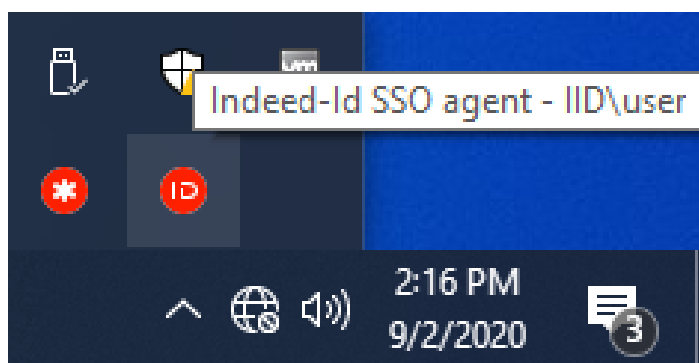


Смена пользователя

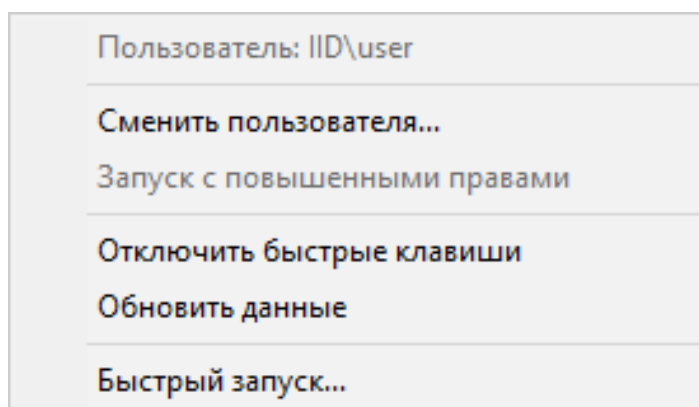
Для изменения пользователя ESSO выполните следующие действия:

Выполните вход в операционную систему и перейдите в контекстное меню Indeed AM ESSO Агент:

- Откройте приложение Indeed AM SSO Агент двойным щелчком по иконке в области уведомлений Windows.



- Нажатием правой кнопки мыши на иконку в области уведомлений Windows вызовите контекстное меню приложения Indeed AM SSO Агент и выберите пункт **Сменить пользователя...**



- В окне Вход в SSO введите имя учетной записи, под которой требуется выполнить вход в приложение.

Вход в SSO

→ Введите имя пользователя

Пользователь:

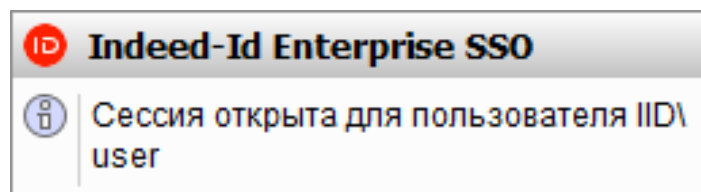
Домен:

IID

Далее

Отмена

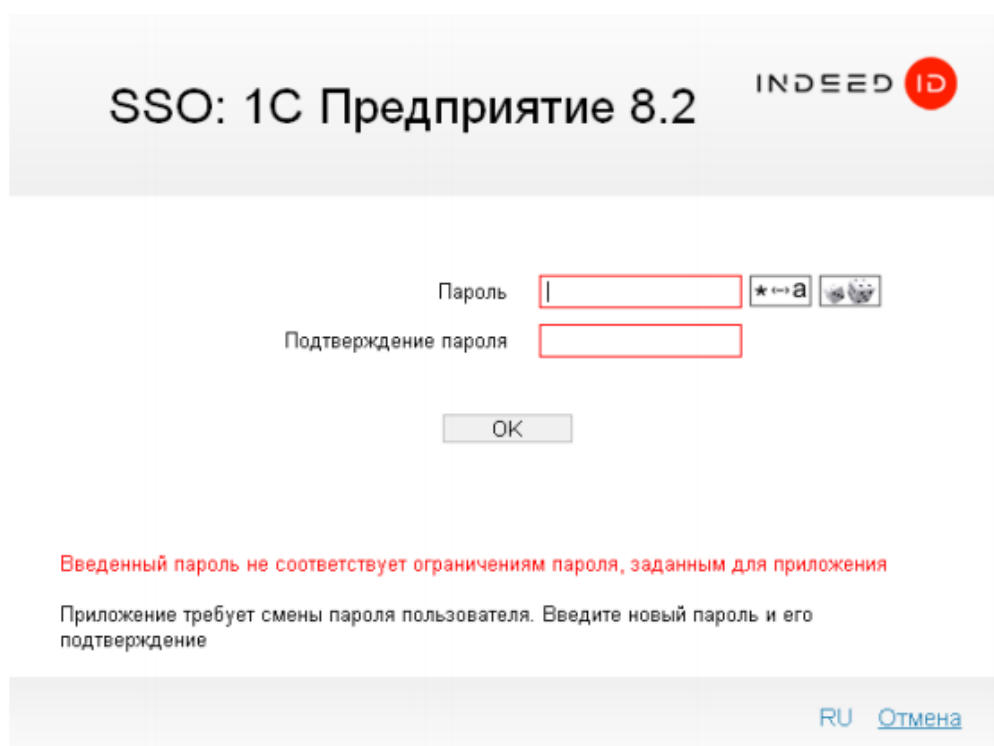
- Выполните аутентификацию по имеющимся у выбранного пользователя аутентификатору. В случае успешной аутентификации Агент ESSO откроет сессию SSO выбранного пользователя:



Управление паролем

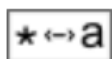
Indeed AM Single Sign-On предусматривает регулярную смену пароля в приложениях. Как правило, пароль меняется автоматически. Самостоятельная ручная смена пароля регулируется установками администратора ESSO. Если ручная смена пароля разрешена, при очередной смене пароля новое значение пароля не генерируется автоматически, а запрашивается у пользователя.

Поведение при запросе нового пароля у пользователя зависит от типа учетной записи пользователя AM SSO, выбранного администратором ESSO: Если администратором настроена ручная смена пароля пользователем, то при смене пароля отобразится следующее окно.



Введите новый пароль и его подтверждение.

- Режим ввода пароля (скрытый пароль/открытый ввод символов) регулируется



нажатием кнопки (Открыть пароль).



- При нажатии кнопки (Генерировать случайный пароль) выполняется автоматическая генерация пароля в соответствии с установленными для данного приложения ограничениями.
- Сгенерированный пароль автоматически вставляется в поле **Пароль**, при этом включается функция **Открыть пароль** и очищается поле **Подтверждение пароля**.

При вводе нового пароля в стандартном режиме выполняется проверка пароля на соответствие критериям сложности, установленным для данного приложения. В случае несоответствия пароля критериям сложности отображается сообщение об ошибке. Если учетная запись AM SSO относится к типу **Учетных данных Active Directory**, при смене пароля отображается следующее сообщение:

SSO: ошибка в 1C 8.2





Операция смены пароля для приложения 1C 8.2 при помощи SSO не может быть завершена успешно.

Причина: Indeed-Id SSO Agent не может контролировать изменение пароля, потому что учетная запись пользователя SSO использует учетные данные Windows. Изменение пароля может быть выполнено вручную с помощью приложения (не рекомендуется), либо штатными средствами Windows. В случае изменения пароля Windows вручную с помощью приложения, произойдет рассинхронизация пароля в Indeed-Id Windows Logon и Indeed-Id ESSO.

Пожалуйста, определите, как ошибка должна быть обработана

Повторить
Завершить приложение
Закрыть окно
Игнорировать

Команды Indeed AM ESSO Агент

В контекстном меню, которое открывается правым щелчком по иконке приложения Indeed AM ESSO Агент в панели уведомлений Windows, доступны следующие команды:

Сменить пользователя – выбрать другую учетную запись для получения доступа в приложение. При выборе команды отображается окно Вход в SSO со списком доступных учетных записей и возможностью выбрать способ входа. По умолчанию используется способ, при помощи которого выполнялся последний вход пользователя.

Отключить быстрые клавиши – отключение использования комбинаций клавиш:

[Ctrl]+[Alt]+[Q] - вызов окна быстрого запуска

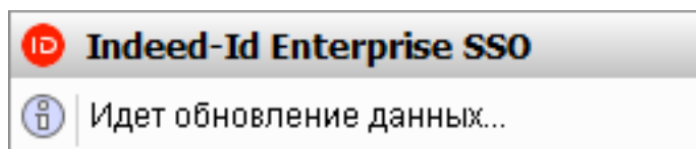
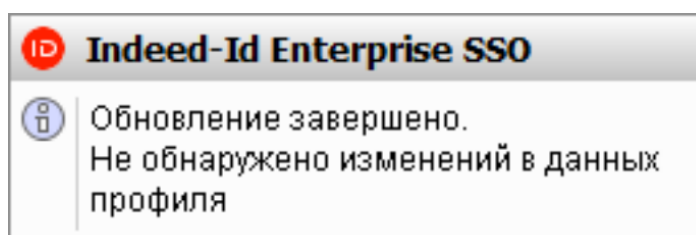
[Ctrl]+[Alt]+[U] - обновление данных ESSO

[Ctrl]+[Alt]+[R] - принудительная обработка формы приложения («рематчинг»)

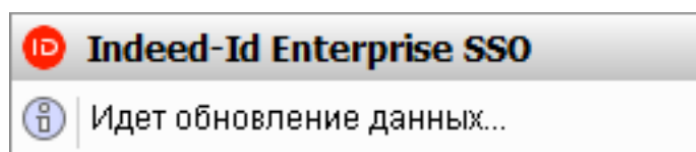
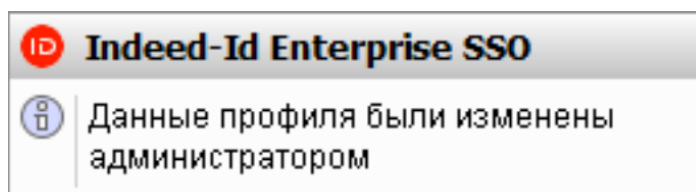
По умолчанию все комбинации включены.

Обновить данные – загрузка изменений профиля SSO. Примеры сообщений приведены на рисунках ниже.

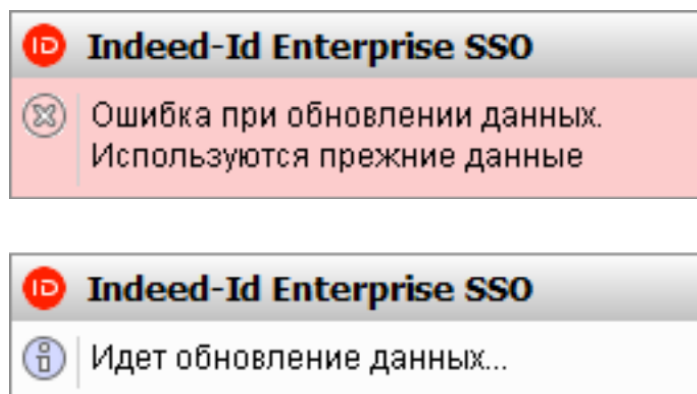
Обновление данных ESSO:



Новые данные ESSO получены:



Ошибка обновления данных:



Быстрый запуск – выполняется при выборе соответствующего пункта в контекстном меню Indeed AM ESSO Агент или нажатии комбинации [Ctrl]+[Alt]+[Q] и предоставляет доступ к списку приложений, разрешенных для запуска (открывается окно **Выбор приложения**).

Информация

Приложение не отображается в списке, если Indeed AM ESSO Агент не может найти его исполняемый файл на рабочей станции пользователя.

Обработка ошибок

При возникновении ошибок во время работы (например, ошибка заполнения формы) Indeed AM ESSO Агент предоставляет возможность выбора действия для обработки ошибки. В таких случаях отображается окно Обработка ошибки:

SSO: ошибка в 1С Предп...



Операция входа в приложение 1С Предприятие 8.2 (русская версия) при помощи SSO не может быть завершена успешно.

Причина: ошибка при автоматическом заполнении формы приложения

Пожалуйста, определите, как ошибка должна быть обработана

Повторить

Завершить приложение

Закрыть окно

Игнорировать

В окне **Обработка ошибки** предлагаются варианты действий (после выбора действия окно закроется автоматически):

- **Повторить** – операция, в ходе которой возникла ошибка, будет выполнена повторно.
- **Завершить приложение** – приложение, при работе с которым возникла ошибка, будет завершено. Не сохраненные данные будут потеряны.
- **Закрыть окно** – будет закрыто текущее окно или форма приложения. При закрытии главного окна приложение может быть завершено.
- **Игнорировать** – не будет предпринято никаких действий.

Вход в целевое приложение при отсутствии сети

Вход в приложение по аутентификатору может быть выполнен даже при отсутствии физического подключения к сети. Действия при входе в приложение в отсутствие сети по кэшированному аутентификатору аналогичны действиям при входе в приложение по аутентификатору при доступной сети.

Данный способ входа доступен, если:

- Для вашей учетной записи было установлено разрешение на кэширование аутентификаторов.
- Было выполнено кэширование аутентификаторов (при первом входе в систему по аутентификатору).
- Был выполнен вход в приложение по кэшированному аутентификатору при доступной сети.

Информация

Срок действия кэшированных аутентификаторов может быть ограничен администратором системы. По умолчанию этот срок составляет 10 дней, отсчитывается с даты последнего входа в приложение и не зависит от того, будет ли выполнен вход в приложение в дальнейшем в течение этого срока. Например, при установленном сроке 10 дней и выполнении входа в приложение в 10 ч 00 мин 12.04.2010 кэшированные аутентификаторы будут действительны с 10 ч 00 мин 12.04.2010 до 10 ч 00 мин 22.04.2010. Если для вашей учетной записи разрешено кэширование аутентификаторов, то уточните у администратора наличие возможных ограничений. Если срок действия кэшированных аутентификаторов истек и серверы Indeed недоступны, при попытке входа в приложение отображается сообщение об ошибке: "Ошибка при входе в систему. Сервер не найден. Кэширование данных пользователя запрещено".

Часто задаваемые вопросы

Ознакомьтесь со списком часто задаваемых вопросов и ответов на них в **Базе знаний**:

- Indeed Enterprise Authentication (<https://support.indeed-id.ru/Knowledgebase/List/Index/1/indeed-enterprise-authentication>)
- Indeed Enterprise Single Sign-On (<https://support.indeed-id.ru/Knowledgebase/List/Index/2/indeed-enterprise-single-sign-on>)

Indeed AM IIS Extension

Продукт **Indeed AM IIS Extension** обеспечивает возможность добавления второго фактора аутентификации пользователей в web приложениях, использующих проверку подлинности с помощью форм (**Forms Authentication**), развернутых на платформе **Microsoft Internet Information Services (IIS)** с использованием технологии аутентификации **Indeed**.

Информация

Файлы для Indeed AM IIS Extension расположены: ***indeed AM <Номер версии>\Indeed AM IIS Extension\<Номер версии>***

- **Indeed.AM.IIS.Extension-<номер версии>.x64.ru-ru.msi** - Пакет для установки Indeed AM IIS Extension.

Установка и настройка Indeed AM IIS Extension

Информация

Indeed AM IIS Extension позволяет настроить двухфакторную аутентификацию для доступа к удаленным рабочим столам и приложениям через web с использованием службы Microsoft Remote Desktop Web Access (RD Web Access).

Двухфакторная аутентификация поддерживается только для приложений, использующих проверку подлинности с помощью форм (Forms Authentication).

Двухфакторная аутентификация реализована с помощью аутентификации по доменному паролю и по второму фактору – одноразовому паролю.

Информация

Для использования расширения необходимо установить **Indeed AM Windows Password Provider** на сервер **Indeed AM**.

1. Выполнить установку IIS Extension через запуск пакета для установки Indeed AM IIS Extension.

2. В разделе **HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\AuthProxy**. Измените параметры:

- а. Параметр **ServerUrlBase**. В данном параметре указывается URL Вашего сервера Indeed AM.



Примечание

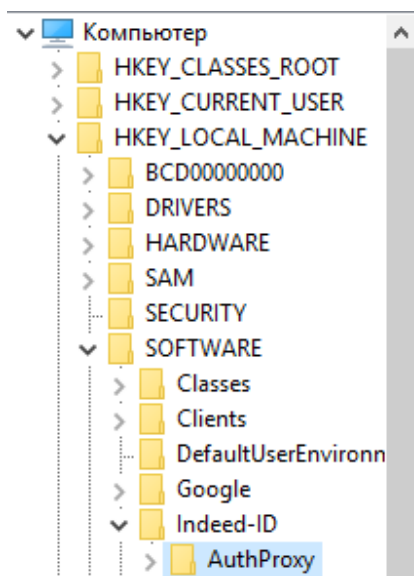
В настройках приложения, в URL не должно быть символов "/" в конце



Информация

При использовании https соединения требуется выполнить [установку клиентского сертификата](#) на каждый сервер Indeed AM.

- б. Параметр **IsIgnoreCertErrors** со значением **0**. Данный параметр предназначен для проверки сертификата сервера **Indeed AM**, при значении **1** происходит игнорирование ошибок сертификата.
- с. Параметр **AppId** со значением **IIS Extension**. В данном параметре задается название используемого компонента.



Имя	Тип	Значение
(По умолчанию)	REG_SZ	(значение не присвоен
AppId	REG_SZ	IIS Extension
IsIgnoreCertErrors	REG_DWORD	0x00000000 (0)
ServerUrlBase	REG_SZ	https://indeedam1.inde

3. Создайте в разделе **HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID** ключ

IISHTTPModule. В созданном ключе создайте:

- а. Строковый параметр **LSUrl**. В данном параметре указывается URL Вашего лог сервера.



Примечание

В настройках приложения, в URL не должно быть символов "/" в конце

- б. Строковый параметр **ProviderId**. Необязательный параметр. Указывается ID провайдера, который станет провайдером по умолчанию при первом входе.



ProviderId может иметь разные ID провайдеров:

{EBB6F3FA-A400-45F4-853A-D517D89AC2A3} - **SMS OTP**

{093F612B-727E-44E7-9C95-095F07CBB94B} - **EMAIL OTP**

{F696F05D-5466-42b4-BF52-21BEE1CB9529} - **Passcode**

{0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0} - **Software OTP**

{AD3FBA95-AE99-4773-93A3-6530A29C7556} - **HOTP Provider**

{CEB3FEAF-86ED-4A5A-BD3F-6A7B6E60CA05} - **TOTP Provider**

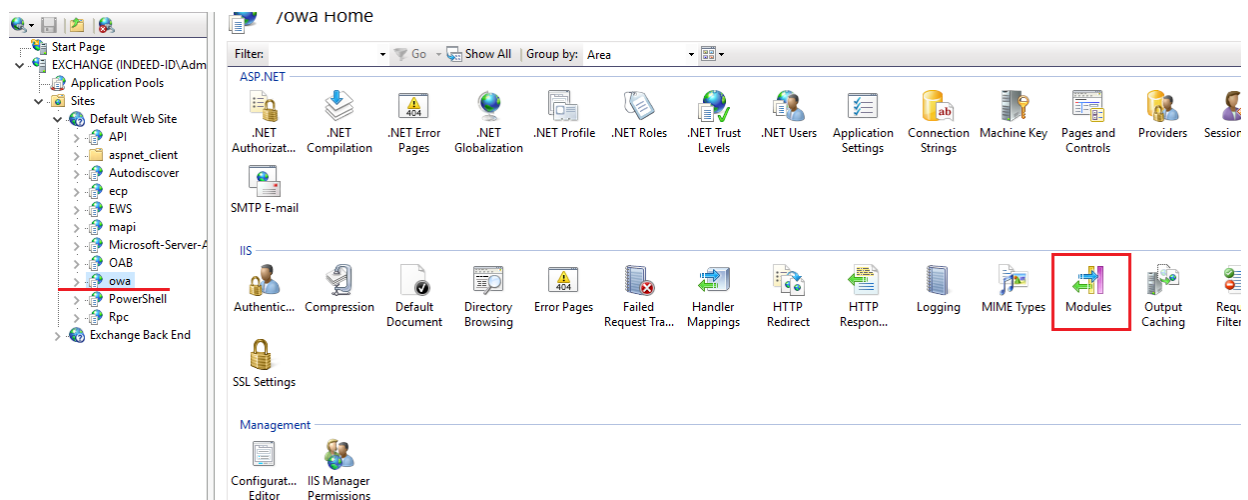
Настройка IIS



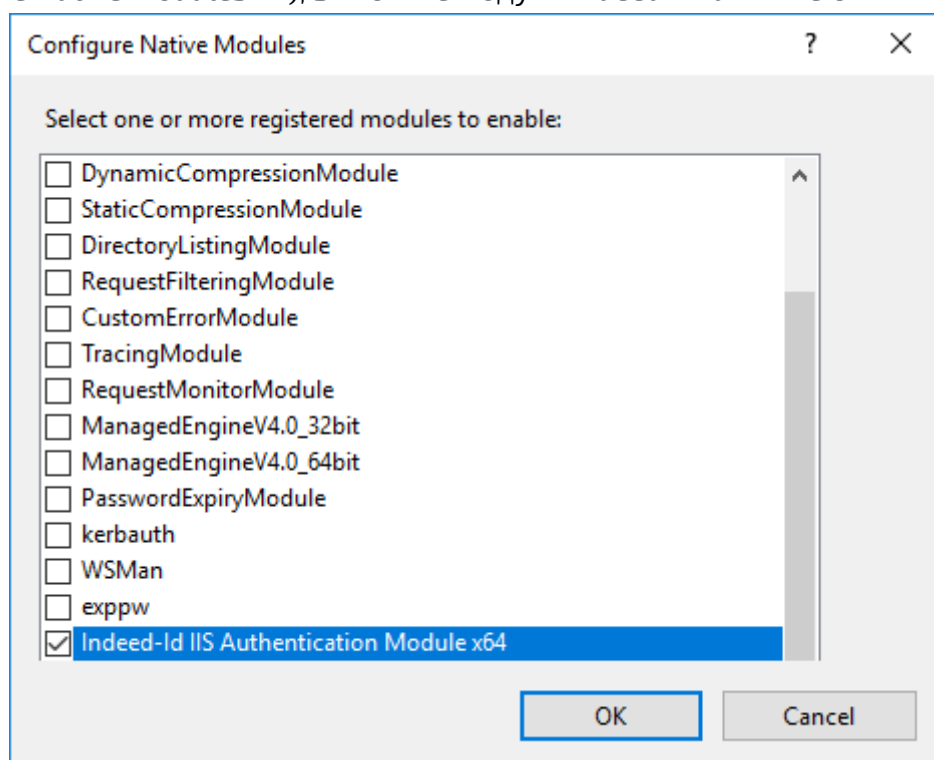
Информация

В данном руководстве рассмотрен пример настройки для Exchange 2016.

1. Откройте в **Диспетчере служб IIS (IIS Manager)** приложение (для Outlook Web Access – это owa), которое будет использовать **IIS Extension** и перейдите в раздел **Модули (Modules)**.



2. В меню Действия (Actions) нажмите **Выполняется настройка собственных модулей. .** (Configure Native Modules. . .), включите модули Indeed и нажмите Ок.

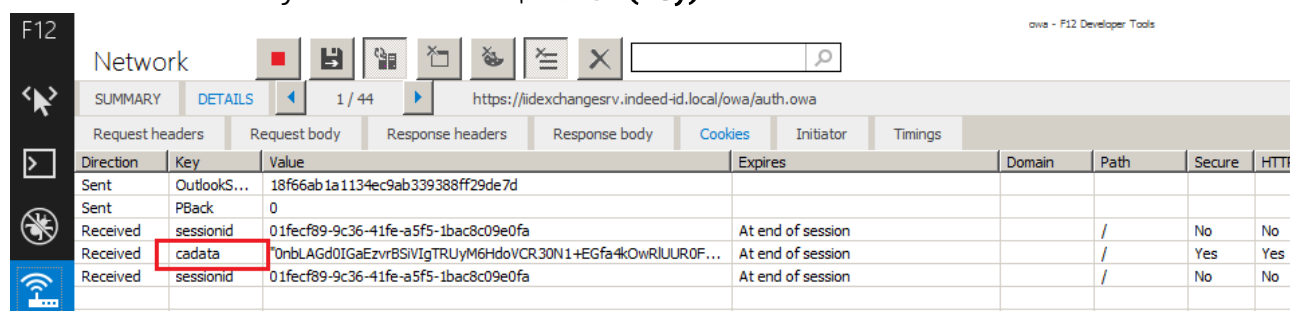


Настройка компонента

Двухфакторная аутентификация настраивается отдельно для каждого целевого приложения. В процессе настройки необходимо создать в разделе **HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\IISHTTPModule** реестра Windows ключ с именем приложения или сайта в IIS (может иметь произвольное значение), создать в этом ключе следующие параметры и определить их значения:

1. **AuthCookie** – Строковый параметр. Название Cookie, которое используется для аутентификации в целевом приложении. Определяется экспериментальным путем для каждого приложения. Значение параметра можно получить из консоли F12 IE Developer Toolbar выполнив следующие действия:

- В разделе **Сеть (Network)** запустите **Сбор сетевого трафика (Enable network traffic capturing)**.
- Выполните аутентификацию в приложении.
- Перейдите в раздел **Подробности (Details)** на вкладку **Cookie (Cookies)**.
- Искомое значение указано в столбце **Ключ (Key)**.



- isMFAEnabled** – DWORD параметр. Включение двухфакторной аутентификации.
- LoginURL** – Строковый параметр. Относительный URL, на который происходит POST-отправка данных формы входа приложения. Должен начинаться с символа /. URL указывается относительно целевого сайта.
- MatchTargetRedirect** – DWORD параметр. При значении 1, страница для ввода второго фактора отображается до перехода на основную страницу. Целевая страница не сохраняется в буфере, после ввода второго фактора происходит редирект на основную страницу (Параметр: TargetURL).
- OTPURL** – Строковый параметр. Альтернативный URL для отправки данных формы аутентификации Indeed второго фактора. По умолчанию данные формы отправляются на тот же URL, что и данные формы целевого приложения. Их перехватывает IIS модуль и подменяет на оригинальные данные, если аутентификация Indeed прошла успешно или же не подменяет их, если аутентификация Indeed не прошла и целевое приложение отображает собственную ошибку аутентификации. Значение необходимо использовать, если целевое приложение не трактует данные формы Indeed как ошибочные для аутентификации или необходимо явным образом демонстрировать ошибки аутентификации Indeed пользователю. Таким образом, значение можно оставить пустым.
- PasswordField** – Строковый параметр. Значение атрибута name поля пароля формы входа приложения.
- RedirectToTarget** – DWORD параметр. Редирект на целевую страницу.

8. **TargetURL** – Строковый параметр. URL целевой страницы, на которую пользователь попадает после аутентификации в приложении.



Информация

Для Exchange 2013 и 2016 указывается **"/owa"** (без завершающего /), для Exchange 2010 указывается **"/owa/"** (с завершающим /)

9. **UsernameField** – Строковый параметр. Значение атрибута name поля имени пользователя формы входа приложения.

Значения всех параметров: **LoginURL, PasswordField, UsernameField** содержатся в форме аутентификации целевого приложения могут быть получены, например, при помощи инструмента Internet Explorer F12 Developer Tools.

```

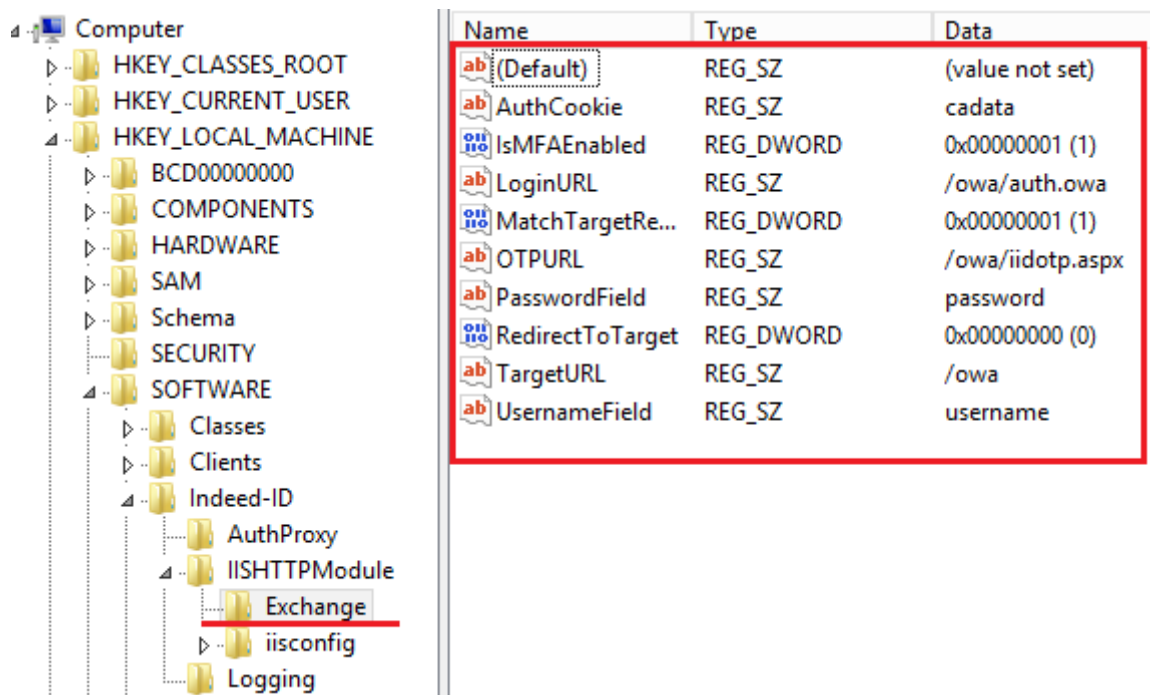
└─ <body class="owaLgnBdy">
  └─ <noscript>...</noscript>
  └─ <form name="logonForm" action="/owa/auth.owa" enctype="application/x-www-form-urlencoded"
    <input name="destination" type="hidden" value="https://iidexchangesrv.indeed-id.1"
    <input name="flags" type="hidden" value="0"></input>
    <input name="forcedownlevel" type="hidden" value="0"></input>
    └─ <table align="center" id="tblMain" cellspacing="0" cellpadding="0">
      └─ <tbody>
        └─ <tr>...</tr>
        └─ <tr>
          └─ <td id="mdlft"></td>
          └─ <td id="mdMid">
            └─ <table class="mid" id="tblMid">
              └─ <tbody>
                └─ <tr>...</tr>
                └─ <tr>...</tr>
                └─ <tr>...</tr>
                └─ <tr>...</tr>
                └─ <tr>...</tr>
                └─ <tr>...</tr>
                └─ <tr>
                  └─ <td>
                    └─ <table class="nonMSIE">
                      └─ <colgroup>...</colgroup>
                      └─ <tbody>
                        └─ <tr>
                          └─ <td nowrap="">...</td>
                          └─ <td class="txtpad">
                            └─ <input name="username" class="txt" id="username" type="text" value="" />
                            └─ </td>
                          └─ </tr>
                        └─ <tr>
                          └─ <td nowrap="">...</td>
                          └─ <td class="txtpad">
                            └─ <input name="password" class="txt" id="password" type="password" value="" />
                            └─ </td>
                          └─ </tr>

```

LoginURL

UsernameField

PasswordField



Информация

Для приложения OWA необходимо в реестре отключить **Basic** аутентификацию. Создайте DWORD параметр: "IsBasicDisabled" со значение "1", по пути: HKEY_LOCAL_MACHINE\SOFTWARE\Indeeds-ID\IISHTTPModule\IISConfig\owa

Отключение запроса второго фактора

Вы можете отменить запрос второго фактора аутентификации для пользователей, которые выполняют вход из доверенной сети.

Эту настройку можно указать глобально для всех приложений в рамках одной установки IIS Extension, либо только для определенного приложения. Глобальная настройка необходима, когда в приложениях есть пересекающиеся доверенные сети.

Если вы хотите переопределить существующую глобальную настройку для определенного

приложения или сайта, продублируйте настройку с другими сетями в ключе с именем сайта или приложения.

Чтобы отключить запрос второго фактора, выполните следующие действия:

- Если вам нужна глобальная настройка, в реестре в папке `HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\IISHTTPModule` добавьте параметр типа `REG_SZ` с именем `bypassNetworks` и укажите через запятую IP-адреса с маской подсети (поддерживаются адреса IPv4 и IPv6).
- Если вы хотите указать доверенные сети для определенного приложения или сайта или переопределить глобальную настройку, в ключе `iisconfig` создайте новый ключ с точным именем сайта или приложения IIS и укажите через запятую IP-адреса с маской подсети (поддерживаются адреса IPv4 и IPv6).

 Максимально вы можете указать 252 адреса.

Компьютер\HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\IISHTTPModule\iisconfig\RDWeb			
	Имя	Тип	Значение
	(По умолчанию)	REG_SZ	(значение не присвоено)
	BypassNetworks	REG_SZ	172.16.3.52/32, 172.16.31.61/24, 21:0db8:11a3:09d6:ffff:ffff:ffff/64

Локализация

Для настройки локализации, на машине, с установленным **IIS Extension**, нужно создать в разделе реестра "`HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\IISHTTPModule`" ключ "`LanguageId`" (DWORD).

Варианты значений (десятичные):

1033 - English (по умолчанию)

1049 - Русский

Варианты написания доменного имени



Информация

В IIS Extension не поддерживается настройка входа в OWA по "User name only".

Для корректной работы IIS Extension, доменное имя необходимо записывать в форматах:

- SAM: домен в виде NetBIOS - **indeed\user**;
- UPN: домен в виде DNS - **user@indeed.local**.



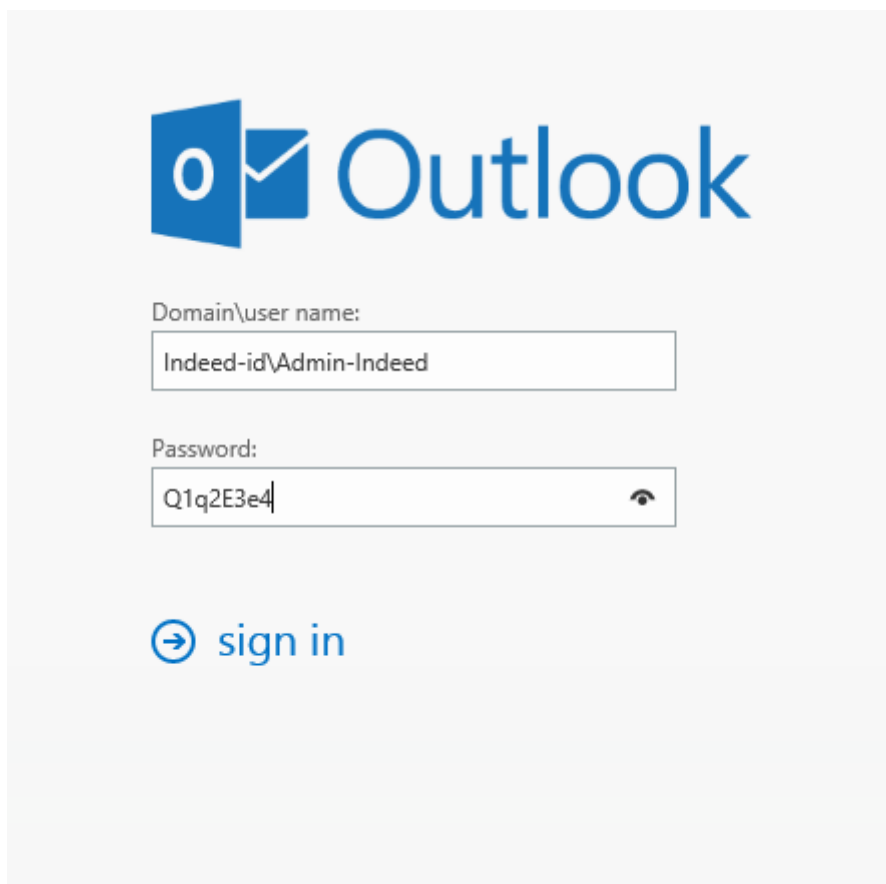
Информация

При включенной нормализации имен (HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\IISHTTPModule ключ DWORD NameTranslationDisabled=0), авторизоваться будет невозможно, если доменное имя введено нестандартным способом:

- SAM: домен в виде DNS вместо NetBIOS **indeed.local/user**
- UPN: домен в виде NetBIOS вместо DNS **user@indeed**

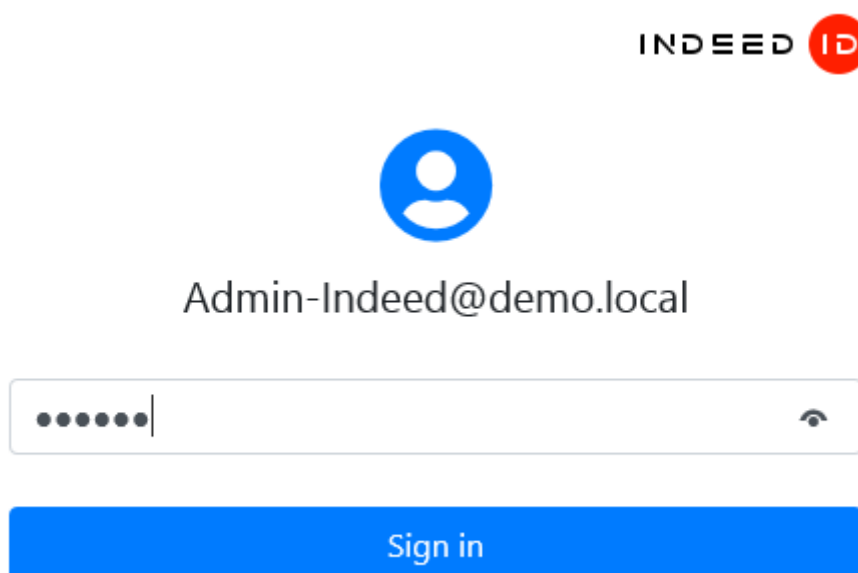
Пример работы расширения

1. Открыть приложение OWA и ввести доменный логин/пароль.



The image shows the Outlook login interface. At the top is the Outlook logo. Below it, there are two input fields. The first is labeled 'Domain\user name:' and contains the text 'Indeed-id\Admin-Indeed'. The second is labeled 'Password:' and contains the text 'Q1q2E3e4'. Below the password field is a small eye icon. At the bottom, there is a blue button with a right-pointing arrow and the text 'sign in'.

2. После корректного ввода появится окно с запросом второго фактора.



The image shows the second factor authentication screen. At the top right is the 'INDEED ID' logo. In the center is a blue circular icon with a white person silhouette. Below it is the email address 'Admin-Indeed@demo.local'. There is a password input field with six dots and a small eye icon. At the bottom is a large blue button with the text 'Sign in'.

3. После успешного ввода откроется приложение.

Примеры внедрения расширения

- [Настройка однофакторной и двухфакторной аутентификации в Remote Desktop Web Access \(RDWeb\) с помощью Indeed IIS Extension](#)
- [Настройка OWA через 1FA в ActiveSync с помощью Indeed-ID IIS Extension](#)

Indeed AM NPS RADIUS Extension

Indeed AM NPS RADIUS Extension (RADIUS Extension) представляет собой модуль расширения Microsoft Network Policy Server (NPS, входит в состав Windows Server) и позволяет реализовать для RADIUS-совместимых сервисов и приложений технологию двухфакторной аутентификации.



Информация

Файлы для Indeed AM NPS Radius Extension расположены: *indeed AM <Номер версии>\Indeed AM RADIUS Extension\<Номер версии>*

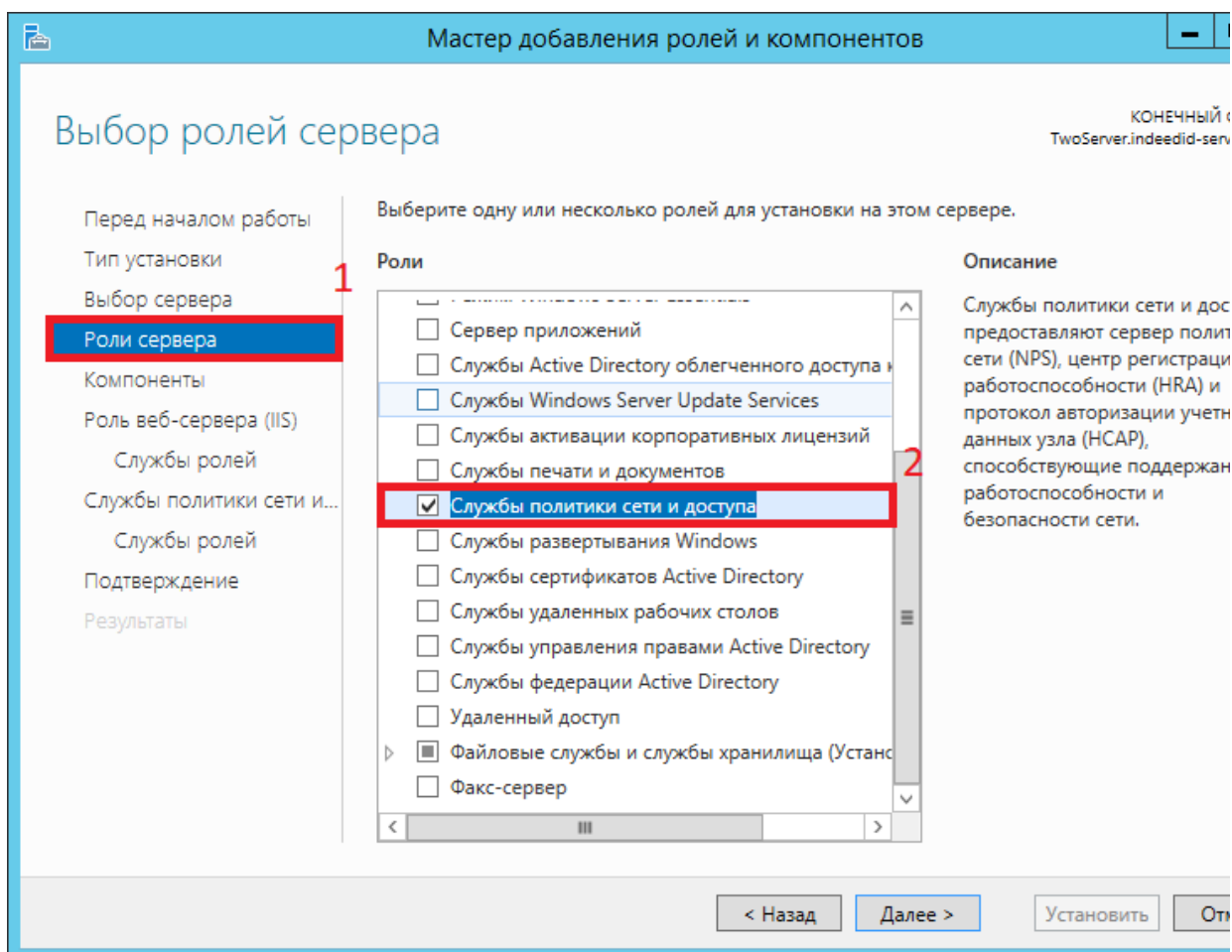
- **IndeedID.EA.RADIUS.Extension-<номер версии>.x64.ru-ru.msi** - Пакет для установки Indeed AM NPS Radius Extension.

Файлы шаблонов политик расположены: *indeed AM <номер версии>\Misc\ADMX Templates*.

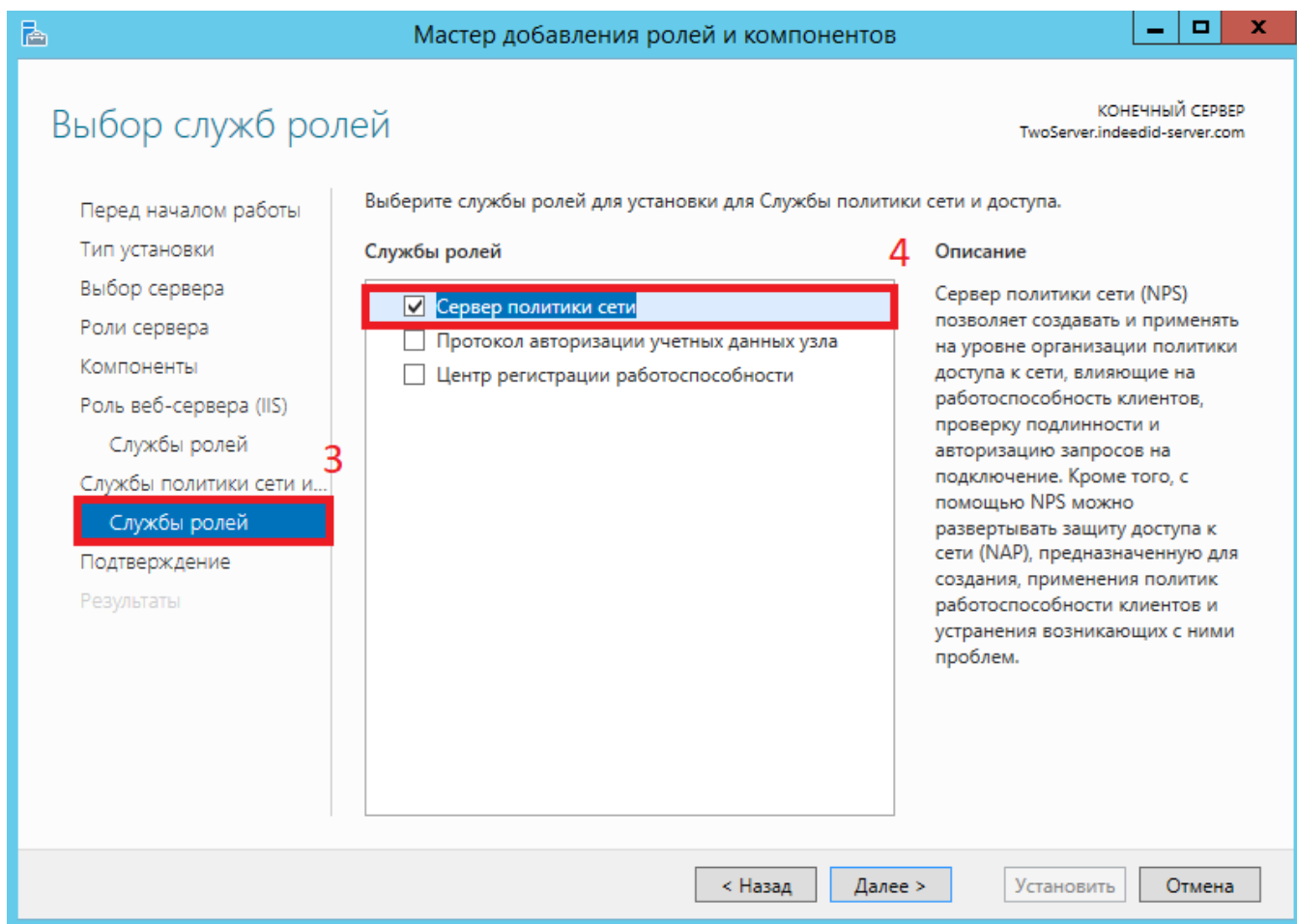
Установка Network Policy Server

1. Запустить **Мастер добавления ролей и компонентов (Add Roles and Features Wizard)**.

2. Из списка ролей выбираем роль **Службы политики сети и доступа (Network Policy and Access Services)**, соглашаемся с установкой дополнительных компонентов.



3. Из списка "Службы ролей" выбираем "Сервер политики сети (Network Policy Server)".



4. В окне "Подтверждение установки компонентов" нажимаем "Установить".

Настройка NPS Сервера

Добавление Radius-клиента

1. Запустите "Сервер сетевых политик".
2. Добавьте в "RADIUS-клиенты" необходимый VPN клиент. Для создания создания клиента нажмите правой кнопкой мыши по "RADIUS - Клиенты" и выберете "Новый документ".



Информация

При использовании проверки подлинности **Chap** необходимо, в параметрах учетной записи пользователя, включить "Хранить пароль, используя обратимое шифрование" и обновить пароль пользователю.

3. В окне "Новый Radius-клиент" выполните настройку клиента.

- а. Добавьте произвольное понятное имя для добавляемого клиента (1).
- б. Укажите IP адрес (2).
- с. Задайте секретный ключ для соединения (3).

Информация

Необходимо указать секретный ключ, который был создан на клиенте. Если подключение со стороны клиента ещё не было настроено, задайте произвольный ключ и запомните его. Данный ключ потребуется указать при настройке подключения со стороны клиента.

Новый RADIUS-клиент

Параметры Дополнительно

☒ Включить этот RADIUS-клиент

☐ Выберите существующий шаблон:

Имя и адрес

Имя (произвольное): VPNServer

Адрес (IP или DNS): 192.168.0.7

Общий секрет

Выберите существующий шаблон общих секретов: Отсутствует

Чтобы ввести общий секрет вручную, щелкните "Вручную". Чтобы автоматически создать общий секрет, щелкните "Создать". Необходимо настроить RADIUS-клиент с введенным здесь общим секретом. В общих секретах учитывается регистр символов.

☒ Вручную ☐ Создать

Общий секрет:

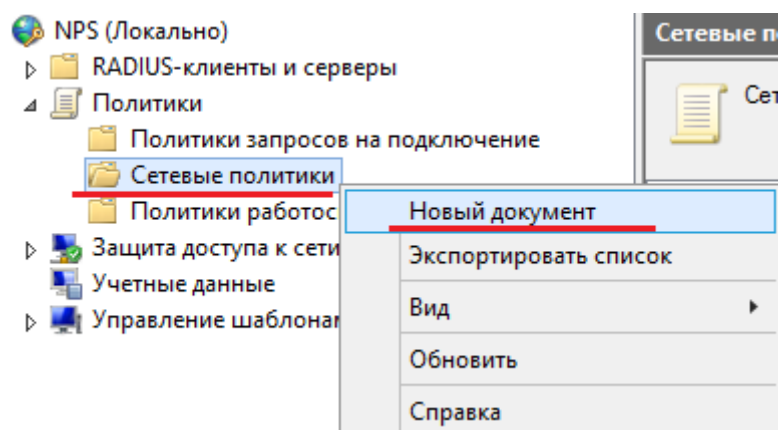
Подтверждение общего секрета:

OK Отмена

Добавление сетевой политики

1. Запустите "Сервер сетевых политик".

2. Раскройте раздел "**Политики**".
3. Нажмите правой кнопкой мыши по разделу "**Сетевые политики**" и выберите "**Новый документ**".



4. В поле "**Имя политики**" укажите произвольное понятное имя для создаваемой политики и нажмите "**Далее**".

Новая политика сети



Укажите имя политики сети и тип подключения

Вы можете указать имя политики сети и тип подключений, к которому применяется политика.

Имя политики:

Netscaler

Способ сетевого подключения

Выберите тип сервера доступа к сети, отправляющего запрос на подключение серверу сетевых политик. Можно выбрать тип сетевого сервера или параметр "Зависящие от поставщика" (ни то, ни другое не является обязательным). Если в качестве сервера сетевых политик используется коммутатор 802.1X или беспроводная точка доступа, выберите "Не указано".

☒ Тип сервера доступа к сети:

Не указано

☐ Зависящие от поставщика:

10

Назад Далее Готово Отмена

5. В окне **"Укажите условия"** добавьте необходимые условия, которые будут проверяться при подключении клиентов. Для добавления нажмите кнопку **"Добавить..."** и выберите необходимое условие. После добавления условия нажмите **"Далее"**.

 Информация

В качестве примера будет добавлено условие **"Группы пользователей"**. При добавлении группы, потребуется указать имя группы пользователей из AD.

Новая политика сети



Укажите условия

Задайте условия, определяющие, используется ли данная политика сети для запросов на подключение. Необходимо указать хотя бы одно условие.

Условия:

Условие	Значение
 Группы пользователей	INDEED\RadiusClient

Описание условия:

Условие "Группы пользователей" указывает, что подключающийся пользователь должен принадлежать к одной из выделенных групп.

Добавить...

Изменить...

Удалить

Назад

Далее

Готово

Отмена

6. В окне **"Укажите разрешения доступа"** выберите **"Доступ разрешен"** и нажмите **"Далее"**.

7. В окне "Настройка методов проверки подлинности" укажите методы проверки подлинности, которые настроены на клиенте, и нажмите "Далее".



Информация

Методы проверки подлинности со стороны Radius сервера и клиента должны совпадать, в противном случае возникнет ошибка аутентификация.

Новая политика сети



Настройка методов проверки подлинности

Настройте один или несколько методов проверки подлинности, которые требуются для соответствия запроса на подключение данной политике. Для проверки подлинности EAP необходимо настроить тип EAP.

Типы EAP согласуются между сервером сетевых политик (NPS) и клиентом в порядке перечисления.

Типы EAP:

Вверх

Вниз

Добавить...

Изменить...

Удалить

Менее безопасные методы проверки подлинности:

- ☒ Шифрованная проверка подлинности (Microsoft), версия 2, (MS-CHAP-v2)
 - ☒ Разрешить смену пароля по истечении срока действия
- ☒ Шифрованная проверка подлинности Майкрософт (MS-CHAP)
 - ☒ Разрешить смену пароля по истечении срока действия
- ☐ Шифрованная проверка подлинности (CHAP)
- ☐ Проверка открытым тестом (PAP, SPAP)
- ☐ Разрешить подключение клиентов без согласования метода проверки подлинности.

Назад

Далее

Готово

Отмена

8. В окнах "Настройка ограничений" и "Настройка параметров" оставьте значения по умолчанию и нажмите "Далее".

9. В окне "Завершение создания политики сети" проверьте данные и нажмите "Готово".

Новая политика сети



Завершение создания политики сети

Успешно создана следующая политика сети:

Netscaler

Условия политики:

Условие	Значение
Группы пользователей	INDEED\RadiusClient

Параметры политики:

Условие	Значение
Метод проверки подлинности	MS-CHAP v1 OR (ИЛИ) MS-CHAP v1 (Разрешить смену па
Права доступа	Разрешение доступа к узлу
Framed-Protocol	PPP
Service-Type	Framed
Игнорировать свойства удаленного доступа пользователя	False (ложь)

Для завершения мастера нажмите кнопку "Готово".

Назад

Далее

Готово

Отмена

Установка Indeed AM NPS RADIUS Extension

1. Выполните установку NPS RADIUS через запуск соответствующего пакета из дистрибутива.
2. В разделе **HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\AuthProxy**. Измените параметры:
 - а. Параметр **ServerUrlBase**. В значении для параметра укажите адрес вашего сервера **Indeed** в формате **http(s)://<DNS_IndeedAM_Server>/am/core/**.

 Информация

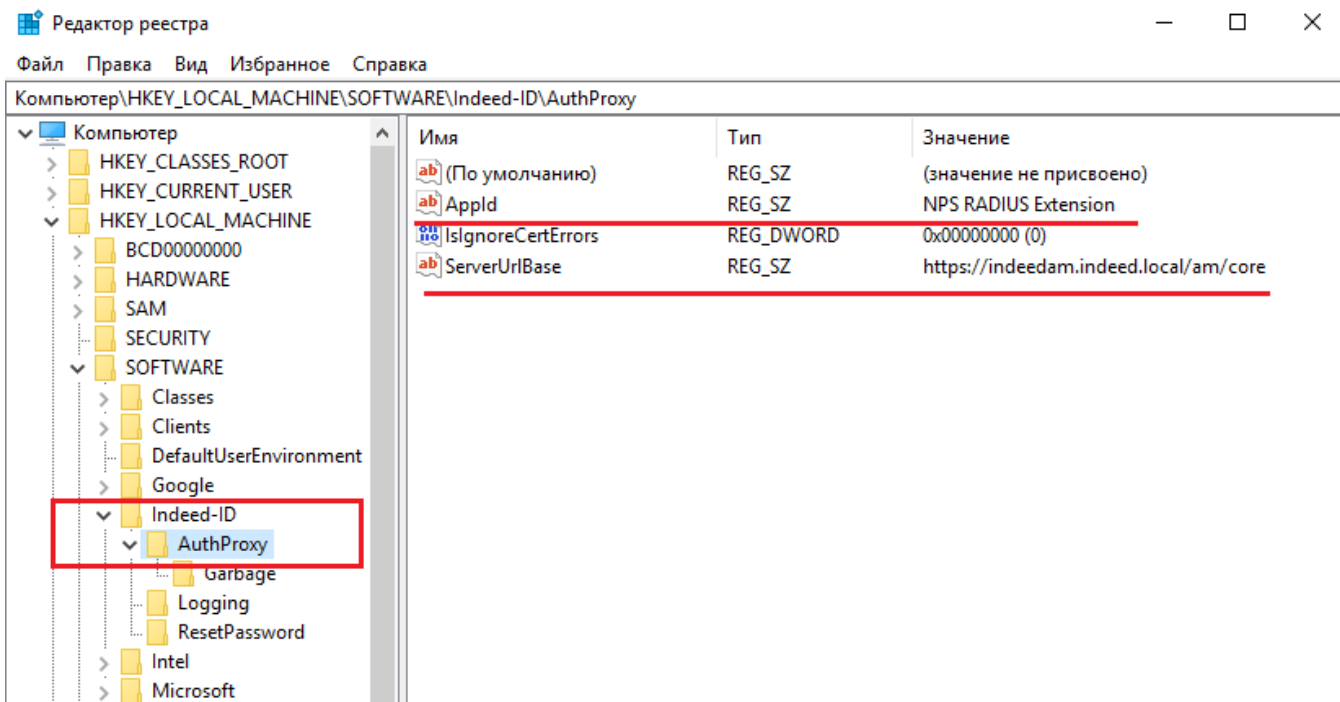
При использовании https соединения требуется выполнить [установку клиентского сертификата](#) на каждый сервер Indeed AM.

- б. Параметр **IsIgnoreCertErrors**, указать значение **0** или **1**.

 Информация

Данный параметр предназначен для игнорирования ошибок сертификата проверки подлинности сервера **Indeed**, при значении **1** происходит игнорирование ошибок сертификата.

- в. Параметр **Appld** со значением **NPS RADIUS Extension**.



Настройка проброса атрибутов Radius

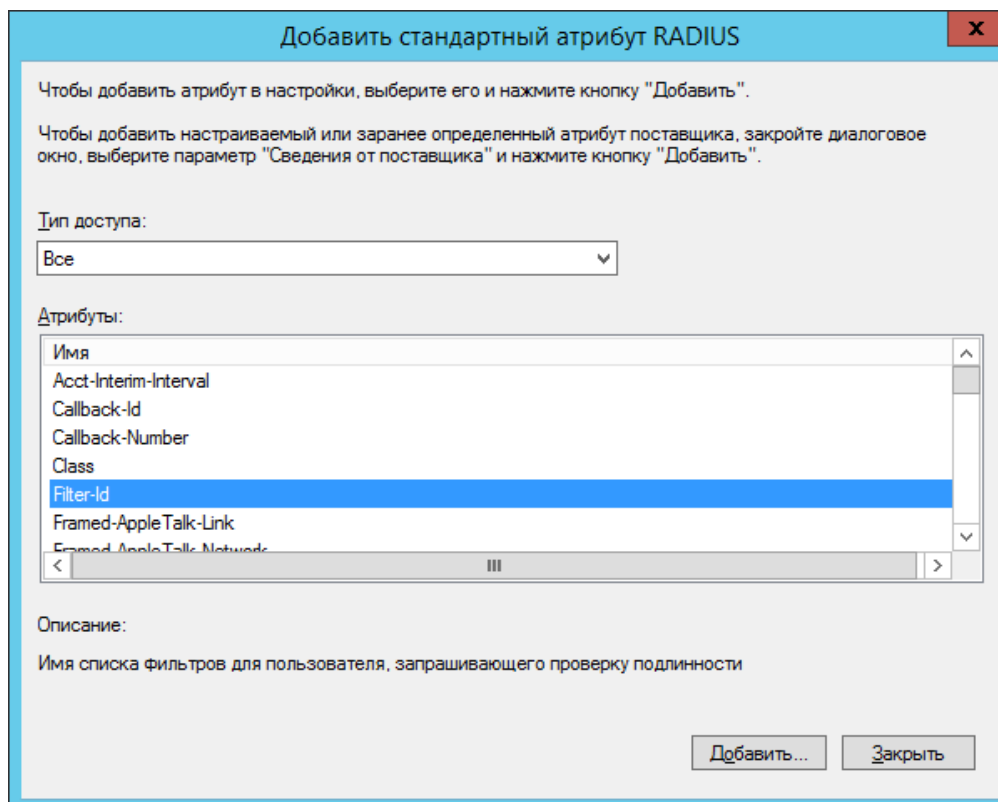
Информация

Данная настройка является опциональной и выполняется только при необходимости проброса атрибутов Radius для клиента.

Информация

Данная настройка позволяет добавить атрибуты в ответ "Access-Accept", которые указаны в сетевой политике NPS сервера.

1. Откройте "**Политику запросов на подключение**".
2. Выберите имеющуюся или создайте новую политику и откройте вкладку "**Параметры**".
3. Выберите параметр "**Стандарт**" и нажмите "**Добавить**".
4. В окне "**Добавить стандартный атрибут Radius**" выберете "**Filter-Id**" и нажмите "**Добавить**".



5. В окне "Сведения об атрибуте" нажмите "Добавить". Убедитесь, что параметр "Формат ввода атрибута" – строковый, и введите строку формата:
IID_CR_AccessAccept_Attributes:<id требуемого атрибута 1>, <id требуемого атрибута 1>

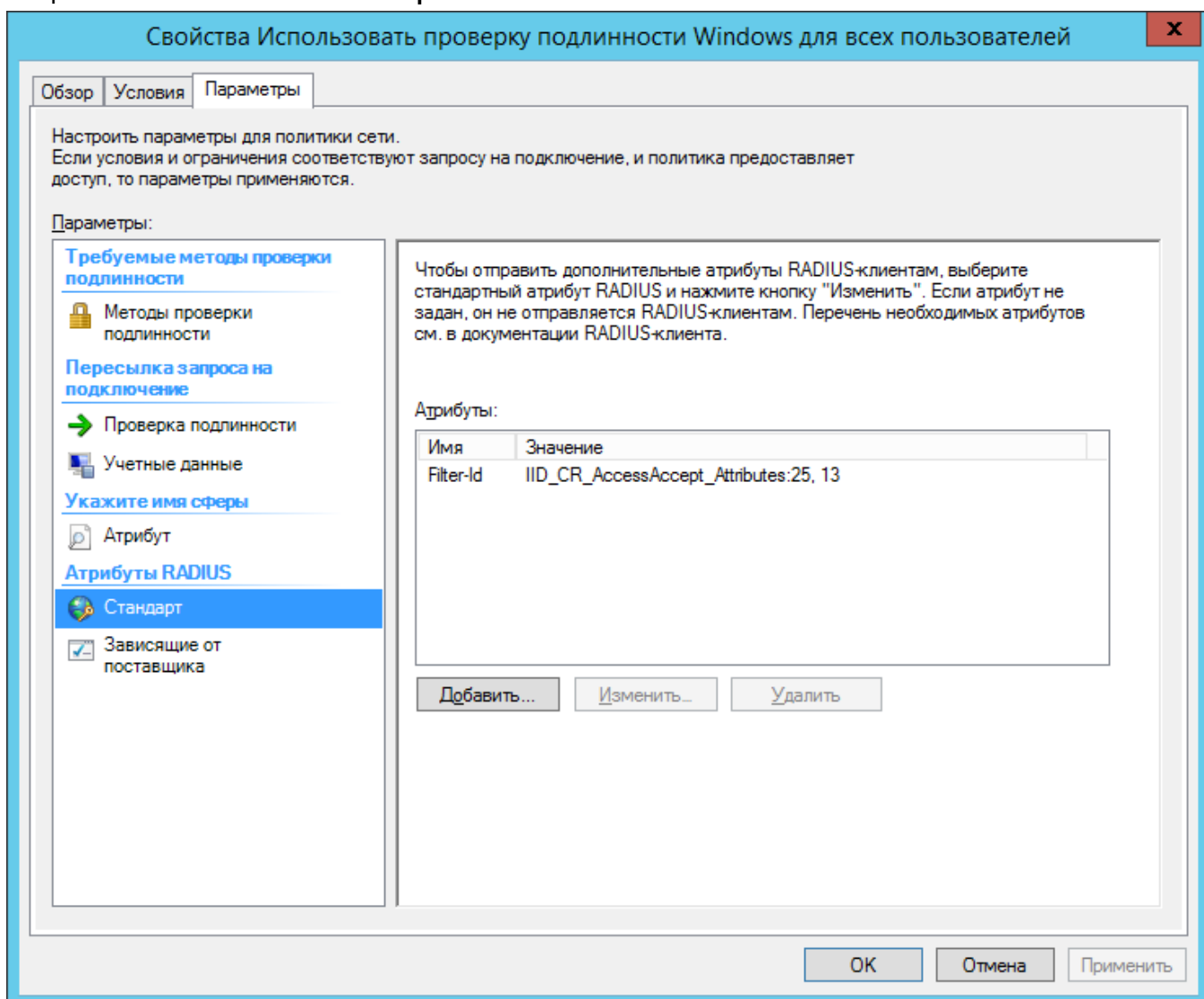
И **Информация**

Если атрибутов несколько, то id атрибутов требуется указывать через запятую.

Пример

IID_CR_AccessAccept_Attributes:25, 13

6. Закройте все окна и нажмите "Применить".



7. Перезапустите службу NPS.

Настройка параметров доступа в политиках на сервере политики сети (NPS)



Информация

Опциональная настройка.

В политике на сервере NPS задаются параметры:

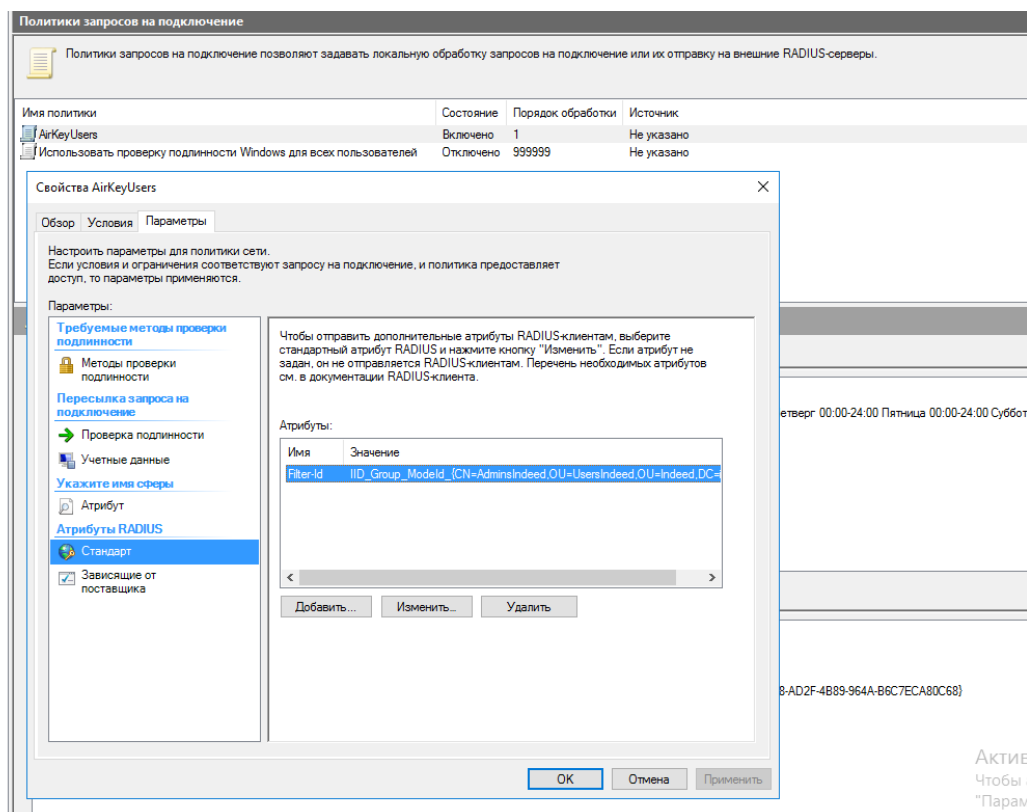
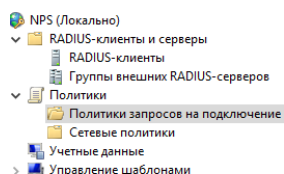
- Общая настройка способа входа
- Настройка способов входа для групп пользователей

Для настройки параметров доступа выполните следующие действия:

1. На сервере сетевых политик (Network Policy Server, NPS) запустите консоль "**Сервер политики сети (Network Policy Server)**" и перейдите в раздел **Политики (Policies)** **Политики запросов на подключение (Connection Request Policies)**.
2. Создайте новую политику или используйте имеющуюся и перейдите в её свойства.
3. На вкладке "**Параметры (Settings)**" перейдите в раздел **Атрибуты RADIUS (RADIUS Attributes)** **Стандарт (Standard)**.
4. Нажмите "**Добавить... (Add..)**", выберите атрибут "**Filter-Id**" и нажмите "**Добавить... (Add...)**".

5. В окне "Сведения об атрибуте (Attribute Information)" укажите необходимые значения, в соответствии с таблицей ниже.

Значение	Описание
ID_Modeld_{ProviderId}	Общая настройка способа входа. Если указано, то пользователи (кроме тех, на которых распространяется действие настройки "Настройка способов входа для групп пользователей") будут использовать указанный провайдер аутентификации Indeed в RADIUS-приложениях. Значение "ProviderId" уникально для каждого провайдера и перечислены в политике "Настройка способов входа для групп пользователей". Пример значения атрибута с Indeed AM Software OTP Provider: ID_Modeld_{B772829C-4076-482B-B9BD-53B55EA1A302}
ID_Group_Modeld_{DN}_{ProviderId}	Настройка способов входа для групп пользователей. Если задано, то пользователи указанной группы Active Directory будут использовать указанный провайдер Indeed AM для аутентификации в RADIUS приложениях. Значение DN – различающееся имя группы (Distinguished Name). При использовании кириллических символов в названиях групп на каждом Сервере политик сети (NPS) необходимо установить русский язык как язык для программ, не поддерживающих Юникод. Без данной настройки членам таких групп будет отказано в аутентификации Сервером политик сети. Пример значения с Indeed AM AirKey Provider: ID_Group_Modeld_{CN=AdminsIndeed,OU=UsersIndeed,OU=Indeed,DC=indeed,DC=local}_{DEEF0CB8-AD2F-4B89-964A-B6C7ECA80C68}



6. Для применения внесенных в политику изменений нажмите "**Применить (Apply)**".

7. Перезапустите службу NPS.

Настройка политик

Информация

Перед настройкой групповой политики необходимо добавить в список административных шаблонов шаблоны политик Indeed AM. Файлы шаблонов политик входят в состав дистрибутива и расположены в каталоге Misc.

Политики применяются к серверам с развернутой ролью NPS и позволяет выполнить дополнительные настройки.

Политики можно настроить как через доменные групповые политики, так и через локальную групповую политику на сервере NPS.

После настройки политик необходимо выполнить перезагрузку службы NPS.

Информация

Действие политики представляет из себя добавление определенных ключей в реестр, при необходимости значения политик можно добавить в реестр вручную.

Настройка способов входа для групп пользователей

Политика задает Id провайдера, который будет использоваться для аутентификации определенной группы пользователей.

Настройка через политику

1. Откройте редактор GPO.
2. Перейдите в раздел "Конфигурация компьютера" "Административные шаблоны" "Indeed ID" "Radius".

3. Откройте политику "Настройка способов входа для групп пользователей".

Состояние	Состояние	Комментарий
EmailOTP		
eTokenPASS		
GoogleOTP		
SMSOTP		
Настройка способов входа для групп пользователей	Включена	Нет
Настройки Challenge\Response	Не задана	Нет
Настройки записи событий	Не задана	Нет
Настройки кэширования групп пользователей	Не задана	Нет

4. Включите (1) данную политику и нажмите "Показать..." для настройки (2).

Настройка способов входа для групп пользователей

Настройка способов входа для групп пользователей

Предыдущий параметр Следующий параметр

☐ Не задано Комментарий:

☒ Включено 1

☐ Отключено

Требования к версии: Windows XP и более поздние версии

Параметры: Справка:

Соответствие групп пользователей и провайдеров аутентификации:

Показать... 2

Данная политика позволяет задать Id провайдера, который будет использоваться для аутентификации оп... группы пользователей.

Введите в поле "Value Name" distinguished name, а в поле "Value" id провайдера аутентификации.

Например:

5. Укажите в "Имя значения" значение атрибута "DistinguishedName", "ObjectGUID" или "SID" целевой группы пользователей.
6. В "Значение" укажите ключ используемого провайдера.

Информация

Параметр **"Значение"** может иметь разные **ID** провайдеров:

{EBB6F3FA-A400-45F4-853A-D517D89AC2A3} - **SMS OTP**

{3F2C1156-B5AF-4643-BFCB-9816012F3F34} - **StorageSms OTP**

{093F612B-727E-44E7-9C95-095F07CBB94B} - **EMAIL OTP**

{B772829C-4076-482B-B9BD-53B55EA1A302} - **Software OTP**

{631F1011-2DEE-47C5-95D8-75B9CAED7DC7} - **HOTP Provider**

{CEB3FEAF-86ED-4A5A-BD3F-6A7B6E60CA05} - **HTOTP Provider**

{DEEF0CB8-AD2F-4B89-964A-B6C7ECA80C68} - **AirKey Provider**

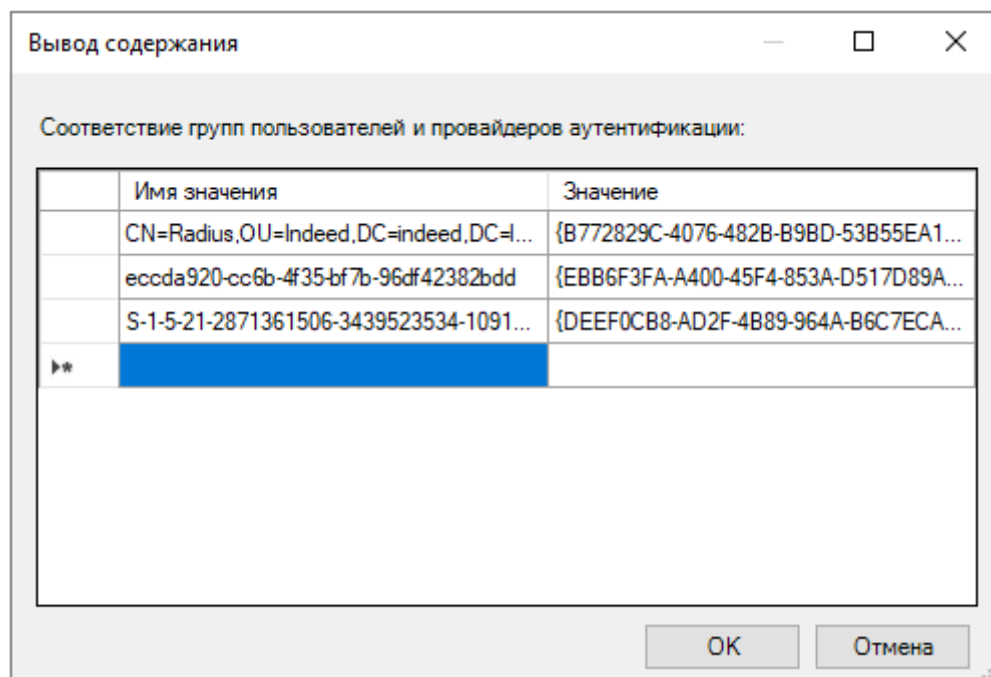
{CA4645CC-5896-485E-A6CA-011FCC20DF1D} - **Telegram OTP**



Для настройки данных провайдеров требуется отключение проверки подлинности запросов на сервере NPS. Настройка выполняется в политике запросов на подключение.

{CB3D3B0A-29C6-4BA4-939D-09B126C10C2E} - **Passcode + GoogleOTP**

{E5D3185C-9A13-4538-BE8F-D4E1C50A329E} - **Passcode + AirKey**



Настройка через реестр

1. Откройте редактор реестра на сервере NPS.
2. Откройте раздел **"HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius"**.

Информация

При необходимости создайте недостающие разделы реестра.

3. Создайте раздел с именем **"GroupDNProviderId"**.
4. Создайте строковый параметр, в качестве имени параметра укажите **"DistinguishedName"**, **"ObjectGUID"** или **"SID"** целевой группы пользователей, в значении укажите ID используемого параметра.

Пример

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius\GroupDNProviderId]
"CN=RadiusClient,OU=UsersIndeed,OU=Indeed,DC=indeed,DC=local"="{EBB6F3FA-A400-45F4-853A-D517D89AC2A3}"
```

Общая настройка способа входа

Настройка политики позволяет задать способ входа, который будет использоваться для аутентификации пользователей.

Настройка через политику

1. Откройте редактор GPO.
2. Перейдите в раздел "Конфигурация компьютера" "Административные шаблоны" "Indeed ID" "Radius".
3. Откройте политику "Общая настройка способа входа".
4. Включите политику и в поле "Способ входа" выберите требуемый провайдер.

Общая настройка способа входа

Общая настройка способа входа

Предыдущий параметр Следующий па

☐ Не задано Комментарий:

☒ Включено

☐ Отключено Требования к версии: Windows XP и более поздние версии

Параметры:

Справка:

Способ входа:

AirKey Cloud

Политика позволяет задать способ входа, который будет использоваться для аутентификации пользователей.

OK Отмена При

Настройка через реестр

1. Откройте редактор реестра на сервере NPS.
2. Откройте раздел "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius".

 Информация

При необходимости создайте недостающие разделы реестра.

3. Создайте строковый параметр с именем "**ProviderId**" в значении укажите требуемый ID провайдера.

 Информация

ID провайдеров указаны выше, в информационном блоке политики "**Настройка способов входа для групп пользователей**".

Пример

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius]
"ProviderId"="{B772829C-4076-482B-B9BD-53B55EA1A302}"
```

Настройка таймаута сессии Challenge\Response

Позволяет задать таймаут сессии при использовании провайдера аутентификации, поддерживающего Challenge\Response.

Настройка через политику

1. Откройте редактор GPO.
2. Перейдите в раздел "Конфигурация компьютера" "Административные шаблоны" "Indeed ID" "Radius".
3. Откройте политику "Настройка таймаута сессии Challenge\Response".
4. Включите политику и в поле "Таймаут сессии в секундах" укажите необходимое значение.

Настройки таймаута сессии Challenge\Response

Настройки таймаута сессии Challenge\Response

Предыдущий параметр Следующий параметр

☐ Не задано Комментарий:

☒ Включено

☐ Отключено

Требования к версии: Windows XP и более поздние версии

Параметры: Таймаут сессии в секундах: 30

Справка: Позволяет задать таймаут сессии при использовании провайдера аутентификации, поддерживающего Challenge \Response.

OK Отмена Применить

Настройка через реестр

1. Откройте редактор реестра на сервере NPS.
2. Откройте раздел "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius".

 Информация

При необходимости создайте недостающие разделы реестра.

3. Создайте параметр типа "DWORD" с именем "SessionLifetimeSec" в качестве значения укажите таймаут сессии в секундах в десятичном формате.

Пример

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius]
"SessionLifetimeSec"=dword:0000001e
```

Challenge\Response: сообщение пользователю

Политика позволяет задать сообщение пользователю при использовании Challenge\Response.

Настройка через политику

1. Откройте редактор GPO.
2. Перейдите в раздел "Конфигурация компьютера" "Административные шаблоны" "Indeed ID" "Radius" "<Имя используемого провайдера>".
3. Откройте политику "Challenge\Response сообщение пользователю".
4. Включите политику и в поле "Сообщение пользователю" введите необходимый текст.

Challenge\Response: сообщение пользователю

Challenge\Response: сообщение пользователю

Предыдущий параметр Следующий параметр

☐ Не задано Комментарий:

☒ Включено

☐ Отключено

Требования к версии: Windows XP и более поздние версии

Параметры: Справка:

Сообщение пользователю:

Введите пароль:

Позволяет задать сообщение пользователю при использовании Challenge\Response.

OK Отмена Применить

Настройка через реестр

1. Откройте редактор реестра на сервере NPS.
2. Откройте раздел "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius".

Информация

При необходимости создайте недостающие разделы реестра.

3. Создайте раздел с именем необходимого провайдера: **EmailOTP**, **eTokenPASS**, **GoogleOTP**, **SMSOTP**.
4. Создайте строковый параметр с именем формата "<имя используемого провайдера>ChallengeResponseReplyMessage", например, "**eTokenPassChallengeResponseReplyMessage**".
5. В качестве значения укажите текст, который будет отображаться пользователю.

Пример

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius>EmailOTP]
"EmailOTPChallengeResponseReplyMessage"="EmailOTP:"
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius\eTokenPASS]
"eTokenPassChallengeResponseReplyMessage"="eTokenPASS OTP: "
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius\GoogleOTP]
"GoogleOTPChallengeResponseReplyMessage"="Software TOTP OTP: "
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius\SMSOTP]
"SMSOTPChallengeResponseReplyMessage"="SMS OTP: "
```

Кэширование групп пользователей

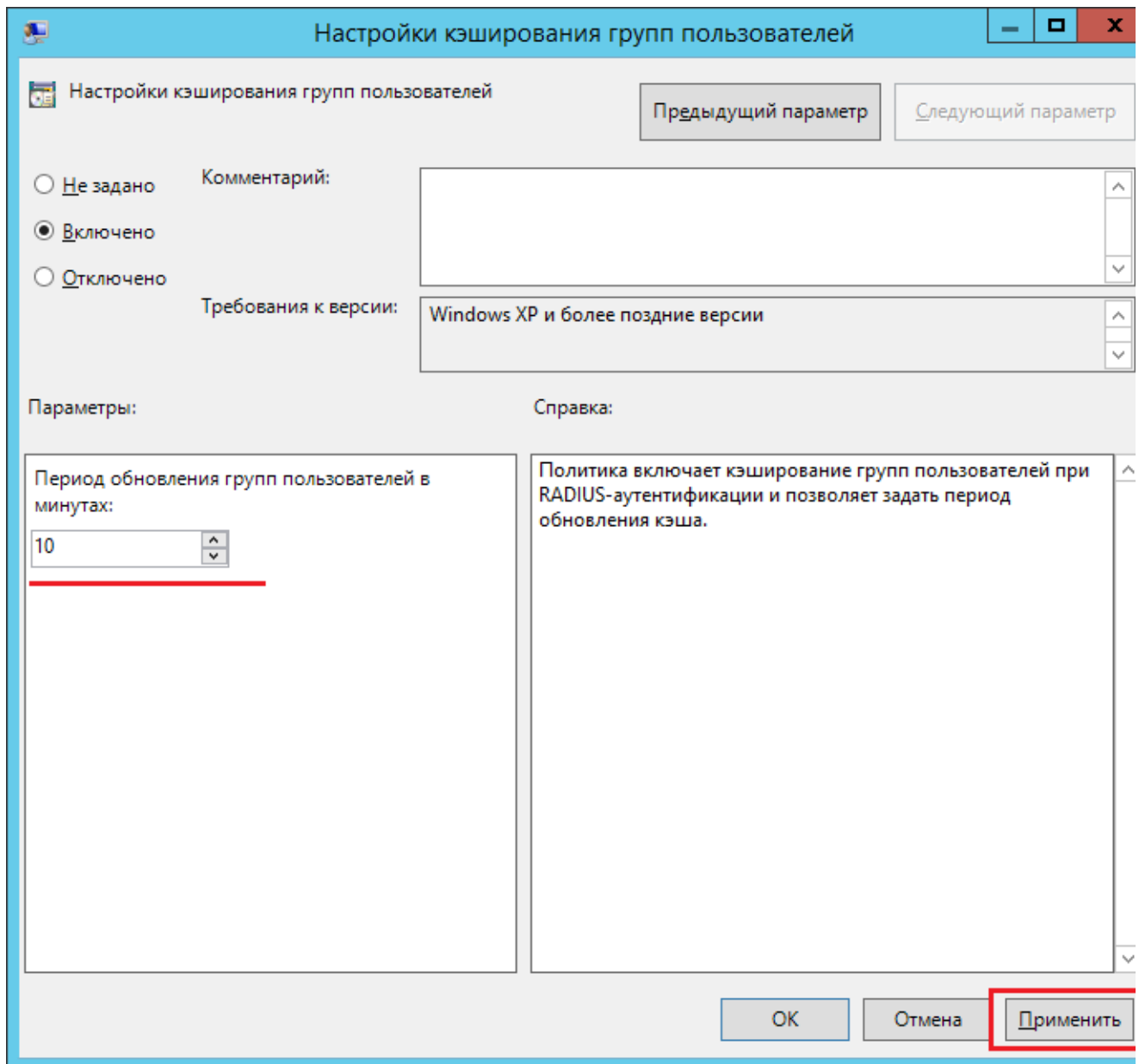
Политика включает кэширование групп пользователей при RADIUS-аутентификации и позволяет задать период обновления кэша.

Информация

Если NPS RADIUS Extension или Indeed AM Server долго отвечают во время работы под нагрузкой с большим количеством пользователей, то необходимо отключить данную настройку.

Настройка через политику

1. Откройте редактор GPO.
2. Перейдите в раздел "Конфигурация компьютера" "Административные шаблоны" "Indeed ID" "Radius".
3. Откройте политику "Настройки кэширования групп пользователей".
4. Включите политику и в поле "Период обновления групп пользователей в минутах" укажите требуемое значение в минутах.



Настройка через реестр

1. Откройте редактор реестра на сервере NPS.
2. Откройте раздел "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius".

Информация

При необходимости создайте недостающие разделы реестра.

3. Создайте параметр типа "DWORD" с именем "UserGroupsCachingEnabled", в значении параметра укажите 1.
4. Создайте параметр типа "DWORD" с именем "UserGroupsCacheUpdateMin", в значении параметра укажите десятичное число в минутах.

Пример

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius]

"UserGroupsCachingEnabled"=dword:00000001

"UserGroupsCacheUpdateMin"=dword:00000021

Настройка имени пользователя

Политика позволяет настроить использование NetBIOS имени домена в случае указания имени пользователя без домена.

Настройка через политику

1. Откройте редактор GPO.
2. Перейдите в раздел "Конфигурация компьютера" "Административные шаблоны" "Indeed ID" "Radius".
3. Откройте политику "Настройка имени пользователя".
4. Включите политику и активируйте параметр: "Использовать NetBIOS имя домена в случае указания имени пользователя без домена".

Настройка имени пользователя

Настройка имени пользователя

Предыдущий параметр Следующий параметр

☐ Не задано Комментарий:

☒ Включено

☐ Отключено

Требования к версии: Windows XP и более поздние версии

Параметры:

☒ Использовать NetBIOS имя домена в случае указания имени пользователя без домена

Справка: Политика позволяет настроить использование NetBIOS имени домена в случае указания имени пользователя без домена

OK Отмена Применить

Настройка через реестр

1. Откройте редактор реестра на сервере NPS.
2. Откройте раздел "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius".

 Информация

При необходимости создайте недостающие разделы реестра.

3. Создайте параметр типа "DWORD" со значением "1" и с именем "UseNetBiosDomainName".

Пример

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius]
"UseNetBiosDomainName"=dword:00000001
```

Настройка кэширования сессий запросов пользователей

Политика включает кэширование сессий запросов пользователей при RADIUS-аутентификации и позволяет задать время жизни сессии запроса в секундах.

Настройка через политику

1. Откройте редактор GPO.
2. Перейдите в раздел "Конфигурация компьютера" "Административные шаблоны" "Indeed ID" "Radius".
3. Откройте политику "Настройка кэширования сессий запросов пользователей".
4. Включите политику и в поле "Время жизни сессии запроса в секундах" укажите значение.

Настройки кэширования сессий запросов пользователей

Настройки кэширования сессий запросов пользователей

Предыдущий параметр Следующий параметр

☐ Не задано Комментарий:

☒ Включено

☐ Отключено

Требования к версии: Windows XP и более поздние версии

Параметры: Справка:

Время жизни сессии запроса в секундах:
60

Политика включает кэширование сессий запросов пользователей при RADIUS-аутентификации и позволяет задать время жизни сессии запроса в секундах.

OK Отмена Применить

Настройка через реестр

1. Откройте редактор реестра на сервере NPS.
2. Откройте раздел "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius".

 Информация

При необходимости создайте недостающие разделы реестра.

3. Создайте параметр типа "DWORD" с именем "RequestSessionCachingEnabled", в значении параметра укажите 1.
4. Создайте параметр типа "DWORD" с именем "RequestSessionLifetimeSec", в значении параметра укажите десятичное число в секундах.

Пример

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius]

"RequestSessionCachingEnabled"=dword:00000001

"RequestSessionLifetimeSec"=dword:0000003c

Примеры внедрения расширения

1. Настройка Cisco ASA для аутентификации через Indeed NPS RADIUS Extension
2. Настройка FortiGate VM для двухфакторной аутентификации через Indeed NPS Radius Extension
3. Установка и настройка аутентификации по OTP в Citrix Netscaler

Indeed AM RDP Windows Logon

Модуль **Indeed AM RDP Windows Logon** позволяет реализовать возможность двухфакторной аутентификации с помощью технологии Indeed AM в процессе подключения по **RDP** или **Remote App**. В качестве второго фактора могут выступать мастер-пароль (**провайдер Passcode**), одноразовый пароль, сгенерированный мобильным приложением (**провайдер Software OTP**), одноразовый пароль, отправленный по SMS или email.

Информация

Файлы для Indeed AM RDP Windows Logon расположены: *indeed AM <Номер версии>\Indeed AM RDP Windows Logon\<Номер версии>*

- **Indeed.EA.RDPWindowsLogon-<номер версии>.x64.ru-ru.msi** - Пакет для установки RDP Windows Logon для x64 битных машин.
- **Indeed.EA.RDPWindowsLogon-<номер версии>.x86.ru-ru.msi** - Пакет для установки RDP Windows Logon для x32 битных машин.

Установка и настройка RDP Windows Logon

Информация

Для работы расширения требуется включение NLA для пользователя.

1. Выполнить установку RDP Windows Logon через запуск соответствующего пакета.
2. Открыть редактор реестра **Windows**.
3. Создать в разделе **HKEY_LOCAL_MACHINE\SOFTWARE** ключ **Indeed-ID** с вложенным ключом **RemoteAuth**.
4. В разделе **RemoteAuth** создать:

- а. Строковый параметр **ProviderId** и задать значение, соответствующее используемому провайдеру.

Информация

ProviderId может иметь разные ID провайдеров:

{EBB6F3FA-A400-45F4-853A-D517D89AC2A3} - **SMS OTP**

{093F612B-727E-44E7-9C95-095F07CBB94B} - **EMAIL OTP**

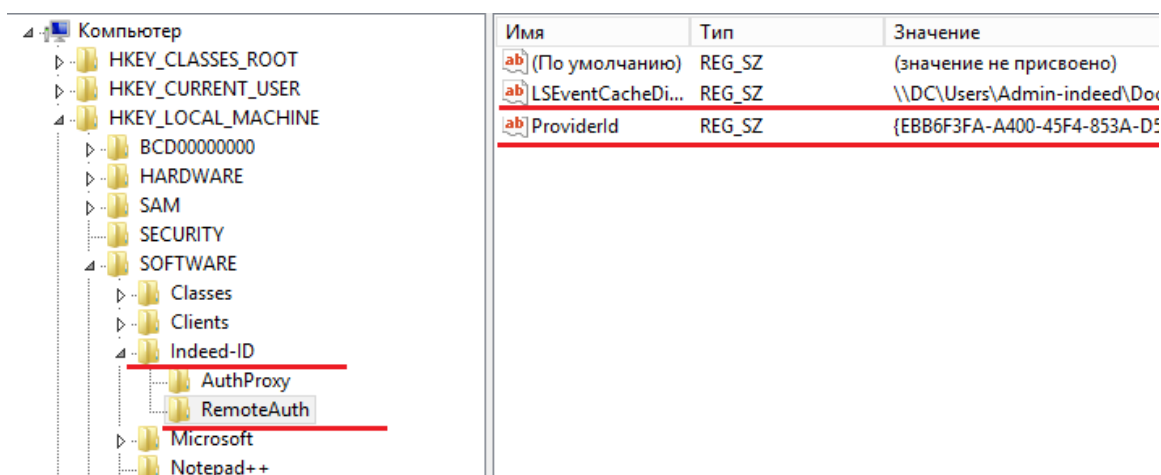
{F696F05D-5466-42b4-BF52-21BEE1CB9529} - **Passcode**

{0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0} - **Software OTP**

{AD3FBA95-AE99-4773-93A3-6530A29C7556} - **HOTP Provider**

{CEB3FEAF-86ED-4A5A-BD3F-6A7B6E60CA05} - **TOTP Provider**

{DEEF0CB8-AD2F-4B89-964A-B6C7ECA80C68} - **AirKey Provider**



5. В разделе **HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\AuthProxy**. Измените параметры:

- a. Параметр **ServerUrlBase**. В значении для параметра укажите адрес вашего сервера **Indeed**.



Информация

При использовании https соединения требуется выполнить [установку клиентского сертификата](#) на каждый сервер Indeed AM.

- b. Параметр **IgnoreCertErrors**, указать значение **0** или **1**.



Информация

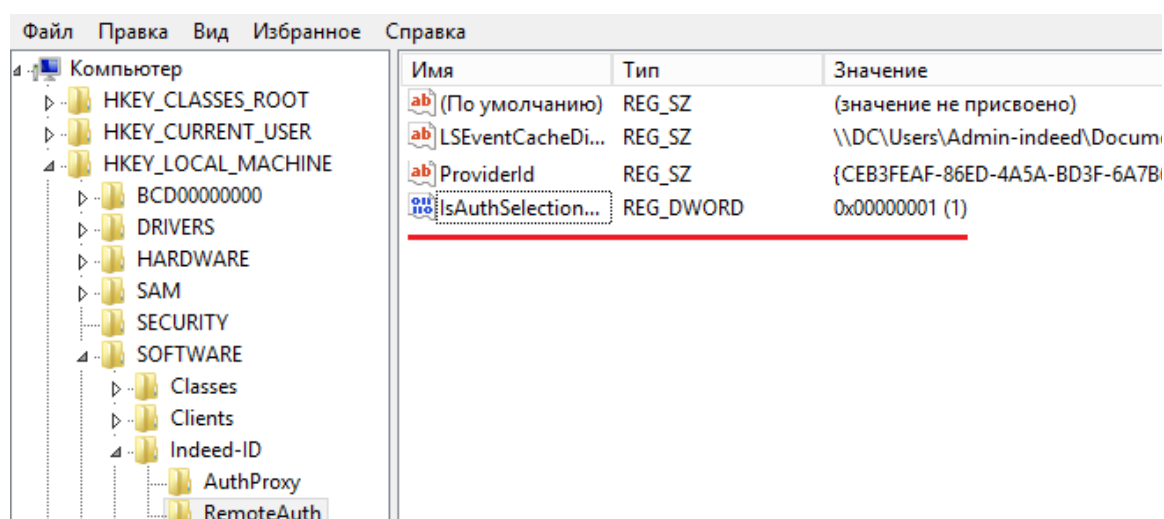
Данный параметр предназначен для проверки сертификата сервера **Indeed**, при значении **1** происходит игнорирование ошибок сертификата.

- c. Параметр **Appld** со значением **RDP Windows Logon**.

Name	Type	Data
(Default)	REG_SZ	(value not set)
Appld	REG_SZ	RDP Windows Logon
IgnoreCertErrors	REG_DWORD	0x00000000 (0)
ServerUrlBase	REG_SZ	https://haproxy.indeed.local/am/

6. Для настройки выбора провайдера аутентификации на стороне пользователя выполните:

- а. В разделе **HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\RemoteAuth** реестра Windows создайте параметр **DWORD** с именем **IsAuthSelectionEnabled**
- б. Определите значение параметра **IsAuthSelectionEnabled** равное 1. Если параметр не задан или его значение 0, то выбор провайдера аутентификации предоставляться не будет. В этом случае будет использоваться провайдер, указанный в значении **ProviderId** или **Indeed AM Passcode Provider**, если **ProviderId** не указан. Если **IsAuthSelectionEnabled=1** и указан провайдер в **ProviderId**, то при подключении пользователя будет выбран указанный провайдер, но пользователь сможет выбрать любой другой из числа поддерживаемых.



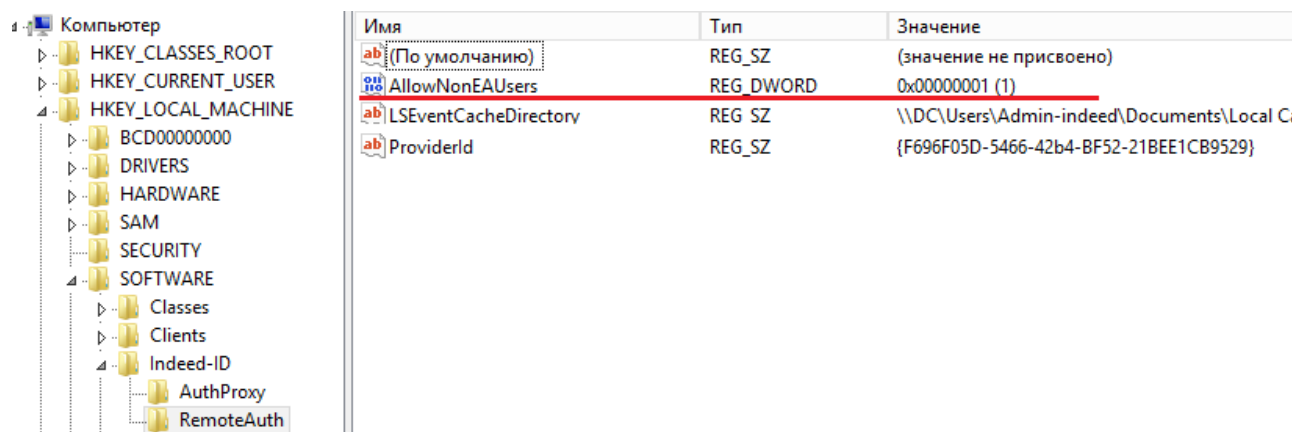
7. Аутентификация пользователей без лицензии на Indeed AM.

По умолчанию **Indeed AM RDP Windows Logon** работает с пользователями, обладающими лицензией **AM RDP Windows Logon**. Для включения аутентификации пользователей без лицензии **RDP Windows Logon** выполните следующие действия:

- Откройте редактор реестра Windows.
- В разделе **HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\RemoteAuth** создайте параметр **DWORD** с именем **AllowNonEAUsers**.

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 не состоит в политике - На пользователей 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 пользователей не действует настройка **AllowNonEAUsers**. Всегда происходит попытка входа с автозахватом лицензии.
- Если значение параметра **AllowNonEAUsers** равно **1**, то пользователи без лицензии RDP WL 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 WL. Пользователь без лицензии аутентифицироваться не сможет.



Настройка одновременной работы с Indeed AM Windows Logon

При условии, что используется сценарий с установкой на одной машине **RDP Windows Logon** и **Windows Logon**, необходимо настроить политику для **Windows Logon**. Для этого:

Через GPO

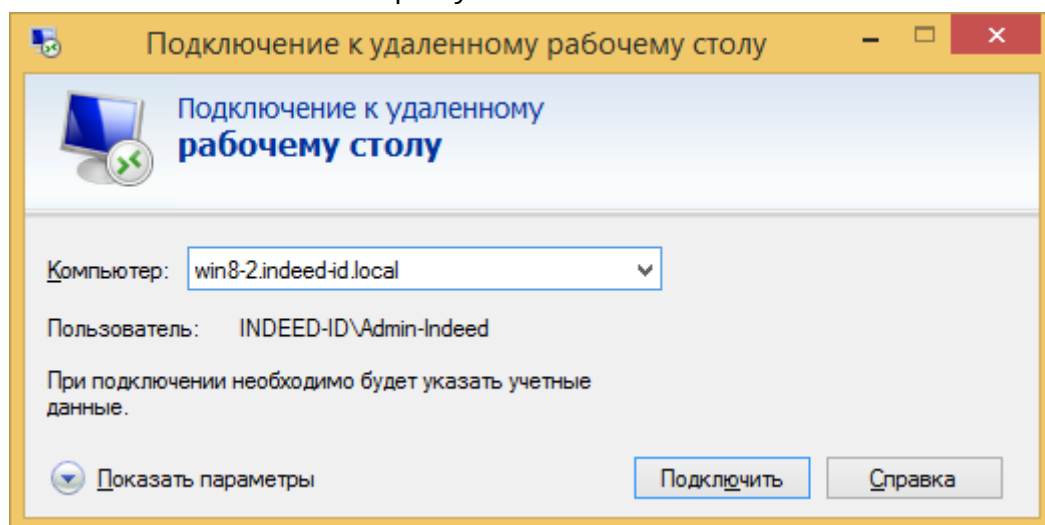
1. Перейдите на машину, на которой установлены компоненты **RDP Windows Logon** и **Windows Logon**;
2. Откройте редактор GPO;
3. Перейдите: **Конфигурация компьютера** **Административные шаблоны** **Indeed ID Windows Logon**;
4. Включите политику "**Настройки Credential Provider**" и установите параметр "**Отображение способов входа**" на "**Все, кроме пароля**".

Через реестр

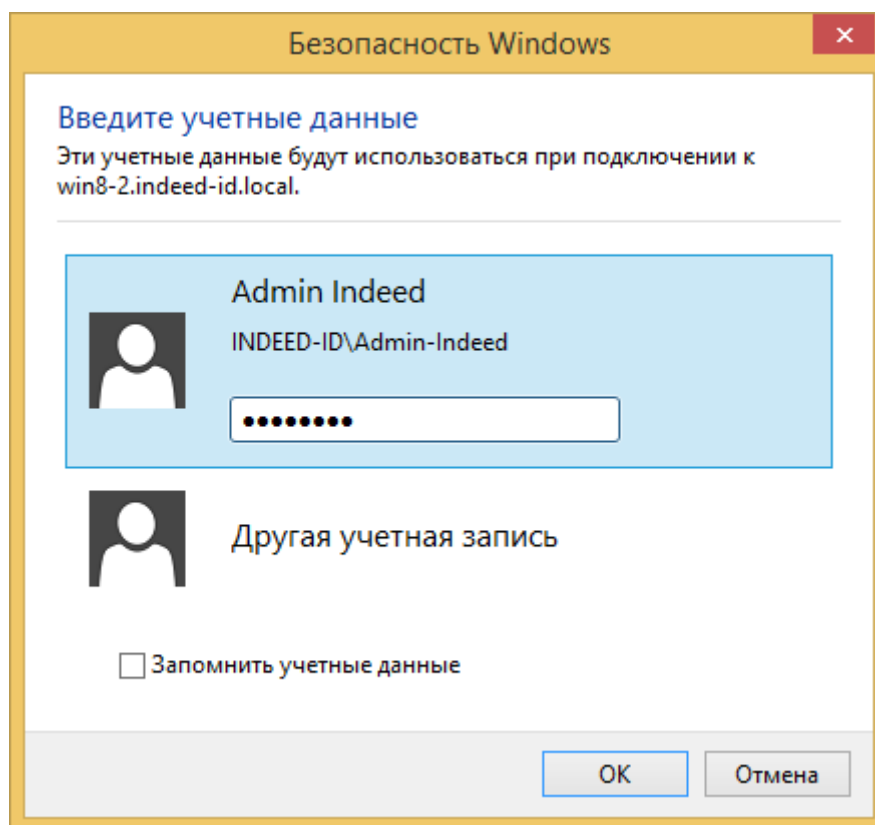
1. Перейдите на машину, на которой установлены компоненты **RDP Windows Logon** и **Windows Logon**;
2. Откройте редактор реестра;
3. Перейдите: **Компьютер\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Logon for Windows**;
4. Создайте параметр DWORD "**CredProvFilter**" и установите ему значение **2**.

Пример работы расширения

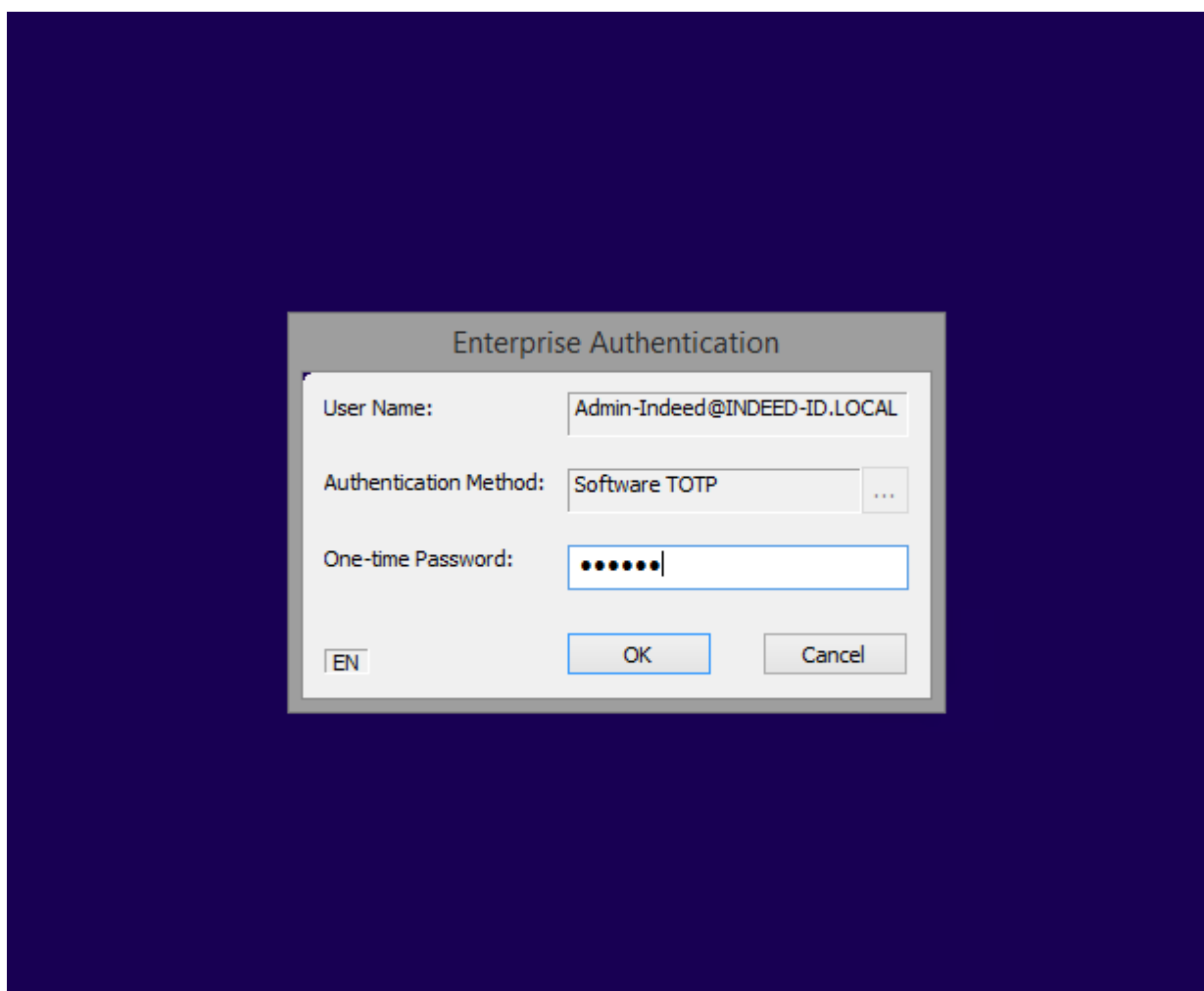
1. Подключаемся к машине на которой установлен **WL RDP**.



2. Указываем пользователя и доменный пароль и нажимаем "Ок".



3. Вводим одноразовый пароль.



Indeed AM Windows Logon

Описание

Возможности Indeed AM Windows® Logon

Продукт Indeed AM Windows® Logon предоставляет пользователям следующие возможности:

- Доступ в операционную систему по паролю учетной записи
- Доступ в операционную систему с применением технологии аутентификации Indeed AM
- Доступ к удаленному рабочему столу с применением технологии аутентификации Indeed AM
- Доступ в операционную систему по кэшированному аутентификатору при отсутствии связи с сервером Indeed.

С целью обеспечения безопасности данных во время отсутствия пользователя на рабочем месте Indeed AM Windows® Logon поддерживает как ручную блокировку рабочей станции, так и автоматическую блокировку (при извлечении устройства аутентификации или использовании экранной заставки). Независимо от способа блокировки для разблокирования рабочей станции всегда требуется повторное подтверждение личности пользователя с помощью аутентификатора.

Дополнительные возможности

Дополнительные возможности, предоставляемые продуктом Indeed AM Windows® Logon, включают:

- Возможность самостоятельной регистрации аутентификаторов и управления ими с помощью приложения "Indeed AM – Управление аутентификаторами".
- Функцию **Indeed AM Paste** – автоматическая подстановка пароля в скрытом виде в нужное поле при нажатии определенной комбинации "горячих клавиш".

Поддерживаемые технологии аутентификации

Продукт Indeed AM Windows® Logon поддерживает более 20 современных технологий аутентификации. К ним относятся двухфакторная аутентификация, биометрическая аутентификация, сертификаты, бесконтактные карты, одноразовые пароли, sms-технологии и др.

Для каждой категории пользователей системы Indeed AM Windows® Logon может быть подобрана собственная оптимальная технология аутентификации. Также пользователям может быть разрешено применение несколько технологий:

- технология аутентификации, адаптированная для работы в удаленном режиме;
- комбинация технологий аутентификации (мультифакторная аутентификация).

Установка

1. Для установки компонента **Indeed AM Windows® Logon** запустите программу установки **IndeedID.WindowsLogon.msi** и следуйте указаниям Мастера установки.
2. После завершения установки компонента необходима перезагрузка системы. Нажмите **Да**, чтобы выполнить перезагрузку сразу, или **Нет**, чтобы сделать это позднее вручную.

Информация

Файлы для **Indeed AM Windows Logon** расположены: *indeed AM <Номер версии>*
\Indeed AM Windows Logon\<Номер версии>

- **IndeedID.WindowsLogon.msi** - Пакет для установки **Indeed AM Windows Logon** на 32-битных ОС.
- **IndeedID.WindowsLogon.x64.msi** - Пакет для установки **Indeed AM Windows Logon** на 64-битных ОС.

Файлы шаблонов политик расположены: *indeed AM <номер версии>\Misc\ADMX Templates*.

Информация

Для развертывания **Indeed AM Windows® Logon** на рабочих станциях пользователей в автоматическом режиме удобно использовать механизм групповых политик (Microsoft Group Policy). Или любой другой инструмент, позволяющий массово распространять и устанавливать msi-пакеты на рабочие станции пользователей (например, Microsoft System Center Configuration Manager). Подробнее со способами распространения компонентов системы **Indeed AM** в автоматическом режиме можно ознакомиться в документе [Indeed-Id Руководство по развертыванию системы.pdf](#).

Настройка

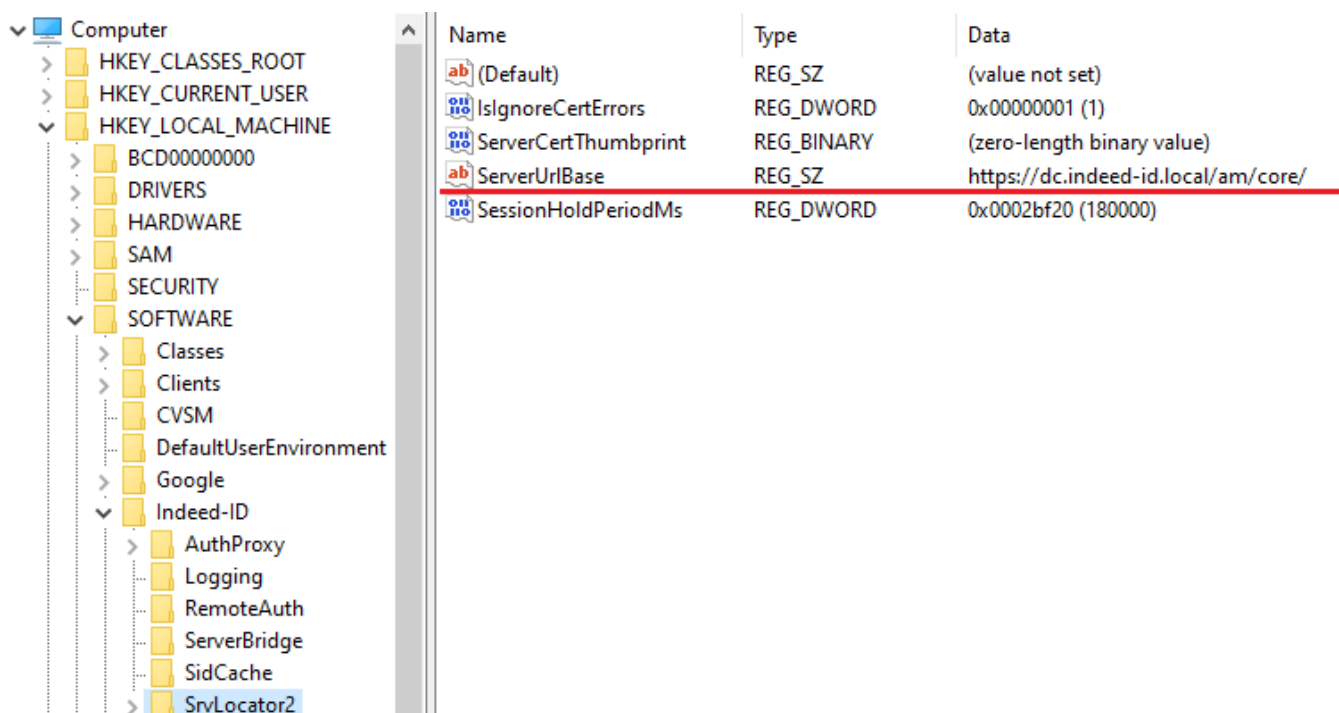
Настройка через реестр

1. Откройте редактор реестра **Windows**.
2. Перейдите в раздел **HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\SrvLocator2**.
3. Измените строковый параметр **ServerUrlBase** и укажите значение URL вашего **Indeed Access Manager Server** (например `http(s)://dc.indeed-id.local/am/core/`).



Информация

При использовании `https` соединения требуется выполнить [установку клиентского сертификата](#) на каждый сервер Indeed AM.



Настройка через GPO



Информация

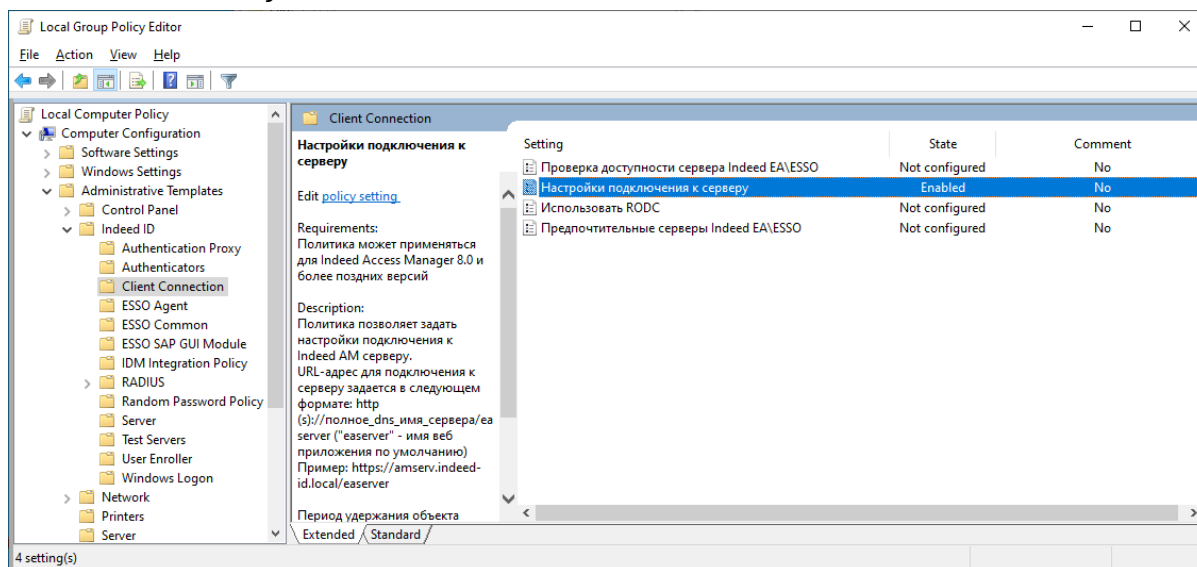
Шаблоны групповых политик расположены *indeed AM\Misc\GroupPolicyTemplates*



Информация

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 значение URL вашего **Indeed Access Manager Server** (например **`http(s)://dc.indeed-id.local/am/core/`**).

Настройки подключения к серверу

Настройки подключения к серверу

☐ Не задано
 ☒ Включено
 ☐ Отключено

Комментарий:

Требования к версии:

Политика может применяться для Indeed Access Manager 8.0 и более поздних версий

Параметры:

URL-адрес AM сервера:

`https://dc.indeed-id.local/am/core/`

☐ Игнорировать ошибки сертификата:

Период удержания объекта сессии (мс):

180000

Справка:

Политика позволяет задать настройки подключения к Indeed AM серверу.
 URL-адрес для подключения к серверу задается в следующем формате: `http(s)://полное_имя_сервера/easerver` ("easerver" - имя веб приложения по умолчанию)
 Пример: `https://amserv.indeed-id.local/easerver`

Период удержания объекта сессии - период удержания объекта сессии для повторного использования при кратковременных разрывах подключения.

Работа с Indeed AM Windows® Logon

Для обеспечения доступа в систему с использованием технологии аутентификации Indeed на вашем рабочем месте должны быть установлены:

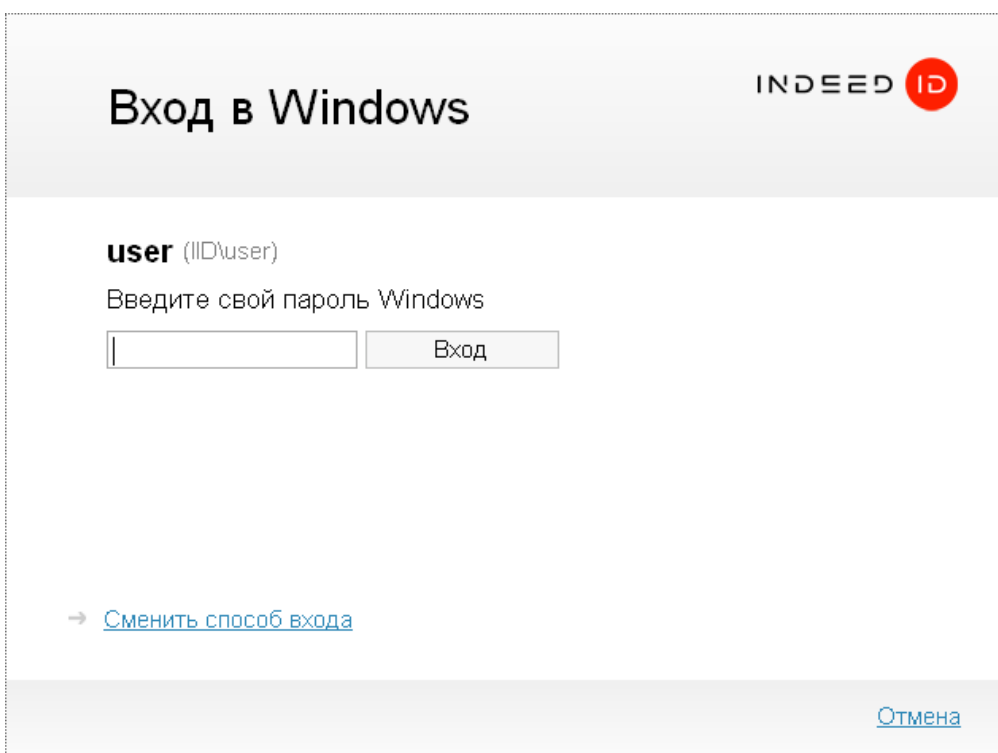
- Модуль **Indeed AM Windows® Logon**, обеспечивающий возможность доступа в систему по аутентификатору.
- Модуль **Indeed AM Provider**, соответствующий выбранной технологии аутентификации.
- Аппаратное устройство аутентификации (в случае необходимости).

Информация

Возможности входа в систему по аутентификатору и управления аутентификаторами доступны только при наличии разрешения, установленного администратором системы.

Первый вход в систему

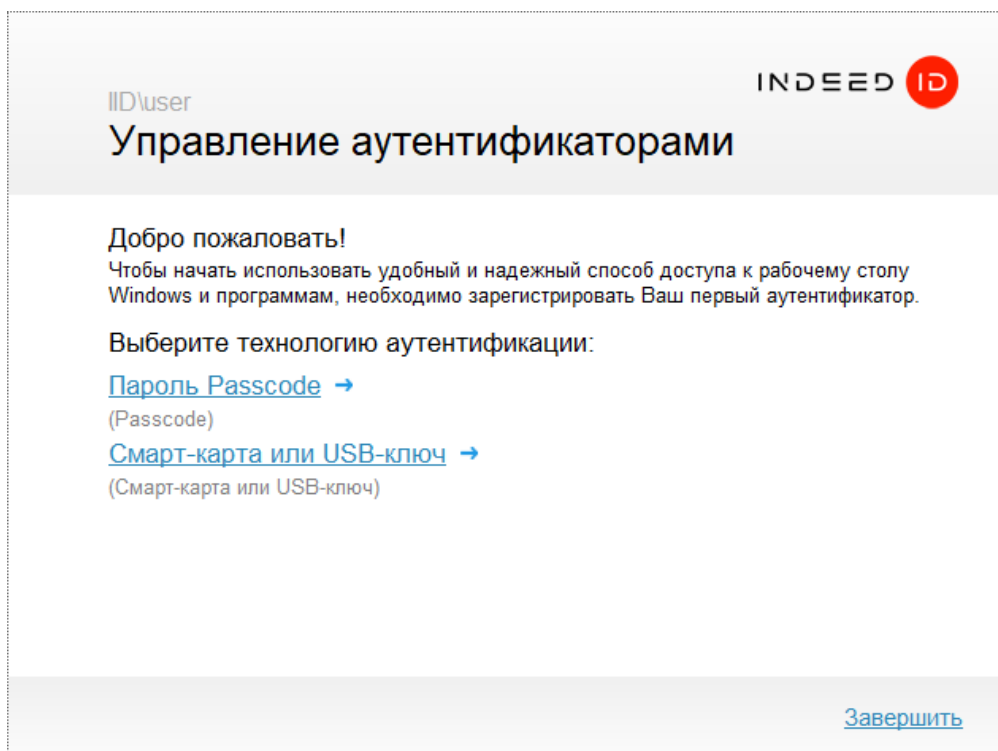
После установки необходимого программного обеспечения на ваш компьютер первый вход в систему осуществляется по паролю учетной записи.



Если для вашей учетной записи разрешена регистрация аутентификаторов, то при входе в систему запустится «Мастер первого входа» (Рисунок 4) и предложит зарегистрировать аутентификатор.

Информация

Мастер первого входа отображается только при условии, что вы являетесь лицензированным пользователем Indeed AM и имеете разрешение на использование технологии аутентификации Indeed AM. Для получения подробной информации обратитесь к администратору системы.



Вы можете зарегистрировать аутентификатор сразу или позднее в любое удобное время.

- Чтобы перейти к регистрации аутентификатора, в окне Управление аутентификаторами выберите один из доступных способов аутентификации (например, «Пароль Passcode»).
- Чтобы выполнить вход 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 найдены необходимые провайдеры Indeed AM, регистрация аутентификаторов невозможна. При отображении данного сообщения обратитесь к администратору системы.

Управление аутентификаторами

Добро пожаловать!

Чтобы начать использовать удобный и надежный способ доступа к рабочему столу Windows и программам, необходимо зарегистрировать Ваш первый аутентификатор.



В системе не обнаружено ни одного провайдера аутентификации. Необходимо установить провайдер и повторно выполнить настройку защищенного входа в систему.

[Завершить](#)

Регистрация первого аутентификатора

Если пользователю разрешено использовать технологию аутентификации Indeed AM, то после входа на рабочую станцию по доменному паролю ему будет предложено зарегистрировать свой первый аутентификатор. Для этого необходимо выбрать способ аутентификации и следовать инструкциям Мастера регистрации аутентификатора. Внешний вид окна и текст подсказок зависят от выбранного способа аутентификации.

- Выполните необходимые действия следуя подсказкам в окне **Управление аутентификаторами**.
- Если вы хотите вернуться на предыдущую страницу и выбрать другой способ входа, нажмите "**Вернуться**".

IID\user

INDEED ID

Управление аутентификаторами



Вставьте смарт-карту или токен

[← Вернуться](#)

[Завершить](#)

После выполнения необходимых действий по регистрации в окне **Управление аутентификаторами** отображается сообщение "**Новый аутентификатор успешно обучен**". Вы можете добавить произвольный текстовый комментарий к зарегистрированному аутентификатору (если данное действие разрешено администратором системы). Для завершения регистрации аутентификатора нажмите "**Сохранить**".

IID\user

INDEED ID

Управление аутентификаторами



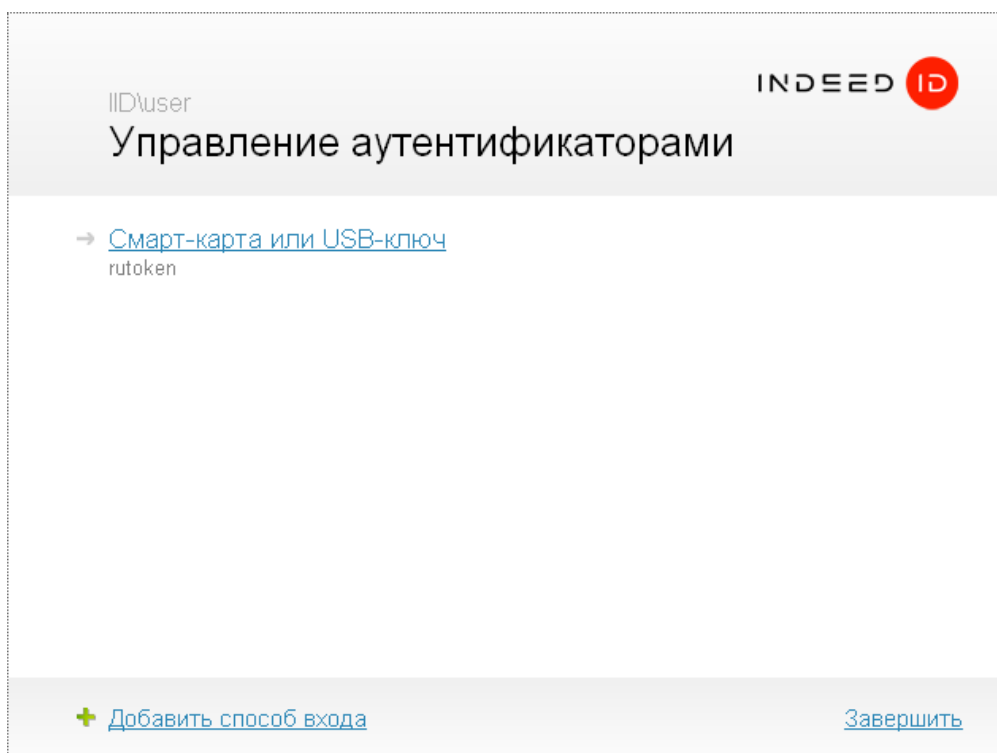
Новый аутентификатор успешно обучен

Все готово для регистрации аутентификатора в системе.
Перед сохранением вы можете задать комментарий
к аутентификатору:

Сохранить

[Завершить](#)

Тип зарегистрированного аутентификатора и комментарий к нему отображаются в окне **Управление аутентификаторами**. Если для учетной записи пользователя разрешено добавление нескольких аутентификаторов, то вы можете перейти к их регистрации, нажав на ссылку **Добавить способ входа**. Также вы можете изменить, проверить или удалить зарегистрированный аутентификатор (если данные действия разрешены администратором системы).

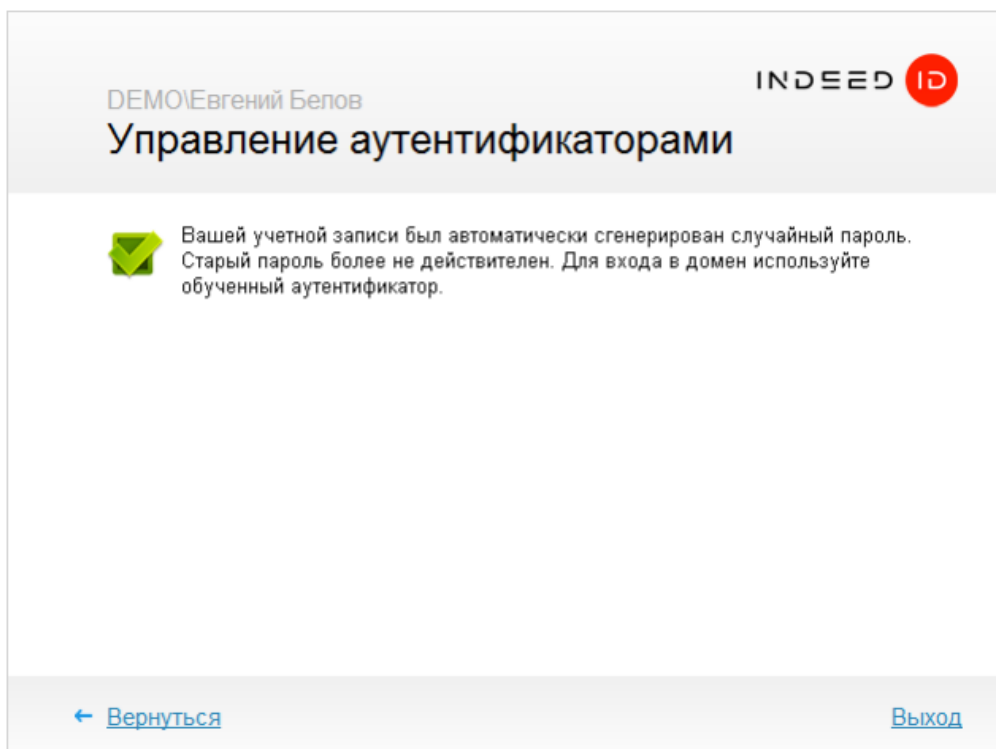


Информация

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.

При следующем входе в систему будет доступен способ входа по зарегистрированному аутентификатору.

Если для вашей учетной записи разрешена генерация случайного пароля, то после регистрации первого аутентификатора в окне **Управление аутентификаторами** отображается сообщение:



Информация

Случайный пароль для учетной записи будет сгенерирован по истечении срока действия текущего пароля. Если для вашей учетной записи был сгенерирован случайный пароль, то следующий вход в систему возможен только с использованием аутентификатора.

Если для учетной записи разрешено кэширование аутентификаторов, то при последующем входе в систему по аутентификатору будет выполнено сохранение аутентификатора в локальную память компьютера. В дальнейшем вы сможете выполнять доступ в систему по кэшированному аутентификатору при отсутствии подключения к серверам Indeed.

Вход в систему с использованием аутентификатора

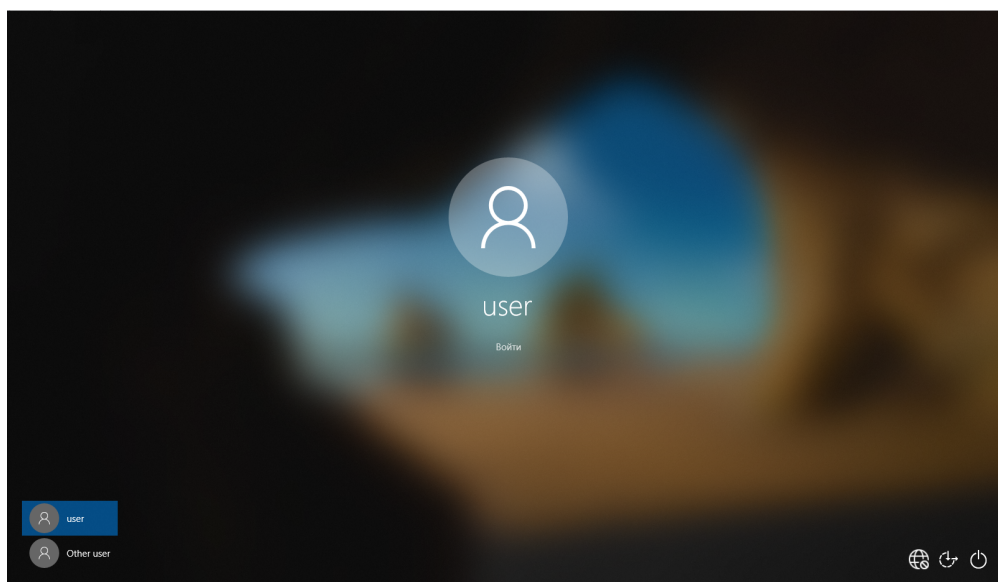
Информация

Этот способ входа доступен только при выполненных условиях:

- Вы являетесь лицензированным пользователем Indeed AM;
- Для вашей учетной записи разрешена регистрация аутентификаторов;
- Вы уже зарегистрировали хотя бы один аутентификатор.

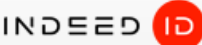
Для входа в систему по паролю выполните следующие действия:

- После загрузки операционной системы перейдите на экран выбора пользователя.
- Выберите вашу учетную запись. Если необходимо изменить имя учетной записи, нажмите **Другой пользователь**



В открывшемся окне Вход в Windows отображается имя пользователя, выполнявшего вход в систему последним и используемый им способ входа.

Вход в Windows



user (IID\user)

Введите свой пароль Windows

Вход

→ [Сменить способ входа](#)

Отмена

Если вы хотите сменить учетную запись, 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 ранее аутентификатору.

Вход в Windows



user (IID\user)

- [Пароль](#)
- [Смарт-карта или USB-ключ](#)
- [Пароль Windows](#)

[Отмена](#)

Чтобы выполнить вход в систему, необходимо предоставить зарегистрированный аутентификатор. Внешний вид окна аутентификации и текст подсказок зависят от выбранного типа аутентификатора. Выполните требуемые действия.

Информация

Если администратором системы установлено требование на смену доменного пароля и разрешена генерация случайного пароля, то при следующей аутентификации с помощью технологии Indeed будет сгенерирован случайный пароль. При этом отображается сообщение об успешной автоматической смене пароля.

Свойства: user

Член групп Входящие звонки Среда Сеансы Удаленное управление
Профиль служб удаленных рабочих столов COM+

Общие Адрес Учетная запись Профиль Телефоны Организация

Имя входа пользователя:
user @iid.local

Имя входа пользователя (пред-Windows 2000):
IID\ user

Время входа... Вход на...

☐ Разблокировать учетную запись

Параметры учетной записи:

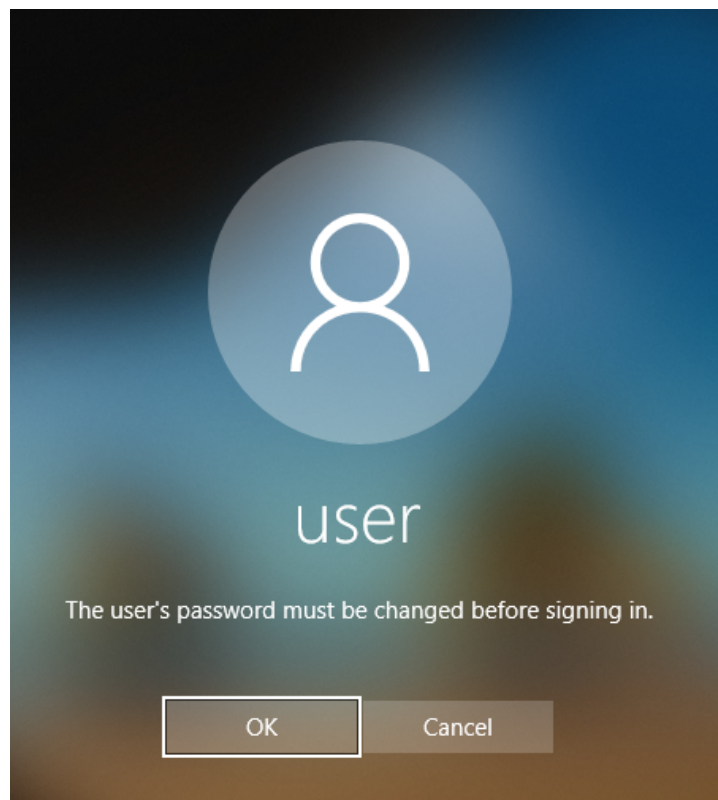
- ☒ Требовать смены пароля при следующем входе в систему
- ☐ Запретить смену пароля пользователем
- ☐ Срок действия пароля не ограничен
- ☐ Хранить пароль, используя обратимое шифрование

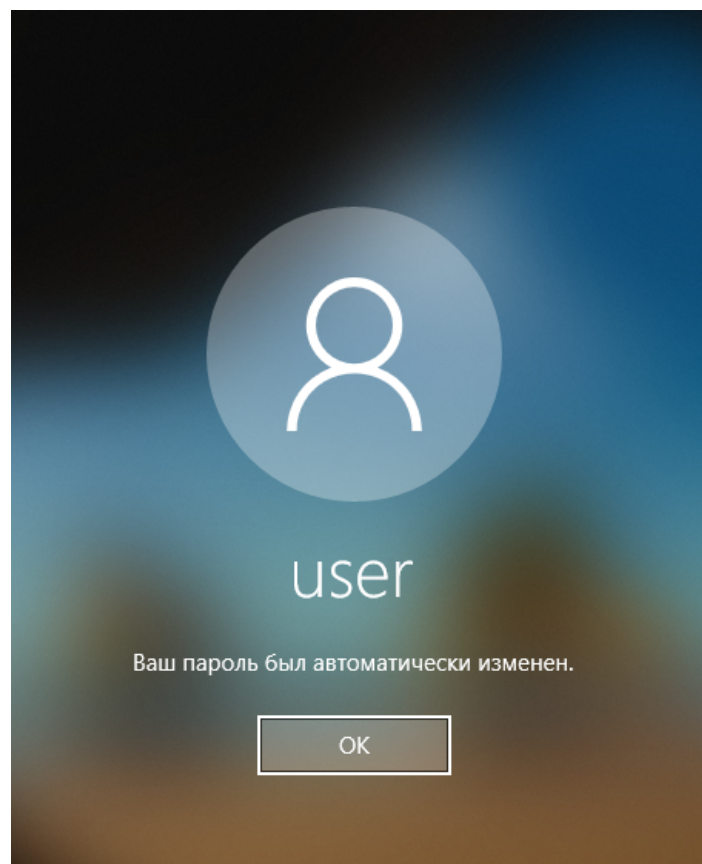
Срок действия учетной записи

☒ Никогда

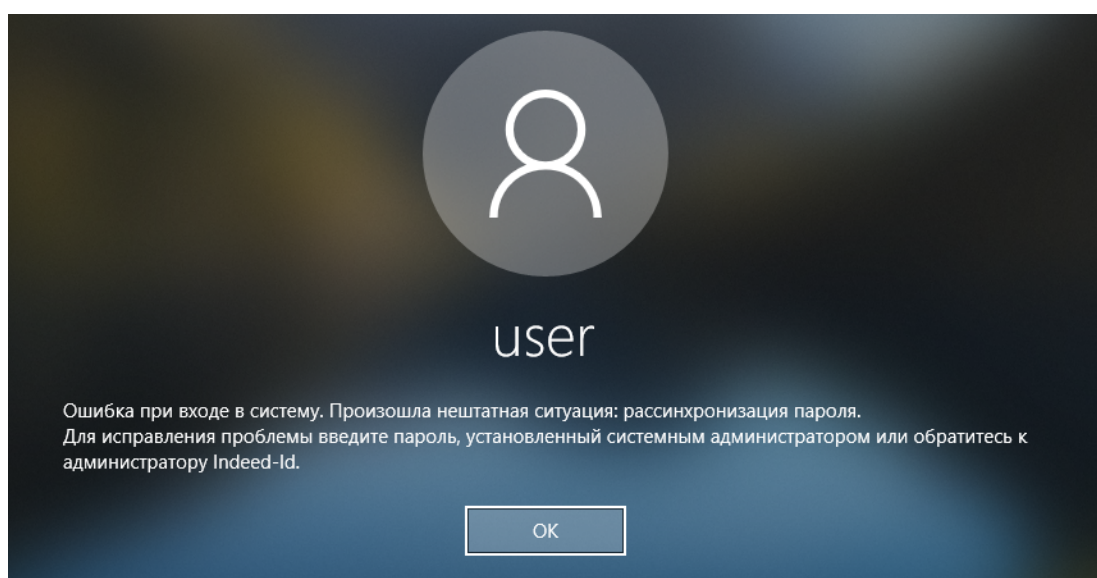
☐ Истекает: 30 сентября 2020 г.

OK Отмена Применить Справка

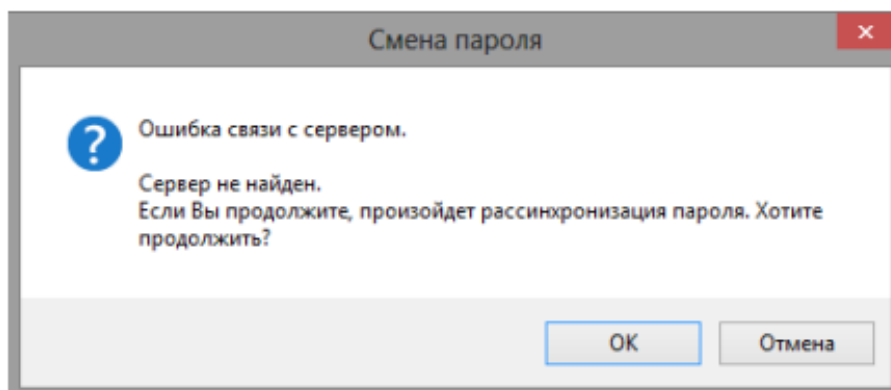




Если доменный пароль был сброшен администратором системы при хотя бы одном зарегистрированном аутентификаторе, то при входе в систему по этому аутентификатору отобразится предупреждение о рассинхронизации пароля. Пользователю потребуется ввести и подтвердить новый доменный пароль.



Если запрос на изменение пароля произойдет в момент, когда ни один из серверов Indeed не будет доступен (но при этом будет доступен хотя бы один контроллер домена), то после ввода нового пароля пользователем также появится сообщение о рассинхронизации пароля, т.к. новый пароль, установленный пользователем, невозможно будет синхронизировать с хранилищем данных Indeed



В этом случае новый доменный пароль необходимо будет синхронизировать с хранилищем данных Indeed при следующем входе в систему с использованием аутентификатора при хотя бы одном доступном сервере Indeed. После успешной синхронизации пароля будет выполнен вход в систему.

Доступ к удаленному рабочему столу с использованием аутентификатора

Для доступа к удаленному рабочему столу по аутентификатору требуются:

- Стандартная утилита Windows `mstsc.exe` (Подключение к удаленному рабочему столу/Remote Desktop) на терминальном клиенте.
- Модуль **Indeed AM Windows® Logon**, установленный на терминальном сервере.
- Модуль **Indeed AM Provider**, соответствующий используемой технологии аутентификации, установленный на терминальном клиенте и терминальном сервере.
- Аппаратное устройство аутентификации, подключенное к терминальному клиенту (не требуется при использовании провайдеров Indeed OTM Provider, Indeed Google Authenticator Provider, Indeed Passcode Provider).

Для доступа к удаленному рабочему столу по аутентификатору выполните следующие действия:

1. Запустите **Подключение к удаленному рабочему столу**.
2. Введите имя/адрес терминального сервера и установите подключение.
3. В отобразившемся окне **Вход в Windows** выберите вашу учетную запись, способ входа (тип аутентификатора) и пройдите аутентификацию.

Информация

Если для вашей учетной записи не сгенерирован случайный пароль, вы можете получить доступ к удаленному рабочему столу по паролю.

Вход в систему при отсутствии сети

Вход в систему по аутентификатору может быть выполнен даже при отсутствии физического подключения к сети. Действия при входе в систему в отсутствие сети по кэшированному аутентификатору аналогичны действиям при входе в систему по аутентификатору при доступной сети.

Данный способ входа доступен, если:

- Для вашей учетной записи было установлено разрешение на кэширование аутентификаторов.
- Было выполнено кэширование аутентификаторов (при первом входе в систему по аутентификатору).
- Был выполнен вход в систему по кэшированному аутентификатору при доступной сети.

Информация

Срок действия кэшированных аутентификаторов может быть ограничен администратором системы. По умолчанию этот срок составляет 10 дней, отсчитывается с даты последнего входа в и не зависит от того, будет ли выполнен вход в систему в дальнейшем в течение этого срока. Например, при установленном сроке 10 дней и выполнении входа в систему в 10 ч 00 мин 12.04.2010 кэшированные аутентификаторы будут действительны с 10 ч 00 мин 12.04.2010 до 10 ч 00 мин 22.04.2010. Если для вашей учетной записи разрешено кэширование аутентификаторов, то уточните у администратора наличие возможных ограничений. Если срок действия кэшированных аутентификаторов истек и серверы Indeed недоступны, при попытке входа в систему отображается сообщение об ошибке: "Ошибка при входе в систему. Сервер не найден. Кэширование данных пользователя запрещено".

Indeed AM Paste

В случаях, когда ввод пароля требуется для доступа в приложения, программный комплекс Indeed AM делает его использование максимально безопасным. С помощью **Indeed AM Paste** вы можете автоматически подставлять скрытый пароль в поле ввода при нажатии определенной комбинации «горячих клавиш» (по умолчанию [Ctrl] [Alt] [V]). **Включить** и **отключить** функцию **Indeed AM Paste** вы можете из приложения Indeed AM Paste Tray. Щелкните на значке в области уведомлений Windows и выберите нужный пункт контекстного меню:



- Разрешить **Indeed AM Paste** (включение функции, выбрано по умолчанию)
- **Запускать при загрузке** (запуск Indeed AM Paste Tray при загрузке Windows, выбран по умолчанию)
- **Выход** (выход из приложения)

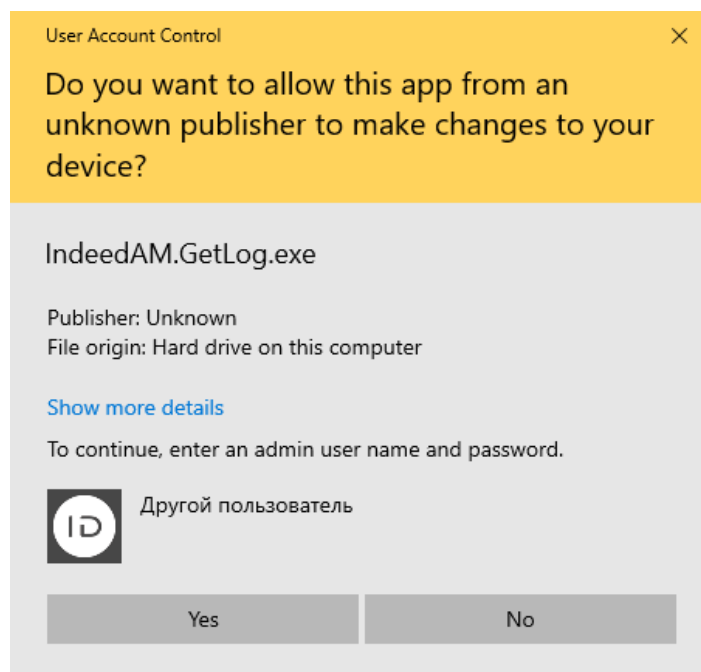
Чтобы воспользоваться функцией **Indeed AM Paste**, выполните следующие действия:

1. В окне приложения установите фокус мыши в поле ввода пароля.
2. Нажмите комбинацию «горячих клавиш».
3. Отображается окно **Аутентификация**. Подтвердите свою личность любым доступным способом (**Аутентификатор/Пароль**).

После успешной аутентификации в поле ввода отображается скрытый пароль.

Запуск от имени администратора

Для Microsoft Windows 7 и выше реализован запрос на аутентификацию по технологии Indeed AM для стандартной команды **Run as administrator**. После запуска данной 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.



Настройка одновременной работы с Indeed AM RDP Windows Logon

При условии, что используется сценарий с установкой на одной машине **Windows Logon** и **RDP Windows Logon**, необходимо настроить политику для **Windows Logon**. Для этого:

Через GPO

1. Перейдите на машину, на которой установлены компоненты **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 компоненты **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 DWORD "**CredProvFilter**" и установите ему значение **2**.

Часто задаваемые вопросы

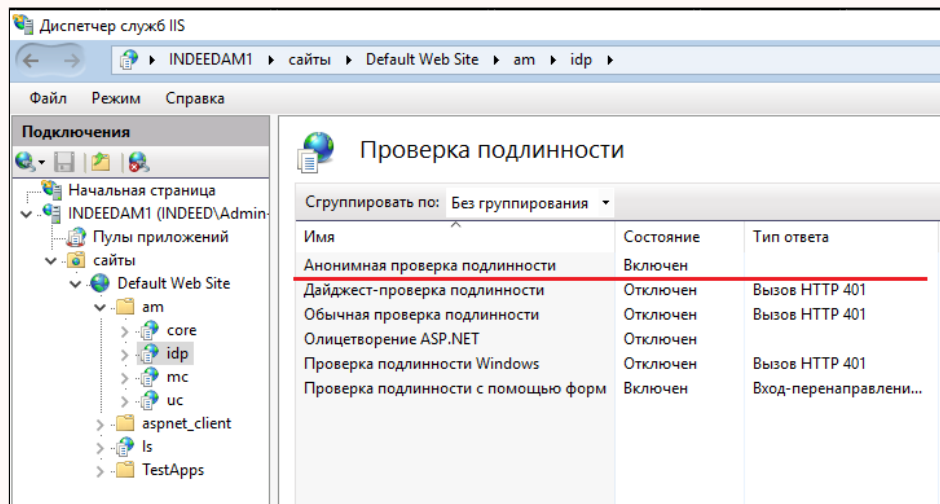
Ознакомиться со списком часто задаваемых вопросов и ответов на них можно в **Базе знаний** по продуктам компании Indeed.

Indeed AM SAML IDP

На этой странице вы найдете информацию об установке и настройке модуля Indeed AM SAML IDP, который входит в состав дистрибутива Indeed AM Access Manager 8.1.4 и ниже.

❗ Информация

По умолчанию Indeed AM SAML IDP настроен на использование Windows аутентификации, для внедоменных сценариев требуется включить анонимную аутентификацию в IIS для idp.



i Информация

Файлы для Indeed AM SAML IDP расположены: ***indeed AM <номер версии>\Indeed AM IDP \<номер версии>***

- **IndeedAM.IDP-<номер версии>.x64.ru-ru.msi** - Пакет для установки indeed SAML IDP с общим именем "idp".
- **Misc\IISScripts\Indeed.SAML.IIS.Install.MSServer.ps1** - Скрипт для установки необходимых компонентов IIS сервера для Windows Server 2012.

Информация

Путь к Identity Provider в браузере: ***http(s)://<днс_сервера>/am/idp***

Путь к Identity Provider в IIS: ***<имя_машины>\сайты\Default Web Site\am\idp***

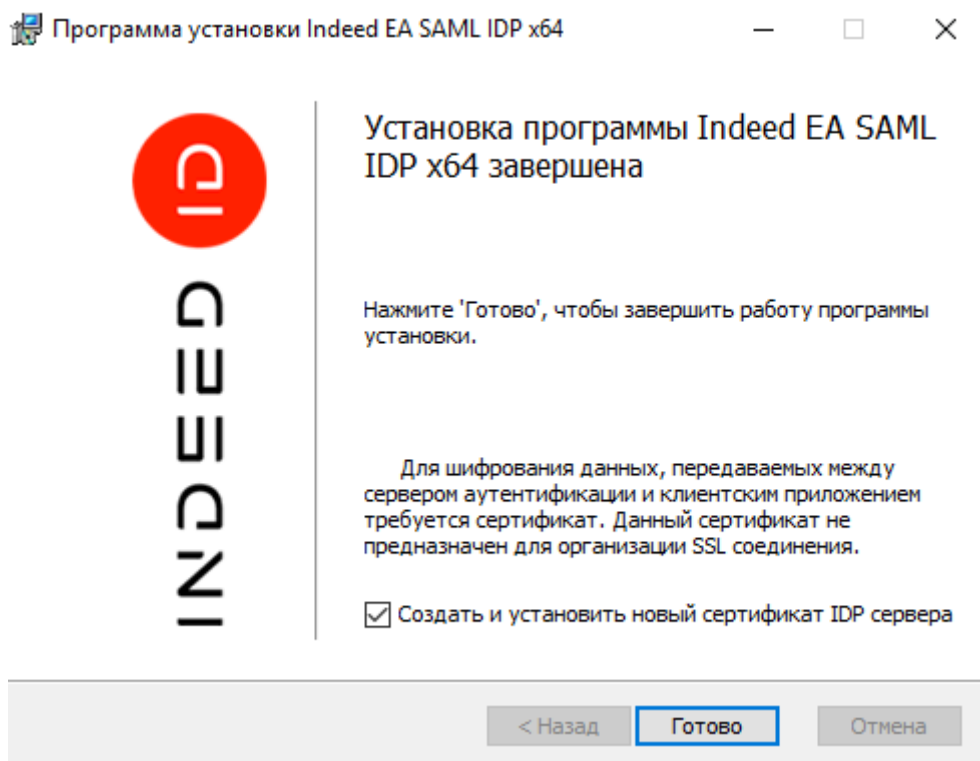
Установка

1. Выполните установку Indeed AM SAML IDP через запуск соответствующего пакета из дистрибутива.
2. По завершению требуется сгенерировать новый IDP сертификат. В хранилище сертификатов (*Local Machine -> Personal*) будет сгенерирован и установлен в новый самоподписанный сертификат. Сертификат используется для шифрования данных, передаваемых между сервером аутентификации и клиентским приложением.

Информация

Данный сертификат не предназначен для организации SSL-соединения.

Если данный сертификат был сгенерирован ранее, то необходимо убрать флажок.



3. Добавить привязку **https** в настройках **Default Web Site** в IIS Manager.



Информация

Indeed AM Identity Provider является Web приложением, которое работает на базе IIS, в процессе установки для него по умолчанию включается обязательно требование SSL в настройках, что в свою очередь требует включенной привязки https.

Если вы не намерены использовать протокол https, необходимо отключить требование SSL в настройках IIS для SAML IDP.

Также в этом случае необходимо в конфигурационном файле **UC (C:\inetpub\wwwroot\am\idp\Web.config)** изменить значение параметра **requireSSL** на **false**:

Пример

```
<httpCookies httpOnlyCookies="true" requireSSL="false" />
```

- a. Запустите **IIS Manager** и раскройте пункт **Сайты (Sites)**.
- b. Выберите сайт **Default Web Site** и нажмите **Привязки (Bindings)** в разделе **Действия (Actions)**.
- c. Нажмите **Добавить (Add)**:
 - i. **Тип (Type)** - https.
 - ii. **Порт (Port)** - 443.
 - iii. Выберите **SSL-сертификат (SSL Certificate)**.
- d. Сохраните привязку.

Редактирование конфигурационного файла

1. Откройте конфигурационный файл Identity Provider **Web.config (C:\inetpub\wwwroot\am\idp\Web.config)**.

2. Укажите **URL** для подключения к серверу **Indeed** для параметра **Url** в тэге **amAuthServer**.

 Информация

При использовании https соединения требуется выполнить установку клиентского сертификата на каждый сервер Indeed AM.

- а. Параметр **Url** - url адрес сервера Indeed в формате **http(s)://полное_dns_имя_сервера/am/core/**

 Информация

Для игнорирования ошибок сертификата сервера необходимо изменить параметр **"isIgnoreCertErrors"** на значение **"true"** в файле **"applicationSettings.config"** (**am\idp\Config**).

Пример

```
<amAuthServer Url="https://amserv.indeed-id.local/am/core/" />
```

3. Укажите **URL** для подключения к **Indeed AM Log Server** в формате **http(s)://полное_dns_имя_сервера/ls/api** для параметра **Url** в тэге **logServer**.

Пример

```
<logServer Url="https://logserver.indeed-id.local/ls/api/" CertificateThumbprint="" CertificateFilePath="" CertificateFilePassword="" />
```

4. Укажите отпечаток сертификата IDP, который был сгенерирован при установке, в тэге **"CertificateThumbprint"** параметра **"amIdentityProviderSettings"**.

 Информация

Сертификат устанавливается в хранилище сертификатов (*Local Machine -> Personal*) с общим именем **"idp"**.

Получить отпечаток можно с помощью Power Shell запроса:

```
Get-Childitem Cert:\LocalMachine\My\ | Where-Object {$_.Subject -eq "CN=idp"}
```

5. В тэге **amAuthMethods** укажите ID провайдера в формате:

а. Если для входа используется 1 провайдер.

Пример

```
<amAuthMethod id="SMSOTP"> <amAuthProviders> <amAuthProvider id="ebb6f3fa-a400-45f4-853a-d517d89ac2a3" /> </amAuthProviders> </amAuthMethod>
```

б. Если для входа используется "цепочка" из провайдеров.



Информация

Если используется цепочка с Windows Password + провайдер:

- Windows Password был введен верно, произвольный провайдер неверно - в "История входов" пользователя будет отображаться успешный вход в Indeed AM SAML IDP с помощью Windows Password.
- Windows Password был введен верно, произвольный провайдер верно - в "История входов" пользователя будет отображаться успешный вход с помощью провайдера пользователя.

Пример

```
<amAuthMethod id="HOTP_Passcode_SMS">  
<amAuthProviders>  
<amAuthProvider id="AD3FBA95-AE99-4773-93A3-6530A29C7556" />  
<amAuthProvider id="F696F05D-5466-42b4-BF52-21BEE1CB9529" />  
<amAuthProvider id="ebb6f3fa-a400-45f4-853a-d517d89ac2a3" />  
</amAuthProviders>  
</amAuthMethod>
```

- Параметр **id** тега **amAuthMethod** - Произвольное уникальное значение.
- Параметр **id** тега **amAuthProvider** - id используемого провайдера.

 Параметр **id** тега **amAuthProvider** может иметь разные ID провайдеров:

{EBB6F3FA-A400-45F4-853A-D517D89AC2A3} - **SMS OTP**

{093F612B-727E-44E7-9C95-095F07CBB94B} - **EMAIL OTP**

{F696F05D-5466-42b4-BF52-21BEE1CB9529} - **Passcode**

{0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0} - **Software OTP**

{AD3FBA95-AE99-4773-93A3-6530A29C7556} - **HOTP Provider**

{CEB3FEAF-86ED-4A5A-BD3F-6A7B6E60CA05} - **TOTP Provider**

{DEEF0CB8-AD2F-4B89-964A-B6C7ECA80C68} - **AirKeyProvider**

{CF189AF5-01C5-469D-A859-A8F2F41ED153} - **Windows Password**

{CA4645CC-5896-485E-A6CA-011FCC20DF1D} - **Telegram OTP**

Аутентификации по имени пользователя без указания домена

В Indeed AM SAML IDP существует возможность выбирать домен из выпадающего списка.

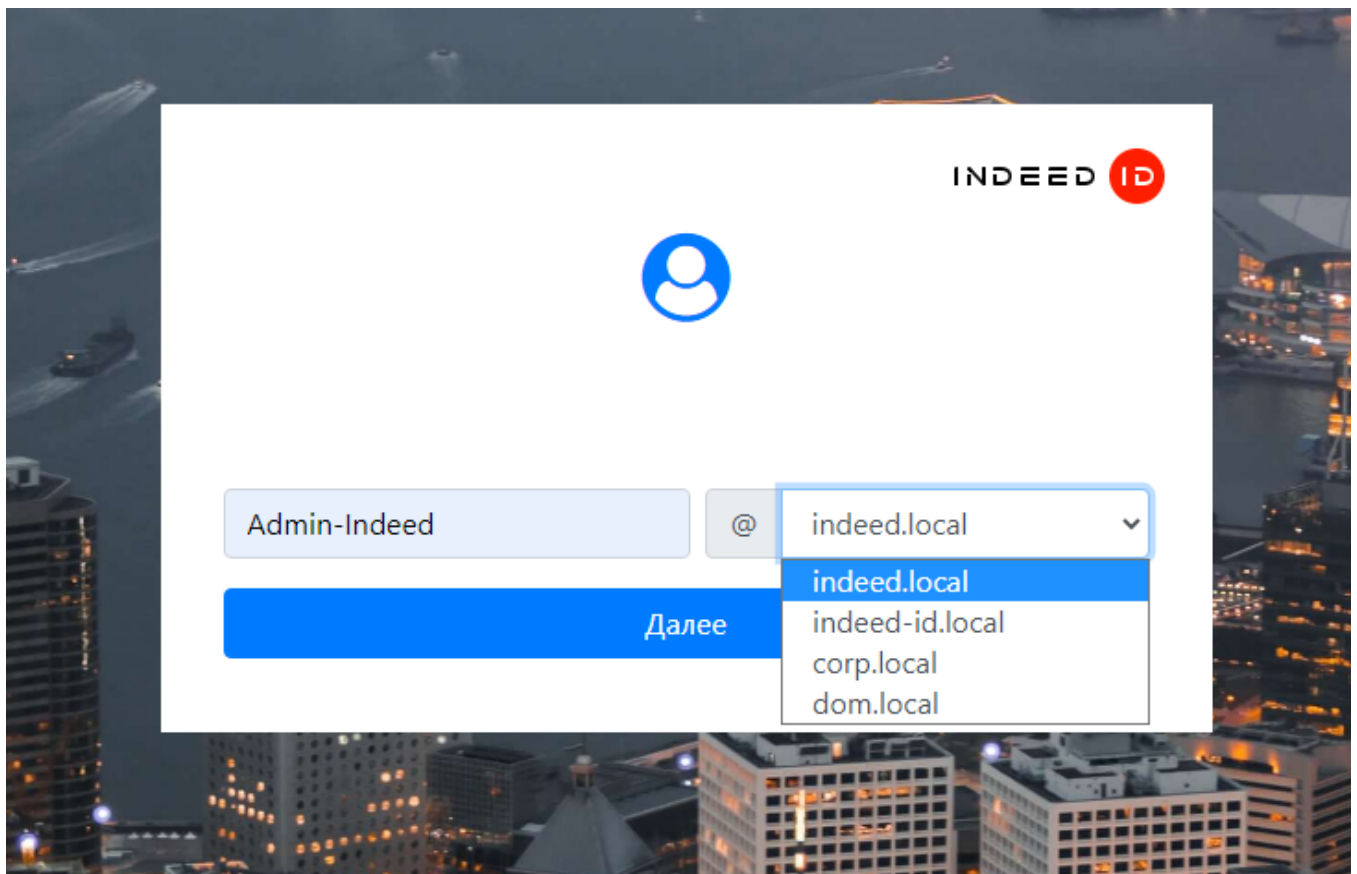
Для включения настройки необходимо выполнить следующее:

1. Откройте конфигурационный файл SAML IDP **Web.config** (C:\inetpub\wwwroot\am\idp\Web.config).
2. В теге "**amAuthDomains**", добавьте теги "**amAuthDomain**" и для параметра "**name**", задайте значения необходимых доменов.

Пример

```
<amAuthSet>
  <amAuthDomains>
    <amAuthDomain name="indeed.local"/>
    <amAuthDomain name="indeed-id.local"/>
    <amAuthDomain name="corp.local"/>
    <amAuthDomain name="dom.local"/>
  </amAuthDomains>
  ...
</amAuthSet>
```

3. По умолчанию выбирается домен, указанный первым в списке.



Включение защиты от перебора

Сервер Indeed AM поддерживает включение защиты от подбора УЗ пользователей для компонента Indeed AM SAML IDP. По умолчанию данная настройка отключена.

При включенной настройке злоумышленник не сможет определить валидные УЗ в домене по возвращаемой от компонента ошибке.

Для включения настройки необходимо выполнить следующее:

1. Откройте конфигурационный файл сервера Indeed AM: C:\inetpub\wwwroot\am\core\Web.config
2. В теге "appSettings", для параметра "**bruteForceProtectionApps**", задайте значение "**SAML Identity Provider**".

Пример

```
<appSettings>
  <add key="bruteForceProtectionApps" value="SAML Identity Provider" />
  ...
</appSettings>
```

3. Сохраните изменения и перезапустите IIS сервер.

Интеграция с приложениями

1. Identity Provider Login URL - http(s)://<полное_DNS_имя_сервера_Indeed_SAML>/am/idp/Account/SsoService
2. Identity Provider Logout URL - http(s)://<полное_DNS_имя_сервера_Indeed_SAML>/am/idp/Account/Logout
3. Identity Provider Name - urn:indeedid:saml_idp

Описание параметров конфигурационного файла saml.config:

- **CertificateThumbprint** - Указывается отпечаток сертификата SP, загруженный в личное хранилище компьютера, где развернут Indeed AM Identity Provider.
 - **CertificateFile** - Вместо отпечатка можно использовать путь к файлу сертификата.
- **WantAuthnRequestSigned** - Параметр указывает должен ли запрос аутентификации SAML быть подписанным. Значение по умолчанию: **false**.
- **SignSAMLResponse** - Параметр указывает должны ли быть подписаны ответы SAML, отправляемые SP. Значение по умолчанию: **false**.
- **SignAssertion** - Параметр указывает должны ли утверждения SAML быть подписаны. Значение по умолчанию: **false**.
- **EncryptAssertion** - Параметр указывает должны ли утверждения SAML шифроваться. Значение по умолчанию: **false**.

Пример работы расширения

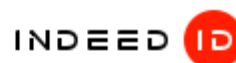
1. Для аутентификации в SAML откройте URL **http(s)://полное_dns_имя_сервера/am/idp/**

2. В появившемся окне аутентификации SAML нажмите **"Back"** для выбора способа аутентификации, по умолчанию используется последний используемый способ.

 Информация

Если доступна **"Проверка подлинности Windows"** и выключена **"Анонимная проверка подлинности"** в методах аутентификации IIS, то логин пользователя подставляется автоматически без возможности изменить, и пробрасывается доменный пароль пользователя.

Если используется **"Анонимная проверка подлинности"** и выключена **"Проверка подлинности Windows"**, то пользователь может изменить логин и потребуется ввод доменного пароля.



DEMO\Admin-Indeed

Enter the windows password

Enter the windows password

Back

Next

3. Выберите способ аутентификации и нажмите **"Select"**.



Информация

Если у пользователя нет обученного аутентификатора, то выберите **"Windows Password"**.



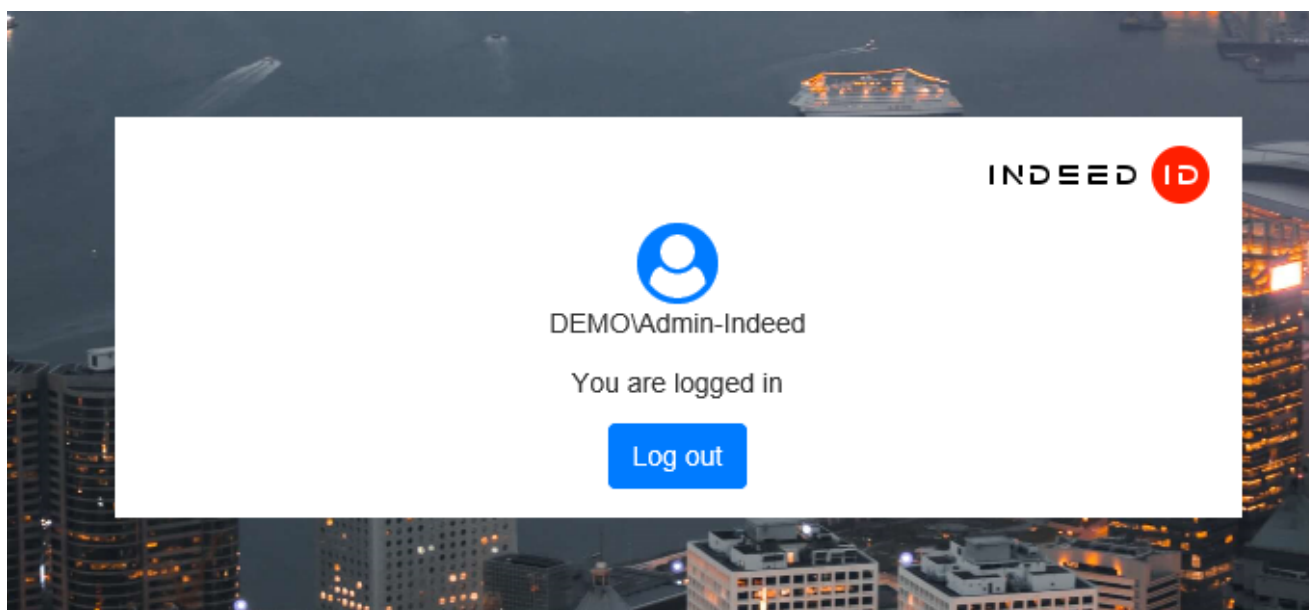
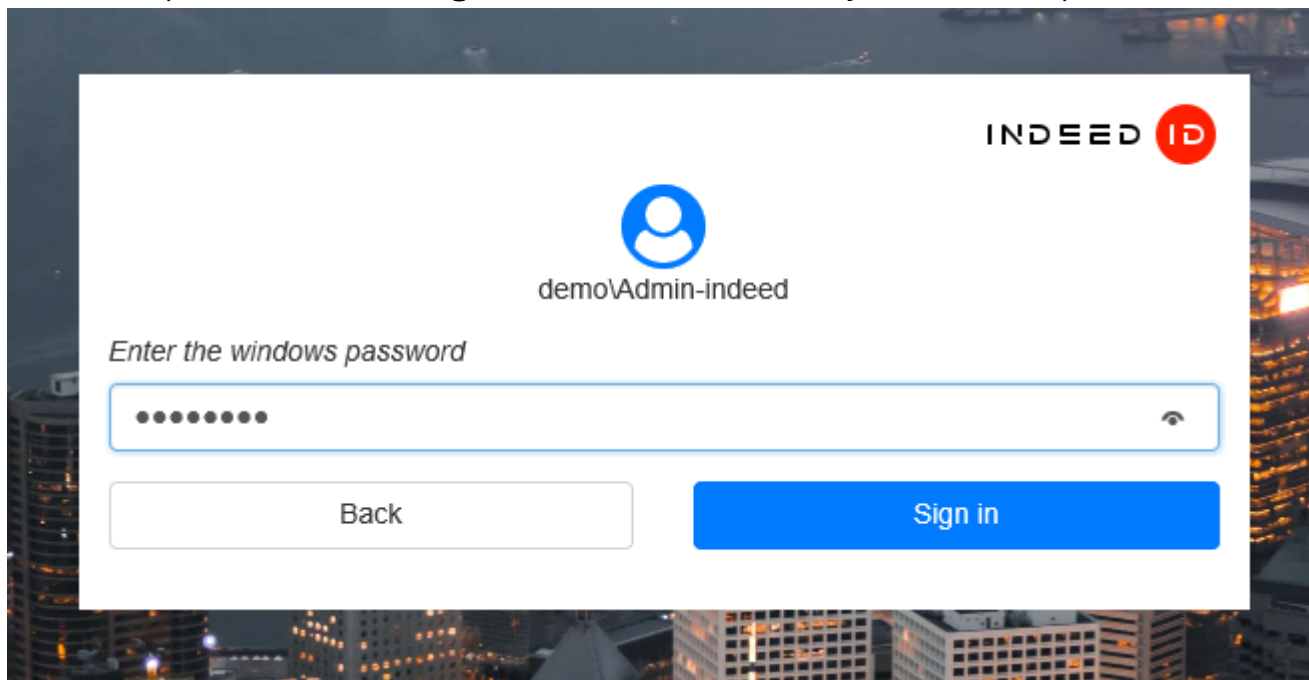
DEMO\Admin-Indeed

Choose an authentication method you want to use

- ☐ Passcode
- ☒ Windows Password + Passcode
- ☐ Hardware OTP + Passcode
- ☐ Hardware TOTP

Select

Введите пароль и нажмите **"Sing in"**. Если ввод данных был успешный, то произойдет вход.



Отключение отображения информации о платформе и версии

Для того, чтобы не добавлять заголовки, содержащие информацию о платформе и версии, на которой разрабатывалось приложение, в response, нужно:

- a. Открыть конфигурационный файл SAML IDP `C:\inetpub\wwwroot\am\idp\Web.config`;
- b. В зависимости от версии IIS:
 - i. Для IIS 10 убрать комментарии со следующих строк:

Пример

```
<security>
  <requestFiltering removeServerHeader="true" />
</security>
```

- ii. IIS старше 10:

- Установить [URL Rewrite](#)
- В секцию `<system.webServer>` добавить:

Пример

```
<rewrite>
  <outboundRules>
    <rule name="replace server header" patternSyntax="Wildcard"
lockItem="false">
      <match serverVariable="RESPONSE_SERVER" pattern="*" />
      <action type="Rewrite" value="MyServer" />
    </rule>
  </outboundRules>
</rewrite>
```

Примеры внедрения расширения

1. [Настройка Keycloak для аутентификации через Indeed AM SAML IDP.](#)

Сбор логов

- [Сбор логов серверных компонентов](#)
- [Indeed AM GetLog](#)

Indeed AM GetLog

Приложение **Indeed AM GetLog** предназначено для локального и удаленного сбора программных логов продуктов компании Indeed.

Информация

Indeed AM GetLog расположен в дистрибутиве по пути: *indeed AM\logging\IndeedAM.GetLog.exe*

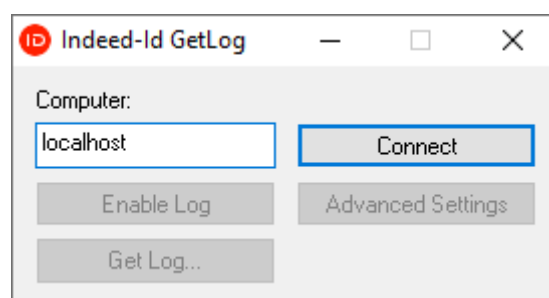
Подключение к компьютеру

Для подключения к компьютеру выполните следующие действия:

1. Запустите утилиту **GetLog** от имени локального администратора.
2. В поле **Computer** введите имя или **ip-адрес** удаленного компьютера. Для подключения к локальному компьютеру введите **localhost** или **ip-адрес 127.0.0.1**.
3. Нажмите **Connect** для соединения с указанным компьютером. После установки соединения станет доступна кнопка **включения/отключения логов (Enable Log/Disable Log)**, кнопка получения логов (**Get Log**), кнопка перехода к дополнительным настройкам (**Advanced Settings**) и кнопка отключения (**Disconnect**).

Информация

Для установки подключения 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 (WMI)).



Включение, отключение и сбор логов

Информация

Запись лог-файлов по умолчанию осуществляется в каталог `\WINDOWS\System32\LogFiles\Indeed-Id`. Для доступа к лог-файлам удаленного компьютера по умолчанию используется сетевой каталог `ADMIN$\System32\LogFiles\Indeed-Id`. Каталог для записи логов задается опцией **Use alternative location** в разделе **Advanced Settings**.

Для включения и отключения логов выполните следующие действия:

1. Выполните подключение к компьютеру.
2. Для включения логов нажмите **"Enable Log"**.
3. Если сбор логов требуется для выявления причин проблемной ситуации, выполните необходимые действия для воспроизведения проблемы.
4. Для отключения 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.

Дополнительные настройки

Для перехода 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 содержимое каталога будет автоматически удалено, за исключением файлов логов, время изменения которых не превышает значение 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 указанного в **Max.log file age**.
- **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 (например, Indeed AM Enterprise Single Sign-On) 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 лог-файла 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 лог-файлов. Значение по умолчанию – 5, без учета текущего записываемого файла. Если установленное количество файлов превышено, самый ранний удалится, а запись логов продолжится во вновь созданный файл.
- **Use alternative location** – альтернативный каталог записи логов. Если опция выключена, логи записываются в каталоги по умолчанию:
 - **Локальный путь:** \WINDOWS\System32\LogFiles\Indeed-Id
 - **Сетевой путь:** ADMIN\$\System32\LogFiles\Indeed-Id

 Advanced Settings ✕

Max. log size (bytes):

Max. log file age (s):

Cleaner interval (s):

Activity checking period (ms):

☒ Enable log cycling

Max. size of a log file (bytes):

Max. number of saved log files:

☐ Use alternative location

Сбор логов серверных компонентов

Сбор логов сервера Indeed AM

Включение логирования

1. Откройте с правами администратора файл: **C:\inetpub\wwwroot\am\core\Config\nlog.config**
2. Для тегов **"logger"**, в параметре **"minlevel"**, установите значение **"Trace"**, в параметре **"enabled"** установите **"true"**.

Пример

```
<rules>
  <logger name="*" writeTo="f1" minlevel="Trace" enabled="true" >
    <filters>
      <when condition="equals('${logger}','metricTime')" action="Ignore" />
      <when condition="equals('${logger}','metricInfo')" action="Ignore" />
    </filters>
  </logger>
  <logger name="metricTime" writeTo="metricTimeTarget" minlevel="Trace" enabled="true" />
  <logger name="metricInfo" writeTo="metricInfoTarget" minlevel="Trace" enabled="true" />
</rules>
```

3. Сохраните файл и выполните перезапуск сервера IIS.

Сбор логов

1. Очистите существующие логи сервера Indeed AM в папке: **C:\inetpub\wwwroot\am\core\Logs**
2. Воспроизведите проблему.
3. Соберите архив с логами и пришлите с подробным описанием действий пользователя и указанием точного времени воспроизведения проблемы нам.

Сбор логов Indeed AM Management Console

Включение логирования

1. Откройте с правами администратора файл: **C:\inetpub\wwwroot\am\mc\Config\nlog.config**
2. Для тега **"logger"**, в параметре **"minlevel"**, установите значение **"Trace"**, в параметре **"enabled"** установите **"true"**.

Пример

```
<rules>
  <logger name="*" writeTo="f1" minlevel="Trace" enabled="true" />
</rules>
```

3. Сохраните файл и выполните перезапуск сервера IIS.

Сбор логов

1. Очистите существующие логи Indeed AM Management Console в папке: **C:\inetpub\wwwroot\am\mc\Logs**
2. Воспроизведите проблему.
3. Соберите архив с логами и пришлите с подробным описанием действий пользователя и указанием точного времени воспроизведения проблемы нам.

Сбор логов Indeed AM Log Server

Включение логирования

1. Откройте с правами администратора файл: **C:\inetpub\wwwroot\ls\nlog.config**
2. Для тега **"logger"**, в параметре **"minlevel"**, установите значение **"Trace"**. Создайте параметр **"enabled"** и установите значение **"true"**.

Пример

```
<rules>
  <logger name="*" minlevel="Trace" writeTo="fileLogErrors" enabled="true" />
</rules>
```

3. Сохраните файл и выполните перезапуск сервера IIS.

Сбор логов

1. Очистите существующие логи Indeed AM Log Server в папке: **C:\inetpub\wwwroot\ls\Logs**
2. Воспроизведите проблему.
3. Соберите архив с логами и пришлите с подробным описанием действий пользователя и указанием точного времени воспроизведения проблемы нам.

Сбор логов Indeed AM AirKey Server

Включение логирования

1. Откройте с правами администратора файл: **C:\inetpub\wwwroot\airkeycloud\Web.Config**
2. Для тега **"logger"**, в параметре **"minlevel"**, установите значение **"Trace"**, в параметре **"enabled"** установите **"true"**.

Пример

```
<rules>
  <logger name="" minlevel="Trace" writeTo="fileLog" enabled="true" />
</rules>
```

3. Сохраните файл и выполните перезапуск сервера IIS.

Сбор логов

1. Очистите существующие логи сервера Indeed AirKey в папке: **C:\inetpub\wwwroot\airkeycloud\logs**
2. Воспроизведите проблему.
3. Соберите архив с логами и пришлите с подробным описанием действий пользователя и указанием точного времени воспроизведения проблемы нам.

Сбор логов Indeed AM User Console

Включение логирования

1. Откройте с правами администратора файл: **C:\inetpub\wwwroot\am\uc\Config\nlog.config**
2. Для тега **"logger"**, в параметре **"minlevel"**, установите значение **"Trace"**, в параметре **"enabled"** установите **"true"**.

Пример

```
<rules>
  <logger name="*" writeTo="f1" minlevel="Trace" enabled="true" />
</rules>
```

3. Сохраните файл и выполните перезапуск сервера IIS.

Сбор логов

1. Очистите существующие логи Indeed AM User Console в папке: **C:\inetpub\wwwroot\am\uc\logs**
2. Воспроизведите проблему.
3. Соберите архив с логами и пришлите с подробным описанием действий пользователя и указанием точного времени воспроизведения проблемы нам.

Сбор логов Indeed AM Identity Provider

Включение логирования

1. Откройте с правами администратора файл:
для Indeed Access Manager 8.1.5 и выше — *C:\inetpub\wwwroot\am\idp\nlog.config*
для Indeed Access Manager 8.1.4 и ниже — *C:\inetpub\wwwroot\am\idp\Config\nlog.config*
2. Для тега **"logger"**, в параметре **"minlevel"**, установите значение **"Trace"**, в параметре **"enabled"** установите **"true"**.

Пример

```
<rules>
  <logger name="*" writeTo="f1" minlevel="Trace" enabled="true" />
</rules>
```

3. Сохраните файл и выполните перезапуск сервера IIS.

Сбор логов

1. Очистите существующие логи Indeed AM Identity Provider в папке: **C:\inetpub\wwwroot\am\idp\logs**
2. Воспроизведите проблему.
3. Соберите архив с логами и пришлите с подробным описанием действий пользователя и указанием точного времени воспроизведения проблемы нам.

Сбор логов кэш сервера Indeed AM

Информация

Сбор логов кэш сервера выполняется на клиентских машинах с установленным компонентом Indeed AM Windows Logon или Indeed ESSO Agent.

Включение логирования

1. Откройте с правами администратора файл: **C:\Program Files (x86)\Common Files\Indeed-Id\AM\CacheServer\NLog.config** для x64 машин или **C:\Program Files\Common Files\Indeed-Id\AM\CacheServer\NLog.config** для x86.
2. Для тегов **"logger"** в параметре **"enabled"** установите **"true"**.

```
<rules>
  <logger name="*" minlevel="Trace" writeTo="f1" encoding="Unicode" enabled="true" >
    <filters>
      <when condition="equals('${logger}','metricTime')" action="Ignore" />
      <when condition="equals('${logger}','metricInfo')" action="Ignore" />
    </filters>
  </logger>
  <logger name="*" minlevel="Trace" writeTo="console" encoding="Unicode" enabled="true" />
  <logger name="metricTime" writeTo="metricTimeTarget" minlevel="Trace" enabled="true" />
  <logger name="metricInfo" writeTo="metricInfoTarget" minlevel="Trace" enabled="true" />
</rules>
```

3. Сохраните изменения в файле.

Сбор логов

1. Очистите существующие логи кэш сервера в папке: **C:\Windows\System32\LogFiles\Indeed-ID Cache**
2. Воспроизведите проблему.
3. Соберите архив с логами и пришлите с подробным описанием действий пользователя и указанием точного времени воспроизведения проблемы нам.

Сбор логов мастера конфигурации Indeed AM

Включение логирования

1. Откройте с правами администратора файл: **C:\Program Files\Indeed AM\Wizard\NLog.config**.
2. Для тега **"logger"**, в параметре **"minlevel"**, установите значение **"Trace"**, в параметре **"enabled"** установите **"true"**.

Пример

```
<rules>
  <logger name="*" writeTo="f1" minlevel="Trace" enabled="true" />
</rules>
```

3. Сохраните файл и перезапустите мастер конфигурации.

Сбор логов

1. Очистите существующие логи мастера конфигурации в папке: **C:\Program Files\Indeed AM\Wizard\Logs**.
2. Воспроизведите проблему.
3. Соберите архив с логами и пришлите с подробным описанием действий пользователя и указанием точного времени воспроизведения проблемы нам.

Миграция с Indeed AM 7.x на Indeed AM 8.1

- [Подготовка к миграции](#)
- [Миграция MS SQL](#)
- [Миграция хранилища Active Directory](#)

Подготовка к миграции

Перед началом процедуры миграции и/или обновления, требуется выполнить следующие действия:

1. Расшифровка файлов конфигурации

- a. Расшифровка конфигурационного файла **easerver** (C:\inetpub\wwwroot\easerver**Web.config**)
- b. Расшифровка конфигурационного файла **airkeycloud** (C:\inetpub\wwwroot\airkeycloud**Web.config**)
- c. Расшифровка конфигурационных файлов **ils** (C:\inetpub\wwwroot\ils\targetConfigs\sampleDb.config и C:\inetpub\wwwroot\ils\targetConfigs\akcSqlTarget.config)

2. Резервное копирование конфигурационных файлов

- a. **easerver** (C:\inetpub\wwwroot\easerver**Web.config**)
- b. **airkeycloud** (C:\inetpub\wwwroot\airkeycloud**Web.config**)
- c. **iidemc** (C:\inetpub\wwwroot\iidemc**Web.config**)
- d. **iidsamlidp** (C:\inetpub\wwwroot\iidsamlidp**Web.config** и C:\inetpub\wwwroot\iidsamlidp\saml.config)
- e. **iidselfservice** (C:\inetpub\wwwroot\iidselfservice**Web.config**)
- f. **ils** (C:\inetpub\wwwroot\ils\clientApps.config и каталога C:\inetpub\wwwroot\ils\targetConfigs\)

3. Резервное копирование веток реестра

- a. Настроек модулей интеграции Indeed

ветка реестра
[HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID]

- b. Политик модулей и провайдеров Indeed

ветка реестра
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID]

4. Резервное копирование баз данных

- a. Полная резервная копия базы данных хранилища **Indeed AM 7.x**
- b. Полная резервная копия базы данных **Indeed AM AirKey Cloud Server**
- c. Полная резервная копия базы данных логов **Indeed AM 7.x**
- d. Полная резервная копия базы данных логов **Indeed AM AirKey Cloud Server**

Миграция MS SQL



Важно

Обязательное условие - **ключи шифрования** хранилища и структура пользовательских каталогов (их идентификаторы) обоих экземпляров **должны совпадать**



Информация

Используется штатный набор инструментов SQL Server (SSMS).

Миграция осуществляется по шагам, интерактивно, прозрачно для DBA.

Используется инструмент экспорта данных БД - Export Wizard.

Миграция базы данных логов системы Indeed AM 7.x

Скопируйте базу данных логов системы с новым именем (например: "indeed_am_81_log"), одним из следующих способов:

- Через **Мастер копирования базы данных**:

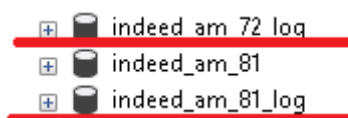
<https://docs.microsoft.com/ru-ru/sql/relational-databases/databases/use-the-copy-database-wizard?view=sql-server-ver15>

- Через **Копирование баз данных путем создания и восстановления резервных копий**:

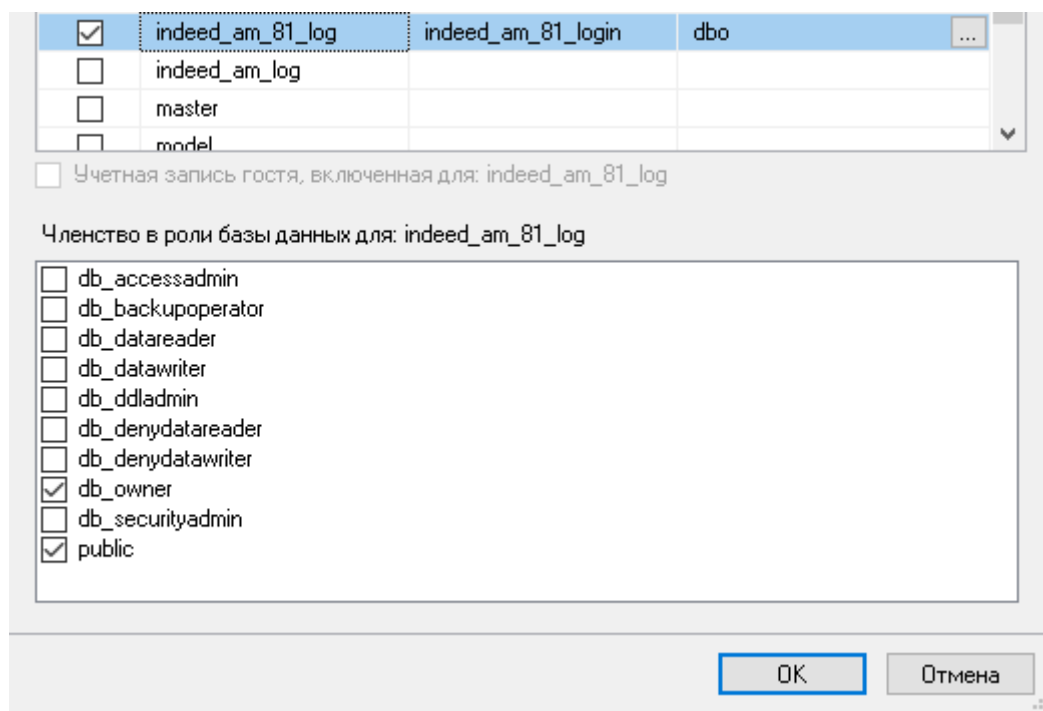
<https://docs.microsoft.com/ru-ru/sql/relational-databases/databases/copy-databases-with-backup-and-restore?view=sql-server-ver15>

- Через **Мастер импорта и экспорта данных SQL Server**:

<https://docs.microsoft.com/ru-ru/sql/integration-services/import-export-data/import-and-export-data-with-the-sql-server-import-and-export-wizard?view=sql-server-ver15>



По завершении копирования, укажите для новой БД логин MS SQL сервера, с правами владельца:



Далее, при настройке Log Server'a Indeed AM 8.1, для **событий системы**, укажите данную БД (например: "indeed_am_81_log") и учетную запись MS SQL сервера ([Установка и настройка Indeed AM Log Server с хранилищем в БД](#))

Миграция базы данных логов AM AirKey Cloud Server версии 7.x

Скопируйте базу данных логов AM AirKey Cloud Server с новым именем (например: "indeed_aks_81_log"), одним из следующих способов:

- Через **Мастер копирования базы данных**:

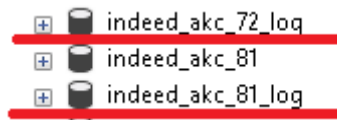
<https://docs.microsoft.com/ru-ru/sql/relational-databases/databases/use-the-copy-database-wizard?view=sql-server-ver15>

- Через **Копирование баз данных путем создания и восстановления резервных копий**:

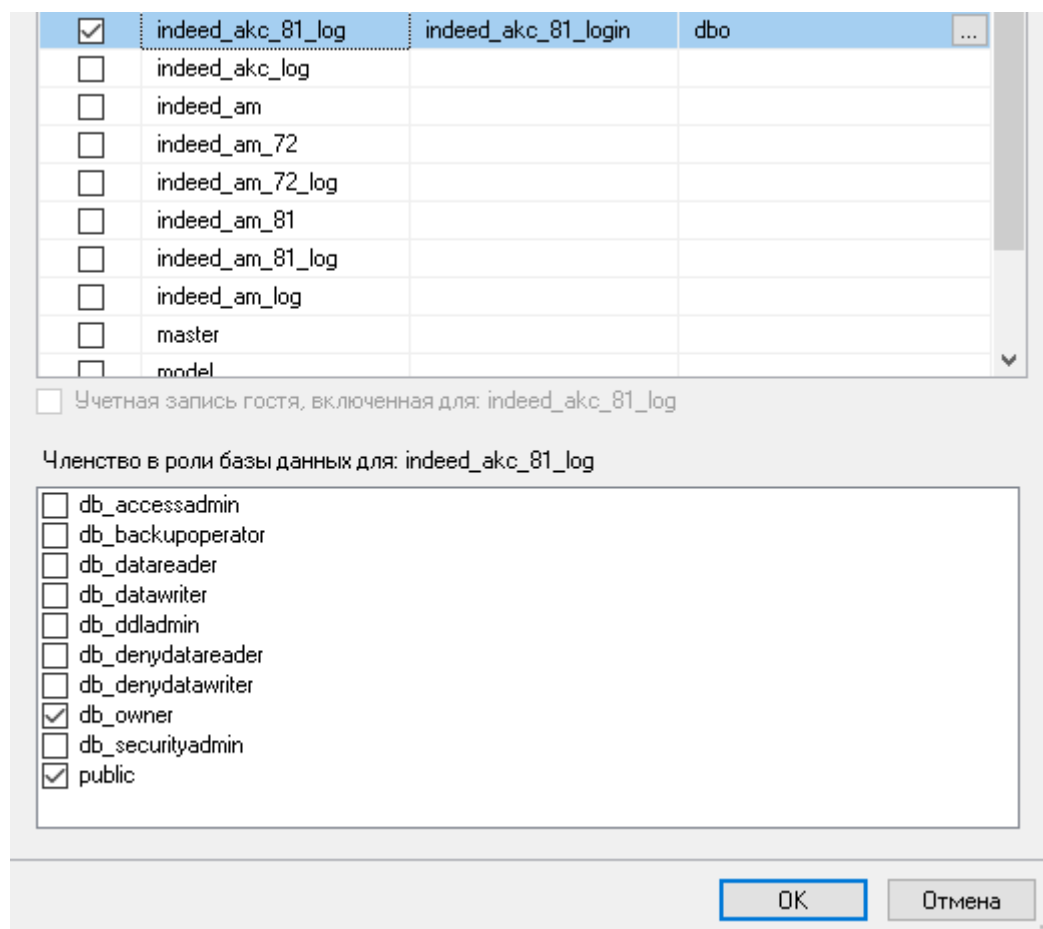
<https://docs.microsoft.com/ru-ru/sql/relational-databases/databases/copy-databases-with-backup-and-restore?view=sql-server-ver15>

- Через **Мастер импорта и экспорта данных SQL Server**:

<https://docs.microsoft.com/ru-ru/sql/integration-services/import-export-data/import-and-export-data-with-the-sql-server-import-and-export-wizard?view=sql-server-ver15>



По завершении копирования, укажите для новой БД логин MS SQL сервера, с правами владельца:



Далее, при настройке Log Server'a Indeed AM 8.1, для **AM AirKey Cloud Server**, укажите данную БД (например: "indeed_akc_81_log") и учетную запись MS SQL сервера ([Indeed Key Server](#))

Миграция базы данных хранилища AM AirKey Cloud Server версии 7.x

Скопируйте базу данных логов AM AirKey Cloud Server с новым именем (например: "indeed_akc_81"), одним из следующих способов:

- Через **Мастер копирования базы данных**:

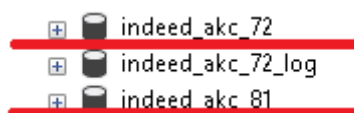
<https://docs.microsoft.com/ru-ru/sql/relational-databases/databases/use-the-copy-database-wizard?view=sql-server-ver15>

- Через **Копирование баз данных путем создания и восстановления резервных копий**:

<https://docs.microsoft.com/ru-ru/sql/relational-databases/databases/copy-databases-with-backup-and-restore?view=sql-server-ver15>

- Через **Мастер импорта и экспорта данных SQL Server**:

<https://docs.microsoft.com/ru-ru/sql/integration-services/import-export-data/import-and-export-data-with-the-sql-server-import-and-export-wizard?view=sql-server-ver15>



По завершении копирования, укажите для новой БД логин MS SQL сервера, с правами владельца:

☒	indeed_akc_81	indeed_akc_81_login	dbo	...
☒	indeed_akc_81_log	indeed_akc_81_login	dbo	...
☐	indeed_akc_log			
☐	indeed_am			
☐	indeed_am_72			
☐	indeed_am_72_log			
☐	indeed_am_81			
☐	indeed_am_81_log			
☐	indeed_am_log			
☐	master			
☐	model			

☐ Учетная запись гостя, включенная для: indeed_akc_81

Членство в роли базы данных для: indeed_akc_81

☐	db_accessadmin
☐	db_backupoperator
☐	db_datareader
☐	db_datawriter
☐	db_ddladmin
☐	db_denydatareader
☐	db_denydatawriter
☒	db_owner
☐	db_securityadmin
☒	public

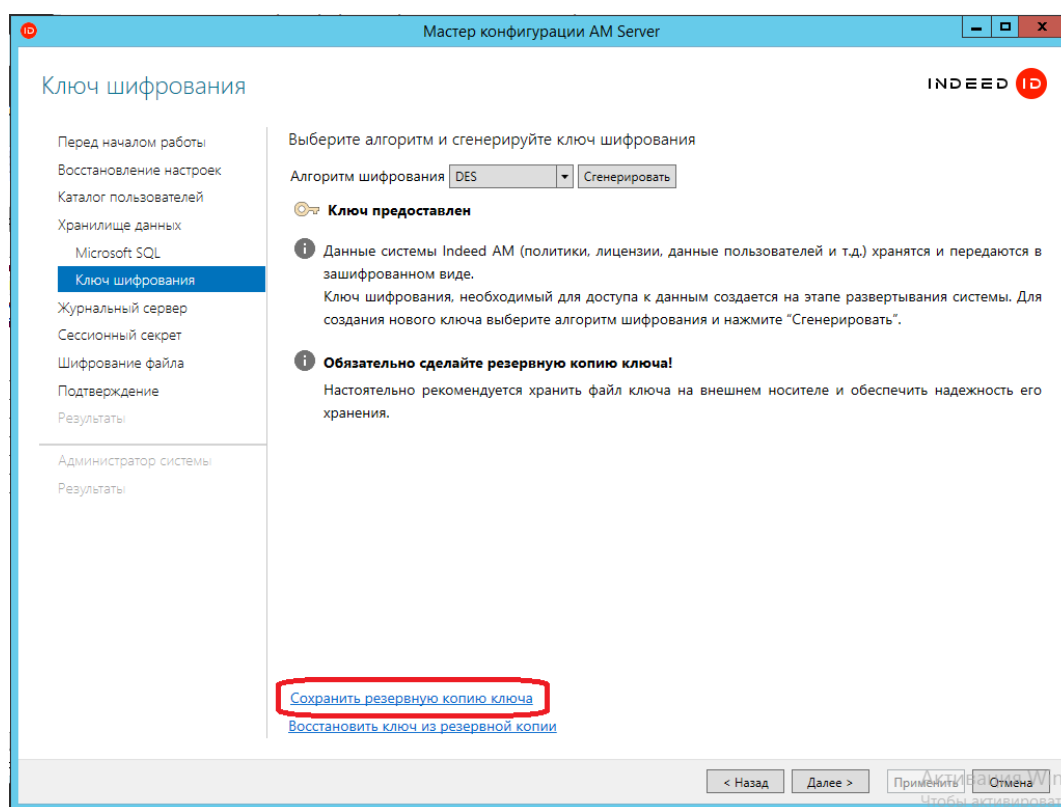
OK Отмена

Далее, при настройке Log Server'a Indeed AM 8.1, для **AM AirKey Cloud Server**, укажите данную БД (например: "indeed_akc_81") и учетную запись MS SQL сервера ([Indeed Key Server](#))

Подготовка базы данных хранилища Indeed AM 8.1

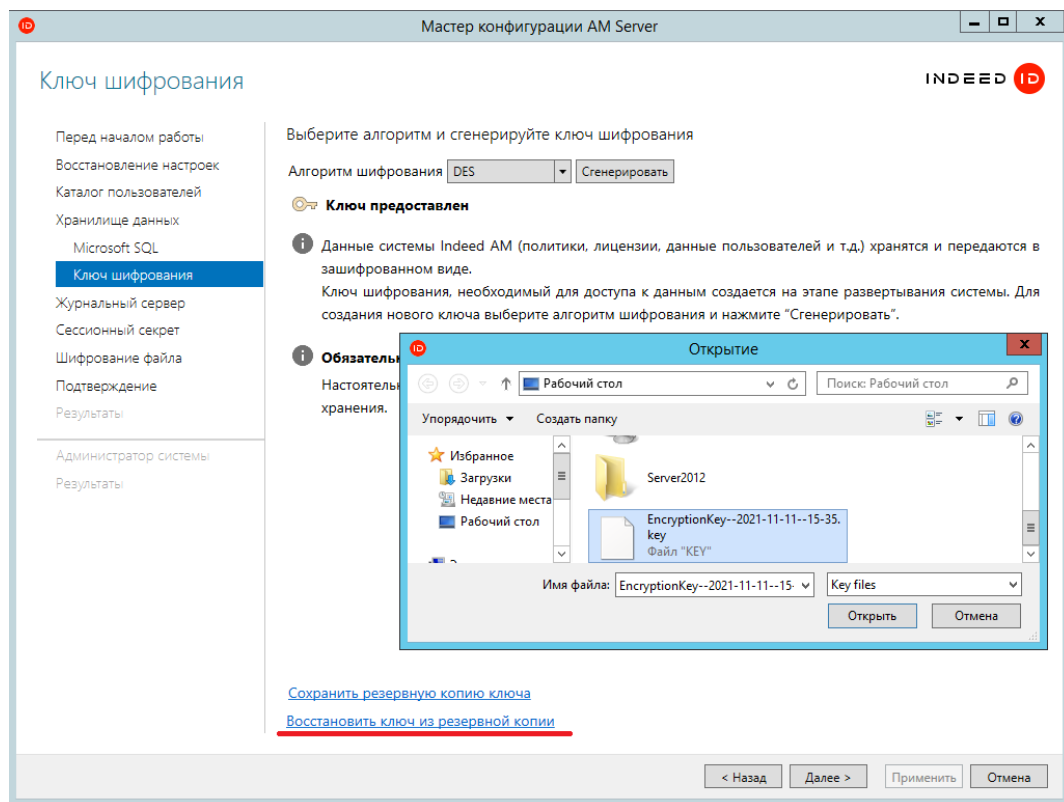
1. Запустите **Мастер конфигурации** на сервере **Indeed AM 7.x**

2. Пройдите в нём без изменений полей, до создания ключа шифрования, и сохраните резервную копию ключа



3. Перенесите полученный файл на сервер **Indeed AM 8.1**
4. Создайте **отдельную БД** для хранилища системы **Indeed AM 8.1** (в примере используется название базы данных "indeed_am_81")

5. Создайте иерархию таблиц в БД, с помощью **Мастера конфигурации** ([Настройка с помощью мастера конфигурации](#)), при создании используйте полученный ключ шифрования с Indeed AM 7.x



6. Остановите IIS сервер, с Indeed AM server 8.1

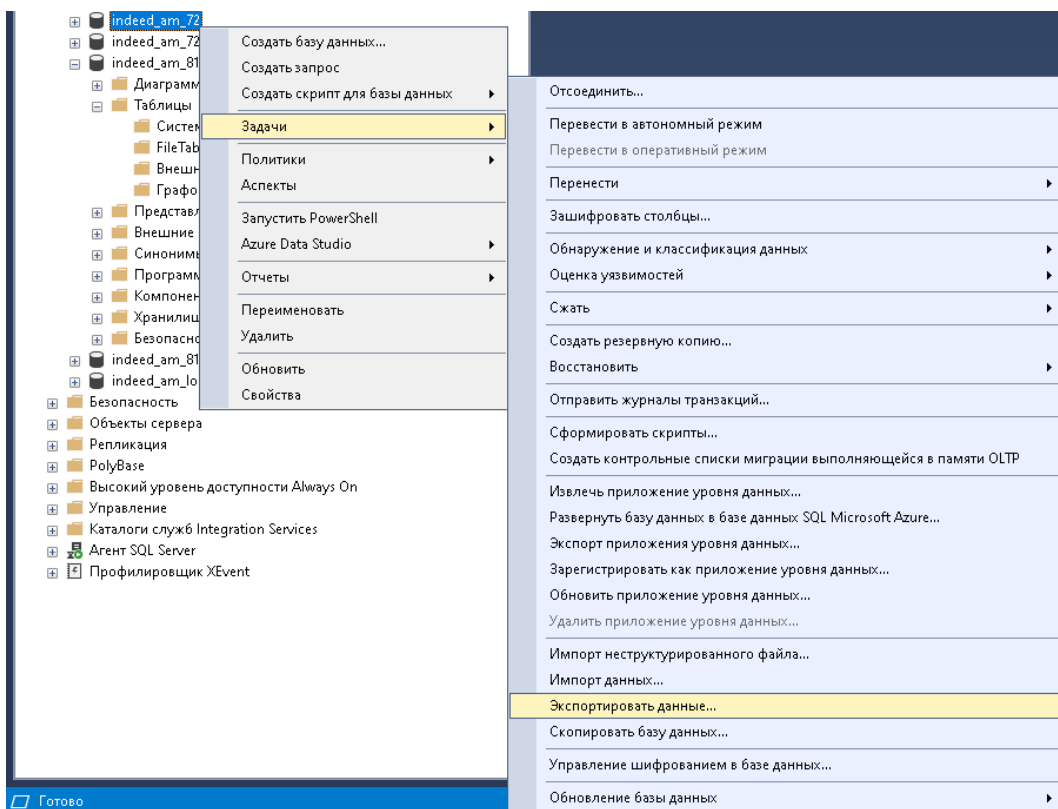
Миграция базы данных хранилища Indeed AM 7.x

Список таблиц для миграции:

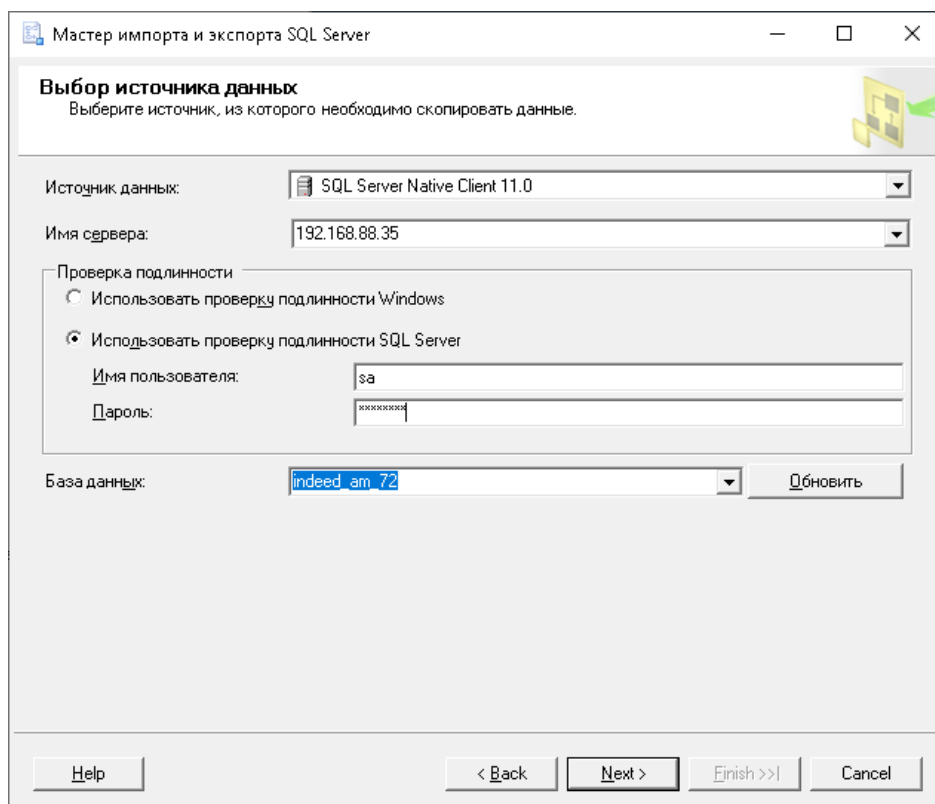
- DbInstanceProperties
- DbLicenses
- DbUserAuthenticators
- DbHardwareDevices
- DbHardwareDeviceProperties

Все шаги повторяются для каждой мигрируемой таблицы.

Запускаем экспорт данных БД - **Export Wizard**



1. Выбираем источник данных – базу данных хранилища 7.x



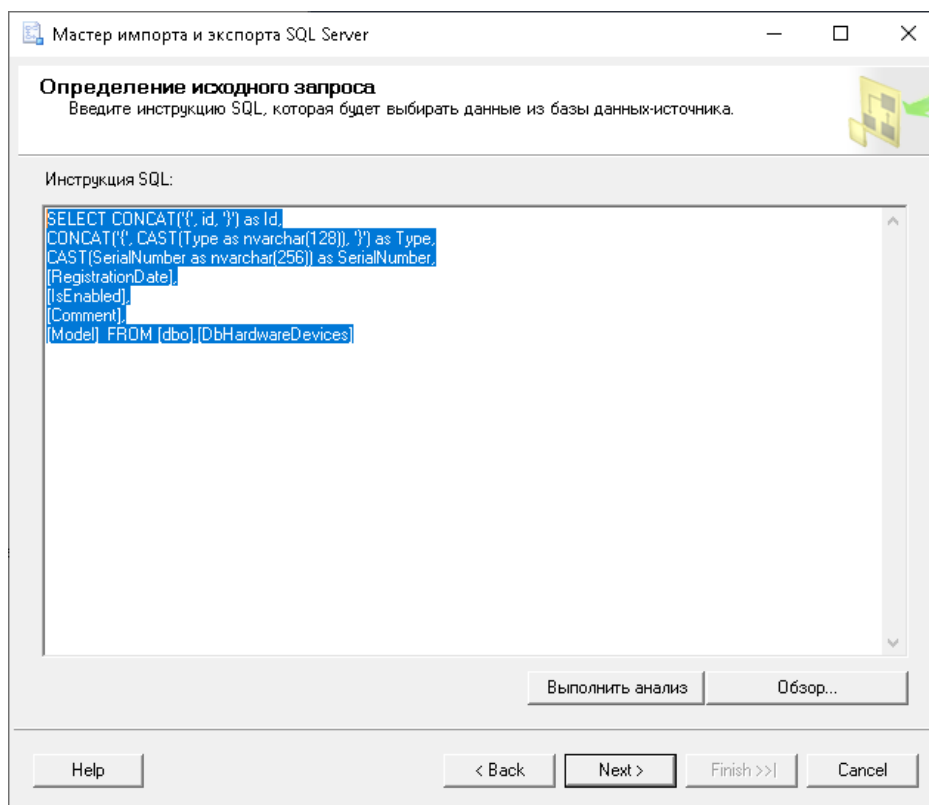
2. Выбираем приемник - базу данных хранилища 8.1

The screenshot shows the 'Master Import and Export SQL Server' dialog box, specifically the 'Выбор назначения' (Select destination) step. The title bar reads 'Мастер импорта и экспорта SQL Server'. The main heading is 'Выбор назначения' with the instruction 'Укажите, куда копировать данные.' (Specify where to copy the data). The 'Назначение:' (Destination) dropdown is set to 'SQL Server Native Client 11.0'. The 'Имя сервера:' (Server name) dropdown is set to '192.168.88.35'. Under the 'Проверка подлинности' (Authentication) section, the 'Использовать проверку подлинности SQL Server' (Use SQL Server authentication) radio button is selected. The 'Имя пользователя:' (Username) field contains 'sa' and the 'Пароль:' (Password) field contains masked characters. The 'База данных:' (Database) dropdown is set to 'indeed_am_81'. There are 'Обновить' (Refresh) and 'Создать...' (Create...) buttons next to the database dropdown. At the bottom, there are 'Help', '< Back', 'Next >', 'Finish >>|', and 'Cancel' buttons.

3. Выбираем получение данных для экспорта пользовательским запросом

The screenshot shows the 'Master Import and Export SQL Server' dialog box, specifically the 'Выбор копирования таблицы или запроса' (Select table or query) step. The title bar reads 'Мастер импорта и экспорта SQL Server'. The main heading is 'Выбор копирования таблицы или запроса' with the instruction 'Укажите, копировать ли таблицы и представления или копировать результаты запроса из источника данных.' (Specify whether to copy tables and views or copy query results from the data source). There are two radio button options: 'Скопировать данные из одной или нескольких таблиц или представлений' (Copy data from one or more tables or views) and 'Записать запрос, указывающий данные для передачи' (Write a query specifying the data to transfer). The second option is selected. Below the options, there is explanatory text for each. At the bottom, there are 'Help', '< Back', 'Next >', 'Finish >>|', and 'Cancel' buttons.

4. Указываем запрос для выборки данных (список всех запросов приведён в пункте "**Запросы получения данных из хранилища 7.x**")



The screenshot shows the 'Master Import and Export SQL Server' dialog box, specifically the 'Specify Source Query' step. The title bar reads 'Мастер импорта и экспорта SQL Server'. The main heading is 'Определение исходного запроса' (Specify Source Query), with a subtitle 'Введите инструкцию SQL, которая будет выбирать данные из базы данных-источника.' (Enter the SQL instruction that will select data from the source database.). Below this, there is a text area labeled 'Инструкция SQL:' (SQL Instruction:). The text area contains the following SQL query:

```
SELECT CONCAT('{', id, '}') as Id,
CONCAT('{', CAST(Type as nvarchar(128)), '}') as Type,
CAST(SerialNumber as nvarchar(256)) as SerialNumber,
[RegistrationDate],
[IsEnabled],
[Comment],
[Model] FROM [dbo].[DbHardwareDevices]
```

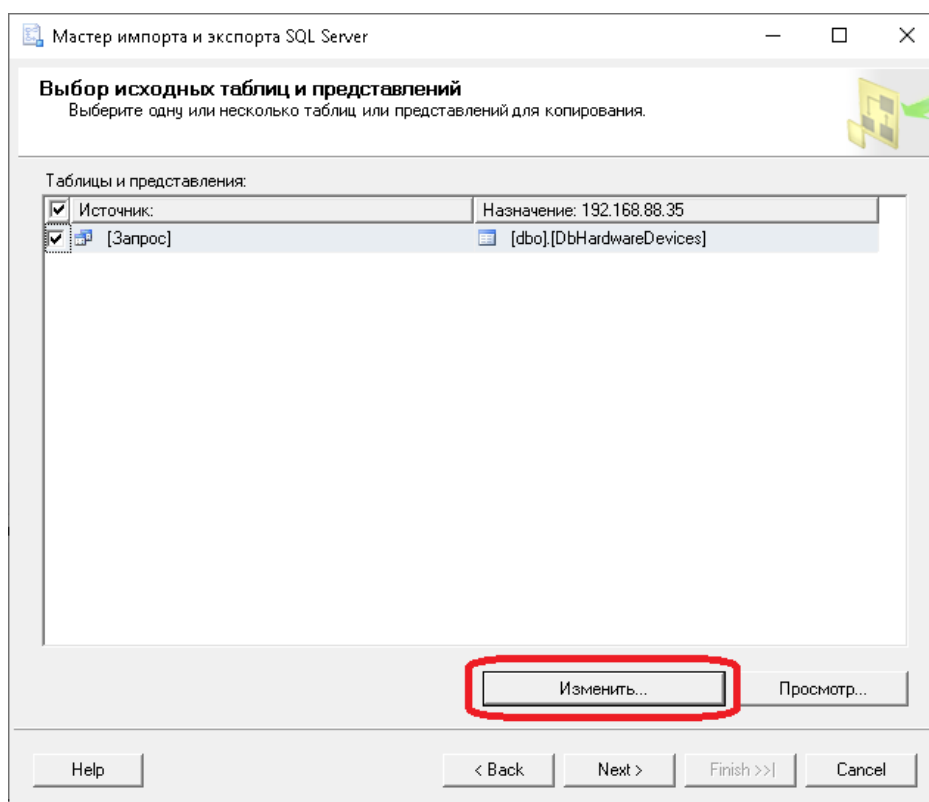
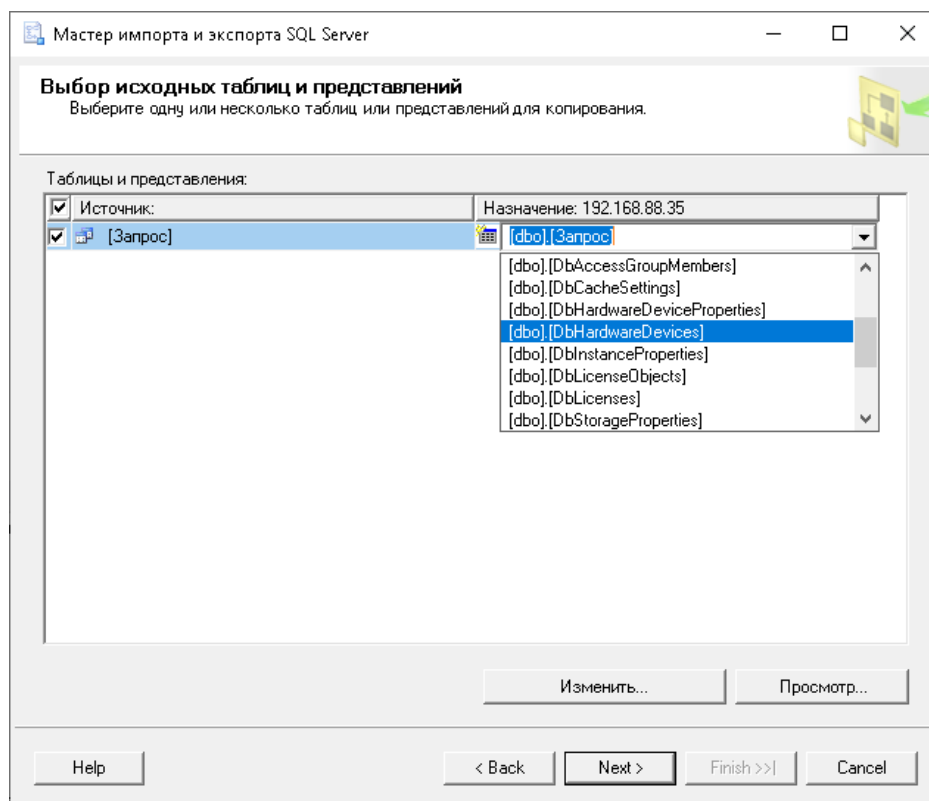
 At the bottom of the dialog, there are several buttons: 'Выполнить анализ' (Analyze), 'Обзор...' (Preview...), 'Help', '< Back', 'Next >', 'Finish >>|', and 'Cancel'.

Информация

Общая особенность экспорта - конвертирование формата идентификаторов записей таблиц из **nvarchar(128)** и **nvarchar(max)** в **uniqueidentifier**.

Текстовый вид **uniqueidentifier** обязательно должен содержать фигурные скобки {}, иначе конвертация sql server не сможет обработать строковое значение.

5. Далее выбираем таблицы для экспорта и импорта



6. В настройках маппинга на этом же экране указываем, что нужно удалять данные из таблицы - приемника

Сопоставления столбцов

Источник: [Запрос]
Назначение: [dbo].[DbHardwareDevices]

☐ Создать целевую таблицу
☒ Удалить строки в целевой таблице ☐ Удалить и создать повторно целевую таблицу
☐ Добавить строки в целевую таблицу ☐ Разрешить вставку в столбец идентификаторов

Сопоставления:

Источник	Назначение	Тип	Допу...	Размер	Точнос...	Мас...
Id	Id	uniqueidentifier	☐			
Type	Type	uniqueidentifier	☐			
SerialNumber	SerialNumber	nvarchar	☒	256		
RegistrationDate	RegistrationDate	datetime2	☐			7
IsEnabled	IsEnabled	bit	☐			
Comment	Comment	nvarchar	☒	max		
Model	Model	nvarchar	☒	max		

Исходный столбец: Id nvarchar (130) NOT NULL

7. Далее, проверяем набор полей и видим предупреждения о конвертировании данных

Мастер импорта и экспорта SQL Server

Просмотр сопоставления типов данных
Выберите таблицу, чтобы просмотреть, как ее типы данных сопоставляются с типами данных в целевом объекте и как обрабатываются проблемы с преобразованием.

Таблица:

Источник	Назначение
[Запрос]	[dbo].[DbHardwareDevices]

Сопоставление типов данных

Исходный столбец	Исходный тип	Целевой столбец	Целевой тип	Преобразование	В случае ошибки	В случае усечения
Id	nvarchar	Id	uniqueidentifier	☒	Использовать глобальную ошибку	Использовать глобальное усечение
Type	nvarchar	Type	uniqueidentifier	☒	Использовать глобальную ошибку	Использовать глобальное усечение
SerialNumber	nvarchar	SerialNumber	nvarchar			
RegistrationDate	datetime2	RegistrationDate	datetime2			
IsEnabled	bit	IsEnabled	bit			
Comment	ntext	Comment	nvarchar			
Model	ntext	Model	nvarchar			

Чтобы просмотреть сведения о преобразовании, дважды щелкните строку, содержащую исходный тип преобразуемого столбца.

В случае ошибки (используется глобально)
В случае усечения (используется глобально)

8. Запускаем процедуру экспорта

Мастер импорта и экспорта SQL Server

Сохранение и запуск пакета
Укажите, нужно ли сохранять пакет служб SSIS.

☒ Запустить немедленно
☐ Сохранить пакет служб SSIS

☒ Сервер SQL Server
☐ Файловая система

Уровень защиты пакета:
Шифровать конфиденциальные данные пользовательским ключом

Пароль:
Подтверждение:

Help < Back Next > Finish >>| Cancel

Мастер импорта и экспорта SQL Server

Выполнение прошло успешно

 **Success** 11 Total 0 Error
11 Success 0 Warning

Details:

Action	Status	Message
 Инициализация задачи потока данных	Success	
 Инициализация соединений	Success	
 Установка команд SQL	Success	
 Установка соединения с источником	Success	
 Установка соединения с назначением	Success	
 Проверка	Success	
 Подготовка к выполнению	Success	
 До выполнения	Success	
 Выполнение	Success	
 Копирование в [dbo].[DbHardwareDevices]	Success	Передано строк: 0
 После выполнения	Success	

Filter Stop Report Close

9. После миграции всех таблиц, запускаем IIS сервер с **Indeed AM 8.1**

Запросы получения данных из хранилища 7.x

1. Запрос к таблице **DbInstanceProperties**

Текст запроса

```
select CONCAT('{', id, '}') as Id
      ,Name
      ,Value
from dbo.dbinstanceproperties
```

2. Запрос к таблице **DbLicenses**

Текст запроса

```
SELECT CONCAT('{', id, '}') as Id
      ,[LicenseUid]
      ,[InstanceId]
      ,[Type]
      ,[AmountValue]
      ,[BeginDate]
      ,[EndDate]
      ,[Description]
      ,[Issuer]
      ,[IssuedTo]
      ,[IssueDate]
      ,[ControlValue]
FROM [dbo].[DbLicenses]
```

3. Запрос к таблице **DbUserAuthenticators**

Текст запроса

```
SELECT CONCAT('{', id, '}') as Id
      ,[UserId]
      ,CONCAT('{', ModelId, '}') as ModelId
      ,[ModeTypeName]
      ,[ModeDeviceName]
      ,[ModeType]
      ,[CreatedOn]
      ,[TemplateRawData]
      ,[Description]
      ,[IsDisabled]
      ,[ExpirationDate]
      ,[AuthenticationCountLimitValue]
      ,[Flags]
      ,[IsLocked]
      ,[SerialNumber]
FROM [dbo].[DbUserAuthenticators]
```

4. Запрос к таблице **DbHardwareDevices**

Текст запроса
<pre>SELECT CONCAT('{', id, '}') as Id ,CONCAT('{', CAST(Type as nvarchar(128)), '}') as Type ,CAST(SerialNumber as nvarchar(256)) as SerialNumber ,[RegistrationDate] ,[IsEnabled] ,[Comment] ,[Model] FROM [dbo].[DbHardwareDevices]</pre>

5. Запрос к таблице **DbHardwareDeviceProperties**

Текст запроса
<pre>SELECT CONCAT('{', id, '}') as Id ,CONCAT('{', CAST(HardwareDeviceId as nvarchar(128)), '}') as HardwareDeviceId ,[PropertyId] ,[Value] FROM [dbo].[DbHardwareDeviceProperties]</pre>

Миграция хранилища Active Directory



Важно

Обязательное условие - **ключи шифрования** хранилища и структура пользовательских каталогов (их идентификаторы) обоих инстансов **должны совпадать**.



Информация

Используется инструмент ADUC.

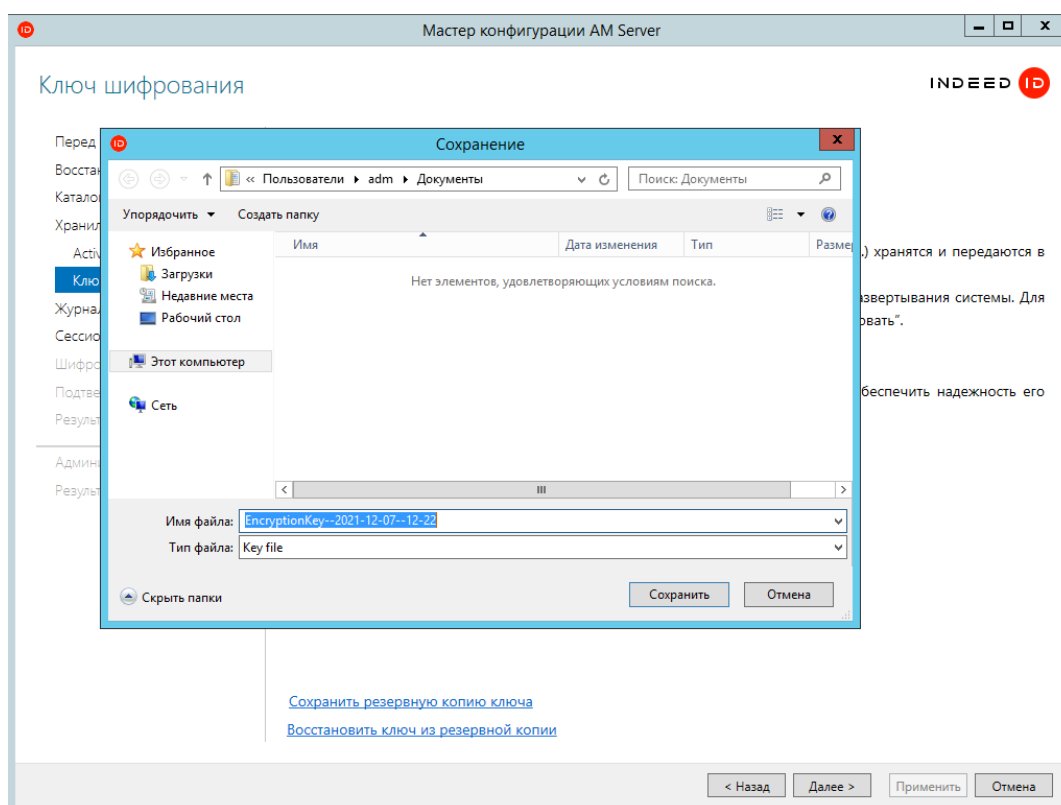
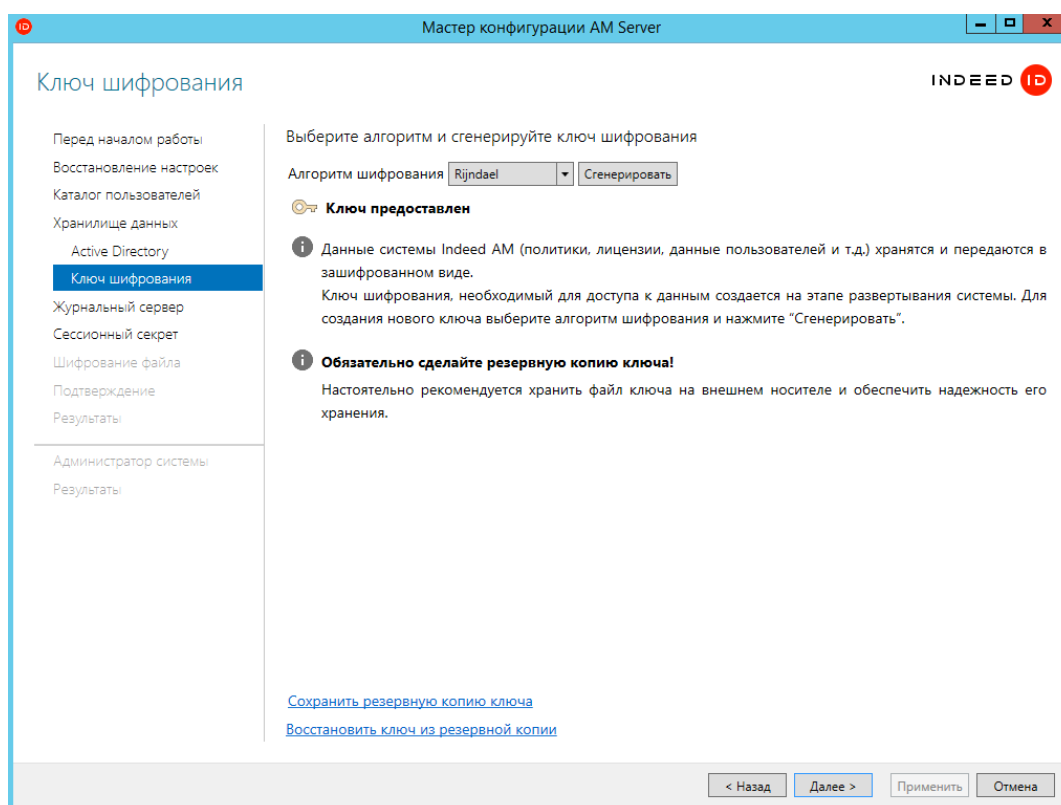
Миграция осуществляется по шагам, интерактивно, прозрачно для администратора AD.

Миграция производится путем перемещения объектов с данными AM из контейнера хранилища EA 7 в хранилище AM 8.

Подготовка AD хранилища Indeed AM 8.1

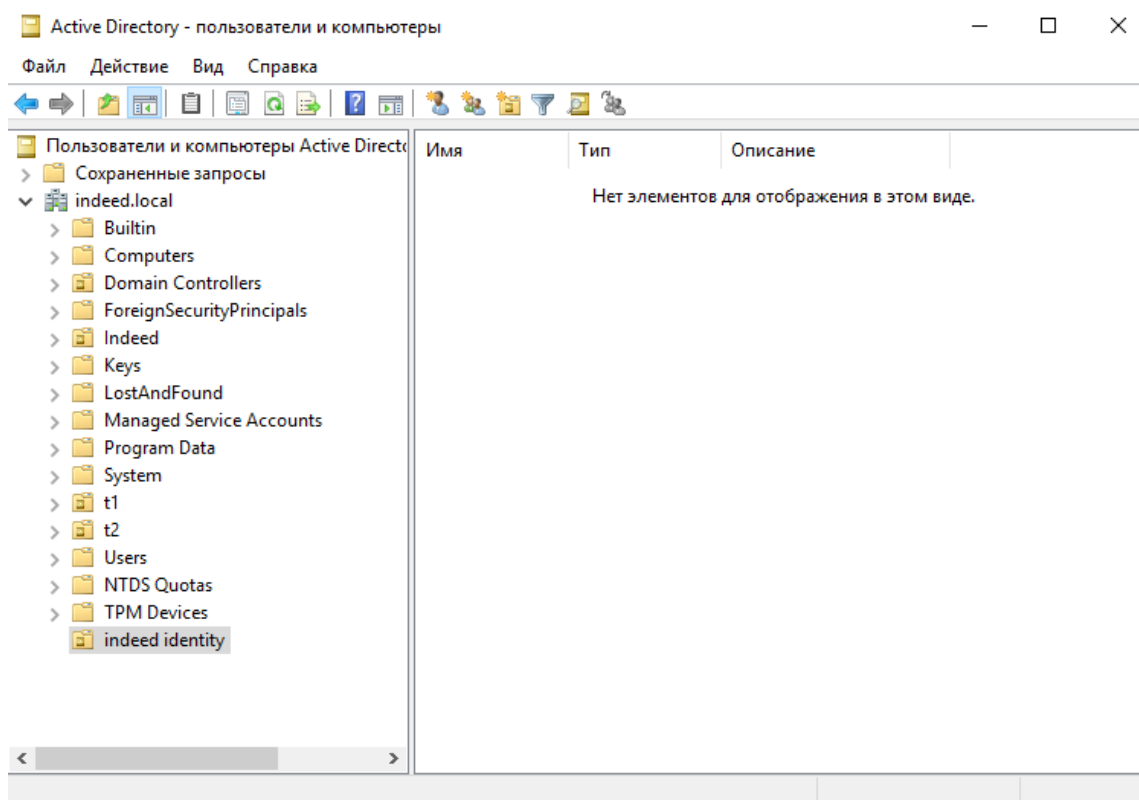
1. Запустите **Мастер конфигурации** на сервере **Indeed AM 7.x**

2. Пройдите в нём без изменений полей, до создания ключа шифрования, и сохраните резервную копию ключа

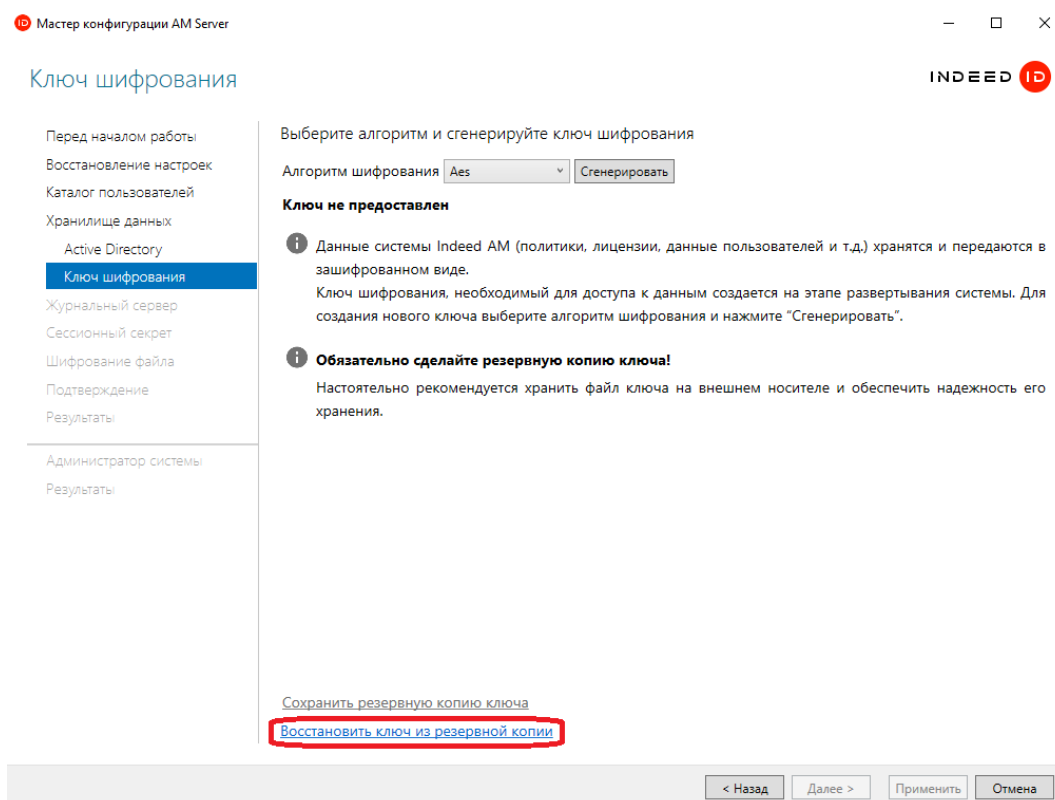


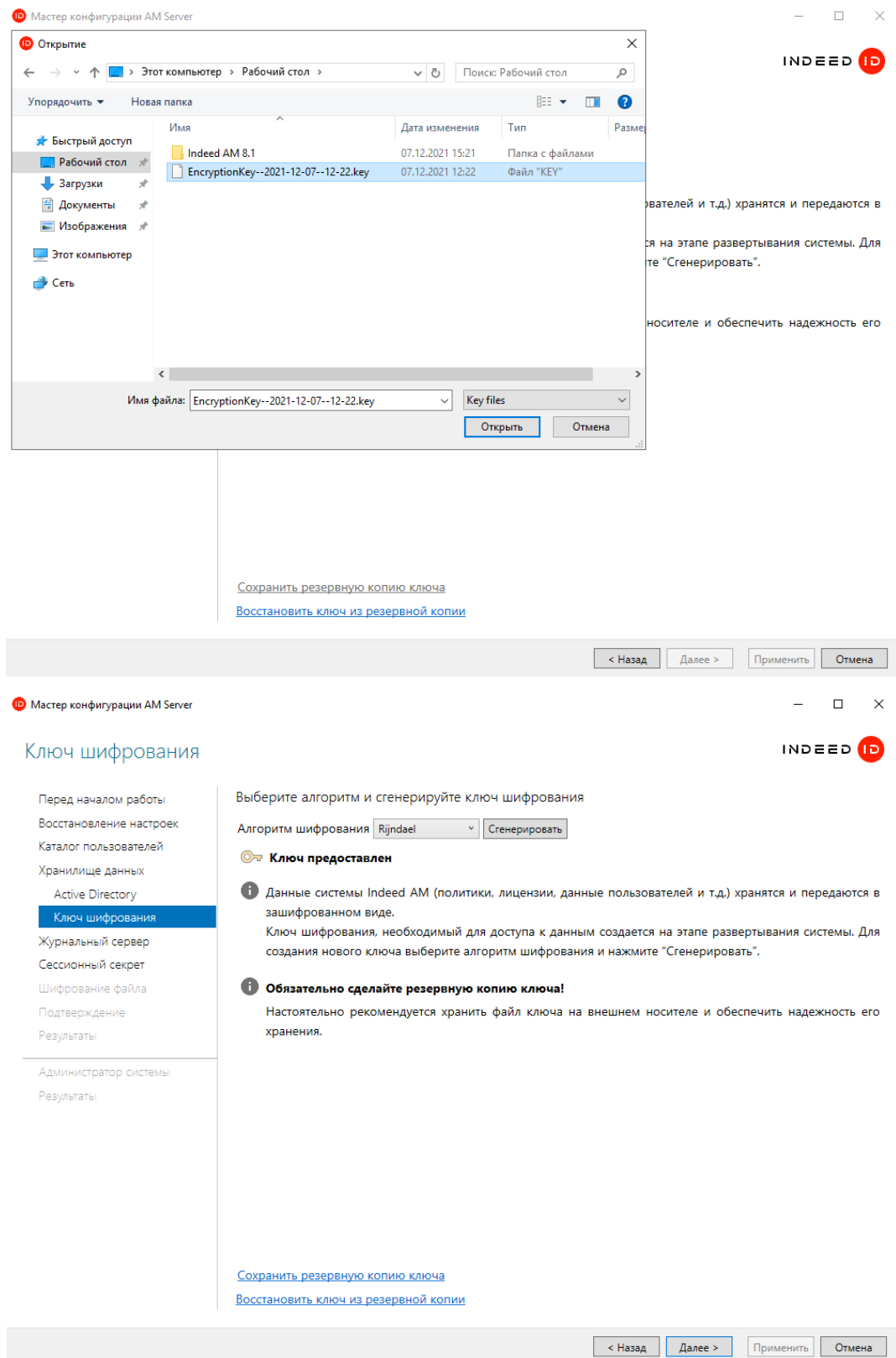
3. Перенесите полученный файл на сервер **Indeed AM 8.1**

4. Создайте **отдельный каталог в AD** для хранилища системы **Indeed AM 8.1** (в примере используется каталог "indeed identity").



5. Создайте **иерархию каталогов в AD**, с помощью **Мастера конфигурации**, при создании используйте полученный ключ шифрования с Indeed AM 7.x





6. Остановите IIS сервер, с Indeed AM server 8.1

Миграция AD хранилища Indeed AM 7.x

Список контейнеров для миграции:

- InstanceProperty
- License
- UserAuthenticator
- HardwareDevice
- HardwareDeviceProperty

В примере указаны два хранилища в AD:

- **Indeed** - хранилище Indeed AM 7.x
- **indeed identity** - хранилище Indeed AM 8.1

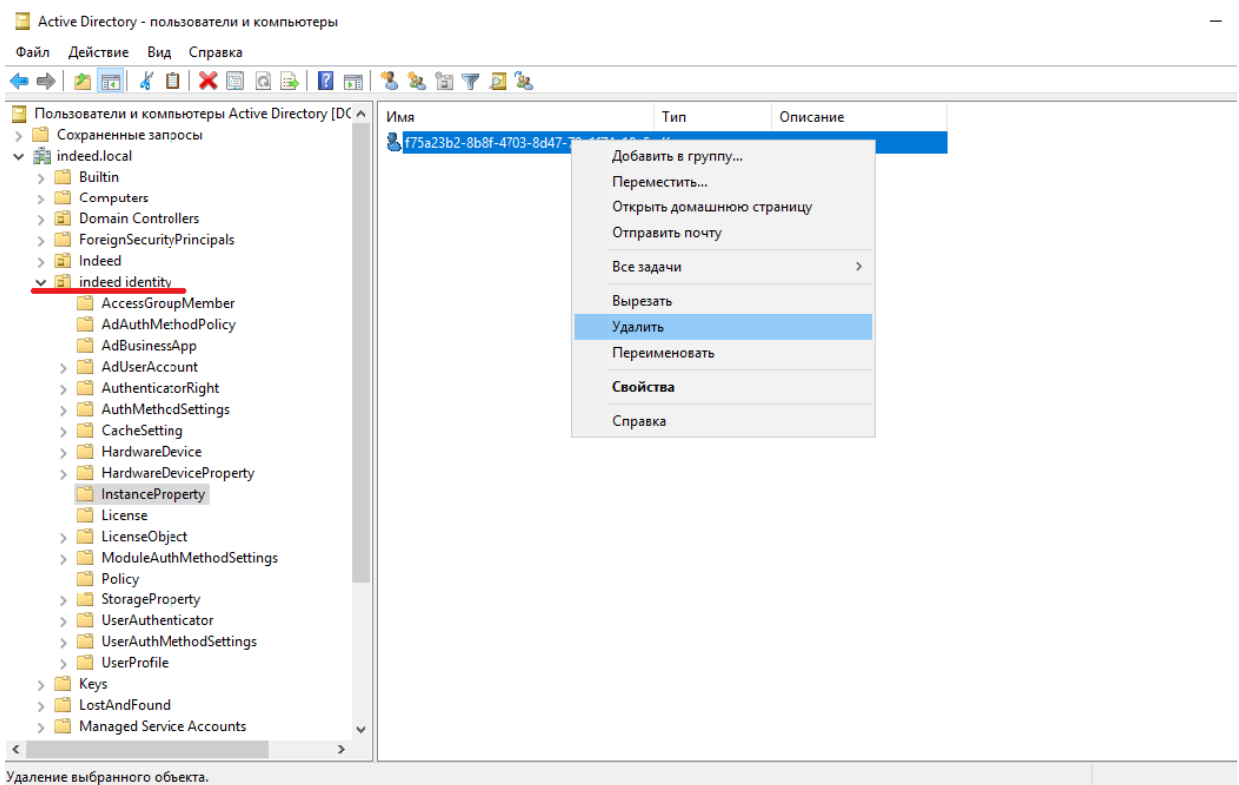
Информация

При необходимости объемных групповых перемещений, можно использовать скрипт **PowerShell** и командлет **Move-ADObject**:

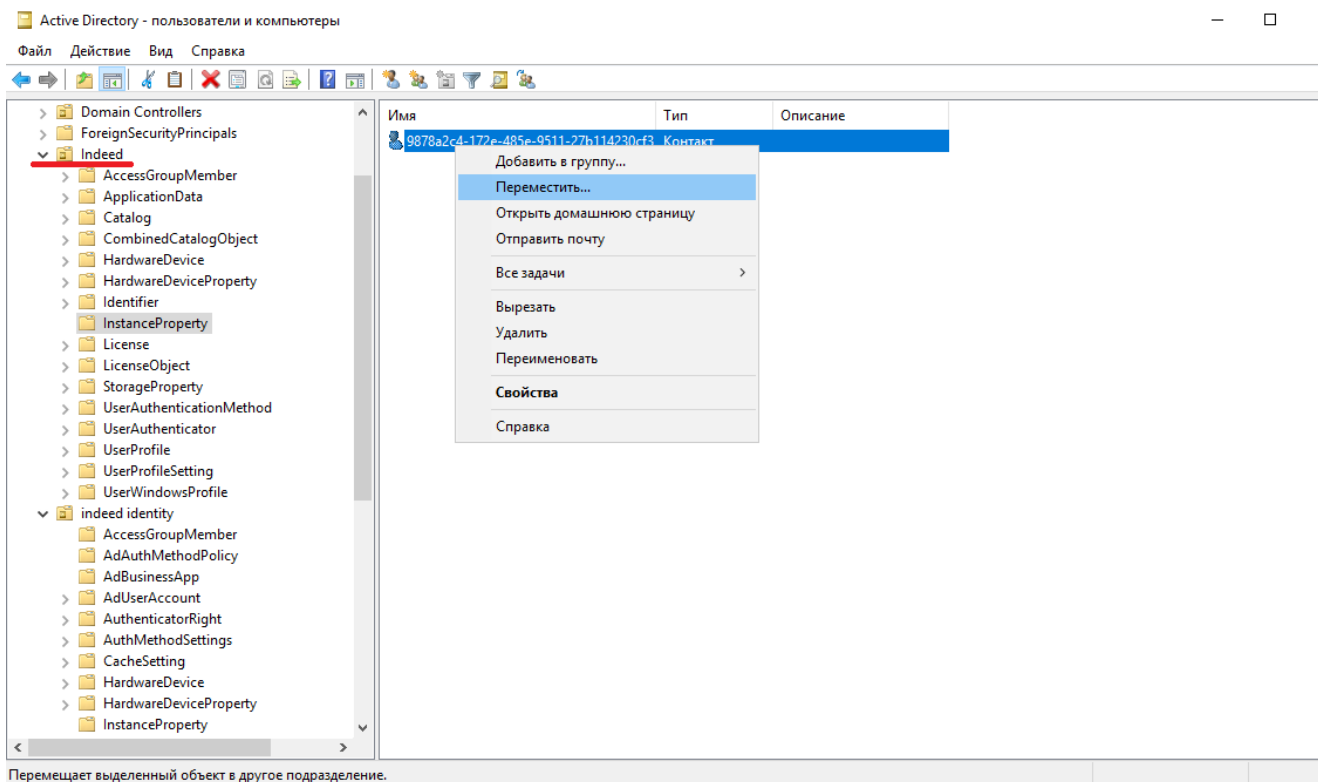
<https://docs.microsoft.com/en-us/powershell/module/activedirectory/move-adobject?view=windowsserver2019-ps>

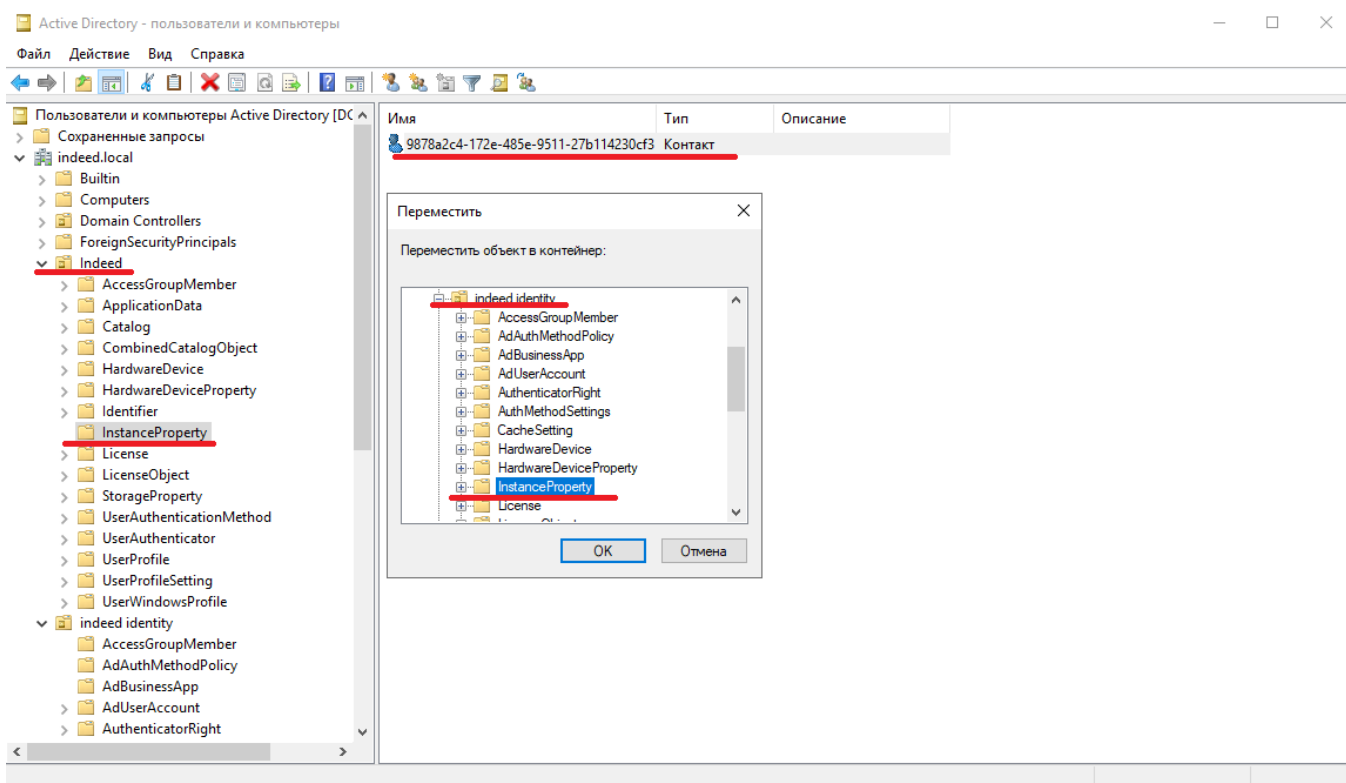
Миграция InstanceProperty

1. Удалим содержимое каталога **indeed identity-InstanceProperty**



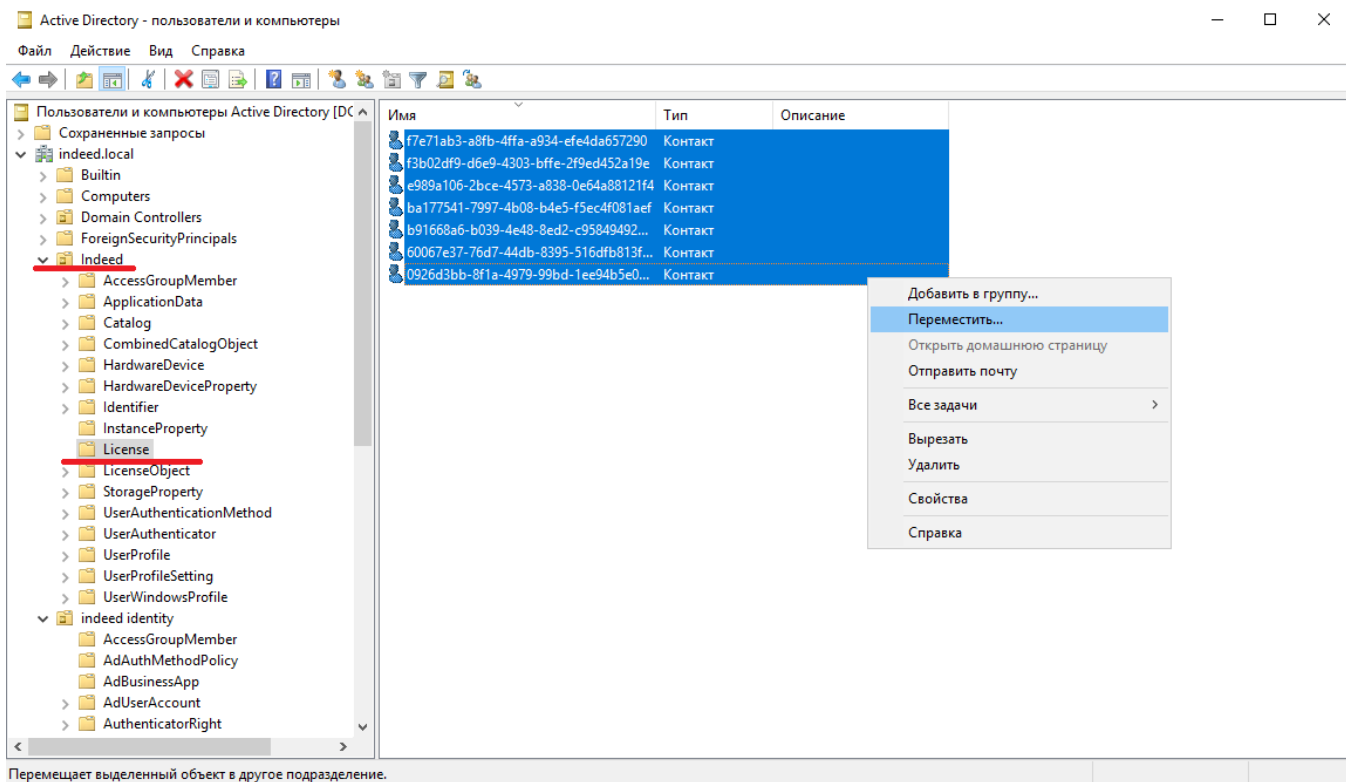
2. Переместим содержимое каталога **indeed-InstanceProperty** в **indeed identity-InstanceProperty**

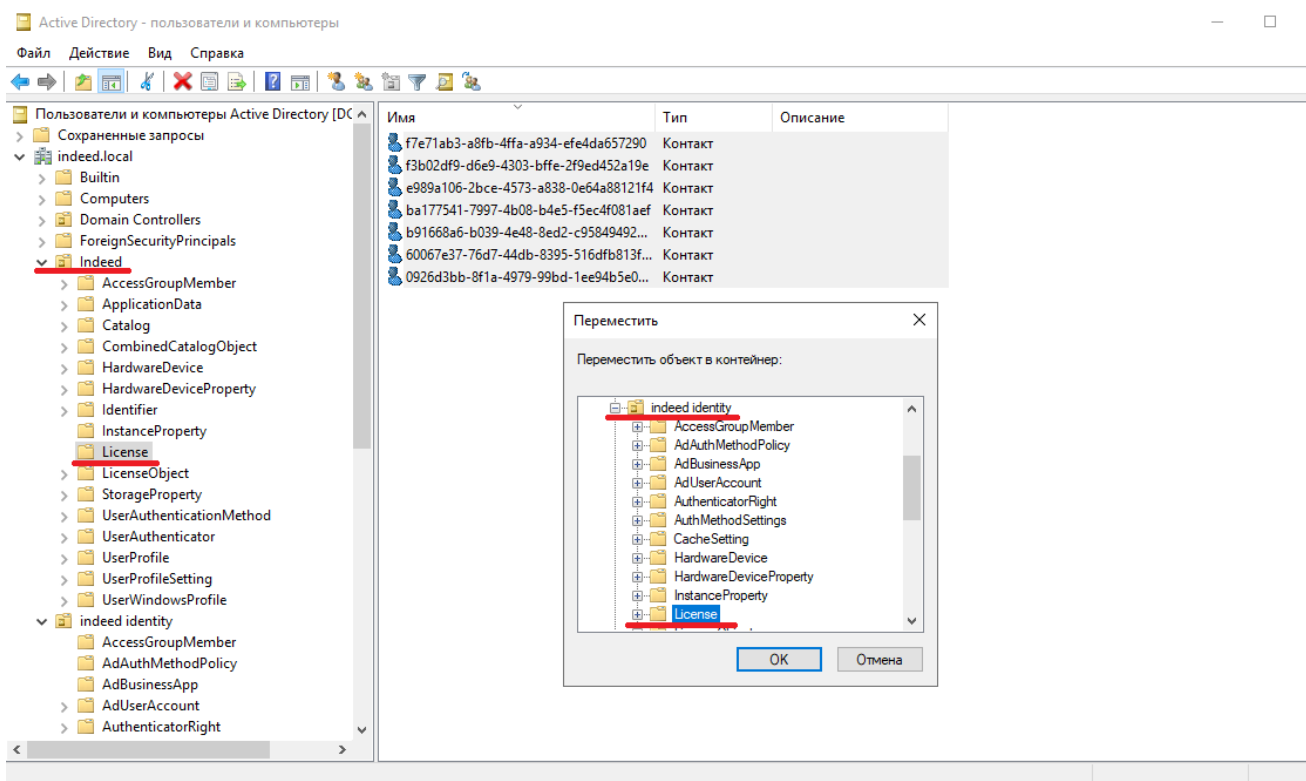




Миграция License

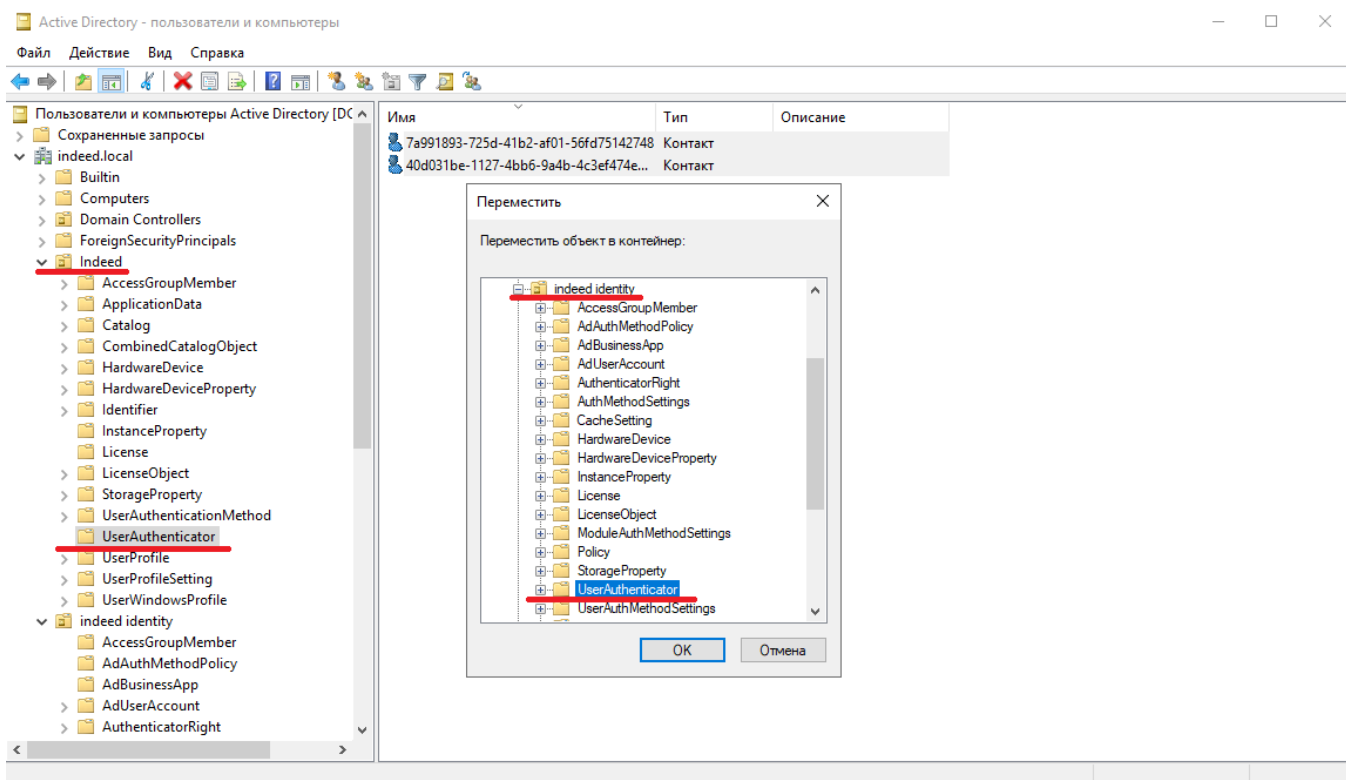
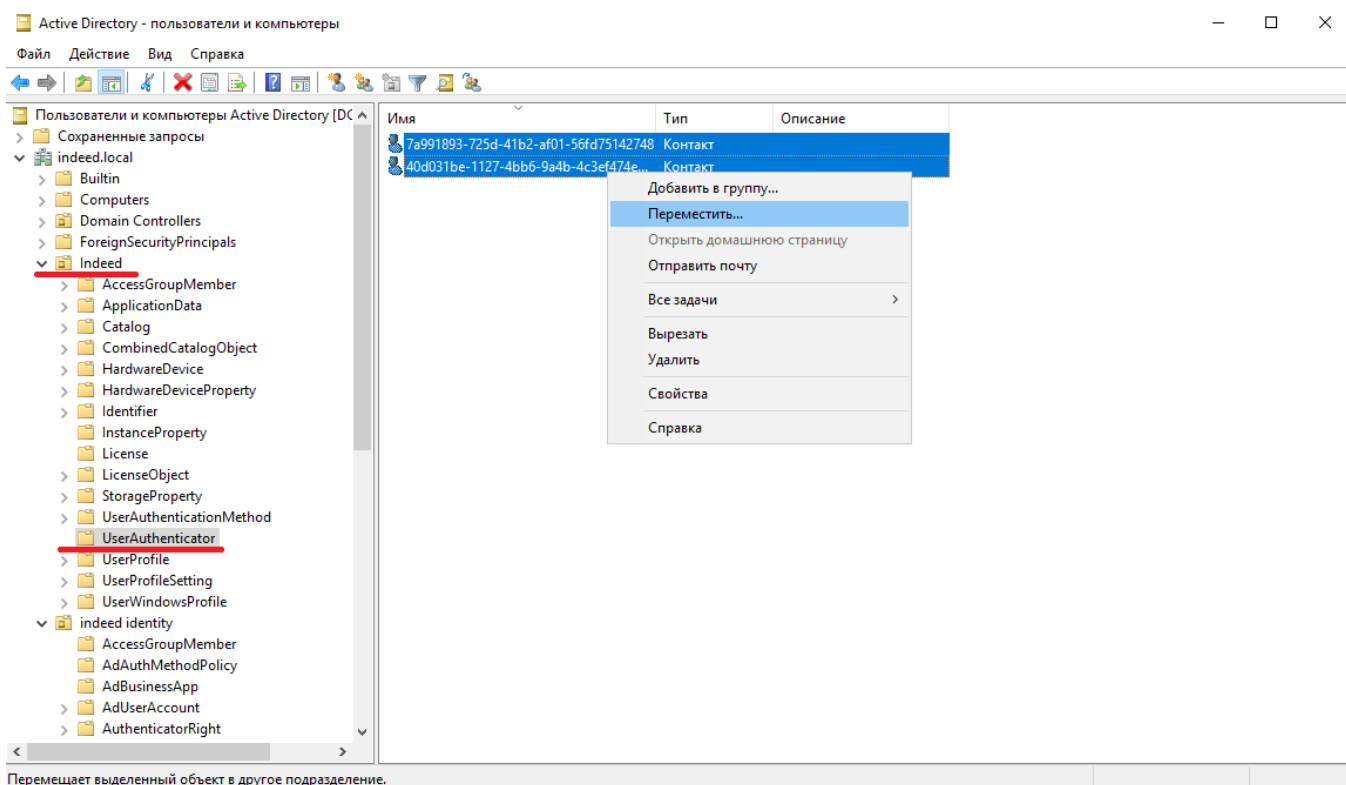
Переместим содержимое каталога **indeed-License** в **indeed identity-License**





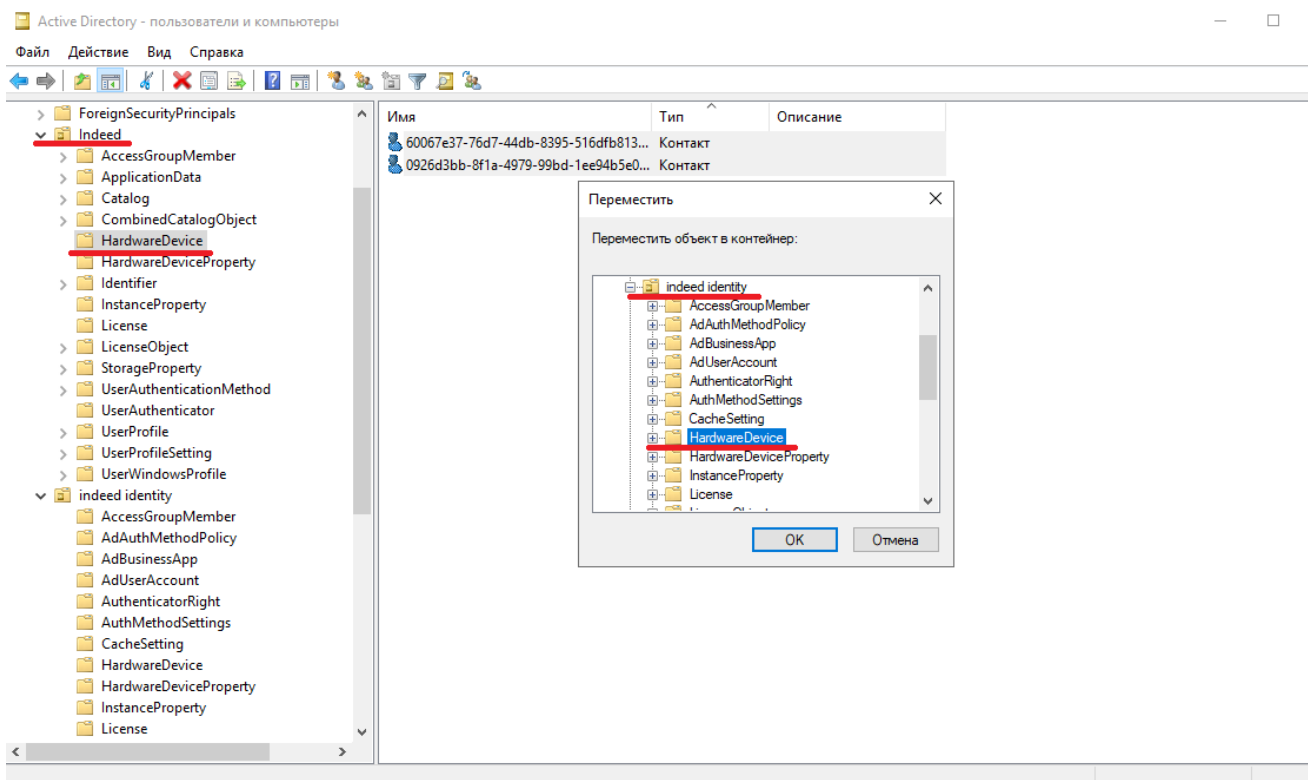
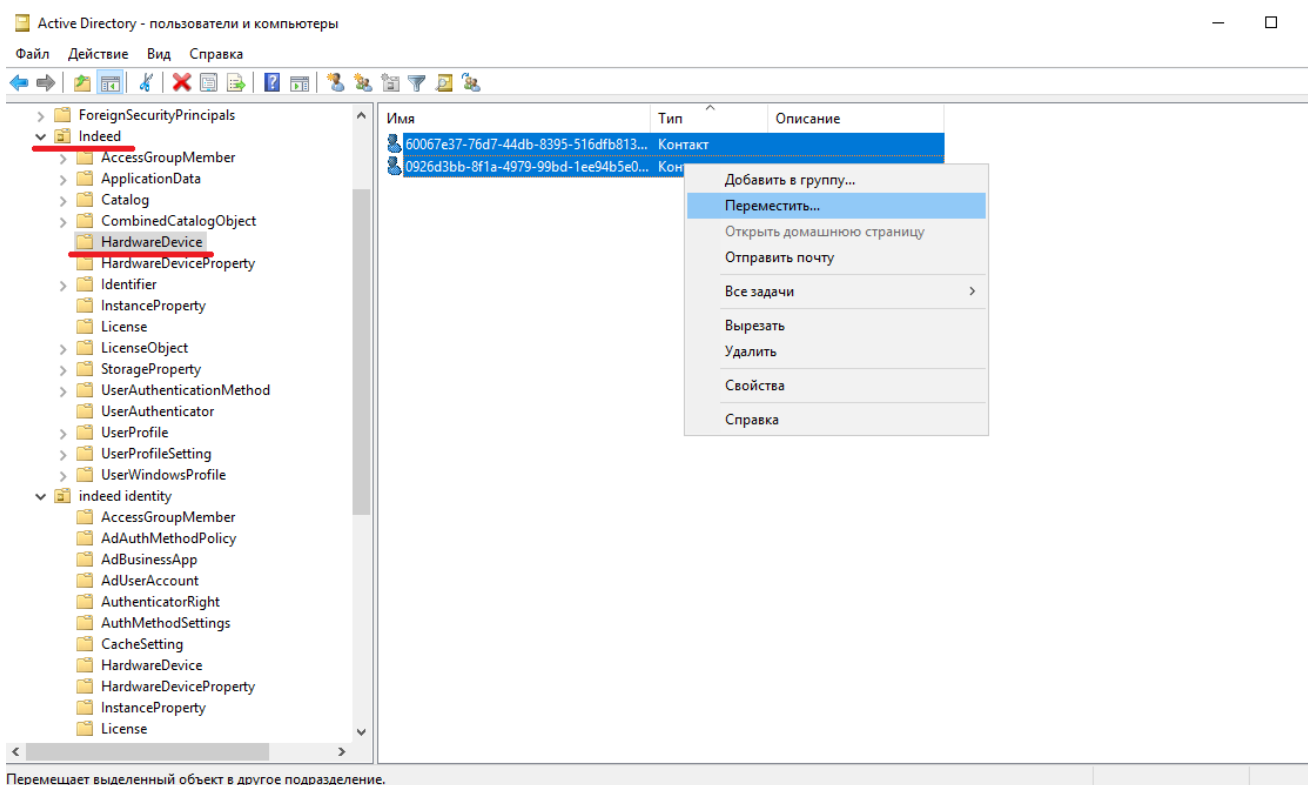
Миграция UserAuthenticator

Переместим содержимое каталога **indeed-UserAuthenticator** в **indeed identity-UserAuthenticator**



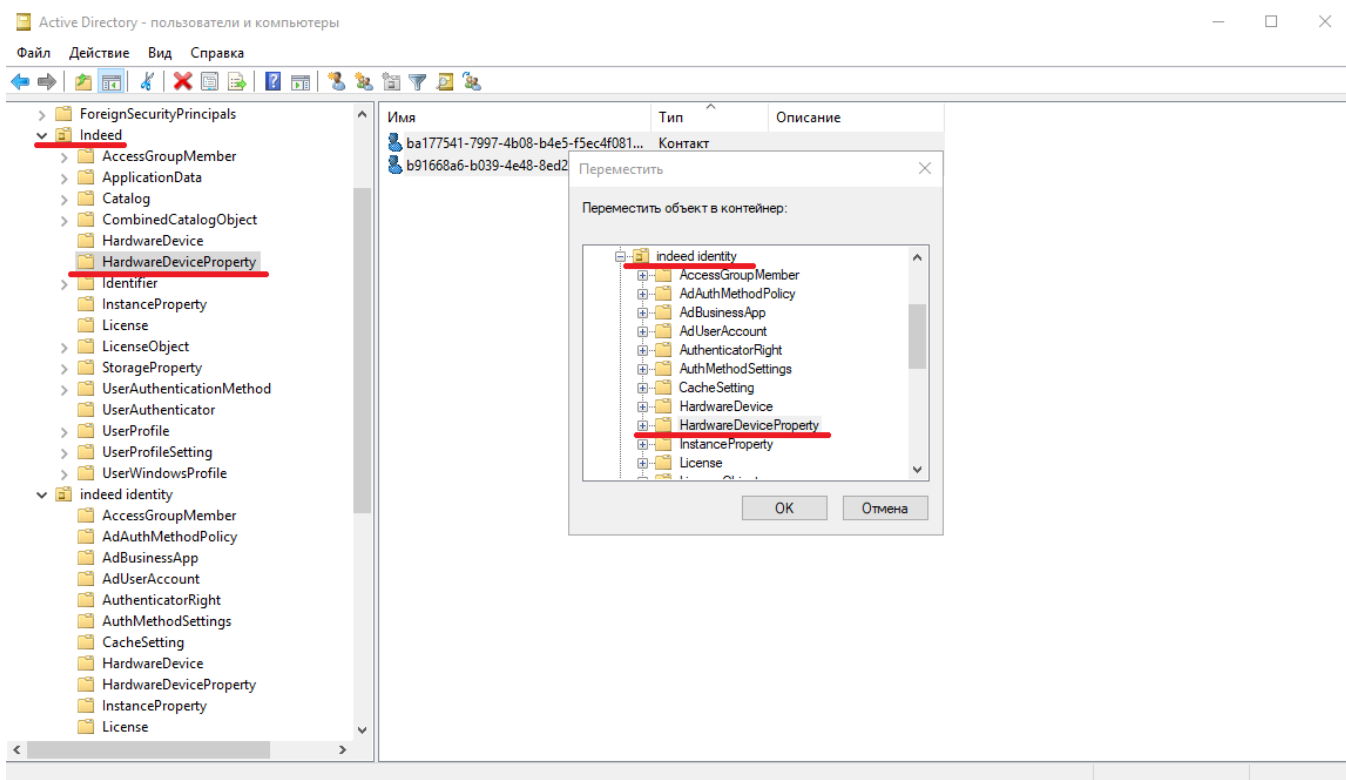
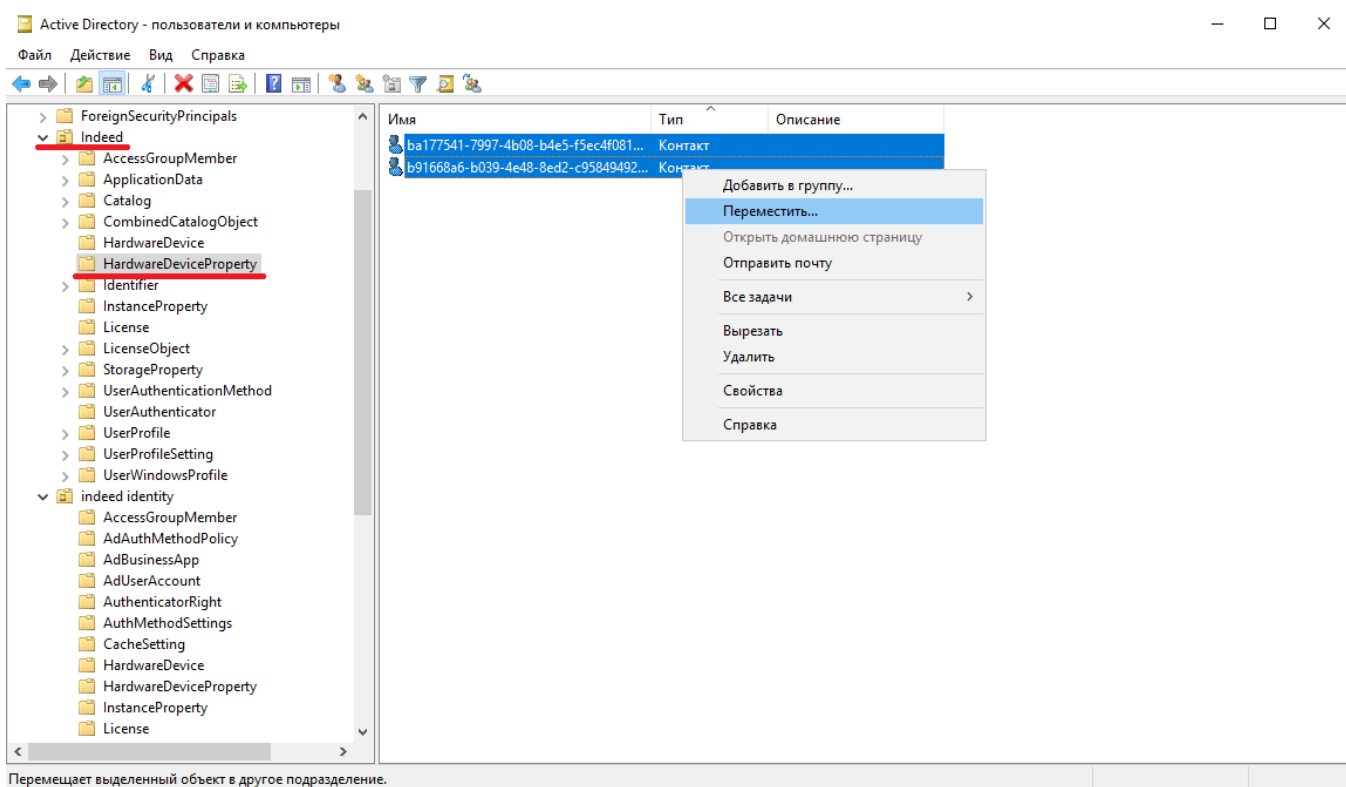
Миграция HardwareDevice

Переместим содержимое каталога **indeed-HardwareDevice** в **indeed identity-HardwareDevice**



Миграция HardwareDeviceProperty

Переместим содержимое каталога **indeed-HardwareDeviceProperty** в **indeed identity-HardwareDeviceProperty**



При завершении миграции, запустите IIS сервер, с **Indeed AM server 8.1**.

Администрирование системы

В разделе описаны возможности управления и администрирования системы.

- API
 - Общая информация
 - Быстрый старт
 - Описание методов API
 - Authenticator
 - License
 - Logon
 - Policy
 - TemplateSession
 - User
 - UserCatalog
 - UserProfile
 - Сценарии использования
 - 2FA аутентификация в API
 - Получение списка лицензий с их общим количеством и количеством использо
 - Получение списка пользователей с лицензиями
 - Сбор статистики по обученным аутентификаторам пользователей
 - Создание отчетов
 - Создание отчета "Количество аутентификаций по указанным провайде
- Консоль администратора
 - Получение и регистрация лицензий
 - Создание и настройка политик
 - Добавление и настройка приложений
 - Кеширование данных пользователя
 - Управление аутентификаторами
 - Поиск пользователей
 - Карточка пользователя
 - Журнал событий
 - Конфигурация
- Консоль управления аутентификаторами пользователя
 - Локализация (User Console)
 - Управление аутентификаторами (User Console)
 - Карточка пользователя (User Console)
- Утилита управления аутентификаторами
 - Удаление аутентификатора
 - Проверка аутентификатора
 - Редактирование аутентификатора
 - Добавление аутентификатора

API



Важно!

Документация находится в процессе наполнения.

- [Общая информация](#)
- [Быстрый старт](#)
- [Описание методов API](#)
- [Сценарии использования](#)

Общая информация

Информация

Для интеграции с различными приложениями может быть использовано API Indeed AM.

В данном разделе описаны основные моменты и общие параметры, которые необходимы для использования API Indeed.

Запрос к API

Для обращения к методу необходимо выполнить POST, для некоторых методов GET, запрос по URL вида *http(s)://<dns_indeedam_server>/am/core/<url_api_method>*, где

- *dns_indeedam_server* — полное DNS имя сервера, где развернут Indeed AM Server.
- *url_api_method* — URL адрес соответствующего метода. URL указаны в документации к соответствующему методу, либо в Swagger.

Пример для метода `authenticateByWindowsToken`, где DNS-имя сервера Indeed AM — *indeedam.indeed.local*

Пример

`https://indeedam.indeed.local/am/core/api/v5/logon/authenticateByWindowsToken`

Важно!

При использовании `https` необходимо загрузить на сервере Indeed AM валидный сертификат.

Идентификатор пользователя

Параметр "UserId"

В данном параметре указывается уникальный идентификатор пользователя из системы Indeed.

1. Данный идентификатор состоит из строкового id, указанного в Web.config AM в параметре "userId", и "objectGuid" пользователя из AD. Например:
 - а. В параметре "userId" указано значение, GUID пользователя "10efa04f-7ba9-47d8-89db-56e166f1679f". UserId пользователя будет **UserId_10efa04f-7ba9-47d8-89db-56e166f1679f**
2. Для получения userId можно воспользоваться методом **[POST] /api/v5/user/searchUserId**

Идентификаторы способов аутентификации



Параметр "modelId"

Уникальный Id способа аутентификации Indeed. Способы аутентификации:

- Indeed AM Windows Password Provider — {CF189AF5-01C5-469D-A859-A8F2F41ED153}
- Indeed AM Smart Card Provider — {0AF65AD8-DB77-4B64-B489-958D9B36E28C}\ +PIN: {42456525-8EC1-4AB1-97B8-45AF8635D10F}
- Indeed AM IronLogic Z2USB Provider — {CB5109DA-B575-422C-8805-524FE12B02F5}\ +PIN: {1EDFD6E1-FD66-4A5B-971A-CBA0C611BA9B}
- Indeed AM OMNIKEY Provider — {4B15AF52-A795-4CA6-B7CD-CDB8ABF2D2C2}\ +PIN: {199B8FA8-FA9D-4ED8-941D-F86A5C681E0C}
- Indeed AM Futronic Provider — {A0EF00AD-1EEB-4D48-8BCF-06E19CD5585F}
- 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 Telegram OTP Provider — {CA4645CC-5896-485E-A6CA-011FCC20DF1D}
- 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}
- Indeed AM RealSense Provider — {3822CAF9-BBFC-4E89-9BAF-E751B38D1DFC}

Для получения всех установленных способов аутентификации на сервере Indeed AM можно воспользоваться методом **[GET] /api/v5/authenticationProvider/getAll**

Идентификаторы приложений



Параметр "ApplicationId"

Внутренний модуль



Важно!

Для работы с внутренним модулем не требуется лицензия, достаточно иметь права на операции, предоставляемые внутренними модулями.

Функционал АМ разбит на группы, за которые отвечают внутренние модули. Они реализуют внутреннюю бизнес-логику решения. Их строковые идентификаторы используются для обращения к разным частям API Core сервера.

Внутренние модули Core сервера:

- 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!

Требуется лицензия для соответствующего модуля

Модуль, реализующий взаимосвязь решения AM и внешних систем, с которыми выполняется интеграция. К ним относятся:

- Windows Logon
- Enterprise SSO
- IIS Extension
- NPS RADIUS Extension
- Indeed AM Identity Provider
- ADFS Extension
- RDP Windows Logon
- Authentication API

Модули интеграции могут представлять собой одно бизнес-приложение (например Windows Logon), а могут иметь набор бизнес-приложений, которые можно добавлять /удалять (например модуль Enterprise SSO. Он предоставляет возможности интеграции с разными типами приложений пользователя (Desktop apps, Web apps) и для каждого нужно создавать отдельное бизнес-приложение ESSO: 1C, Lotus Notes и пр.).

Идентификатор политики

Чтобы узнать идентификатор политик, выполните следующие:

1. Откройте консоль администратора системы Indeed.
2. Перейдите на вкладку "Политики".
3. Нажмите на целевую политику.
4. Скопируйте значение id политики из GET параметра в URL

`am/mc/Policies/Summary?policyId=f38dbe13-c809-4962-a0c2-2af1ed52af6f`

Быстрый старт

Swagger

Для вызовов методов API, тестирования запросов удобно использовать интерфейс Swagger, который встроен в "core". Для включения доступа к интерфейсу выполните следующие действия:

1. Откройте конфигурационный файл сервера Indeed AM "**web.config**" (C:\inetpub\wwwroot\am\core).
2. Для параметра "**enableSwagger**" установите значение "**true**".
3. Интерфейс Swagger будет доступен по ссылке **http(s)://<DNS_IndeedAM_Server>/am/core/swagger/**

 **swagger**

https://indeedam.indeed.local/am/core/v5/swagger

api_key

Explore

EA.Server API

Created by Indeed Id
[Contact the developer](#)

AccessControl	Show/Hide	List Operations	Expand Operations
AuthenticationMethod	Show/Hide	List Operations	Expand Operations
AuthenticationProvider	Show/Hide	List Operations	Expand Operations
Authenticator	Show/Hide	List Operations	Expand Operations
BusinessApplication	Show/Hide	List Operations	Expand Operations
ESSO	Show/Hide	List Operations	Expand Operations
HardwareDevice	Show/Hide	List Operations	Expand Operations
HealthCheck	Show/Hide	List Operations	Expand Operations
Identification	Show/Hide	List Operations	Expand Operations
InstanceInfo	Show/Hide	List Operations	Expand Operations
License	Show/Hide	List Operations	Expand Operations
Logon	Show/Hide	List Operations	Expand Operations
Module	Show/Hide	List Operations	Expand Operations

Токен администратора

Для большинства запросов API требуются определенные права в системе Indeed для выполнения. 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.

Получение токена с помощью `"authenticateByWindowsToken"`

Данный способ получения токена является самым простым. Для получения необходимо вызвать один метод от имени пользователя, для которого будет выдан токен.

- Если запрос выполняется через браузер, то браузер должен быть запущен от имени требуемого пользователя.
- В Powershell, например, при запросе необходимо использовать дополнительный параметр `"UseDefaultCredentials"` ([пример](#) функции `"postRequestForWin"` в Powershell).

В качестве идентификатора приложения может быть указано любое приложение из [списка a Indeed](#).



Важно!

Используемое приложение будет указываться в событиях аутентификации.

Response Body

```
{
  "ValidPropertiesMask": 5,
  "Token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJleHAiOjE2NjE2OTAwOTEuMCwidXNlc19pZCI6I1VzZXJJZjZlMGVmYTA0Zi03YmE5LTQ3ZDgtC",
  "LogonResult": null,
  "UserId": "UserId_10efa04f-7ba9-47d8-89db-56e166f1679f"
}
```

Получение токена с помощью `"authenticate"`

В данном способе получения токена можно использовать методы аутентификации, которые доступны пользователю.

В результате аутентификации будет получен аналогичный токен.

Описание методов API

- [Authenticator](#)
- [License](#)
- [Logon](#)
- [Policy](#)
- [TemplateSession](#)
- [User](#)
- [UserCatalog](#)
- [UserProfile](#)

Authenticator

Информация

Пример функций на PowerShell: [ссылка](#)

getUserAuth

POST /api/v5/authenticator/getUserAuth

 Получение всех обученных аутентификаторов пользователя по внутреннему идентификатору Indeed. Для получения внутреннего идентификатора используется метод **"findByUserIds"**.

Объект запроса

- Id - обязательный параметр. Внутренний идентификатор системы Indeed.
- [UserId](#) - обязательный параметр. Внутренний идентификатор пользователя в системе Indeed.
- AccessToken - обязательный параметр. Токен администратора, от имени которого выполняется запрос к API.
- [ApplicationId](#) - обязательный параметр. Строковый идентификатор модуля Indeed AM.

 {
 "Id": "00000000-0000-0000-0000-000000000000",
 "UserId": "string",
 "AccessToken": "string",
 "ApplicationId": "string"
}

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",
  "ModelId": "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

POST /api/v5/authenticator/findByUserIds

Объект запроса

- [UserId](#) - обязательный параметр. Внутренний идентификатор пользователя в системе Indeed.
- [AccessToken](#) - обязательный параметр. Токен администратора, от имени которого выполняется запрос к API.
- [ApplicationId](#) - обязательный параметр. Строковый идентификатор модуля Indeed AM.

 {
 "UserId": "string",
 "AccessToken": "string",
 "ApplicationId": "string"
}

Объект ответа

 [
 "00000000-0000-0000-0000-000000000000"
]

License

getAllLicenses

POST /api/v5/license/getAllLicenses

 Метод возвращает все зарегистрированные в системе Indeed лицензии.

Объект запроса

- **AccessToken** - обязательный параметр. Токен администратора, от имени которого выполняется запрос к API.
- **ApplicationId** - обязательный параметр. Строковый идентификатор модуля Indeed AM.

 {
 "AccessToken": "string",
 "ApplicationId": "string"
}

Объект ответа

 {
 "LicenseUid": "string",
 "InstancelId": "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

POST /api/v5/license/getCatalogObjectLicenses

 Метод возвращает зарегистрированные лицензии для конкретного объекта каталога.

Объект запроса

- **ObjectId** - Id 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.

 {
 "ObjectId": "string",
 "AccessToken": "string",
 "ApplicationId": "string"
}

Объект ответа

 [
 {
 "ApplicationId": "string",
 "CatalogObjectId": "string",
 "PolicyId": "00000000-0000-0000-0000-000000000000"
 }
]

getAcquiredLicenseCount

POST /api/v5/license/getAcquiredLicenseCount

 Метод возвращает количество зарегистрированных лицензий для указанного приложения.

Объект запроса

- `LicenseType` - тип лицензии, количество которой необходимо получить.
- `AccessToken` - обязательный параметр. Токен администратора, от имени которого выполняется запрос к API.
- `ApplicationId` - обязательный параметр. Строковый идентификатор модуля Indeed AM.

 {
 "LicenseType": "string",
 "AccessToken": "string",
 "ApplicationId": "string"
}

Объект ответа

 {
 "Message": "string",
 "AdditionalMessage": "string",
 "StackTrace": "string",
 "Status": 0
}

Logon

Информация

Пример функций на PowerShell: [ссылка](#)

isAvailable

[POST] /api/v5/logon/isAvailable

 Метод выполняет проверка доступности аутентификации пользователя в приложении.

- В параметре "**ApplicationId**" указывается идентификатор приложения.
- В параметре "**UserId**" указывается Id целевого пользователя.
- В параметре "**ExcludeWindowsPassword**" указывается true/false.
 - Если указано "**true**", значит из проверки исключается возможность аутентификации по доменному паролю. В таком случае у пользователя должен быть доступен любой другой метод аутентификации, иначе запрос вернет "**false**".
 - Если указано "**false**", доменный пароль не исключается из возможных способов аутентификации в сценарии.

Объект запроса

- ApplicationId - Обязательный параметр. Строковый идентификатор модуля Indeed AM.
- UserId - Обязательный параметр. Идентификатор пользователя в системе Indeed AM.
- ExcludeWindowsPassword - Опциональный параметр. Значение по умолчанию "**true**".

```
{
  "ApplicationId": "string",
  "UserId": "string",
  "ExcludeWindowsPassword": true
}
```

Ответ

true>false

authenticate

[POST] /api/v5/logon/authenticate



Метод выполняет аутентификацию пользователя в приложении "**BusinessApplication**" по зарегистрированному шаблону "**TemplateId**".

Подробнее про процесс аутентификации через API описано в разделе "**Сценарии использования**"

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

[POST] /api/v5/logon/getAvailableMethods

 Метод возвращает массив доступных способов аутентификации для пользователя "UserId" в указанном в "ApplicationId" приложении.

Объект запроса

- ApplicationId - Обязательный параметр. Строковый идентификатор модуля Indeed AM.
- UserId - Обязательный параметр. Идентификатор пользователя в системе Indeed AM.
- IncludeModelIds - Опциональный параметр. GUID методов аутентификации Indeed, которые **будут учитываться** при проверке возможности аутентификации.
- ExcludeModelIds - Опциональный параметр. GUID методов аутентификации Indeed, которые **будут исключаться** при проверке возможности аутентификации.

```
{
  "ApplicationId": "string",
  "UserId": "string",
  "IncludeModelIds": [
    "00000000-0000-0000-0000-000000000000"
  ],
  "ExcludeModelIds": [
    "00000000-0000-0000-0000-000000000000"
  ]
}
```

Объект ответа

```
{
  "AutheticationMethods": [
    "00000000-0000-0000-0000-000000000000"
  ]
}
```

Пример ответов

Нет доступных
методов

```
{
  "ValidPropertiesMask": 1,
  "AutheticationMethods": []
}
```

Доступен доменный пароль

```
{
  "ValidPropertiesMask": 1,
  "AutheticationMethods": [
    "cf189af5-01c5-469d-a859-a8f2f41ed153"
  ]
}
```

authenticateByWindowsToken

[POST] /api/v5/logon/authenticateByWindowsToken



Аутентификация пользователя с использованием токена сессии Windows. Токен передается в запрос посредством Windows аутентификации и билетов Kerberos.

Объект запроса

- ApplicationId - Обязательный параметр. Строковый идентификатор модуля Indeed AM.
- BusinessApplication - Опциональный параметр. Имя бизнес приложения Indeed AM.

```
{
  "ApplicationId": "string",
  "BusinessApplication": "string"
}
```

Объект ответа

```
{
  "Token": "string",
  "LogonResult": {
    "Result": "string"
  },
  "UserId": "string"
}
```

Пример успешного объекта ответа

```
{
  "ValidPropertiesMask": 5,
  "Token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJleHAiOi.....",
  "LogonResult": null,
  "UserId": "UserId_10efa04f-7ba9-47d8-89db-56e166f1679f"
}
```

Policy

 Информация

Пример функций на PowerShell: [ссылка](#)

get

POST /api/v5/policy/get

 Получение информации и настроек политик по идентификатору политики.

Объект 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.

 {
 "Id": "00000000-0000-0000-0000-000000000000",
 "AccessToken": "string",
 "ApplicationId": "string"
}

Объект ответа

SettingType:

- 0 - область действия политики.

 Информация

Возвращается внутренний GUID объектов области действия.

- 1 - приложения политики.
- 2 - приоритет политики.

 {
 "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"
 }
],
 "CreatedBy": "string",
 "CreatedTime": "2022-10-26T07:23:08.768Z",
 "LastEditedBy": "string",
 "LastEditedTime": "2022-10-26T07:23:08.768Z"
}

TemplateSession

Информация

Пример функций на PowerShell: [ссылка](#)

createTemplate

[POST] /api/v5/templateSession/createTemplate

Создание шаблона для аутентификации по идентификатору открытой сессии

Объект запроса

- SessionId - Обязательный параметр. Указывается GUID открытой сессии, полученный из метода "openVerifySession".

```
{
  "SessionId": "00000000-0000-0000-0000-000000000000"
}
```

Объект ответа

```
"00000000-0000-0000-0000-000000000000"
```

openEnrollSession

[POST] /api/v5/templateSession/openEnrollSession

В процессе

openVerifySession

[POST] /api/v5/templateSession/openVerifySession

 Открытие сессии для аутентификации пользователя указанного в "**UserSearchParams**" в приложении "**ApplicationId**" с использованием способа аутентификации "**ModelId**"

Объект запроса

- UserSearchParams - Массив параметров для поиска пользователя
 - Id - Внутренний идентификатор пользователя в системе Indeed AM.
 - Email - Email адрес из каталога пользователя.
 - Phone - номер телефона пользователя из каталога пользователя.
 - 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
- ModelId - Обязательный параметр. Строковый идентификатор используемого способа аутентификации.
- ApplicationId - Обязательный параметр. Строковый идентификатор модуля Indeed AM.

```
{
  "UserSearchParams": {
    "Id": "string",
    "Email": "string",
    "Phone": "string",
    "NameFormat": 0,
    "Name": "string",
    "ApplicationId": "string"
  },
  "ModelId": "00000000-0000-0000-0000-000000000000",
  "ApplicationId": "string"
}
```

Объект ответа

 GUID Открытой сессии

"00000000-0000-0000-0000-000000000000"

openIdentifySession

[POST] /api/v5/templateSession/openIdentifySession

 В процессе

prepareTemplateData

[POST] /api/v5/templateSession/prepareTemplateData

 Добавление информации о шаблоне пользователя.

Объект запроса

- Data - Аутентификационные данные пользователя (*OTP или пароль и т.д в зависимости от используемого способа аутентификации*)
- SessionId - Идентификатор открытой сессии, полученный в "**openVerifySession**".

```
{
  "Data": {},
  "SessionId": "00000000-0000-0000-0000-000000000000"
}
```

Объект ответа

- EnoughData - Признак того, что данных от клиента для формирования шаблона достаточно.

```
{
  "EnoughData": true,
  "BinaryData": "string",
  "StringData": "string"
}
```

Пример объекта ответа

```
{  
  "ValidPropertiesMask": 1,  
  "EnoughData": true,  
  "BinaryData": null,  
  "StringData": null  
}
```

User

Информация

Пример функций на PowerShell: [ссылка](#)

searchUserId

POST /api/v5/user/searchUserId

 Получение [UserId](#) по входным параметрам.

Объект запроса

NameFormat:

- 0 - Undefined
- 1 - CanonicalName
- 2 - PrincipalName
- 3 - SamCompatibleName
- 4 - DistinguishedName
- 5 - Sid

 {
 "Id": "string",
 "Email": "string",
 "Phone": "string",
 "NameFormat": 0,
 "Name": "string",
 "ApplicationId": "string"
}

Объект ответа

 "xxxx_00000000-0000-0000-0000-000000000000"

UserCatalog

Информация

Пример функций на PowerShell: [ссылка](#)

getObjects

POST /api/v5/userCatalog/getObjects

 Получение данных объекта каталога пользователя Indeed по внутреннему идентификатору.

Объект 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.

 {
 "Ids": [
 "string"
],
 "AccessToken": "string",
 "ApplicationId": "string"
}

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

POST /api/v5/userCatalog/searchUsers

 Поиск пользователя по входным параметрам.

Объект запроса

- Operation
 - 0 - ИЛИ
 - 1 - И
- Filters - массив фильтров для поиска.
- - AttributeName - имя атрибута AD для поиска.
 - Value - значение атрибута AD для поиска.
 - Negation - отрицание заданного фильтра. Значения true\false.

 {
 "Operation": 0,
 "Filters": [
 {
 "AttributeName": "string",
 "Value": {},
 "Negation": true
 }
],
 "Limit": 0,
 "LoadParentObjects": true,
 "AccessToken": "string",
 "ApplicationId": "string"
}

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

POST /api/v5/userCatalog/searchGroups

 Поиск группы по входным параметрам.

Объект запроса

- Operation
 - 0 - ИЛИ
 - 1 - И

- Filters - массив фильтров для поиска.
- - AttributeName - имя атрибута AD для поиска.
 - Value - значение атрибута AD для поиска.
 - Negation - отрицание заданного фильтра. Значения true\false.

```
 {  
  "Operation": 0,  
  "Filters": [  
    {  
      "AttributeName": "string",  
      "Value": {},  
      "Negation": true  
    }  
  ],  
  "Limit": 0,  
  "LoadParentObjects": true,  
  "AccessToken": "string",  
  "ApplicationId": "string"  
}
```

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

POST /api/v5/userCatalog/searchContainers

 Поиск подразделения по входным параметрам.

Объект запроса

- Operation
 - 0 - ИЛИ
 - 1 - И

- Filters - массив фильтров для поиска.
 - AttributeName - имя атрибута AD для поиска.
 - Value - значение атрибута AD для поиска.
 - Negation - отрицание заданного фильтра. Значения true\false.

```
i {  
  "Operation": 0,  
  "Filters": [  
    {  
      "AttributeName": "string",  
      "Value": {},  
      "Negation": true  
    }  
  ],  
  "Limit": 0,  
  "LoadParentObjects": true,  
  "AccessToken": "string",  
  "ApplicationId": "string"  
}
```

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

Информация

Пример функций на PowerShell: [ссылка](#)

findLogonInfoByUser

POST /api/v5/userProfile/findLogonInfoByUser

Получение информации по аутентификациям пользователя.

Объект запроса

 {
 "UserId": "string",
 "AccessToken": "string",
 "ApplicationId": "string"
}

Объект ответа

- [UserId](#) - Внутренний идентификатор пользователя.
- [ApplicationId](#) - Идентификатор приложения, в которое был выполнен вход.
- `LogonDate` - Дата и время входа.
- [ModelId](#) - Идентификатор способа входа.

 {
 "UserId": "xxxx_000000-0000-0000-0000-000000000000",
 "ApplicationId": "Native Enroller",
 "LogonDate": "2022-05-04T10:54:05.821+03:00",
 "ModelId": "000000-0000-0000-0000-000000000000"
}

Сценарии использования

Информация

В данном разделе описаны сценарии использования API Indeed AM с помощью PowerShell

- [2FA аутентификация в API](#)
- [Получение списка лицензий с их общим количеством и количеством используемых](#)
- [Получение списка пользователей с лицензиями](#)
- [Сбор статистики по обученным аутентификаторам пользователей](#)
- [Создание отчетов](#)

2FA аутентификация в API

Информация

Для выполнения 2Fa аутентификации через API можно воспользоваться скриптом на PS по ссылке: [ссылка](#)

Описание работы скрипта

Информация

Скрипт выполняет аутентификацию через стандартное API сервера Indeed AM. В качестве провайдеров аутентификации поддерживаются провайдеры с OTP, Passcode, Windows Password.

Процесс аутентификации через API:

1. Необходимо вызвать метод: `/api/v5/templateSession/openVerifySession`
 - а. В качестве примера в скрипте используется формат имени "PrincipalName".
2. При успешном выполнении метода вернется идентификатор сессии - переменная "\$SessionId" в скрипте.
3. Следующие шаги отличаются в зависимости от используемого провайдера аутентификации.
 - а. Если OTP известен и его не нужно отправлять, то аутентификация выполняется по следующему алгоритму(функция "**SimpleLogon**" в скрипте):
 - i. Запрос на ввод OTP.
 - ii. Подготовка шаблона аутентификации, вызывается метод: `/api/v5/templateSession/prepareTemplateData`
 1. В качестве "**Data**" передается OTP строкой. Срока 12 в скрипте.
 - iii. Если подготовка прошла успешно, то создается шаблон, вызывается метод: `/api/v5/templateSession/createTemplate`
 - iv. Завершающий шаг - это аутентификация пользователя, метод: `/api/v5/logon/authenticate`
 - v. При успешной аутентификации будет возвращен токен в JSON формате.
 - б. Если OTP не известен, то первоначально нужно инициировать его отправку(функция "**LogonByOtp**" в скрипте).
 - i. Вызывается метод: `/api/v5/templateSession/prepareTemplateData`
 1. Первоначально в качестве "Data" передается Null. Первый вызов необходим для того, чтобы сервер сделал отправку OTP, например, отправку смс.
 2. Также при первоначальном запросе параметр "EnoughData" будет **false**.
 - ii. Запрос на ввод OTP.
 - iii. Подготовка шаблона аутентификации, вызывается метод: `/api/v5/templateSession/prepareTemplateData`
 1. В качестве "**Data**" уже передается OTP строкой. Срока 12 в скрипте.
 2. Запрос вернет объект, где "EnoughData" будет **true**.
 - iv. Если подготовка прошла успешно, то создается шаблон, вызывается метод: `/api/v5/templateSession/createTemplate`
 - v. Завершающий шаг - это аутентификация пользователя, метод: `/api/v5/logon/authenticate`
 - vi. При успешной аутентификации будет возвращен токен в JSON формате.

Предварительные требования

1. Работоспособный сервер Indeed AM.
2. Наличие лицензии "Authentication API".

Настройка

Для работы скрипта необходимо сконфигурировать файл Config.ps1, который находится в корне папки со скриптом.

1. **\$serverUrl** — URL адрес сервера Indeed AM. Обязательный параметр.
2. **\$logsOnFile** — включение\отключение логирования в файл. Обязательный параметр. По умолчанию включено.
3. **\$logsOnConsole** — включение\отключение логирования в консоль. Обязательный параметр. По умолчанию отключено.
4. **\$apiVersion** — версия API, используемая в скрипте. Обязательный параметр. Значение по умолчанию: v5

В основном файле "main.ps1" задайте:

1. **\$ProviderGuid** - GUID провайдера аутентификации, который будет использоваться в скрипте.
 - а. В качестве примера в скрипте используется провайдер: **Indeed AM SMS OTP Provider** — {EBB6F3FA-A400-45F4-853A-D517D89AC2A3}
2. **\$UserName** - Имя пользователя в формате UPN.

Пример работы

```

PS C:\Indeed\PowerShell> .\main.ps1
Type OTP: 1146
@{ValidPropertiesMask=5; Token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJleHAiOiJlNzgyNzgyODg0dG9uMCwidXNlc19pZCI6I1VzZXJJZjF8x
MGVmYTA0ZjM3YmE5LTQ3ZDQgOTdkY01lNmUxNjZmMTY3OWYlLCJwcm92aWRlcii6ImViYjZmM2ZlLWE0MDAtdNDVmc04NTNhLWQ1MTdkODhYzJhMyIsImF1
dGhFZmxhZ3MiOiJnZW51cmF5IiwiaXYXByX2lkiOiQXV0gAGVudG1jYXRpb24gV083JiIiwiaWF0IjpmZTgwOj01NWVlOmMwZDE6Y2ZzInp1YmYlNiJ9
.X3o13HC4CEEB1p2wWnSSTYNgLzyRaG01-PCcYx6wAqW-gV3K3vhvlpTuX-h0PYUn5pDDdi-0yspWsE5Q1qD03vg_SWPgTmU_Lh_div4KKcNi3db8ZEBdy8i
amaauj6wTxc_aMoNi9T1r3meJcY7gtQjgCujoepeSwnZJBm5h88K4jUgfnVjU049muJABfTXxpJ20TtgZ7sZtCnfsEA_mJGDbbyKY0gCX0f8INDsVud7wpq
eQKMNO0YB1z8FI1fx8Q019h_HxITEIeYvJ2ruRMVjLvtYfj0okHNQ6IMWwTq93PoTrZnq-GdyGpJHTYy67aEuMLoDUCQAMAAb98xJFQ; LogonResult=; U
serId=UserId_10efa04f-7ba9-47d8-89db-56e166f1679f}
PS C:\Indeed\PowerShell>

```

Disable checkingPremium suggestions

Получение списка лицензий с их общим количеством и количеством используемых

Информация

Для получения списка лицензий [скачайте](#) репозиторий со скриптом.

Описание работы скрипта

Информация

Скрипт выводит в консоль таблицу со следующей информацией в виде таблицы: тип лицензии, количество.

Лицензии, которые выводятся в консоль - все добавленные лицензии в Indeed AM.

1. Формируется массив загруженных в систему лицензий с помощью метода API `"/license/getAllLic`
2. Из массива лицензий в цикле извлекается:
 - Тип лицензии;
 - Количество используемых лицензий;
 - Общее количество лицензий;
3. Полученные данные формируются в строку json формата и с помощью метода `ConvertFrom-Json` PowerShell.
4. Каждая строка помещается в общий массив.
5. Массив выводится в консоль в виде таблицы.

Предварительные требования

1. Установленный модуль Active Directory для PowerShell в Windows Server.
2. Работоспособный сервер Indeed AM.
3. Пользователь, от имени которого будет запускаться скрипт, должен обладать минимальными правами "Администратор **Инспектор**" в системе Indeed AM.

Настройка

Для работы скрипта необходимо сконфигурировать файл [Config.ps1](#), который находится в корне папки

1. **\$serverUrl** — URL адрес сервера Indeed AM. Обязательный параметр.
2. **\$logsOnFile** — включение\отключение логирования в файл. Обязательный параметр. По умолчанию включено.
3. **\$logsOnConsole** — включение\отключение логирования в консоль. Обязательный параметр. По умолчанию включено.
4. **\$apiVersion** — версия API, используемая в скрипте. Обязательный параметр. Значение по умолчанию 1.0.

Пример работы

1. Для запуска скрипта запустите файл "[main.ps1](#)"
2. После того, как скрипт отработает, в консоль будет выведен результат:

```
PS C:\Users\Admin-Indeed\Documents\VSProjects\Projects> . 'c:\Users\Admin-Indeed\Documents\VSProjects\Projects\mai
```

LicenseType	In use	Amount
IIS Extension	7	100
ADFS Extension	3	100
Identity Provider	3	100
Windows Logon	11	100
Authentication API	0	100
SAML Identity Provider	1	100
NPS RADIUS Extension	2	100
RDP Windows Logon	1	100
Enterprise SSO	11	100

Получение списка пользователей с лицензиями

Информация

Для получения списка пользователей [скачайте](#) репозиторий со скриптом.

Описание работы скрипта

Информация

Скрипт формирует CSV таблицу формата: <UserName>; <true>; <false>. Где true/false - это столбцы с соответствующим названием лицензии.

Массив лицензий, наличие которых проверяется у пользователя - это список всех зарегистрированных лицензий.

1. Формируется массив загруженных в систему лицензий с помощью метода API `"/license/getAllLicenses"`.
2. С помощью метода API `"/api/v5/policy/get"` запрашивается информация о политике.
3. Из свойства области действия запрашивается информация по настроенным объектам с помощью метода API `"/api/v5/userCatalog/getObjects"`.
4. Из полученных объектов запрашиваются пользователи
 - а. С помощью командлета Powershell `"Get-ADGroup"` в функции `"getUsersCN"` файла ["Base/AdditionalFunctions/GetUsers.ps1"](#) для группы AD.
 - б. С помощью командлета Powershell `"Get-ADUser"` в функции `"getUsersOU"` файла ["Base/AdditionalFunctions/GetUsers.ps1"](#) для подразделения AD.
5. С помощью метода API `"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 CSV формате.

Предварительные требования

1. Установленный модуль Active Directory для PowerShell в Windows Server.
2. Работоспособный сервер Indeed AM.
3. Пользователь, от имени которого будет запускаться скрипт, должен обладать минимальными глобальными правами **"Инспектор"** в системе Indeed AM.

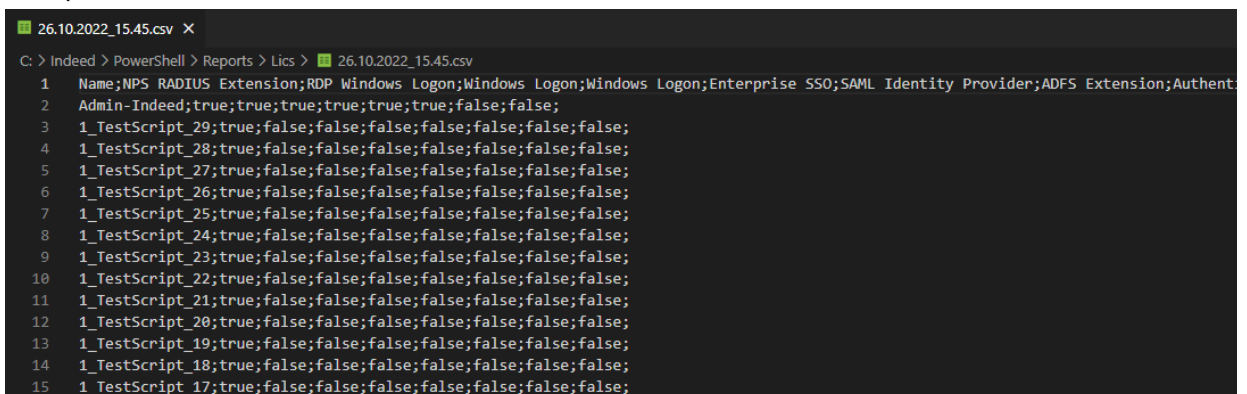
Настройка

Для работы скрипта необходимо сконфигурировать файл [Config.ps1](#), который находится в корне папки со скриптом.

1. **\$serverUrl** — URL адрес сервера Indeed AM. Обязательный параметр.
2. **\$logsOnFile** — включение\отключение логирования в файл. Обязательный параметр. По умолчанию включено.
3. **\$logsOnConsole** — включение\отключение логирования в консоль. Обязательный параметр. По умолчанию отключено.
4. **\$apiVersion** — версия API, используемая в скрипте. Обязательный параметр. Значение по умолчанию: v5
5. **\$policyIds** — [идентификаторы политик](#), с области действия которых запрашиваются пользователи.
6. **\$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 csv файл.



```
26.10.2022_15.45.csv X
C: > Indeed > PowerShell > Reports > Lics > 26.10.2022_15.45.csv
1 Name;NPS_RADIUS_Extension;RDP_Windows_Logon;Windows_Logon;Windows_Logon;Enterprise_SSO;SAML_Identity_Provider;ADFS_Extension;Authent
2 Admin-Indeed;true;true;true;true;true;true;false;false;
3 1_TestScript_29;true;false;false;false;false;false;false;false;
4 1_TestScript_28;true;false;false;false;false;false;false;false;
5 1_TestScript_27;true;false;false;false;false;false;false;false;
6 1_TestScript_26;true;false;false;false;false;false;false;false;
7 1_TestScript_25;true;false;false;false;false;false;false;false;
8 1_TestScript_24;true;false;false;false;false;false;false;false;
9 1_TestScript_23;true;false;false;false;false;false;false;false;
10 1_TestScript_22;true;false;false;false;false;false;false;false;
11 1_TestScript_21;true;false;false;false;false;false;false;false;
12 1_TestScript_20;true;false;false;false;false;false;false;false;
13 1_TestScript_19;true;false;false;false;false;false;false;false;
14 1_TestScript_18;true;false;false;false;false;false;false;false;
15 1_TestScript_17;true;false;false;false;false;false;false;false;
```

Сбор статистики по обученным аутентификаторам пользователей

Информация

Для сбора статистики [скачайте](#) репозиторий со скриптом.

Описание работы скрипта

1. Скрипт перебирает идентификаторы политик из массива конфигурационного файла [Config.ps1](#).
2. С помощью метода API `/api/v5/policy/get` запрашивается информация о политике.
3. Из свойства области действия запрашивается информация по настроенным объектам с помощью метода API `/api/v5/userCatalog/getObjects`.
4. Из полученных объектов запрашиваются пользователи
 - а. С помощью командлета PowerShell `Get-ADGroup` в функции `getUsersCN` файла [Base/AdditionalFunctions/GetUsers.ps1](#) для группы AD.
 - б. С помощью командлета PowerShell `Get-ADUser` в функции `getUsersOU` файла [Base/AdditionalFunctions/GetUsers.ps1](#) для подразделения AD.
5. По полученным пользователям составляется отчет по состоянию аутентификаторов, которые указаны в переменной `"AuthForReport"` файла [Config.ps1](#).
 - а. С помощью метода API `/api/v5/authenticator/findByUserIds` запрашивается информация со всеми внутренними GUID аутентификаторов пользователя.
 - б. С помощью метода API `/api/v5/authenticator/getUserAuth` запрашивается информация по-конкретному GUID из 5.а.
6. С помощью функции `"addDataToCSV"` файла [Base/AdditionalFunctions/CsvReport.ps1](#) собирается таблица в CSV формате.

Предварительные требования

1. Установленный модуль Active Directory для PowerShell в Windows Server.
2. Работоспособный сервер Indeed AM.
3. Пользователь, от имени которого будет запускаться скрипт, должен обладать минимальными глобальными правами **"Инспектор"** в системе Indeed AM.

Настройка

Для работы скрипта необходимо сконфигурировать файл [Config.ps1](#), который находится в корне папки со скриптом.

1. **\$serverUrl** — URL адрес сервера Indeed AM. Обязательный параметр.
2. **\$logsOnFile** — включение\отключение логирования в файл. Обязательный параметр. По умолчанию включено.
3. **\$logsOnConsole** — включение\отключение логирования в консоль. Обязательный параметр. По умолчанию отключено.
4. **\$apiVersion** — версия API, используемая в скрипте. Обязательный параметр. Значение по умолчанию: v5
5. **\$policyIds** — идентификаторы политик, с области действия которых запрашиваются пользователи.
6. **\$AuthForReport** - в переменной указываются GUID аутентификаторов Indeed и их название для репорта. Название может быть произвольным. Значения указываются в следующем формате 'GUID' = "Наименование".

Пример настройки для Indeed Key и Passcode

```
$AuthForReport = @{  
    'F696F05D-5466-42b4-BF52-21BEE1CB9529' = 'Паскод'  
    'DEEF0CB8-AD2F-4B89-964A-B6C7ECA80C68' = 'Пуш'  
}
```

7. **\$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 csv файл.

 Информация

Пользователи добавляются в отчёт последовательно.

```
26.10.2022_9.39.csv X
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
```

Создание отчетов

Информация

Чтобы начать создавать отчеты, [скачайте](#) репозиторий со скриптом.

Предварительные требования

1. Установленный модуль Active Directory для PowerShell в Windows Server.
2. Работоспособный сервер Indeed AM.
3. Пользователь, от имени которого будет запускаться скрипт, должен обладать минимальными глобальными правами **"Инспектор"** в системе Indeed AM.

Описание работы скрипта

Скрипт формирует отчёты по подготовленным сценариям. Для создания отчетов используется API Indeed AM Core и Indeed AM LS. Скрипт поддерживает настройку фильтрации для формирования отчета:

- Выборка из контейнера пользовательского каталога.
- Выборка по конкретному пользователю.
- Выборка по дате.

Описание фильтров

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 API **"searchContainers"** в соответствующей функции в файле [Base/AMAPI/UserCatalog.ps1](#).

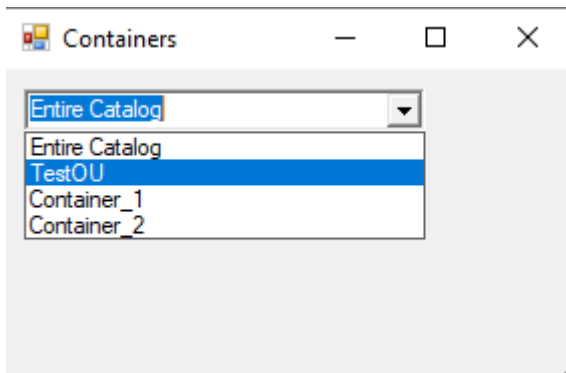
Информация

Выгрузка контейнеров выполняется из пользовательского каталога. Значение в поле не редактируемое.

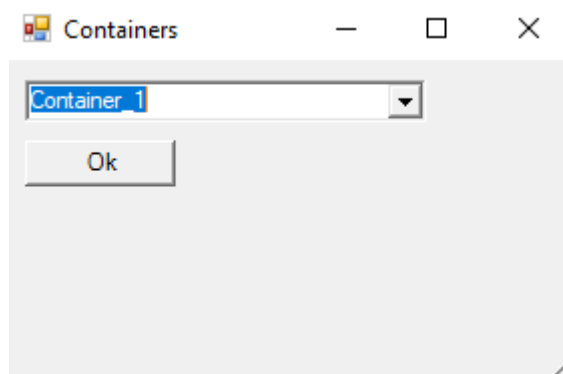
Имя корневых каталогов пользователей, заданных в конфигурационном файле core, не отображается.

Для выбора необходимого подразделения из каталога выполните следующие действия:

1. Нажмите кнопку **"Select"**.



2. В выпадающем списке окна **"Containers"** выберите требуемый контейнер.



3. Нажмите **"Ok"**.

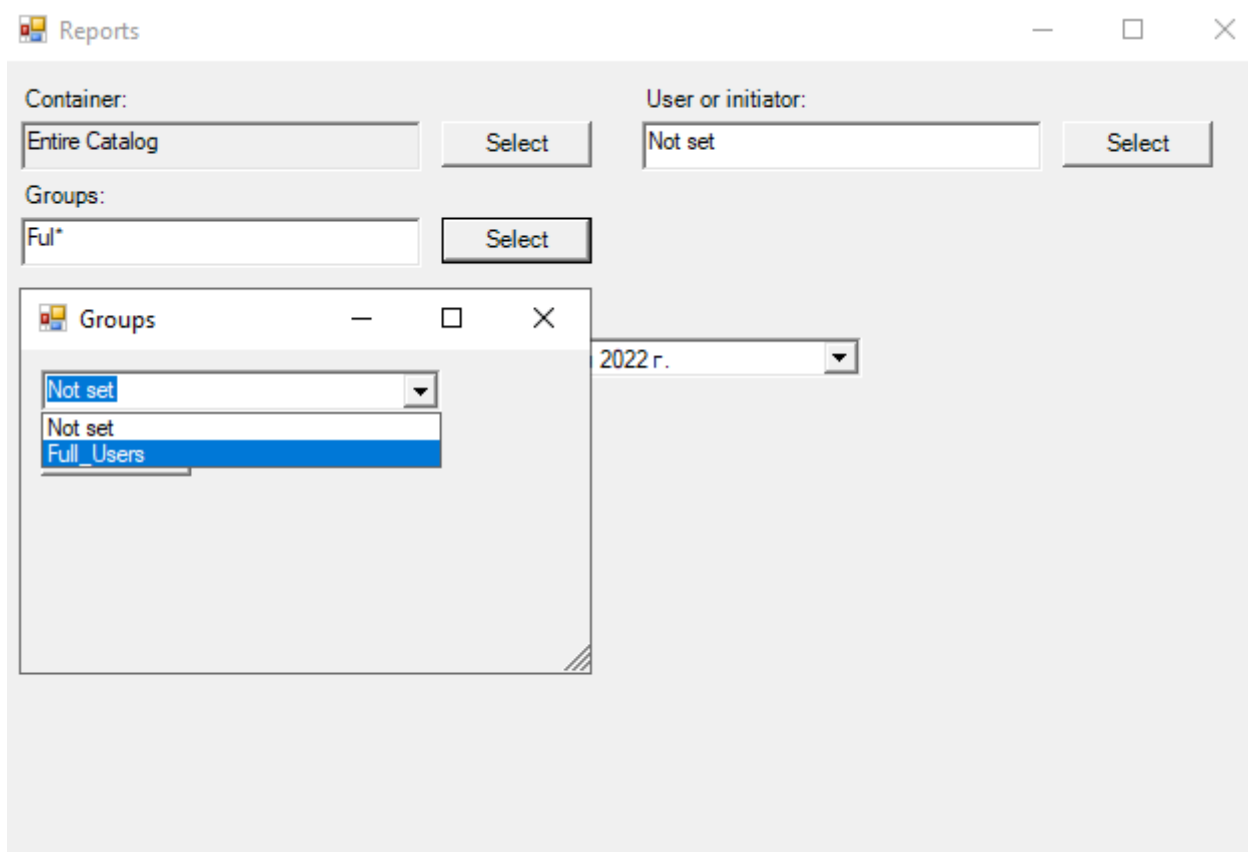
Поле "Groups"

Поле предназначено для поиска групп в домене или в выбранном в поле **"Container"** подразделении. Значение по умолчанию **"Not set"**.

Поиск пользователя выполняется с использованием метода API **"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 AD **"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 выбранном в поле "**Container**" подразделении или группе из поля "**Groups**". Значение по умолчанию "**Not set**".

Поиск пользователя выполняется с использованием метода API "**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](#).

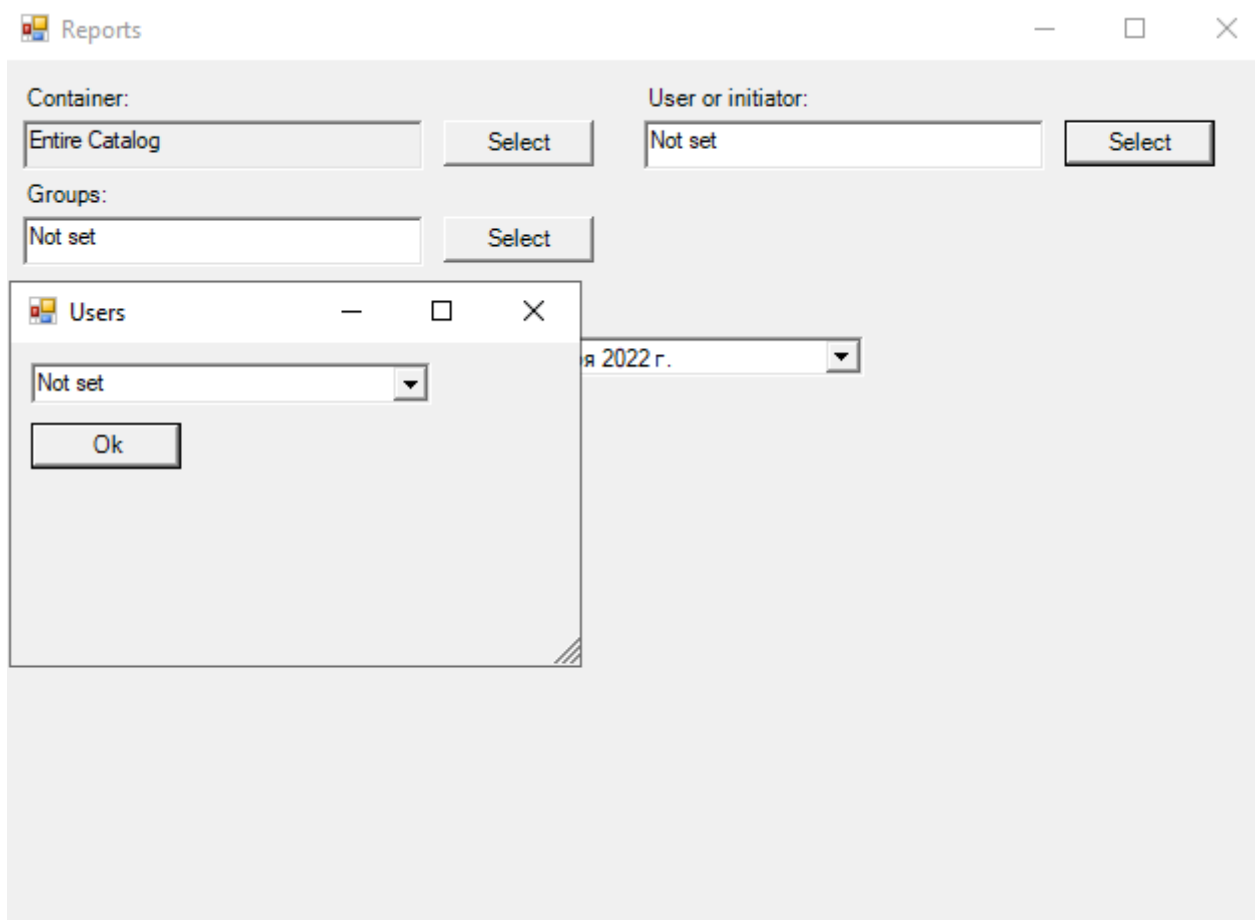
В поиске учитываются следующие параметры:

Информация

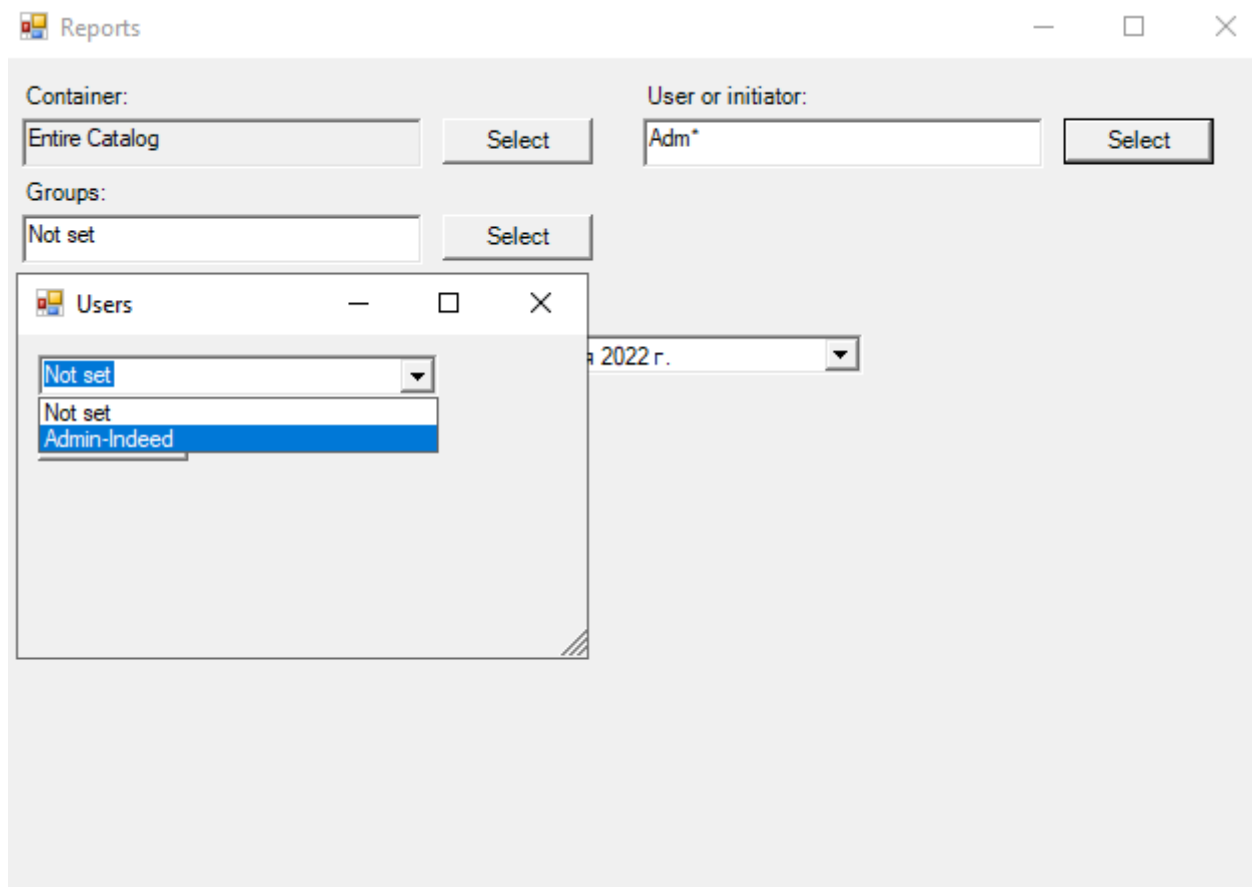
Все параметры используются с логической операцией "or".

- **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 AD.

Для поиска пользователей можно нажать кнопку **"Select"** и выбрать всех найденных пользователей.



Для поиска пользователя можно указать часть имени, в конце указанной части необходимо добавить символ *.



Общая настройка

Для работы скрипта необходимо сконфигурировать файл **Config.ps1**, который находится в корне папки со скриптом.



Информация

В данном разделе описана общая настройка скрипта. Для отдельных отчетов может потребоваться дополнительная настройка.

1. **\$domainName** — указывается имя домена. Обязательный параметр.
2. **\$eventsCount** — ограничение по выгрузке событий. Опциональный параметр. По умолчанию количество получаемых событий не ограничено, параметр закомментирован.
3. **\$serverUrl** — URL адрес сервера Indeed AM. Обязательный параметр.
4. **\$logServerUrl** — URL адрес Indeed AM Log Server. Обязательный параметр.
5. **\$logsOnFile** — включение\отключение логирования в файл. Обязательный параметр. По умолчанию включено.
6. **\$logsOnConsole** — включение\отключение логирования в консоль. Обязательный параметр. По умолчанию отключено.
7. **\$apiVersion** — версия API, используемая в скрипте. Обязательный параметр.

Создание отчетов

- [Создание отчета "Количество аутентификаций по указанным провайдерам"](#)

Создание отчета "Количество аутентификаций по указанным провайдерам"

В данном отчете формируется таблица с количеством аутентификаций пользователя по указанному в файле "Config.ps1" массиву аутентификаторов в конкретном приложении Indeed.

Создание отчета выполняется в функции "createLogonsByProviderReport" в файле [Create-reports/Scenarios/Reports/CreateReports.ps1](#).

Настройка



Информация

В разделе описаны настройки для конкретного отчета. Перед началом работы необходимо выполнить базовую настройку, описанную в разделе [Создание отчетов](#).

Откройте файл Config.ps1 и задайте следующие значения:

1. В переменной "**AuthForReport**" задайте id провайдера Indeed и наименование для отчета.
 - a. Значения должны задаваться в формате: "*GUID провайдера Indeed*" = "*Наименование для отчёта*".
 - b. Значения GUID провайдеров можно найти в разделе [Идентификаторы способов аутентификации](#).
 - c. 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' = 'Палец'  
}
```

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. Вы можете выгружать отчет в двух форматах одновременно. Если обе переменные не определены, это приведет к ошибке выгрузки.

Для включения выгрузки отчета в CSV задайте переменной **CsvReport** значение *true*.

```
$CsvReport = 'true'
```

Для включения выгрузки отчета 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 PS, перейдите в папку со скриптом и запустите файл "Start.ps1": **.\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 html-таблица 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				

Консоль администратора

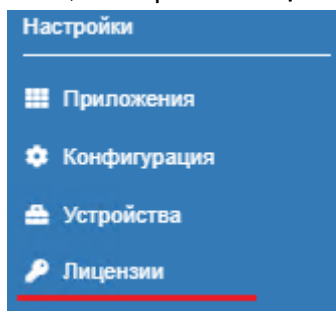
- [Получение и регистрация лицензий](#)
- [Создание и настройка политик](#)
- [Добавление и настройка приложений](#)
- [Кеширование данных пользователя](#)
- [Управление аутентификаторами](#)
- [Поиск пользователей](#)
- [Карточка пользователя](#)
- [Журнал событий](#)
- [Конфигурация](#)

Получение и регистрация лицензий

Получение лицензий

Для получения лицензий необходимо сообщить идентификатор системы.

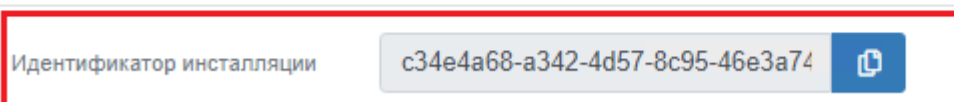
1. Откройте Management Console.
2. В левом меню, в блоке "Настройки", выберите "Лицензии".



3. Скопируйте значение из поля "Идентификатор инсталляции" и отправьте закрепленному за вашей организацией менеджеру или в службу технической поддержки support@indeed-id.com

Лицензии

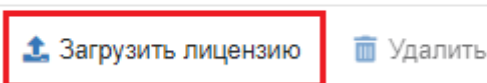
 Загрузить лицензию  Удалить



Регистрация лицензий.

1. Откройте Management Console.
2. В левом меню, в блоке "Настройки", выберите "Лицензии".
3. Нажмите кнопку "Загрузить лицензию".

Лицензии



4. Нажмите "**Выбрать файл**".

Зарегистрировать лицензии >

Файл лицензий

Выбрать файл

Отмена

Зарегистрировать

5. Выберите файл с лицензией и нажмите "**Зарегистрировать**".

Зарегистрировать лицензии >

Файл лицензий

ADFS Extension.lic

Выбрать файл

Отмена

Зарегистрировать

И Информация

После успешной регистрации лицензий, все лицензии отобразятся в таблице.

Таблица состоит из следующих столбцов:

- a. Тип лицензии** - Имя компонента для которого будет применена лицензия.
- b. Количество** - Количество полученных лицензий.
- c. Используется** - Количество используемых в данный момент лицензий.
- d. Дата начала** - Дата начала действия лицензий.
- e. Дата окончания** - Дата окончания срока действий лицензий.
- f. Дата выпуска** - Дата выпуска лицензии.

Лицензии

 Загрузить лицензию  Удалить

Идентификатор инсталляции

c34e4a68-a342-4d57-8c95-46e3a74a0ea4



ТИП ЛИЦЕНЗИИ	КОЛИЧЕСТВО	ИСПОЛЬЗУЕТСЯ	ДАТА НАЧАЛА	ДАТА ОКОНЧАНИЯ	ДАТА ВЫПУСКА
Enterprise SSO	10	0			
☐ Enterprise SSO	10		27.08.2020	-	27.08.2020
Windows Logon	10	1			
☐ Windows Logon	10		27.08.2020	-	27.08.2020
IIS Extension	10	1			
☐ IIS Extension	10		28.08.2020	-	28.08.2020
RDP Windows Logon	10	1			
☐ RDP Windows Logon	10		28.08.2020	-	28.08.2020

Выдача и отзыв лицензий

В системе Indeed AM выдача лицензий пользователю осуществляется автоматически для всех пользователей, которые входят в целевую политику Indeed. Лицензия будет закреплена за пользователем после успешной аутентификации в соответствующем модуле.

Освобождение лицензий осуществляется с использованием механизма автоматического отзыва лицензий. Лицензия будет отозвана для пользователя:

- Если пользователь будет удален из политики.
- Если пользователь был отключен или перемещен из области действия политики.
- Если пользователь был заблокирован\удален из Active Directory.

Информация

Механизм автоматического освобождения лицензия по умолчанию включен и срабатывает каждые сутки(86400 секунд).

По результатам работы события фиксируется итоговое событие - 1094. В событии отображается общее количество лицензий, которые были отозваны.

Время удаления лицензии можно изменить в конфигурационном файле сервера(C:\inetpub\wwwroot\am\core\Web.config), значения указываются в секундах, минимальное значение: 60. Если параметр не указан, то применяется стандартное значение - 86400 секунд.

```
/* Задаётся минимальное значение параметра - 1 минута */  
<cleanLicense intervalSec="60" />
```

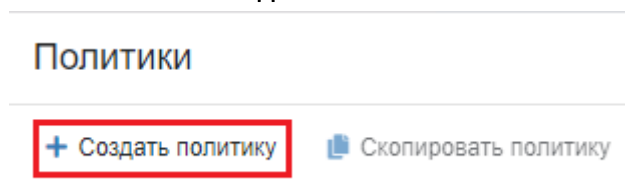
```
/* Параметр не указан, применяется стандартное значение*/  
<cleanLicense/>
```

```
/* Пользовательское значение параметра - 3 минуты */  
<cleanLicense intervalSec="180"/>
```

Создание и настройка политик

Создание политики

1. Откройте Management Console.
2. В левом меню выберите "Политики".
3. На странице "Политики" нажмите "Создать".



4. Укажите приоритет политики, имя, описание(Опциональный параметр) и нажмите "Создать".

Создать политику ×

Приоритет*

Имя*

Описание

Отмена Создать

Настройка политики

1. Откройте Management Console.
2. В левом меню выберите "Политики".
3. Выберите необходимую политику.

Информация

В данном разделе указывается основная информация о политике, информация о создании политики и редактировании. Для редактирования информации необходимо нажать "Редактировать", для удаления политики - "Удалить".

Общая политика - Информация

Информация	✎ Редактировать	🗑 Удалить
Приложения	Имя Общая политика	
Область действия	Описание Общая политика для всех пользователей системы Indeed AM	
Администраторы	Приоритет 999	
Аутентификаторы	Количество приложений в политике 0	
Политику создал Admin-Indeed		Дата создания 2020.08.31 11:03
Последний, кто изменял политику Admin-Indeed		Дата последнего изменения 2020.08.31 11:03

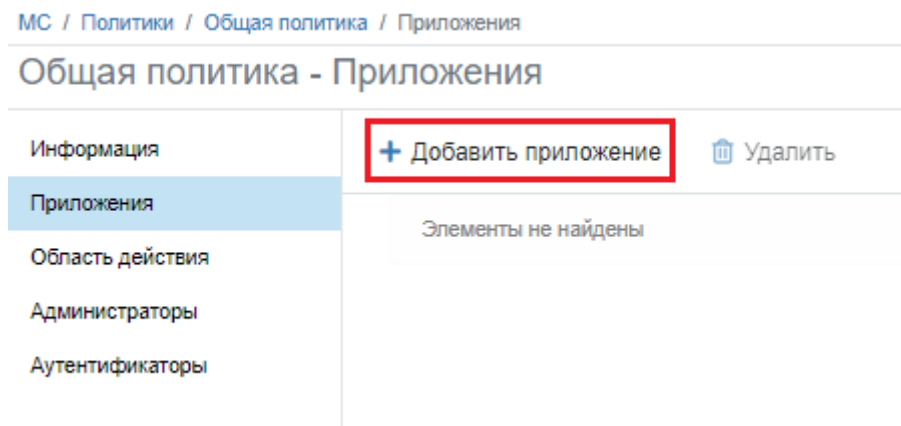
Приложения

В данном разделе отображаются приложения политики. Для добавления приложения выполните следующие действия:

** Информация**

Под приложениями системы Indeed AM подразумеваются приложения компонента Indeed AM ESSO Agent, а также модули интеграции Indeed AM(Indeed Am Windows Logon, Indeed AM NPS Radius, RDP Windows Logon и др.)

1. Нажмите **"Добавить приложение"**.



2. В окне **"Добавить приложение"** выберите необходимое приложение и нажмите **"Добавить"**.

 **Информация**

Добавить приложение можно только при наличии зарегистрированной лицензии для данного модуля.

Добавить приложение

×

Приложение*

Модуль интеграции NPS RADIUS

▼

Отмена

Добавить

- а. Чтобы удалить приложение, выберите необходимое приложение и нажмите **"Удалить"**.

Область действия

В данном разделе отображаются объекты, на которые распространяется действие политики. Для добавления выполните следующие действия:

1. Нажмите **"Добавить"**.

Общая политика - Область действия

Информация	+ Добавить  Удалить
Приложения	
Область действия	Элементы не найдены
Администраторы	
Аутентификаторы	

2. В поле **"Тип объекта"** выберите тип: Пользователь, Группа, Контейнер.
3. В поле **"Расположение"** выберите расположение объекта - это может быть весь пользовательский каталог или отдельный контейнер.
4. В поле **"Название"** укажите полное или часть имени объекта и нажмите **"Поиск"**.

[МС](#) / [Политики](#) / [Общая политика](#) / [Область действия](#)

Общая политика - Область действия

Информация	+ Добавить ✕ Отмена
Приложения	
Область действия	
Администраторы	
Аутентификаторы	

Название	Тип объекта	
Admins	Пользователь <input checked="" type="button" value="Группа"/> Подразделение	
Расположение		
Весь каталог Выбрать		
Поиск Сбросить		
НАЗВАНИЕ	ТИП ОБЪЕКТА	РАСПОЛОЖЕНИЕ
☐  AdminsIndeed	Группа	indeed.local/Indeed/UsersIndeed/Admi

5. Выберите найденный объект и нажмите **"Добавить"**.
6. После успешного добавления объект будет отображаться в разделе.

[МС](#) / [Политики](#) / [Общая политика](#) / [Область действия](#)

Общая политика - Область действия

Информация	+ Добавить  Удалить
Приложения	
Область действия	
Администраторы	
Аутентификаторы	

НАЗВАНИЕ ▾	ТИП ОБЪЕКТА	РАСПОЛОЖЕНИЕ
☐  AdminsIndeed	Группа	indeed.local/Indeed/UsersIndeed/A

Администраторы

В данном разделе отображаются администраторы приложения. Для добавления администратора выполните следующие действия:

1. Нажмите "**Добавить**" и выберите роль: Администратор, Оператор, Инспектор.
2. В поле "**Тип объекта**" выберите тип: Пользователь, Группа.
3. В поле "**Расположение**" выберите расположение объекта - это может быть весь пользовательский каталог или отдельный контейнер.
4. В поле "**Название**" укажите полное или часть имени объекта и нажмите "**Поиск**".

[МС](#) / [Политики](#) / [Общая политика](#) / [Администраторы](#)

Общая политика - Администраторы

Информация
Приложения
Область действия
Администраторы
Аутентификаторы

+ Добавить
× Отмена

Название

Vlad

Тип объекта

Пользователь

Группа

Расположение

Весь каталог

Выбрать

Поиск

Сбросить

НАЗВАНИЕ	ТИП ОБЪЕКТА	РАСПОЛОЖЕНИЕ
☐ INDEED/vladislav.fomichev	Пользователь	indeed.local/Indeed/UsersIndeed/Novgorod/Владислав Фомичёв

5. Выберите найденный объект и нажмите "**Добавить**".
6. После успешного добавления объект будет отображаться в разделе.

[МС](#) / [Политики](#) / [Общая политика](#) / [Администраторы](#)

Общая политика - Администраторы

Информация
Приложения
Область действия
Администраторы
Аутентификаторы

+ Добавить
Удалить

ИМЯ
ГРУППА БЕЗОПАСНОСТИ

Администратор

☐ Владислав Фомичёв
Администратор

Оператор

Элементы не найдены

Инспектор

Элементы не найдены

Аутентификаторы

В данном разделе отображается информация по доступным аутентификаторам и дополнительные настройки.

Общая политика - Аутентификаторы

Информация
Приложения
Область действия
Администраторы
Аутентификаторы

Сохранить
Отмена
Разрешить использовать
Запретить использовать
Максимальное количество

ТИП АУТЕНТИФИКАТОРА	УСТРОЙСТВО	СТАТУС	МАКСИМАЛЬНОЕ КОЛИЧЕСТВО
☐ Multi-factor authentication	MFA	Разрешен	
☐ Push-аутентификация	Indeed AirKey	Разрешен	1
☐ Одноразовый пароль по SMS	SMS	Разрешен	
☐ Пароль Passcode	Passcode	Разрешен	1
☐ Пароль Windows	Windows Password	Разрешен	
☐ Программный генератор TOTP	Software TOTP token	Разрешен	1

Доступные пользователю действия

Регистрация новых аутентификаторов

Разрешить Запретить

Редактирование имеющихся аутентификаторов

Разрешить Запретить

Удаление имеющихся аутентификаторов

Разрешить Запретить

Разрешить редактирование комментария к аутентификатору

Всегда
При регистрации аутентификатора
Запретить

Блокировка аутентификатора

Чтобы запретить использовать аутентификатор для всех пользователей политики выполните следующие действия:

1. Выберите необходимый аутентификатор и нажмите **"Запретить использовать"**.

Сохранить
Отмена
Разрешить использовать
Запретить использовать
Максимальное кс

ТИП АУТЕНТИФИКАТОРА	УСТРОЙСТВО	СТАТУС	МАКСИМАЛЬНОЕ КОЛИЧЕСТВО
☐ Multi-factor authentication	MFA	Разрешен	
☒ Push-аутентификация	Indeed AirKey	Разрешен	1

2. После выполнения действия статус аутентификатора будет **"Запрещён"**.

Изменение максимального количества аутентификаторов

Чтобы изменить максимальное количество аутентификаторов, которое пользователь может зарегистрировать для себя, необходимо выполнить следующие действия:

1. Выберите необходимый аутентификатор и нажмите "**Максимальное количество**".

Сохранить Отмена Разрешить использовать Запретить использовать # Максимальное количество			
ТИП АУТЕНТИФИКАТОРА	УСТРОЙСТВО	СТАТУС	МАКСИМАЛЬНОЕ КОЛИЧЕСТВО
☐ Multi-factor authentication	MFA	Разрешен	
☐ Push-аутентификация	Indeed AirKey	Запрещен	1
☐ Одноразовый пароль по SMS	SMS	Разрешен	
☒ Пароль Passcode	Passcode	Разрешен	1

2. В окне "**Максимальное количество**" укажите требуемое значение и нажмите "**Сохранить**".

Максимальное количество

Максимальное количество*

3

Отмена Сохранить

3. После успешного выполнения действия число максимального количество для аутентификатора будет изменено.

Доступные пользователю действия

1. **Регистрация новых аутентификаторов** - Данный параметр определяет, может ли пользователь самостоятельно обучать себе аутентификаторы. Значение по умолчанию: **Разрешить**
2. **Редактирование имеющихся аутентификаторов** - Данный параметр определяет, может ли пользователь самостоятельно редактировать имеющиеся аутентификаторы. Значение по умолчанию: **Запретить**
3. **Удаление имеющихся аутентификаторов** - Данный параметр определяет, может ли пользователь самостоятельно удалять имеющиеся аутентификаторы. Значение по умолчанию: **Запретить**
4. **Разрешить редактирование комментария к аутентификатору** - Данный параметр определяет, может ли пользователь самостоятельно редактировать комментарии к имеющимся аутентификаторам. Значение по умолчанию: **Всегда**

Доступные пользователю действия

Регистрация новых аутентификаторов

Разрешить

Запретить

Редактирование имеющихся аутентификаторов

Разрешить

Запретить

Удаление имеющихся аутентификаторов

Разрешить

Запретить

Разрешить редактирование комментария к аутентификатору

Всегда

При регистрации аутентификатора

Запретить

Добавление и настройка приложений

На данной странице осуществляется добавление приложений компонента ESSO Agent в систему Indeed AM.

Информация

Для добавления приложений ESSO необходима регистрация лицензии Enterprise SSO.

Остальные компоненты системы не требуют отдельного добавления, они автоматически добавляются в систему после регистрации лицензии.

Загрузка шаблона

1. Откройте Management Console.
2. В левом меню, в блоке "**Настройки**", выберите "**Приложения**".
3. Нажмите "**Добавить приложение**".

Приложения

 **Добавить приложение**  **Удалить**

4. В окне "**Добавить приложение**" выберите модуль интеграции "**Enterprise SSO**", выберите файл шаблона для приложения и нажмите "**Создать**".

Добавить приложение

Модуль интеграции*

Enterprise SSO 

Файл шаблона ESSO*

Keepersecurity.xml

Выбрать файл

Отмена

Создать

Настройка приложения

После успешной загрузки шаблона откроется страница с настройками приложения.

Общая информация

В данном разделе отображается информация о приложении из загруженного шаблона.

1. Если требуется изменить название или описание нажмите "**Редактировать**" и укажите требуемые данные и нажмите "**Сохранить**".

Редактирование

Название*

Keepersecurity

Описание

Шаблон приложения Keepersecurity v 2.0

Отмена Сохранить

2. При необходимости можно загрузить логотип для приложения.
 - а. В блоке "**Логотип**" нажмите "**Загрузить**".

Информация

Поддерживаются изображения формата JPG и PNG, максимальный размер - 512KB.

 Редактировать

 Удалить приложение

Название
Keepersecurity

Описание
Шаблон приложения Keepersecurity v 2.0

Модуль интеграции
Enterprise SSO

Логотип

Загрузить

Требования к изображению:
512KB
JPG или PNG формат

в. Выберите необходимый файл и нажмите "Загрузить".

Логотип

✕

Файл логотипа

keep.png

Выбрать файл

Отмена

Загрузить

Keepersecurity - Общая информация

Общая информация	Редактировать Удалить приложение
ЕССО шаблон	
Администраторы	
Ярлыки	
Парольная политика	
Клиентские модули	
	Название Keepersecurity Описание Шаблон приложения Keepersecurity v 2.0 Модуль интеграции Enterprise SSO Логотип Требования к изображению: 512КБ JPG или PNG формат Загрузить Параметры по умолчанию Аутентификация при входе в приложение Запрашивать каждый раз Входить прозрачно

ЕССО шаблон

В данном разделе можно загрузить новый шаблон приложения или выгрузить использующийся в данный момент шаблон.

Keepersecurity - ЕССО шаблон

Общая информация	Загрузить шаблон Выгрузить шаблон
ЕССО шаблон	
Администраторы	
Ярлыки	
Парольная политика	
Клиентские модули	
	Имя файла шаблона Keepersecurity.app

Администраторы

В данном разделе можно добавить администраторов для данного приложения.

1. Нажмите **"Добавить"**.
2. Выберите тип объекта - Пользователь или Группа.
3. Укажите расположение - Весь пользовательский каталог или отдельный контейнер.
4. В поле **"Название"** введите имя или часть имени для поиска.
5. Нажмите **"Поиск"**.
6. Выберите необходимого пользователя и нажмите **"Добавить"**.

[+ Добавить](#) [✕ Отмена](#)

Название

vlad

Тип объекта

[Пользователь](#) [Группа](#)

Расположение

[Novgorod](#) [Выбрать](#)

[Поиск](#) [Сбросить](#)

НАЗВАНИЕ ▾	ТИП ОБЪЕКТА	РАСПОЛОЖЕНИЕ
☒  INDEED\vladislav.fomichev	Пользователь	indeed.local/Indeed/Users/Indeed/Novgorod/Владисла

Keepersecurity - Администраторы

Общая информация

ESSO шаблон

Администраторы

Ярлыки

Парольная политика

Клиентские модули

[+ Добавить](#) [🗑 Удалить](#)

НАЗВАНИЕ ▾	ТИП ОБЪЕКТА
☐  Владислав Фомичёв	Пользователь

Ярлыки

В данном разделе указывается информация для быстрого запуска приложения.



Информация

Если при создании шаблона была указана данная информация, то она будет отображаться в данном разделе.

1. Нажмите "**Добавить ярлык**".
2. В поле "**Описание**" укажите дополнительную информацию для создаваемого ярлыка.
3. В поле "**Тип**" выберите "**Командная строка**".
4. В поле "**Адрес**" укажите полную команду для запуска приложения и нажмите "**Добавить**".



Информация

На скриншоте представлена информация для Web-приложения.

Добавить ярлык



Описание*

Запуск Web приложения через IE

Тип*

Командная строка



Адрес*

"%ProgramFiles%\Internet Explorer\iexplore.exe" "https://keepersecurity.com/vault/"

Отмена

Добавить

Keepersecurity - Ярлыки

Общая информация

ESSO шаблон

Администраторы

Ярлыки

Парольная политика

Клиентские модули

+ Добавить ярлык

Удалить

ОПИСАНИЕ

ТИП

АДРЕС



Запуск Web приложения
через IE

Командная строка

"%ProgramFiles%\Internet Explorer\iexplore.exe" "https://keepersecurity.com/vault/"

Парольная политика

В данном разделе указывается политика для генерации пароля при его смене в приложении.

1. В поле "**Минимальная длина пароля**" указывается минимальное количество символов пароля.

2. В поле "**Максимальное количество вхождений каждого символа**" указывается количество вхождений символов из группы символов. Для работы параметра необходимо создать группу символов.



Информация

При добавлении пользовательской группы требуется указать свою группу символов в поле "**Символы группы**".

а. Нажмите **"Добавить группу"**.

[+ Добавить группу](#) [Удалить](#) [Сохранить](#) [Отменить](#)

Минимальная длина пароля*

8

Максимальное количество вхождений каждого символа*

0

Элементы не найдены

б. В поле **"Тип группы"** выберите предлагаемые типы символов или пользовательский.

с. В поле **"Число символов"** укажите количество символов и нажмите **"Добавить"**.

Добавить группу ×

Тип группы*

Все символы ▼

Число символов*

3

Отмена [Добавить](#)

Keepersecurity - Парольная политика

Общая информация

ESSO шаблон

Администраторы

Ярлыки

Парольная политика

Клиентские модули

[+ Добавить группу](#) [Удалить](#) [Сохранить](#) [Отменить](#)

Минимальная длина пароля*

8

Максимальное количество вхождений каждого символа*

3

ТИП ГРУППЫ	ЧИСЛО СИМВОЛОВ	СИМВОЛЫ ГРУППЫ
☐ Все символы	3	A..Z, a..z, 0..9, .,<>/?[]+=+_-\\!@#5%^^&*()

Клиентские модули

В разделе "**Клиентские модули**" указывается целевой URL приложения или путь к исполняемому файлу. Значение данного параметра берется из шаблона и при необходимости может быть изменено. Для изменения необходимо выполнить следующее:

 Информация

В качестве значения может быть использовано регулярное выражение.

1. Выберите необходимый клиентский модуль и нажмите "**Редактировать**".

 Редактировать  Удалить		
ТИП КЛИЕНТА	РЕГ. ВЫРАЖЕНИЕ	СТРОКА ПОИСКА
☒ Web	Нет	https://keepersecurity.com/vault/

2. Измените URL\Путь приложения. При необходимости использования регулярного выражения выберите "**Да**" в опции "**Использовать регулярное выражение**".

Кеширование данных пользователя

Информация

Данная настройка позволяет включить кеширование данных пользователя на локальном компьютере для приложений Indeed AM ESSO Agent и компонента Windows Logon.

Если данный параметр был включен для приложений, то вход в систему по аутентификатору может быть выполнен даже при отсутствии физического подключения к сети. При отсутствии подключения будут использоваться закешированные данные пользователя.

1. Откройте консоль администратора, выберите политику где необходимо включить кеширование.
2. Откройте вкладку "**Приложения**" и выберите приложение ESSO или компонент Windows Logon для которого необходимо включить кеширование данных.

Информация

При включении кеширования для одного приложения ESSO, настройки кеширования будут применены для всех ESSO приложений, добавленных в политику

3. На странице выбранного приложения нажмите "**Кеширование данных**".

[МС](#) / [Политики](#) / [Main](#) / [Приложения](#) / [Trello](#)

Main - Trello

Информация	 Сохранить  Отмена  Добавить учетную запись  Удалить  <u>Кеширование данных</u>		
Приложения			
Область действия			
Администраторы			
Аутентификаторы			
	УЧЕТНАЯ ЗАПИСЬ	ТИП УЧЕТНЫХ ДАННЫХ	ОПИСАНИЕ
	☐ Не задана	Индивидуальные	Самообучение
	Доступные методы аутентификации		

4. Для параметра "**Разрешить кешировать учетные данные на ПК пользователя**" выберите "**Да**".

Управление аутентификаторами

 Информация

Для управления аутентификаторами у пользователя должны быть необходимые права доступа.

Для управления аутентификаторами откройте вкладку "**Аутентификаторы**" в карточке пользователя.

На вкладке сосредоточена информация по количеству зарегистрированных аутентификаторов пользователя и их параметры.

МС / Пользователи / Владислав Фомичёв / Аутентификаторы

Владислав Фомичёв - Аутентификаторы

Общая информация

Приложения

Аутентификаторы

История входов

Лицензии

Зарегистрировать

Удалить

Разблокировать

Разрешить использовать

Запретить

ТИП АУТЕНТИФИКАТОРА	УСТРОЙСТВО	КОММЕНТАРИЙ	ДАТА РЕГИСТРАЦИИ	ЗАРЕГИСТРИРОВАЛ	СТАТУС
☐  Multi-factor authentication	MFA	BSP for Multi-factor authentication			Действующий
☐  Push-аутентификация	Indeed AirKey		2020.08.29 15:19	Admin-Indeed	Действующий
☐  Одноразовый пароль по SMS	SMS	SMS OTP			Действующий
☐  Пароль Passcode	Passcode		2020.08.29 14:49	Admin-Indeed	Действующий
☐  Пароль Windows	Windows Password	Windows Password			Действующий
☐  Программный генератор TOTP	Software TOTP token		2020.08.29 14:50	Admin-Indeed	Действующий

Отключение аутентификатора



Информация

Способ аутентификации Windows Password не может быть заблокирован, в случае блокировки доменный пароль все равно может быть использован.

1. Выберите необходимый аутентификатор.
2. Нажмите "**Запретить**".

+ Зарегистрировать Удалить Разблокировать Разрешить использовать Запретить						
	ТИП АУТЕНТИФИКАТОРА	УСТРОЙСТВО	КОММЕНТАРИЙ	ДАТА РЕГИСТРАЦИИ	ЗАРЕГИСТРИРОВАЛ	Статус
☐	Multi-factor authentication	MFA	BSP for Multi-factor authentication			Действующий
☒	Push-аутентификация	Indeed AirKey		2020.08.29 15:19	Admin-Indeed	Действующий

3. После отключения аутентификатора пользователь не сможет использовать данный способ входа. Статус аутентификатора будет "**Запрещено**".

☐	Push-аутентификация	Indeed AirKey		2020.08.29 15:19	Admin-Indeed	
--------------------------	---------------------	---------------	--	------------------	--------------	--

Включение аутентификатора

1. Выберите необходимый аутентификатор.
2. Нажмите "**Разрешить использовать**".

+ Зарегистрировать Удалить Разблокировать Разрешить использовать Запретить						
ТИП АУТЕНТИФИКАТОРА	УСТРОЙСТВО	КОММЕНТАРИЙ	ДАТА РЕГИСТРАЦИИ	ЗАРЕГИСТРИРОВАЛ	СТАТУС	
☐  Multi-factor authentication	MFA	BSP for Multi-factor authentication			Действующий	
☒  Push-аутентификация	Indeed AirKey		2020.08.29 15:19	Admin-Indeed	Запрещён	

3. После включения аутентификатора пользователь сможет использовать данный способ входа. Статус аутентификатора будет "**Действующий**".

☐  Push-аутентификация	Indeed AirKey		2020.08.29 15:19	Admin-Indeed	Действующий	
--	---------------	--	------------------	--------------	-------------	--

Регистрация аутентификаторов

Информация

Перед регистрацией аутентификаторов необходимо создать политику и распространить на целевых пользователей

Информация

Провайдеры Email и SMS не требуют регистрации и могут использоваться если у пользователя задан email или номер телефона соответственно. Если параметры не заданы, то аутентификаторы не будут отображаться в списке доступных для пользователя.

1. Нажмите "**Зарегистрировать**" и выберите необходимый метод аутентификации из выпадающего списка.



Информация

Если у пользователя зарегистрировано максимальное количество аутентификаторов для определенного метода, то данный метод аутентификации отображаться не будет.

2. Выполните действия для обучения аутентификатора.



Примечание

Для различных аутентификаторов будут отличаться окна и действия для обучения.

Сохранить Отмена

Пароль Passcode

Пароль*

.....

Подтвердите пароль*

.....

Комментарий

Passcode 2

3. После успешной регистрации статус аутентификатора будет "**Действующий**".

☐	***	Пароль Passcode	Passcode	Passcode 2	2020.08.31 13:31	Admin-Indeed	Дей
--------------------------	-----	-----------------	----------	------------	------------------	--------------	-----

4. Если был удален провайдер, имеющий зарегистрированные аутентификаторы, то статус аутентификатора будет "**Не установлен**".

☐	***	Пароль Passcode	Passcode	Passcode 2	2020.08.31 13:31	Admin-Indeed	Не
--------------------------	-----	-----------------	----------	------------	------------------	--------------	----

Удаление аутентификатора

1. Выберите необходимый аутентификатор и нажмите "Удалить".

+ Зарегистрировать Удалить Разблокировать Разрешить использовать Запретить						
	ТИП АУТЕНТИФИКАТОРА	УСТРОЙСТВО	КОММЕНТАРИЙ	ДАТА РЕГИСТРАЦИИ	ЗАРЕГИСТРИРОВАЛ	СТАТУС
☐	Multi-factor authentication	MFA	BSP for Multi-factor authentication			Действующий
☐	Push-аутентификация	Indeed AirKey		2020.08.29 15:19	Admin-Indeed	Действующий
☐	Пароль Passcode	Passcode		2020.08.29 14:49	Admin-Indeed	Действующий
☒	Пароль Passcode	Passcode	Passcode 2	2020.08.31 15:23	Admin-Indeed	Действующий

2. Подтвердите удаление.

Подтверждение действия

Вы действительно хотите удалить выбранные элементы?

Отмена

Удалить

Поиск пользователей

1. Откройте Management Console.
2. В левом меню выберите "Пользователи".
3. В поле "Имя" введите имя пользователя или UPN.



Информация

Поддерживается поиск по части имени.

4. В поле "Контейнер" выберите место поиска — весь контейнер или отдельное OU.
5. Нажмите "Поиск".

Пользователи

Имя

Admin

Контейнер

Весь каталог

Выбрать

Поиск

Сбросить

ИМЯ

ИМЯ УЧЕТНОЙ ЗАПИСИ

ПОЛИТИКА



Admin-Indeed

Admin-Indeed@indeed.local

Main [↗](#)

Карточка пользователя

В карточке пользователя содержится информация о пользователе из Active Directory и настройки для пользователя в системе Indeed.

Общая информация

В данном разделе содержится:

1. Информация о пользователе из AD:

- **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**.

2. Данные из системы Indeed AM:

- Политика** — название политики, которая распространяется на пользователя.
- Количество приложений** — число приложений, которые доступны пользователю.
- Количество аутентификаторов** — общее число зарегистрированных аутентификаторов для пользователя.

3. События

— пять последних событий, связанных с данным пользователем.

МС / Пользователи / Владислав Фомичёв

Владислав Фомичёв - Общая информация

Общая информация

Приложения

Аутентификаторы

История входов

Лицензии



Учётная запись
vladislav.fomichev@indeed.local
Email
vladislav.fomichev@indeed.com
Телефон
89524855
Путь в каталоге
indeed.local/Indeed/Users/Indeed/Novgorod/Владислав Фомичёв

Политика

Main [↗](#)

Количество приложений

7

Количество аутентификаторов

2

СОБЫТИЕ	ДАТА	ИНИЦИАТОР
Аутентификатор для целевого пользователя был зарегистрирован администратором.	2020.08.29 14:50:37	Admin-Indeed
Аутентификатор для целевого пользователя был зарегистрирован администратором.	2020.08.29 14:49:52	Admin-Indeed
Целевой объект каталога был добавлен администратором в группу доступа для целевого приложения	2020.08.29 12:56:53	Admin-Indeed
Ошибка при попытке администратора добавить целевой объект каталога в группу доступа для целевого приложения	2020.08.29 12:56:53	Admin-Indeed

Приложения

В данном разделе отображается информация по всем доступным приложениям для пользователя.

[МС](#) / [Пользователи](#) / [Владислав Фомичёв](#) / [Приложения](#)

Владислав Фомичёв - Приложения

Общая информация				
Приложения				
Аутентификаторы				
История входов				
Лицензии				
		НАЗВАНИЕ	МОДУЛЬ ИНТЕГРАЦИИ	ТЕХНОЛОГИИ АУТЕНТИФИКАЦИИ
		☐  IIS Extension	IIS Extension	Любые доступные
		☐  Keepersecurity	Enterprise SSO	Любые доступные
		☐  NPS RADIUS Extension	NPS RADIUS Extension	Любые доступные
		☐  RDP Windows Logon	RDP Windows Logon	Любые доступные
		☐  rollApp	Enterprise SSO	Любые доступные
		☐  SAML Identity Provider	SAML Identity Provider	Любые доступные
		☐  Trello	Enterprise SSO	Любые доступные
		☐  Windows Logon	Windows Logon	Любые доступные

Аутентификаторы

В данном разделе отображается информация по всем доступным аутентификаторам пользователя.

[МС](#) / [Пользователи](#) / [Владислав Фомичёв](#) / [Аутентификаторы](#)

Владислав Фомичёв - Аутентификаторы

Общая информация	+ Зарегистрировать Удалить Разблокировать Разрешить использовать Запретить					
Приложения						
Аутентификаторы						
История входов						
Лицензии						
		ТИП АУТЕНТИФИКАТОРА	УСТРОЙСТВО	КОММЕНТАРИЙ	ДАТА РЕГИСТРАЦИИ	ЗАРЕГИСТРИРОВАЛ
		☐  Multi-factor authentication	MFA	BSP for Multi-factor authentication		Действующий
		☐  Push-аутентификация	Indeed AirKey		2020.08.29 15:19	Admin-Indeed
		☐  Одноразовый пароль по SMS	SMS	SMS OTP		Действующий
		☐  Пароль Passcode	Passcode		2020.08.29 14:49	Admin-Indeed
		☐  Пароль Windows	Windows Password	Windows Password		Действующий

История входов

В данном разделе отображается информация по последним аутентификациям пользователя в приложениях.

Владислав Фомичёв - История входов

Общая информация
Приложения
Аутентификаторы
История входов
Лицензии

Экспортировать

Начальная дата

2020/08/26 00:00

Конечная дата

2020/08/30 00:00

Приложение

Не задано

Модуль

Не задано

Тип аутентификатора

Не задано

Статус

Не задано

Применить

Сбросить

Дата	Приложение	Пользователь	Аутентификатор	Статус
2020.08.29 15:31:32	Enterprise SSO	Владислав Фомичёв	Windows Token	Успешный вход
2020.08.29 15:31:17	Windows Logon	Владислав Фомичёв	AirKey Cloud	Успешный вход
2020.08.29 15:29:17	Windows Logon	Владислав Фомичёв	AirKey Cloud	Успешный вход
2020.08.29 15:22:45	NPS RADIUS Extension	Владислав Фомичёв	AirKey Cloud	Успешный вход
2020.08.29 15:21:30	IIS Extension	Владислав Фомичёв	Passcode	Успешный вход
2020.08.29 15:21:15	IIS Extension	Владислав Фомичёв	Windows Password	Успешный вход

Лицензии

В данном разделе отображается информация по зарегистрированным у пользователя лицензиям.

Владислав Фомичёв - Лицензии

Общая информация	модуль интеграции	политика
Приложения	Управление модулем Windows Logon	Main
Аутентификаторы	Управление модулем Enterprise SSO	Main
История входов	Управление модулем IIS Extension	Main
Лицензии	Управление модулем NPS RADIUS Extension	Main

Журнал событий

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, выполните следующие действия:

1. В левом меню, в блоке "**Аудит**", выберите "**События**".
2. 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.



Информация

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 "*" (Звездочка) 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.

Выберите события

☐	Номер	Категория	Описание
☐	1000	Info	Пользователь был аутентифицирован по предоставленному аутентификатору. Приложение: {requestApplication}. Инициатор: {requestUser}. Компьютер: {requestComputer}. Способ аутентификации: {authMode}. Комментарий аутентификатора: {authComment}. Имя бизнес приложения: {businessApplication}.
☐	2000	Error	Ошибка при попытке аутентифицировать пользователя по предоставленному способу аутентификации. Приложение: {requestApplication}. Инициатор: {requestUser}. Компьютер: {requestComputer}. Способ аутентификации: {authMode}. Описание ошибки: {errorDescription}. Имя бизнес приложения: {businessApplication}.
☐	1001	Info	Сервер Indeed-Id был запущен. Компьютер: {computer}.

[Отмена](#)
[Выбрать](#)

События

Экспортировать

Пользователь или инициатор Admin-Indeed Выбрать	Приложение Windows Logon	Начальная дата 2020/08/26 00:00	Конечная дата 2020/08/30 00:00
Тип аутентификатора AirKey Cloud	Модуль Не задано	Описание содержит	Тип события Информация

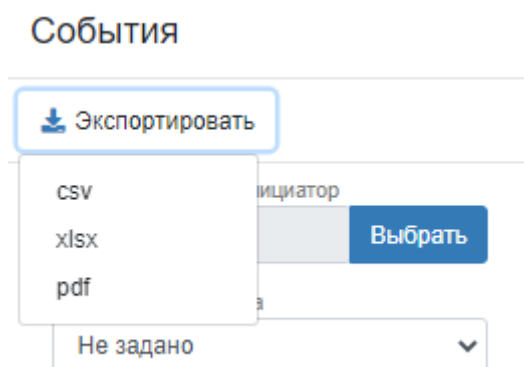
Код события

1000 [Выбрать](#)

[Применить](#) [Сбросить](#)

СОБЫТИЕ	ДАТА	МОДУЛЬ	ИНИЦИАТОР
Пользователь был аутентифицирован по предоставленному аутентификатору.	2020.08.28 21:49:41	Windows Logon	Admin-Indeed
Пользователь был аутентифицирован по предоставленному аутентификатору.	2020.08.28 21:49:26	Windows Logon	Admin-Indeed
Пользователь был аутентифицирован по предоставленному аутентификатору.	2020.08.28 13:21:36	Windows Logon	Admin-Indeed
Пользователь был аутентифицирован по предоставленному аутентификатору.	2020.08.28 13:16:19	Windows Logon	Admin-Indeed
Пользователь был аутентифицирован по предоставленному аутентификатору.	2020.08.28 13:15:19	Windows Logon	Admin-Indeed

3. Для экспорта событий нажмите на значок в верхней части страницы. Экспорт возможен в форматах: **csv, xlsx, pdf**.



Описание событий

События компонента Indeed AM Server

Код	Категория	Текст сообщения	Причины возникновения
1000	Информация	Пользователь был аутентифицирован по предоставленному аутентификатору. Приложение: Пользователь: Компьютер: Способ аутентификации: Комментарий аутентификатора:	Успешная аутентификация пользователя
1001	Информация	Сервер Indeed-Id был запущен. Компьютер:	Успешный запуск Indeed AM Server вручную.
1002	Информация	Сервер Indeed-Id был остановлен. Компьютер:	Успешная остановка сервера вручную.

1003	Информация	Пользователь был идентифицирован по предоставленному способу аутентификации. Приложение: Пользователь: Компьютер: Способ аутентификации:	Успешная идентификация пользователя.
1004	Информация	Аутентификатор для целевого пользователя был зарегистрирован администратором. Приложение: Целевой пользователь: Администратор: Компьютер: Способ аутентификации: Комментарий аутентификатора:	Успешная регистрация нового аутентификатора администратором системы.
1005	Информация	Настройка 'Максимальное количество аутентификаторов' для целевого пользователя была изменена администратором. Администратор: Компьютер: Целевой пользователь: Старое значение: Новое значение:	Успешная смена параметра "Максимальное количество аутентификаторов" для пользователя администратором системы.
1006	Информация	Настройка 'Право на регистрацию аутентификатора' для целевого пользователя была изменена администратором. Администратор: Компьютер: Целевой пользователь: Старое значение: Новое значение:	Успешная смена параметра "Право на регистрацию аутентификатора" для пользователя администратором системы.

1007	Информация	Настройка 'Право на изменение аутентификатора' для целевого пользователя была изменена администратором. Администратор: Компьютер: Целевой пользователь: Старое значение: Новое значение:	Успешная смена параметра "Право на изменение аутентификатора" для пользователя администратором системы.
1008	Информация	Настройка 'Право на удаление аутентификатора' для целевого пользователя была изменена администратором. Администратор: Компьютер: Целевой пользователь: Старое значение: Новое значение:	Успешная смена параметра "Право на удаление аутентификатора" для пользователя администратором системы.
1009	Информация	Настройка 'Право на изменение комментария аутентификатора при регистрации' для целевого пользователя была изменена администратором. Администратор: Компьютер: Целевой пользователь: Старое значение: Новое значение:	Успешная смена параметра "Право на изменение комментария аутентификатора при регистрации" для пользователя администратором системы.

1010	Информация	Настройка 'Право на изменение комментария аутентификатора' для целевого пользователя была изменена администратором Администратор: Компьютер: Целевой пользователь: Старое значение: Новое значение:	Успешная смена параметра "Право на изменение комментария аутентификатора" для пользователя администратором системы.
1011	Информация	Настройка 'Кэширование данных начиная с' для целевого пользователя была изменена администратором. Администратор: Компьютер: Целевой пользователь: Старое значение: Новое значение:	Успешная смена параметра "Кэширование данных начиная с" для пользователя администратором системы.
1012	Информация	Настройка 'Кэширование данных вплоть до' для целевого пользователя была изменена администратором. Администратор: Компьютер: Целевой пользователь: Старое значение: Новое значение:	Успешная смена параметра "Кэширование данных вплоть до" для пользователя администратором системы.
1014	Информация	Настройка 'Кэширование данных в период' для целевого пользователя была изменена администратором. Администратор: Компьютер: Целевой пользователь: Старое значение: Новое значение:	Успешная смена параметра "Кэширование данных в период" для пользователя администратором системы.

1015	Информация	Настройка 'Начальная дата замещения пользователя' для целевого пользователя была изменена администратором. Администратор: Компьютер: Целевой пользователь: Старое значение: Новое значение:	Успешная смена параметра "Начальная дата замещения пользователя" для пользователя администратором системы.
1016	Информация	Настройка 'Конечная дата замещения пользователя' для целевого пользователя была изменена администратором. Администратор: Компьютер: Целевой пользователь: Старое значение: Новое значение:	Успешная смена параметра "Конечная дата замещения пользователя" для пользователя администратором системы.
1017	Информация	Настройка 'Список заместителей' для целевого пользователя была изменена администратором. Администратор: Компьютер: Целевой пользователь: Старое значение: Новое значение:	Успешная смена параметра "Список заместителей" для пользователя администратором системы.
1018	Информация	Настройка 'Разрешить кэширование' для целевого пользователя была изменена администратором. Администратор: Компьютер: Целевой пользователь: Старое значение: Новое значение:	Успешная смена параметра "Разрешить кэширование" для пользователя администратором системы.

1019	Информация	Настройка 'Разрешить замещение' для целевого пользователя была изменена администратором. Администратор: Компьютер: Целевой пользователь: Старое значение: Новое значение:	Успешная смена параметра "Разрешить замещение" для пользователя администратором системы.
1020	Информация	Лицензия была выдана целевому объекту каталога администратором. Компьютер: Администратор: Идентификатор приложения: Целевой объект каталога: Тип лицензии:	Успешная выдача лицензии целевому объекту каталога администратором системы.
1021	Информация	Лицензия была добавлена пользователем. Идентификатор лицензии: Дата начала: Дата окончания: Количество: Описание: Пользователь: Компьютер:	Успешное добавление лицензии пользователем.

1022	Информация	Лицензия была удалена пользователем. Идентификатор лицензии: Дата начала: Дата окончания: Количество: Описание: Пользователь: Компьютер:	Успешное удаление лицензии пользователем.
1023	Информация	Лицензия целевого объекта каталога была удалена администратором. Идентификатор лицензии: Компьютер: Администратор: Идентификатор приложения: Целевой объект каталога: Тип лицензии:	Успешное удаление лицензии администратором системы.
1024	Информация	Аутентификатор целевого пользователя был изменен администратором. Приложение: Целевой пользователь: Администратор: Компьютер: Способ аутентификации: Комментарий аутентификатора:	Успешное изменение аутентификатора пользователя администратором системы.

1025	Информация	Комментарий аутентификатора целевого пользователя был изменен администратором. Приложение: Целевой пользователь: Администратор: Компьютер: Способ аутентификации: Старый комментарий аутентификатора: Новый комментарий аутентификатора:	Успешное изменение комментария аутентификатора пользователя администратором системы.
1026	Информация	Аутентификатор целевого пользователя был удален администратором. Приложение: Целевой пользователь: Администратор: Компьютер: Способ аутентификации: Комментарий аутентификатора:	Успешное удаление аутентификатора пользователя администратором системы.
1027	Информация	Лицензия целевого пользователя была удалена сервером. Идентификатор лицензии: Идентификатор приложения: Целевой пользователь:	Успешное удаление пользовательской лицензии сервером.

1028	Информация	Целевой объект каталога был добавлен администратором в группу доступа для целевого приложения Приложение: Инициатор: Компьютер: Целевое приложение: Целевой объект каталога: Политика: Группа доступа: Область действия:	Успешное добавление объекта в группу доступа для целевого приложения.
1029	Информация	Целевой объект каталога был удален администратором из группы доступа для целевого приложения. Приложение: Инициатор: Компьютер: Целевое приложение: Целевой объект каталога: Политика: Группа доступа: Область действия:	Успешное удаление объекта из группы доступа для целевого приложения.
1030	Информация	Устройство было добавлено пользователем. Приложение: Пользователь: Компьютер: Устройство: Комментарий: Серийный номер:	Успешное добавление устройства пользователем.

1031	Информация	Устройство было удалено пользователем. Приложение: Пользователь: Компьютер: Устройство: Комментарий: Серийный номер: Идентификатор устройства:	Успешное удаление устройства пользователем.
1032	Информация	Способ аутентификации для целевого пользователя был запрещен администратором. Приложение: Администратор: Компьютер: Целевой пользователь: Способ аутентификации:	Администратор системы запретил использование способа аутентификации для пользователя.
1033	Информация	Способ аутентификации для целевого пользователя был разрешен администратором. Приложение: Администратор: Компьютер: Целевой пользователь: Способ аутентификации:	Администратор системы разрешил использование способа аутентификации для пользователя.

1034	Информация	Аутентификатор целевого пользователя был заблокирован администратором. Приложение: Администратор: Компьютер: Целевой пользователь: Способ аутентификации: Комментарий аутентификатора:	Администратор системы заблокировал использование аутентификатора для пользователя.
1035	Информация	Аутентификатор целевого пользователя был разблокирован администратором. Приложение: Администратор: Компьютер: Целевой пользователь: Способ аутентификации: Комментарий аутентификатора:	Администратор системы разблокировал использование аутентификатора для пользователя.
1036	Информация	Способ аутентификации был заблокирован пользователем. Приложение: Пользователь: Компьютер: Способ аутентификации:	Пользователь системы с необходимыми правами доступа заблокировал способ аутентификации.
1037	Информация	Способ аутентификации для целевого пользователя был разблокирован администратором. Приложение: Администратор: Компьютер: Целевой пользователь: Способ аутентификации:	Администратор системы разблокировал использование способа аутентификации для пользователя.

1038	Информация	SMS-сообщение отправлено пользователем. Приложение: Инициатор: Компьютер: Способ аутентификации: Телефон: Время отправки: Параметры отправки: Идентификатор сообщения:	Успешная отправка SMS-сообщения пользователем.
1039	Информация	Email-сообщение отправлено пользователем. Приложение: Пользователь: Компьютер: Способ аутентификации: Email:	Успешная отправка Email-сообщения пользователем.
1040	Информация	Часть каталогов сервера недоступна. Компьютер: Описание ошибки:	
1041	Информация	Аутентификатор был изменен пользователем. Приложение: Пользователь: Компьютер: Способ аутентификации: Комментарий аутентификатора:	Пользователь системы с необходимыми правами доступа успешно изменил аутентификатор.

1042	Информация	Аутентификатор был зарегистрирован пользователем. Приложение: Пользователь: Компьютер: Способ аутентификации: Комментарий аутентификатора:	Пользователь системы с необходимыми правами доступа успешно зарегистрировал аутентификатор.
1043	Информация	Комментарий аутентификатора был изменен пользователем. Приложение: Пользователь: Компьютер: Способ аутентификации: Старый комментарий аутентификатора: Новый комментарий аутентификатора:	Пользователь системы с необходимыми правами доступа успешно изменил аутентификатор.
1044	Информация	Аутентификатор был удален пользователем. Приложение: Пользователь: Компьютер: Способ аутентификации: Комментарий аутентификатора:	Пользователь системы с необходимыми правами доступа успешно удалил аутентификатор.
1045	Информация	Аутентификатор целевого пользователя был отключен администратором. Приложение: Администратор: Компьютер: Целевой пользователь: Способ аутентификации: Комментарий аутентификатора:	Администратор системы отключил аутентификатор пользователя.

1046	Информация	Аутентификатор целевого пользователя был включен администратором. Приложение: Администратор: Компьютер: Целевой пользователь: Способ аутентификации: Комментарий аутентификатора:	Администратор системы включил аутентификатор пользователя.
1047	Информация	Лицензия целевого объекта каталога была удалена администратором. Компьютер: Администратор: Идентификатор приложения: Целевой объект каталога: Тип лицензии:	Администратор системы удалил лицензию целевого объекта каталога.
1048	Информация	Лицензия была добавлена пользователем. Идентификатор лицензии: Дата начала: Дата окончания: Количество: Описание: Пользователь: Компьютер: Идентификатор приложения:	Пользователь системы с необходимыми правами доступа успешно добавил лицензию.

1049	Информация	Лицензия была удалена пользователем. Идентификатор лицензии: Дата начала: Дата окончания: Количество: Описание: Пользователь: Компьютер: Идентификатор приложения:	Пользователь системы с необходимыми правами доступа успешно удалил лицензию.
1050	Информация	Лицензия целевого пользователя была удалена сервером. Идентификатор приложения: Целевой пользователь:	Успешное удаление пользовательской лицензии сервером.
1051	Информация	Политика успешно создана. Идентификатор: Имя: Описание: Приоритет: Новые объекты каталога: Новые приложения: Приложение: Инициатор: Компьютер:	Успешное создание политики.

1052	Информация	Политика удалена. Идентификатор: Имя: Описание: Приоритет: Удалённые объекты каталога: Удалённые приложения: Приложение: Инициатор: Компьютер:	Успешное удаление политики.
1053	Информация	Политика изменена. Идентификатор: Имя: Описание: Приоритет: Новые объекты каталога: Новые приложения: Удалённые объекты каталога: Удалённые приложения: Приложение: Инициатор: Компьютер:	Успешное изменение политики.
1054	Информация	Пароль пользователя был успешно синхронизирован. Инициатор: Компьютер: Клиентский пользователь: Клиентский компьютер:	Успешная синхронизация доменного пароля пользователя с паролем в хранилище Indeed.

1055	Информация	Пользователь успешно выполнил вход по предоставленному паролю. Инициатор: Компьютер: Клиентский пользователь: Клиентский компьютер:	Успешная аутентификация пользователя по паролю операционной системы.
1056	Информация	Пользователь успешно выполнил вход по кэшированному аутентификатору. Инициатор: Способ входа: Комментарий аутентификатора: Компьютер: Клиентский пользователь: Клиентский компьютер:	Успешная аутентификация пользователя по кэшированному аутентификатору.
1057	Информация	Пользователь успешно выполнил вход по предоставленному аутентификатору. Инициатор: Способ входа: Комментарий аутентификатора: Компьютер: Клиентский пользователь: Клиентский компьютер:	Успешная аутентификация пользователя по предоставленному аутентификатору.
1058	Информация	Пользователь убрал устройство входа. Сессия завершена. Инициатор: Комментарий аутентификатора: Компьютер: Клиентский пользователь: Клиентский компьютер:	Успешная автоматическая блокировка компьютера при извлечении устройства аутентификации (токена, смарт-карты).

1059	Информация	Пользователь вышел из системы. Инициатор: Комментарий аутентификатора: Компьютер: Клиентский пользователь: Клиентский компьютер:	Успешный выход пользователя из операционной системы (завершение рабочей сессии).
1060	Информация	Пользователь убрал устройство входа. Компьютер заблокирован. Инициатор: Комментарий аутентификатора: Компьютер: Клиентский пользователь: Клиентский компьютер:	Успешное автоматическое завершение рабочей сессии пользователя при извлечении устройства аутентификации (токена, смарт-карты).
1061	Информация	Пользователь заблокировал компьютер. Инициатор: Комментарий аутентификатора: Компьютер: Клиентский пользователь: Клиентский компьютер:	Успешная блокировка компьютера пользователем вручную или успешная автоматическая блокировка экранной заставкой.
1062	Информация	Пользователь разблокировал компьютер по предоставленному паролю. Инициатор: Компьютер: Клиентский пользователь: Клиентский компьютер:	Успешная разблокировка компьютера пользователем с использованием пароля.

1063	Информация	Пользователь разблокировал компьютер по кэшированному аутентификатору. Инициатор: Способ входа: Комментарий аутентификатора: Компьютер: Клиентский пользователь: Клиентский компьютер:	Успешная разблокировка компьютера пользователем с использованием кэшированного аутентификатора.
1064	Информация	Пользователь разблокировал компьютер по предоставленному аутентификатору. Инициатор: Способ входа: Комментарий аутентификатора: Компьютер: Клиентский пользователь: Клиентский компьютер:	Успешная разблокировка компьютера пользователем с использованием аутентификатора.
1065	Информация	Пользователь снова подключился к своему терминальному сеансу. Инициатор: Комментарий аутентификатора: Компьютер: Клиентский пользователь: Клиентский компьютер:	Успешный вход пользователя в операционную систему в терминальной сессии после отключения от терминального сервера.
1067	Информация	Пароль пользователя был успешно сменен автоматически. Инициатор: Компьютер: Клиентский пользователь: Клиентский компьютер:	Успешная смена пароля пользователя.

1068	Информация	Пароль пользователя был успешно сменен. Инициатор: Компьютер: Клиентский пользователь: Клиентский компьютер:	Успешная смена пароля пользователя.
1069	Информация	Пароль пользователя рассинхронизирован. Инициатор: Компьютер: Клиентский пользователь: Клиентский компьютер:	Возможные причины: • Доменный пароль пользователя был изменен вне системы Indeed EA/ESSO. Например, сброшен администратором Active Directory. • Аутентификатор был зарегистрирован без ввода пользователем доменного пароля. Например, в результате выпуска смарт-карты в системах Indeed CM, Aladdin JMS и SAM с коннектором к Indeed EA/ESSO.
1070	Информация	Пользователь был аутентифицирован для целевого приложения. Приложение: Инициатор: Компьютер: Целевой пользователь:	Успешная аутентификация пользователя в целевом приложении.
1073	Информация	Изменение настроек метода аутентификации: Приложение: Инициатор: Компьютер: Провайдер: Настройки:	Успешное изменение настроек метода аутентификации.

1076	Информация	Изменение настройки прав аутентификатора - Успешно: Политика: Пользователь: Обучение: Переобучение: Удаление: Изменение комментария только при обучении: Изменение комментария: Приложение: Инициатор: Компьютер:	Успешное изменение настройки прав аутентификатора.
1077	Информация	Создание настройки учётной записи. Политика: Целевой пользователь: Роль: 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:	Успешное создание настройки учётной записи.

1078	Информация	Удаление настройки учётной записи. Политика: Целевой пользователь: Роль: 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:	Успешное удаление настройки учётной записи.
------	------------	---	---

1079	Информация	Изменение настройки учётной записи. Политика: Целевой пользователь: Роль: 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:	Успешное изменение настройки учётной записи.
1082	Информация	Изменение настроек метода аутентификации для пользователя: Целевой пользователь: Провайдер: Приложение: Инициатор: Компьютер: Настройки:	Успешное изменение настроек метода аутентификации для пользователя.

1085	Информация	Изменение настроек метода аутентификации для модуля: Модуль: Провайдер: Политика: Id политики: Приложение: Инициатор: Компьютер: Настройки:	Успешное изменение настроек метода аутентификации для модуля.
1086	Информация	Настройки кэширования данных пользователя были успешно изменены: Целевое приложение: Целевой пользователь: Старые значения: Новые значения: Приложение: Инициатор: Компьютер:	Успешное изменение настроек кэширования данных пользователя.
1087	Информация	Настройки кэширования данных пользователя в политике были успешно изменены: Целевое приложение: Политика: Старые значения: Новые значения: Приложение: Инициатор: Компьютер:	Успешное изменение настроек кэширования данных пользователя в политике.

1088	Информация	Телефонный номер успешно зарегистрирован. Пользователь: Инициатор: Пользователь API: Телефон:	Успешная регистрация телефонного номера.
1089	Информация	Телефонный номер успешно изменен. Пользователь: Инициатор: Пользователь API: Телефон:	Успешное изменение телефонного номера.
1090	Информация	Телефонный номер успешно удален. Пользователь: Инициатор: Пользователь API:	Успешное удаление телефонного номера.
1091	Информация	Пароль пользователя был успешно сменен автоматически. Целевой пользователь: Приложение: Инициатор: Компьютер:	Успешное изменение пароля пользователя автоматически.
1092	Информация	Пароль пользователя был успешно сменен. Целевой пользователь: Приложение: Инициатор: Компьютер:	Успешное изменение пароля пользователя.

1093	Информация	Изменение политики метода аутентификации: Провайдер: Политика: Id политики: Приложение: Инициатор: Компьютер: Настройки:	Успешное изменение политики метода аутентификации.
1094	Информация	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:	Успешное завершения работы службы отзыва лицензий.
1095	Информация	Лицензия целевого пользователя была удалена сервером в связи с превышением периода неактивности пользователя. Идентификатор приложения: Целевой пользователь:	Пользователь превысил период не активности, установленный на сервере, в связи с чем лицензия была отозвана сервером.
1097	Информация	Indeed-Id ESSO Agent успешно инициализировался и начал работу Инициатор: Компьютер: Идентификатор процесса: Компьютер:	Успешный запуск Агента Enterprise SSO.

1098	Информация	Indeed-Id ESSO Agent завершает работу Инициатор: Компьютер: Идентификатор процесса: Компьютер:	Завершение работы Агента Enterprise SSO.
1099	Информация	Приложение было принудительно завершено Инициатор: Компьютер: Описание приложения: Путь исполняемого файла приложения: Компьютер: Командная строка:	Принудительное завершение приложения Агентом Enterprise SSO в случае ошибки (например, если предоставленный пользователем аутентификатор не совпадает с обученным, аутентификация отменена пользователем и др.).
1100	Информация	Форма приложения была принудительно закрыта Инициатор: Компьютер: Описание приложения: Путь исполняемого файла приложения: Тип формы: Компьютер: Командная строка:	Принудительное закрытие формы Агентом Enterprise SSO в случае ошибки. Если для приложения не назначен способ аутентификации «Только Indeed ESSO Агент», при возникновении ошибки смены пароля будет закрыта только форма смены пароля без завершения работы приложения. Если для приложения назначен способ аутентификации «Только Indeed ESSO Агент», при возникновении ошибки на форме смены пароля будет завершена работа приложения. В ряде случаев ошибка на форме может привести к принудительному закрытию приложения.
1101	Информация	Пользователь аутентифицировался в Indeed-Id ESSO Инициатор: Компьютер: Имя пользователя: Компьютер:	Предоставленный пользователем Агенту Enterprise SSO аутентификатор совпадает с обученным

1102	Информация	Пользователь реаутентифицировался в Indeed-Id ESSO Инициатор: Компьютер: Имя пользователя: Компьютер:	Успешная повторная аутентификация пользователя в Агенте Enterprise SSO.
1103	Информация	Пользователь выполнил вход в приложение. Инициатор: Компьютер: Описание приложения: Путь исполняемого файла приложения: Имя пользователя: Имя учетной записи пользователя в приложении: Компьютер: Описание учетной записи SSO: {ssoAccountDescription} Командная строка:	Успешно выполнен вход в приложение через Агент Enterprise SSO.
1104	Информация	Пароль пользователя был успешно сменен. Инициатор: Компьютер: Описание приложения: Путь исполняемого файла приложения: Имя пользователя: Имя учетной записи пользователя в приложении: Компьютер: Описание пользователя: Командная строка:	Успешная автоматическая смена пароля пользователю Indeed Enterprise Single Sign-On.

1105	Информация	Добавлено сетевое подключение для пользователя Indeed-Id ESSO Инициатор: Компьютер: Имя пользователя: Диск подключения: Путь подключения: Компьютер:	Создано сетевое подключение для пользователя Indeed ESSO.
1106	Информация	Удалено сетевое подключение для пользователя Indeed-Id ESSO Инициатор: Компьютер: Имя пользователя: Диск подключения: Компьютер:	Удалено сетевое подключение для пользователя Indeed ESSO.
1107	Информация	Ошибка при удалении сетевого подключения для пользователя Indeed-Id ESSO Инициатор: Компьютер: Имя пользователя: Диск подключения: Компьютер:	Отсутствует связь с сервером Indeed.

1108	Информация	Пользователь успешно разблокировал приложение. Инициатор: Компьютер: Описание приложения: Путь исполняемого файла приложения: Имя пользователя: Имя учетной записи пользователя в приложении: Компьютер: Описание пользователя: Командная строка:	Приложение успешно разблокировано.
1109	Информация	Замещающий пользователь аутентифицировался в Indeed-Id ESSO Инициатор: Компьютер: Имя пользователя: Замещающий пользователь: Компьютер:	Предоставленный замещающим пользователем Агенту Enterprise SSO аутентификатор совпадает с обученным.
1110	Информация	Замещающий пользователь реаутентифицировался в Indeed-Id ESSO Инициатор: Компьютер: Имя пользователя: Замещающий пользователь: Компьютер:	Успешная повторная аутентификация замещающего пользователя в Агенте Enterprise SSO.

1111	Информация	Пароль пользователя был успешно сгенерирован и сменен автоматически. Инициатор: Компьютер: Описание приложения: Путь исполняемого файла приложения: Имя пользователя: Имя учетной записи пользователя в приложении: Компьютер: Описание пользователя: Командная строка:	Успешная автоматическая генерация и смена пароля пользователя.
1112	Информация	Добавлено новое приложение. Название: Описание: Модуль интеграции: Приложение: Инициатор: Компьютер:	Добавление шаблона приложения.
1113	Информация	Приложение удалено. Название: Описание: Модуль интеграции: Приложение: Инициатор: Компьютер:	Удаление приложения.

2000	Ошибка	Ошибка при попытке аутентифицировать пользователя по предоставленному способу аутентификации. Приложение: Пользователь: Компьютер: Способ аутентификации: Описание ошибки:	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	Ошибка при попытке запустить сервер Indeed-Id Компьютер: Описание ошибки:	Неуспешная попытка запуска Indeed AM Server вручную. Возможные причины: • Ошибка в конфигурационном файле сервера. • Сервер уже запущен. • Повреждено хранилище данных. • Ошибка IIS.
2002	Ошибка	Ошибка при попытке остановить сервер Indeed-Id Компьютер: Описание ошибки:	Неуспешная попытка остановки Indeed AM Server вручную. Возможные причины: • Недостаточно прав для выполнения операции. • Indeed AM Server уже остановлен
2003	Ошибка	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	Ошибка при попытке администратора зарегистрировать аутентификатор для целевого пользователя. Приложение: Целевой пользователь: Администратор: 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	Ошибка при попытке администратора изменить аутентификатор целевого пользователя. Приложение: Целевой пользователь: Администратор: 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	Ошибка при попытке администратора удалить аутентификатор целевого пользователя. Приложение: Целевой пользователь: Администратор: Компьютер: Способ аутентификации: Комментарий аутентификатора: Описание ошибки:	Неуспешная попытка администратора системы Indeed AM удалить аутентификатор пользователя. Возможные причины: • Аутентификатор уже удален. • Повреждено хранилище данных.

2007	Ошибка	Ошибка при попытке администратора выдать лицензию для целевого объекта каталога. Компьютер: Администратор: Идентификатор приложения: Целевой объект каталога: Тип лицензии: 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	Ошибка при попытке администратора удалить лицензию целевого объекта каталога. Компьютер: Администратор: 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	Ошибка при попытке пользователя удалить лицензию. Идентификатор лицензии: Пользователь: 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	Ошибка при попытке пользователя добавить лицензию. Идентификатор лицензии: Пользователь: 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	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.
2012	Ошибка	Ошибка при попытке администратора изменить настройку 'Максимальное количество аутентификаторов' для целевого пользователя. Администратор: 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	Ошибка при попытке администратора изменить настройку 'Право на регистрацию аутентификатора' для целевого пользователя. Администратор: 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	Ошибка при попытке администратора изменить настройку 'Право на изменение аутентификатора' для целевого пользователя. Администратор: 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	Ошибка при попытке администратора изменить настройку 'Право на удаление аутентификатора' для целевого пользователя. Администратор: 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	Ошибка при попытке администратора изменить настройку 'Право на изменение комментария аутентификатора при регистрации' для целевого пользователя. Администратор: 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.

2017	Ошибка	Ошибка при попытке администратора изменить настройку 'Право на изменение комментария аутентификатора' для целевого пользователя. Администратор: 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	Ошибка при попытке администратора изменить настройку 'Кэширование данных начиная с' для целевого пользователя. Администратор: 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	Ошибка при попытке администратора изменить настройку 'Кэширование данных вплоть до' для целевого пользователя. Администратор: 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	Ошибка при попытке администратора изменить настройку 'Кэширование данных в период' для целевого пользователя. Администратор: 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	Ошибка при попытке администратора изменить настройку 'Начальная дата замещения пользователя' для целевого пользователя. Администратор: 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.
2022	Ошибка	Ошибка при попытке администратора изменить настройку 'Конечная дата замещения пользователя' для целевого пользователя. Администратор: 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	Ошибка при попытке администратора изменить настройку 'Список заместителей' для целевого пользователя. Администратор: 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	Ошибка при попытке администратора изменить настройку 'Разрешить кэширование' для целевого пользователя. Администратор: 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	Ошибка при попытке администратора изменить настройку 'Разрешить замещение' для целевого пользователя. Администратор: 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	Ошибка при попытке администратора добавить целевой объект каталога в группу доступа для целевого приложения Приложение: Инициатор: Компьютер: Целевое приложение: Целевой объект каталога: Политика: Группа доступа: 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.
2027	Ошибка	Ошибка при попытке администратора удалить целевой объект каталога из группы доступа для целевого приложения. Приложение: Инициатор: Компьютер: Целевое приложение: Целевой объект каталога: Политика: Группа доступа: 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	Ошибка при попытке пользователя добавить устройство. Приложение: Пользователь: 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	Ошибка при попытке пользователя удалить устройство. Приложение: Пользователь: 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	Ошибка при попытке администратора запретить способ аутентификации для целевого пользователя. Приложение: Администратор: 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	Ошибка при попытке администратора разрешить способ аутентификации для целевого пользователя. Приложение: Администратор: 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.
2032	Ошибка	Ошибка при попытке администратора заблокировать аутентификатор целевого пользователя. Приложение: Администратор: 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	Ошибка при попытке администратора разблокировать аутентификатор целевого пользователя. Приложение: Администратор: 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	Ошибка при попытке пользователя заблокировать способ аутентификации. Приложение: Пользователь: Компьютер: Способ аутентификации: Описание ошибки:	Неуспешная попытка при блокировки способа аутентификации пользователем. Возможные причины: • Способ аутентификации уже заблокирован. • Недостаточно прав. • Сервер Indeed AM неактивен. • Повреждено хранилище данных.
2035	Ошибка	Ошибка при попытке администратора разблокировать способ аутентификации для целевого пользователя. Приложение: Администратор: Компьютер: Целевой пользователь: Способ аутентификации: Описание ошибки:	Неуспешная попытка при разблокировки способа аутентификации пользователем. Возможные причины: • Способ аутентификации уже разблокирован. • Недостаточно прав. • Сервер Indeed AM неактивен. • Повреждено хранилище данных.
2036	Ошибка	Ошибка при попытке отправить SMS-сообщение. Приложение: Инициатор: Компьютер: Способ аутентификации: Телефон: Описание ошибки: Время отправки: Параметры отправки: Идентификатор сообщения:	Неуспешная попытка при при отправки SMS. Возможные причины: • Ошибка при подключении к SMPP серверу. • Не задан номер телефона.

2037	Ошибка	Ошибка при попытке пользователя отправить Email-сообщение. Приложение: Пользователь: Компьютер: Способ аутентификации: Email:	Неуспешная попытка при при отправки Email-сообщения. Возможные причины: • Ошибка при подключении к SMTP серверу. • Не задан email пользователя.
2038	Ошибка	Хранилище сервера недоступно. Компьютер: Описание ошибки:	Неуспешная попытка при при соединении с сервером Indeed. Возможные причины: • Сервер Indeed AM неактивен. • Повреждено хранилище данных.
2039	Ошибка	Каталоги сервера недоступны. Компьютер: Описание ошибки:	
2040	Ошибка	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	Ошибка при попытке пользователя изменить аутентификатор. Приложение: Пользователь: 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.

2042	Ошибка	Ошибка при попытке пользователя зарегистрировать аутентификатор. Приложение: Пользователь: 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	Ошибка при попытке пользователя удалить аутентификатор. Приложение: Пользователь: 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	Ошибка при попытке администратора отключить аутентификатор целевого пользователя. Приложение: Администратор: 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	Ошибка при попытке администратора включить аутентификатор целевого пользователя. Приложение: Администратор: 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	Ошибка при попытке пользователя добавить лицензию. Идентификатор лицензии: Пользователь: 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.
2047	Ошибка	Ошибка при попытке пользователя удалить лицензию. Идентификатор лицензии: Пользователь: Компьютер: Идентификатор приложения: Описание ошибки:	Неуспешная попытка при удалении лицензии пользователем. Возможные причины: • Недостаточно прав. • Сервер Indeed AM неактивен. • Повреждено хранилище данных.
2048	Ошибка	Ошибка при попытке сервера удалить лицензию целевого пользователя. Идентификатор приложения: Целевой пользователь: Описание ошибки:	Неуспешная попытка при удалении лицензии сервером.

2049	Ошибка	Ошибка при создании политики. Идентификатор: Имя: Описание: Приоритет: Новые объекты каталога: Новые приложения: Ошибка: Приложение: Инициатор: Компьютер:	Неуспешное создание политики.
2050	Ошибка	Ошибка при удалении политики. Идентификатор: Имя: Описание: Приоритет: Удалённые объекты каталога: Удалённые приложения: Ошибка: Приложение: Инициатор: Компьютер:	Неуспешное удаление политики.

2051	Ошибка	Ошибка при изменении политики. Идентификатор: Имя: Описание: Приоритет: Новые объекты каталога: Новые приложения: Удалённые объекты каталога: Удалённые приложения: Ошибка: Приложение: Инициатор: Компьютер:	Неуспешное изменение политики.
2052	Ошибка	Сервер Indeed-Id не найден. Компьютер: Описание ошибки: Код ошибки:	Ошибка при попытке подключения к серверу Indeed AM • Указан неверный URL • Проблема в DNS
2053	Ошибка	Не удалось сменить пароль пользователя. Инициатор: Компьютер: Клиентский пользователь: Клиентский компьютер: Описание ошибки: Код ошибки:	Неуспешная смена пароля пользователя.

2054	Ошибка	Не удалось сменить пароль пользователя автоматически. Инициатор: Компьютер: Клиентский пользователь: Клиентский компьютер: Описание ошибки: Код ошибки:	Неуспешная смена пароля пользователя автоматически.
2055	Ошибка	Не удалось синхронизировать пароль пользователя. Инициатор: Компьютер: Клиентский пользователь: Клиентский компьютер: Описание ошибки: Код ошибки:	Ошибка синхронизации доменного пароля пользователя с паролем в хранилище Indeed. Возможные причины: • Сервер Indeed недоступен. • Повреждено хранилище данных.
2058	Ошибка	Изменение настроек метода аутентификации: Приложение: Инициатор: Компьютер: Провайдер: Настройки: Описание ошибки:	Неуспешное изменение настроек метода аутентификации.

2061	Ошибка	Изменение настройки прав аутентификатора - Сбой: Политика: Пользователь: Обучение: Переобучение: Удаление: Изменение комментария только при обучении: Изменение комментария: Приложение: Инициатор: Компьютер: Ошибка:	Неуспешное изменение настройки прав аутентификатора.
------	--------	--	---

2062	Ошибка	Ошибка создания настройки учётной записи. Политика: Целевой пользователь: Роль: 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 учётной записи
------	--------	---	--

2063	Ошибка	Ошибка удаления настройки учётной записи. Политика: Целевой пользователь: Роль: 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 удаление настройки учётной записи.
------	--------	---	--

2064	Ошибка	Ошибка изменения настройки учётной записи. Политика: Целевой пользователь: Роль: 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 изменение настройки учётной записи.
2067	Ошибка	Изменение настроек метода аутентификации для пользователя: Целевой пользователь: Провайдер: Приложение: Инициатор: Компьютер: Настройки: Описание ошибки:	Неуспешное изменение настроек метода аутентификации для пользователя.

2070	Ошибка	Изменение настроек метода аутентификации для модуля: Модуль: Провайдер: Политика: Id политики: Приложение: Инициатор: Компьютер: Настройки: Описание ошибки:	Неуспешное изменение настроек метода аутентификации для модуля
2071	Ошибка	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	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.
2073	Ошибка	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	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	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	Ошибка	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	Ошибка	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]).
2078	Ошибка	Ошибка изменения политики метода аутентификации: Провайдер: Политика: Id политики: Приложение: Инициатор: Компьютер: Настройки: Описание ошибки:	Неуспешное изменение политики метода аутентификации.

2079	Ошибка	Ошибка при сохранении пароля пользователя в базе данных Indeed-Id 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	Ошибка при загрузке данных ESSO для аутентифицировавшегося пользователя Инициатор: Компьютер: 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	Ошибка	Обнаружен сбой в Indeed-Id ESSO Agent Инициатор: Компьютер: Компьютер: Описание ошибки: Код ошибки:	Не удалось завершить процесс приложения.

2082	Ошибка	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	Ошибка при добавлении нового приложения. Название: Описание: Модуль интеграции: Приложение: Инициатор: Компьютер: Описание ошибки:	Неуспешная попытка добавления нового приложения: • Недостаточно прав для выполнения операции. • Отсутствует связь с сервером Indeed AM.
2084	Ошибка	Ошибка при удалении приложения. Название: Описание: Модуль интеграции: Приложение: Инициатор: Компьютер: Описание ошибки:	Неуспешная попытка удаления приложения: • Недостаточно прав для выполнения операции. • Отсутствует связь с сервером Indeed AM.

2085	Ошибка	Ошибка при изменении параметров приложения. Название: Описание: Список изменений: Приложение: Инициатор: Компьютер: Описание ошибки:	Неуспешная попытка изменения параметров приложения: • Недостаточно прав для выполнения операции. • Отсутствует связь с сервером Indeed AM.
2086	Ошибка	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	Ошибка при попытке отправить сообщение Telegram. Приложение: Инициатор: Способ аутентификации: Описание ошибки:	Произошла одна или несколько ошибок. Произошла ошибка при отправке запроса: • нет доступа / связи с сервера AM core до api.telegram.org.
2088	Ошибка	Ошибка регистрации контакта Telegram. Пользователь: Инициатор: Описание ошибки: Телефон:	Доступ запрещен. Пользователь не может быть авторизован. Произошла одна или несколько ошибок. У пользователя нет следующих прав: <i>ReadUserAuthenticators</i> для приложения Authenticator Management: • сервисная УЗ Telegram не добавлена в глобальные администраторы Management Console.

События компонента Indeed AirKey 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 AirKey	Запрос на аутентификацию пользователя {userLogin} отправлен. Приложение: {appld}
1001	Информация	Indeed AirKey	Запрос на регистрацию пользователя {userLogin} отправлен. Приложение: {appld}
1002	Информация	Indeed AirKey	Обработан ответ пользователя {userLogin} на запрос аутентификации. Приложение: {appld}. Результат: {state}. Сообщение: {message}
1003	Информация	Indeed AirKey	Запрос на установку сертификата пользователю {userLogin} отправлен. Приложение: {appld}
1004	Информация	Indeed AirKey	Регистрация пользователя {userLogin} успешно завершена. Приложение: {appld}
1005	Информация	Indeed AirKey	Удаление пользователя {userLogin} успешно завершено. Приложение: {appld}
2000	Ошибка	Indeed AirKey	Ошибка при отправке запроса на аутентификацию пользователя {userLogin}. Приложение: {appld}. Ошибка:
2001	Ошибка	Indeed AirKey	Ошибка при отправке запроса на регистрацию пользователя {userLogin}. Приложение: {appld}. Ошибка:
2002	Ошибка	Indeed AirKey	Ошибка при отправке запроса на установку сертификата пользователю {userLogin}. Приложение: {appld}. Ошибка:
2003	Ошибка	Indeed AirKey	Ошибка при регистрации пользователя {userLogin}. Приложение: {appld}. Ошибка:
2004	Ошибка	Indeed AirKey	Ошибка при удалении пользователя {userLogin}. Приложение: {appld}. Ошибка:

Конфигурация

Права доступа

Роли

В данном разделе представлены описания к ролям доступа системы Indeed AM: **Администратор, Оператор, Инспектор**. Для подробного просмотра прав доступа необходимо нажать на соответствующую роль.

МС / Конфигурация / Роли

Конфигурация - Роли

Права доступа	ИМЯ РОЛИ	ОПИСАНИЕ
Роли	Администратор	Полный доступ ко всем функциям и настройкам системы
Глобальные администраторы	Оператор	Права только на изменение настроек пользователей и устройств аутентификации
Аутентификаторы	Инспектор	Доступ на чтение всех данных и настроек системы
Multi-factor authentication		
Push-аутентификация		

МС / Конфигурация / Роли / Администратор

Конфигурация - Администратор

Права доступа	Общая информация	
Роли	Название	Администратор
Глобальные администраторы	Описание	Полный доступ ко всем функциям и настройкам системы
Аутентификаторы	Права доступа	
Multi-factor authentication	ОПЕРАЦИЯ	СТАТУС
Push-аутентификация	Регистрация аутентификаторов	
Одноразовый пароль по SMS	Регистрация первого аутентификатора	☒
Пароль Passcode	Регистрация любого аутентификатора	☒
Пароль Windows	Аутентификаторы пользователя	
Программный генератор TOTP	Просмотр аутентификаторов пользователя	☒
	Отключение аутентификаторов пользователя	☒
	Включение аутентификаторов пользователя	☒

Глобальные администраторы

В данном разделе отображаются глобальные администраторы системы для каждой подгруппы. Для добавления администратора выполните следующие действия:

1. Нажмите "**Добавить**" и выберите необходимую роль.
2. Выберите тип объекта - Пользователь или Группа.
3. Укажите расположение - Весь пользовательский каталог или отдельный контейнер.
4. В поле "**Название**" введите имя или часть имени для поиска.
5. Нажмите "**Поиск**".
6. Выберите необходимого пользователя и нажмите "**Добавить**".

+ Добавить
✕ Отмена

Название

Тип объекта

Пользователь
Группа

Расположение

Весь каталог

Выбрать

Поиск

Сбросить

НАЗВАНИЕ	ТИП ОБЪЕКТА	РАСПОЛОЖЕНИЕ
☒ INDEED\Inspector-Indeed	Пользователь	indeed.local/Indeed/UsersIndeed/Inspector

7. После успешного добавления объект будет отображаться в соответствующем разделе.

Конфигурация - Глобальные администраторы

Права доступа	+ Добавить ✕ Удалить			
Роли				
Глобальные администраторы	ИМЯ ▾	ГРУППА БЕЗОПАСНОСТИ ⚙	ТИП ОБЪЕКТА	РАСПОЛОЖЕНИЕ
Аутентификаторы	Администратор			
Multi-factor authentication	☐ Admin-Indeed	Администратор	Пользователь	indeed.local/Indeed/UsersIndeed
Push-аутентификация	Оператор			
Одноразовый пароль по SMS	☐ Operator	Оператор	Пользователь	indeed.local/Indeed/UsersIndeed
Пароль Passcode	Инспектор			
Пароль Windows	☐ Inspector	Инспектор	Пользователь	indeed.local/Indeed/UsersIndeed

Аутентификаторы

В данном разделе задается настройка для автоматической блокировки и разблокировки аутентификаторов. Для настройки выполните следующие действия:

1. Выберите необходимый аутентификатор.
2. Для параметра **"Блокировать способ аутентификации в случае серии неудачных попыток"** установите значение **"Да"**.
3. Для параметра **"Количество попыток аутентификации до блокировки"** установите необходимое количество попыток. Значение по умолчанию: **5**
4. Для параметра **"Сброс счетчика блокировки через (минут)"** установите необходимое количество. Значение по умолчанию: **5**
5. Для параметра **"Таймаут до разблокировки способа входа (минут)"** установите необходимое количество. Значение по умолчанию: **5**
6. Нажмите **"Сохранить"**.

Конфигурация - Push-аутентификация

Права доступа
Роли
Глобальные администраторы
Аутентификаторы
Multi-factor authentication
Push-аутентификация
Одноразовый пароль по SMS
Пароль Passcode
Пароль Windows
Программный генератор TOTP

Сохранить
Отмена

Блокировать способ аутентификации в случае серии неудачных попыток

Да
Нет

Количество попыток аутентификации до блокировки ⓘ

5

Сброс счетчика блокировки через (минут) ⓘ

5

Таймаут до разблокировки способа входа (минут) ⓘ

5

Таблица с правами доступа

Операция	Администратор	Оператор	Инспектор
Регистрация аутентификаторов			
Регистрация первого аутентификатора	✓	✓	
Регистрация любого аутентификатора	✓		
Аутентификаторы пользователя			
Просмотр аутентификаторов пользователя	✓	✓	✓

Отключение аутентификаторов пользователя	✓	✓	
Включение аутентификаторов пользователя	✓	✓	
Удаление аутентификаторов пользователя	✓	✓	
Разблокирование методов аутентификации пользователя	✓	✓	
Получение методов аутентификации пользователя	✓	✓	✓
Включение методов аутентификации пользователя	✓	✓	
Выключение методов аутентификации пользователя	✓	✓	
Просмотр состояния метода аутентификации пользователя	✓	✓	✓
Изменение настроек метода аутентификации	✓		
Просмотр настроек метода аутентификации	✓		✓
Изменение настроек метода аутентификации пользователя	✓	✓	
Просмотр настроек метода аутентификации пользователя	✓	✓	✓
Изменение настроек метода аутентификации приложения	✓	✓	
Просмотр настроек метода аутентификации приложения	✓	✓	✓
Изменение прав доступа для аутентификатора	✓	✓	
Просмотр прав доступа для аутентификатора	✓	✓	✓
Изменение настроек метода аутентификации в политике	✓	✓	
Просмотр настроек метода аутентификации в политике	✓	✓	✓
Лицензии			

Регистрация лицензий	✓		
Отмена регистрации лицензий	✓		
Просмотр зарегистрированных лицензий	✓	✓	✓
Выдача лицензий пользователю	✓	✓	
Отзыв лицензии у пользователя	✓	✓	
Просмотр лицензий пользователя	✓	✓	✓
Административный доступ			
Добавление объекта каталога в группу доступа	✓		
Удаление объекта каталога из группы доступа	✓		
Просмотр членов группы доступа	✓	✓	✓
Устройства аутентификации			
Регистрация устройства	✓		
Обновление устройства	✓		
Просмотр списка устройств	✓	✓	✓
Удаление устройства	✓		
Политики			
Создание политики	✓		
Изменение политики	✓		
Удаление политики	✓		

Просмотр списка политик	✓	✓	✓
Просмотр списка пользователей политики	✓	✓	✓
Изменение списка пользователей политики	✓	✓	
Просмотр списка приложений политики	✓	✓	
Изменение списка приложений политики	✓		
Просмотр приоритета политики	✓	✓	✓
Изменение приоритета политики	✓		
Кэширование данных пользователя на ПК			
Включение кэширования	✓	✓	
Отключение кэширования	✓	✓	
Проверка состояния кэша	✓	✓	
Изменение настроек кэширования	✓		
Просмотр настроек кэширования	✓	✓	✓
Учетные записи ESSO			
Добавление учетной записи	✓		
Удаление учетной записи	✓		
Просмотр учетных записей пользователя	✓	✓	✓
Чтения состояния учетных записей пользователя	✓	✓	
Изменение пароля учетных записей пользователя	✓		

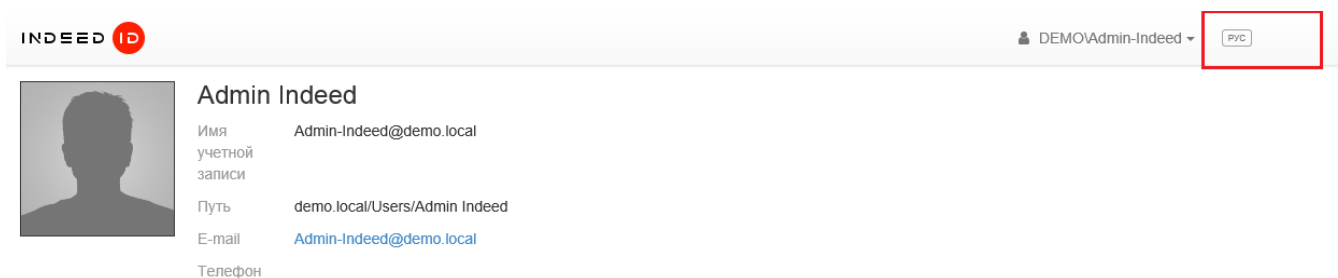
Просмотр состояния пароля аккаунта пользователя	✓	✓	✓
Изменение имени учетной записи пользователя	✓	✓	
Просмотр имени учетной записи пользователя	✓	✓	✓
Изменение настроек учетной записи пользователя	✓	✓	
Просмотр настроек учетной записи пользователя	✓	✓	✓
Изменение дополнительных данных учетной записи пользователя	✓	✓	
Просмотр дополнительных данных учетной записи пользователя	✓	✓	✓
Установка случайного пароля учетной записи пользователя	✓		
Изменение пароля учетной записи	✓		
Приложения			
Просмотр списка бизнес-приложений	✓	✓	✓
Создание бизнес-приложения	✓		
Изменение бизнес-приложения	✓	✓	
Удаление бизнес-приложения	✓		

Консоль управления аутентификаторами пользователя

- [Локализация \(User Console\)](#)
- [Управление аутентификаторами \(User Console\)](#)
- [Карточка пользователя \(User Console\)](#)

Локализация (User Console)

Смена языка осуществляется через нажатие в правом верхнем углу кнопки с выбранным языком.



Для отключения возможности смены языка выполните следующие действия:

1. Откройте конфигурационный файл консоли **Web.config** (C:\inetpub\wwwroot\am\uc\Web.config).
2. Укажите **false** для параметра **isEnabled** тега **amCulture**.

Пример

```
<amCulture isEnabled="false" />
```

3. Перезапустите IIS сервер.

Управление аутентификаторами (User Console)

Информация

Для управления аутентификаторами у пользователя должны быть необходимые права доступа. Права по умолчанию позволяют **только зарегистрировать** аутентификатор.

На странице пользователя содержится информация о количестве зарегистрированных аутентификаторов пользователя и их параметры.



Имя
учетной
записи

Admin-Indeed@ind.loc

Путь

ind.loc/Users/Admin Indeed

Е-mail

Admin-Indeed@ind.loc

Телефон

[+789524855904](tel:+789524855904)

Аутентификаторы 1

Лицензии

Настройки

 Windows Password

Без регистрации



 Passcode



 Software TOTP

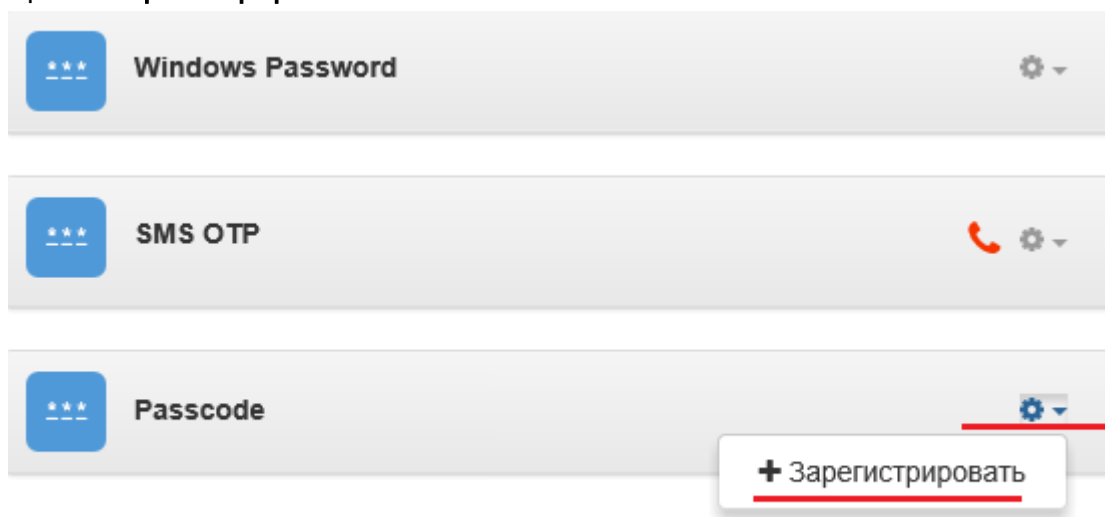


Дата регистрации	Комментарий	
12.11.2018 12:21:49	<Не задан>	

Регистрация аутентификаторов

1. Выберите необходимый аутентификатор.
2. Нажмите значок шестеренки.

3. Выберите "Зарегистрировать".



4. Введите данные для обучения выбранного аутентификатора и нажмите "Сохранить".



Примечание

Окна и действия для обучения могут отличаться в зависимости от аутентификатора.

Passcode ×

Пароль

Подтвердите пароль

Комментарий

 ×

Отмена

Сохранить

5. После успешной регистрации аутентификатор отобразится как зарегистрированный.

 Информация

Если у пользователя зарегистрировано максимальное количество аутентификаторов, то регистрация завершится ошибкой: **"Доступ запрещен: Достигнуто максимальное количество аутентификаторов."**

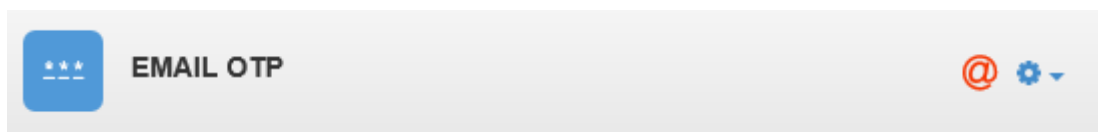
 Passcode 		
Дата регистрации		Комментарий
16.04.2019	14:07:02	q1q2e3e4 

6. Если был удален провайдер, имеющий зарегистрированные аутентификаторы, то в правой части панели аутентификатора будет отображаться значок **"Недоступно"**.

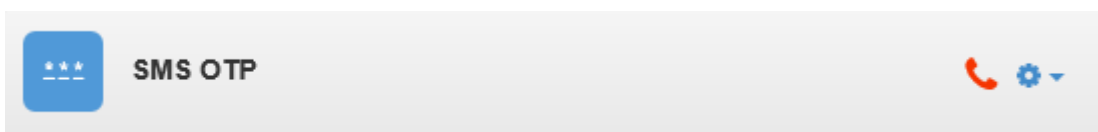
 Software TOTP  		
Дата регистрации		Комментарий
12.03.2019	12:48:30	<Не задан> 

7. Провайдеры **Email** и **SMS** регистрируются автоматически, если у пользователя задан **email** или **номер телефона** соответственно.

- а. Если у пользователя после установки **Email** провайдера не был задан email, то аутентификатор не будет использоваться. В правой части панели аутентификатора будет отображаться значок "@".



- б. Если у пользователя после установки **SMS** провайдера не был задан номер телефона, то аутентификатор не будет использоваться. В правой части панели аутентификатора будет отображаться значок телефонной трубки.



Автоматическая блокировка и разблокировка аутентификаторов

Через GPO

Информация

Автоматическая блокировка/разблокировка настраивается через групповые политики. Перед настройкой групповой политики необходимо добавить в список административных шаблонов шаблоны политик Indeed AM. Файлы шаблонов политик входят в состав дистрибутива провайдера и расположены в каталоге *Indeed Enterprise Server\<Номер версии>\Misc\Templates*.

Для настройки необходимо открыть политику "Блокировка способов входа" (Конфигурация компьютера/Политики/Административные шаблоны/Indeed ID/Server).

Политика применяется к серверам Indeed и позволяет настроить автоматическую блокировку/разблокировку аутентификаторов.

Не задан (Not Configured) или Отключен (Disabled)

Если политика не задана или отключена, то блокировка аутентификаторов не будет осуществляться.

Включен (Enabled)

Блокировка/Разблокировка аутентификаторов будет осуществляться согласно заданных в политике параметров.

Параметры:

- **Количество попыток аутентификации до блокировки.**
Настройка определяет количество неудачных попыток аутентификации до блокировки способа входа. Заблокированный способ входа становится недоступным для использования до момента разблокировки администратором или до истечения таймаута до разблокировки. Если установить это значение равным 0, то способ входа никогда не будет заблокирован.
- **Таймаут до разблокировки способа входа.**
Настройка задает время таймаута в минутах, на которое заданный способ входа будет заблокирован. По истечении таймаута способ входа будет автоматически разблокирован. Если для длительности блокировки способа входа установлено значение 0, способ входа останется заблокированным до тех пор, пока не будет явно разблокирован администратором.
- **Сброс счетчика блокировки через.**
Этот параметр определяет, сколько минут должно пройти после неудачной попытки входа, прежде чем счетчик неудачных попыток будет сброшен в 0. Этот параметр может принимать значения от 1 до 99 999 минут. Если количество попыток аутентификации до блокировки определено, то данный интервал сброса не должен быть больше параметра "Таймаут до разблокировки способа входа".

Блокировка способов входа

Блокировка способов входа

Предыдущий параметр Следующий параметр

☐ Не задано
 ☒ Включено
 ☐ Отключено

Комментарий:

Требования к версии: Windows XP и более поздние версии

Параметры:

Справка:

Количество попыток аутентификации до блокировки: 1

Таймаут до разблокировки способа входа (минут): 0

Сброс счетчика блокировки через (минут): 1

Настройка задает время таймаута в минутах, на которое заданный способ входа будет заблокирован. По истечению таймаута способ входа будет автоматически разблокирован. Если для длительности блокировки способа входа установлено значение 0, способ входа останется заблокированным до тех пор, пока не будет явно разблокирован администратором.

Количество попыток аутентификации до блокировки

Настройка определяет количество неудачных попыток аутентификации до блокировки способа входа. Заблокированный способ входа становится недоступным для использования до момента разблокировки администратором или до истечения таймаута до разблокировки. Если установить это значение равным 0, то способ входа никогда не будет заблокирован.

Сброс счетчика блокировки через

Этот параметр определяет, сколько минут должно пройти после неудачной попытки входа, прежде чем счетчик неудачных попыток будет сброшен в 0. Этот параметр может принимать значения от 1 до 99 999 минут. Если количество попыток аутентификации до блокировки определено, то данный интервал сброса не должен быть больше параметра "Таймаут до разблокировки способа входа".

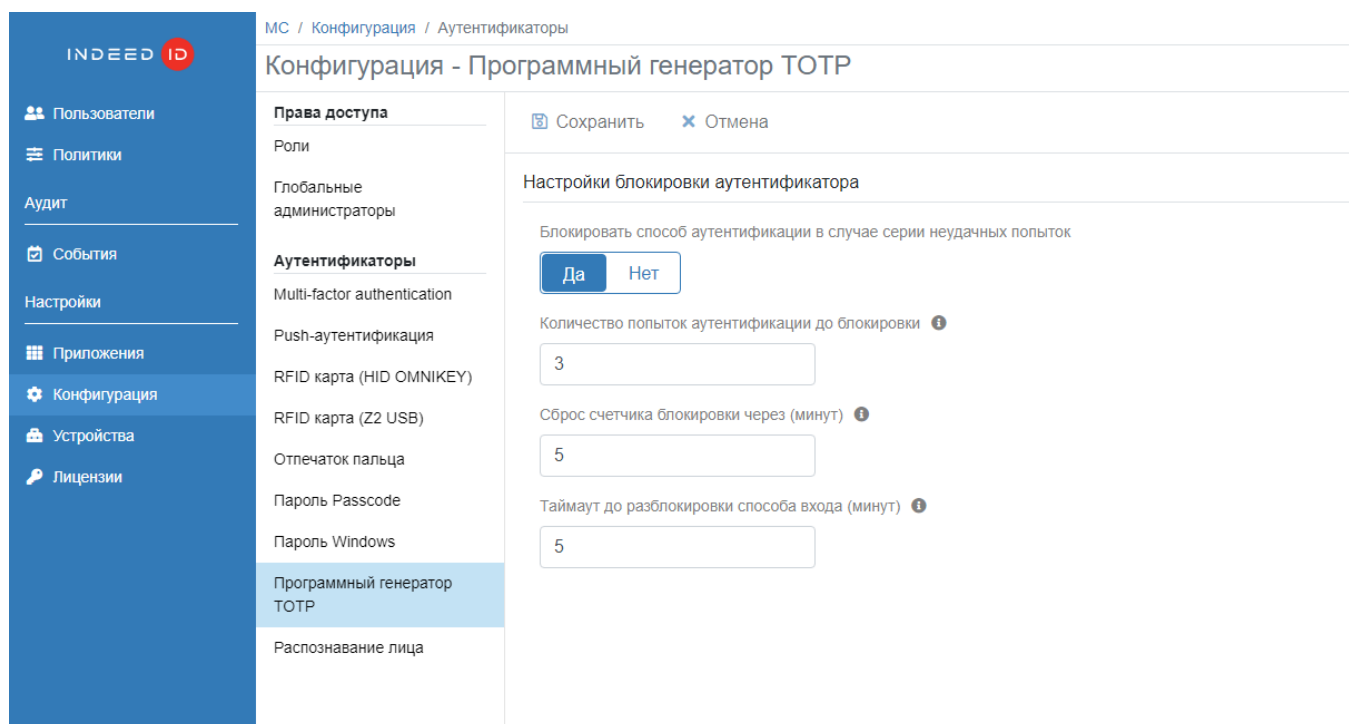
OK Отмена Применить

Если аутентификатор был заблокирован через групповую политику, то в правой части панели аутентификатора будет отображаться значок "Блокировки".

Software TOTP		
ОТР Software TOTP 🔒 ⚙️		
Дата регистрации		Комментарий
14.03.2019	11:22:21	<Не задан>
		⚙️

Через Management Console

Для настройки необходимо открыть **Management Console**, зайти в меню "Конфигурация" и выбрать необходимый аутентификатор.



Параметры:

- **Количество попыток аутентификации до блокировки.**

Настройка определяет количество неудачных попыток аутентификации до блокировки способа входа. Заблокированный способ входа становится недоступным для использования до момента разблокировки администратором или до истечения таймаута до разблокировки. Если установить это значение равным 0, то способ входа никогда не будет заблокирован.

- **Сброс счетчика блокировки через.**

Этот параметр определяет, сколько минут должно пройти после неудачной попытки входа, прежде чем счетчик неудачных попыток будет сброшен в 0. Этот параметр может принимать значения от 1 до 99 999 минут. Если количество попыток аутентификации до блокировки определено, то данный интервал сброса не должен быть больше параметра "Таймаут до разблокировки способа входа".

- **Таймаут до разблокировки способа входа.**

Настройка задает время таймаута в минутах, на которое заданный способ входа будет заблокирован. По истечении таймаута способ входа будет автоматически разблокирован. Если для длительности блокировки способа входа установлено значение 0, способ входа останется заблокированным до тех пор, пока не будет явно разблокирован администратором.

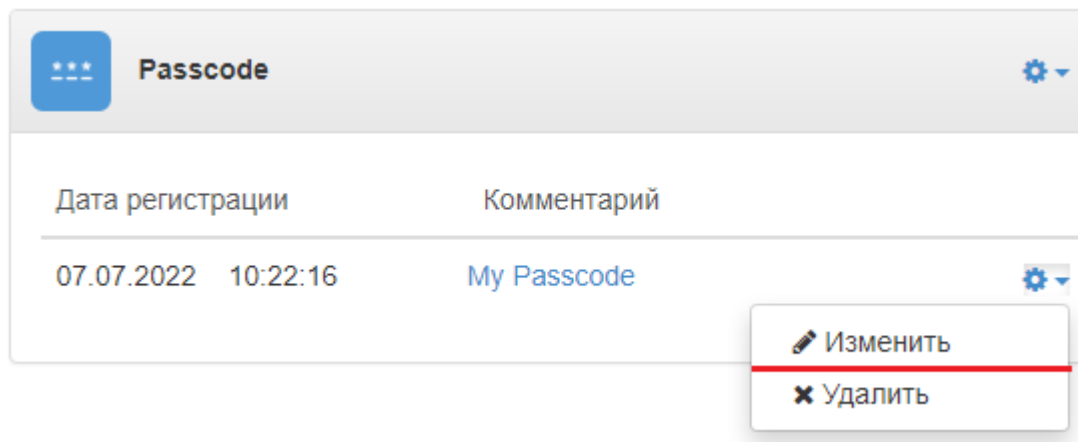
Изменение и удаление аутентификатора

1. Выберите необходимый аутентификатор.

2. Нажмите значок шестеренки.

а. **Изменение аутентификатора.**

- Для изменения аутентификатора выберите **"Изменить"**.



Дата регистрации	Комментарий
07.07.2022 10:22:16	My Passcode

Изменить

Удалить

- Введите новые данные для аутентификатора и нажмите **"Сохранить"**.

Passcode

Пароль

••••••••

Подтвердите пароль

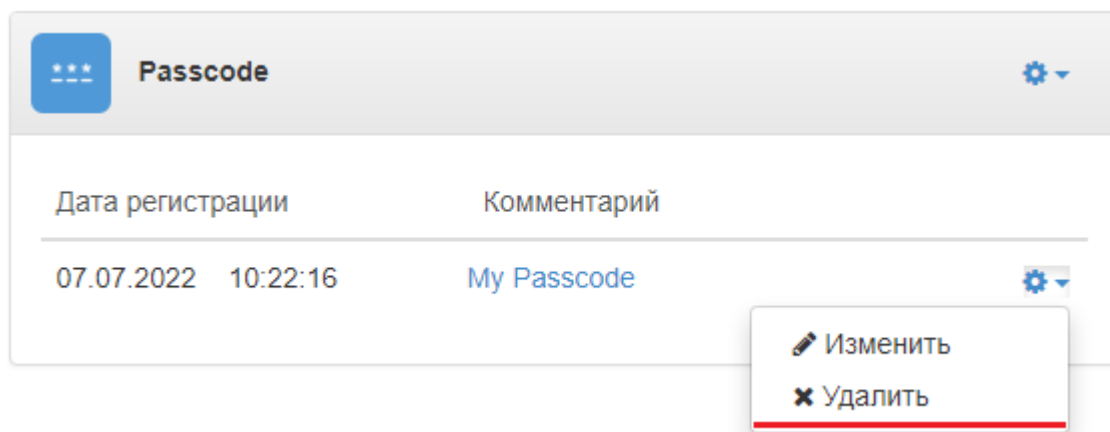
••••••••

Отмена

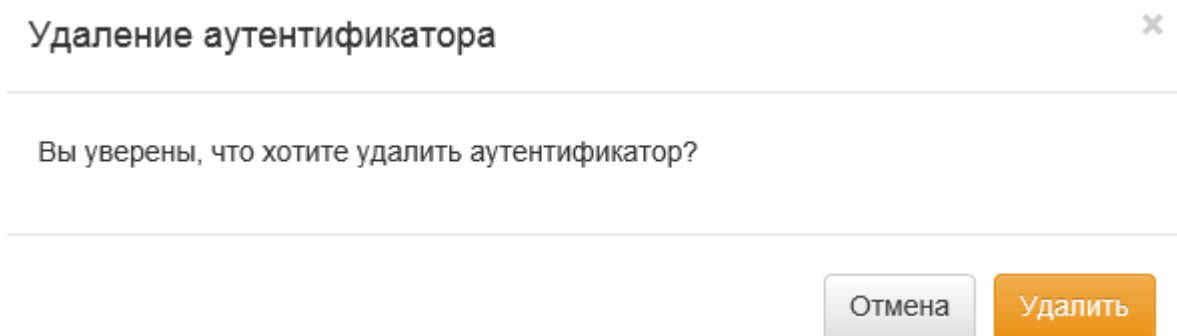
Сохранить

в. Удаление аутентификатора.

- Для удаления аутентификатора выберите "Удалить".



- В окне подтверждения нажмите "Удалить".



Карточка пользователя (User Console)

В карточке пользователя содержится информация о пользователе:

- Данные из профиля Active Directory
 - 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 по зарегистрированным аутентификаторам.

INDEED 

DEMO\Admin-Indeed ▾ Р/С



Admin Indeed

Имя
учетной
записи

Admin-Indeed@demo.local

Путь

demo.local/Users/Admin Indeed

E-mail

Admin-Indeed@demo.local

Телефон

Аутентификаторы 1

EMAIL OTP



Software TOTP



Hardware OTP



Hardware TOTP



Windows Password



SMS OTP



Passcode



Дата регистрации		Комментарий	
10.04.2019	13:08:11	q1q2e3e4	

Утилита управления аутентификаторами

Вы можете управлять аутентификаторами с помощью приложения **Indeed AM Управление аутентификаторами**. Данное приложение позволяет добавлять новые аутентификаторы, редактировать, проверять и удалять имеющиеся.



Информация

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** (Программы > **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 часть функций будет недоступна.

Выполните требуемые действия (в зависимости от выбранного способа входа).



Информация

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.

3. После успешной аутентификации отображается окно **Управление аутентификаторами**.

Информация по работе с утилитой доступна в данном разделе:

- [Удаление аутентификатора](#)
- [Проверка аутентификатора](#)
- [Редактирование аутентификатора](#)
- [Добавление аутентификатора](#)

Удаление аутентификатора

Для удаления аутентификатора выполните следующие действия:

В окне **Управление аутентификаторами** выберите аутентификатор и нажмите **Удалить**.

Для подтверждения действия нажмите **Да**.

IID\user

INDEED ID

Управление аутентификаторами

→ [Смарт-карта или USB-ключ](#)
rutoken

→ **Пароль**
pascode
[Изменить](#) | [Проверить](#) | [Удалить](#)

+ [Добавить способ входа](#)

[Завершить](#)

Подтверждение

?

Вы действительно хотите удалить этот способ входа?

Да

Нет

Если для вашей учетной записи был сгенерирован случайный пароль, при попытке удалить единственный имеющийся аутентификатор система отображает диалог-предупреждение:

Подтверждение

?

Вам разрешена автоматическая генерация пароля.

После удаления последнего способа входа вы не сможете выполнить вход по паролю.

Продолжить?

Да

Нет

Информация

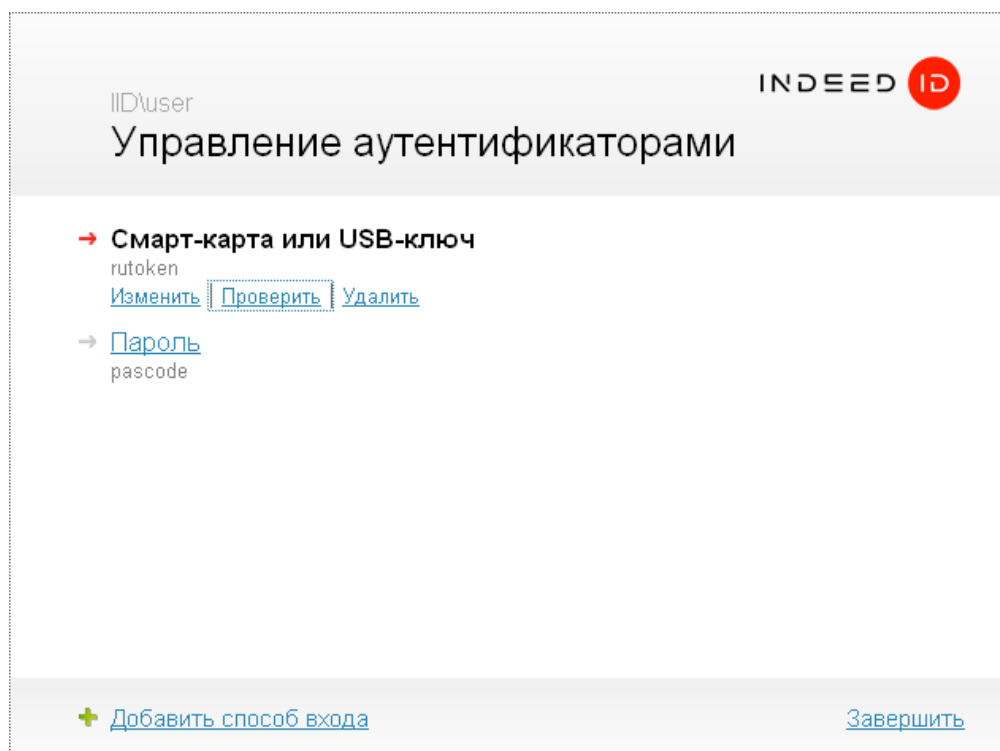
Если вы удалили все аутентификаторы и не можете выполнить вход в систему по паролю, обратитесь к администратору системы. После сброса пароля вы снова сможете выполнить вход в систему и зарегистрировать новые аутентификаторы.

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.

Проверка аутентификатора

Для проверки аутентификатора выполните следующие действия:

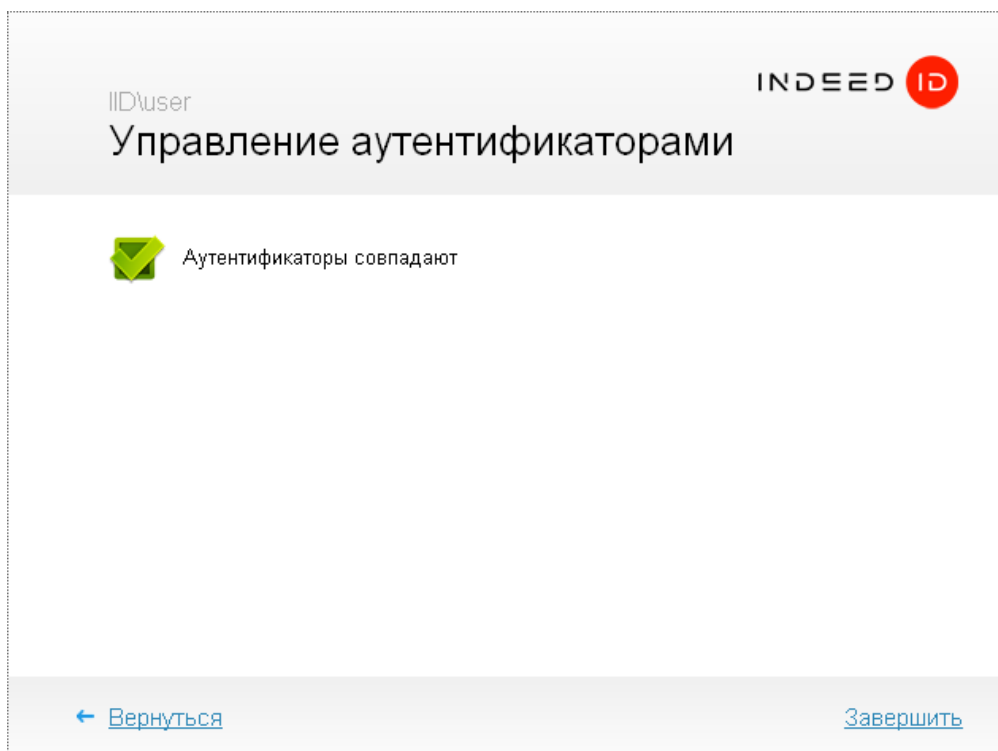
В окне **Управление аутентификаторами** выберите аутентификатор и нажмите **Проверить**.



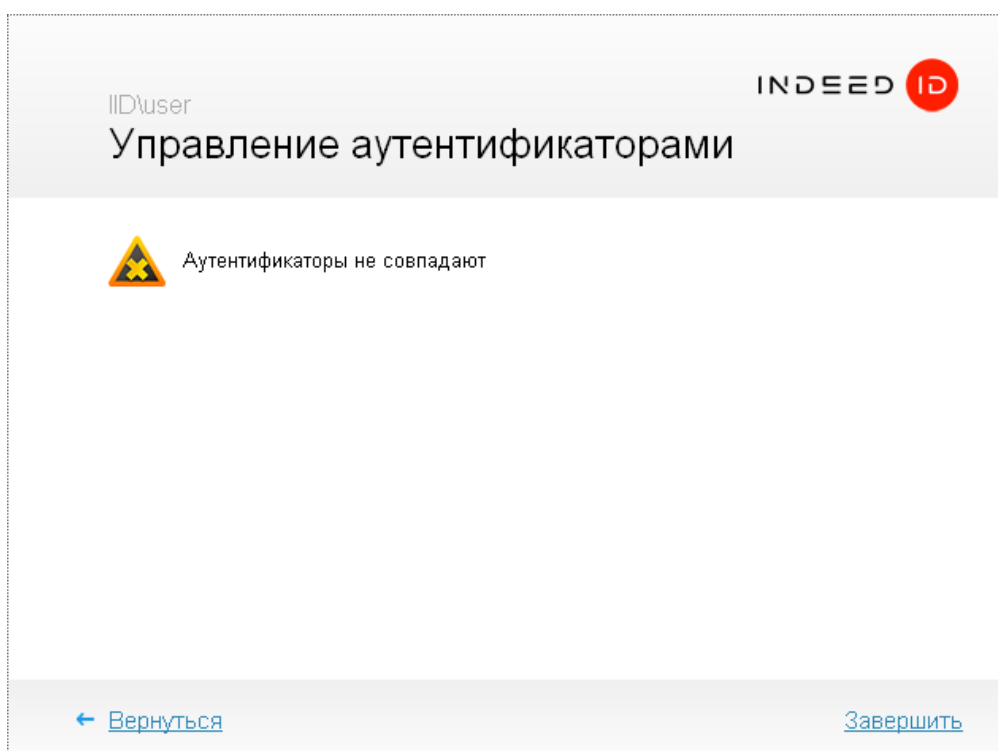
После нажатия на ссылку **Проверить** в окне **Управление аутентификаторами** отображаются инструкции по регистрации аутентификатора. Внешний вид окна и текст подсказок зависят от выбранного типа аутентификатора. Выполните требуемые действия.

После завершения проверки в окне **Управление аутентификаторами** отображается сообщение о результате.

- Если аутентификаторы совпадают



- Если аутентификаторы не совпадают



Если аутентификаторы не совпадают, нажмите **Вернуться** и повторите процедуру проверки или заново обучите аутентификатор.

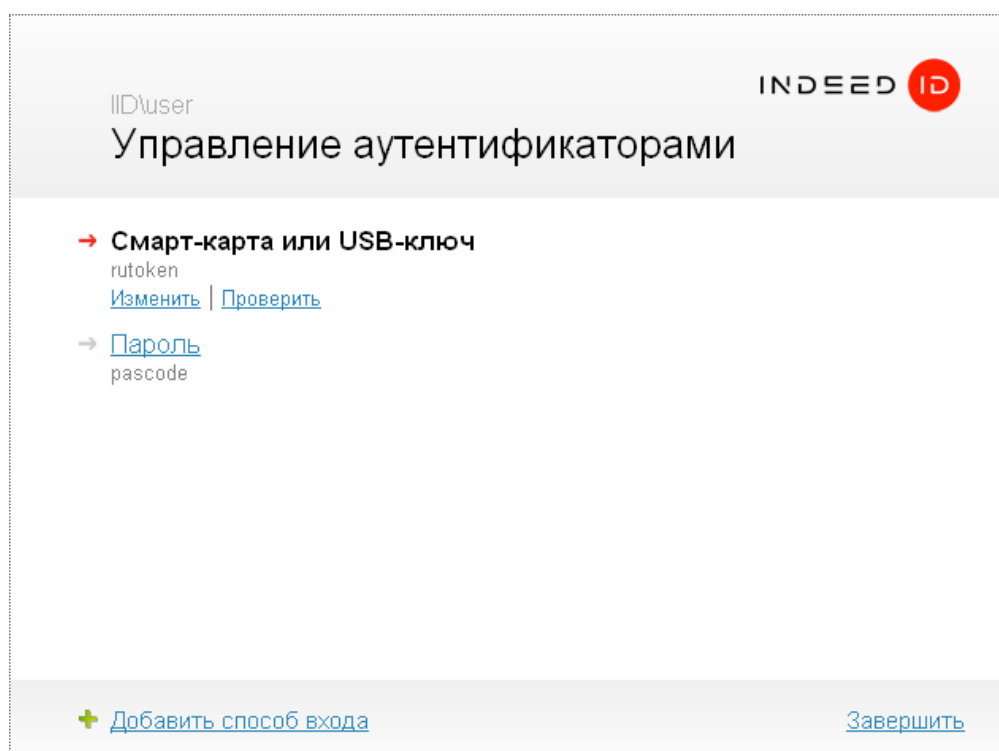
Редактирование аутентификатора

Информация

Вы можете отредактировать (повторно зарегистрировать) аутентификатор или изменить только комментарий к аутентификатору (если это действие разрешено администратором системы).

Для редактирования аутентификатора выполните следующие действия:

В окне **Управление аутентификаторами** выберите аутентификатор и нажмите **Изменить**.



Выполните одно из указанных действий:

- Чтобы отредактировать только комментарий к аутентификатору, введите его в соответствующее поле и нажмите **Сохранить**.

IID\user

INDEED ID

Управление аутентификаторами



Вы можете изменить комментарий к аутентификатору:

rutoken

Сохранить

[← Вернуться](#)[Завершить](#)

- Чтобы перейти к редактированию самого аутентификатора, нажмите **Задать заново**. После нажатия на ссылку **Задать заново** в окне отобразятся инструкции по регистрации аутентификатора. Внешний вид окна и текст подсказок зависят от выбранного типа аутентификатора. выполните требуемые действия.

IID\user

INDEED ID

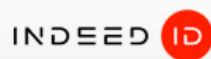
Управление аутентификаторами

→ **Смарт-карта или USB-ключ**
rutoken
[Изменить](#) | [Проверить](#) | [Удалить](#)

→ **Пароль**
pascode

[+ Добавить способ входа](#)[Завершить](#)

IID\user



Управление аутентификаторами



[Задать заново](#) →

Вы можете изменить комментарий к аутентификатору:

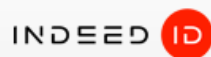
rutoken

Сохранить

[← Вернуться](#)

[Завершить](#)

IID\user



Управление аутентификаторами



Выберите смарт-карту или токен

Rutoken S : 0783311828

Ok

[← Вернуться](#)

[Завершить](#)

После успешной регистрации аутентификатора в окне нажмите **Сохранить**.

Управление аутентификаторами

[Задать заново](#) →

Вы можете изменить комментарий к аутентификатору:

[← Вернуться](#)[Завершить](#)

Добавление аутентификатора

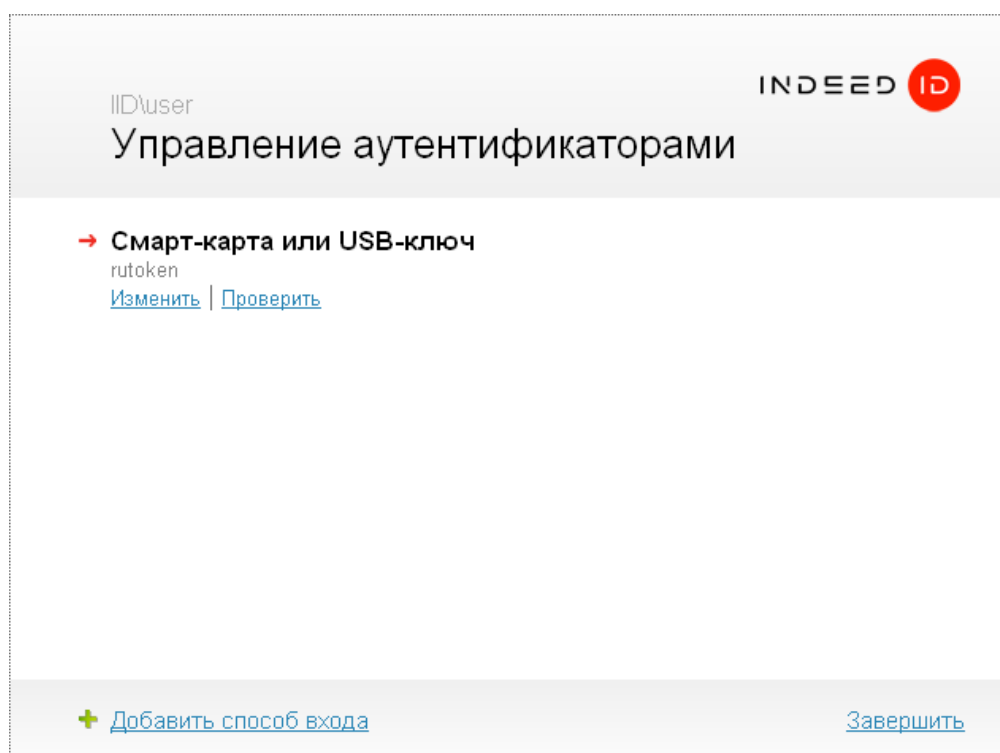
Информация

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:

В окне **Управление аутентификаторами** нажмите **Добавить способ входа**



Выберите технологию аутентификации. Например, «Пароль».

IID\user

INDEED ID

Управление аутентификаторами

Выберите технологию аутентификации:

[Пароль →](#)
(Passcode)

[Смарт-карта или USB-ключ →](#)
(Смарт-карта или USB-ключ)

[← Вернуться](#)[Завершить](#)

Следуйте инструкциям по регистрации аутентификатора. Внешний вид окна и текст подсказок зависят от выбранного типа аутентификатора.

IID\user

INDEED ID

Управление аутентификаторами

Введите свой пароль

Пароль:

Подтверждение:

[← Вернуться](#)[Завершить](#)

После успешной регистрации аутентификатора в окне **Управление аутентификаторами** отображается сообщение **"Новый аутентификатор успешно обучен"**.

IID\user

INDEED ID

Управление аутентификаторами



Новый аутентификатор успешно обучен

Все готово для регистрации аутентификатора в системе.
Перед сохранением вы можете задать комментарий
к аутентификатору:

[← Вернуться](#)[Завершить](#)

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 на 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.

Предыдущие версии

- [Indeed Access Manager 8.0](#)
- [Indeed Access Manager 7.2](#)
- [Indeed Access Manager 7.1](#)
- [Indeed Access Manager 7.0](#)