



# Indeed Access Manager

Техническая документация

Версия: 8.2

Дата: 05.05.2026

# Содержание

|                                                                 |     |
|-----------------------------------------------------------------|-----|
| <b>О продукте</b>                                               | 7   |
| Базовые компоненты                                              | 8   |
| <b>Модули интеграции</b>                                        | 10  |
| Indeed ADFS Extension                                           | 11  |
| Indeed Enterprise Single Sign-On                                | 13  |
| Indeed Identity Provider                                        | 16  |
| Indeed IIS Extension                                            | 18  |
| Indeed NPS RADIUS Extension                                     | 20  |
| Indeed RDP Windows Logon                                        | 22  |
| Indeed Windows Logon                                            | 24  |
| Технологии аутентификации                                       | 27  |
| Политики доступа                                                | 28  |
| <b>Лицензирование</b>                                           | 29  |
| <b>Системные требования</b>                                     | 31  |
| Серверные компоненты                                            | 32  |
| Модули интеграции                                               | 40  |
| <b>Настройка окружения</b>                                      | 47  |
| Размещение компонентов                                          | 48  |
| Сетевое взаимодействие                                          | 52  |
| Компоненты Internet Information Services                        | 55  |
| Хранилище данных                                                | 56  |
| Каталог пользователей                                           | 68  |
| Клиентский сертификат                                           | 74  |
| <b>Установка и настройка серверных компонентов</b>              | 75  |
| Indeed Log Server                                               | 77  |
| Indeed Core Server                                              | 100 |
| Проверка состояния сервера                                      | 124 |
| Включение защиты от перебора                                    | 125 |
| Настройка нескольких пользовательских каталогов                 | 126 |
| LDAP-фильтр при поиске пользователей и групп в Active Directory | 130 |
| Настройка механизма отзыва лицензий                             | 133 |
| Indeed Management Console                                       | 135 |
| Настройка срока жизни сессии                                    | 143 |
| Настройка поиска пользователя                                   | 144 |
| Отключение отображения информации о платформе и версии          | 146 |

|                                                                          |            |
|--------------------------------------------------------------------------|------------|
| Выход с помощью Identity Provider .....                                  | 148        |
| Indeed User Console .....                                                | 149        |
| Выход с помощью Identity Provider .....                                  | 159        |
| Включение защиты от перебора .....                                       | 160        |
| Настройка срока жизни сессии .....                                       | 161        |
| Отключение отображения информации о платформе и версии .....             | 162        |
| Отключение смены локализации .....                                       | 163        |
| Indeed Key Server .....                                                  | 164        |
| Indeed Phone Management Server .....                                     | 173        |
| Indeed Reset Password .....                                              | 188        |
| Расположение конфигурационных файлов .....                               | 193        |
| <b>Установка и настройка модулей интеграции .....</b>                    | <b>195</b> |
| Indeed Identity Provider .....                                           | 197        |
| Интеграция с приложениями по протоколам OpenID Connect и OAuth 2.0 ..... | 207        |
| Интеграция с приложениями по протоколу SAML .....                        | 211        |
| Включение защиты от перебора .....                                       | 214        |
| Аутентификация по имени пользователя без указания домена .....           | 215        |
| Переключение режима работы Telegram Provider .....                       | 216        |
| Indeed ADFS Extension .....                                              | 217        |
| Indeed ADFS Extension (2012) .....                                       | 218        |
| Indeed ADFS Extension (2016) .....                                       | 225        |
| Indeed IIS Extension .....                                               | 234        |
| Отключение запроса второго фактора .....                                 | 243        |
| Смена локализации .....                                                  | 244        |
| Настройка срока хранения сессии .....                                    | 245        |
| Формат доменного имени для OWA .....                                     | 246        |
| Indeed RDP Windows Logon .....                                           | 247        |
| Аутентификация пользователей без лицензии .....                          | 252        |
| Настройка срока хранения сессии .....                                    | 254        |
| Одновременная работа с Indeed Windows Logon .....                        | 255        |
| Indeed NPS RADIUS Extension .....                                        | 256        |
| Установка и настройка NPS .....                                          | 258        |
| Установка и настройка RADIUS Extension .....                             | 264        |
| Добавление и настройка интегрированного приложения .....                 | 266        |
| Indeed Mobile Device Provisioning .....                                  | 275        |
| Indeed Enterprise Single Sign-On .....                                   | 293        |
| Создание шаблонов приложений .....                                       | 304        |

|                                                               |            |
|---------------------------------------------------------------|------------|
| Работа с ESSO Agent .....                                     | 324        |
| Вход при отсутствии сети .....                                | 332        |
| Управление паролем .....                                      | 335        |
| Обработка ошибок .....                                        | 337        |
| Прозрачный вход для группы пользователей .....                | 338        |
| Indeed Windows Logon .....                                    | 339        |
| Первый вход в систему .....                                   | 344        |
| Вход в систему по аутентификатору .....                       | 348        |
| Рассинхронизация пароля .....                                 | 350        |
| Доступ к удаленному рабочему столу .....                      | 352        |
| Вход при отсутствии сети .....                                | 355        |
| Опциональные настройки .....                                  | 358        |
| Утилита управления аутентификаторами .....                    | 364        |
| Добавление аутентификатора .....                              | 366        |
| Проверка аутентификатора .....                                | 370        |
| Редактирование аутентификатора .....                          | 373        |
| Удаление аутентификатора .....                                | 378        |
| <b>Установка и настройка провайдеров аутентификации .....</b> | <b>380</b> |
| Indeed Key Provider .....                                     | 383        |
| Indeed AM Telegram Provider .....                             | 395        |
| Indeed AM Secured TOTP Provider .....                         | 407        |
| Indeed AM Software OTP Provider .....                         | 413        |
| Indeed AM Hardware OTP Provider .....                         | 415        |
| Indeed AM Hardware TOTP Provider .....                        | 422        |
| Indeed AM SMS OTP Provider .....                              | 428        |
| Indeed AM Messages Proxy .....                                | 432        |
| Indeed AM SMS Proxy .....                                     | 442        |
| Indeed AM Storage SMS OTP Provider .....                      | 452        |
| Indeed AM Email OTP Provider .....                            | 455        |
| Indeed AM Windows Password Provider .....                     | 460        |
| Indeed AM Passcode Provider .....                             | 462        |
| Indeed AM MFA Provider .....                                  | 464        |
| Indeed AM Smart Card Provider .....                           | 468        |
| Indeed AM IronLogic Z2USB Provider .....                      | 473        |
| Indeed AM OMNIKEY Provider .....                              | 478        |
| Indeed AM Futronic Provider .....                             | 482        |
| Миграция настроек провайдеров .....                           | 485        |



|                                                          |     |
|----------------------------------------------------------|-----|
| <b>Административные шаблоны групповых политик (ADMX)</b> | 488 |
| <b>Провайдеры аутентификации</b>                         | 490 |
| Indeed Key                                               | 492 |
| Telegram                                                 | 493 |
| Software OTP                                             | 494 |
| HOTP                                                     | 498 |
| Hardware TOTP                                            | 499 |
| SMS OTP                                                  | 502 |
| Storage SMS OTP                                          | 528 |
| Email OTP                                                | 533 |
| Passcode                                                 | 535 |
| MFA                                                      | 537 |
| Smart Card                                               | 544 |
| IronLogic Z2USB                                          | 548 |
| Omnikey                                                  | 551 |
| Futronic                                                 | 554 |
| RADIUS Extension                                         | 558 |
| RDP Windows Logon                                        | 572 |
| Enterprise Single Sign-On                                | 573 |
| Windows Logon                                            | 576 |
| <b>Резервное копирование</b>                             | 581 |
| <b>Руководство администратора</b>                        | 584 |
| Приложения                                               | 586 |
| Модуль Enterprise SSO                                    | 587 |
| Модуль NPS Radius Extension                              | 594 |
| Кеширование данных пользователя                          | 600 |
| Лицензии                                                 | 603 |
| Аутентификаторы                                          | 606 |
| Пользователи                                             | 612 |
| Политики                                                 | 617 |
| Устройства                                               | 623 |
| События                                                  | 626 |
| Конфигурация                                             | 629 |
| <b>Руководство пользователя</b>                          | 632 |
| Карточка пользователя                                    | 633 |
| Управление аутентификаторами                             | 634 |
| Локализация                                              | 636 |

|                                                                   |     |
|-------------------------------------------------------------------|-----|
| Управление Windows Password .....                                 | 637 |
| <b>API</b> .....                                                  | 638 |
| Общая информация .....                                            | 639 |
| Быстрый старт .....                                               | 643 |
| <b>Методы API</b> .....                                           | 645 |
| Authenticator .....                                               | 647 |
| License .....                                                     | 650 |
| Logon .....                                                       | 654 |
| Policy .....                                                      | 660 |
| TemplateSession .....                                             | 662 |
| User .....                                                        | 666 |
| UserCatalog .....                                                 | 668 |
| UserProfile .....                                                 | 676 |
| <b>Сценарии использования</b> .....                               | 678 |
| Создание отчетов .....                                            | 679 |
| Сбор статистики по обученным аутентификаторам пользователей ..... | 687 |
| Получение списка пользователей с лицензиями .....                 | 690 |
| Двухфакторная аутентификация в API .....                          | 693 |
| Удаление пользователей из политики .....                          | 696 |
| Получение списка пользователей из политики .....                  | 698 |
| <b>Миграция с Indeed AM 7.x на Indeed AM 8.x</b> .....            | 700 |
| Подготовка к миграции .....                                       | 701 |
| Миграция MS SQL .....                                             | 703 |
| Миграция хранилища Active Directory .....                         | 722 |
| <b>Решение проблем</b> .....                                      | 733 |
| Сбор программных логов .....                                      | 734 |
| Сбор логов серверных компонентов .....                            | 739 |
| База знаний .....                                                 | 750 |
| Техническая поддержка .....                                       | 751 |
| <b>История версий</b> .....                                       | 754 |
| <b>Справочник</b> .....                                           | 756 |
| Журнал событий .....                                              | 757 |
| Роли .....                                                        | 802 |

# О продукте

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

Indeed AM включает в себя различные модули для интеграции с целевыми системами с применением таких технологий как **SAML**, **OpenID Connect**, **RADIUS**, **ADFS**, **Enterprise SSO**, агенты аутентификации. Такой подход позволяет защитить доступ во все информационные системы предприятия и адаптировать решение под нужды заказчика.

## Модули интеграции в Indeed AM

## Аутентификация и управление доступом

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

Различные технологии можно объединять в один способ аутентификации, реализуя таким образом мультифакторную аутентификацию (MFA). Архитектура решения позволяет оперативно добавлять поддержку новых технологий.

## Какие технологии аутентификации поддерживаются в Indeed AM

## Установка

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

Indeed AM поддерживает масштабирование мощностей (установку в режиме кластера), для обеспечения требуемых уровней отказоустойчивости и производительности. Кластерная схема развертывания не требует приобретения дополнительных лицензий.

# Базовые компоненты

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

## Сервер аутентификации и управления Core Server

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

**Установка и настройка Core Server**

## Каталог пользователей

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

**Подготовка каталога пользователей**

## Базы данных

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

**Создание и настройка хранилища данных**

## Management Console

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

**Установка и настройка Management Console**

# User Console

Дает возможность зарегистрировать или изменить аутентификационные данные (смарт-карты, генераторы одноразовых паролей, отпечатки и другие), а также просмотреть историю входов.

Установка и настройка User Console

# Модули интеграции



## Indeed ADFS Extension

Двухфакторная аутентификация с использованием ADFS



## Indeed Enterprise Single Sign-On

Single Sign-on для унаследованных приложений



## Indeed Identity Provider

Многофакторная аутентификация и сквозной доступ



## Indeed IIS Extension

Аутентификация в приложения на базе Internet Information Services



## Indeed NPS RADIUS Extension

Двухфакторная аутентификация для протокола RADIUS



## Indeed RDP Windows Logon

Двухфакторная аутентификация для протокола Remote Desktop Protocol



## Indeed Windows Logon

Доступ в Windows с помощью строгой аутентификации

# Indeed ADFS Extension

Веб-приложения на базе сервера Internet Information Services (IIS) могут быть интегрированы с программным комплексом Indeed AM с использованием механизма ADFS и компонента Indeed ADFS Extension.

Компонент ADFS Extension реализует провайдер многофакторной аутентификации для сервера Microsoft ADFS, добавляя в процесс получения доступа второй фактор. Такой подход дает возможность интегрироваться с целевыми приложениями без их модификации: при входе в приложение пользователь перенаправляется на веб-страницу аутентификации ADFS, где через провайдер аутентификации Indeed ADFS Extension запрашивается второй фактор, после успешной аутентификации пользователь возвращается в целевое приложение.

## Установка и настройка ADFS Extension

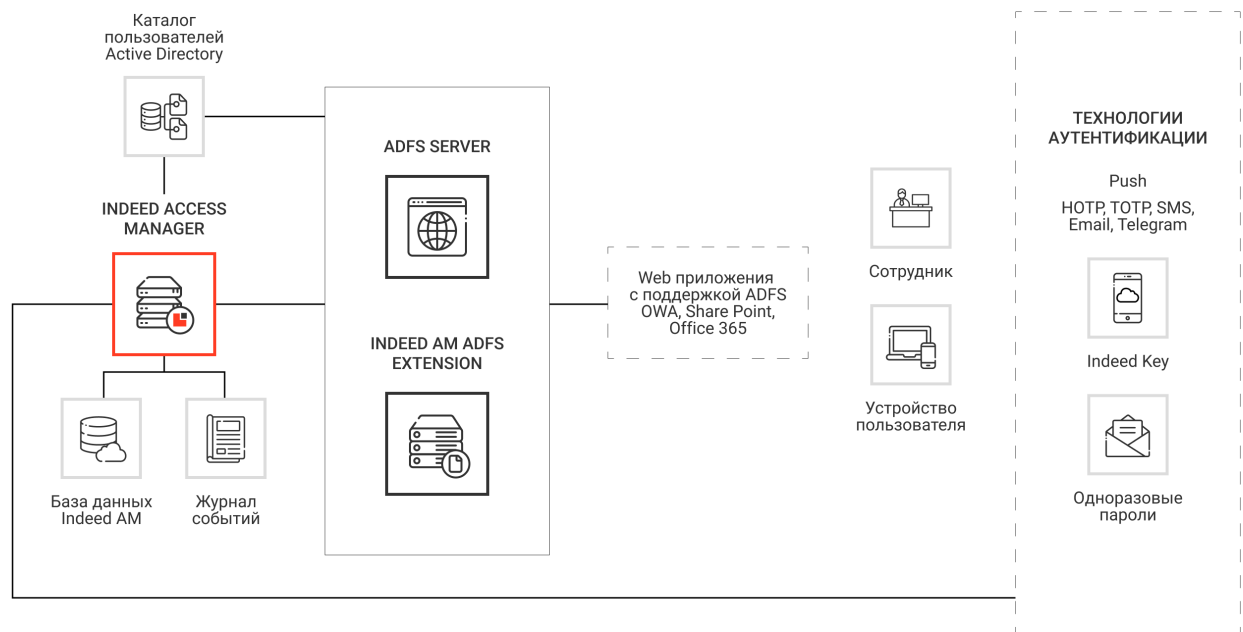
## Технологии аутентификации

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

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

## Где можно использовать

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





# Indeed Enterprise Single Sign-On

Indeed Enterprise Single Sign-On (Enterprise SSO) реализует подход Single Sign-on для унаследованных приложений, которые не поддерживают механизмы SSO. Система централизованно хранит пароли пользователя от всех приложений, требующих ввода учетных данных и автоматически подставляет их в экранные формы, когда приложение того требует.

Enterprise SSO избавляет сотрудников от запоминания и хранения паролей в секрете, от ручного ввода паролей с клавиатуры, от периодической смены паролей согласно парольных политик безопасности.

Для этих целей на рабочей станции пользователя устанавливается Enterprise SSO агент, который отслеживает запуск приложений и выполняет перехват форм аутентификации, когда они появляются на экране. Агент также включает в себя расширения для популярных браузеров (Internet Explorer, Google Chrome, Mozilla Firefox), что позволяет работать с веб-приложениями.

## Установка и настройка Enterprise SSO

### Добавление и настройка интегрированных приложений

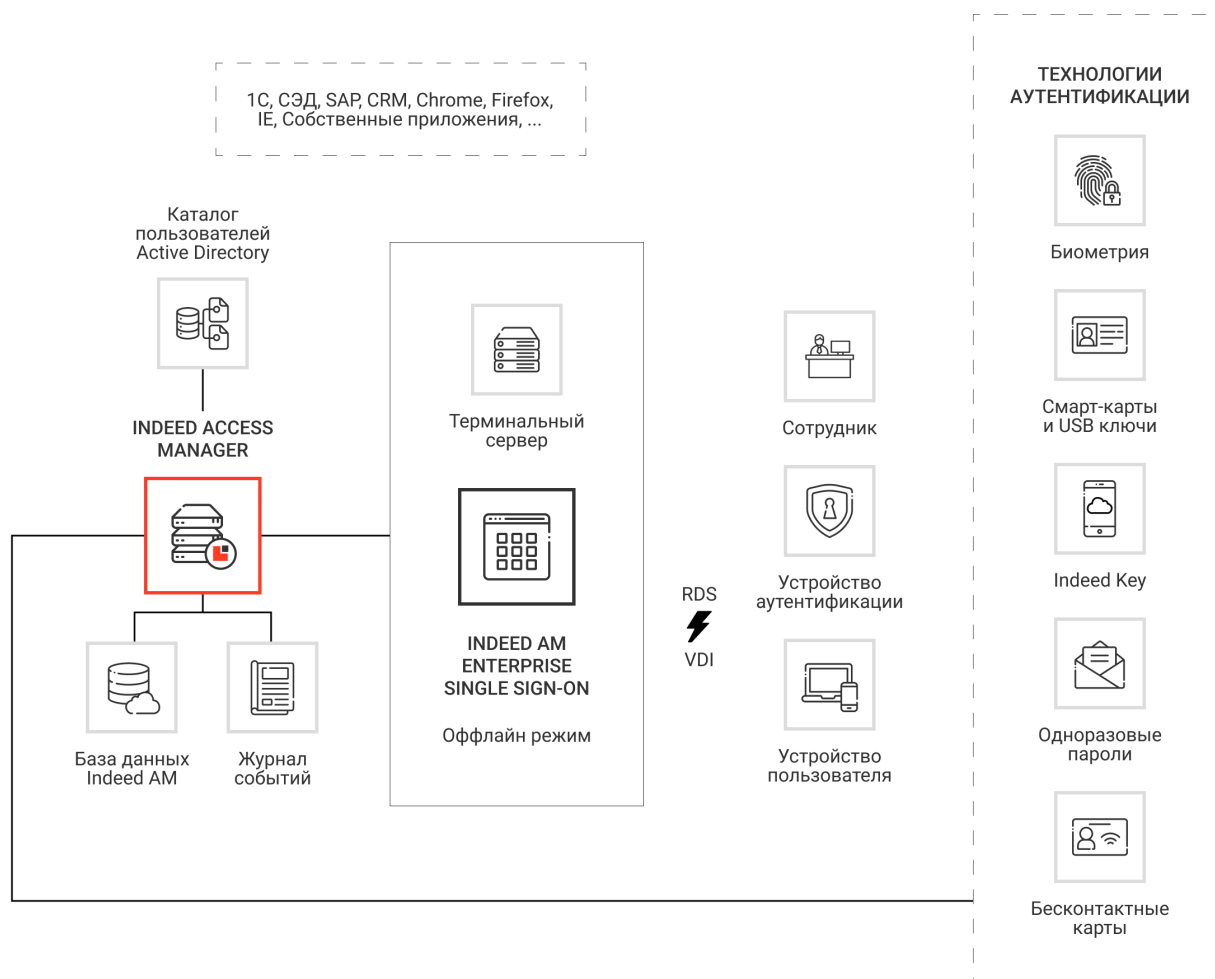
## Где можно использовать

Технология Enterprise SSO может быть применена для любых типов приложений (Windows, Java, Web, .Net) независимо от архитектуры: однозвенная, двухзвенная, трехзвенная, толстый клиент, тонкий клиент, терминальные приложения.

## Технологии аутентификации

Enterprise SSO поддерживает следующие технологии аутентификации:

- одноразовые пароли TOTP и HOTP,
- одноразовые коды через СМС и email,
- одноразовые коды и push-уведомления в мобильном приложении Indeed Key,
- смарт-карты и USB-ключи.



## Принцип интеграции Enterprise SSO с целевыми системами

Enterprise SSO позволяет настраиваться на работу с приложением без программного вмешательства в серверную или клиентскую части данного приложения. Поддержка нового приложения подразумевает создание специального шаблона xml-формата, реализация которого выполняется на внутреннем языке Enterprise SSO скриптового типа. Язык позволяет указать, на какие формы приложения необходимо определить реакцию. Реакция Enterprise SSO может включать в себя повторную строгую аутентификацию пользователя, заполнение полей регистрационными данными (например логин, пароль), нажатие необходимых элементов управления (например нажатие кнопки входа).

## Смена пароля в целевом приложении

В целях минимизации рисков информационной безопасности большинство информационных систем поддерживают возможность требовать от пользователя изменить значение пароля сразу

после того, как пользователь осуществил первый вход в систему, либо по истечении заданного времени жизни пароля. Enterprise SSO обрабатывает данную ситуацию и позволяет в автоматическом режиме (прозрачно для пользователя) заблокировать на этот момент доступ пользователя к окну смены пароля, сгенерировать новое значение, заполнить поля формы *Новое значение* и *Подтверждение*, нажать кнопку *OK*. Дождавшись от целевой системы уведомления об успешной смене пароля, Enterprise SSO агент сохраняет новое значение в базе данных Indeed AM. С этого момента ни пользователь, ни администратор не знают новое значение пароля и, следовательно, не могут войти в целевую систему в обход Enterprise SSO.

Возможность обрабатывать ситуацию смены пароля появляется только в том случае, если ESSO шаблон приложения поддерживает реакцию на появление данного типа окна.

## Поддержка терминальной среды исполнения

Indeed Enterprise SSO адаптирован к работе в терминальной среде, позволяя избавить сотрудников от явного использования своих паролей в моменты, когда работа с приложением происходит внутри терминальной сессии. Для этого агент Enterprise SSO должен быть установлен на терминальном сервере.

В некоторых ситуациях, в момент получения доступа к особо критичным приложениям, от сотрудника может потребоваться пройти дополнительную процедуру аутентификации. Если технология предполагает использование внешнего оборудования, подключенного к ПК сотрудника (например сканер отпечатка пальца), то между агентом Enterprise SSO терминального сервера и оборудованием возникает коммуникация. Enterprise SSO осуществляет коммуникацию по протоколам Microsoft RDP или Citrix ICA. Это означает, что на стороне ПК сотрудника не требуется установка дополнительного программного обеспечения за исключением драйвера и набора run-time библиотек, необходимых для работы оборудования.

# Indeed Identity Provider

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

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

Это гарантирует совместимость с широким спектром коммерческих систем. Применение IDP избавляет пользователя от необходимости запоминать множество учетных данных: для доступа во все интегрированные системы требуется только один комплект учетных данных.

Аутентификация выполняется централизованно на стороне Identity Provider (IDP, поставщик удостоверений).

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

## Установка и настройка Identity Provider

## Технологии аутентификации

Indeed IDP поддерживает следующие технологии аутентификации пользователей:

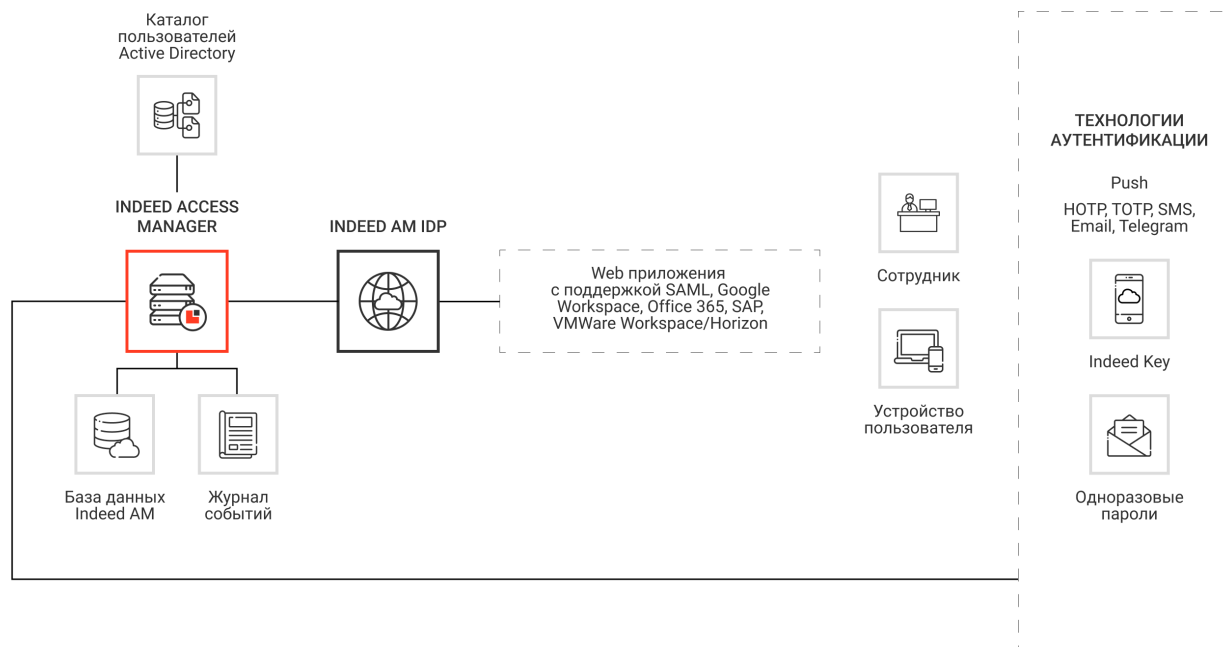
- доменный пароль,
- одноразовые пароли OATH: TOTP и HOTP,
- одноразовые коды через СМС и email,
- одноразовые коды и push-уведомления в мессенджере Telegram,
- одноразовые коды и push-уведомления в мобильном приложении Indeed Key.

## Где можно использовать

В контур WebSSO и MFA могут быть включены как корпоративные on-premise приложения (например решения от компаний SAP, Citrix и др.), так и облачные сервисы, такие как Office 365,

Salesforce, Slack, Google Workspace (ранее G Suite) и другие.

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



# Indeed IIS Extension

Для аутентификации в веб-приложениях, использующих Internet Information Services (IIS) и не поддерживающих механизм ADFS, компанией Индид разработан специализированный модуль интеграции Indeed IIS Extension (IIS Extension).

IIS Extension устанавливается на веб-сервер, где развернуто целевое приложение, и позволяет обеспечить двухфакторную аутентификацию без вмешательства в его программный код. Модуль перехватывает попытки аутентификации, и после ввода имени и пароля пользователь перенаправляется на отдельную страницу, где он должен подтвердить вход с помощью одноразового пароля.

Также поддерживается режим однофакторной аутентификации. Такой режим востребован для приложения Exchange ActiveSync (EAS) и позволяет исключить доменный пароль из схемы аутентификации. Для доступа к EAS в этом случае используется недоменный пароль, который, по сути, представляет собой так называемый application password, используемый только для EAS. Этот пароль вводится пользователем в мобильном клиенте для доступа к корпоративной почте.

## Установка и настройка IIS Extension

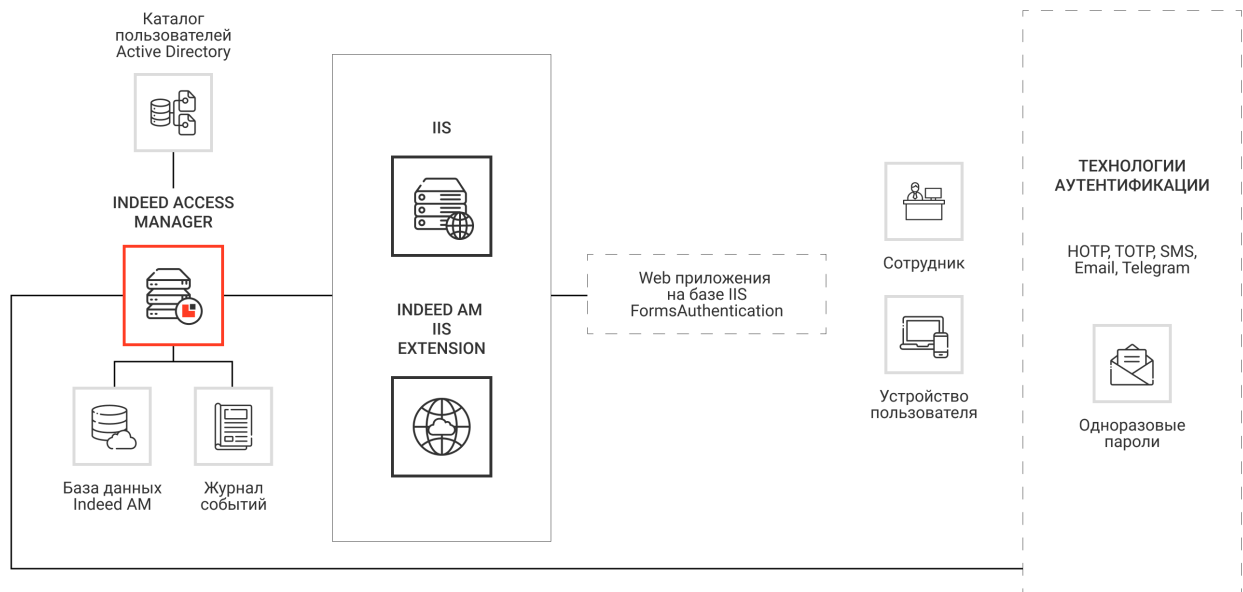
## Технологии аутентификации

IIS Extension поддерживает следующие технологии аутентификации пользователей:

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

## Где можно использовать

IIS Extension может использоваться для любых веб-приложений на базе IIS, например Outlook Web Access, RD Web Access, Exchange ActiveSync и другие.



# Indeed NPS RADIUS Extension

Indeed NPS RADIUS Extension (RADIUS Extension) представляет собой модуль расширения Microsoft Network Policy Server (NPS входит в состав Windows Server) и позволяет реализовать технологию двухфакторной аутентификации для RADIUS-совместимых сервисов и приложений.

Для этого требуется:

- Развернуть в сети предприятия сервер NPS, который предоставляет возможность аутентификации по протоколу RADIUS с использованием учетных данных пользователей каталога Active Directory.
- Настроить целевое приложение на аутентификацию пользователей по протоколу RADIUS на сервере NPS.
- Установить на сервер NPS расширение RADIUS Extension, которое будет обрабатывать запросы на аутентификацию и требовать от пользователя второй фактор аутентификации.

Аутентификация по второму фактору выполняется на сервере Indeed Access Manager и результат проверки через сервер NPS транслируется в целевое приложение.

## Установка и настройка NPS RADIUS Extension

## Технологии аутентификации

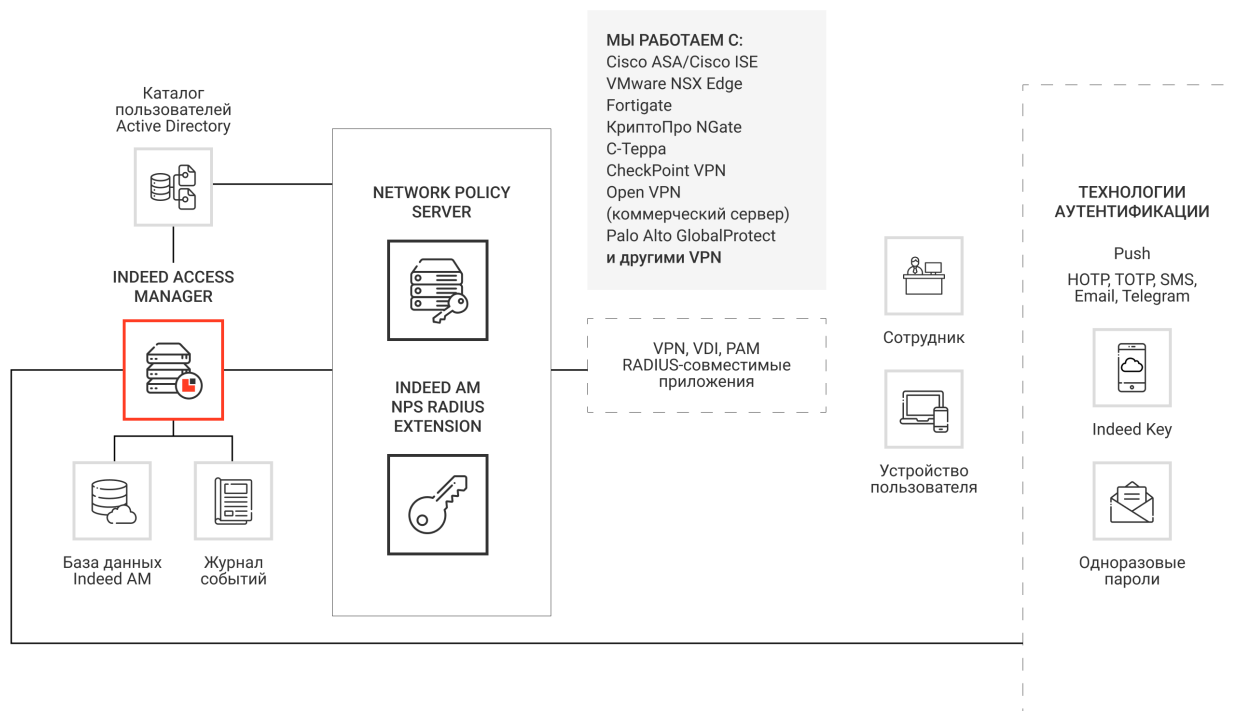
RADIUS Extension в качестве второго фактора поддерживает аутентификацию с помощью следующих технологий:

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

## Где можно использовать

Аутентификация по протоколу RADIUS может быть использована во многих VPN и VDI решениях, например в программных продуктах компаний Cisco, Citrix, Check Point, VMWare, C-Терра.





# Indeed RDP Windows Logon

Модуль Indeed RDP Windows Logon (RDP Windows Logon) используется для реализации двухфакторной аутентификации при подключениях по протоколу RDP. В этом случае первым фактором выступает доменный пароль, а вторым — одноразовый пароль (one-time password) или подтверждение входа в мобильном приложении Indeed Key. Одноразовый пароль может быть либо сгенерирован на стороне пользователя в приложении на смартфоне, либо с помощью специального брелока (OTP-токена), либо отправлен пользователю по СМС или email.

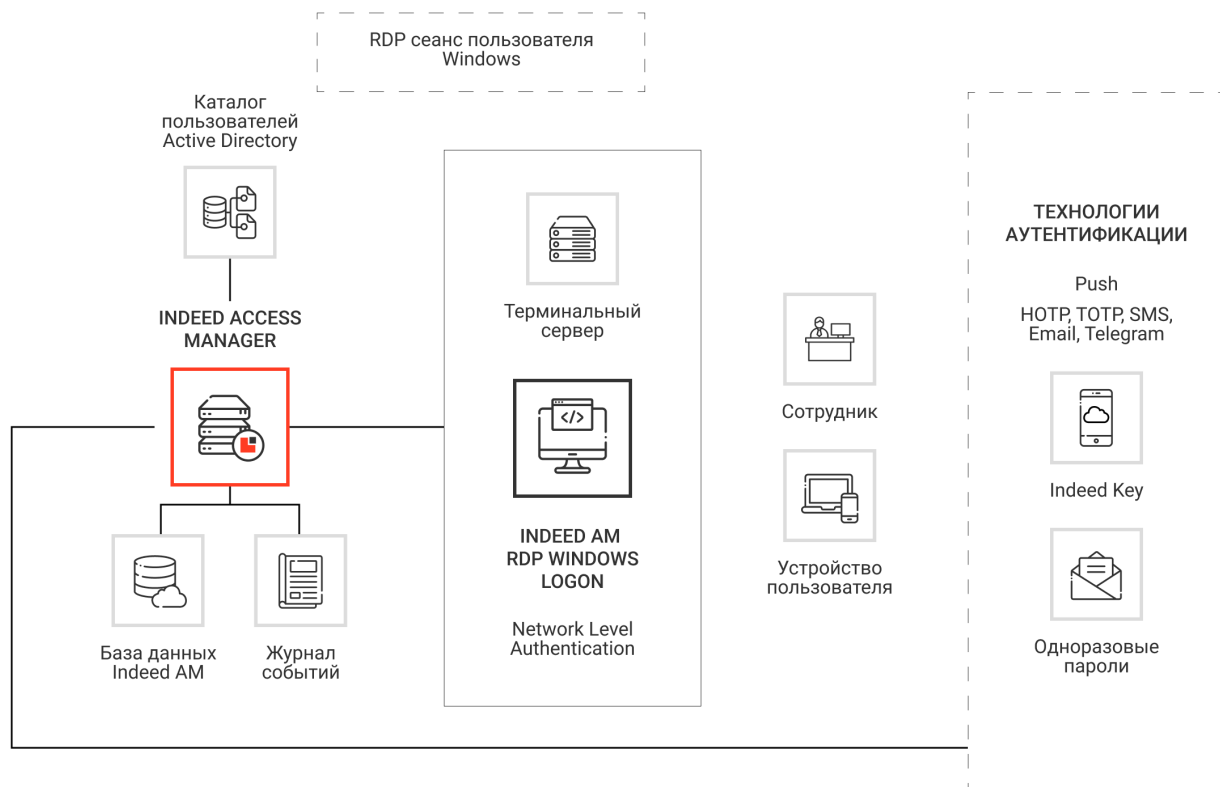
RDP Windows Logon следует устанавливать на конечный терминальный сервер, куда выполняет вход пользователь. Установка каких-либо компонентов на клиентский компьютер не требуется. Поддерживается конфигурация с Remote Desktop Gateway.

## Установка и настройка RDP Windows Logon

## Технологии аутентификации

RDP Windows Logon поддерживает следующие технологии аутентификации пользователей:

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



# Indeed Windows Logon

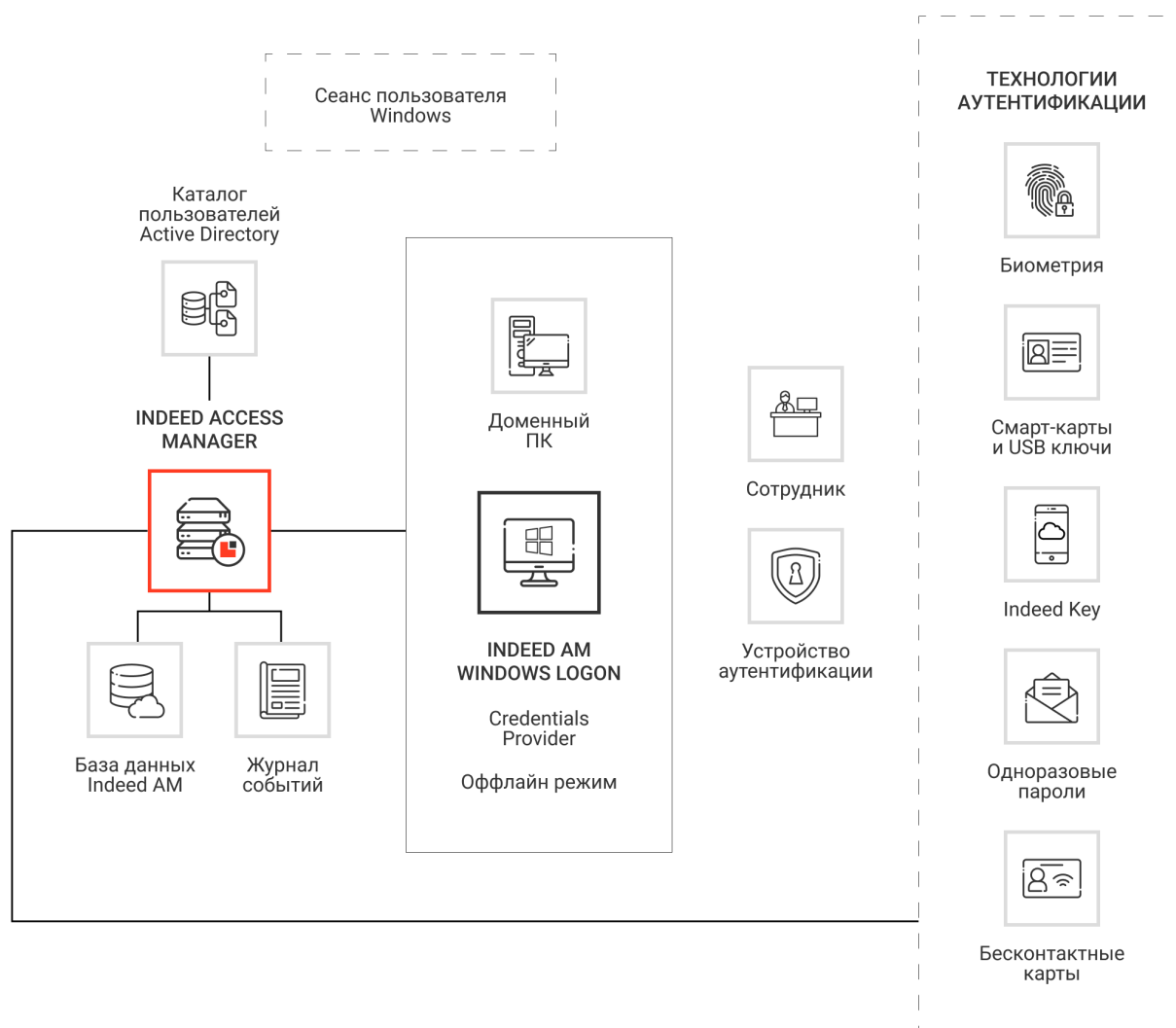
Indeed Windows Logon (Windows Logon) представляет возможность получать доступ в Windows с использованием технологий строгой аутентификации в среде Microsoft Active Directory. Для этого на рабочие места пользователей устанавливается агент Windows Logon.

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

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

В Windows Logon поддерживаются все технологии аутентификации, доступные в Indeed Access Manager — смарт-карты, карты RFID, одноразовые пароли.

## Установка и настройка Windows Logon



## Технологии аутентификации

Windows Logon поддерживает следующие технологии аутентификации:

- доменный пароль,
- одноразовые пароли TOTP и HOTP,
- одноразовые коды через СМС и email,
- одноразовые коды и push-уведомления в мобильном приложении Indeed Key,
- смарт-карты и USB-ключи.

## Оффлайн-режим

Для повышения отказоустойчивости Windows Logon может создавать локальный кеш на компьютере пользователя. Такой кеш содержит аутентификационные данные и используется в моменты, когда отсутствует связь с серверной инфраструктурой (оффлайн-режим), например вследствие обрыва связи или в командировке.

Время жизни локального кеша можно ограничить количеством дней или календарной датой, кеш создается только для тех пользователей, для кого это явно разрешено администратором Indeed AM. Для защиты локальных данных используется технология Windows Data Protection API.

## Управление паролями пользователей Active Directory

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

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

# Технологии аутентификации

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

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

## Установка и настройка провайдеров аутентификации

Indeed Access Manager поддерживает следующие технологии аутентификации:

- криптографические смарт-карты и USB-носители, такие как Рутокен, eToken, JaCarta и другие;
- бесконтактные карты RFID (используемые в качестве пропуска в системах контроля и управления доступом) форматов EM-Marin, HID iClass, HID Proximity, Mifare;
- аппаратные и программные токены генерации одноразовых паролей по протоколам OATH, TOTP и HOTP;
- одноразовые коды, высылаемые по СМС или email;
- аутентификация с использованием мобильного приложения и push-уведомлений на базе приложения Indeed Key.

Мобильное приложение Indeed Key доступно для операционных систем iOS и Android.

Используя Indeed Key, пользователь подтверждает операцию входа в приложении на смартфоне. Детали операции отображаются на экране смартфона, где пользователь может убедиться, в какую именно систему выполняется вход. Кроме этого, Indeed Key поддерживает генерацию одноразовых паролей по протоколу TOTP.

Различные технологии можно объединять в один способ аутентификации, реализуя таким образом мультифакторную аутентификацию (MFA).

# Политики доступа

Политика — это совокупность настроек базовых компонентов, модулей интеграции, бизнес-приложений и учетных записей, которые могут быть распространены на определенную выборку пользователей из пользовательского каталога. Все пользователи, которые включены в политику, получают учетные записи для приложений с соответствующими настройками или сами настройки из политики.

У политики могут быть определены:

- область действия — пользователи, которые попадают под действие правил, заданных в этой политике;
- администраторы;
- набор и настройки доступных способов аутентификации;
- набор доступных бизнес-приложений и их ролевых учетных записей;
- приоритет политики.

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

Если в политиках, в область действия которых попадает пользователь, одно и то же приложение встречается более одного раза, то пользователю присваиваются настройки доступа в это приложение из политики с максимальным приоритетом.

Например, если в политике №1 для ADFS Extension указано использование SMS OTP, а в более приоритетной политике №2 для ADFS Extension указано использование Email OTP, то пользователь должен выполнять вход через ADFS с использованием Email OTP.

Если в политике с максимальным приоритетом нет настроек для приложения, используются настройки из следующей по приоритету политики.

В сценариях ESSO могут быть исключения, связанные с особенностями реализации ESSO Agent.



# Лицензирование

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

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

## Как управлять лицензиями в Management Console

Лицензии Indeed Access Manager делятся на следующие типы:

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

## Основная лицензия

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

## Лицензии для дополнительных модулей

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

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

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

- *Лицензия Indeed AM Windows Logon.* Дает право на использование модуля Windows Logon для строгой и многофакторной аутентификации в операционных системах Microsoft Windows.
- *Лицензия Indeed AM RDP Windows Logon.* Дает право на использование модуля RDP Windows Logon для двухфакторной аутентификации с использованием одноразовых паролей при терминальном доступе в операционные системы Microsoft Windows.
- *Лицензия Indeed AM Enterprise Single Sign-On.* Дает право на использование модуля Enterprise Single Sign-On для организации сквозной аутентификации в десктопных и веб-приложениях на рабочих станциях конечных пользователей.
- *Лицензия Indeed AM Identity Provider.* Дает право на использование модуля Identity Provider для построения системы Web Single Sign-On с применением протоколов SAML и OpenID Connect.
- *Лицензия Indeed AM NPS RADIUS Extension.* Дает право на использование модуля RADIUS для реализации двухфакторной аутентификации в приложениях, совместимых с протоколом RADIUS (VPN, VDI и другими).
- *Лицензия Indeed AM IIS Extension.* Дает право на использование модуля IIS для реализации строгой и двухфакторной аутентификации в веб-приложениях на базе сервера IIS (Internet Information Services).
- *Лицензия Indeed AM API.* Дает право на использование программного интерфейса для интеграции со сторонними системами.
- *Лицензия Indeed AM ADFS Extension.* Дает право на использование модуля ADFS для построения системы с применением протокола ADFS.
- *Лицензия Indeed AM Mobile Device Provisioning.* Дает право на использование сервиса подготовки мобильных устройств для вывода устройств из карантина.

# Системные требования



## Серверные компоненты

Системные требования для серверных компонентов



## Модули интеграции

Системные требования для модулей интеграции

# Серверные компоненты

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

## Indeed Core Server

|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Домен                 | Active Directory                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Операционная система  | Windows Server 2012 R2 и выше                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Версия IIS и модули   | <p>Internet Information Services 7.0 и выше со следующими модулями:</p> <ul style="list-style-type: none"><li>• Статическое содержимое (Static Content)</li><li>• Перенаправление HTTP (HTTP Redirection)</li><li>• ASP.NET</li><li>• Расширяемость .NET (.NET Extensibility)</li><li>• Расширения ISAPI (ISAPI Extensions)</li><li>• Фильтры ISAPI (ISAPI Filters)</li><li>• Обычная проверка подлинности (Basic Authentication)</li><li>• Windows-проверка подлинности (Windows Authentication)</li><li>• Консоль управления службами IIS (IIS Management Console)</li></ul> |
| Компоненты Microsoft  | Microsoft .NET Framework 4.5.2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Microsoft SQL Server  | Microsoft SQL Server 2012 всех редакций и более новые версии                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| PostgreSQL            | <ul style="list-style-type: none"><li>• PostgreSQL</li><li>• PostgreSQL Pro</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Аппаратные требования | <ul style="list-style-type: none"><li>• Не менее 4 ГБ оперативной памяти</li><li>• Не менее 50 ГБ свободного пространства на диске</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                   |

 **ПРИМЕЧАНИЕ**

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

## Indeed Log Server

|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Операционная система  | Windows Server 2012 R2 и выше                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Версия IIS и модули   | Internet Information Services 7.0 и выше со следующими модулями: <ul style="list-style-type: none"><li>• Статическое содержимое (Static Content)</li><li>• Перенаправление HTTP (HTTP Redirection)</li><li>• ASP.NET</li><li>• Расширяемость .NET (.NET Extensibility)</li><li>• Расширения ISAPI (ISAPI Extensions)</li><li>• Фильтры ISAPI (ISAPI Filters)</li><li>• Обычная проверка подлинности (Basic Authentication)</li><li>• Windows-проверка подлинности (Windows Authentication)</li><li>• Консоль управления службами IIS (IIS Management Console)</li></ul> |
| 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 | <ul style="list-style-type: none"><li>• Не менее 4 ГБ оперативной памяти</li><li>• Не менее 50 ГБ свободного пространства на диске</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                            |

 **ПРИМЕЧАНИЕ**

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

## Indeed Management Console

 **ПРИМЕЧАНИЕ**

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

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Операционная система          | Windows Server 2012 R2 и выше                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Версия IIS и модули           | <p>Internet Information Services 7.0 и выше со следующими модулями:</p> <ul style="list-style-type: none"><li>• Статическое содержимое (Static Content)</li><li>• Перенаправление HTTP (HTTP Redirection)</li><li>• ASP.NET</li><li>• Расширяемость .NET (.NET Extensibility)</li><li>• Расширения ISAPI (ISAPI Extensions)</li><li>• Фильтры ISAPI (ISAPI Filters)</li><li>• Обычная проверка подлинности (Basic Authentication)</li><li>• Windows-проверка подлинности (Windows Authentication)</li><li>• Консоль управления службами IIS (IIS Management Console)</li></ul> |
| Компоненты Microsoft          | Microsoft .NET Framework 4.8 и выше                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Веб-браузер актуальной версии | <ul style="list-style-type: none"><li>• Google Chrome</li><li>• Mozilla Firefox</li><li>• Microsoft Edge</li><li>• Internet Explorer</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                 |

|                       |                                                                                                                                                 |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Аппаратные требования | <ul style="list-style-type: none"> <li>• Не менее 4 ГБ оперативной памяти</li> <li>• Не менее 50 ГБ свободного пространства на диске</li> </ul> |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|

#### ⓘ ПРИМЕЧАНИЕ

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

## Indeed User Console

#### ⓘ ПРИМЕЧАНИЕ

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

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Операционная система | Windows Server 2012 R2 и выше                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Версия IIS и модули  | <p>Internet Information Services 7.0 и выше со следующими модулями:</p> <ul style="list-style-type: none"> <li>• Статическое содержимое (Static Content)</li> <li>• Перенаправление HTTP (HTTP Redirection)</li> <li>• ASP.NET</li> <li>• Расширяемость .NET (.NET Extensibility)</li> <li>• Расширения ISAPI (ISAPI Extensions)</li> <li>• Фильтры ISAPI (ISAPI Filters)</li> <li>• Обычная проверка подлинности (Basic Authentication)</li> <li>• Windows-проверка подлинности (Windows Authentication)</li> <li>• Консоль управления службами IIS (IIS Management Console)</li> </ul> |
| Компоненты Microsoft | Microsoft .NET Framework 4.5.2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

|                               |                                                                                                                                                     |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| Веб-браузер актуальной версии | <ul style="list-style-type: none"> <li>• Google Chrome</li> <li>• Mozilla Firefox</li> <li>• Microsoft Edge</li> <li>• Internet Explorer</li> </ul> |
| Аппаратные требования         | <ul style="list-style-type: none"> <li>• Не менее 4 Гб оперативной памяти</li> <li>• Не менее 50 Гб свободного пространства на диске</li> </ul>     |

### ⚠ ПРИМЕЧАНИЕ

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

## Indeed Phone Management Server

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Операционная система | Windows Server 2012 R2 и выше                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Версия IIS и модули  | <p>Internet Information Services 7.0 и выше со следующими модулями:</p> <ul style="list-style-type: none"> <li>• Статическое содержимое (Static Content)</li> <li>• Перенаправление HTTP (HTTP Redirection)</li> <li>• ASP.NET</li> <li>• Расширяемость .NET (.NET Extensibility)</li> <li>• Расширения ISAPI (ISAPI Extensions)</li> <li>• Фильтры ISAPI (ISAPI Filters)</li> <li>• Обычная проверка подлинности (Basic Authentication)</li> <li>• Консоль управления службами IIS (IIS Management Console)</li> <li>• Авторизация URL-адреса (URL Authorization) — установка данного компонента не входит в скрипт Powershell с автоматической установкой компонентов IIS.</li> </ul> |
| Компоненты Microsoft | <ul style="list-style-type: none"> <li>• Microsoft .NET Framework 4.5.2</li> <li>• <b>Web Deploy Package</b></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |



|                       |                                                                                                                                                 |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Аппаратные требования | <ul style="list-style-type: none"> <li>• Не менее 4 ГБ оперативной памяти</li> <li>• Не менее 50 ГБ свободного пространства на диске</li> </ul> |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|

### ⓘ ПРИМЕЧАНИЕ

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

## Indeed Key Server

### ⓘ ПРИМЕЧАНИЕ

Сервер поддерживает работу вне домена.

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Операционная система | Windows Server 2012 R2 и выше                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Версия IIS и модули  | <p>Internet Information Services 7.0 и выше со следующими модулями:</p> <ul style="list-style-type: none"> <li>• Статическое содержимое (Static Content)</li> <li>• Перенаправление HTTP (HTTP Redirection)</li> <li>• ASP.NET 4.6</li> <li>• Расширяемость .NET (.NET Extensibility)</li> <li>• Расширения ISAPI (ISAPI Extensions)</li> <li>• Фильтры ISAPI (ISAPI Filters)</li> <li>• Анонимная проверка подлинности (Anonymous Authentication)</li> <li>• Консоль управления службами IIS (IIS Management Console)</li> </ul> |
| Компоненты Microsoft | Microsoft .NET Framework 4.6.2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

|                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Microsoft SQL Server                              | <ul style="list-style-type: none"> <li>• Microsoft SQL Server 2012 SP2 всех редакций</li> <li>• Microsoft SQL Server 2014 всех редакций</li> <li>• Microsoft SQL Server 2016 всех редакций</li> <li>• Microsoft SQL Server 2019 всех редакций</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| PostgreSQL                                        | <ul style="list-style-type: none"> <li>• PostgreSQL</li> <li>• PostgreSQL Pro</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Аппаратные требования                             | <p>Аппаратные требования совпадают с требованиями, предъявляемыми к операционным системам, на которых функционирует ПО.</p> <ul style="list-style-type: none"> <li>• Не менее 8 ГБ оперативной памяти</li> <li>• Не менее 200 ГБ свободного пространства на диске</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Взаимодействие с мобильным приложением Indeed Key | <ul style="list-style-type: none"> <li>• Для отправки push-уведомлений серверу Indeed Key требуется внешний доступ к интернету (для доступа к <i>fcm.googleapis.com:443</i> и <i>oauth2.googleapis.com:443</i>).</li> <li>• Сервер Indeed Key должен быть доступен по указанному в настройках имени dns и порту (данные параметры задаются при настройке Indeed Key) из внешней сети.</li> <li>• Имя DNS-сервера Indeed Key не должно содержать нижнего подчеркивания _.</li> <li>• Для отправки push-уведомлений на устройства Huawei требуется доступ к сервису HUAWEI Push по следующим адресам: <ul style="list-style-type: none"> <li>◦ <i>push-api.cloud.huawei.com</i></li> <li>◦ <i>oauth-login.cloud.huawei.com</i></li> </ul> </li> </ul> |

## Требования к сертификатам для устройств на базе iOS



### ПРИМЕЧАНИЕ

Сертификат должен быть установлен на устройстве и должно быть настроено доверие к сертификату.

## ИНФОРМАЦИЯ

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

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

# Модули интеграции

## Программные требования

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

### Как работает лицензирование в Indeed Access Manager

#### Indeed ADFS Extension

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

#### Indeed NPS RADIUS Extension

- Windows Server 2012 R2 и выше;
- Установленная роль *Network Policy Server*;

#### Indeed IIS Extension

- Windows Server 2012 R2 и выше;
- Установленный сервер Internet Information Services;

#### Indeed RDP Windows Logon

- Windows Server 2012 R2 и выше;
- Windows 7 32/64bit;
- Windows 8.1 32/64bit;
- Windows 10 32/64bit;
- Windows 11 32/64bit.

## Indeed Identity Provider

### ⓘ ПРИМЕЧАНИЕ

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

|                      |                               |
|----------------------|-------------------------------|
| Операционная система | Windows Server 2012 R2 и выше |
|----------------------|-------------------------------|

## Версия IIS и модули

Internet Information Services 7.5 и выше со следующими модулями:

- Статическое содержимое (Static Content)
- 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)

|                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                 | <ul style="list-style-type: none"> <li>• Ограничения по IP-адресам и доменам (IP and Domain Restrictions)</li> <li>• Сжатие статического содержимого (Static Content Compression)</li> <li>• Сжатие динамического содержимого (Dynamic Content Compression)</li> <li>• Консоль управления IIS (IIS Management Console)</li> <li>• Сценарии и средства управления IIS (IIS Management Scripts and Tools)</li> <li>• Служба управления (Management Service)</li> </ul> |
| Компоненты Microsoft                            | .NET 6.0                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Компоненты для активации Windows Server 2012 R2 | <ul style="list-style-type: none"> <li>• Активация по HTTP (HTTP Activation)</li> <li>• Активация по MSMQ (Message Queuing Activation)</li> <li>• Активация по TCP (TCP Activation)</li> <li>• Совместное использование портов TCP (TCP Port Sharing)</li> </ul>                                                                                                                                                                                                     |
| Требования к окружению клиентской части         | <ul style="list-style-type: none"> <li>• Internet Explorer 11</li> <li>• Google Chrome 42.0 и выше</li> <li>• Mozilla FireFox 37.0 и выше</li> <li>• Opera 28.0 и выше</li> <li>• MS Edge</li> </ul>                                                                                                                                                                                                                                                                 |

## Indeed Mobile Device Provisioning

|                      |                               |
|----------------------|-------------------------------|
| Операционная система | Windows Server 2012 R2 и выше |
| Компоненты Microsoft | .NET 6.0                      |

|                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Версия IIS и модули                     | <p>Internet Information Services 7.0 и выше со следующими модулями:</p> <ul style="list-style-type: none"> <li>• Статическое содержимое (Static Content)</li> <li>• Перенаправление HTTP (HTTP Redirection)</li> <li>• ASP.NET</li> <li>• Расширяемость .NET (.NET Extensibility)</li> <li>• Расширения ISAPI (ISAPI Extensions)</li> <li>• Фильтры ISAPI (ISAPI Filters)</li> <li>• Обычная проверка подлинности (Basic Authentication)</li> <li>• Windows-проверка подлинности (Windows Authentication)</li> <li>• Консоль управления службами IIS (IIS Management Console)</li> </ul> |
| Требования к окружению клиентской части | <ul style="list-style-type: none"> <li>• Internet Explorer 11</li> <li>• Google Chrome 42.0 и выше</li> <li>• Mozilla FireFox 37.0 и выше</li> <li>• Opera 28.0 и выше</li> <li>• MS Edge</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                     |

## Аппаратные требования

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

## Indeed Windows Logon

|                                                        |                                                                                                                                                         |
|--------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| Аппаратные требования к рабочим станциям пользователей | <ul style="list-style-type: none"> <li>• не менее 50 МБ свободного пространства на диске</li> <li>• наличие .NET Framework версии 4.5 и выше</li> </ul> |
|--------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|



|                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Поддерживаемые операционные системы | <ul style="list-style-type: none"> <li>• Windows 7 SP1 32/64bit</li> <li>• Windows 8.1 32/64bit</li> <li>• Windows 10 32/64bit</li> <li>• Windows 11 32/64bit</li> <li>• Windows Server 2012/2012 R2</li> <li>• Windows Server 2016</li> <li>• Windows Server 2019</li> <li>• Windows Server 2022</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Требования к окружению              | Настроенный DNS-сервер (необходимо добавление Reverse lookup zones). Параметры DNS-сервера необходимо указать в настройках сетевого подключения на каждой рабочей станции.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Требуемые административные права    | Для установки Indeed Windows Logon требуются права локального Администратора (Administrator).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Настройки межсетевого экрана        | <p>Для корректной работы системы Indeed AM измените следующие настройки межсетевого экрана на Indeed AM Server и на рабочих станциях, на которых установлен компонент Indeed Windows Logon:</p> <ul style="list-style-type: none"> <li>• Открыть порт 53 (DNS) (TCP и UDP) для всех процессов в обоих направлениях. Этот порт используется системой Indeed AM для определения наличия сети.</li> <li>• Открыть порт 135 (RPC) для всех процессов в обоих направлениях. Этот порт используется системой для коммуникации между рабочими станциями пользователей и Core Server.</li> <li>• Открыть порт 389 (LDAP) для всех процессов в обоих направлениях. Этот порт используется системой для получения доступа в Active Directory (в том числе при поиске Core Server).</li> </ul> |

# Indeed Enterprise Single Sign-On

|                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Аппаратные требования к рабочим станциям пользователей | <ul style="list-style-type: none"><li>• не менее 50 МБ свободного пространства на диске</li><li>• наличие .NET Framework версии 4.5 и выше</li><li>• Веб-браузеры:<ul style="list-style-type: none"><li>◦ Internet Explorer 8 и выше</li><li>◦ Mozilla Firefox 52.6 и выше</li><li>◦ Google Chrome 49.0 и выше</li></ul></li><li>• USB-порт для подключения устройства аутентификации</li></ul>                                                                                                                                                                                                                                                                                                                                                          |
| Поддерживаемые операционные системы                    | <ul style="list-style-type: none"><li>• Windows Server 2012/2012 R2</li><li>• Windows Server 2016</li><li>• Windows Server 2019</li><li>• Windows Server 2022</li><li>• Windows 7 SP1 32/64bit</li><li>• Windows 8.1 32/64bit</li><li>• Windows 10 32/64bit</li><li>• Windows 11 32/64bit</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Настройки межсетевого экрана                           | <p>Задайте следующие настройки межсетевого экрана на сервере Indeed ESSO и на рабочих станциях с установленным Indeed AM ESSO Agent:</p> <ul style="list-style-type: none"><li>• Открыть порт 53 (DNS) (TCP и UDP) для всех процессов в обоих направлениях. Этот порт используется системой Indeed AM для определения наличия сети.</li><li>• Открыть порт 135 (RPC) для всех процессов в обоих направлениях. Этот порт используется системой для коммуникации между рабочими станциями пользователей и Indeed AM Enterprise Server.</li><li>• 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 Enterprise Server).</li></ul> |

# Настройка окружения



## Размещение компонентов

Требования для работы компонентов Indeed AM



## Сетевое взаимодействие

Взаимодействие компонентов Indeed AM



## Компоненты Internet Information Services

Обязательные компоненты для работы Indeed Access Manager



## Хранилище данных

Содержит данные для Core Server, Log Server и Key Server



## Каталог пользователей

Содержит данные о пользователях системы Indeed Access Manager



## Клиентский сертификат

Проверяет запросы к серверу

# Размещение компонентов

## Размещение №1

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

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

Модули интеграции могут быть развернуты на отдельных машинах.

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

## Системные требования

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

## Размещение №2

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

| Наименование сервера                                                      | Требование                                                                                                                                                                                                   | Компоненты Indeed AM                                                        |
|---------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| Indeed AM Server\Indeed AM Log Server                                     | Обязательный компонент                                                                                                                                                                                       | Indeed AM Server, Indeed AM Log Server                                      |
| Indeed AM Server\Indeed AM Management Console\Indeed AM Identity Provider | Обязательный компонент. Indeed AM Identity Provider обязателен только для сценариев, где требуется выполнять обучение аутентификаторов внешним пользователям.                                                | Indeed AM Server, Indeed AM Management Console, Indeed AM Identity Provider |
| Indeed AM Indeed Key Server\Indeed AM User Console                        | Опциональный компонент. Indeed Key Server требуется только для сценариев с использованием push-аутентификации. Indeed AM User Console требуется для обучения аутентификаторов внешним пользователям системы. | Indeed AM Indeed Key Server, Indeed AM User Console                         |

| Наименование сервера                               | Требование                                                                         | Компоненты Indeed AM                                 |
|----------------------------------------------------|------------------------------------------------------------------------------------|------------------------------------------------------|
| Indeed AM Indeed Key Server\Indeed AM User Console | Опциональный компонент. Только для сценариев с использованием push-аутентификации. | Indeed AM Indeed Key Server, Indeed AM User Console  |
| Indeed AM Extensions                               | Обязательный компонент. Тип модуля интеграции зависит от конечного сценария.       | Модули интеграции системы Indeed AM                  |
| Балансировщик нагрузки                             | Системные требования зависят от выбранного балансировщика.                         | Балансировка осуществляется сторонними компонентами. |

## Системные требования

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

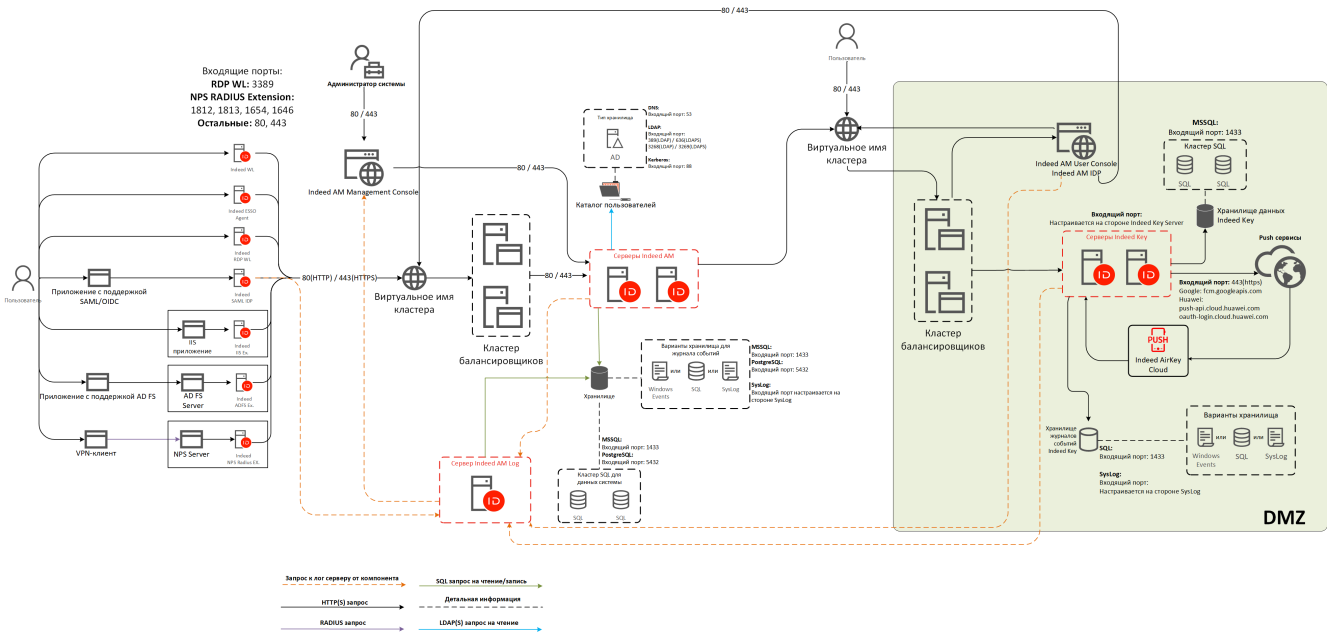
| Наименование сервера                                                      | CPU     | RAM  | HDD   | Network    |
|---------------------------------------------------------------------------|---------|------|-------|------------|
| Indeed AM Server\Indeed AM Log Server                                     | 8 cores | 8 ГБ | 200ГБ | 100 Мбит/с |
| Indeed AM Server\Indeed AM Management Console\Indeed AM Identity Provider | 8 cores | 8 ГБ | 200ГБ | 100 Мбит/с |
| Indeed AM Indeed Key Server\Indeed AM User Console                        | 8 cores | 8 ГБ | 150ГБ | 100 Мбит/с |
| Indeed AM Indeed Key Server\Indeed AM User Console                        | 8 cores | 8 ГБ | 150ГБ | 100 Мбит/с |

| Наименование сервера                 | CPU                                                          | RAM  | HDD   | Network    |
|--------------------------------------|--------------------------------------------------------------|------|-------|------------|
| Indeed AM Extensions                 | Системные требования зависят от выбранного модуля интеграции |      |       |            |
| ПК с БД Indeed и событиями Indeed №1 | 8 cores                                                      | 8 ГБ | 500ГБ | 100 Мбит/с |
| ПК с БД Indeed и событиями Indeed №2 | 8 cores                                                      | 8 ГБ | 500ГБ | 100 Мбит/с |

# Сетевое взаимодействие

На изображении представлена 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, Indeed Log Server также может варьироваться в зависимости от ваших потребностей.



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

| 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   |



| Наименование                                   | Протокол | Входящий порт                                       | Исходящий порт |
|------------------------------------------------|----------|-----------------------------------------------------|----------------|
| 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   |

| Наименование                | Протокол | Входящий порт       | Исходящий порт |
|-----------------------------|----------|---------------------|----------------|
| 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   |

Для корректной работы Indeed AM необходимо обеспечить сетевую доступность между компонентами. На межсетевых экранах (файерволах) каждого из компонентов должны быть настроены правила, разрешающие входящий и исходящий трафик по протоколам и портам, указанным в таблице выше.

# Компоненты 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 серверным компонентам](#) и [модулям интеграции](#).



## ВАЖНО!

Запустите Powershell от имени администратора.

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

- скрипт *Indeed.Main.IIS.Install.MSServer.ps1* используется для серверных компонентов;
- скрипт *Indeed.SAML.IIS.Install.MSServer.ps1* используется для серверных компонентов и модуля Identity Provider.

Если политикой безопасности запрещено запускать неподписанные скрипты, выполните команду, чтобы отменить запрет:

```
Set-ExecutionPolicy Unrestricted
```

Если возможности отменить запрет нет, откройте скрипт с помощью текстового редактора, скопируйте содержимое целиком и вставьте в Powershell — скрипт запустится.

# Хранилище данных

Для работы Indeed Access Manager нужны две базы данных. В одной из баз данных хранится информация для компонента **Indeed AM Core Server**. В другой — для компонента **Indeed AM Log Server**.

Если вы планируете использовать мобильное приложение Indeed Key, вам необходима отдельная база данных для сервера приложения **Indeed AM Key Server**.

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

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

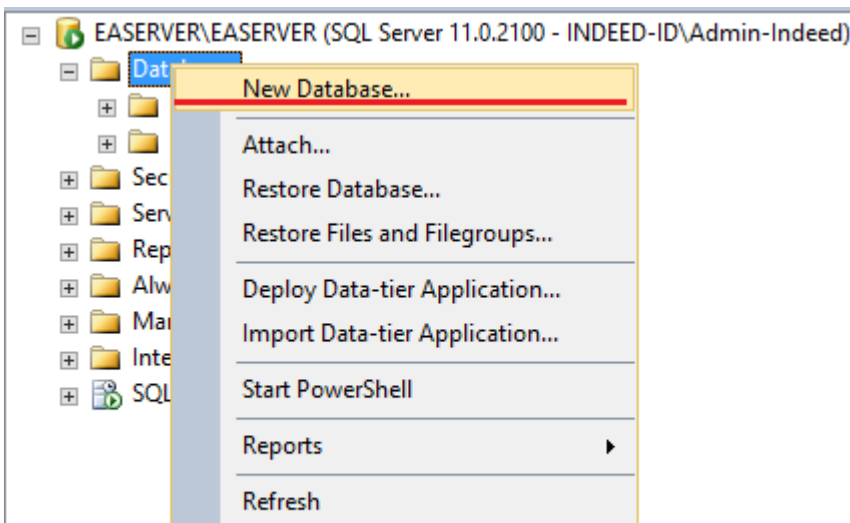
## Microsoft SQL

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.

### 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.



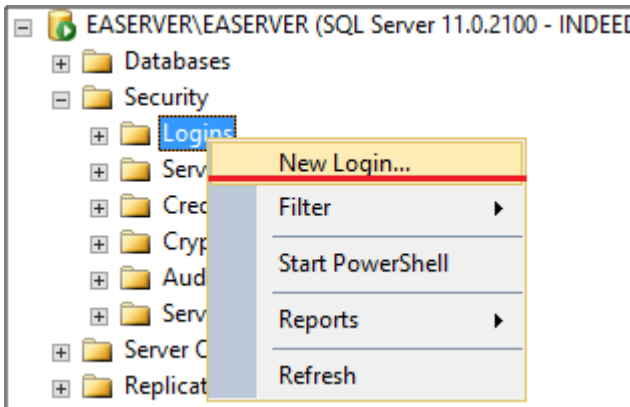
#### ВАЖНО!

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

5. Включите смешанную аутентификацию:

1. Правой кнопкой мыши нажмите узел экземпляра сервера SQL Server и выберите Properties.
  2. На странице Security в разделе Server authentication выберите SQL Server and Windows Authentication mode.
6. Убедитесь, что у сервисной учетной записи включена следующая настройка:

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

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

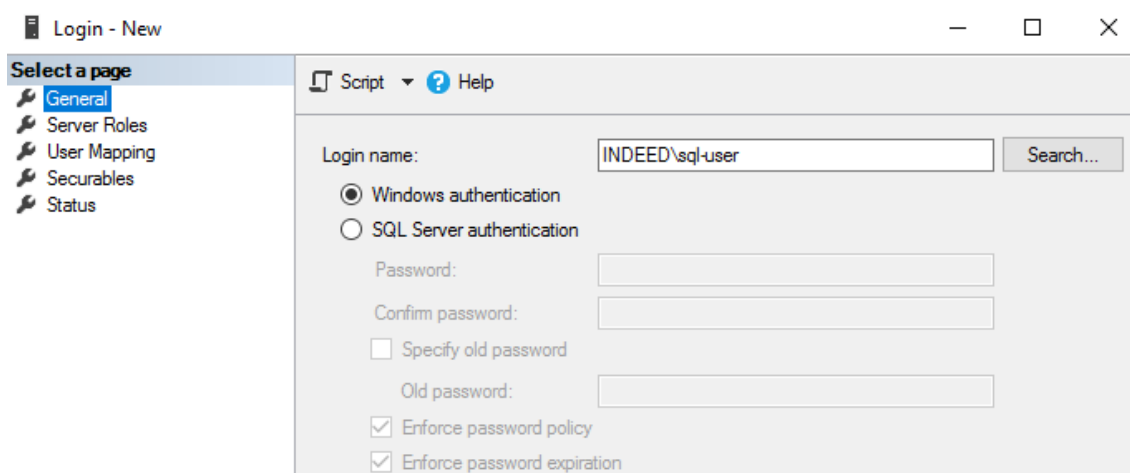
1. Во вкладке Настройка клиента Native client SQL выберите Клиентские протоколы.
2. Нажмите правой кнопкой мыши на TCP/IP, выберите Свойства и установите значение Да для включения протокола TCP/IP.
3. Включите TCP/IP во всех вкладках Настройка клиента Native client SQL.

## 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:

1. Найдите ранее созданного пользователя.
2. В меню слева выберите User Mapping.
3. Выберите ранее созданные базы.
4. Для каждой базы выберите роль db\_owner и нажмите ОК.

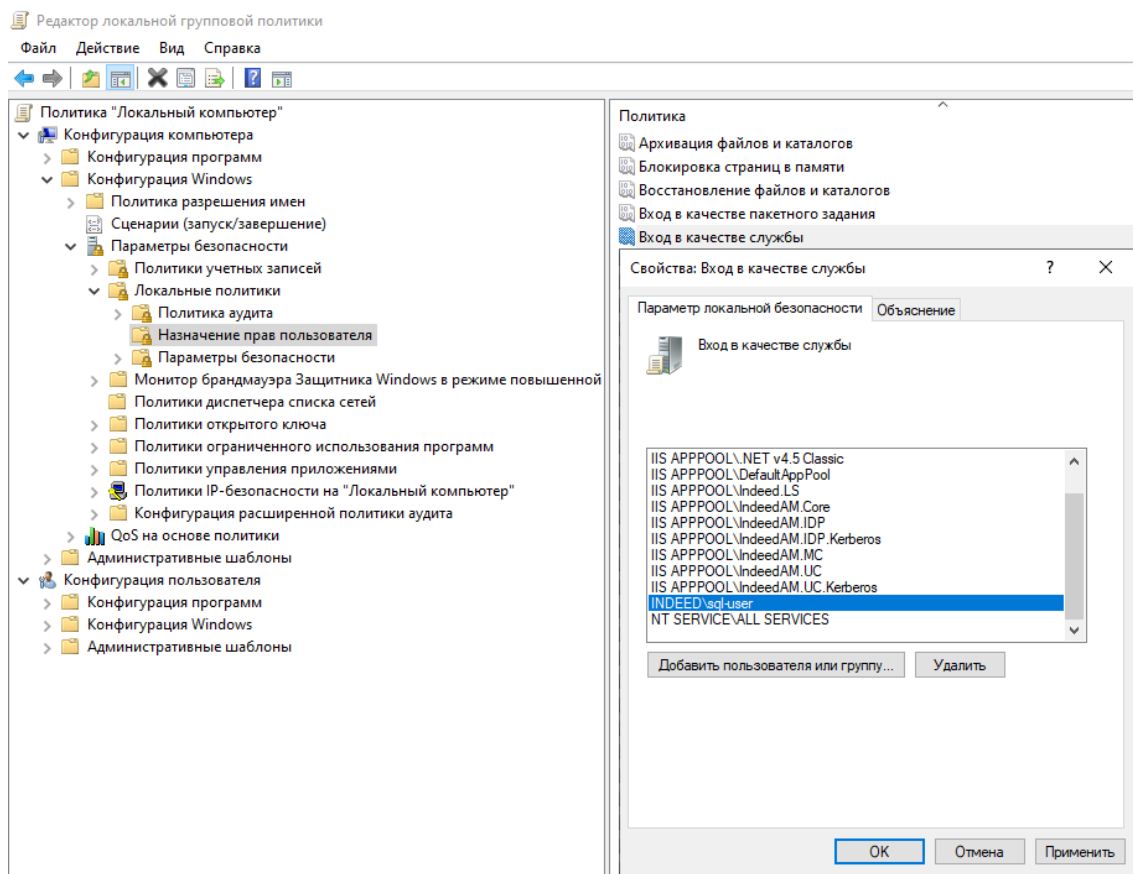


7. Запустите редактор локальной групповой политики и выполните следующие действия:

1. Раскройте панель Конфигурация компьютера→Конфигурация Windows→Параметры безопасности→Локальные политики→Назначение прав

пользователя.

2. В списке справа выберите политику Вход в качестве службы.
3. Нажмите Добавить пользователя или группу, введите имя ранее созданного пользователя и нажмите Проверить имена.
4. Нажмите ОК, чтобы добавить пользователя в политику.



8. Откройте в текстовом редакторе конфигурационный файл компонента, для которого вы создаете базу:

1. Файл для компонента Indeed AM Server хранится в  
*C:\inetpub\wwwroot\am\core\Web.config.*
2. Файл для компонента Indeed AM Log Server хранится в  
*C:\inetpub\wwwroot\ls\targetConfigs\sampleDb.config.*

9. 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>
```

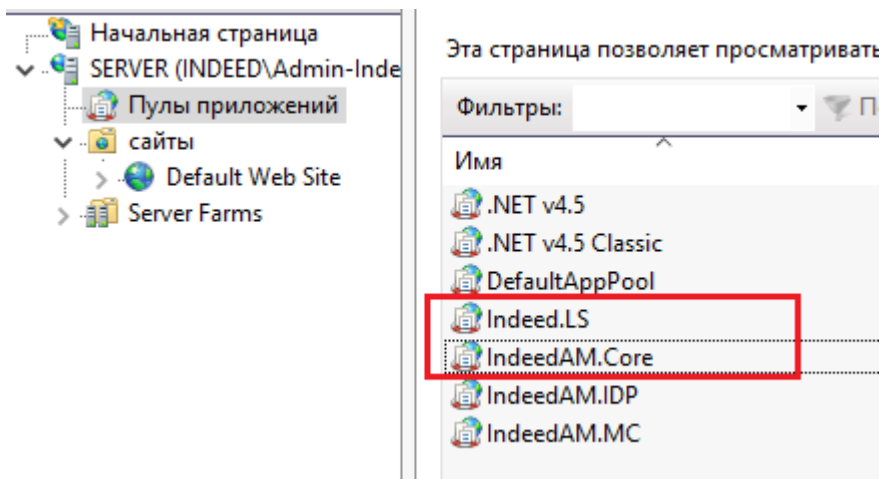
Пример для Indeed AM Log Server

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

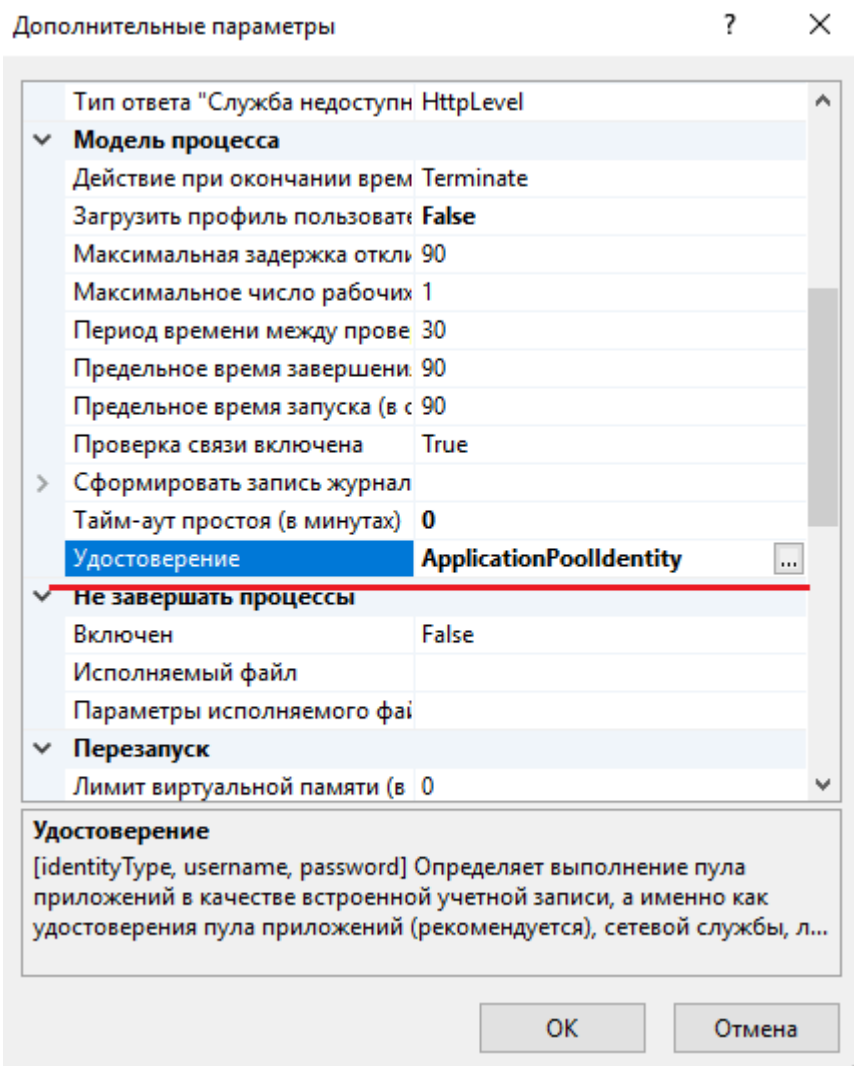
10. Сохраните конфигурационный файл.

Далее настройте пулы приложений в Internet Information Services.

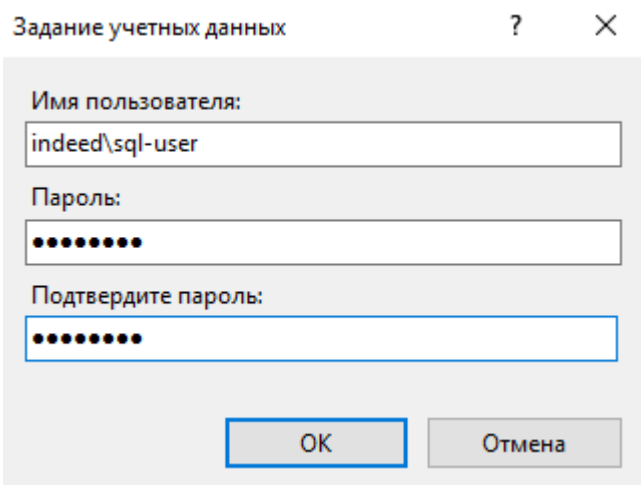
1. Запустите Диспетчер служб IIS.
2. Выберите Пулы приложений→IndeedAM.Core (для Indeed AM Server)\Indeed.LS (для Indeed AM Log Server).



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.



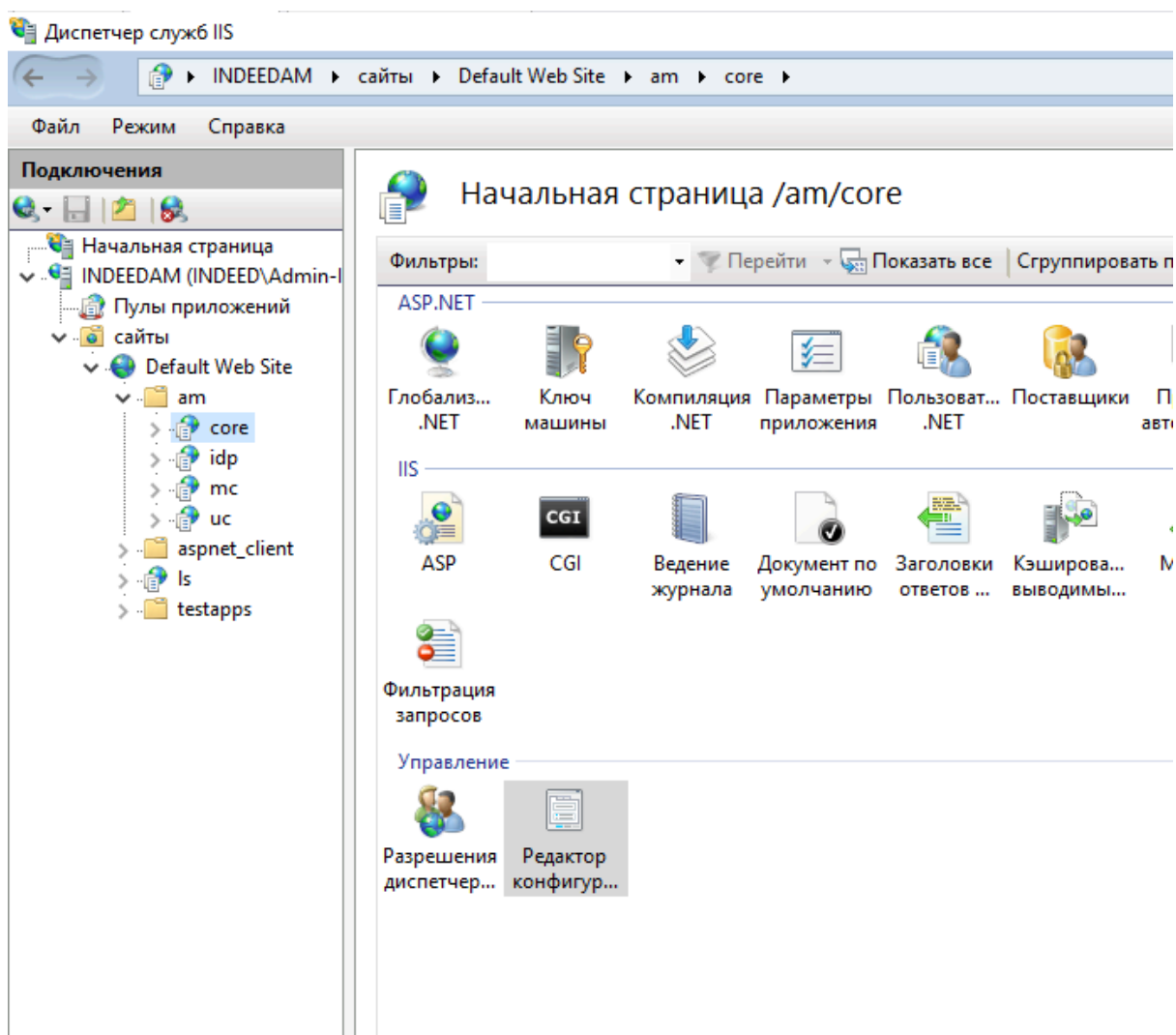
7. В разделе Действия перезапустите пул приложения, для которого выполнялась настройка, и откройте начальную страницу приложения в IIS.

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.

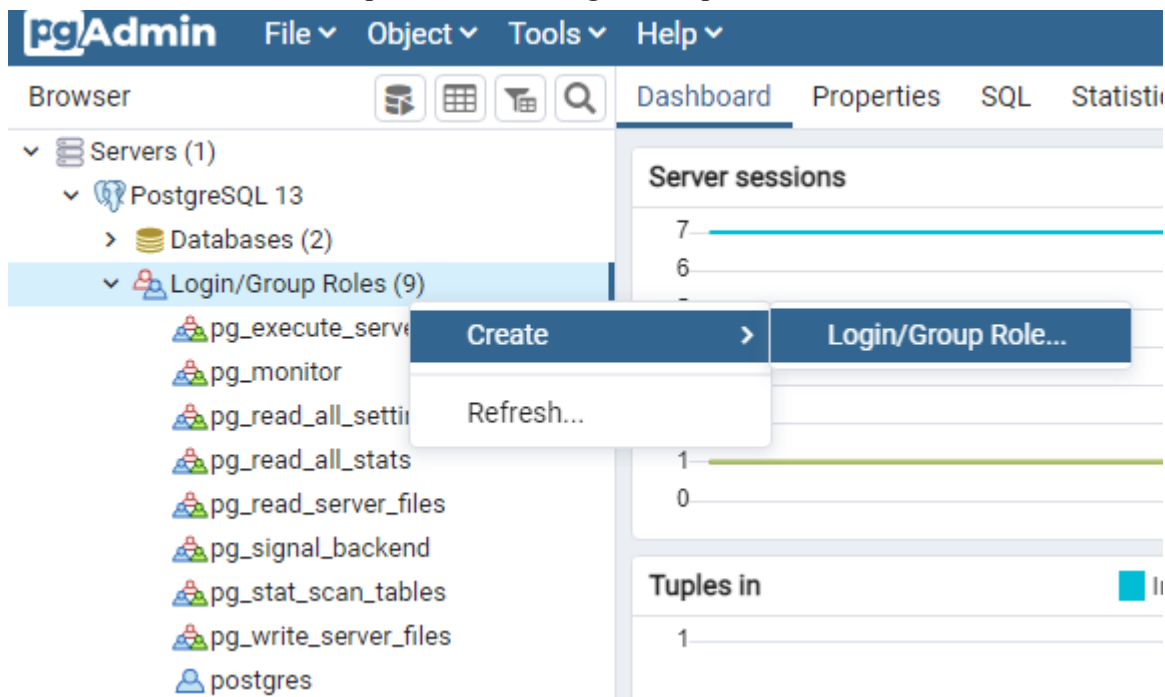
На сервере с установленным PostgreSQL Server создайте две базы данных — одну для Indeed AM Server, другую для Indeed AM Log Server — и сервисную учетную запись.

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 Create→Login/Group Role...



4. В окне Create-Login/Group Role выполните следующие действия:

1. На вкладке General в поле Name введите имя пользователя.
2. На вкладке Definition в поле Password введите пароль. В поле Account Expires укажите значение No expiry.

 Create - Login/Group Role ✕

General Definition Privileges Membership Parameters Security SQL

|                                                                                  |                                                                                               |
|----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| Password                                                                         | .....                                                                                         |
| Account expires                                                                  | No Expiry  |
| Please note that if you leave this field blank, then password will never expire. |                                                                                               |
| Connection limit                                                                 | -1                                                                                            |

3. На вкладке Privileges включите опцию Can login? и нажмите Save.

 Create - Login/Group Role ✕

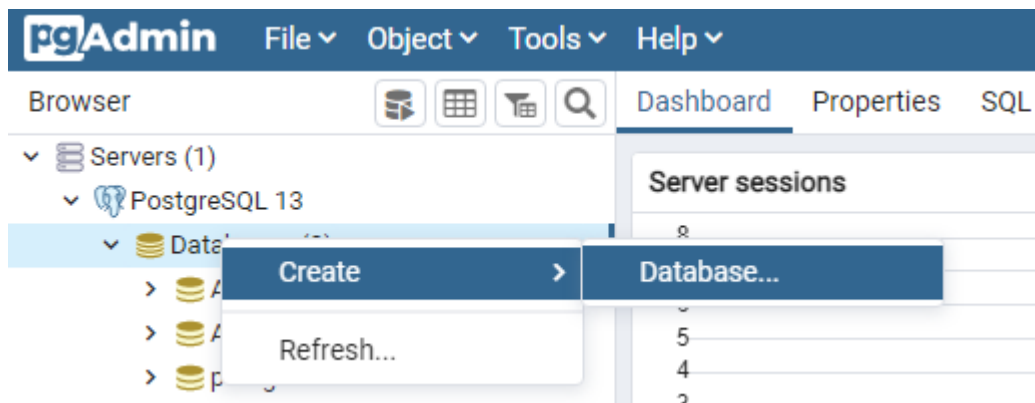
General Definition Privileges Membership Parameters Security SQL

|                                                 |                                         |
|-------------------------------------------------|-----------------------------------------|
| Can login?                                      | <input checked="" type="checkbox"/> Yes |
| Superuser?                                      | <input type="checkbox"/> No             |
| Create roles?                                   | <input type="checkbox"/> No             |
| Create databases?                               | <input type="checkbox"/> No             |
| Update catalog?                                 | <input type="checkbox"/> No             |
| Inherit rights from the parent roles?           | <input checked="" type="checkbox"/> Yes |
| Can initiate streaming replication and backups? | <input type="checkbox"/> No             |

## Создание базы данных

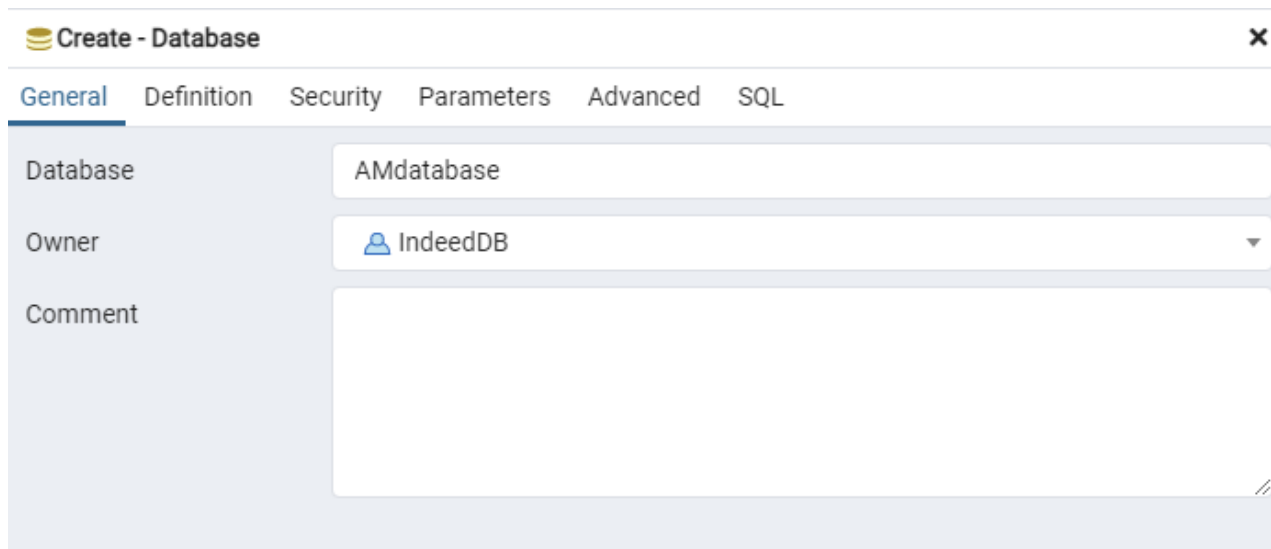
Чтобы создать базу данных, выполните следующие действия:

1. Откройте pgAdmin и подключитесь к серверу.
2. Раскройте компоненты вашего сервера SQL.
3. Правкой кнопкой мыши нажмите Databases.
4. Выберите Create→Database...



5. В окне Create-Database выполните следующие действия:

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



## Настройка удаленного подключения к базе данных

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

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

```
TYPE DATABASE USER ADDRESS METHOD
```

**TYPE** — тип подключения. Если вы не указываете тип подключения, по умолчанию используется подключение по TCP/IP.

**DATABASE** — имя базы данных, для которой вы настраиваете подключение.

**USER** — имя пользователя, который будет подключаться к этой базе данных.

**ADDRESS** — IP-адрес машины, на которой установлен компонент Indeed AM. Укажите значение с маской.

**METHOD** — метод аутентификации пользователя. Возможные значения: **md5**, **scram-sha-256**.

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.

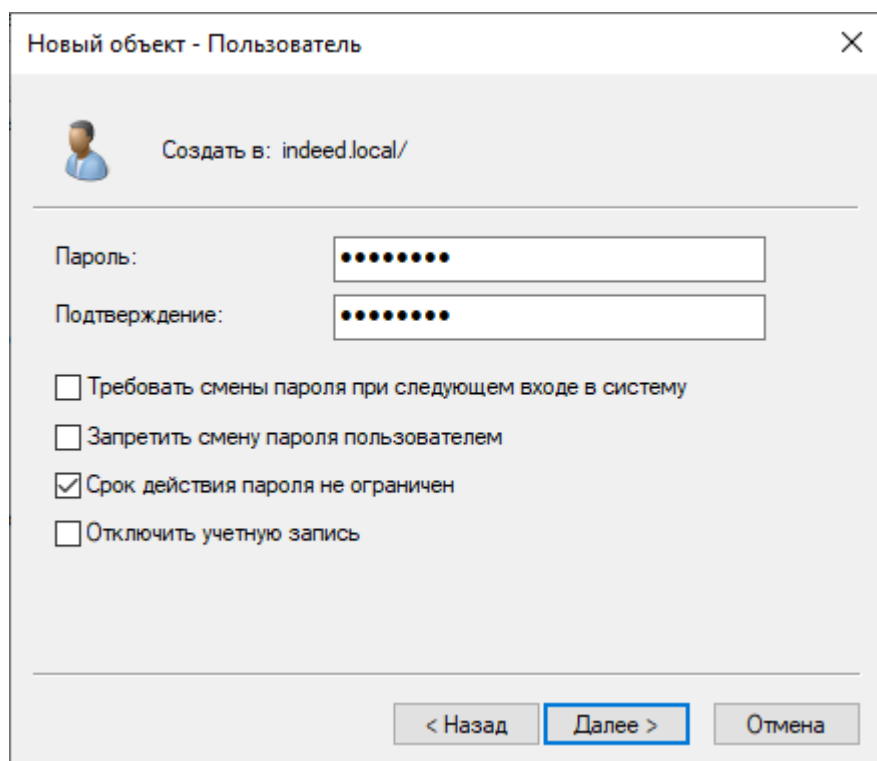
Indeed Access Manager только читает данные из Active Directory, новые данные не записываются.

## 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

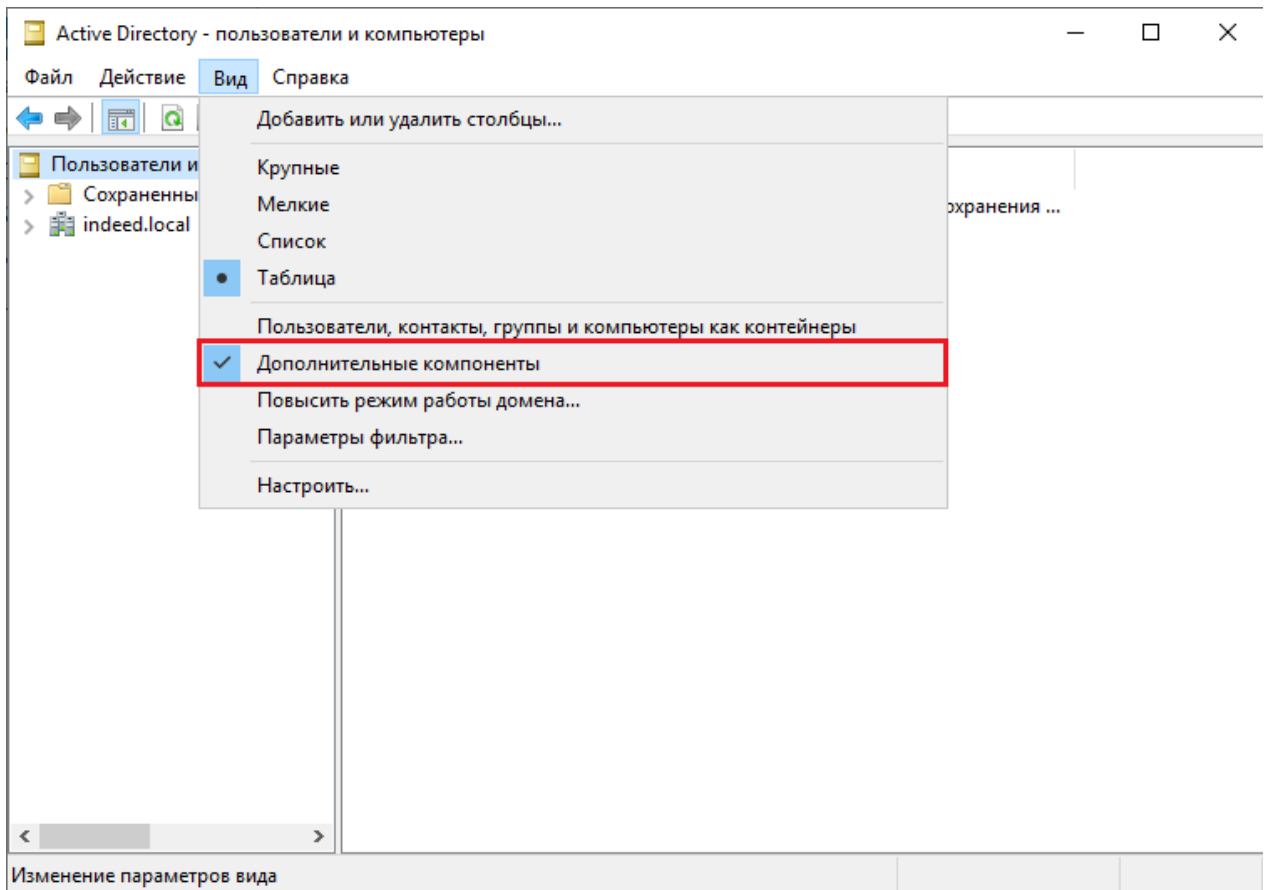
< Назад **Далее >** Отмена

## 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:

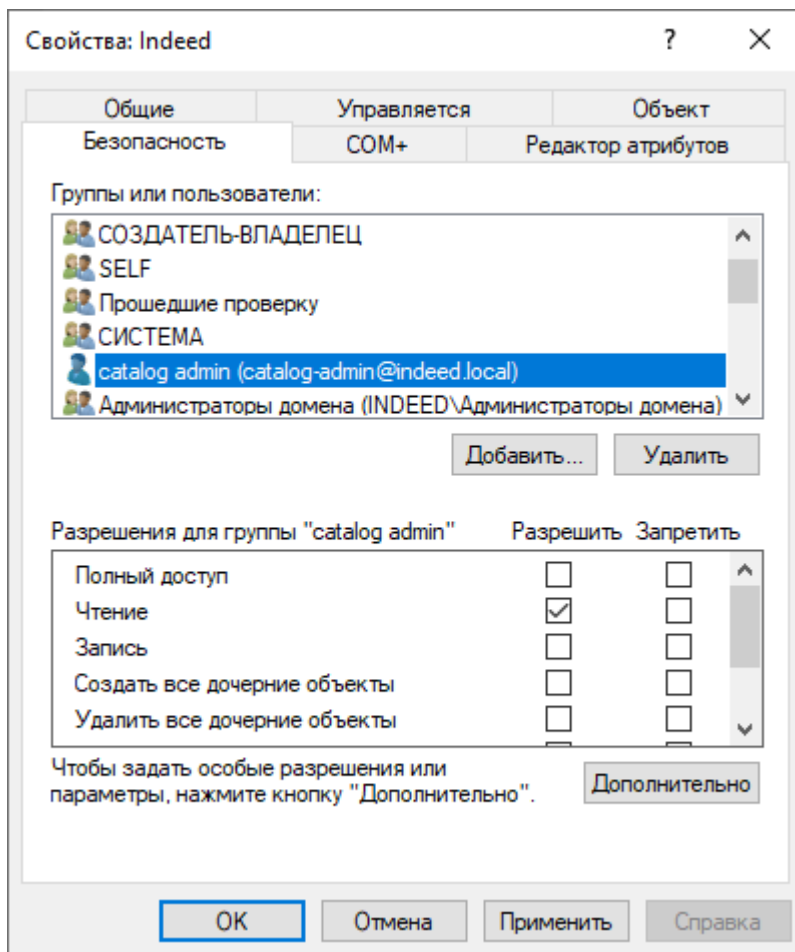
1. Откройте Active Directory Users and Computers.
2. Во вкладке View включите опцию Advanced Features.



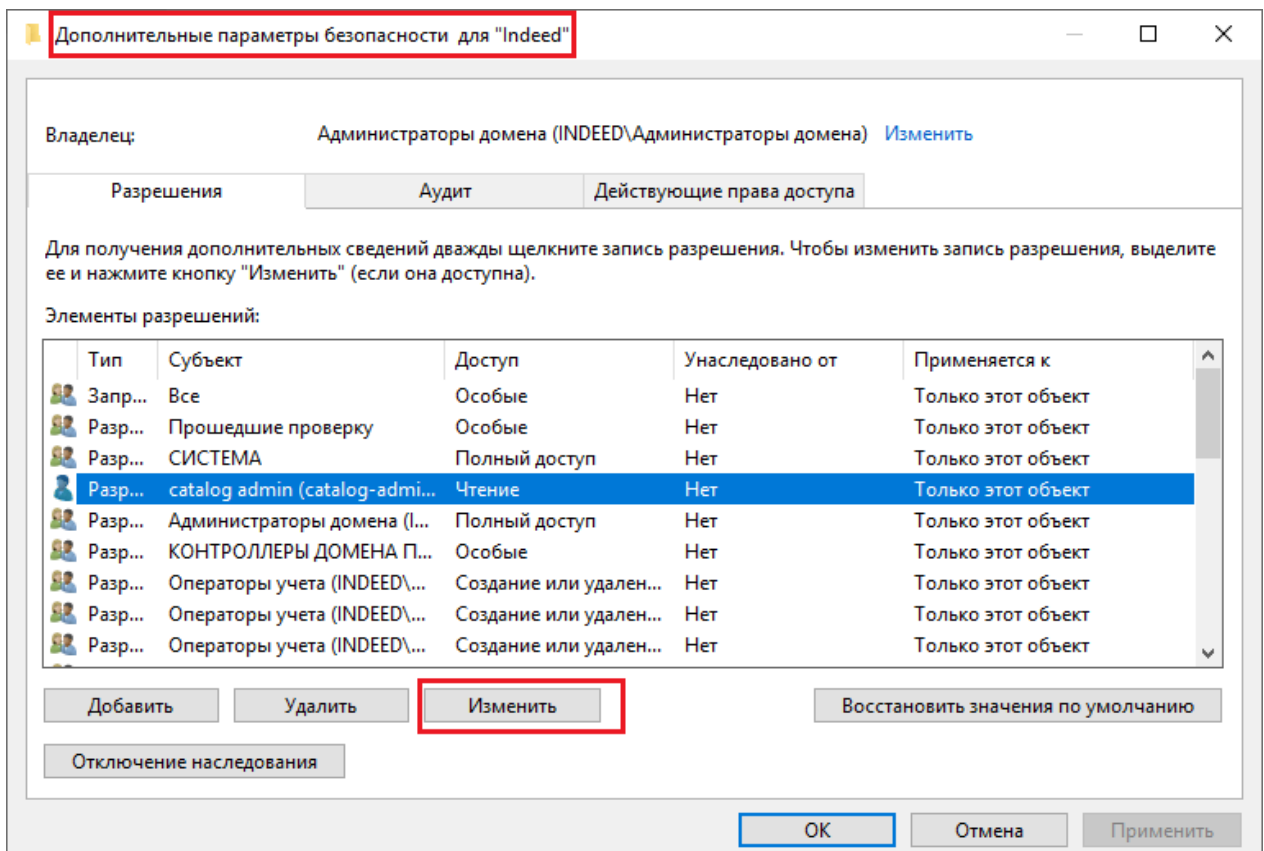
3. Правой кнопкой мыши нажмите объект с пользователями и выберите Properties.

4. В окне Properties выполните следующие действия:

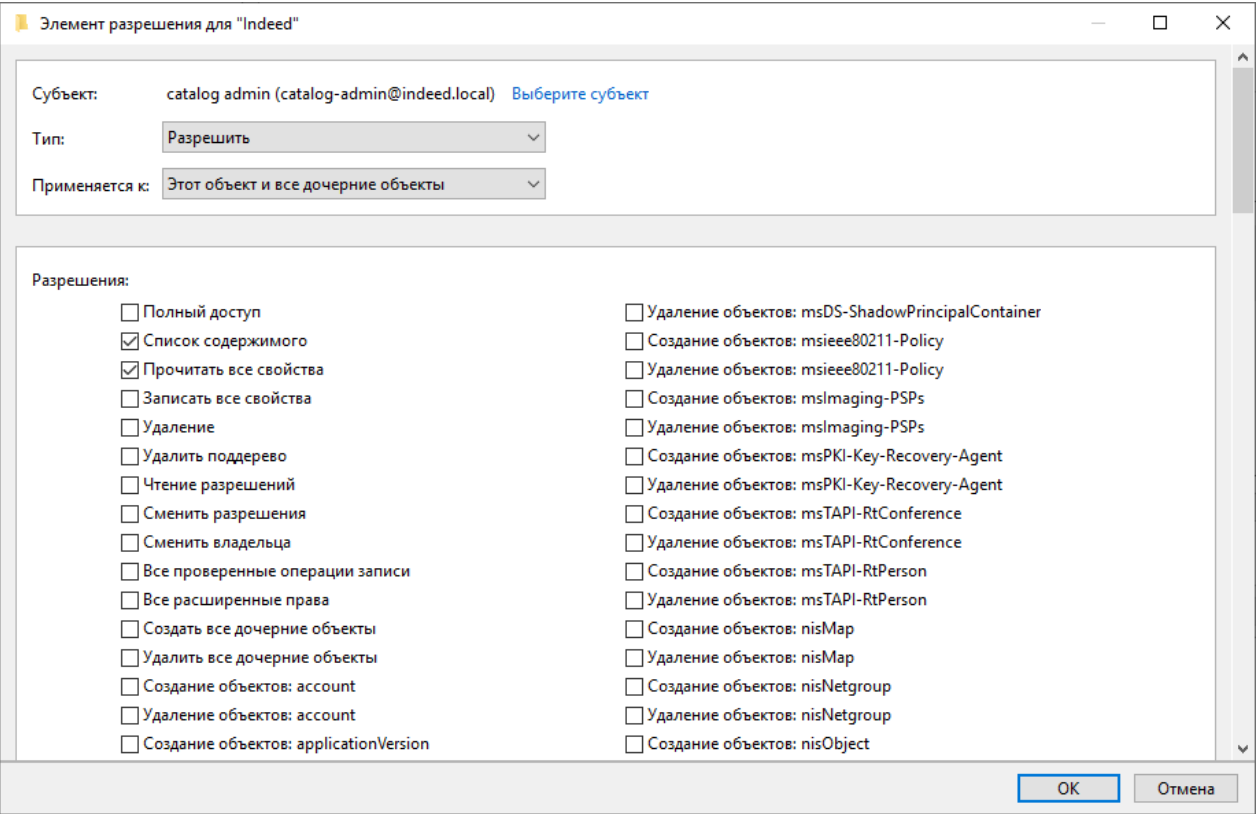
1. Откройте вкладку Security.
2. В разделе Group or user names добавьте созданную ранее сервисную учетную запись.
3. В разделе Permissions for выберите опцию Read и нажмите кнопку Advanced.



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



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



## Атрибуты пользователей Active Directory

| Атрибут пользователя | Описание                                                                                                                                                                           |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| objectGUID           | Глобальный уникальный идентификатор объекта                                                                                                                                        |
| objectSid            | Уникальный идентификатор безопасности, присваиваемый каждому объекту в Active Directory. Используется для управления доступом к ресурсам и аутентификации пользователей и объектов |
| distinguishedName    | Уникальное имя объекта в иерархии Active Directory, состоящее из полного пути к объекту. Например,<br><i>CN=testuser;OU=Users,DC=domain,DC=com</i>                                 |

| Атрибут<br>пользователя | Описание                                                                                                                                          |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| tokenGroups             | Вычисляемый атрибут, содержащий список Sid всех групп, в том числе и вложенных, в которых состоит пользователь на момент входа в систему          |
| memberOf                | Атрибут, содержащий distinguishedName групп, прямыми членами которых является пользователь или компьютер                                          |
| sAMAccountName          | Учетное имя пользователя, группы или компьютера, используемое для поддержки совместимости с предыдущими версиями Windows. Например, <i>ivanov</i> |
| msDS-PrincipalName      | Каноническое имя пользователя. Например <i>DOMAIN\username</i>                                                                                    |

# Клиентский сертификат

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 Далее→Готово.

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

1. Откройте Диспетчер служб IIS.
2. Выберите Indeed AM→Сайты→Default Web Site→am→core.
3. Нажмите Параметры SSL.
4. Выберите опцию Принимать клиентские сертификаты.

# Установка и настройка серверных КОМПОНЕНТОВ



## Indeed Log Server

Сервер для управления событиями Indeed Access Manager



## Indeed Core Server

Количество глав: 5



## Indeed Management Console

Количество глав: 4



## Indeed User Console

Количество глав: 5



## Indeed Key Server

Сервер для работы приложения Indeed Key



## Indeed Phone Management Server

Приложение для управления номерами пользователей



## Indeed Reset Password

Утилита для сброса пароля пользователя



## Расположение конфигурационных файлов

Как найти конфигурационные файлы



# Indeed Log Server

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

События записываются в базы данных.

## Как создать и настроить базу данных

Чтобы настроить Log Server:

1. **Установите** Log Server и Eventlog.
2. **Создайте** привязку HTTPS в настройках IIS.
3. **Настройте** Log Server в соответствии с подходящим хранилищем данных.
4. При необходимости измените параметры **кеширования событий** и **локализацию**.

## Установить Log Server и EventLog

Прежде чем начать установку, ознакомьтесь с **системными требованиями**.

1. Установите Log Server, запустив файл *Indeed AM <номер версии>\Indeed AM Log Server\Indeed.LogServer-<номер версии>.x64.ru-ru.msi*.
2. Установите EventLog на компьютере с Log Server, запустив файл *Indeed AM <номер версии>\Indeed AM Log Server\IndeedAM.Server.EventLog-<номер версии>.x64.ru-ru.msi*.

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

## Создать привязку HTTPS

В процессе установки для Log Server в настройках IIS включается обязательное требование SSL-сертификата. Поэтому для корректной работы модуля необходимо создать привязку HTTPS.

Чтобы создать привязку HTTPS:

1. В Диспетчере служб IIS в левом меню выберите Indeed AM → сайты → Default Web Site
2. В правом меню в разделе Действия нажмите Привязки.

3. Нажмите Добавить и в открывшемся окне задайте следующие параметры:

- В поле Тип выберите *https*.
- В поле Порт укажите *443*.
- В поле SSL-сертификат выберите сертификат Core Server.

4. Нажмите ОК, чтобы сохранить привязку.

Если вы не намерены использовать протокол HTTPS, **отключите требование SSL-сертификата** в настройках IIS для Log Server.

## Настроить Log Server с разным типом хранилища данных

Вы можете выбрать доступное вам хранилище данных:

- базы данных Microsoft SQL или PostgreSQL
- хранилище в EventLog
- хранилище в SysLog
- резервное хранилище

## Microsoft SQL

1. Откройте конфигурационный файл `C:\inetpub\wwwroot\ls\targetConfigs\sampleDb.config`.
2. Укажите данные для подключения к базе данных в теге `connectionString`.

- `Data Source` — задает экземпляр сервера. Эта настройка является обязательной 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>
```

3. Откройте конфигурационный файл сервера `C:\inetpub\wwwroot\ls\clientApps.config`.
4. Раскомментируйте блок с `"Application`  
`Id"="ea"`. В тегах `TargetId` и `ReadTargetId` укажите значение `sampleDb`.

❗ ПРИМЕЧАНИЕ

В тегах `ReadTargetId` указывается идентификатор хранилища, откуда будут считываться события.

В блоке `WriteTargets`, в тегах `TargetId` указывается идентификатор хранилища, куда будут записываться события.

Идентификаторы заданы в теге `Targets`, конфигурационные файлы для каждого типа находятся в папке `targetConfigs` с соответствующим именем.

#### Пример

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

#### Шифрование/Расшифрование конфигурационного файла

1. Запустите командную строку от имени администратора.
2. В командной строке перейдите в папку с утилитой для шифрования *Indeed.LogServer.Config.Encryptor*.

#### Шифрование конфигурационного файла

Чтобы зашифровать конфигурационный файл, запустите 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 таргета конфигурационного файла. Опциональный  
параметр, значение по умолчанию – Sql.

### Расшифровка конфигурационного файла

Чтобы расшифровать конфигурационный файл, запустите 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 таргета конфигурационного файла. Опциональный  
параметр, значение по умолчанию – Sql.

## ▼ PostgreSQL

### PostgreSQL

1. Перейдите в папку `C:\inetpub\wwwroot\ls\targetConfigs`.
2. Создайте файл с произвольным именем и расширением `.CONFIG`, например `postgresDb.config`.
3. Добавьте в файл следующие строки:

```
<?xml version="1.0" encoding="utf-8"?>
<Settings>
  <ConnectionString>server=server_dns_name;port=5432;user
id=account_name;password=account_password;database=database_name</
</Settings>
```

4. В строке `ConnectionString` задайте значения следующих параметров:

- `server` — DNS/IP-адрес сервера с базой данных PostgreSQL.
- `port` — порт, по которому будет происходить подключение. Значение по умолчанию — 5432, но его можно изменить.
- `user ID` — имя пользователя, который имеет полные права для базы данных Database.
- `password` — пароль пользователя.
- `database` — имя базы данных Log Server.

#### Пример

```
server=192.200.1.2;port=5432;user
id=IndeedDB;password=Passw0rd;database=LogServerDB
```

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 укажите значение postgresDb.

ⓘ ПРИМЕЧАНИЕ

В тегах ReadTargetId указывается идентификатор хранилища, откуда будут считываться события.

В блоке WriteTargets, в тегах TargetId указывается идентификатор хранилища, куда будут записываться события.

Идентификаторы заданы в теге 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

## События

Экспортировать

|                                                              |                                        |                                                          |                                                  |
|--------------------------------------------------------------|----------------------------------------|----------------------------------------------------------|--------------------------------------------------|
| Пользователь или инициатор<br>Не задано <span>Выбрать</span> | Приложение<br>Не задано <span>▼</span> | Начальная дата<br>2020/09/05 00:00 <span>📅</span>        | Конечная дата<br>2020/09/09 00:00 <span>📅</span> |
| Тип аутентификатора<br>Не задано <span>▼</span>              | Модуль<br>Не задано <span>▼</span>     | Описание содержит <span>ℹ</span><br><input type="text"/> | Тип события<br>Не задано <span>▼</span>          |
| Код события<br><input type="text"/> <span>Выбрать</span>     |                                        |                                                          |                                                  |
| <span>Применить</span> <span>Сбросить</span>                 |                                        |                                                          |                                                  |

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

## Шифрование/Расшифрование конфигурационного файла

1. Запустите командную строку от имени администратора.
2. В командной строке перейдите в папку с утилитой для шифрования  
*Indeed.LogServer.Config.Encryptor.*

## Шифрование конфигурационного файла

Чтобы зашифровать конфигурационный файл, запустите утилиту со следующими параметрами:

### Пример

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

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

-t, --type Тип таргета конфигурационного файла. Опциональный параметр, значение по умолчанию – Sql.

## Расшифровка конфигурационного файла



Чтобы расшифровать конфигурационный файл, запустите утилиту со следующими параметрами:

#### Пример

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

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

-t, --type      Тип таргета конфигурационного файла. Опциональный параметр, значение по умолчанию – Sql.

## Хранилище в EventLog

Редактирование конфигурационного файла

1. Откройте конфигурационный файл сервера *C:\inetpub\wwwroot\ls\clientApps.config*.
2. Раскомментируйте блок с `"Application`  
`Id"="ea"`. В тегах `TargetId` и `ReadTargetId` укажите значение *sampleEventLog*.

### ⚠ ПРИМЕЧАНИЕ

В тегах `ReadTargetId` указывается идентификатор хранилища, откуда будут считываться события.

В блоке `WriteTargets`, в тегах `TargetId` указывается идентификатор хранилища, куда будут записываться события.

Идентификаторы заданы в теге `Targets`, конфигурационные файлы для каждого типа находятся в папке *targetConfigs* с соответствующим именем.

### Пример

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

Пример отображения

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

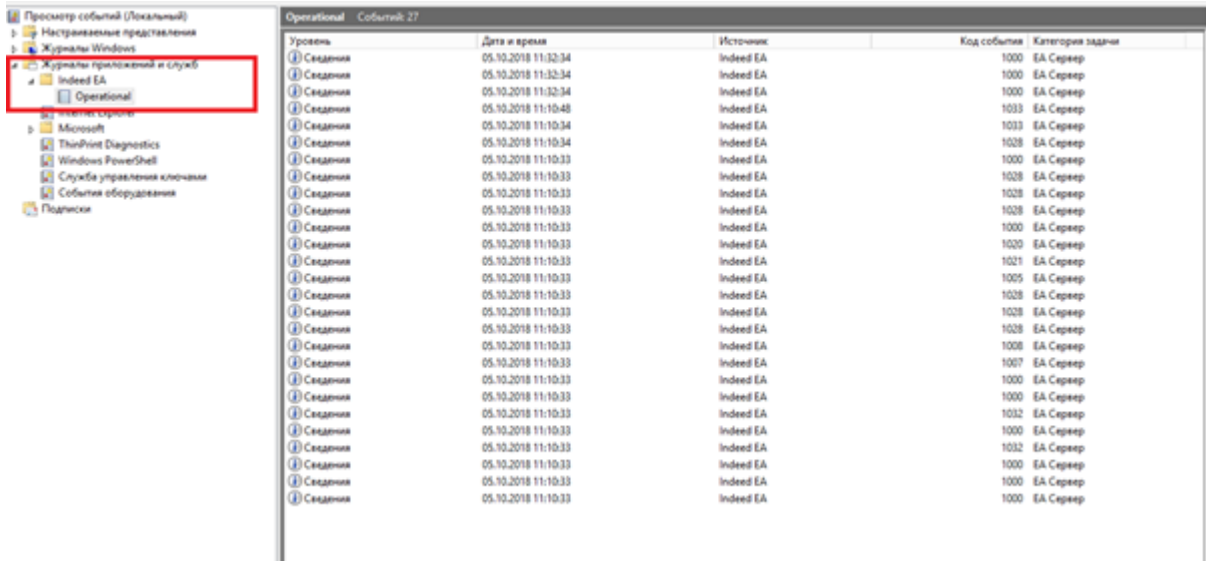
Выбрать

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 |

Отображение журнала в событиях Windows



## Хранилище в SysLog

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

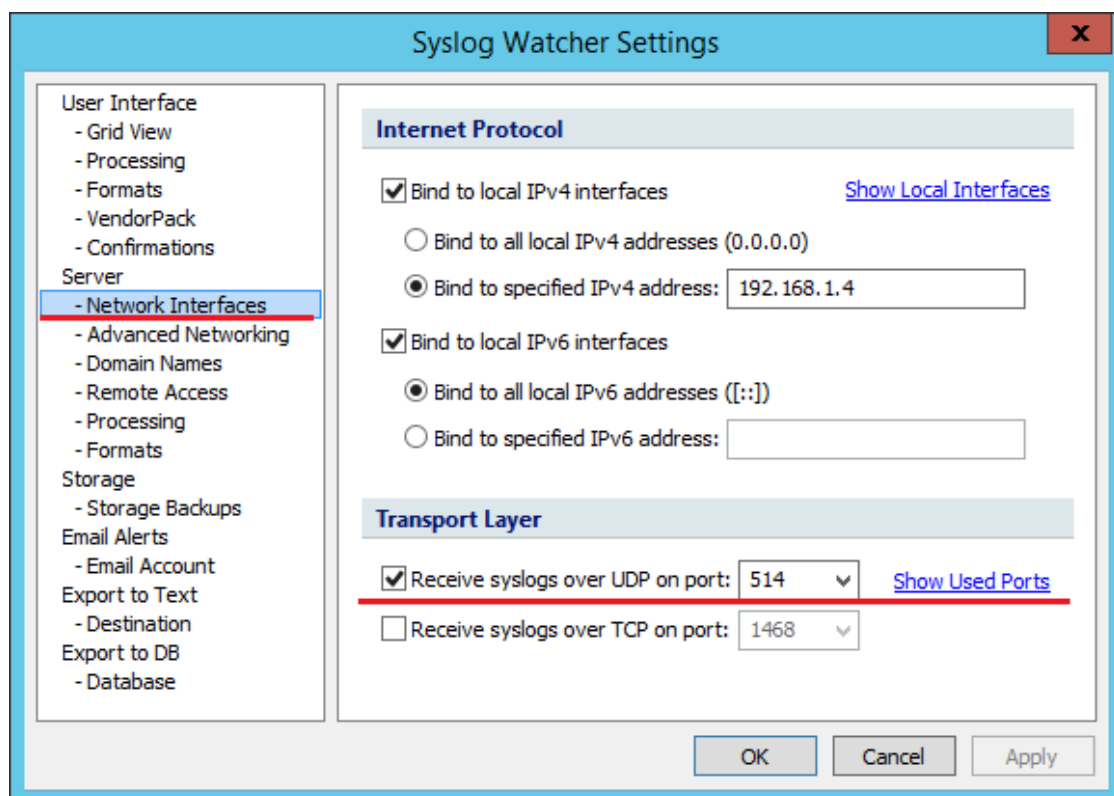
Скачать утилиту можно на официальном сайте <https://syslogwatcher.com>

Чтобы установить syslog-сервер:

1. Запустите установочный файл *SyslogWatcherSetup-\*.\*. \*-win32.msi*.
2. В окне License Agreement примите лицензионное соглашение.
3. В окне Installation Type выберите тип установки Install Syslog Watcher Service and GUI.
4. В окне Select installation Folder выберите путь установки для syslog-сервера.
5. В окне Windows Firewall Exception разрешите добавление правила на все входящие соединения для Syslog Watcher в брандмауэр Windows (Add Windows firewall exception (allow incoming connections)).
6. В окне Confirm Installation нажмите Next.
7. Дождитесь завершения установки сервера.

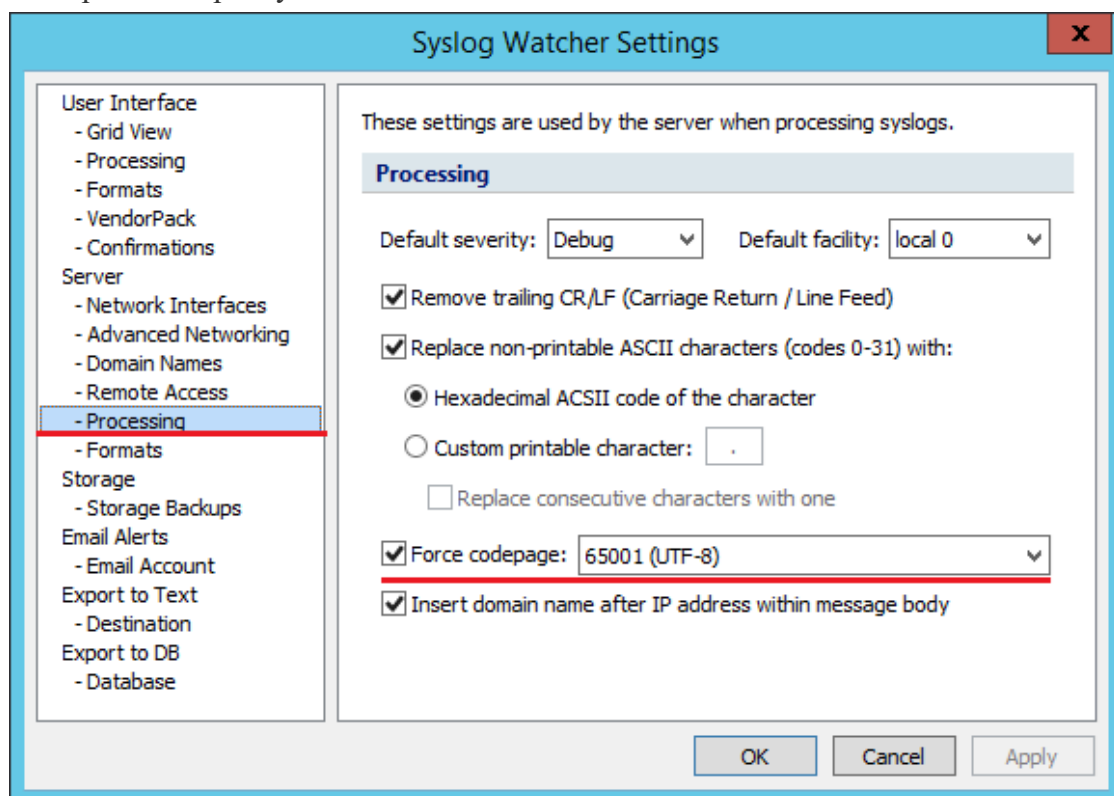
Чтобы настроить syslog-сервер:

1. Запустите Syslog Watcher и выберите Manage Local Syslog Server.
2. Нажмите Settings в верхнем меню программы.
  1. Перейдите в раздел Network Interfaces.
  2. Проверьте, что выбрано использование протокола udp и указан порт.



3. Перейдите в раздел Processing.

4. Выберите кодировку UTF-8.



Редактировать конфигурационный файл

1. Откройте конфигурационный

файл *sampleSyslog.config* (*C:\inetpub\wwwroot\ls\targetConfigs\sampleSyslog.config*) и

укажите следующие параметры в теге `ConnectionString`:

- `HostName` — имя или IP-адрес Syslog-сервера.
- `Port` — порт Syslog-сервера (514 — порт по умолчанию).
- `Protocol` — тип подключения к Syslog-серверу: UDP, TCP, TCPoverTLS.
- `Format` — опциональный параметр, определяет формат логов: Plain (по умолчанию), CEF, LEEF.
- `SyslogVersion` — опциональный параметр, спецификация протокола: RFC3164, RFC5424.

Пример настройки для Syslog Watcher

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

2. Откройте конфигурационный файл `C:\inetpub\wwwroot\ls\clientApps.config`.
3. Для блока с `"Application Id"="ea"` в теге `TargetId` для `WriteTargets` укажите `sampleSyslog`. Тег `ReadTargetId` оставьте пустым, так как чтение выполняется сторонней программой, в данном примере Syslog Watcher.

#### ⚠ ПРИМЕЧАНИЕ

В тегах `ReadTargetId` указывается идентификатор хранилища, откуда будут считываться события.

В блоке `WriteTargets`, в тегах `TargetId` указывается идентификатор хранилища, куда будут записываться события.

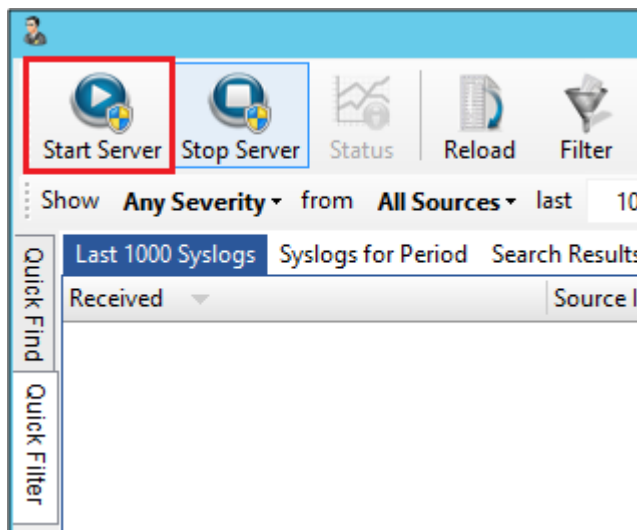
Идентификаторы заданы в теге `Targets`, конфигурационные файлы для каждого типа находятся в папке `targetConfigs` с соответствующим именем.

```

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

```

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



Пример отображения

Start Server
 Stop Server
 Status
 Reload
 Filter
 Find
 Search
 Import
 Export
 Delete
 Reports
 Storage
 Settings

Vendor Pack
 Help
 Info

Show **Any Severity** from **LOG** last 1000 messages | Update every 10 seconds | Updated at 26.11.2018 12:01:26

☒ AutoScroll

Last 1000 Syslogs
 Syslogs for Period
 Search Results (0)
 Sources (1)
 Server Log
 Backups

| 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 [indee...    |
| 26.11.2018 11:00:... | ::1       | LOG        | local 7  | Info     | 2018-11-2... | ea  | unk... | server LogonByAuthenticatorSucceeded [indee...    |
| 26.11.2018 12:00:... | ::1       | LOG        | local 7  | Info     | 2018-11-2... | ea  | unk... | server AcquirePersonalLicense [indeed@32473 r...  |
| 26.11.2018 12:00:... | ::1       | LOG        | local 7  | Info     | 2018-11-2... | ea  | unk... | server ReleasePersonalLicense [indeed@32473 li... |
| 26.11.2018 12:00:... | ::1       | LOG        | local 7  | Info     | 2018-11-2... | ea  | unk... | server ReleasePersonalLicense [indeed@32473 li... |
| 26.11.2018 12:00:... | ::1       | LOG        | local 7  | Info     | 2018-11-2... | ea  | unk... | server AcquirePersonalLicense [indeed@32473 r...  |
| 26.11.2018 12:00:... | ::1       | LOG        | local 7  | Info     | 2018-11-2... | ea  | unk... | server AcquirePersonalLicense [indeed@32473 r...  |
| 26.11.2018 12:00:... | ::1       | LOG        | local 7  | Info     | 2018-11-2... | ea  | unk... | server ReleasePersonalLicense [indeed@32473 li... |
| 26.11.2018 12:00:... | ::1       | LOG        | local 7  | Info     | 2018-11-2... | ea  | unk... | server ReleasePersonalLicense [indeed@32473 li... |
| 26.11.2018 12:00:... | ::1       | LOG        | local 7  | Info     | 2018-11-2... | ea  | unk... | server AcquirePersonalLicense [indeed@32473 r...  |

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 Fil: 0 Sel: 1 UDP: 514 TCP: 1468



## Резервное хранилище

Настройка с несколькими хранилищами разного типа

### ⓘ ПРИМЕЧАНИЕ

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

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

### ⓘ ПРИМЕЧАНИЕ

В тегах `ReadTargetId` указывается идентификатор хранилища, откуда будут считываться события.

В блоке `WriteTargets`, в тегах `TargetId` указывается идентификатор хранилища, куда будут записываться события.

Идентификаторы заданы в теге `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 `C:\inetpub\wwwroot\ls\targetConfigs\sampleDb.config`.
5. Укажите данные для подключения к базе данных в теге `connectionString`:
  - `Data Source` — задает экземпляр сервера. Эта настройка является обязательной 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>
```

#### ❗ ПРИМЕЧАНИЕ

При такой конфигурации события считываются из событий Windows, события будут записываться 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 `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` укажите `sampleDb`.

### ⚠ ПРИМЕЧАНИЕ

В тегах `ReadTargetId` указывается идентификатор хранилища, откуда будут считываться события.

В блоке `WriteTargets`, в тегах `TargetId` указывается идентификатор хранилища, куда будут записываться события.

Идентификаторы заданы в теге `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>`.

### ⚠ ПРИМЕЧАНИЕ

При такой конфигурации чтение событий будет осуществляться из базы данных, указанной в конфигурационном файле `ls\targetConfigs\sampleDb.config`.

Записываться события будут 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 *C:\inetpub\wwwroot\ls\targetConfigs\sampleDb.config*.

6. Укажите данные для подключения к базе данных в теге `connectionString`:

#### ⚠ ПРИМЕЧАНИЕ

Укажите данные для подключения к основной базе данных.

- `Data Source` — задает экземпляр сервера. Эта настройка является обязательной 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*.

 **ВАЖНО**

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

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

 **ПРИМЕЧАНИЕ**

Укажите данные для подключения к резервной базе данных.

- `Data Source` — задает экземпляр сервера. Эта настройка является обязательной 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=LogServBackup;User
Id=log;Password=Q1q2E3e4</ConnectionString>
</Settings>
```

## Настроить кеширование событий

Если Log Server недоступен, события кешируются в локальную папку на Core Server.

Информация о недоступности Log Server отображается в событиях Windows во вкладке *Приложение* со следующими параметрами:

- Код события — 500.

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

Чтобы изменить параметры хранения событий:

1. Откройте конфигурационный файл сервера *Indeed Web.config*.
2. Внесите следующие изменения:
  - Чтобы задать путь к папке для хранения событий, измените значение параметра `EventCacheDirectory` в теге `logServerClient`. Значение по умолчанию — `./EventCache`.
  - Чтобы изменить время отправки логов после возобновления работы LogServer, измените значение параметра `EventCacheSendingIntervalSec` в теге `logServerClient`. Значение по умолчанию — *600 секунд*.

Не рекомендуется устанавливать значение для параметра

`EventCacheSendingIntervalSec` менее 30 секунд.

## Сменить локализацию

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

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

Чтобы настроить локализацию:

1. Откройте конфигурационный файл  
*C:\ProgramData\Indeed\LogServer\Schemes\eaSchema.config*.
2. Измените значение параметра `DefaultLanguage`.

Пример локализации событий en-En

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

Пример локализации событий ru-RU

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

3. Сохраните изменения.

# Indeed Core Server

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

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

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

## Файлы для установки

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\AccessManager.Tools.KeyGen.Console.exe* — утилита для генерации пары ключей для подписи токена пользователя;
- */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 Core Server

### Системные требования



Выполните установку Core Server через запуск пакета *IndeedAM.Server-<номер версии>.x64.ru-ru.msi*.

## Привязка HTTPS в настройках в IIS Manager

Core Server является веб-приложением, которое работает на базе IIS, в процессе установки для него по умолчанию включается обязательное требование SSL в настройках, что в свою очередь требует включенной привязки HTTPS.

### ▼ Как это сделать

1. Запустите IIS Manager и раскройте пункт Сайты (Sites).
2. Выберите сайт *Default Web Site* и нажмите Привязки (Bindings) в разделе Действия (Actions).
3. Нажмите Добавить (Add):
  - *Тип* (Type) — https.
  - *Порт* (Port) — 443.
  - Выберите *SSL-сертификат* (SSL Certificate).
4. Сохраните привязку.

Если вы не намерены использовать протокол HTTPS, отключите требование SSL в настройках IIS для core и в конфигурационном файле сервера (*C:\inetpub\wwwroot\am\core\Web.config*) измените значение параметра *requireHttps* на *false*.

### Пример

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

# Настройка с помощью мастера конфигурации

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 мастере включена автоматическая проверка введенных данных. Если данные корректные, поле поменяет цвет на зеленый, и вы сможете перейти к следующему шагу. Если данные введены некорректно, поля будут подсвечены красным, и вы не сможете перейти к следующему шагу, пока не укажете корректные данные.

Дальнейшие шаги зависят от используемой базы данных.

### Microsoft SQL

#### Настройка для базы данных Microsoft SQL

1. На шаге Перед началом работы нажмите Далее.
2. На шаге Восстановление настроек нажмите Далее.
3. На шаге Каталог пользователей нажмите кнопку Добавить и укажите следующие параметры:
  - *Имя домена (FQDN)* — полное имя домена Active Directory, в котором находится каталог, например *domain.local*.
  - *Сервисная учетная запись* — сервисная учетная запись, обладающая правами доступа к пользовательскому каталогу. Нажмите кнопку Изменить и укажите данные учетной записи.
  - *LDAP путь к каталогу* — путь к каталогу с пользователями. Нажмите кнопку Выбрать и выберите контейнер или домен целиком.

Нажмите Настроить соответствие атрибутов, чтобы задать соответствие атрибутов Active Directory и Access Manager.

## ▼ Список атрибутов

---

- `FirstName` — имя пользователя.
- `MiddleName` — отчество пользователя.
- `LastName` — фамилия пользователя.
- `Email` — адрес электронной почты пользователя.
- `Phone` — номер телефона пользователя.
- `Name` — отображаемое имя пользователя.
- `CanonicalName` — каноническое имя пользователя, например *domain.com/Users/testuser*.
- `PrincipalName` — уникальное имя пользователя в определенном формате, например *testuser@domain.com*.
- `SamCompatibleName` — имя пользователя, совместимое с системой учетных записей Security Account Manager (SAM). Например, *domain\testuser*.
- `DistinguishedName` — уникальное имя объекта в иерархии Active Directory, состоящее из полного пути к объекту. Например, *CN=testuser,OU=Users,DC=domain,DC=com*.
- `Sid` — уникальный идентификатор безопасности, присваиваемый каждому объекту в Active Directory. Sid используется для управления доступом к ресурсам и аутентификации пользователей и объектов.

Нажмите Настроить фильтрацию объектов каталогов, чтобы задать критерии поиска записей в каталогах пользователей.

### ▼ Список фильтров

---

- LDAP-фильтр — фильтр в виде LDAP-запроса, применяется на этапе обращения к каталогу пользователя. Подробнее можно узнать в статье [LDAP-фильтр при поиске пользователей и групп в Active Directory](#).
- DN-фильтр — фильтр distinguishedName в виде регулярного выражения, используется для фильтрации результатов после выполнения LDAP-запроса.

4. На шаге Хранилище данных выберите 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.

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

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



#### СОВЕТ

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

7. На шаге Журнальный сервер укажите следующие данные:

 **ПРИМЕЧАНИЕ**

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

- *Адрес журнального сервера* — URL для подключения к серверу в формате *http(s)://полное\_dns\_имя\_сервера/ls/*, например *http://logserver.demo.local/ls/*.
- *Сертификат* — сертификат для настройки двухстороннего TLS- соединения между сервером Indeed AM и Indeed AM Log Server.

 **ВАЖНО**

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

- *Журналируемое поле объекта каталога* — укажите формат, в котором будет осуществляться логирование имени пользователя.
- *Журналируемое поле компьютера* — укажите формат, в котором будет осуществляться логирование поля *Компьютер*.

 **ПРИМЕЧАНИЕ**

Для логирования в формате DNS потребуется дополнительная настройка.  
Подробнее по настройке логирования в формате DNS.

8. Шаг Сессионный секрет. Сгенерируйте пару ключей для подписи токена пользователя, для этого нажмите Сгенерировать.

Публичный ключ сохраняется в файле *SessionPublicKey.pub*. Этот ключ необходимо распространить на все машины, на которых установлен **Windows Logon** или **ESSO Agent**. Для распространения используйте политику *Настройки публичного ключа ceanca* (расположена в каталоге *indeed AM <номер версии> \Misc\ADMX Templates*).

9. Шаг Шифрование файла. Вы можете выполнить шифрование настроек конфигурационного файла.

 **СОВЕТ**

В целях повышения безопасности рекомендуется выполнить шифрование конфигурационного файла.

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

 **СОВЕТ**

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

 **ПРИМЕЧАНИЕ**

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.

 **ПРИМЕЧАНИЕ**

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. Убедитесь в корректности указанных данных и нажмите Применить.

3. На шаге Результаты отображается статус настройки конфигурационного файла и статус настройки администратора системы.

## PostgreSQL

### Настройка для базы данных PostgreSQL

1. На шаге Перед началом работы нажмите Далее.
2. На шаге Восстановление настроек нажмите Далее.
3. На шаге Каталог пользователей нажмите кнопку Добавить и укажите следующие параметры:
  - *Имя домена (FQDN)* — полное имя домена Active Directory, в котором находится каталог, например *domain.local*.
  - *Сервисная учетная запись* — сервисная учетная запись, обладающая правами доступа к пользовательскому каталогу. Нажмите кнопку Изменить и укажите данные учетной записи.
  - *LDAP путь к каталогу* — путь к каталогу с пользователями. Нажмите кнопку Выбрать и выберите контейнер или домен целиком.

Нажмите Настроить соответствие атрибутов, чтобы задать соответствие атрибутов Active Directory и Access Manager.

## ▼ Список атрибутов

---

- `FirstName` — имя пользователя.
- `MiddleName` — отчество пользователя.
- `LastName` — фамилия пользователя.
- `Email` — адрес электронной почты пользователя.
- `Phone` — номер телефона пользователя.
- `Name` — отображаемое имя пользователя.
- `CanonicalName` — каноническое имя пользователя, например *domain.com/Users/testuser*.
- `PrincipalName` — уникальное имя пользователя в определенном формате, например *testuser@domain.com*.
- `SamCompatibleName` — имя пользователя, совместимое с системой учетных записей Security Account Manager (SAM). Например, *domain\testuser*.
- `DistinguishedName` — уникальное имя объекта в иерархии Active Directory, состоящее из полного пути к объекту. Например, *CN=testuser,OU=Users,DC=domain,DC=com*.
- `Sid` — уникальный идентификатор безопасности, присваиваемый каждому объекту в Active Directory. Sid используется для управления доступом к ресурсам и аутентификации пользователей и объектов.

Нажмите Настроить фильтрацию объектов каталогов, чтобы задать критерии поиска записей в каталогах пользователей.



### ▼ Список фильтров

---

- LDAP-фильтр — фильтр в виде LDAP-запроса, применяется на этапе обращения к каталогу пользователя. Подробнее можно узнать в статье [LDAP-фильтр при поиске пользователей и групп в Active Directory](#).
- DN-фильтр — фильтр distinguishedName в виде регулярного выражения, используется для фильтрации результатов после выполнения LDAP-запроса.

4. На шаге Хранилище данных выберите тип хранилища PostgreSQL.

5. В поле Строка подключения к базе данных укажите следующие данные:

- *server* — ip-адрес сервера базы данных.
- *port* — используемый порт. По умолчанию — 5432.
- *user id* — имя пользователя, который имеет полные права для базы данных.
- *password* — пароль пользователя.
- *database* — база данных, содержащая данные об Indeed AM Server.

Нажмите Тест, чтобы проверить подключение к базе данных.

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



#### СОВЕТ

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

7. На шаге Журнальный сервер укажите следующие данные:



#### ПРИМЕЧАНИЕ

Чтобы при тестировании соединения не возникли ошибки, требуется полностью настроенный Log Server с настроенной базой данных или установленным компонентом EventLog. Если журнальный сервер не готов к работе, вы можете пропустить этот шаг.

- *Адрес журнального сервера* — URL для подключения к серверу в формате *http(s)://полное\_dns\_имя\_сервера/ls/*, например *http://logserver.demo.local/ls/*.
- *Сертификат* — сертификат для настройки двухстороннего TLS- соединения между сервером Indeed AM и Indeed AM Log Server.

#### **ВАЖНО**

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

- *Журналируемое поле объекта каталога* — укажите формат, в котором будет осуществляться логирование имени пользователя.
- *Журналируемое поле компьютера* — укажите формат, в котором будет осуществляться логирование поля *Компьютер*.

#### **ПРИМЕЧАНИЕ**

Для логирования в формате DNS потребуется дополнительная настройка

- Шаг Сессионный секрет. Сгенерируйте публичный ключ для подписи токена, для этого нажмите Сгенерировать.

Публичный ключ сохраняется в файле *SessionPublicKey.pub*. Этот ключ необходимо распространить на все машины, на которых установлен **Windows Logon** или **ESSO Agent**. Для распространения используйте политику *Настройки публичного ключа ceanca* (расположена в каталоге *indeed AM <номер версии>\Misc\ADMX Templates*).

- Шаг Шифрование файла. Вы можете выполнить шифрование настроек конфигурационного файла.

#### **СОВЕТ**

В целях повышения безопасности рекомендуется выполнить шифрование конфигурационного файла.

- Шаг Подтверждение. Убедитесь в корректности указанных данных и нажмите Применить.



#### СОВЕТ

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. Убедитесь в корректности указанных данных и нажмите Применить.
3. На шаге Результаты отображается статус настройки конфигурационного файла и статус настройки администратора системы.

## Ручная настройка



#### ИНФОРМАЦИЯ

Рекомендуем редактировать конфигурационный файл с учетом пиковой нагрузки на сервер.

Чтобы сохранить изменения в конфигурационном файле, запустите редактор от имени администратора.

Ошибки, возникшие при разворачивании сервера Access Manager (например, ошибка в конфигурационном файле), будут логироваться исходя из настроек Log Server.

### ▼ Требования к символам в пароле для сервисных пользователей

---

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: &amp;. Пример(AD\SQL):  
password="Q1q2E3e4&"\Password='Q1q2E3e4&';
- Символ двойные кавычки (") — при указании пароля для пользователя из AD или SQL символ требуется заменить на: &quot;. Для пользователя из SQL дополнительно требуется указать пароль в одинарных кавычках. Пример(AD\SQL):  
password="Q1q2E3e4""\Password='Q1q2E3e4&quot;';
- 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: &lt;. Пример(AD\SQL):  
password="Q1q2E3e4<"\Password='Q1q2E3e4&lt;';
- 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 &quot;;, символ кавычки указать в обычном виде . Пример(AD\SQL):  
password="Q1q2E3e4""\Password=&quot;Q1q2E3e4'&quot;.

1. Откройте конфигурационный файл сервера *Web.config* (*C:\inetpub\wwwroot\am\core\Web.config*).
2. В параметре `sessionEncryptionSettings` укажите публичный и секретный ключи для подписи токена пользователя. Чтобы сгенерировать ключи, запустите утилиту *AccessManager.KeyGen.Console.exe* (расположена в каталоге *Indeed Access Manager Server/<номер версии>/Misc*).

В параметре `--name` укажите имена файлов. Это обязательный параметр. Файлы генерируются с одинаковым именем, однако у файла публичного ключа указывается расширение PUB.

В параметре `--output-directory` укажите путь к каталогу, в который сохранятся файлы ключевой пары. Вы можете указать относительный или абсолютный путь. Это необязательный параметр. Если вы не укажете путь, файлы ключевой пары сохранятся в каталоге *Misc*.

3. Задайте каталог пользователя системы, для этого необходимо отредактировать параметры в теге `adUserCatalogProvider`:

- `id` — произвольный уникальный идентификатор каталога.
- `serverName` — имя домена Active Directory, в котором находится каталог.
- `containerPath` — путь к контейнеру в виде Distinguished Name или весь домен, если для хранения пользователей используется весь домен.
- `userName` — имя сервисной учетной записи для подключения к каталогу пользователей.
- `password` — пароль сервисной учетной записи каталога пользователей в Active Directory.

#### Пример

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

4. Укажите корневой идентификатор провайдера работы с каталогом, необходимо отредактировать атрибут `rootUserCatalogProviderId` в теге `userCatalogProviderSettings`.

- `rootUserCatalogProviderId` — задать значение, которое уже было задано в теге `adUserCatalogProvider` в атрибуте `id`.

Пример

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

5. Задайте 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 теге `rootDbContextId`.

6. Добавьте параметр `connectionString` со встроенными параметрами:

- `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.
- `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>
```

7. Задайте ключ шифрования данных системы. Отредактируйте параметры в теге `encryptionSettings`.

- `cryptoAlgName` — укажите использованный алгоритм шифрования.  
Допустимые значения:
  - DES,
  - TripleDES,
  - RC2,
  - AES,
  - Rijndael.
- `cryptoKey` — значение ключа, сгенерированного утилитой.
- `certificateThumbprint` — отпечаток сертификата, которым зашифрован ключ (чтобы не учитывать, нужно удалить атрибут).

Пример

```
<encryptionSettings cryptoAlgName="Aes"
cryptoKey="90ce7dbc3ff94a7867abc6672c23cce2c3717d38af42f04293130cb6
```

8. Задайте администратора системы. Отредактируйте параметр `userId` тега `accessControlAdminSettings`.

- `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
```

9. Задайте url для подключения к Log Server. Отредактируйте тег `logServer`.

- `URL` — url для подключения к Log Server в формате *http(s)://имя сервера/ls/api*.

 **ПРИМЕЧАНИЕ**

Если используется несколько серверов, укажите адрес балансировщика нагрузки.

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



#### Пример

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

### Шифрование/Расшифрование конфигурационного файла

1. Запустите командную строку от имени администратора.
2. В командной строке перейдите в папку с утилитой для шифрования.



#### СОВЕТ

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

- Шифрование/Расшифрование отдельных секций. Для шифрования отдельной секции выполните команду вида:

```
EA.Config.Encryptor /encrypt "Путь к конфигурационному файлу  
сервера Имя секции"
```

#### Пример команды

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

Для расшифровки отдельной секции выполните команду вида:

```
EA.Config.Encryptor /decrypt "Путь к конфигурационному файлу  
сервера" "Имя секции"
```

#### Пример команды

```
EA.Config.Encryptor /decrypt
```

```
"C:\inetpub\wwwroot\am\core\Web.config" "logServer"
```

- Шифрование/Расшифрование всех секций. Для шифрования всех секций запустите скрипт `encryptConfigs.bat`.

Для расшифровки всех секций выполните скрипт `decryptConfigs.bat`.

## PostgreSQL

1. Откройте конфигурационный файл сервера *Web.config* (*C:\inetpub\wwwroot\am\core\Web.config*).
2. В параметре `sessionEncryptionSettings` укажите публичный и секретный ключи для подписи токена пользователя. Чтобы сгенерировать ключи, запустите утилиту *AccessManager.KeyGen.Console.exe* (расположена в каталоге *Indeed Access Manager Server/<номер версии>/Misc*).

В параметре `--name` укажите имена файлов. Это обязательный параметр. Файлы генерируются с одинаковым именем, однако у файла публичного ключа указывается расширение PUB.

В параметре `--output-directory` укажите путь к каталогу, в который сохранятся файлы ключевой пары. Вы можете указать относительный или абсолютный путь. Это необязательный параметр. Если вы не укажете путь, файлы ключевой пары сохранятся в каталоге *Misc*.

3. Задайте каталог пользователя системы, для этого необходимо отредактировать параметры в теге `adUserCatalogProvider`:
  - `id` — произвольный уникальный идентификатор каталога.
  - `serverName` — имя домена Active Directory, в котором находится каталог.
  - `containerPath` — путь к контейнеру в виде Distinguished Name или весь домен, если для хранения пользователей используется весь домен.
  - `userName` — имя сервисной учетной записи для подключения к каталогу пользователей.

- `password` — пароль сервисной учетной записи каталога пользователей в AD.

Пример

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

4. Укажите корневой идентификатор провайдера работы с каталогом, необходимо отредактировать атрибут `rootUserCatalogProviderId` в теге `userCatalogProviderSettings`.

- `rootUserCatalogProviderId` — задайте значение, которое уже было задано в теге `adUserCatalogProvider` в атрибуте `id`.

Пример

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

5. Задайте хранилище данных системы. Для хранилища данных в PostgreSQL Server редактируем тег `dbContextSettings` и создайте тег `postgresqlDbContexts` с параметрами `id` и `connectionString`.

- `rootDbContextId` — задайте произвольно уникальное значение идентификатора хранилища.
- `id` — задайте значение, которое уже было задано в теге `rootDbContextId`.

6. Добавьте параметр `connectionString` со встроенными параметрами:

- `Server` — DNS\IP-адрес сервера с базой данных 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=!QAZ2wsx;database=indeedamcore"
      id="postgreSql" />
    </postgresqlDbContexts>
  </dbContextSettings>
```

7. Задайте ключ шифрования данных системы. Отредактируйте параметры в теге `encryptionSettings`.

- `cryptoAlgName` — укажите использованный алгоритм шифрования.  
Допустимые значения:
  - DES,
  - TripleDES,
  - RC2,
  - AES,
  - Rijndael.
- `cryptoKey` — значения ключа, сгенерированного утилитой.
- `certificateThumbprint` — отпечаток сертификата, которым зашифрован ключ (чтобы не учитывать, нужно удалить атрибут).

### Пример

```
<encryptionSettings cryptoAlgName="Aes"
  cryptoKey="90ce7dbc3ff94a7867abc6672c23cce2c3717d38af42f04293130cb6
```

8. Задайте администратора системы. Отредактируйте параметр `userId` тега `accessControlAdminSettings`.

- `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
```

9. Задайте url для подключения к Log Server. Отредактируйте тег `logServer`.

- `URL` — url для подключения к Log Server в формате *http(s)://имя сервера/ls/api*.

 **ПРИМЕЧАНИЕ**

Если используется несколько серверов, укажите адрес балансировщика нагрузки.

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

#### Пример

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

### Шифрование/Расшифрование конфигурационного файла

1. Запустите командную строку от имени администратора.
2. В командной строке перейдите в папку с утилитой для шифрования.



#### СОВЕТ

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

- Шифрование/Расшифрование отдельных секций. Для шифрования отдельной секции выполните 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 выполните 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"
```

- Шифрование/Расшифрование всех секций. Для шифрования всех секций запустите скрипт `encryptConfigs.bat`.

Для расшифровки всех секций выполните скрипт `decryptConfigs.bat`.

# 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/v6/healthCheck/index*.

Страница обновляется автоматически каждые 60 секунд.

На странице доступна следующая информация о состоянии сервера:

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



## ПРИМЕЧАНИЕ

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



# Включение защиты от перебора

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

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

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

По умолчанию данная настройка отключена.

Чтобы настроить защиту от перебора, выполните следующие действия:

1. Откройте конфигурационный файл сервера Indeed AM *web.config* из *C:\inetpub\wwwroot\am\core*.
2. Измените параметр *appSettings*. В строке *bruteForceProtectionApps* через запятую укажите значение модулей, для которых вы хотите включить защиту от перебора.

## Пример

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

3. Сохраните изменения и перезапустите IIS.

# Настройка нескольких пользовательских каталогов

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.



## СОВЕТ

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="inforest.demo.local"
containerPath="OU=UsersInForest,DC=inforest,DC=demo,DC=local"
userName="inforest\cataloguser1" password="Q1q2E3e4" />
      <adUserCatalogProvider id="Ad3" serverName="newforest.local"
containerPath="OU=Usersoutforest,DC=newforest,DC=local"
userName="newforest\cataloguser2" password="Q1q2E3e4" />
    </adUserCatalogProviders>
  </userCatalogProviders>

```

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 незадаанными 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" />
    </userCatalogProviders>
  </orUserCatalogProvider>
</orUserCatalogProviders>
```

Пример структуры файла

```

<accessControlAdminSettings userId="UserId_891f2b6c-9a55-4e1a-b69b-
b4d6418f4c4c"/>
<loginSettings 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 Active Directory (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 задать в ней атрибуты `catalogFilter` и `dnFilter` для фильтрации элементов пользовательского каталога:
  1. `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`);
  2. `dnFilter` (фильтр `distinguishedName`) — регулярное выражение для фильтрации результатов после выполнения LDAP-запроса к AD.

## Примеры использования фильтров

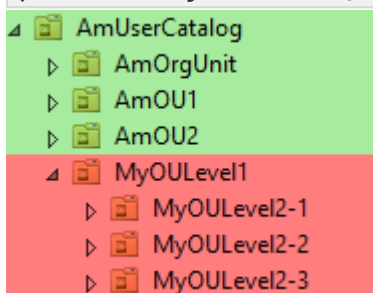
### `catalogFilter`

- исключение определенных пользователей `&(!(name=AmUser1))(!(name=AmUser2))(!(name=AmUser3))`
- исключение всех дочерних элементов первого 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`

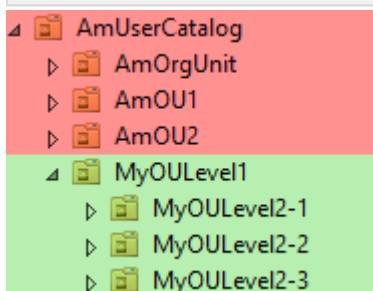
- исключение OU и всех дочерних элементов

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



- использование только указанной OU

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

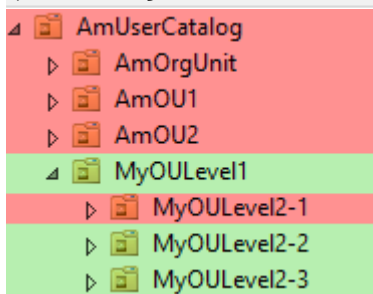


- комбинированный фильтр — использование только указанной OU без определенных дочерних элементов

```
(?!.*OU=MyOULevel2-
```

```
1,OU=MyOULevel1,OU=AmUserCatalog,DC=dom,DC=local$)
```

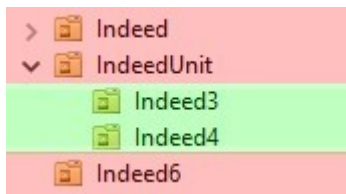
```
(^.*OU=MyOULevel1,OU=AmUserCatalog,DC=dom,DC=local$)
```



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

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

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





# Настройка механизма отзыва лицензий

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

Лицензия отзывается у пользователя, если:

- пользователь удален из политики;
- пользователь отключен или перемещен из области действия политики;
- пользователь заблокирован/удален из Active Directory.

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

Чтобы изменить время, после которого лицензия будет отозвана:

1. Откройте конфигурационный файл сервера `C:\inetpub\wwwroot\am\core\Web.config`.
2. В теге `cleanLicense` внесите следующие изменения:
  - Для параметра `intervalSec` укажите необходимое значение в секундах. Не рекомендуется устанавливать значение менее 600 секунд.
  - Для параметра `enabled` укажите значение `true`.
3. Сохраните изменения.
4. Перезапустите IIS. Внесенные изменения применятся после перезапуска.

## ПРИМЕЧАНИЕ

Рекомендуем редактировать конфигурационный файл и перезапускать IIS с учетом пиковой нагрузки на сервер.

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

1. Откройте конфигурационный файл сервера `C:\inetpub\wwwroot\am\core\Web.config`.

2. В теге `cleanLicense` для параметра `enabled` установите значение `false`.
3. Сохраните изменения.
4. Перезапустите IIS.
5. В файле *Web.config* в теге `cleanLicense` верните значение `true` для параметра `enabled`.
6. Повторно сохраните изменения и перезапустите IIS.



#### ПРИМЕЧАНИЕ

По результатам отзыва лицензий в журнале событий создается запись с кодом 1094. Запись о событии содержит общее число отозванных лицензий.

# Indeed Management Console

Indeed Management Console (Management Console) — это веб-приложение, которое работает на базе IIS. Оно позволяет управлять большинством настроек системы и пользователей.

## ❗ КАК ОТКРЫТЬ MANAGEMENT CONSOLE

- в браузере: `http(s)://<днс_сервера>/am/mc`
- в IIS: `<имя_машины>\сайты\Default Web Site\am\mc`

Чтобы настроить Management Console:

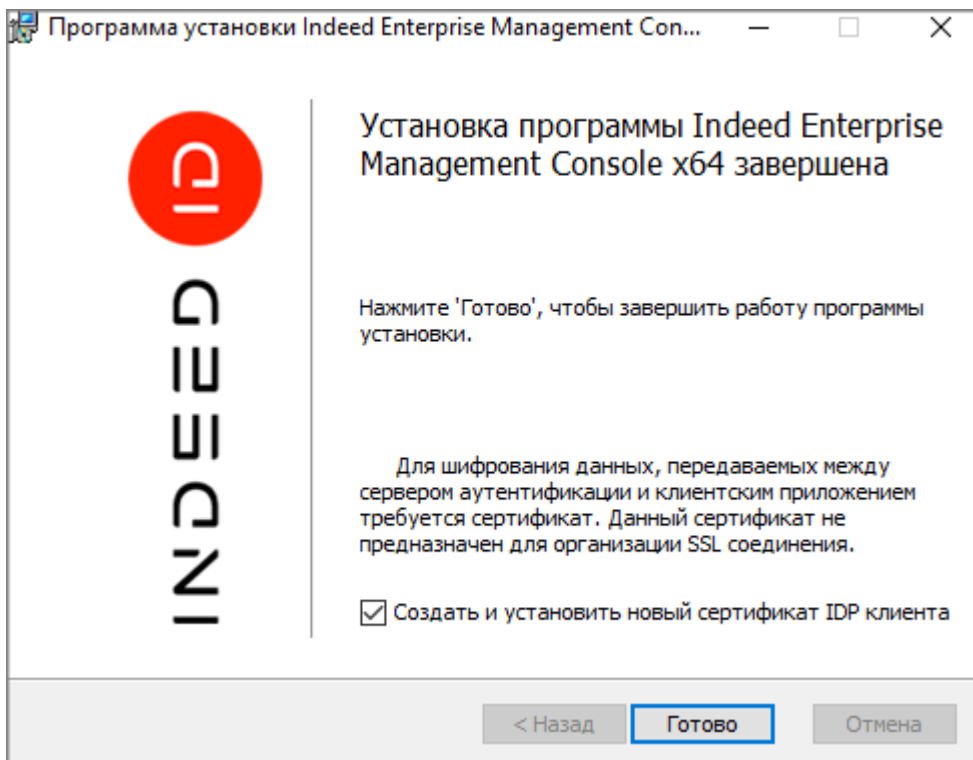
1. Установите **модуль**.
2. Создайте **привязку HTTPS** в настройках IIS.
3. Настройте **аутентификацию**.
4. При необходимости задайте **опциональные настройки**.

## Установить Management Console

Прежде чем установить Management Console, ознакомьтесь с **системными требованиями**.

Чтобы установить Management Console:

1. Запустите `IndeedAM.ManagementConsole-<номер версии>.x64.ru-ru.msi`, расположенный по пути `Indeed AM <номер версии>\Indeed AM Management Console\<номер версии>`.
2. По завершении установки будет предложено сгенерировать новый сертификат IDP. Это необязательная настройка.



Сертификат необходим при аутентификации в Management Console **с использованием Indeed Identity Provider**. Данный сертификат не предназначен для организации SSL-соединения.

Если данный сертификат был сгенерирован ранее, отключите опцию.

Если опция включена, то новый самоподписанный сертификат сгенерируется и установится в хранилище сертификатов *Local Machine*→*Personal*. Сертификат используется для шифрования данных, передаваемых между сервером аутентификации и клиентским приложением.

## Создать привязку HTTPS

В процессе установки для Management Console в настройках IIS включается обязательное требование SSL-сертификата. Поэтому для корректной работы модуля необходимо создать привязку HTTPS.

Чтобы создать привязку HTTPS:

1. В Диспетчере служб IIS в левом меню выберите Indeed AM → сайты → Default Web Site
2. В правом меню в разделе Действия нажмите Привязки.
3. Нажмите Добавить и в открывшемся окне задайте следующие параметры:

- В поле Тип выберите *https*.
- В поле Порт укажите *443*.
- В поле SSL-сертификат выберите сертификат Core Server.

4. Нажмите ОК, чтобы сохранить привязку.

Если вы не намерены использовать протокол HTTPS, **отключите требование SSL-сертификата** в настройках IIS для Management Console.

Также в конфигурационном файле *C:\inetpub\wwwroot\am\mc\Web.config* измените значение параметра `requireSSL` на *false*:

Пример

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

## Настроить аутентификацию

Для входа в Management Console можно задать разные способы аутентификации.

### Windows Authentication

#### С помощью Windows Authentication

Чтобы настроить аутентификацию в Management Console с помощью Windows Password, включите **проверку подлинности Windows** и отредактируйте **конфигурационный файл консоли**.

Включить проверку подлинности Windows

1. В Диспетчере служб IIS в левом меню раскройте узел Indeed AM → сайты → Default Web Site → am → mc.
2. Нажмите Проверка подлинности.
3. Включите Олицетворение ASP.NET и Проверка подлинности Windows. Все остальные методы проверки подлинности должны быть отключены.

Изменить конфигурационный файл

1. Откройте конфигурационный файл консоли `C:\inetpub\wwwroot\am\mc\Web.config`.
2. В разделе `amAuthServer` в параметре `Url` укажите адрес для подключения к Core Server `http(s)://полное_dns_имя_сервера/am/core/`.

Пример

```
<amAuthServer Url="https://amcore.test.local/am/core/">
```

3. В разделе `logServer` в параметре `Url` укажите адрес для подключения к Log Server в формате `http(s)://полное_dns_имя_сервера/ls/api`.

Пример

```
<logServer Url="http://amcore.test.local/ls/api/">
```

Если используется несколько серверов, укажите адрес балансировщика нагрузки.

4. Сохраните изменения в файле и перезапустите сервер IIS.

Management Console будет доступна по адресу: `http(s)://полное_dns_имя_сервера/am/mc/`.



#### ПРИМЕЧАНИЕ

Чтобы при входе в консоль игнорировались ошибки сертификата сервера, измените значение параметра `isIgnoreCertErrors` на `true` в файле `C:\inetpub\wwwroot\am\mc\Config\applicationSettings.config`.

## Indeed Identity Provider

### С помощью Indeed Identity Provider

Чтобы настроить защищенный вход в Management Console с использованием Identity Provider:

1. Установите и настройте модуль **Identity Provider**.
2. Установите и настройте **провайдер аутентификации**.
3. Настройте **проверку подлинности** в Диспетчере служб IIS.

4. Отредактируйте конфигурационные файлы **Management Console** и **Identity Provider**.

Также можно настроить выход из Management Console с использованием **Identity Provider**.

Настроить проверку подлинности

1. В Диспетчере служб IIS в левом меню раскройте узел Indeed AM → сайты → Default Web Site → am → mc.
2. Нажмите Проверка подлинности.
3. Включите опции Анонимная проверка подлинности и Проверка подлинности с помощью форм. Все остальные методы проверки подлинности должны быть отключены.

Изменить конфигурационный файл Management Console

1. Откройте конфигурационный файл консоли *C:\inetpub\wwwroot\am\mc\Web.config*.
2. В разделе `amAuthServer` в параметре `Url` укажите адрес для подключения к Core Server *http(s)://полное\_dns\_имя\_сервера/am/core/*.

Пример

```
<amAuthServer Url="https://amcore.test.local/am/core/">
```

3. В разделе `logServer` в параметре `Url` укажите адрес для подключения к Log Server в формате *http(s)://полное\_dns\_имя\_сервера/ls/api*.

Пример

```
<logServer Url="http://amcore.test.local/ls/api/">
```

Если используется несколько серверов, укажите адрес балансировщика нагрузки.

4. В разделе *amAuthentication* внесите следующие изменения:

- В параметре `mode` укажите значение `Saml`
- В параметре `loginUrl` укажите адрес Identity Provider в формате *http(s)://полное\_dns\_имя\_сервера/am/idp/*

#### Пример

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

- В параметре `identityProviderCertificateThumbprint` укажите отпечаток сертификата Identity Provider.

Чтобы получить отпечаток сертификата, используйте запрос PowerShell:

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



#### СОВЕТ

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. Добавьте сертификат в хранилище сертификатов в раздел *Local Machine* → *Personal*.

- В параметре `serviceProviderCertificateThumbprint` укажите отпечаток сертификата Management Console, который был сгенерирован при установке пакета. Сертификат устанавливается в хранилище сертификатов *Local Machine* → *Personal* с общим именем *mcsp*.

Чтобы получить отпечаток сертификата, используйте запрос PowerShell:

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

5. Сохраните изменения и перезапустите IIS.

Management Console будет доступна по адресу: `http(s)://полноеднсия_сервера/am/mc/`.



### ⚠ ПРИМЕЧАНИЕ

Чтобы при входе в консоль игнорировались ошибки сертификата сервера, измените значение параметра `isIgnoreCertErrors` на `true` в файле `C:\inetpub\wwwroot\am\mc\Config\applicationSettings.config`.

Изменить конфигурационный файл Identity Provider

1. Откройте конфигурационный файл `C:\inetpub\wwwroot\am\idp\app-settings.json`.
2. В разделе `PartnerServiceProviderConfigurations` внесите следующие изменения:
  - В параметре `SingleLogoutServiceUrl` укажите адрес сервера с установленным компонентом Management Console в формате `http(s)://  
полное_dns_имя_сервера/am/mc/Account/SLOService`
  - В параметре `Thumbprint` укажите отпечаток сертификата Management Console, который был сгенерирован при установке пакета.

### 💡 СОВЕТ

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. Добавьте сертификат в хранилище сертификатов в раздел *Local Machine* → *Personal*.

Чтобы получить отпечаток сертификата, используйте запрос 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.

## Опциональные настройки

- Настроить срок жизни сессии
- Настроить поиск по пользователям
- Отключить отображение информации о платформе и версии
- Настроить выход с помощью Identity Provider

# Настройка срока жизни сессии

Чтобы изменить срок жизни сессии в Management Console:

1. Откройте конфигурационный файл `C:\inetpub\wwwroot\am\mc\Config\applicationSettings.config`.
2. В параметре `sessionExpirationTimeInMinutes` укажите необходимое значение. Значение по умолчанию 30 (минут).

## ▼ Пример

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

3. Сохраните изменения.

# Настройка поиска пользователя

Вы можете настроить **поиск пользователей в Management Console** по следующим параметрам:

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

Чтобы настроить поиск:

1. Откройте файл `C:\inetpub\wwwroot\am\mc\Config\userSearchSettings.config`.
2. В параметре `searchTemplate` укажите шаблон поиска. Примеры допустимых шаблонов:  
`**{0}`, `{0}*`, `*{0}**`.
3. Включите или отключите поиск по следующим параметрам, указав значение `true` или `false`:
  - `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 и фамилии. Значение по умолчанию `true`.
  - `searchByName` — поиск по имени, которое отображается в списке пользователей в Active Directory. Значение по умолчанию `true`.

Для удобства поиска можно 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». |

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

# Отключение отображения информации о платформе и версии

Чтобы в ответе на запрос API не отображалась информация о платформе и версии, на которой разрабатывалось приложение:

1. Откройте конфигурационный файл Management Console

*C:\inetpub\wwwroot\am\mc\Web.config.*

2. В зависимости от версии IIS:

- Для IIS 10 в разделе `security` перенесите комментарий со второй на третью строчку.

## ▼ Пример

До

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

</requestFiltering>
</security>
```

После

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

</requestFiltering>
</security>
```

- Для IIS выше 10 версии:

1. Установите модуль переопределения адресов **URL Rewrite**.
2. В конфигурационном файле `C:\inetpub\wwwroot\am\mc\Web.config` в раздел `system.webServer` добавьте следующее:

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

3. Сохраните изменения и перезагрузите IIS.

# Выход с помощью Identity Provider

Чтобы настроить выход из Management Console с помощью Identity Provider:

1. Откройте конфигурационный файл консоли *C:\inetpub\wwwroot\am\mc\Web.config*.
2. В разделе `amAuthentication` добавьте параметр `enableLogout` со значением `true`.

Пример

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

3. Откройте конфигурационный файл Identity Provider *app-settings.json*, расположенный в папке *C:\inetpub\wwwroot\am\idp*.
4. В разделе `PartnerServiceProviderConfigurations` в параметре `SingleLogoutServiceUrl` укажите адрес сервера с компонентом Management Console в формате *http(s)://полное\_имя\_сервера/am/mc/Account/SLOService*.

## ▼ Пример

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

5. Сохраните изменения и перезапустите IIS.



# Indeed User Console

Indeed User Console (User Console) — это веб-приложение, которое работает на базе IIS. В User Console пользователь может управлять своими аутентификаторами.



## КАК ОТКРЫТЬ USER CONSOLE

- в браузере: `http(s)://<днс_сервера>/am/uc`
- в IIS: `<имя_машины>\сайты\Default Web Site\am\uc`

Чтобы настроить User Console:

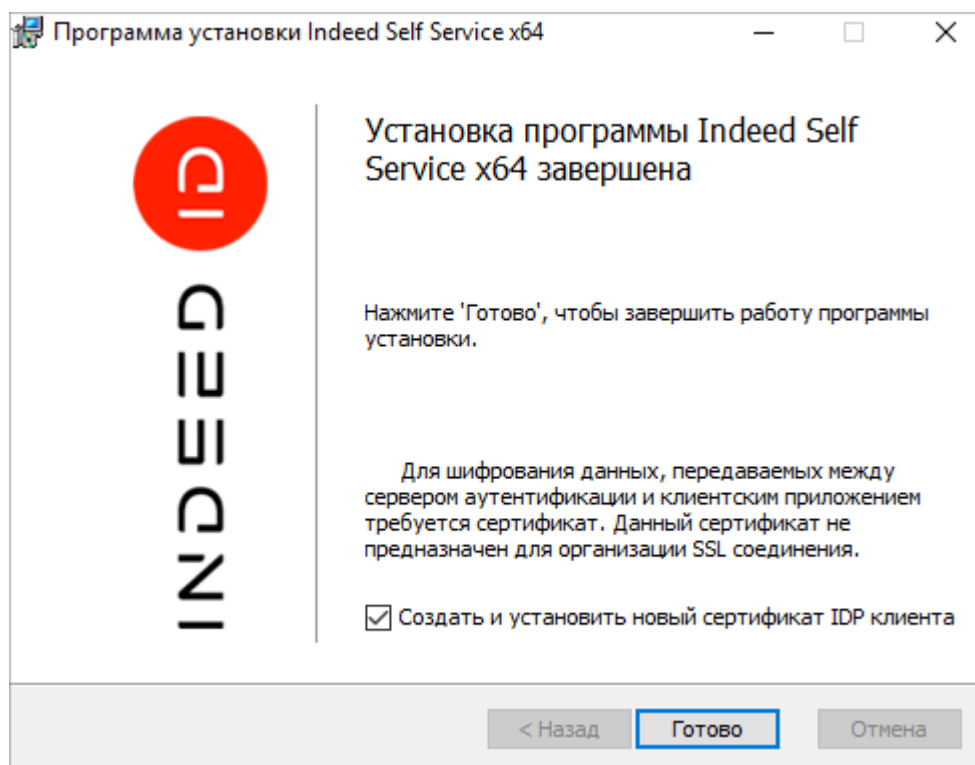
1. Установите **модуль**.
2. Создайте **привязку HTTPS** в настройках IIS.
3. Настройте **аутентификацию**.
4. При необходимости задайте **опциональные настройки**.

## Установить User Console

Прежде чем начать установку, ознакомьтесь с **системными требованиями**.

Чтобы установить User Console:

1. Запустите `IndeedAM.UserConsole-<номер версии>.x64.ru-ru.msi`, расположенный по пути `Indeed AM <номер версии>\User Console\<номер версии>`.
2. По завершении установки будет предложено сгенерировать новый сертификат IDP. Это необязательная настройка.



Сертификат необходим при аутентификации в User Console **с использованием Indeed Identity Provider**. Данный сертификат не предназначен для организации SSL-соединения.

Если данный сертификат был сгенерирован ранее, отключите опцию.

Если опция включена, то новый самоподписанный сертификат сгенерируется и установится в хранилище сертификатов *Local Machine*→*Personal*. Сертификат используется для шифрования данных, передаваемых между сервером аутентификации и клиентским приложением.

## Создать привязку HTTPS

В процессе установки для User Console в настройках IIS включается обязательное требование SSL-сертификата. Поэтому для корректной работы модуля необходимо создать привязку HTTPS.

Чтобы создать привязку HTTPS:

1. В Диспетчере служб IIS в левом меню выберите Indeed AM → сайты → Default Web Site
2. В правом меню в разделе Действия нажмите Привязки.
3. Нажмите Добавить и в открывшемся окне задайте следующие параметры:
  - В поле Тип выберите *https*.
  - В поле Порт укажите *443*.
  - В поле SSL-сертификат выберите сертификат Core Server.

4. Нажмите ОК, чтобы сохранить привязку.

Если вы не намерены использовать протокол HTTPS, **отключите требование SSL-сертификата** в настройках IIS для User Console.

Также в конфигурационном файле *C:\inetpub\wwwroot\am\uc\Web.config* измените значение параметра `requireSSL` на *false*:

Пример

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

## Настроить аутентификацию

По умолчанию для User Console настроена SAML-аутентификация, но можно настроить другие способы аутентификации.

### Windows Authentication

#### С помощью Windows Authentication

Чтобы настроить аутентификацию в User Console с помощью Windows Password, включите **проверку подлинности Windows** и отредактируйте **конфигурационный файл консоли**.

Включить проверку подлинности Windows

1. В Диспетчере служб IIS в левом меню раскройте узел Indeed AM → сайты → Default Web Site → am → uc.
2. Нажмите Проверка подлинности.
3. Включите Олицетворение ASP.NET и Проверка подлинности Windows. Все остальные методы проверки подлинности должны быть отключены.

Изменить конфигурационный файл

1. Откройте конфигурационный файл консоли *C:\inetpub\wwwroot\am\uc\Web.config* от имени администратора.
2. В разделе `amAuthServer` в параметре `Url` укажите адрес для подключения к Core Server *http(s)://полное\_имя\_сервера/am/core/*.

#### Пример

```
<amAuthServer Url="https://amcore.test.local/am/core/" />
```

3. В разделе `amAuthentication` в параметре `mode` укажите значение *Windows*.

Опционально вы можете добавить параметр `enableLogout="true"`, чтобы настроить возможность выйти из User Console.

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

#### Пример

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

4. Сохраните изменения в файле и перезапустите сервер IIS.

User Console будет доступна по адресу: *http(s)://полное\_dns\_имя\_сервера/am/uc/*.



#### ПРИМЕЧАНИЕ

Чтобы при входе в консоль игнорировались ошибки сертификата сервера, измените значение параметра `isIgnoreCertErrors` на `true` в файле

*C:\inetpub\wwwroot\am\uc\Config\applicationSettings.config*.

## Indeed Identity Provider

### С помощью Indeed Identity Provider

Чтобы настроить защищенный вход в User Console с использованием Identity Provider:

1. Установите и настройте модуль **Identity Provider**.
2. Установите и настройте **провайдер аутентификации**.
3. Настройте **проверку подлинности** в Диспетчере служб IIS.

4. Отредактируйте конфигурационные файлы **User Console** и **Identity Provider**.

Также можно настроить выход из User Console с использованием **Identity Provider**.

Настроить проверку подлинности

1. В Диспетчере служб IIS в левом меню раскройте узел Indeed AM → сайты → Default Web Site → am → uc.
2. Нажмите Проверка подлинности.
3. Включите опции Анонимная проверка подлинности и Проверка подлинности с помощью форм. Все остальные методы проверки подлинности должны быть отключены.

Изменить конфигурационный файл User Console

1. Откройте конфигурационный файл консоли `C:\inetpub\wwwroot\am\uc\Web.config`.
2. В разделе `amAuthServer` в параметре `Url` укажите адрес для подключения к Core Server `http(s)://полное_имя_сервера/am/core/`.

Пример

```
<amAuthServer Url="https://amcore.test.local/am/core/">
```

3. В разделе `amAuthentication` внесите следующие изменения:

- В параметре `mode` укажите значение `Saml`
- В параметре `loginUrl` укажите адрес Identity Provider в формате `http(s)://полное_имя_сервера/am/idp/`

Пример

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

- В параметре `identityProviderCertificateThumbprint` укажите отпечаток сертификата Identity Provider.

Чтобы получить отпечаток сертификата, используйте запрос PowerShell:

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



#### СОВЕТ

Если Identity Provider и User Console установлены на разные серверы, экспортируйте сертификат без закрытого ключа с сервера с модулем Identity Provider на сервер с User Console. Добавьте сертификат в хранилище сертификатов в раздел *Local Machine* → *Personal*.

- В параметре `serviceProviderCertificateThumbprint` укажите отпечаток сертификата User Console, который был сгенерирован при установке пакета. Сертификат устанавливается в хранилище сертификатов *Local Machine* → *Personal* с общим именем *ucsp*.

Чтобы получить отпечаток сертификата, используйте запрос PowerShell:

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

#### 4. Сохраните изменения и перезапустите IIS.

User Console будет доступна по адресу: `http(s)://полное_имя_сервера/am/uc/`.

Изменить конфигурационный файл Identity Provider

- Откройте конфигурационный файл `C:\inetpub\wwwroot\am\idp\app-settings.json`.
- В разделе `PartnerServiceProviderConfigurations` внесите следующие изменения:

- В параметре `SingleLogoutServiceUrl` укажите адрес сервера с установленным компонентом Management Console в формате `http(s)://полное_имя_сервера/am/uc/Account/SLOService`

- В параметре `Thumbprint` укажите отпечаток сертификата User Console, который был сгенерирован при установке пакета.

#### СОВЕТ

Если Identity Provider и User Console были установлены на разные серверы, экспортируйте сертификат без закрытого ключа с сервера с User Console на сервер с модулем Identity Provider. Добавьте сертификат в хранилище сертификатов в раздел *Local Machine* → *Personal*.

Чтобы получить отпечаток сертификата, используйте запрос PowerShell:

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

#### ▼ Пример

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

3. В параметре `AllowWinPwdIfAuthMethodsAreNotAvailable` вы можете установить значение `true`, что позволит войти через IDP в User Console с использованием Windows Password, даже если этот способ не указан в конфигурационном файле *app-settings.json*.

Если в параметре `AllowWinPwdIfAuthMethodsAreNotAvailable` указано значение `true`, возможны следующие сценарии:

- Отображаются только зарегистрированные и доступные пользователю методы аутентификации. При многофакторной аутентификации если хотя бы один из методов аутентификации не доступен, вся цепочка не отображается.
- При отсутствии любых доступных методов аутентификации, включая методы, не требующие регистрации в User Console (Windows Password, Email и SMS), отображается Windows Password.

4. Сохраните изменения и перезапустите IIS.



## ▼ Пример входа в User Console с использованием Identity Provider

---

1. Откройте в браузере интерфейс User Console. Пример адреса консоли: *http(s)://полное\_dns\_имя\_сервера/am/uc/*.
2. В появившемся окне аутентификации нажмите Back для выбора способа аутентификации. По умолчанию используется последний используемый способ.
3. Выберите способ аутентификации и нажмите Select.

### ⓘ ПРИМЕЧАНИЕ

Если у пользователя нет зарегистрированного аутентификатора, выберите *Windows Password*.

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

4. Введите пароль и нажмите Sing in. Если данные введены успешно, то отобразится карточка пользователя.
5. Если у вас настроен **выход из User Console с помощью Identity Provider**, чтобы выйти из консоли:
  - Нажмите имя пользователя в верхней части окна.
  - Выберите Выйти из выпадающего списка.

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

## Опциональные настройки

- **Настроить выход с помощью Identity Provider**
- **Включить защиту от перебора**
- **Настроить срок жизни сессии**

- Отключить отображение информации о платформе и версии
- Отключить возможность смены локализации

# Выход с помощью Identity Provider

Чтобы настроить выход из User Console с помощью Identity Provider:

1. Откройте конфигурационный файл консоли `C:\inetpub\wwwroot\am\uc\Web.config`.
2. В разделе `amAuthentication` добавьте параметр `enableLogout` со значением `true`.  
Значение по умолчанию — `false`.

Пример

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

3. Откройте конфигурационный файл Identity Provider из папки  
`C:\inetpub\wwwroot\am\idp\app-settings.json`.
4. В разделе `PartnerServiceProviderConfigurations` в параметре  
`SingleLogoutServiceUrl` укажите адрес сервера с компонентом User Console в формате  
`http(s)://полное_имя_сервера/am/uc/Account/SLOService`

## ▼ Пример

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

5. Сохраните изменения и перезапустите IIS.

# Включение защиты от перебора

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

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

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

По умолчанию данная настройка отключена.

Чтобы включить защиту от перебора:

1. Откройте конфигурационный файл Core Server `C:\inetpub\wwwroot\am\core\Web.config`.
2. В разделе `appSettings` для параметра `bruteForceProtectionApps` укажите значения *Self Service* и *Identity Provider*.

Пример

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

3. Сохраните изменения и перезапустите сервер IIS.

# Настройка срока жизни сессии

Чтобы изменить срок жизни сессии в User Console:

1. Откройте конфигурационный файл из папки  
*C:\inetpub\wwwroot\am\uc\Config\applicationSettings.config*.
2. В параметре `sessionExpirationTimeInMinutes` укажите необходимое значение.  
Значение по умолчанию 30 (минут).

Пример

```
<amApplicationSettings ignoreCertErrors="false"  
sessionExpirationTimeInMinutes="30"/>
```

3. Сохраните изменения.

# Отключение отображения информации о платформе и версии

Чтобы в ответе на запрос API не отображалась информация о платформе и версии, на которой разрабатывалось приложение:

1. Откройте конфигурационный файл User Console `C:\inetpub\wwwroot\am\uc\Web.config`.

2. В зависимости от версии IIS:

- Для IIS 10 уберите комментарии со следующих строк:

Пример

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

- Для IIS выше 10 версии выполните следующее:

1. Установите модуль переопределения адресов **URL Rewrite**.

2. В секцию `<system.webServer>` добавьте следующее:

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

3. Сохраните изменения и перезагрузите IIS.

# Отключение смены локализации

Чтобы запретить пользователю менять язык в User Console:

1. Откройте конфигурационный файл консоли *Web.config* (*C:\inetpub\wwwroot\am\uc\Web.config*).
2. Укажите значение *false* для параметра `isEnabled` тега `amCulture`.

Пример

```
<amCulture isEnabled="false" />
```

3. Перезапустите сервер IIS.

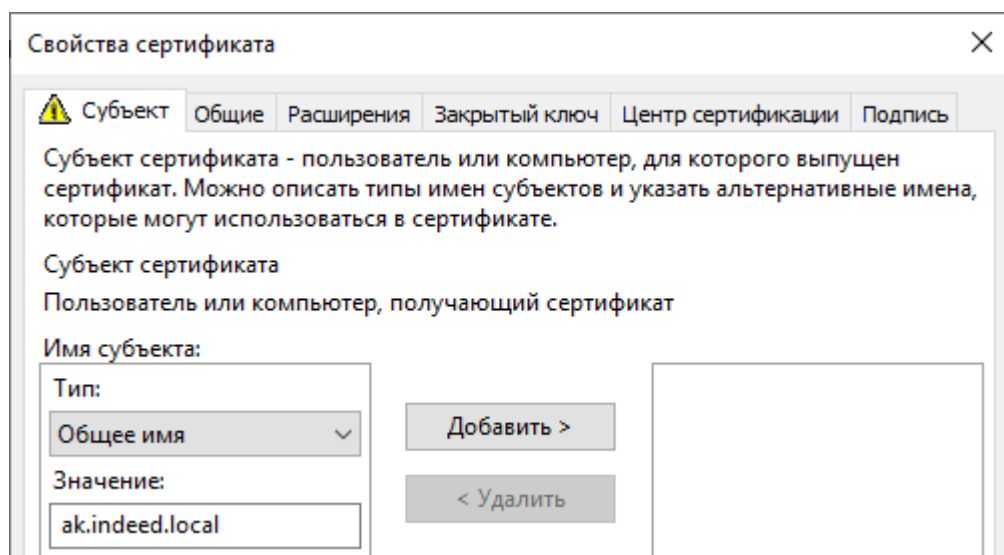
# Indeed Key Server

Indeed Key Server (Key Server) — это сервер, необходимый для работы мобильного приложения Indeed Key. С помощью Key Server отправляются push-уведомления и устанавливается связь с Core Server.

Связь с мобильным приложением Indeed Key осуществляется по протоколу HTTP или HTTPS.

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

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



## Файлы для установки

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

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



## Создание базы данных и сервисной учетной записи

Key Server поддерживает работу с базами PostgreSQL и Microsoft SQL.

Подробнее о создании базы данных и сервисной учетной записи вы можете узнать в разделе [Хранилище данных](#).

### ПРИМЕЧАНИЕ

После создания базы данных (после первого запроса) можно уменьшить права для пользователя. Достаточно права *db\_owner* для созданной базы данных.

## Привязка HTTPS в настройках в IIS Manager

Key Server является веб-приложением, которое работает на базе IIS, в процессе установки для Key Server включается обязательно требование SSL в настройках, что в свою очередь требует включенной привязки HTTPS.

### ▼ Как это сделать

1. Запустите IIS Manager и раскройте пункт Сайты (Sites).
2. Выберите сайт *Default Web Site* и нажмите Привязки (Bindings) в разделе Действия (Actions).
3. Нажмите Добавить (Add):
  - *Тип* (Type) — https.
  - *Порт* (Port) — 443.
  - Выберите *SSL-сертификат* (SSL Certificate).
4. Сохраните привязку.

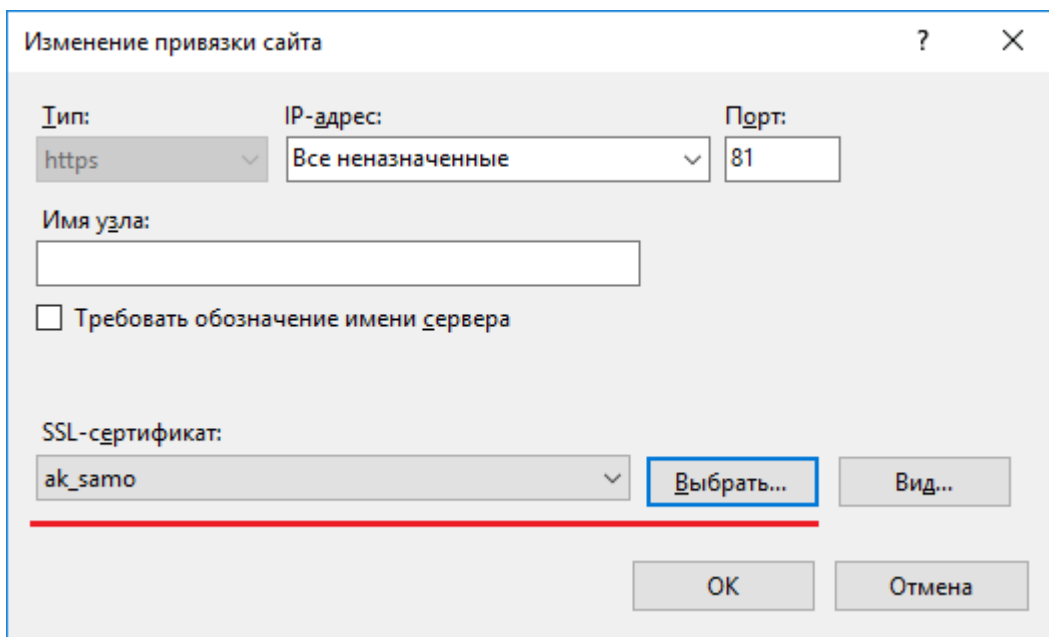
Если вы не намерены использовать протокол HTTPS, отключите требование SSL в настройках IIS для Key Server.

## Установка и настройка Indeed Key Server

### ВАЖНО!

Для корректной работы Key Server установите на хосте ASP.NET 4.7 и ознакомьтесь с системными требованиями.

1. Установите Key Server через запуск пакета *Indeed.IndeedKey.Server-<номер версии>.x64.ru.ru.msi*.
2. Откройте IIS Manager.
3. Выберите *Indeed Key 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.



### СОВЕТ

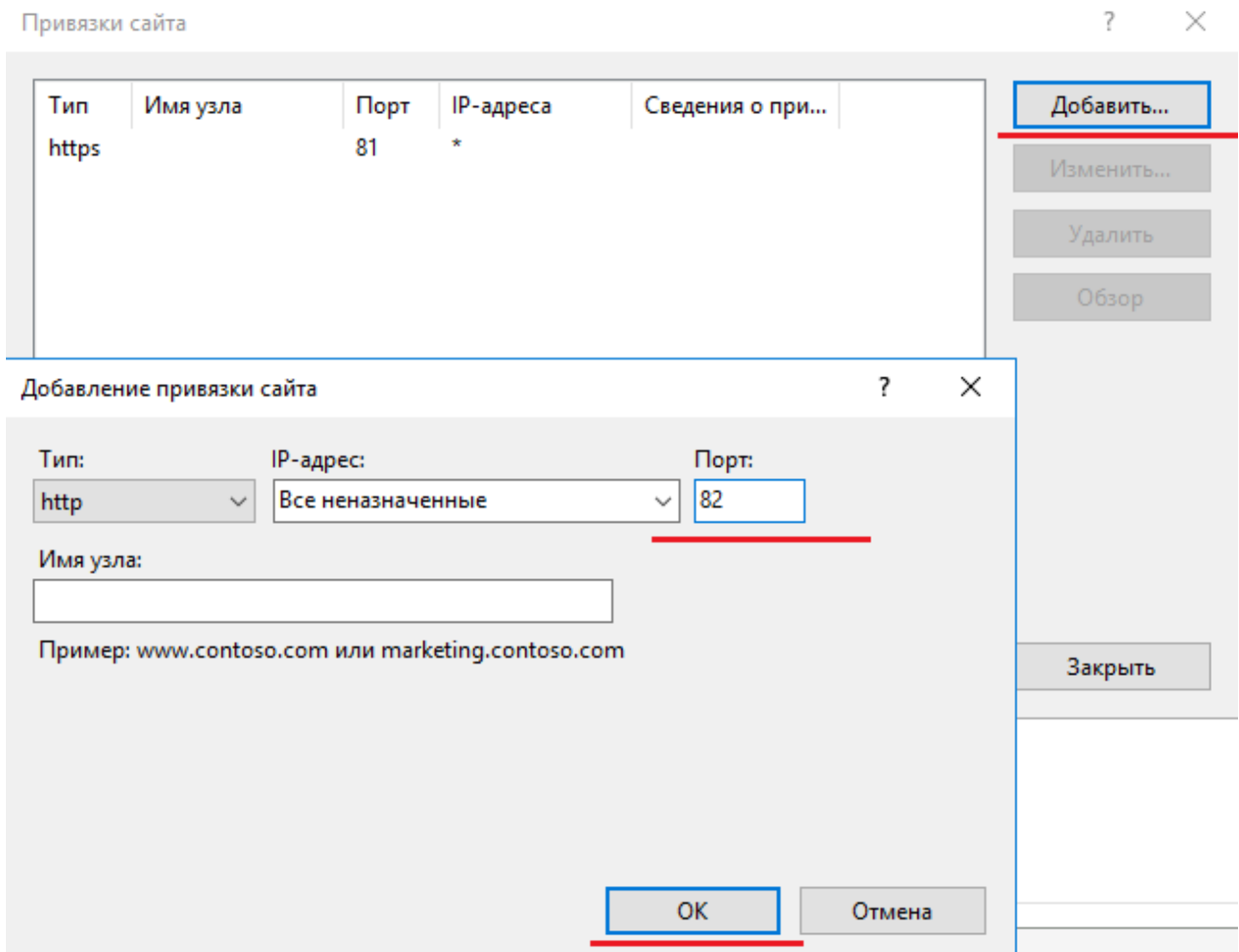
Чтобы сохранить изменения в конфигурационном файле приложения, запустите редактор с правами администратора.

5. Если вы используете протокол HTTP, добавьте привязку с произвольным доступным портом и нажмите Ок. В конфигурационном файле сервера *Web.config* (находится в папке

*C:\inetpub\wwwroot\indeedkey*) отключите требование HTTPS. Для этого измените значение с *true* на *false* для ключа `requireHttps`.

Пример

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



6. В параметре `rootDbContextId` укажите значение *mssql*, если вы используете базу данных Microsoft SQL, или *postgresql*, если вы используете базу данных PostgreSQL.

7. В секции `dbContextSettings` укажите строку для подключения к базе:

- для базы данных Microsoft SQL используйте параметр `mssqlDbContexts`;
- для базы данных PostgreSQL используйте параметр `postgresqlDbContexts`;

**❗ ПРИМЕЧАНИЕ**

В данной версии не поддерживается аутентификация Windows.

8. В параметре `value` с ключом `ServerUrl` укажите URL для подключения к Key Server.

**❗ ПРИМЕЧАНИЕ**

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

При использовании соединения по HTTP укажите порт, отличающийся от 80 (порт 80 используется как порт по умолчанию для HTTP-соединений сервера IIS ).

**❗ ПРИМЕЧАНИЕ**

Key Server должен быть доступен с мобильного телефона.

Пример

```
Для HTTPS — <add key="ServerUrl"
value="https://airkeycloud.indeed.local:81" />
```

```
Для HTTP — <add key="ServerUrl"
value="http://airkeycloud.indeed.local:82" />
```

9. Укажите URL для подключения к Log Server в параметре `Url` тега `logServer`.

Пример

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

10. Сохраните изменения и перезагрузите сервер IIS.

# Настройка событий сервера

Установка и настройка осуществляется на Log Server.

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

Отслеживать события можно следующими способами:

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



## ВАЖНО!

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

Чтобы настроить события Key Server, выполните следующее:

1. На Log Server выполните установку пакета *Indeed.IndeedKey.EventLog*.
2. Откройте файл *clientApps.config* (находится в папке *C:\inetpub\wwwroot\ls*).
3. Для параметра **SchemaId** со значением *akcSchema* задайте место хранения лог-файлов. Для этого в разделе **ReadTargetId** укажите подходящее значение для тега **TargetId**:

- *akcEventLogTarget* — чтение и запись событий производится из отдельного журнала событий Windows. Это значение задано по умолчанию.



## ПРИМЕЧАНИЕ

Просмотр событий осуществляется в журнале событий Windows на Log Server:  
Панель управления→Администрирование→Просмотр событий→Журналы приложений и служб→Indeed AirKey→Operational.

- *akcSqlTarget* — чтение и запись событий производится из базы данных Microsoft SQL.

 **ПРИМЕЧАНИЕ**

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

Чтобы чтение и запись событий производились из нескольких хранилищ, укажите несколько тегов `TargetId`.

Пример

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

Если в качестве хранилища событий вы используете базу данных, выполните настройку подключения к базе в файле *akcSqlTarget.config* (находится в папке C:\inetpub\wwwroot\ls\targetConfigs).

 **ВАЖНО!**

Для событий Key Server необходимо использовать отдельную базу данных.

## Сервис очистки старых данных

В файле *Web.config* (находится в папке C:\inetpub\wwwroot\indeedkey) можно задать параметры сервиса очистки старых данных из таблицы `AkDatas`:

Пример

```

<jobSettings>
  <cleanAkDatas enabled="true" firstRunTime="00:00"
intervalSec="86400" akDataLifeTimeSec="86400"
batchDeleteDelayMsec="1000" />
</jobSettings>

```

#### Описание атрибутов примера

| Имя атрибута                      | Описание                         | Значение                                    | Значение по умолчанию        | Минимально допустимое значение |
|-----------------------------------|----------------------------------|---------------------------------------------|------------------------------|--------------------------------|
| <code>enabled</code>              | Флаг включения сервиса           | <code>true</code> \ <code>false</code>      | <code>true</code>            | Отсутствует                    |
| <code>firstRunTime</code>         | Время первого запуска сервиса    | Строка в формате времени <code>hh:mm</code> | <code>00:00</code> (полночь) | Отсутствует                    |
| <code>intervalSec</code>          | Интервал запуска сервиса         | Число секунд                                | <code>86400</code> (24 ч)    | <code>600</code>               |
| <code>akDataLifeTimeSec</code>    | Время жизни данных               | Число секунд                                | <code>86400</code> (24 ч)    | <code>600</code>               |
| <code>batchDeleteDelayMsec</code> | Интервал между удалениями данных | Число миллисекунд                           | <code>1000</code>            | <code>0</code>                 |

## Проверка состояния сервера

Чтобы проверить состояние Key Server, используйте метод API `/api/HealthCheck`. Сервер в фоновой задаче осуществляет проверку состояния хранилища. Интервал выполнения фоновой задачи задается в конфигурационном файле *Web.config* (находится в папке *C:\inetpub\wwwroot\indeedkey*) в секции `jobSettings`:

Пример

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

## Шифрование/Расшифрование конфигурационного файла

Используйте следующие пакетные файлы, расположенные в дистрибутиве Indeed AM в папке *Indeed AM <номер версии> \Indeed AM Indeed Key Server\8.2.2\Misc\EA.Config.Encryptor*:

- *EncryptConfig.bat* — для шифрования конфигурационного файла;
- *DecrypConfig.bat* — для расшифрования конфигурационного файла.



# Indeed Phone Management Server

Indeed Phone Management Server (Phone Management Server ) — это веб-приложение, которое работает на базе IIS. Этот компонент предоставляет облегченное API для регистрации, изменения и удаления номеров в базе данных SQL.

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

## ВАЖНО!

Для работы с приложением установите компонент *Обычная проверка подлинности (Basic Authentication)* для сервера IIS.

## Установить Phone Management Server

Перед установкой компонента установите WebDeploy версии 10.0.1973 или выше и ознакомьтесь с **системными требованиями**.

Чтобы установить Phone Management Server:

1. Откройте командную строку с правами администратора.
2. Перейдите в папку *Distrib* компонента *EAPhoneServer*.
3. Чтобы запустить установку компонента, используйте команду:

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

После успешной установки в Диспетчере IIS отобразится отдельное веб-приложение *EAPhoneServer*.

## Настроить Phone Management Server

1. Откройте компонент *EAPhoneServer* в Диспетчере IIS.

2. Откройте Проверка подлинности и включите параметр Обычная проверка подлинности. Отключите все остальные методы проверки подлинности.
3. Откройте Правила авторизации. Измените существующее правило или добавьте новое. В настройках укажите пользователя или группу пользователей, которым будет доступен вызов методов API:
  - При указании группы пользователей указывается значение атрибута *name* данной группы.
  - При указании пользователя указывается значение атрибута *sAMAccountName* или *userPrincipalName*.



#### ПРИМЕЧАНИЕ

Данная настройка рекомендуется для обеспечения безопасного доступа к компоненту EAPhoneServer.

## Настроить политику

Чтобы предоставить сервисному пользователю необходимые права для работы, настройте политику. Для этого:

1. В Management Console перейдите на страницу основной политики, которая распространяется на целевых пользователей системы.
2. Перейдите на вкладку Администраторы и **добавьте** сервисного пользователя для компонента Phone Management Server с **ролью** *Администратор* или *Оператор*.

## Редактировать конфигурационный файл

1. Откройте конфигурационный файл `C:\inetpub\wwwroot\EAPhoneServer\Web.config` от имени администратора.
2. В разделе `appSettings` задайте значения следующих параметров:
  - 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 Phone Management Server. От имени этого пользователя будут выполняться запросы к API.

Пример

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

- В строке с параметром `key` со значением *password* задайте значение для параметра `value`. В значении укажите пароль пользователя, созданного для работы с Phone Management Server.

Пример

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

- В строке с параметром `key` со значением *lognames* задайте формат логирования имен пользователей. Если необходимо указать несколько форматов, укажите их значения через запятую. 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" />
```

3. Задайте URL для подключения к Indeed Log Server. Для этого отредактируйте раздел **logServer**:

- **URL** — URL для подключения к Log Server в формате *http(s)://полное\_dns\_имя\_сервера/ls/api*;
- **CertificateThumbprint** — если закрытый ключ в реестре, а сертификат в хранилище компьютера;
- **CertificateFilePath** — если ключевая пара в формате pfx;
- **CertificateFilePassword** — пароль от файла pfx.

Пример

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

4. Создайте папку для хранения локального кеша 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. В параметре `connectionString` укажите полный URL доступного Core Server или балансировщика в формате:

```
http/https://<полное DNS-имя Core Server или  
балансировщика>/am/core/
```

Пример

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

## Зашифровать/расшифровать конфигурационный файл

### ⚠ ПРИМЕЧАНИЕ

Настройка рекомендована в целях обеспечения безопасности.

Чтобы зашифровать конфигурационный файл, 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!
```

Чтобы расшифровать конфигурационный файл, 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!
```

## Удалить Phone Management Server

Чтобы удалить компонент:

1. Остановите сервер IIS с компонентом Phone Management 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.

## Настроить доступ к UI API

Чтобы получить доступ к UI Phone Management Server:

1. Перейдите по адресу: `http(s)://<полное DNS-имя сервера с компонентом Phone Management Server>/EAPhoneServer/swagger`.
2. Выполните авторизацию под пользователем, который входит в группу, настроенную в разделе **Правила авторизации**. Для входа укажите имя пользователя в формате `UPN`.

## Методы API Phone Management Server

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

```
http/https://<полное DNS-имя сервера с компонентом Phone Management Server>/EAPhoneServer/<метод API>
```

## Регистрация

### ⓘ ПРИМЕЧАНИЕ

Скрипт для работы с данным методом API доступен [в этой статье базы знаний](#).

Для регистрации номера телефона используется POST-запрос к методу API:

```
/api/IID/CreatePhone
```

- Входные данные:
  - *Username* — имя пользователя в формате *UPN*, для которого нужно зарегистрировать номер телефона;
  - *Phone* — номер телефона пользователя, который нужно зарегистрировать в системе;
- Выходные данные: HTTP-ответ с кодом состояния HTTP;
- Пример запроса:
  - URL — <http://AmIndeed.demo.local/EAPhoneServer/api/IID/CreatePhone>
  - Данные — `{ "Username": "User@demo.local", "Phone": "123456" }`

## ▼ Успешная регистрация

---

### ⓘ ПРИМЕЧАНИЕ

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

При успешной регистрации провайдера генерируется событие с уникальным идентификатором *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 Phone Management Server в конфигурационном файле. Формат имени пользователя задается в конфигурационном файле в параметре `LogNames`.
- *Пользователь API* — в данном параметре указывается пользователь, который был аутентифицирован по обычной проверке подлинности (Basic Authentication) 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.



## ▼ Ошибка при регистрации

---

### ⓘ ПРИМЕЧАНИЕ

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

При возникновении ошибки во время регистрации провайдера генерируется событие с уникальным идентификатором 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 Phone Management Server в конфигурационном файле. Формат имени пользователя задается в конфигурационном файле в параметре `LogNames`.
- *Пользователь API* — в данном параметре указывается пользователь, который был аутентифицирован по обычной проверке подлинности (Basic Authentication) 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.

❗ **ПРИМЕЧАНИЕ**

В случае возникновения ошибки при входе в систему или возникновения ошибки доступа (403) в параметре *Телефон* будут отображаться данные сервисного пользователя.

## Изменение

❗ **ПРИМЕЧАНИЕ**

Если в конфигурационном файле Phone Management Server для параметра `ReplaceUpdateWithCreate` задано значение `true`, вместо этого метода будут последовательно использоваться методы удаления и регистрации номера телефона.

Скрипт по работе с данным методом API доступен [в этой статье базы знаний](#).

Для изменения номера телефона используется POST-запрос к методу API:

```
/api/IID/UpdatePhone
```

- Входные данные :
  - *Phone* — номер телефона пользователя, который нужно зарегистрировать в системе;
  - *Username* — имя пользователя в формате *UPN*, для которого нужно изменить номер телефона;
- Выходные данные: HTTP-ответ с кодом состояния HTTP;
- Пример запроса:
  - URL — <http://AmIndeed.demo.local/EAPhoneServer/api/IID/UpdatePhone>
  - Данные — `{ "Username": "User@demo.local", "Phone": "654321" }`

## ▼ Успешное изменение

---

### ⓘ ПРИМЕЧАНИЕ

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

При успешном изменении провайдера генерируется событие с уникальным идентификатором *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 Phone Management Server в конфигурационном файле. Формат имени пользователя задается в конфигурационном файле в параметре `LogNames`.
- *Пользователь API* — в данном параметре указывается пользователь, который был аутентифицирован по обычной проверке подлинности (Basic Authentication) 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.

## ▼ Ошибка при изменении

---

При возникновении ошибки во время изменения провайдера генерируется событие с уникальным идентификатором 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 Phone Management Server в конфигурационном файле. Формат имени пользователя задается в конфигурационном файле в параметре `LogNames`.
- *Пользователь API* — в данном параметре указывается пользователь, который был аутентифицирован по обычной проверке подлинности (Basic Authentication) перед использованием метода API. Имя отображается в формате, который был указан при вводе в форму аутентификации.
- *Описание ошибки* — в данном параметре указывается 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.

### ⚠ ПРИМЕЧАНИЕ

В случае возникновения ошибки при входе в систему или возникновения ошибки доступа (403) в параметре *Телефон* будут отображаться данные сервисного пользователя.

## Удаление

### ⚠ ПРИМЕЧАНИЕ

Скрипт по работе с данным методом API доступен [в этой статье базы знаний](#).

Для удаления номера телефона используется POST-запрос к методу API:

```
/api/IID/DeletePhone
```

- Входные данные:
  - *Username* — имя пользователя в формате *UPN*, для которого нужно 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](#)" }’

## ▼ Успешное удаление

---



### ПРИМЕЧАНИЕ

В качестве примера используется формат имени:

*DistinguishedName, SamCompatibleName.*

При успешном удалении провайдера генерируется событие с уникальным идентификатором *1090*.

Тело события содержит:

- *Описание* — телефонный номер успешно удален.
- *Пользователь* — в данном параметре указывается пользователь, для которого был удален номер телефона. Формат имени пользователя задается в конфигурационном файле в параметре `LogNames`.
- *Инициатор* — в данном параметре указывается пользователь, который указан в качестве администратора компонента Phone Management Server в конфигурационном файле. Формат имени пользователя задается в конфигурационном файле в параметре `LogNames`.
- *Пользователь API* — в данном параметре указывается пользователь, который был аутентифицирован по обычной проверке подлинности (Basic Authentication) перед использованием метода API. Имя отображается в формате, который был указан при вводе в форму аутентификации.

## ▼ Ошибка при удалении

---

При возникновении ошибки во время удаления провайдера генерируется событие с уникальным идентификатором 2075.

Тело события содержит:

- *Описание* — ошибка удаления телефонного номера.
- *Пользователь* — в данном параметре указывается пользователь, для которого был удален номер телефона. Формат имени пользователя задается в конфигурационном файле в параметре `LogNames`.
- *Инициатор* — в данном параметре указывается пользователь, который указан в качестве администратора компонента Phone Management Server в конфигурационном файле. Формат имени пользователя задается в конфигурационном файле в параметре `LogNames`.
- *Пользователь API* — в данном параметре указывается пользователь, который был аутентифицирован по обычной проверке подлинности (Basic Authentication) перед использованием метода API. Имя отображается в формате, который был указан при вводе в форму аутентификации.
- *Описание ошибки* — в данном параметре указывается подробное описание возникшей ошибки.
- *Инициатор ошибки* — в данном параметре указывается пользователь, по причине которого возникла ошибка.



### ПРИМЕЧАНИЕ

В случае возникновения ошибки при входе в систему или возникновения ошибки доступа (403) в данном параметре будут отображаться данные сервисного пользователя.

# Indeed Reset Password

Indeed Reset Password (Reset Password) — утилита, предназначенная для сброса пароля пользователю с автоматической синхронизацией в системе Indeed Access Manager.

При сбросе пароля через данную утилиту пароль будет сгенерирован автоматически, сложность генерируемого пароля задается администратором системы при настройке утилиты.

Сгенерированный пароль отправляется пользователю по email или СМС.

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 по email или СМС на Core Server должны быть установлены провайдеры Indeed AM SMS OTP или Indeed AM Email OTP.

## Установка Indeed AM Reset Password

1. Запустите рабочую станцию/сервер, где в дальнейшем будет выполняться запуск утилиты.
2. Запустите файл для установки, расположенный по пути *Indeed AM <номер версии>/Indeed AM Reset Password*, и следуйте шагам мастера установки.

## Настройка

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:

- *Server URL* — URL-адрес Core Server в формате *http(s)://<DNS имя Indeed AM сервера>/am/core/*.
- *Тип провайдера* — способ получения сгенерированного пароля для пользователя. Доступно использование СМС или email.
- *Текст темы сообщения* — указывается тема письма со сгенерированным паролем.



#### **ВАЖНО!**

Это обязательный параметр при использовании email для получения пароля.

- *Текст сообщения* — указывается текст сообщения со сгенерированным паролем.



#### **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

☐ Не задано
 ☒ Включено
 ☐ Отключено

Комментарий:

Требования к версии: Windows XP и более поздние версии

Параметры:
 Справка:

Server URL:

<https://indeedam.indeed.local/am/core/>

Тип провайдера: SMS

Текст темы сообщения:

Текст сообщения:

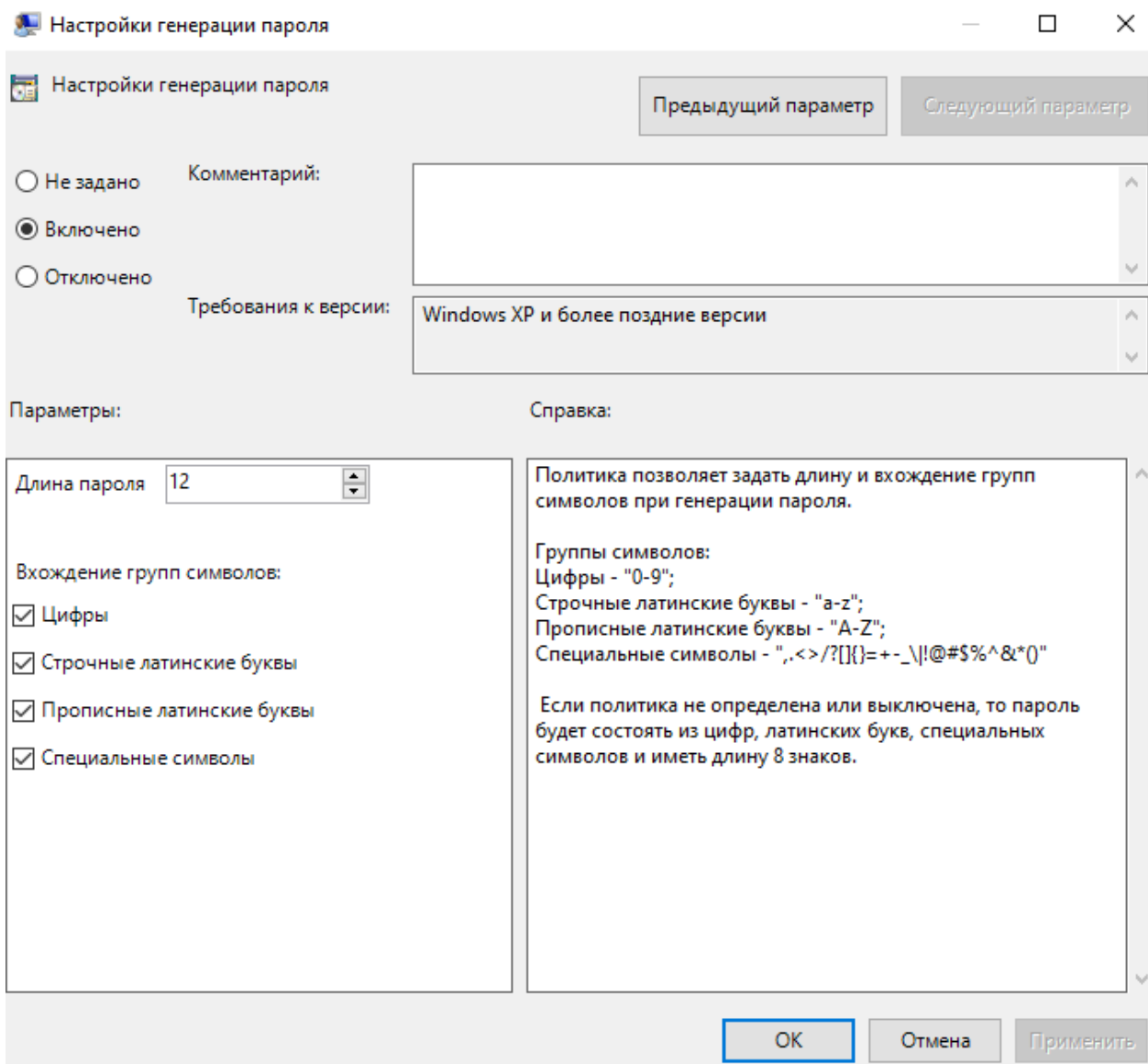
Ваш новый пароль:

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

OK Отмена Применить

4. Выберите и настройте политику *Настройки генерации пароля*. В политике укажите необходимые критерии для генерации пароля.



## Пример использования утилиты

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 Active Directory.
2. В основном окне утилиты нажмите кнопку Login.



### ПРИМЕЧАНИЕ

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.
4. На странице с пользователем нажмите кнопку Сбросить пароль AD и подтвердите действие.



#### ПРИМЕЧАНИЕ

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 должен быть указан 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 появится сообщение, что пароль был успешно сброшен и сообщение отправлено.

# Расположение конфигурационных файлов

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

В таблице ниже представлены полные пути к конфигурационным файлам.

| Компонент                                        | Конфигурационный файл                                          |
|--------------------------------------------------|----------------------------------------------------------------|
| Основной конфигурационный файл<br>Log Server     | <i>C:\inetpub\wwwroot\ls\clientApps.config</i>                 |
| Core Server                                      | <i>C:\inetpub\wwwroot\am\core\Web.config</i>                   |
| Management Console                               | <i>C:\inetpub\wwwroot\am\mc\Web.config</i>                     |
| User Console                                     | <i>C:\inetpub\wwwroot\am\uc\Web.config</i>                     |
| Key Server (Indeed Key) 8.1.x и<br>ниже          | <i>C:\inetpub\wwwroot\airkeycloud\Web.config</i>               |
| Key Server (Indeed Key) 8.2 и выше               | <i>C:\inetpub\wwwroot\indeedkey\Web.config</i>                 |
| Identity Provider (IDP) 8.1.4 и ниже             | <i>C:\inetpub\wwwroot\am\idp\Web.config</i>                    |
| Identity Provider (IDP) 8.1.5 и выше             | <i>C:\inetpub\wwwroot\am\idp\app-settings.json</i>             |
| Конфигурация хранения событий в<br>Microsoft SQL | <i>C:\inetpub\wwwroot\ls\targetConfigs\sampleDb.config</i>     |
| Конфигурация хранения событий в<br>PostgreSQL    | <i>C:\inetpub\wwwroot\ls\targetConfigs\postgresDb.config</i>   |
| Конфигурация хранения событий в<br>SysLog        | <i>C:\inetpub\wwwroot\ls\targetConfigs\sampleSyslog.config</i> |



#### ПРИМЕЧАНИЕ

- Для Identity Provider 8.1.5 и выше используется конфигурационный файл *app-settings.json* вместо *Web.config*.
- В Access Manager версии 8.2 и выше компонент Key Server переименован в Indeed Key. Соответственно, название директории переименовано в *indeedkey* вместо *airkeycloud*.

# Установка и настройка модулей интеграции



## Indeed Identity Provider

Количество глав: 5



## Indeed ADFS Extension

Количество глав: 2



## Indeed IIS Extension

Количество глав: 4



## Indeed RDP Windows Logon

Количество глав: 3



## Indeed NPS RADIUS Extension

Количество глав: 3



## Indeed Mobile Device Provisioning

Настройка синхронизации устройства, помещенного в карантин



## Indeed Enterprise Single Sign-On

Количество глав: 6



## Indeed Windows Logon

Количество глав: 6



## Утилита управления аутентификаторами

Количество глав: 4



# Indeed Identity Provider

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

Начиная с версии Indeed AM Access Manager 8.1.5 модуль Indeed 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 можно найти в [документации Indeed Access Manager 8.1](#).

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

В Identity Provider вы можете выполнить аутентификацию по следующим аутентификаторам:

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

# Предварительная настройка

Перед установкой Identity Provider:

1. Установите на сервере .NET 6.

Для этого запустите утилиту *dotnet-hosting-6.0.10-win.exe*, расположенную по пути *Indeed AM <номер версии>/Indeed AM Idp*.

Корректная работа Identity Provider гарантируется только при использовании .NET 6.

2. Установите необходимые компоненты **Internet Information Services**.

Для этого запустите скрипт *Indeed.SAML.IIS.Install.MSSserver.ps1* из *Indeed AM <номер версии>/Misc/IISScripts* в PowerShell от имени администратора.

Если настройки безопасности не позволяют запустить скрипт, откройте *Indeed.SAML.IIS.Install.MSSserver.ps1* с помощью блокнота, скопируйте все команды и выполните их в PowerShell от имени администратора.

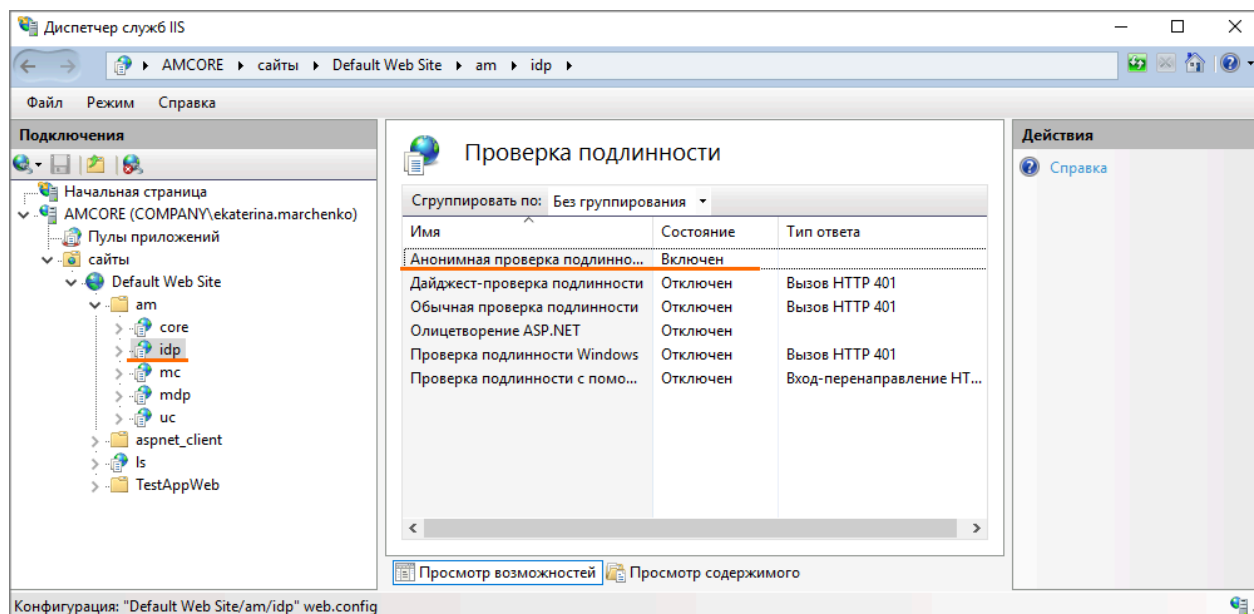


## ВАЖНО!

По умолчанию Identity Provider использует аутентификацию Windows. Для внедоменных сценариев включите анонимную аутентификацию.

## ▼ Включить анонимную аутентификацию

1. В Диспетчере служб IIS в левом меню выберите Indeed AM → сайты → Default Web Site → am → idp и нажмите Проверка подлинности.
2. Включите опцию Анонимная проверка подлинности, остальные опции оставьте выключенными.



## Установить и настроить Identity Provider

Чтобы установить и настроить Identity Provider:

1. Запустите *IndeedAM.IDP-<номер версии>.ru-ru.msi*, расположенный по пути *Indeed AM <номер версии>/Indeed AM Idp*.

По умолчанию после установки пакета создается и устанавливается новый сертификат сервера IDP. Сертификат шифрует данные, передаваемые между Core Server и конечными приложениями, например Management Console.

Сертификат не предназначен для организации соединения по протоколу SSL.

Если сертификат был сгенерирован ранее, в окне мастера установки уберите флажок **Создать и установить новый сертификат IDP сервера**.

## 2. Добавьте привязку в настройках PIS:

1. В Диспетчере служб PIS в левом меню выберите Indeed AM → сайты → Default Web Site
2. Нажмите Привязки в разделе Действия в правом меню.
3. Нажмите Добавить и в открывшемся окне задайте следующие параметры:
  - В поле Тип выберите https.
  - В поле Порт укажите 443.
  - В поле SSL-сертификат выберите сертификат веб-сервера.
4. Нажмите ОК, чтобы сохранить привязку.

## ❗ ПРИМЕЧАНИЕ

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, отредактируйте файл *Web.config* в папке *C:\inetpub\wwwroot\am\idp*.

### ▼ Изменить файл *Web.config*

В теге `aspNetCore` добавьте следующие строки:

```
<environmentVariables>
  <environmentVariable name="ASPNETCORE_ENVIRONMENT"
value="Development" />
</environmentVariables>
```

Результат:

```
<aspNetCore processPath="dotnet" arguments=".\\AM.IDP.dll"
stdoutLogEnabled="false" stdoutLogFile=".\logs\stdout"
hostingModel="inprocess">
  <environmentVariables>
    <environmentVariable name="ASPNETCORE_ENVIRONMENT"
value="Development" />
  </environmentVariables>
</aspNetCore>
```

## Редактировать конфигурационный файл

Чтобы настроить модуль Identity Provider:

1. Откройте конфигурационный файл `app-settings.json`, расположенный по пути `C:\inetpub\wwwroot\am\idp`.
2. В разделе `AuthenticationServer` в параметре `Url` укажите адрес Core Server 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/`



#### ВАЖНО!

Для корректной работы рекомендуем установить клиентский сертификат на каждый Core Server.

Чтобы ошибки сертификата сервера игнорировались, измените значение параметра `IsIgnoreCertErrors` на значение `true`.

3. В разделе `Server` в параметре `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. В разделе `LocalIdentityProviderConfiguration` задайте значения следующих параметров:

- В параметре `SingleSignOnServiceUrl` укажите адрес Identity Provider в формате *http(s)://полное\_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
```

- В параметре `Thumbprint` укажите отпечаток сертификата Identity Provider, который был сгенерирован при установке.

```
"LocalIdentityProviderConfiguration": {  
    "LocalCertificates": [  
        {  
            "Thumbprint": "ВАШ_ОПЕЧАТОК_СЕРТИФИКАТА"  
        }  
    ]  
}
```

Чтобы получить отпечаток сертификата, используйте запрос PowerShell:

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

5. В разделе `AuthenticationMethods` удалите ненужные строки и добавьте идентификаторы провайдеров, которые вы планируете использовать, в следующем формате:

- В параметре `Name` укажите произвольное уникальное значение.
- В параметре `Providers` укажите идентификатор используемого провайдера.

### ▼ Доступные идентификаторы для Identity Provider

---

- SMS OTP {EBB6F3FA-A400-45F4-853A-D517D89AC2A3}
- Storage SMS OTP {3F2C1156-B5AF-4643-BFCB-9816012F3F34}
- Email OTP {093F612B-727E-44E7-9C95-095F07CBB94B}
- Passcode {F696F05D-5466-42b4-BF52-21BEE1CB9529}
- Software OTP {0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0}
- Secured TOTP {F15FD7EC-19EA-4384-846E-A2D0BE149FA2}
- Hardware OTP {AD3FBA95-AE99-4773-93A3-6530A29C7556}
- Hardware TOTP {CEB3FEAF-86ED-4A5A-BD3F-6A7B6E60CA05}
- Indeed Key {DEEF0CB8-AD2F-4B89-964A-B6C7ECA80C68}
- Windows Password {CF189AF5-01C5-469D-A859-A8F2F41ED153}
- Telegram Provider {CA4645CC-5896-485E-A6CA-011FCC20DF1D}

#### Пример использования одного провайдера

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

#### Пример использования нескольких провайдеров



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

7. В разделе **SelfService** задайте параметру

**AllowWinPwdIfAuthMethodsAreNotAvailable** одно из значений:

- Если задать значение **true**, тогда в User Console можно будет войти через Identity Provider, используя Windows Password, даже если у пользователя нет аутентификатора. Также это значение позволяет войти в User Console по любому аутентификатору, даже если он не указан в разделе **AuthenticationMethods**.
- Если задать значение **false**, то авторизация по Windows Password будет недоступна, если этот способ аутентификации отсутствует в разделе **AuthenticationMethods**. Войти в User Console можно будет только с помощью указанного в этом разделе аутентификатора.

#### ❗ ПРИМЕЧАНИЕ

Если вы одновременно используете аутентификацию по Windows Password и по провайдеру, журнал событий отображает следующее:

- Если Windows Password был введен верно, а провайдер неверно, то в событиях пользователя регистрируется успешный вход в Identity Provider с помощью Windows Password.
- Если и Windows Password, и провайдер введены верно, то в событиях пользователя регистрируется успешный вход с помощью провайдера.

8. В разделе **OIDC** в параметре **CertificateThumbprint** укажите отпечаток сертификата Identity Provider, который был сгенерирован при установке.

Чтобы получить отпечаток сертификата, используйте запрос PowerShell:

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

9. (Опционально) Чтобы настроить работу AM 8.2 с **Mobile Device Provisioning 9.x** и аутентификацией через IDP 8.2, в блоке **SAML** для приложения `urn:indeedid:mobiledeviceprovisioning` добавьте параметры:

- **SignLogoutResponse** со значением **true** — параметр необходим для корректной работы кнопки Выход в интерфейсе MDP 9.x, без данной настройки может отображаться ошибка;
- **Thumbprint** с отпечатком сертификата Identity Provider 8.2.

Чтобы получить отпечаток сертификата, используйте запрос PowerShell:

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

#### ▼ Пример

```
{
  "Name": "urn:indeedid:mobiledeviceprovisioning",
  "SingleLogoutServiceUrl": "https://amcore.indeed-
test.com/am/mdp/Account/SLOService",
  "SignLogoutResponse": true,
  "PartnerCertificates": [
    {
      "Thumbprint": "67446E7995669269987637CA26F953D4B9E9F2DC"
    }
  ]
},
```

9. Сохраните конфигурационный файл и перезапустите IIS.

# Интеграция с приложениями по протоколам OpenID Connect и OAuth 2.0

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

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

| Параметр                      | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>CustomAttributes</code> | В блоке указываются атрибуты <code>ServiceProvider</code> и <code>Attributes</code> (с параметрами <code>Name</code> и <code>UserNameFormat</code> ).                                                                                                                                                                                                                                                                                                                                                                                          |
| <code>ServiceProvider</code>  | Значение параметра соответствует <code>ClientId</code> из секции <code>OIDC</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <code>Name</code>             | Определяет с каким ключом будет отображаться передаваемый атрибут в результате расшифровки значения <code>IdToken</code> или запроса к <code>Userinfo</code> . При этом если параметр <code>Name</code> не соответствует одному из возможных значений ( <code>email</code> , <code>name</code> , <code>family_name</code> , <code>given_name</code> , <code>middle_name</code> ), то передаваемый атрибут не будет отображаться в ответе на запрос к <code>Userinfo</code> , но в расшифровке <code>IdToken</code> атрибут будет отображаться. |
| <code>UserNameFormat</code>   | Определяет какая информация о пользователе будет передана <code>OIDC</code> -клиенту. Данный параметр может принимать строго определенный перечень значений: <code>Id</code> , <code>ObjectGUID</code> , <code>Name</code> , <code>CanonicalName</code> , <code>PrincipalName</code> , <code>SamCompatibleName</code> , <code>DistinguishedName</code> , <code>Sid</code> , <code>FirstName</code> , <code>MiddleName</code> , <code>LastName</code> , <code>Email</code> , <code>Phone</code> .                                               |

| Параметр                           | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>CertificateThumbprint</code> | <p>Указывается отпечаток сертификата Identity Provider.</p> <p>Сертификат загружается в хранилище компьютера, где установлен Indeed AM Identity Provider.</p>                                                                                                                                                                                                                                                                               |
| <code>Clients</code>               | <p>В блоке указываются настройки для каждого клиентского приложения. Клиентских приложений может быть несколько.</p>                                                                                                                                                                                                                                                                                                                        |
| <code>ClientId</code>              | <p>Уникальный идентификатор, который используется для определения клиентского приложения при обмене токенов, а также для аутентификации и авторизации пользователя.</p> <p>Когда клиентское приложение запрашивает доступ к защищенным ресурсам, оно предоставляет свой <code>ClientId</code> вместе с другими учетными данными для получения токена доступа. Значение по умолчанию: <i>example-client</i>.</p>                             |
| <code>ClientSecret</code>          | <p>Представляет собой строку символов, которая известна только клиентскому приложению и серверу IDP.</p> <p><code>ClientSecret</code> используется в процессе обмена токенов для подтверждения идентификации клиентского приложения.</p> <p>При запросе токена доступа клиент должен предоставить свой <code>ClientId</code> и <code>ClientSecret</code> для аутентификации.</p> <p>Значение по умолчанию: <i>secret_secret_secret</i>.</p> |
| <code>DisplayName</code>           | <p>Имя клиентского приложения. Используется для отображения информации в интерфейсе клиента. Значение по умолчанию: <i>Example client application</i>.</p>                                                                                                                                                                                                                                                                                  |
| <code>Permissions</code>           | <p>В блоке указываются атрибуты, которые будут разрешены приложению. После успешной аутентификации и предоставления разрешений приложение может использовать полученные данные. Данные, указанные в <code>Permissions</code>, могут быть переданы в ответе по протоколу OIDC (ept — Endpoints, gt — GrantTypes, rst — ResponseTypes, scp — Scopes).</p>                                                                                     |

| Параметр                           | Описание                                                                                                                                                             |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>ept:authorization</code>     | Инициирование авторизации.                                                                                                                                           |
| <code>ept:logout</code>            | Завершение сессии, связанной с токеном по идентификатору.                                                                                                            |
| <code>ept:token</code>             | Используется для получения токена.                                                                                                                                   |
| <code>gt:authorization_code</code> | Используется для получения токенов (ID Token и Access Token) с помощью промежуточного кода авторизации.                                                              |
| <code>gt:refresh_token</code>      | Используется для получения нового токена доступа без необходимости повторной аутентификации пользователя.                                                            |
| <code>rst:code</code>              | Используется для получения кода авторизации.                                                                                                                         |
| <code>scp:email</code>             | Адрес электронной почты пользователя.                                                                                                                                |
| <code>scp:profile</code>           | Информация о профиле пользователя включает следующие компоненты: <code>name</code> , <code>given_name</code> , <code>family_name</code> , <code>middle_name</code> . |
| <code>scp:openid</code>            | Указывает, что клиентское приложение запрашивает аутентификацию пользователя.                                                                                        |
| <code>scp:offline_access</code>    | Позволяет клиентскому приложению запрашивать токен обновления ( <code>refresh token</code> ).                                                                        |
| <code>PostLogoutRedirectUri</code> | Содержит допустимые URL-адреса, на которые перенаправляется пользователь после выхода из клиентского приложения.                                                     |
| <code>RedirectUri</code>           | Содержит допустимые URL-адреса, на которые перенаправляется пользователь после успешного входа в клиентское приложение.                                              |

| Параметр                  | Описание                                                                                                                                          |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>Requirements</code> | Определяет дополнительные требования к клиентским запросам, которые должны быть выполнены для успешной аутентификации и авторизации пользователя. |

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

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

Подробнее о настройке интеграции с приложениями по протоколам OpenID Connect и OAuth 2.0 вы можете узнать в базе знаний в статьях [Настройка OIDC на примере Keycloak](#) и [Настройка NextCloud + OIDC](#).

# Интеграция с приложениями по протоколу SAML

- Identity Provider Login URL —  
*http(s)://<полное\_DNS\_имя\_сервера\_Identity\_Provider>/am/idp/Account/SsoService.*
- Identity Provider Logout URL —  
*http(s)://<полное\_DNS\_имя\_сервера\_Identity\_Provider>/am/idp/Account/Logout.*
- Identity Provider Name — *urn:indeedid:saml\_idp.*

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

| Параметр                            | Описание                                                                                                                                                                                         |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>SingleSignOnServiceUrl</code> | Содержит URL-адрес Single SignOn Service, который получает сообщения SAML о входе в клиентское приложение                                                                                        |
| <code>LocalCertificates</code>      | Указывается сертификат Identity Provider. Сертификат загружается в хранилище компьютера, где развернут Indeed AM Identity Provider. Сертификат указывается в параметре <code>Thumbprint</code> . |
| <code>SingleLogoutServiceUrl</code> | Содержит URL-адрес Single Logout, который получает сообщения SAML о выходе из клиентского приложения.                                                                                            |
| <code>PartnerCertificates</code>    | Указывается сертификат клиентского приложения. Сертификат указывается в параметре <code>Thumbprint</code> .                                                                                      |
| <code>Name</code>                   | Указывается имя клиентского приложения.                                                                                                                                                          |
| <code>Description</code>            | Указывается описание клиентского приложения.                                                                                                                                                     |

| Параметр                              | Описание                                                                                                                                                                   |
|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>WantAuthnRequestSigned</code>   | Параметр указывает, должен ли запрос аутентификации SAML быть подписанным. Рекомендуемое значение: <i>true</i> .                                                           |
| <code>SignSAMLResponse</code>         | Параметр указывает, должны ли быть подписаны ответы SAML, отправляемые клиентскому приложению. Рекомендуемое значение: <i>true</i> .                                       |
| <code>WantSamlResponseSigned</code>   | Параметр указывает, должны ли утверждения SAML шифроваться. Рекомендуемое значение: <i>true</i> .                                                                          |
| <code>SignLogoutRequest</code>        | Параметр указывает, должны ли быть подписаны запросы SAML, отправляемые клиентскому приложению, на выход из клиентского приложения. Рекомендуемое значение: <i>true</i> .  |
| <code>SignLogoutResponse</code>       | Параметр указывает, должны ли быть подписаны ответы SAML, отправляемые клиентскому приложению, на выход из клиентского приложения. Рекомендуемое значение: <i>true</i> .   |
| <code>SignAssertion</code>            | Параметр указывает, должны ли утверждения SAML быть подписаны. Рекомендуемое значение: <i>true</i> .                                                                       |
| <code>WantLogoutRequestSigned</code>  | Параметр указывает, должны ли быть подписаны запросы SAML, полученные от клиентского приложения, на выход из клиентского приложения. Рекомендуемое значение: <i>true</i> . |
| <code>WantLogoutResponseSigned</code> | Параметр указывает, должны ли быть подписаны ответы SAML, полученные от клиентского приложения, на выход из клиентского приложения. Рекомендуемое значение: <i>true</i> .  |



| Параметр                                 | Описание                                                                                                      |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| <code>AssertionConsumerServiceUrl</code> | Параметр содержит URL-адрес Assertion Consumer Service клиентского приложения, который получает запросы SAML. |

Пример интеграции по протоколу SAML IDP и Nextcloud вы можете посмотреть в [базе знаний](#).

# Включение защиты от перебора

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

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

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

По умолчанию данная настройка отключена.

Чтобы включить защиту от перебора:

1. Откройте конфигурационный файл сервера Indeed AM *web.config*, расположенный в папке *C:\inetpub\wwwroot\am\core*.
2. Измените параметр `appSettings`. В строке `bruteForceProtectionApps` укажите значение *Identity Provider*.

## Пример

```
<appSettings>
  <add key="requireHttps" value="true" />
  <add key="enableSwagger" value="false" />
  <add key="bruteForceProtectionApps" value="Identity Provider" />
</appSettings>
```

3. Сохраните изменения и перезапустите IIS.

# 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*, расположенный в папке *C:\inetpub\wwwroot\am\idp*.
2. Измените параметр `AuthenticationSettings`. В строке `Domains` укажите значения необходимых доменов.

## Пример

```
"AuthenticationSettings": {  
  "SessionExpirationTimeInMinutes": 30,  
  "Domains": [  
    "test.local",  
    "demo.local",  
    "indeed.local"  
  ]  
}
```

3. Сохраните файл и перезапустите IIS.

# Переключение режима работы Telegram Provider

Выполнить вход в Identity Provider с помощью Telegram Provider можно через одноразовый пароль или через push-уведомление с запросом подтвердить или отклонить вход.

Чтобы выбрать способ подтверждения входа:

1. На боковой панели Management Console откройте раздел Политики.
2. Из списка политик выберите политику с добавленным приложением Identity Provider.
3. Откройте вкладку Приложения и перейдите в приложение Identity Provider.
4. В пункте Режим работы Telegram выберите способ аутентификации — одноразовый пароль или push-уведомление.

# Indeed ADFS Extension



## Indeed ADFS Extension (2012)

Двухфакторная аутентификация с использованием ADFS



## Indeed ADFS Extension (2016)

Двухфакторная аутентификация с использованием ADFS

# Indeed ADFS Extension (2012)

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

В ADFS Extension вы можете выполнить аутентификацию по следующим аутентификаторам:

- push-уведомления с подтверждением входа и одноразовые пароли в мобильном приложении Indeed Key,
- push-уведомления с подтверждением входа и одноразовые пароли в Telegram Provider,
- Email OTP,
- SMS OTP,
- Storage SMS OTP,
- Secured TOTP,
- Software OTP,
- Passcode,
- Hardware TOTP,
- Hardware OTP.

Примеры внедрения расширения:

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

## Установка и настройка ADFS Extension

1. Запустите файл для установки, расположенный по пути *Indeed AM <номер версии>/Indeed AM ADFS Extension/<номер версии>*, и следуйте шагам мастера установки.
2. Создайте конфигурационный файл *MFAAdapter.json*, содержащий следующие параметры:
  - `EANetServerURL` — адрес сервера Indeed;
  - `ModeId` — идентификатор используемого метода аутентификации.

❗ **MODEID МОЖЕТ ИМЕТЬ СЛЕДУЮЩИЕ ЗНАЧЕНИЯ:**

- SMS OTP {EBB6F3FA-A400-45F4-853A-D517D89AC2A3}
- Storage SMS OTP {3F2C1156-B5AF-4643-BFCB-9816012F3F34}
- Secured TOTP {F15FD7EC-19EA-4384-846E-A2D0BE149FA2}
- Email OTP {093F612B-727E-44E7-9C95-095F07CBB94B}
- Passcode {F696F05D-5466-42b4-BF52-21BEE1CB9529}
- Software OTP {0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0}
- Hardware OTP {AD3FBA95-AE99-4773-93A3-6530A29C7556}
- Hardware TOTP {CEB3FEAF-86ED-4A5A-BD3F-6A7B6E60CA05}
- Indeed Key Provider {DEEF0CB8-AD2F-4B89-964A-B6C7ECA80C68}
- Telegram Provider {CA4645CC-5896-485E-A6CA-011FCC20DF1D}

Пример

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

❗ **ПРИМЕЧАНИЕ**

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

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

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

 **ВАЖНО!**

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

Пример

```
$typeName = "IndeedId.ADFS.MFAAdapter.MFAAdapter,  
IndeedId.ADFS.MFAAdapter, Version=1.0.6.0, Culture=neutral,  
PublicKeyToken=1ebb0d9282100d91"  
Register-AdfsAuthenticationProvider -TypeName $typeName -Name  
"Indeed Id MFA Adapter" -ConfigurationFilePath  
'YourPath\MFAAdapter.json'
```

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

Пример

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

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

Пример

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

4. Чтобы удалить адаптер, выполните следующую команду:

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

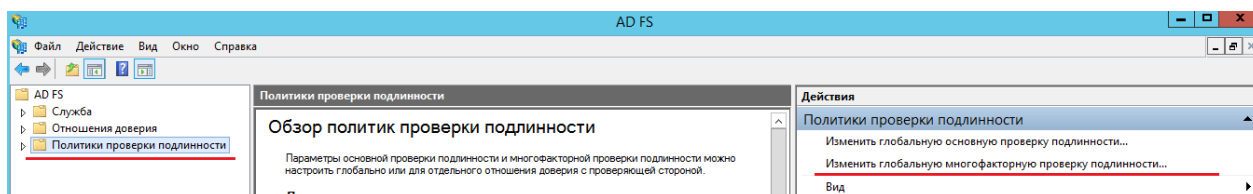


5. Чтобы обновить конфигурацию, выполните следующую команду:

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

## Включение многофакторной аутентификации для ADFS

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



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

## Регистрация аутентификатора при первом входе в ADFS

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

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

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

# Переключение режима работы Telegram Provider

Выполнить вход в ADFS с помощью Telegram Provider можно через одноразовый пароль или через push-уведомление с запросом подтвердить или отклонить вход.

Чтобы выбрать способ подтверждения входа, выполните следующее:

1. В Management Console в меню слева выберите Политики.
2. Из списка политик выберите политику с добавленным приложением ADFS.
3. В меню политики слева выберите пункт Приложения и перейдите в приложение ADFS.
4. В пункте Режим работы Telegram выберите способ аутентификации – одноразовый пароль или push-уведомление.

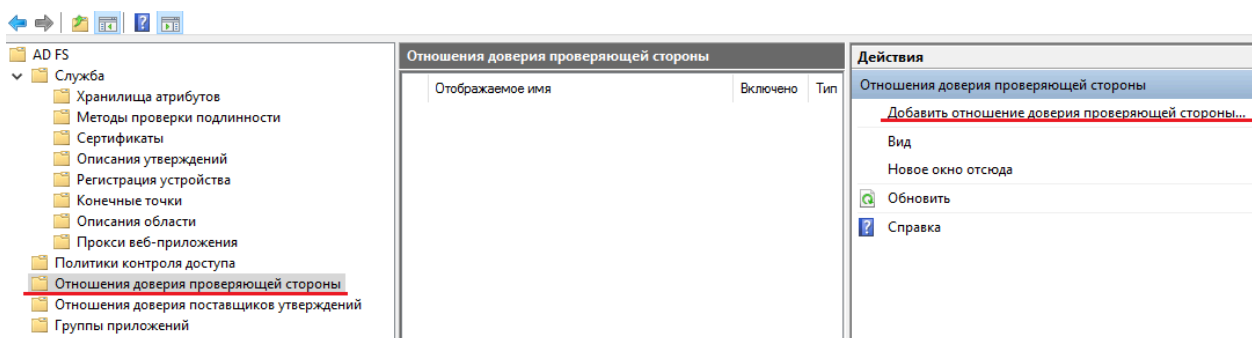
## Пример работы модуля на странице ADFS idpinitiatedsignon

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

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

Настройка тестовой страницы

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



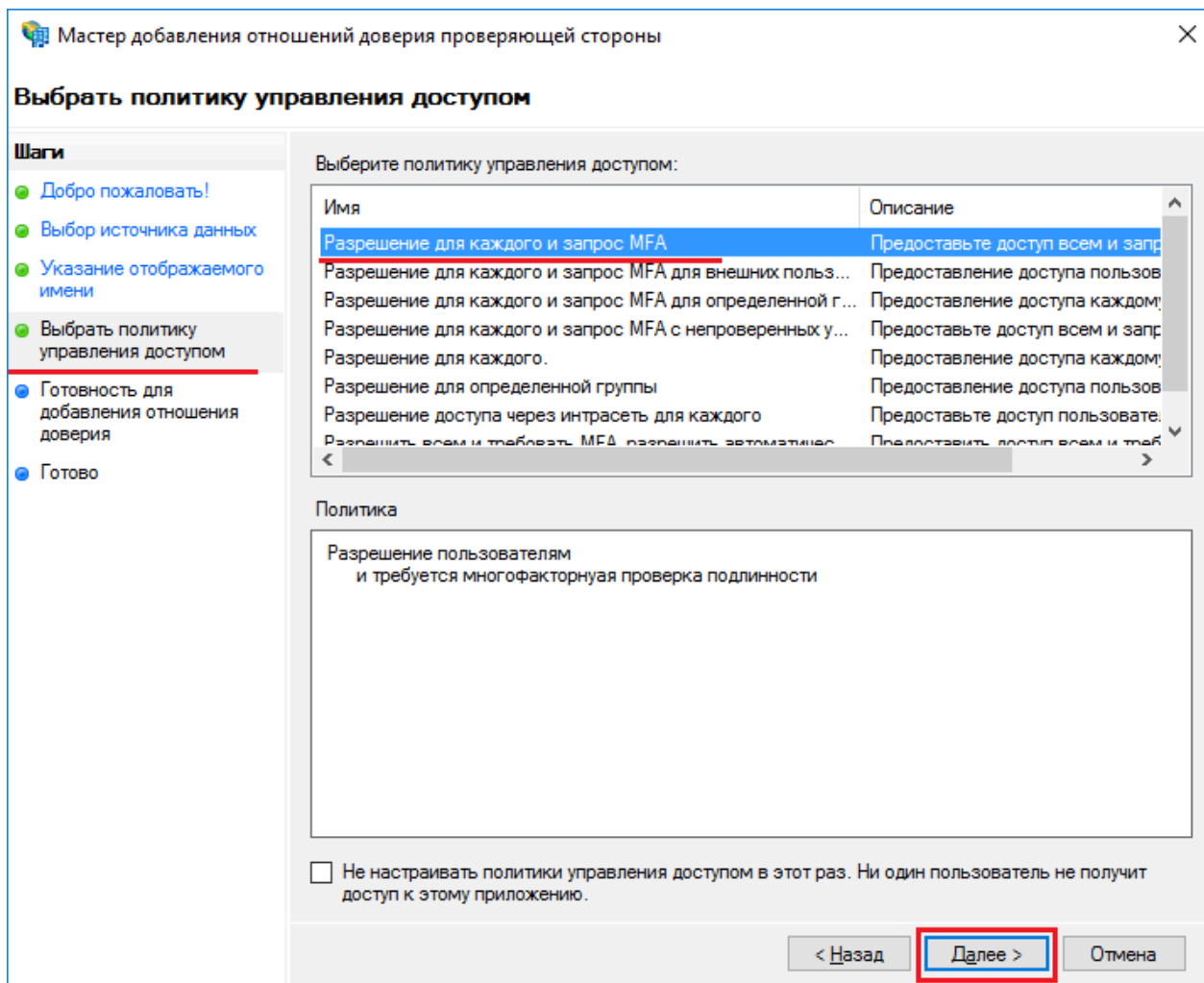
2. На вкладке Добро пожаловать! выберите Поддерживающие утверждения и нажмите Запустить.
3. На вкладке Выбор источника данных укажите URL вашего приложения и нажмите Далее.

## ❗ ИНФОРМАЦИЯ

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

The screenshot shows the 'Master of Trust Relationships' wizard window. The title bar reads 'Мастер добавления отношений доверия проверяющей стороны'. The main heading 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 contains 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', a 'Пример:' line, and an 'Обзор...' button. 2. 'Импорт данных о проверяющей стороне из файла'. 3. 'Ввод данных о проверяющей стороне вручную'. At the bottom, there are three buttons: '< Назад', 'Далее >' (highlighted with a red rectangle), and 'Отмена'.

4. На вкладке Указание отображаемого имени введите имя и описание для вашего отношения доверия и нажмите Далее.
5. На вкладке Выбрать политику управления доступом выберите подходящую вам политику с запросом MFA из предложенных по умолчанию, также вы можете добавить произвольные политики контроля доступа.



6. Остальные параметры оставьте по умолчанию.

7. Для применения изменений перезапустите службу ADFS.

#### Работа модуля

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

# Indeed ADFS Extension (2016)

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

В ADFS Extension вы можете выполнить аутентификацию по следующим аутентификаторам:

- push-уведомления с подтверждением входа и одноразовые пароли в мобильном приложении Indeed Key,
- push-уведомления с подтверждением входа и одноразовые пароли в Telegram Provider,
- Email OTP,
- SMS OTP,
- Storage SMS OTP,
- Secured TOTP,
- Software OTP,
- Passcode,
- Hardware TOTP,
- Hardware OTP.

Примеры внедрения расширения

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

## Установка и настройка ADFS Extension



### ПРИМЕЧАНИЕ

Перед запуском пакета для установки Indeed ADFS Extension добавьте роль службы федерации Active Directory (AD FS).

1. Запустите файл для установки, расположенный по пути *Indeed AM <номер версии>/Indeed AM ADFS Extension/<номер версии>*, и следуйте шагам мастера установки.

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

- **EANetServerURL** — адрес сервера Indeed;
- **ModeId** — идентификатор используемого метода аутентификации.



**MODEID МОЖЕТ ИМЕТЬ СЛЕДУЮЩИЕ ЗНАЧЕНИЯ:**

- SMS OTP {EBB6F3FA-A400-45F4-853A-D517D89AC2A3}
- Storage SMS OTP {3F2C1156-B5AF-4643-BFCB-9816012F3F34}
- Secured TOTP {F15FD7EC-19EA-4384-846E-A2D0BE149FA2}
- Email OTP {093F612B-727E-44E7-9C95-095F07CBB94B}
- Passcode {F696F05D-5466-42b4-BF52-21BEE1CB9529}
- Software OTP {0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0}
- Hardware OTP {AD3FBA95-AE99-4773-93A3-6530A29C7556}
- Hardware TOTP {CEB3FEAF-86ED-4A5A-BD3F-6A7B6E60CA05}
- Indeed Key Provider {DEEF0CB8-AD2F-4B89-964A-B6C7ECA80C68}
- Telegram Provider {CA4645CC-5896-485E-A6CA-011FCC20DF1D}

Пример

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



**ПРИМЕЧАНИЕ**

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

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

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



### ВАЖНО!

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

#### Пример

```
$typeName = "IndeedId.ADFS.MFAAdapter.MFAAdapter,
IndeedId.ADFS.MFAAdapter, Version=1.0.12.0, Culture=neutral,
PublicKeyToken=1ebb0d9282100d91"
Register-AdfsAuthenticationProvider -TypeName $typeName -Name
"Indeed Id MFA Adapter" -ConfigurationFilePath
'YourPath\MFAAdapter.json'
```

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

#### Пример

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

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

#### Пример

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

4. Чтобы удалить адаптер, выполните следующую команду:

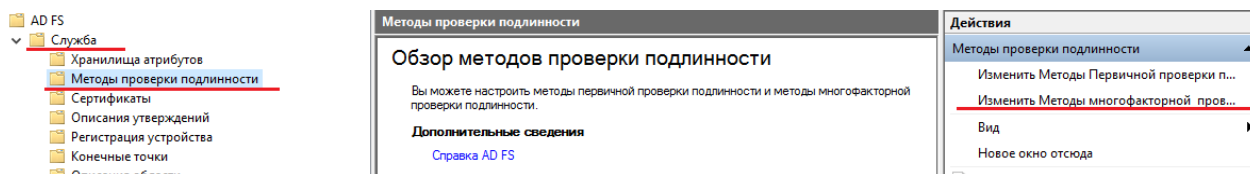
```
Unregister-AdfsAuthenticationProvider -Name "Indeed Id MFA Adapter"
```

5. Чтобы обновить конфигурацию, выполните следующую команду:

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

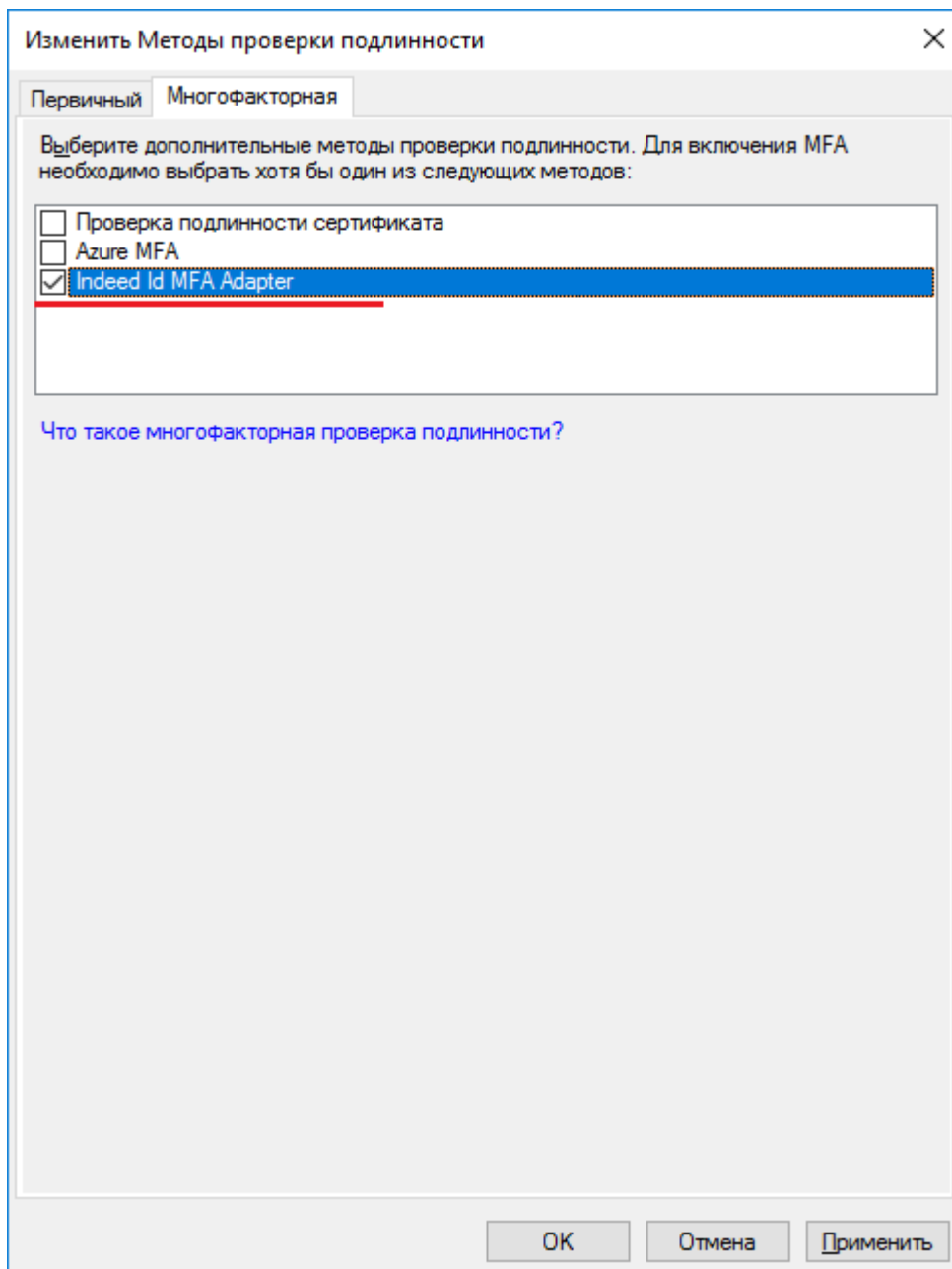
## Включение многофакторной аутентификации для ADFS

1. Откройте консоль управления ADFS.
2. Выберите Служба→Методы проверки подлинности.
3. В окне Действия выберите Изменить методы многофакторной проверки....



4. На вкладке Многофакторная выберите созданный ранее провайдер и нажмите Применить.
5. Для применения изменений перезапустите службу AD FS.





## Регистрация аутентификатора при первом входе в ADFS

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

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

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

# Переключение режима работы Telegram Provider

Выполнить вход в ADFS с помощью Telegram Provider можно через одноразовый пароль или через push-уведомление с запросом подтвердить или отклонить вход.

Чтобы выбрать способ подтверждения входа, выполните следующее:

1. В Management Console в меню слева выберите Политики.
2. Из списка политик выберите политику с добавленным приложением ADFS.
3. В меню политики слева выберите пункт Приложения и перейдите в приложение ADFS.
4. В пункте Режим работы Telegram выберите способ аутентификации – одноразовый пароль или push-уведомление.

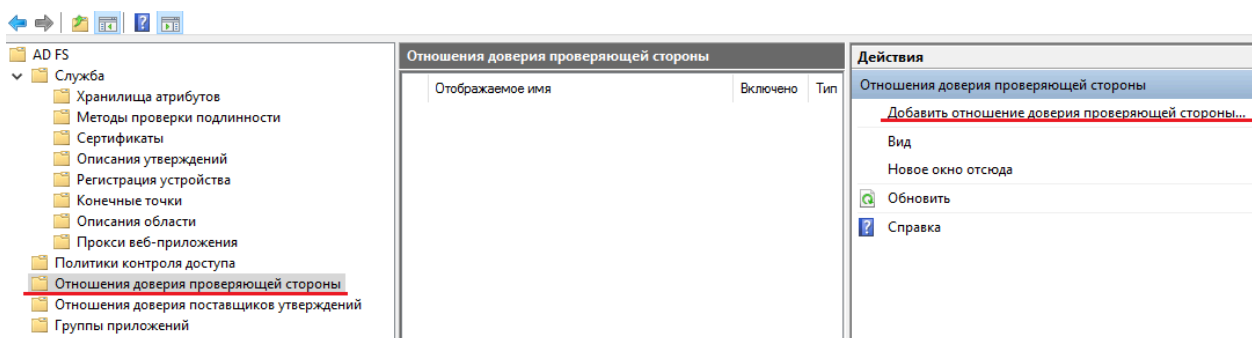
## Пример работы модуля на странице ADFS idpinitiatedsignon

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

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

Настройка тестовой страницы

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



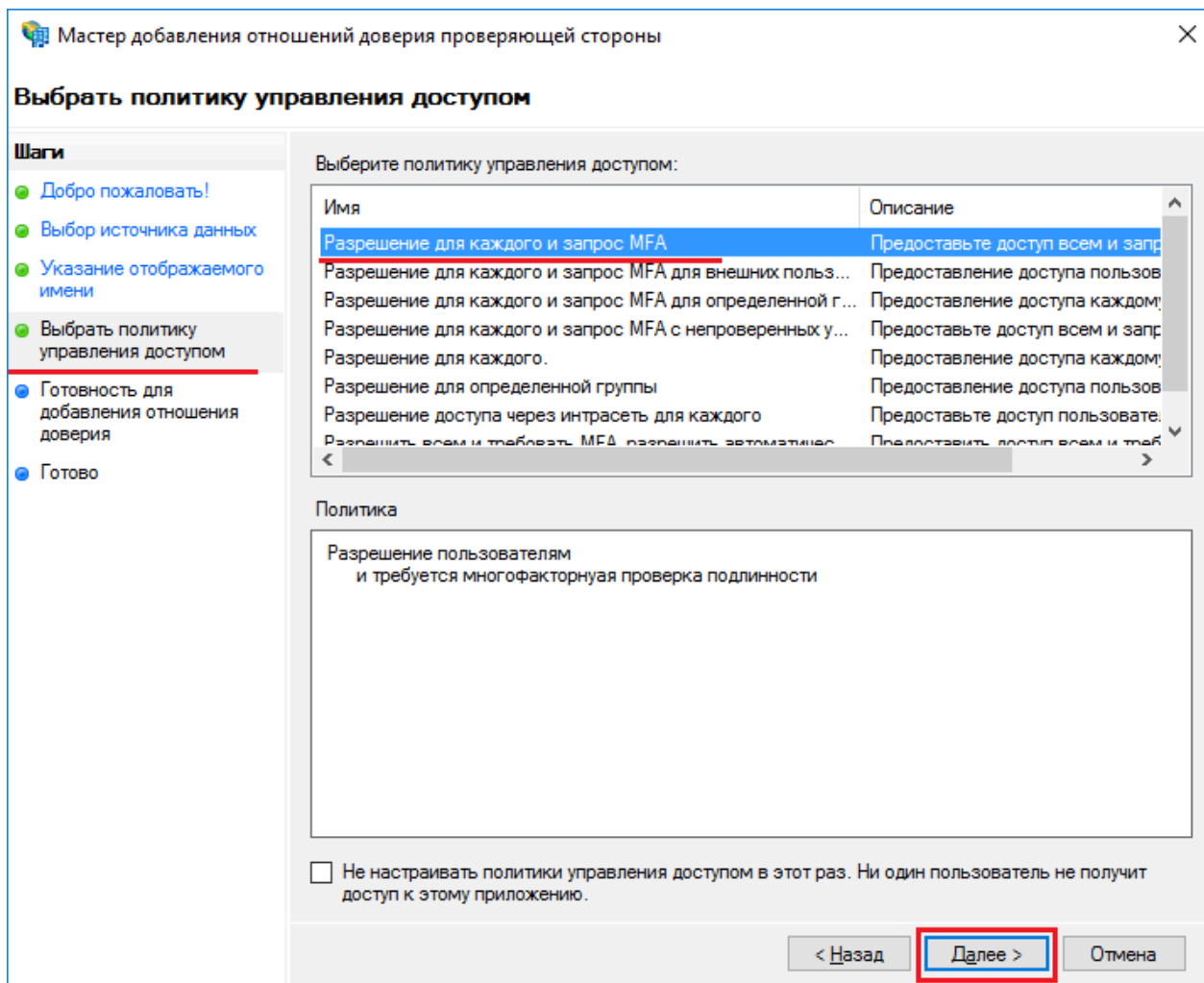
2. На вкладке Добро пожаловать! выберите Поддерживающие утверждения и нажмите Запустить.
3. На вкладке Выбор источника данных укажите URL вашего приложения и нажмите Далее.

## ❗ ИНФОРМАЦИЯ

В качестве примера работы расширения используется стандартная страница ADFS *idpinitiatedsignon.htm*. Используется адрес метаданных для данной страницы, например, *https://<полное\_dns\_имя\_сервера>/federationmetadata/2007-06/federationmetadata.xml*.

The screenshot shows a Windows wizard titled 'Мастер добавления отношений доверия проверяющей стороны' (Master of adding trust relationships for the relying party). The current step is 'Выбор источника данных' (Select data source). On the left, a 'Шаги' (Steps) pane shows five steps: 'Добро пожаловать!' (Welcome!), 'Выбор источника данных' (Select data source), 'Выбор политики управления доступом' (Select access control policy), 'Готовность для добавления отношения доверия' (Ready to add trust relationship), and 'Готово' (Finish). The 'Выбор источника данных' step is highlighted. The main area contains three radio button options: 1. 'Импорт данных о проверяющей стороне, опубликованных в Интернете или локальной сети' (Import data about the relying party published on the Internet or local network). This option is selected. Below it, a text box contains the URL 'https://adfsnew.indeed.local/federationmetadata/2007-06/federationmetadata.xml', which is underlined in red. A note below the text box says 'Пример: fs.contoso.com или https://www.contoso.com/app'. 2. 'Импорт данных о проверяющей стороне из файла' (Import data about the relying party from a file). 3. 'Ввод данных о проверяющей стороне вручную' (Enter data about the relying party manually). At the bottom right, there are three buttons: '< Назад' (Back), 'Далее >' (Next), and 'Отмена' (Cancel). The 'Далее >' 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.



6. Остальные параметры оставьте по умолчанию.

7. Для применения изменений перезапустите службу ADFS.

## Работа модуля

По умолчанию страница *idpinitiatedsignon.htm* отключена в ADFS 2016, для включения запустите PowerShell от имени администратора и выполните команду:

```
Set-AdfsProperties -EnableIdpInitiatedSignonPage $True
```

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

4. После корректного ввода данных будет выполнен вход.

# Indeed IIS Extension

С помощью Indeed IIS Extension (IIS Extension) вы можете настроить двухфакторную аутентификацию в веб-приложениях, использующих проверку подлинности с помощью форм (Forms Authentication) и развернутых на платформе Microsoft Internet Information Services (IIS).

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 или push-уведомлению в приложении Indeed Key.

В IIS Extension вы можете выполнить аутентификацию по следующим аутентификаторам:

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

Примеры внедрения IIS Extension:

- **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**

## Предварительная настройка

Чтобы использовать модуль IIS Extension:

1. Установите **Indeed AM Windows Password Provider** на компьютер с установленным Core Server.
2. При использовании соединения по протоколу HTTPS выполните **установку клиентского сертификата** на каждый Core Server.
3. **Установите и настройте** IIS Extension.
4. Настройте **IIS**.
5. Настройте интеграцию IIS Extension с **бизнес-приложением**.
6. При необходимости задайте **опциональные настройки**.

## Установить и настроить IIS Extension

Чтобы установить модуль:

1. Запустите файл для установки *Indeed.AM.IIS.Extension-<номер версии>.x64.ru-ru.msi*, расположенный по пути *Indeed AM <номер версии>/Indeed AM IIS Extension/<номер версии>*, и следуйте шагам мастера установки. При необходимости вы можете изменить папку для установки.
2. Откройте редактор реестра Windows.
3. В разделе *HKEY\_LOCAL\_MACHINE\SOFTWARE\Indeed-ID\SrvLocator2* измените следующие параметры:
  - В параметре **ServerUrlBase** укажите URL вашего Core Server в формате *http(s)://полное\_dns\_имя\_сервера/am/core*.
  - В параметре **IsIgnoreCertErrors** укажите значение 0 или 1. Этот параметр предназначен для проверки сертификата сервера Indeed, при значении 1 ошибки сертификата игнорируются.
4. В разделе *HKEY\_LOCAL\_MACHINE\SOFTWARE\Indeed-ID* в разделе **IISHTTPModule** создайте следующие параметры:
  - Строковый параметр **LSUrl**. В значении параметра укажите URL вашего Core Server в формате *http(s)://полное\_dns\_имя\_сервера/ls/api*.
  - Строковый параметр **ProviderId**. Это необязательный параметр. В значении укажите идентификатор провайдера, который станет провайдером по умолчанию при первом входе.

▼ Возможные значения **ProviderId**

- SMS OTP {EBB6F3FA-A400-45F4-853A-D517D89AC2A3}
- Email OTP {093F612B-727E-44E7-9C95-095F07CBB94B}
- Passcode {F696F05D-5466-42b4-BF52-21BEE1CB9529}
- Software OTP {0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0}
- Hardware OTP {AD3FBA95-AE99-4773-93A3-6530A29C7556}
- Hardware TOTP {CEB3FEAF-86ED-4A5A-BD3F-6A7B6E60CA05}
- Indeed Key (только в режиме push-уведомлений) {DEEF0CB8-AD2F-4B89-964A-B6C7ECA80C68}
- Telegram Provider {CA4645CC-5896-485E-A6CA-011FCC20DF1D}

## Настроить IIS

ⓘ **ПРИМЕЧАНИЕ**

В этой инструкции рассмотрен пример настройки для Exchange 2016.

Чтобы настроить IIS:

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), выберите модули Indeed и нажмите ОК.

## Интеграция IIS Extension с бизнес-приложением

Двухфакторную аутентификацию необходимо настраивать отдельно для каждого целевого приложения.

Чтобы настроить интеграцию:

1. Откройте редактор реестра Windows.

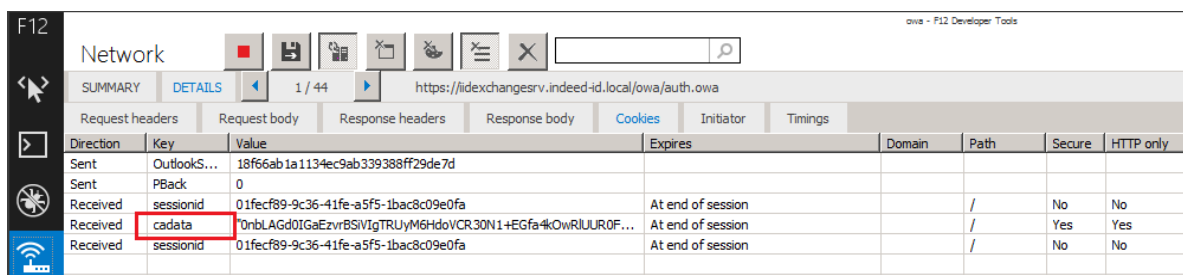


2. В разделе *HKEY\_LOCAL\_MACHINE\SOFTWARE\Indeed-ID\IISHTTPModule* создайте раздел с именем приложения или сайта в IIS. Значение может быть произвольным.

3. В созданном разделе создайте следующие параметры:

- **AuthCookie** — строковый параметр. Название cookie, которое используется для аутентификации в целевом приложении. Определяется экспериментальным путем для каждого приложения. Чтобы получить значение параметра из консоли F12 IE Developer Toolbar:

1. В разделе Сеть (Network) запустите Сбор сетевого трафика (Enable network traffic capturing).
2. Выполните аутентификацию в приложении.
3. Перейдите в раздел Подробности (Details) на вкладку Cookie (Cookies).
4. Найдите значение в столбце Ключ (Key).



| Direction | Key         | Value                                                    | Expires           | Domain | Path | Secure | HTTP only |
|-----------|-------------|----------------------------------------------------------|-------------------|--------|------|--------|-----------|
| Sent      | OutlookS... | 18f66ab1a1134ec9ab339388ff29de7d                         |                   |        |      |        |           |
| Sent      | PBack       | 0                                                        |                   |        |      |        |           |
| Received  | sessionid   | 01fecf89-9c36-41fe-a5f5-1bac8c09e0fa                     | At end of session |        | /    | No     | No        |
| Received  | cadata      | 0nbLAGd0IGaEzvrBSIVigTRUyM6HdoVCR30N1+EGfa4kOwRIUUR0F... | At end of session |        | /    | Yes    | Yes       |
| Received  | sessionid   | 01fecf89-9c36-41fe-a5f5-1bac8c09e0fa                     | At end of session |        | /    | No     | No        |

- **isMFAEnabled** — параметр типа DWORD. Включение двухфакторной аутентификации.
- **LoginURL** — строковый параметр. Относительный URL, на который происходит POST-отправка данных формы входа приложения. Должен начинаться с косой черты (/). URL указывается относительно целевого сайта.
- **MatchTargetRedirect** — параметр типа DWORD. 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 переход 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 модуль IIS 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.
- **LoginReferer** — строковый параметр. Позволяет разделить запросы от приложений, которые используют одну и ту же страницу входа. Создайте параметр с уникальным значением для каждого приложения.



#### ВАЖНО!

Если адрес сервера соответствует имени приложения, источник запроса для страницы входа будет содержать это имя приложения, даже если вы установите разные значения **LoginReferer**.

#### ▼ Пример

Например, адрес сервера *ecp.indeed.local*. Вы настроили два **LoginReferer** — *%2fowa* и *%2fecp*. Страница входа и для приложения OWA, и для приложения ECP будет содержать часть имени сервера *%2fecp.indeed.local*.

Для решения этой проблемы в **LoginReferer** укажите:

- для OWA: *%2fecp.indeed.local%2fowa*
- для ECP: *%2fecp.indeed.local%2fecp*

- **RedirectToTarget** — параметр типа DWORD. Переход на целевую страницу.
- **TargetURL** — строковый параметр. URL целевой страницы, на которую пользователь попадает после аутентификации в приложении.



### ВАЖНО!

Для Exchange 2013 и 2016 указывается `/owa` (без завершающей косой черты `/`), для Exchange 2010 указывается `/owa/` (с завершающей косой чертой `/`).

- `UsernameField` — строковый параметр. Значение атрибута `name` поля имени пользователя формы входа приложения.

Значения всех параметров — `LoginURL, PasswordField, UsernameField` — содержатся в форме аутентификации целевого приложения и 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

| Computer                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Name             | Type      | Data             |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|-----------|------------------|
| <ul style="list-style-type: none"> <li>Computer <ul style="list-style-type: none"> <li>HKEY_CLASSES_ROOT</li> <li>HKEY_CURRENT_USER</li> <li>HKEY_LOCAL_MACHINE <ul style="list-style-type: none"> <li>BCD00000000</li> <li>COMPONENTS</li> <li>HARDWARE</li> <li>SAM</li> <li>Schema</li> <li>SECURITY</li> <li>SOFTWARE <ul style="list-style-type: none"> <li>Classes</li> <li>Clients</li> <li>Indeed-ID <ul style="list-style-type: none"> <li>AuthProxy</li> <li>IISHTTPModule <ul style="list-style-type: none"> <li>Exchange</li> <li>iisconfig</li> <li>Logging</li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> | (Default)        | REG_SZ    | (value not set)  |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | AuthCookie       | REG_SZ    | cadata           |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | IsMFAEnabled     | REG_DWORD | 0x00000001 (1)   |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | LoginURL         | REG_SZ    | /owa/auth.owa    |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | MatchTargetRe... | REG_DWORD | 0x00000001 (1)   |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | OTPURL           | REG_SZ    | /owa/iidotp.aspx |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | PasswordField    | REG_SZ    | password         |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | RedirectToTarget | REG_DWORD | 0x00000000 (0)   |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | TargetURL        | REG_SZ    | /owa             |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | UsernameField    | REG_SZ    | username         |



#### ПРИМЕЧАНИЕ

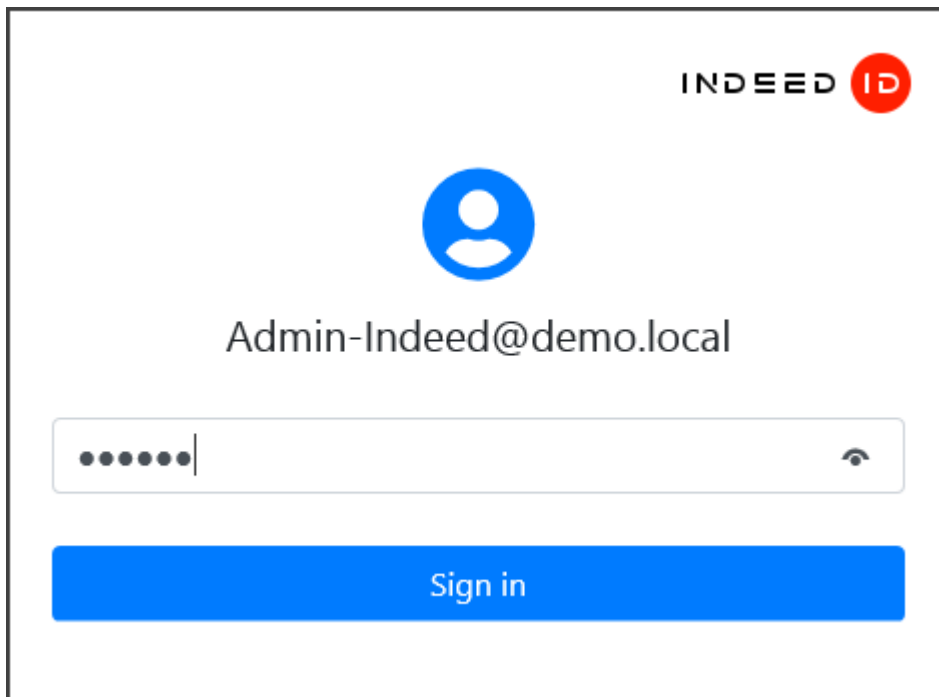
Если используете приложение OWA, в редакторе реестра отключите обычную проверку подлинности (Basic authentication). Создайте параметр типа DWORD **IsBasicDisabled** со значением *1* по следующему пути: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Indeed-ID\IISHTTPModule\IISConfig\owa*.

## Опциональные настройки

- Отключение запроса **второго фактора**
- Смена **локализации**
- Настройка **хранения сессии в кеше**
- Варианты написания **доменного имени для OWA**

## Пример работы модуля

1. Откройте приложение OWA и введите доменный логин и пароль.
2. После корректного ввода появится окно с запросом второго фактора.



The image shows a login interface for 'Indeed ID'. In the top right corner, the text 'INDEED' is in black and 'ID' is in white inside a red circle. In the center, there is a blue circular icon with a white person silhouette. Below the icon, the email address 'Admin-Indeed@demo.local' is displayed. Underneath the email is a password input field with six dots and a cursor, and a small eye icon on the right. At the bottom is a large blue button with the text 'Sign in' in white.

3. После успешного ввода одноразового пароля откроется приложение.

# 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:

- 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).



## ПРИМЕЧАНИЕ

Вы можете указать не более 252 адресов.

| 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 |  |

# Смена локализации

Вы можете настроить локализацию на машине с установленным модулем IIS Extension. Для этого:

1. Откройте редактор реестра Windows.
2. В разделе *HKEY\_LOCAL\_MACHINE\SOFTWARE\Indeed-ID\IISHTTPModule* создайте ключ `LanguageId` типа DWORD.
3. Задайте одно из значений в десятичном формате:
  - *1033* — English;
  - *1049* — русский.

По умолчанию указана локализация устанавливаемого дистрибутива.



# Настройка срока хранения сессии

При кратковременных разрывах подключения к Core Sever можно настроить период, в течение которого сессию можно будет использовать повторно.

В течение заданного периода сессия хранится в кеше и может быть повторно использована при запросе на новое соединение с сервером. При этом проверка работоспособности сервера повторно не происходит, вместо этого используется закешированный результат проверки.

По истечении периода хранения сессия завершается. По новому запросу на соединение с сервером создается новая сессия.

Чтобы настроить срок хранения сессии в кеше:

## Через GPO

1. Откройте редактор GPO.
2. Откройте раздел Конфигурация компьютера → Административные шаблоны → Indeed ID → Client Connection.
3. Включите политику Настройки подключения к серверу.
4. В свойствах политики задайте нужное значение для параметра Период удержания объекта сессии (мс). Значение по умолчанию — 180000 мс (3 минуты).

## Через реестр

1. Откройте редактор реестра.
2. Откройте раздел Компьютер\HKEY\_LOCAL\_MACHINE\SOFTWARE\Indeed-ID\SrvLocator2.
3. Для параметра `SessionHoldPeriodMs` типа *DWORD* установите нужное значение. Значение по умолчанию — 180000 мс (3 минуты).

# Формат доменного имени для OWA

В IIS Extension не поддерживается настройка входа в OWA (Outlook Web Access) только по имени пользователя (*User name only*).

Для корректной работы IIS Extension записывайте доменное имя в следующих форматах:

- SAM: домен в виде NetBIOS — *indeed\user*;
- UPN: домен в виде DNS — *user@indeed.local*.

Если в редакторе реестра Windows включить нормализацию имен (*HKEY\_LOCAL\_MACHINE\SOFTWARE\Indeed-ID\IISHTTPModule*, параметр типа 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*.

# Indeed RDP Windows Logon

Модуль Indeed RDP Windows Logon (RDP Windows Logon) позволяет реализовать двухфакторную аутентификацию с помощью Indeed Access Manager в процессе подключения по протоколу RDP (Remote Desktop Protocol) или в приложении Remote App.

В качестве второго фактора могут выступать:

- push-уведомления с подтверждением входа в мобильном приложении Indeed Key,
- Email OTP,
- SMS OTP,
- Secured TOTP,
- Software OTP,
- Passcode,
- Hardware TOTP,
- Hardware OTP.

## Предварительная настройка

Чтобы использовать модуль RDP Windows Logon:

1. Включите NLA (Network Level Authentication) для пользователя.
2. При использовании соединения по протоколу HTTPS **установите клиентский сертификат** на каждый сервер Indeed.
3. **Установите и настройте** RDP Windows Logon.
4. **Настройте** выбор провайдера аутентификации на стороне пользователя.
5. При необходимости задайте **опциональные настройки**.

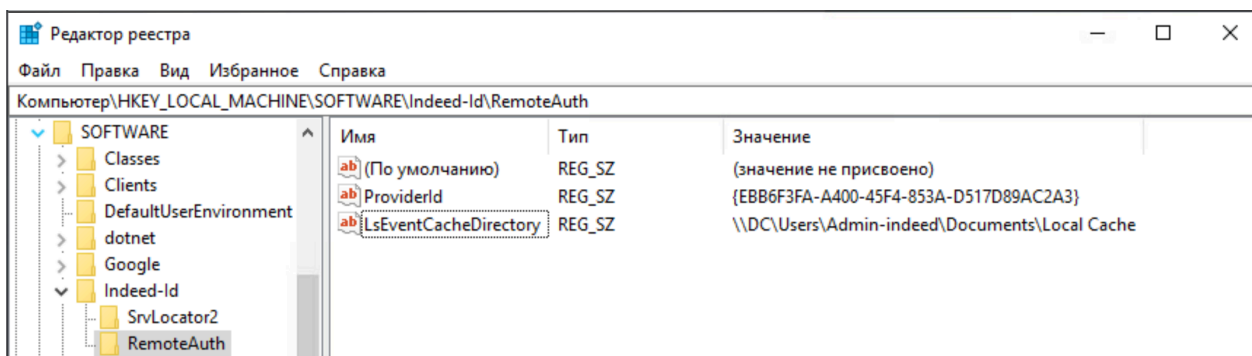
## Установить и настроить RDP Windows Logon

1. Запустите файл для установки, расположенный по пути *Indeed AM <номер версии>/Indeed AM RDP Windows Logon/<номер версии>*, и следуйте шагам мастера установки.
2. Откройте редактор реестра Windows.
3. В разделе *HKEY\_LOCAL\_MACHINE\SOFTWARE\Indeed-ID* создайте раздел RemoteAuth.

4. В разделе **RemoteAuth** создайте строковый параметр **ProviderId** и задайте значение, соответствующее используемому провайдеру.

▼ **Возможные значения** **ProviderId**

- SMS OTP {EBB6F3FA-A400-45F4-853A-D517D89AC2A3}
- Email OTP {093F612B-727E-44E7-9C95-095F07CBB94B}
- Passcode {F696F05D-5466-42b4-BF52-21BEE1CB9529}
- Software OTP {0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0}
- Secured TOTP {F15FD7EC-19EA-4384-846E-A2D0BE149FA2}
- Hardware OTP {AD3FBA95-AE99-4773-93A3-6530A29C7556}
- Hardware TOTP {CEB3FEAF-86ED-4A5A-BD3F-6A7B6E60CA05}
- Indeed Key (только в режиме push-уведомлений с подтверждением входа)  
{DEEF0CB8-AD2F-4B89-964A-B6C7ECA80C68}



5. В разделе *HKEY\_LOCAL\_MACHINE\SOFTWARE\Indeed-ID\SrvLocator2* измените следующие параметры:

- В параметре **ServerUrlBase** укажите URL вашего Core Server в формате *http(s)://полное\_dns\_имя\_сервера/am/core*.

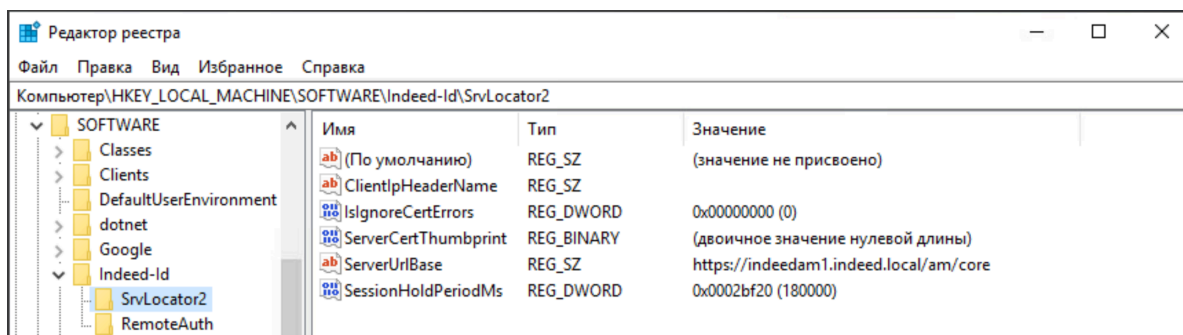


**ВАЖНО!**

В настройках приложения URL не должен содержать косую черту (/) в конце адреса.

- В параметре **IsIgnoreCertErrors** укажите значение *0* или *1*. Этот параметр предназначен для проверки сертификата Core Server, при значении *1* ошибки

сертификата игнорируются.

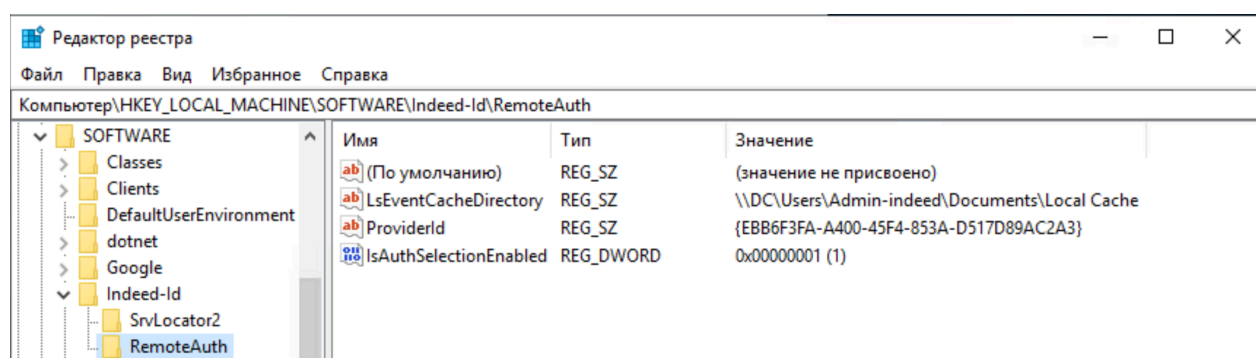


## Настроить выбор провайдера аутентификации для пользователя

1. В реестре Windows в разделе `HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\RemoteAuth` создайте параметр DWORD с именем `IsAuthSelectionEnabled`.
2. В значении параметра `IsAuthSelectionEnabled` укажите `1`.

Если параметр не задан или его значение равно `0`, то выбор провайдера аутентификации предоставляться не будет. В этом случае будут отображаться все доступные методы аутентификации.

Если `IsAuthSelectionEnabled=1` и указан провайдер в `ProviderId`, то при подключении пользователя будет выбран указанный провайдер. При этом пользователь сможет выбрать любой другой из числа поддерживаемых.

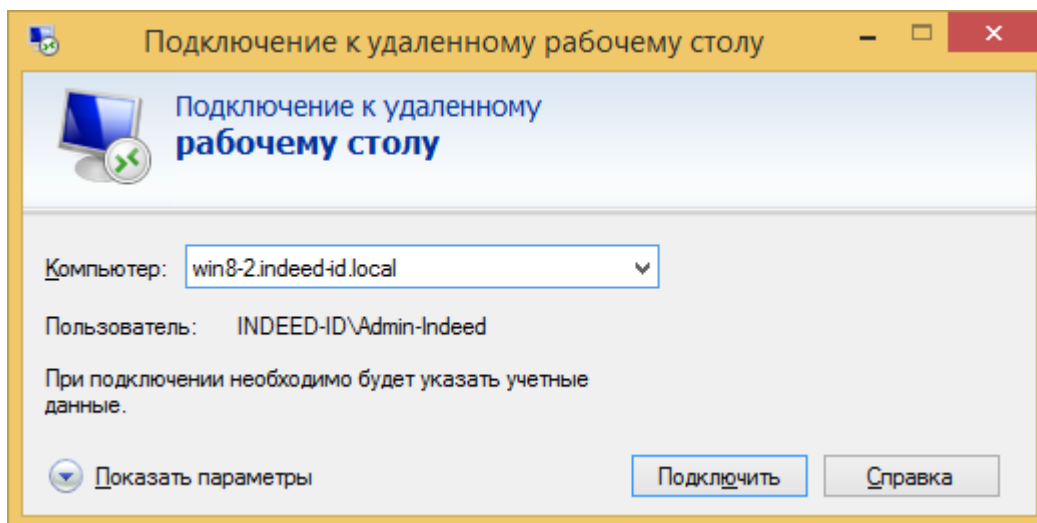


## Опциональные настройки

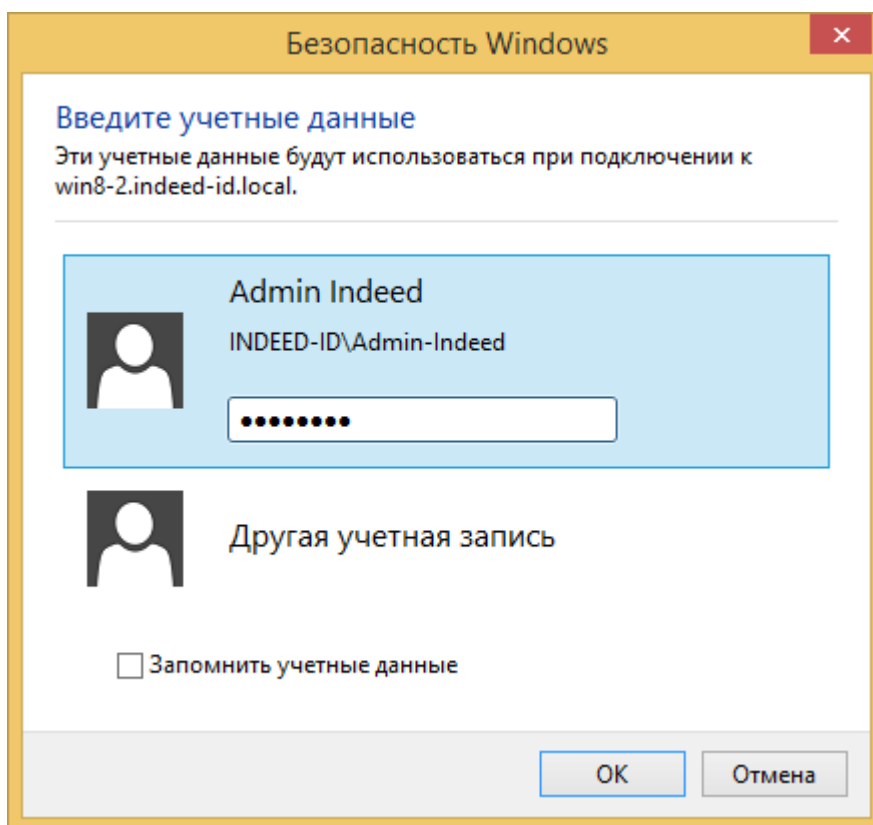
- Аутентификация пользователей **без лицензии**.
- Настройка срока **хранения сессии**.
- Одновременная работа с **Indeed Windows Logon**.

## Пример работы модуля

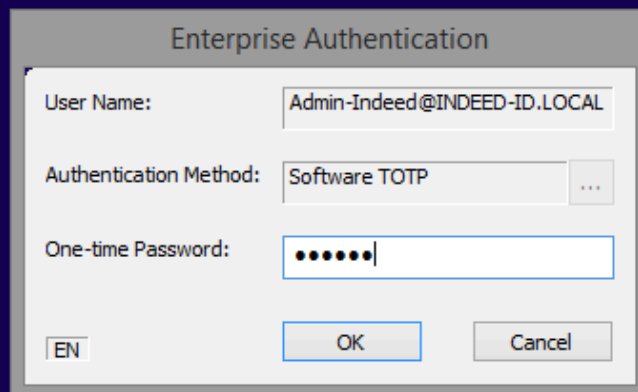
1. Подключитесь к машине, на которой установлен RDP Windows Logon.



2. Укажите пользователя и доменный пароль и нажмите ОК.



3. Введите одноразовый пароль.



The image shows a Windows-style dialog box titled "Enterprise Authentication". It contains three input fields: "User Name:" with the text "Admin-Indeed@INDEED-ID.LOCAL", "Authentication Method:" with a dropdown menu showing "Software TOTP" and a small "..." button to its right, and "One-time Password:" with a text box containing seven dots and a cursor. At the bottom left is a checkbox labeled "EN", and at the bottom right are "OK" and "Cancel" buttons.

**ⓘ ПРИМЕЧАНИЕ**

Если у пользователя нет доступных способов аутентификации, отображается сообщение *Нет доступных способов аутентификации. Доступ запрещен.* и сессия Remote Desktop завершается.

# Аутентификация пользователей без лицензии

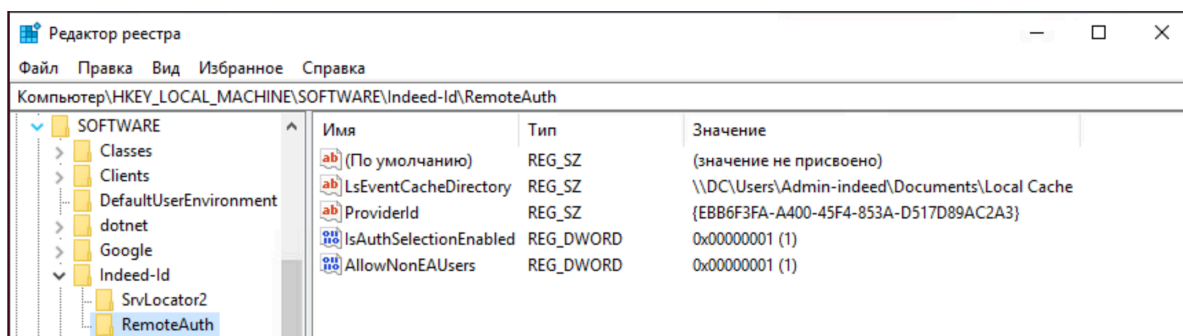
По умолчанию RDP Windows Logon работает с пользователями, обладающими лицензией *AM RDP Windows Logon*.

Тем не менее, можно настроить аутентификацию пользователей без лицензии. Для этого:

1. Откройте редактор реестра Windows.

2. В разделе `HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\RemoteAuth` создайте параметр `DWORD` с именем `AllowNonEAUsers`:

- Если значение параметра `AllowNonEAUsers` равно `1`, то пользователи без лицензии RDP Windows Logon смогут аутентифицироваться по доменному паролю (без использования технологии Indeed).
- Если значение параметра `AllowNonEAUsers` равно `0` или не задано, то аутентификация осуществляется только для пользователей с лицензией RDP Windows Logon. Пользователь без лицензии аутентифицироваться не сможет.





### ▼ Сценарии работы параметра

---

- Если пользователь находится вне пользовательского каталога Indeed — на пользователя действует настройка *AllowNonEAUsers*, пользователь не сможет аутентифицироваться, если значение параметра не равно 1.
- Если пользователь находится в пользовательском каталоге без лицензии, но в политике для пользователя нет приложения или пользователь не состоит в политике — на пользователя действует настройка *AllowNonEAUsers*, пользователи не смогут аутентифицироваться, если значение параметра не равно 1.
- Если пользователь находится в пользовательском каталоге без лицензии и в политике пользователя есть приложение — на пользователя не действует настройка *AllowNonEAUsers*. Всегда происходит попытка входа с автозахватом лицензии.

# Настройка срока хранения сессии

При кратковременных разрывах подключения к Core Sever можно настроить период, в течение которого сессию можно будет использовать повторно.

В течение заданного периода сессия хранится в кеше и может быть повторно использована при запросе на новое соединение с сервером. При этом проверка работоспособности сервера повторно не происходит, вместо этого используется закешированный результат проверки.

По истечении периода хранения сессия завершается. По новому запросу на соединение с сервером создается новая сессия.

Чтобы настроить срок хранения сессии в кеше:

## Через GPO

1. Откройте редактор GPO.
2. Откройте раздел Конфигурация компьютера → Административные шаблоны → Indeed ID → Client Connection.
3. Включите политику Настройки подключения к серверу.
4. В свойствах политики задайте нужное значение для параметра Период удержания объекта сессии (мс). Значение по умолчанию — 180000 мс (3 минуты).

## Через реестр

1. Откройте редактор реестра.
2. Откройте раздел Компьютер\HKEY\_LOCAL\_MACHINE\SOFTWARE\Indeed-ID\SrvLocator2.
3. Для параметра `SessionHoldPeriodMs` типа *DWORD* установите нужное значение. Значение по умолчанию — 180000 мс (3 минуты).

# Одновременная работа с Indeed Windows Logon

Если модули Windows Logon и RDP Windows Logon установлены на одном устройстве, настройте политику для **Windows Logon**.

## Через GPO

1. Перейдите на устройство, на котором установлены модули RDP Windows Logon и Windows Logon.
2. Откройте редактор GPO.
3. Откройте раздел Конфигурация компьютера → Административные шаблоны → Indeed ID → Windows Logon.
4. Включите политику Настройки Credential Provider.
5. Для параметра Отображение способов входа выберите значение Все, кроме пароля.

## Через реестр

1. Перейдите на устройство, на котором установлены модули RDP Windows Logon и Windows Logon.
2. Откройте редактор реестра.
3. Откройте раздел Компьютер\HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Indeed-ID\Logon for Windows.
4. Создайте параметр типа *DWORD* с именем **CredProvFilter** и установите ему значение 2.

# Indeed NPS RADIUS Extension

Indeed NPS RADIUS Extension (RADIUS Extension) — это модуль расширения Microsoft Network Policy Server (NPS, входит в состав Windows Server), который позволяет реализовать технологию двухфакторной аутентификации для RADIUS-совместимых сервисов и приложений.

В RADIUS Extension вы можете выполнить аутентификацию по следующим аутентификаторам:

- **Indeed Key**,
- **Telegram Provider**,
- **Email OTP**,
- **SMS OTP**,
- **Storage SMS OTP**,
- **Secured TOTP**,
- **Software OTP**,
- **Passcode**,
- **Hardware TOTP**,
- **Hardware OTP**,
- **MFA**.

## ИНФОРМАЦИЯ

С помощью Indeed Key реализуется двухфакторная аутентификация: первым фактором выступает Windows Password, вторым — push-уведомления с подтверждением входа в мобильном приложении Indeed Key.

В зависимости от версии Access Manager аутентификатор может называться как *Indeed Key*, так и *2FA: Windows Password + Indeed Key (Push)*.

Чтобы настроить модуль RADIUS Extension:

1. **Установите и настройте** Network Policy Server (NPS).
2. **Установите и настройте** RADIUS Extension.
3. **Зарегистрируйте лицензию модуля** в Management Console.
4. **Установите и настройте** провайдеры аутентификации.
5. Интегрируйте бизнес-приложение с NPS Radius Extension.

### ▼ Примеры интеграции бизнес-приложений

---

- Cisco ASA
- FortiGate VM
- Citrix Netscaler
- S-Crypto VPN
- C-Терра VPN
- КриптоПро NGate

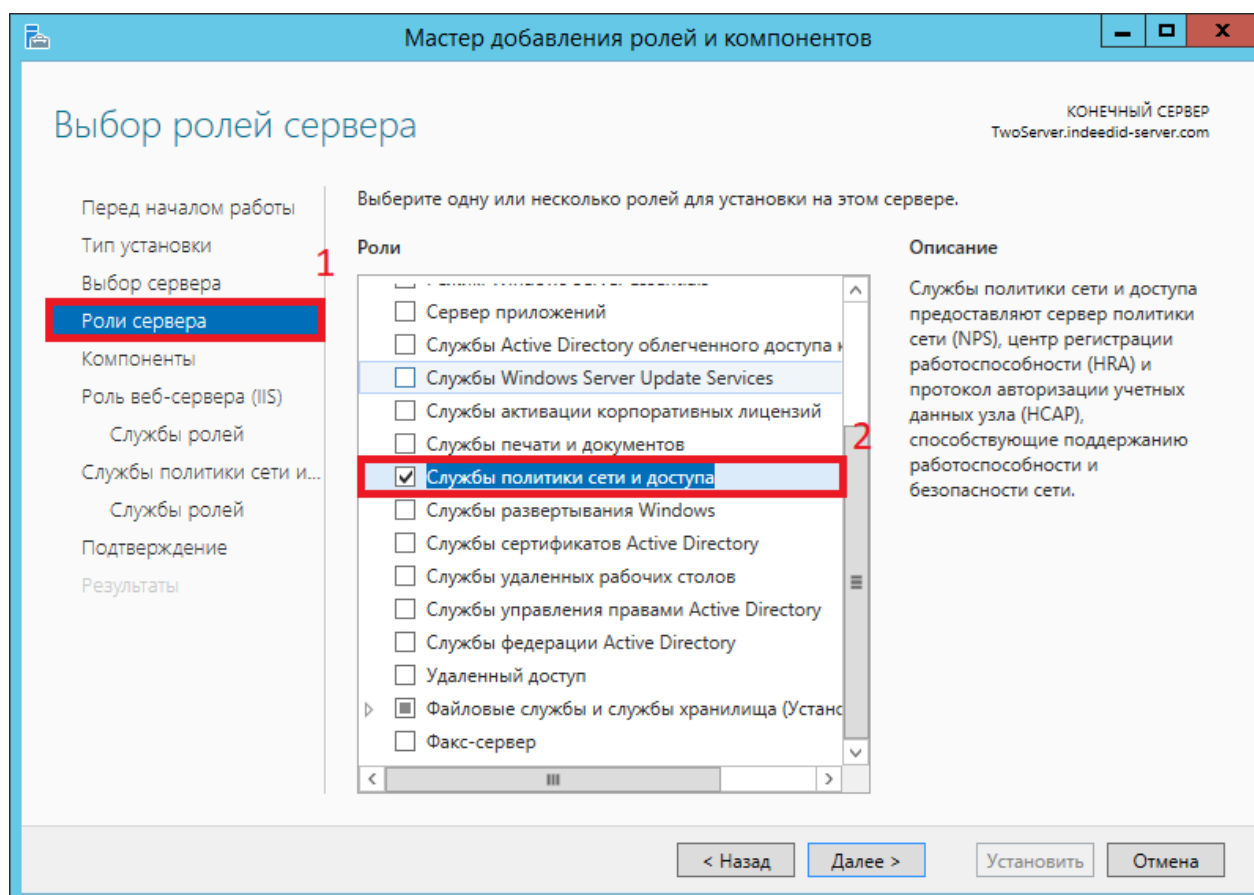
6. **Добавьте и настройте** интегрированное приложение в Management Console.
7. При необходимости задайте **дополнительные настройки**.

# Установка и настройка NPS

Indeed NPS RADIUS Extension (RADIUS Extension) — это модуль расширения Microsoft Network Policy Server (NPS, входит в состав Windows Server). Поэтому, прежде чем приступить к **установке RADIUS Extension**, обязательно установите и настройте NPS. В противном случае расширение работать не будет.

## Установить NPS

1. Откройте диспетчер серверов.
2. В правом верхнем углу нажмите Управление → Добавить роли и компоненты
3. В мастере добавления ролей и компонентов на вкладке Тип установки выберите Установка ролей и компонентов.
4. На вкладке Выбор сервера выберите сервер для установки.
5. На вкладке Роли сервера выберите роль Службы политики сети и доступа (Network Policy and Access Services), согласитесь с установкой дополнительных компонентов.



6. Пройдите шаги мастера до вкладки Подтверждение установки компонентов, оставляя настройки по умолчанию.
7. Нажмите Установить.

## Настроить NPS

### Добавить RADIUS-клиент

1. Запустите Сервер сетевых политик.
2. Раскройте раздел RADIUS-клиенты и серверы.
3. Нажмите правой кнопкой мыши RADIUS-клиенты и выберите Новый документ.
4. В окне Новый RADIUS-клиент задайте настройки клиента:
  - В поле Понятное имя введите произвольное понятное имя.
  - В поле Адрес (IP или DNS) введите адрес сервера клиентского компонента.
  - В разделе Общий секрет задайте секретный ключ для соединения.



#### ПРИМЕЧАНИЕ

Укажите общий секрет, который был задан при настройке клиентского компонента. Если подключение со стороны клиента еще не было настроено, задайте произвольный секрет и запомните его. Данный ключ потребуется при настройке подключения клиентского компонента.

Новый RADIUS-клиент

Параметры Дополнительно

☒ Включить этот RADIUS-клиент

☐ Выберите существующий шаблон:

Имя и адрес

Имя (или имя хоста): VPNServer

Адрес (IP или DNS): 192.168.0.7 Проверить...

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: .....

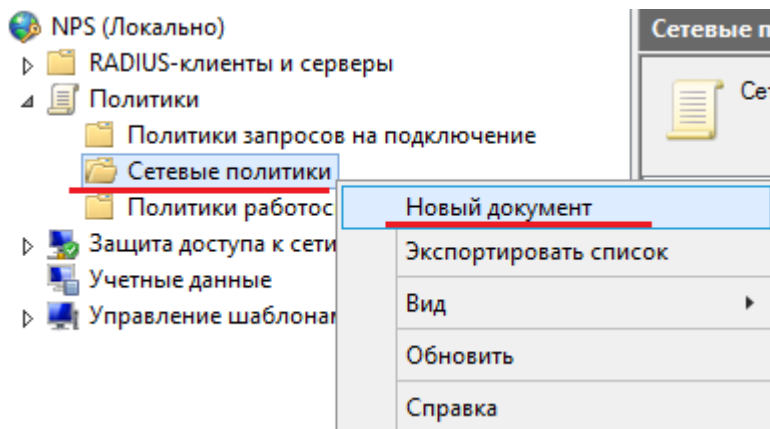
OK Отмена

5. Нажмите ОК.

## Добавить сетевую политику

1. Запустите Сервер сетевых политик.
2. Раскройте раздел Политики.
3. Нажмите правой кнопкой мыши Сетевые политики и выберите Новый документ.





4. В поле Имя политики укажите произвольное имя 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 условия, которые будут проверяться при подключении клиентов. Для этого нажмите кнопку Добавить... и выберите подходящее условие. После добавления условия нажмите Далее.

 **ПРИМЕЧАНИЕ**

В качестве примера будет добавлено условие *Группы пользователей*. При добавлении группы потребуется указать имя группы пользователей из Active Directory.

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 выбранных 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 выберите методы проверки подлинности, которые настроены на клиенте, и нажмите Далее.



**ВАЖНО!**

Методы проверки подлинности со стороны сервера Radius и клиента должны совпадать, в противном случае возникнет ошибка аутентификации.



## 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](#)

### ПРИМЕЧАНИЕ

Если вы используете проверки подлинности MS-CHAP (Challenge Handshake Authentication Protocol), в параметрах учетной записи пользователя в Active Directory включите опцию Хранить пароль, используя обратимое шифрование и обновите пароль пользователя.

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.

# Установка и настройка RADIUS Extension

После **установки и настройки NPS**, установите и настройте RADIUS Extension. Для этого:

1. Запустите *IndeedID.EA.RADIUS.Extension-<номер версии>.x64.ru-ru.msi*, расположенный по пути *Indeed AM <номер версии>\Indeed AM NPS RADIUS Extension\<номер версии>*.
2. Настройте RADIUS Extension с помощью реестра или групповых политик.

## Через реестр

1. Откройте редактор реестра.
  2. В разделе *HKEY\_LOCAL\_MACHINE\SOFTWARE\Indeed-ID\SrvLocator2* измените следующие параметры:
- В строковом параметре **ServerUrlBase** укажите адрес Core Server в формате *https://полное\_dns\_имя\_сервера/am/core/*.

### ПРИМЕЧАНИЕ

Для корректной работы рекомендуем установить клиентский сертификат на каждый Core Server.

- В числовом параметре **IsIgnoreCertErrors** укажите значение *0* или *1*.

Данный параметр предназначен для игнорирования ошибок сертификата проверки подлинности Core Server. При значении *1* ошибки сертификата игнорируются.

- При необходимости в числовом параметре **SessionHoldPeriodMs** можно задать период удержания сессии. Это период, в течение которого сессию можно использовать повторно при кратковременных разрывах подключения к Core Server. В течение заданного периода сессия хранится в кеше и может быть повторно использована при запросе на новое соединение с сервером. При этом проверка работоспособности сервера повторно не происходит, вместо этого используется закешированный результат проверки. По истечении периода сессия завершается. По новому запросу на

соединение с сервером создается новая сессия. Значение параметра по умолчанию — 180000 секунд (3 минуты).

#### Через политики

1. **Добавьте шаблоны групповых политик.**
2. Откройте редактор GPO.
3. Перейдите в раздел Конфигурация компьютера → Административные шаблоны → Indeed ID → Client Connection.
4. Откройте свойства политики Настройки подключения к серверу.
5. Включите политику.
6. В поле URL-адрес АМ сервера введите адрес Core Server в формате *https://  
полное\_dns\_имя\_сервера/am/core/*.
7. При необходимости включите опцию Игнорировать ошибки сертификата.
8. Для настройки Период удержания объекта сессии оставьте значение по умолчанию — 180000 секунд (3 минуты) — или задайте новое.
9. Нажмите ОК.

Подробнее о настройках RADIUS Extension с помощью политик и реестра — в разделе **RADIUS Extension**.

## Настройка доступа к недобавленным приложениям

Если приложения работают через NPS (Network Policy Server) с установленным RADIUS Extension, но аутентификация для них будет осуществляться не через Access Manager, настройте для них доступ в Management Console. В противном случае вход в эти приложения будет невозможен.

Чтобы настроить доступ для RADIUS-приложений, не добавленных в Access Manager:

1. На боковой панели Management Console откройте раздел Конфигурация.
2. На вкладке Модули интеграции выберите NPS RADIUS Extension.
3. Разрешите или запретите доступ в настройке Для RADIUS приложений, которые не зарегистрированы в Access Manager.

# Добавление и настройка интегрированного приложения

В Management Console вы можете:

- **добавить приложение**, интегрированное через RADIUS Extension;
- **выбрать способ входа** для интегрированных приложений;
- **настроить атрибуты** для поиска повторных запросов на аутентификацию и выполнить прочие опциональные настройки.

## Опциональные настройки

### ▼ Настроить передачу атрибутов Radius

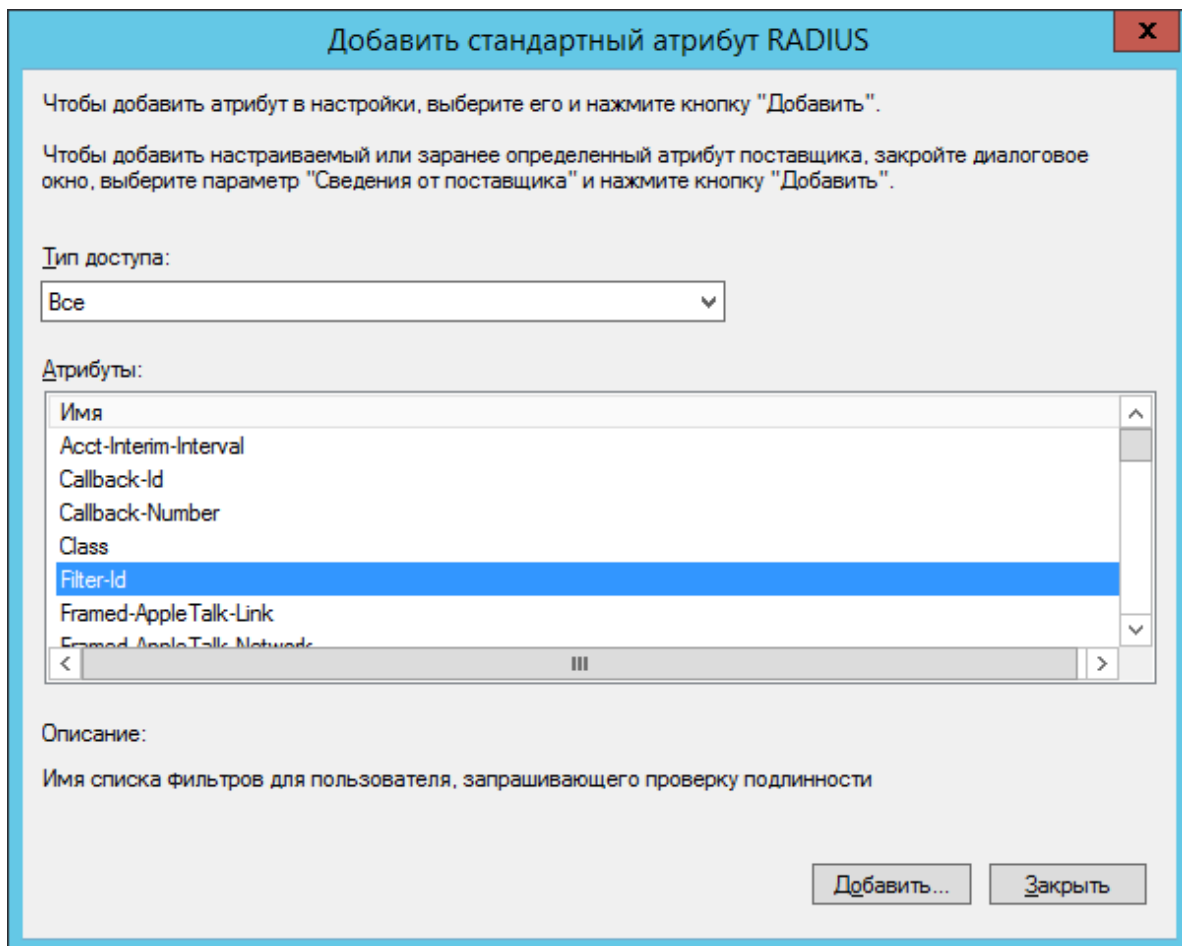
---

Данная настройка позволяет добавить атрибуты в ответ `Access-Accept` (Доступ принят), которые указаны в сетевой политике сервера NPS.

Это необязательная настройка, выполняется только при необходимости передачи атрибутов Radius для клиента.

Чтобы настроить передачу атрибутов Radius:

1. Откройте Сервер сетевых политик.
2. Раскройте раздел Политики → Политики запросов на подключение.
3. Выберите существующую политику или создайте новую и откройте ее свойства.
4. На вкладке Параметры перейдите в раздел Атрибуты RADIUS → Стандарт.
5. Нажмите Добавить.
6. В окне Добавить стандартный атрибут RADIUS в списке Атрибуты выберите Filter-Id и нажмите Добавить.



7. В окне Сведения об атрибуте нажмите Добавить.
8. Убедитесь, что параметр Формат ввода атрибута — строковый, и введите строку формата `IID_CR_AccessAccept_Attributes:<идентификатор требуемого атрибута 1>`, `<идентификатор требуемого атрибута 1>`

#### ПОДСКАЗКА

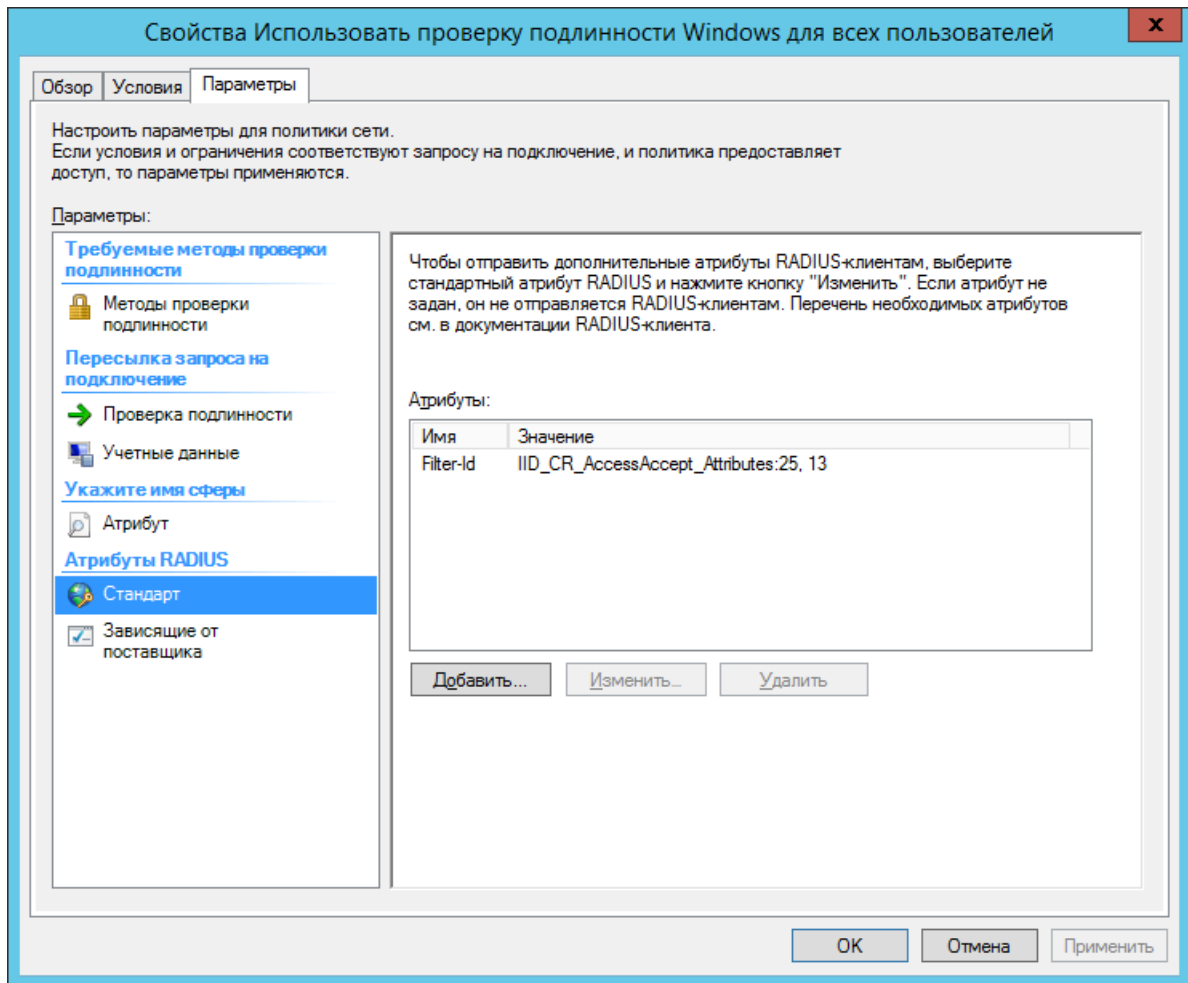
Если атрибутов несколько, укажите идентификаторы через запятую.

Пример

```
IID_CR_AccessAccept_Attributes:25, 13
```

9. Закройте все окна, нажмите Применить и перезапустите службу NPS.





## ▼ Настроить параметры доступа в политиках на NPS

---

В политике на сервере NPS можно задать следующие параметры:

- общий способ входа;
- способы входа для групп пользователей.

Это необязательная настройка.

Чтобы настроить параметры доступа:

1. Запустите Сервер сетевых политик.
2. Перейдите в раздел Политики → Политики запросов на подключение.
3. Создайте новую политику или используйте существующую и перейдите в ее свойства.
4. На вкладке Параметры перейдите в раздел Атрибуты RADIUS → Стандарт.
5. Нажмите Добавить.
6. В окне Добавить стандартный атрибут RADIUS в списке Атрибуты выберите Filter-Id и нажмите Добавить.
7. В окне Сведения об атрибуте нажмите Добавить.
8. Убедитесь, что параметр Формат ввода атрибута строковый, и введите соответствующие значения.

### Общий способ входа

Если настроить общий способ входа, те пользователи, на которых не распространяется действие параметра Настройка способов входа для групп пользователей, будут использовать заданный провайдер аутентификации в RADIUS-приложениях.

Чтобы настроить общий способ входа, введите значение формата IID\_ModelId\_{ProviderId}, где **ProviderId** — идентификатор провайдера.

Значение **ProviderId** уникально для каждого провайдера.

▼ **Значения идентификаторов провайдеров, поддерживающих RADIUS-аутентификацию**

---

- {0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0} — Software TOTP,
- {B772829C-4076-482B-B9BD-53B55EA1A302} — Software TOTP (Challenge\Response),
- {F696F05D-5466-42b4-BF52-21BEE1CB9529} — Passcode,
- {EBB6F3FA-A400-45F4-853A-D517D89AC2A3} — SMS OTP,
- {CA4645CC-5896-485E-A6CA-011FCC20DF1D} — Telegram,
- {093F612B-727E-44E7-9C95-095F07CBB94B} — Email OTP,
- {AD3FBA95-AE99-4773-93A3-6530A29C7556} — Hardware OTP,
- {AD3FBA95-AE99-4773-93A3-6530A29C7556} — Hardware OTP (Challenge\Response),
- {CEB3FEAF-86ED-4A5A-BD3F-6A7B6E60CA05} — Hardware TOTP,
- {D338344E-7AB7-4D82-9B53-C3678662B153} — Hardware TOTP (Challenge\Response),
- {DEEF0CB8-AD2F-4B89-964A-B6C7ECA80C68} — IndeedKey,
- {CB3D3B0A-29C6-4BA4-939D-09B126C10C2E} — Passcode + Software TOTP (Challenge\Response),
- {E5D3185C-9A13-4538-BE8F-D4E1C50A329E} — Passcode + IndeedKey,
- {F15FD7EC-19EA-4384-846E-A2D0BE149FA2} — Secured TOTP,
- {7F3DE86F-59D1-4476-AA5D-F277E5DD5938} — Secured TOTP (Challenge\Response),
- {882C1787-FD32-44A2-BA89-F1F529FBE7AB} — Passcode + Secured TOTP (Challenge\Response),
- {4E32199B-9A21-4CD7-8646-C70C48B55ED9} — Passcode + SMS OTP (Challenge\Response).

**ⓘ ПРИМЕЧАНИЕ**

Challenge\Response (Вызов\Ответ) — способ аутентификации, когда одна сторона отправляет запрос («вызов»), а другая должна предоставить верный «ответ» для успешной аутентификации.

#### Пример значения атрибута с Indeed AM Software OTP Provider

`IID_ModeId_{B772829C-4076-482B-B9BD-53B55EA1A302}`

#### Для групп пользователей

Если настроить способ входа для группы пользователей Active Directory, то пользователи этой группы будут использовать заданный провайдер для аутентификации в RADIUS-приложениях.

Чтобы настроить способы входа для групп пользователей, введите значение формата `IID_Group_ModeId_{DN}_{ProviderId}`, где:

- `DN` — уникальное имя группы в Active Directory (Distinguished Name). Если нужно задать несколько групп, укажите значения через запятую.
- `ProviderId` — идентификатор провайдера.

Значение `ProviderId` уникально для каждого провайдера.

▼ **Значения идентификаторов провайдеров, поддерживающих RADIUS-аутентификацию**

---

- {0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0} — Software TOTP,
- {B772829C-4076-482B-B9BD-53B55EA1A302} — Software TOTP (Challenge\Response),
- {F696F05D-5466-42b4-BF52-21BEE1CB9529} — Passcode,
- {EBB6F3FA-A400-45F4-853A-D517D89AC2A3} — SMS OTP,
- {CA4645CC-5896-485E-A6CA-011FCC20DF1D} — Telegram,
- {093F612B-727E-44E7-9C95-095F07CBB94B} — Email OTP,
- {AD3FBA95-AE99-4773-93A3-6530A29C7556} — Hardware OTP,
- {AD3FBA95-AE99-4773-93A3-6530A29C7556} — Hardware OTP (Challenge\Response),
- {CEB3FEAF-86ED-4A5A-BD3F-6A7B6E60CA05} — Hardware TOTP,
- {D338344E-7AB7-4D82-9B53-C3678662B153} — Hardware TOTP (Challenge\Response),
- {DEEF0CB8-AD2F-4B89-964A-B6C7ECA80C68} — IndeedKey,
- {CB3D3B0A-29C6-4BA4-939D-09B126C10C2E} — Passcode + Software TOTP (Challenge\Response),
- {E5D3185C-9A13-4538-BE8F-D4E1C50A329E} — Passcode + IndeedKey,
- {F15FD7EC-19EA-4384-846E-A2D0BE149FA2} — Secured TOTP,
- {7F3DE86F-59D1-4476-AA5D-F277E5DD5938} — Secured TOTP (Challenge\Response),
- {882C1787-FD32-44A2-BA89-F1F529FBE7AB} — Passcode + Secured TOTP (Challenge\Response),
- {4E32199B-9A21-4CD7-8646-C70C48B55ED9} — Passcode + SMS OTP (Challenge\Response).

**ⓘ ПРИМЕЧАНИЕ**

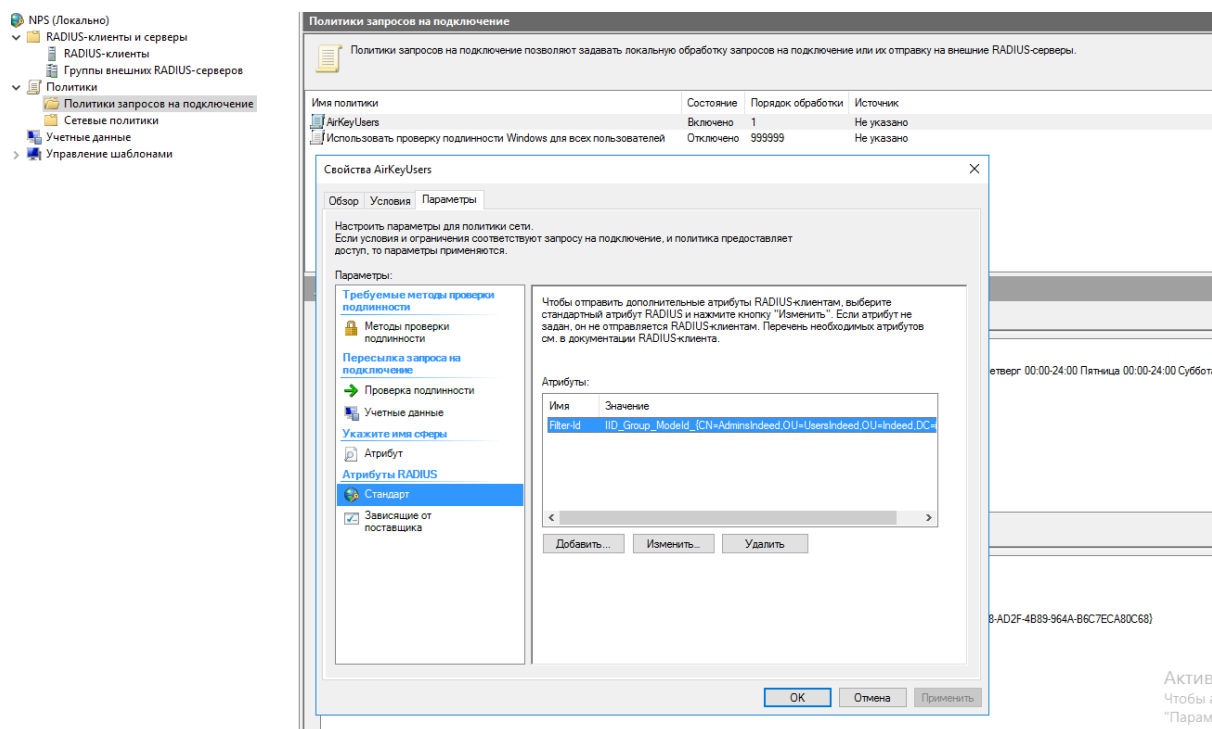
Challenge\Response (Вызов\Ответ) — способ аутентификации, когда одна сторона отправляет запрос («вызов»), а другая должна предоставить верный «ответ» для успешной аутентификации.

## ❗ ПРИМЕЧАНИЕ

Если в названиях групп Active Directory используются кириллические символы, установите на каждом сервере политик сети (NPS) русский язык как язык для программ, не поддерживающих Unicode. Без данной настройки членам таких групп будет отказано в аутентификации сервером политик сети.

### Пример значения атрибута с Indeed Key Provider

`IID_Group_ModeId_{CN=AdminsIndeed,OU=UsersIndeed,OU=Indeed,DC=indee  
AD2F-4B89-964A-B6C7ECA80C68}`



9. Нажмите Применить, чтобы сохранить внесенные в политику изменения.

10. Перезапустите службу NPS.

# Indeed Mobile Device Provisioning

Когда пользователь настраивает почтовый аккаунт на новом устройстве через Exchange ActiveSync, устройство автоматически попадает в карантин. Чтобы начать получать почту, необходимо вывести устройство из карантина. Сделать это можно с помощью модуля Indeed Mobile Device Provisioning (MDP).

## Системные требования

Чтобы настроить модуль Indeed Mobile Device Provisioning:

1. **Создайте и настройте** сервисную учетную запись для взаимодействия MDP и Active Directory.
2. **Установите модуль** с помощью MSI-пакета.
3. **Зарегистрируйте лицензию модуля** в Management Console.
4. **Выполните настройки** в Internet Information Services (IIS).
5. **Отредактируйте** конфигурационный файл модуля.
6. **Настройте аутентификацию** через Identity Provider.
7. **Настройте отображение вкладки** в User Console.
8. При необходимости **включите логирование**.

## Создать и настроить сервисную учетную запись

Модуль Indeed Mobile Device Provisioning будет обращаться к Active Directory через сервисную учетную запись, чтобы сформировать список устройств в карантине. От имени этой учетной записи происходит поиск по электронному адресу пользователя.

Чтобы настроить сервисную учетную запись:

1. В Active Directory создайте сервисную учетную запись.

## ▼ Пример

Свойства: Mail Admin

Член групп Входящие звонки Среда Сеансы Удаленное управление

Профиль служб удаленных рабочих столов COM+

Общие Адрес Учетная запись Профиль Телефоны Организация

Имя входа пользователя:  
mail.admin @company.local

Имя входа пользователя (пред-Windows 2000):  
COMPANY\ mail.admin

Время входа... Вход на...

2. Откройте панель управления Exchange (ECP).
3. В разделе Разрешения на вкладке Роли администраторов нажмите **+**, чтобы создать новую группу ролей.
4. В открывшемся окне задайте следующие настройки:
  - В поле Имя введите название группы.
  - В разделе Роли добавьте:
    - *Mail Recipients* — роль для получения данных по устройствам.
    - *Mailbox Search* — роль для получения электронного адреса. Если этой роли не будет, то под сервисной учетной записью можно будет получить только свой электронный адрес.
    - *Organization Client Access* — роль для предоставления доступа к устройству и для блокировки.
  - В разделе Участники добавьте созданную ранее сервисную учетную запись.



▼ **Пример**

Группа ролей - Google Chrome

exchange.company.local/ecp/UsersGroups/EditAdminRoleGroup.aspx?Activity...

## Service Exchange

\*Имя:

Service Exchange

Описание:

Область записи:

☒ По умолчанию

Подразделение:

Роли:

+ -

ИМЯ

Mail Recipients

Mailbox Search

Organization Client Access

Участники:

+ -

| ИМЯ        | ОТОБРАЖАЕМОЕ ИМЯ |
|------------|------------------|
| Mail Admin | Mail Admin       |

Сохранить

Отмена

5. Нажмите Сохранить.

## Установить модуль

Запустите *IndeedAM.MobileDevProv-v8.2.2.x64.ru-ru.msi*, расположенный по пути *indeed AM <номер версии>/Indeed AM Mobile Device Provisioning/<номер версии>*.

По завершении установки будет предложено сгенерировать новый сертификат IDP. Сертификат необходим для аутентификации через Identity Provider.

## Настройки в Internet Information Services

После установки выполните следующие настройки в Internet Information Services:

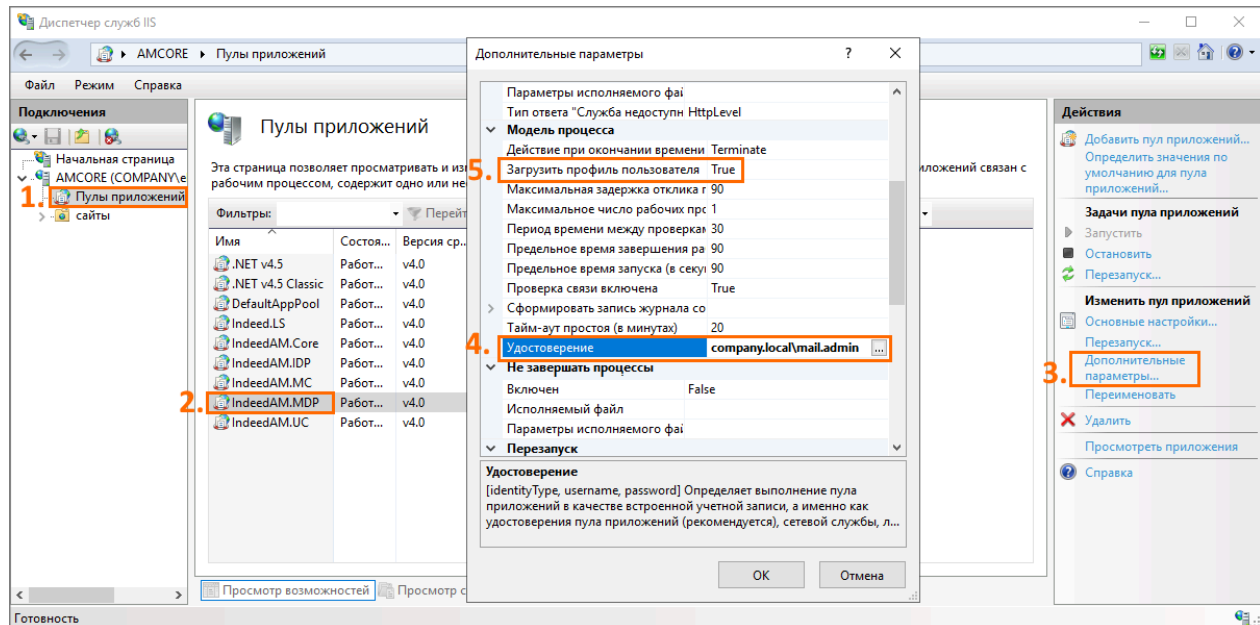
- **добавьте сервисную учетную запись** в удостоверение пула приложений;
- **измените версию** среды CLR.

### Добавить сервисную учетную запись

Чтобы добавить сервисную учетную запись в пул приложений, выполните следующее:

1. Откройте Диспетчер служб IIS.
2. В левом меню Подключения разверните узел, соответствующий вашему серверу Indeed Access Manager.
3. Выберите Пулы приложений.
4. В списке выберите *IndeedAM.MDP*. В открывшемся справа меню выберите Изменить пул приложений→Дополнительные параметры.
5. В открывшемся окне Дополнительные параметры в разделе Модель процесса выберите Удостоверение и нажмите .
6. В открывшемся окне Удостоверение пула приложений выберите Особая учетная запись и введите имя пользователя и пароль для созданной сервисной записи Active Directory.
7. Нажмите ОК. Окно Удостоверение пула приложений закроется.
8. В окне Дополнительные параметры в разделе Модель процесса выберите Загрузить профиль пользователя и в выпадающем списке выберите значение *True*.
9. Сохраните изменения.

## ▼ Пример

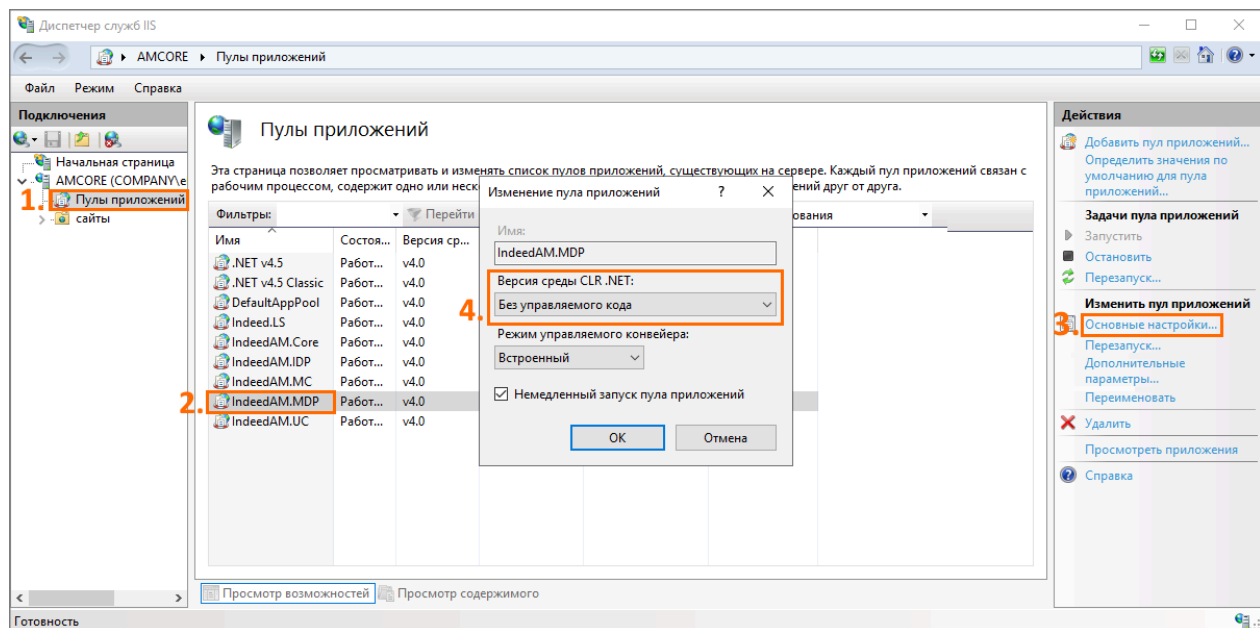


## Изменить версию среды CLR

Чтобы изменить версию среды CLR:

1. Откройте Диспетчер служб IIS.
2. В левом меню Подключения разверните узел, соответствующий вашему серверу Indeed Access Manager.
3. Выберите Пулы приложений.
4. В списке выберите *IndeedAM.MDP*. В открывшемся справа меню выберите Изменить пул приложений→Основные настройки.
5. В открывшемся окне Изменение пула приложений в выпадающем списке Версия среды CLR.NET выберите Без управляемого кода и нажмите ОК.

## Пример



## Настроить конфигурацию модуля

В конфигурационном файле MDP `C:\inetpub\wwwroot\am\mdp\app-settings.json` внесите изменения:

1. В разделе `Exchange` в параметре `ServerUrl` укажите адрес подключения к удаленному серверу PowerShell Exchange в формате `https://полное_dns_имя_сервера/Powershell`.

### Пример

```
"Exchange": {  
  "ServerUrl": "https://exchange.indeed-test.com/Powershell"
```

## ▼ Проверка в панели управления Exchange (ECP)

В панели управления Exchange откройте раздел Серверы и перейдите на вкладку Виртуальные каталоги. В свойствах PowerShell (Default Web Site) убедитесь, что указанный в конфигурационном файле адрес совпадает с внутренним URL-адресом.

PowerShell (Default Web Site)

► **общие**

проверка подлинности

Сервер: EXCHANGE

Время последнего изменения: 04.03.2025 18:04

**Внутренний URL-адрес:** https://indeed-test.com/powershell

Внешний URL-адрес: https://indeed-test.com/powershell

2. В разделе **Server** в параметре **Url** укажите адрес Log Server в формате *https://  
полное\_dns\_имя\_сервера/ls/api/*.

Пример

```
"Server": {  
  "Url": "https://amcore.indeed-test.com/ls/api/"
```

3. В разделе **SAML** настройте подключение к Identity Provider:

- в секции **LocalServiceProviderConfiguration** в параметре **Thumbprint** укажите отпечаток сертификата MDP;

Чтобы получить отпечаток сертификата с помощью запроса PowerShell, используйте команду:

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

- в секции **PartnerIdentityProviderConfigurations**:
  - в параметре **SingleSignOnServiceUrl** укажите адрес Single SignOn Service в формате *https://полное\_имя\_сервера/am/idp/Account/SsoService*;
  - в **SingleLogoutServiceUrl** укажите адрес Single Logout Service в формате *https://полное\_имя\_сервера/am/idp/Account/SloService*;
  - в **Thumbprint** укажите отпечаток сертификата **сертификат Identity Provider**.

Чтобы получить отпечаток сертификата с помощью запроса PowerShell, используйте команду:

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

### ▼ Пример

```
"SAML": {
  "$schema": "https://www.componentsspace.com/schemas/saml-
config-schema-v1.0.json",
  "Configurations": [
    {
      "LocalServiceProviderConfiguration": {
        "AssertionConsumerServiceUrl":
"Account/AssertionConsumerService",
        "LocalCertificates": [
          {
            "Thumbprint":
"3FD40F59795C9F5977E33E18FCE2D5BB27FDC65C"
          }
        ]
      },
      "PartnerIdentityProviderConfigurations": [
        {
          "Name": "urn:indeedid:saml_idp",
          "SingleSignOnServiceUrl": "https://amcore.indeed-
test.com/am/idp/Account/SsoService",
          "SingleLogoutServiceUrl": "https://amcore.indeed-
test.com/am/idp/Account/SLOService",
          "PartnerCertificates": [
            {
              "Thumbprint":
"D520DC2E6BEDB1400526842CA88485FFB2F8D757"
            }
          ]
        }
      ]
    }
  ]
}
```

## Настроить аутентификацию через Identity Provider

Для Indeed Mobile Device Provisioning предусмотрена двухфакторная аутентификация через Identity Provider. Если пользователь прошел аутентификацию в User Console, он автоматически проходит аутентификацию в модуль.



## Как установить и настроить Identity Provider

Чтобы настроить аутентификацию в MDP:

1. Откройте конфигурационный файл Identity Provider *C:\inetpub\wwwroot\am\idp\app-settings.json*.
2. Внесите следующие изменения:

- В секции `CustomAttributes` в параметре `ServiceProvider` укажите urn сервиса MDP и атрибуты пользователя из AD, например:

```
"CustomAttributes": [  
  {  
    "ServiceProvider": "urn:indeedid:mobiledeviceprovisioning",  
    "Attributes": [  
      {  
        "Name": "user_name",  
        "UserNameFormat": "PrincipalName"  
      }  
    ]  
  }  
]
```

- В разделе `SAML` в секцию `PartnerServiceProviderConfigurations` добавьте блок:

```
{  
  "Name": "urn:indeedid:mobiledeviceprovisioning",  
  "SingleLogoutServiceUrl": "https://  
полное_dns_имя_сервера/am/mdp/Account/SLOService",  
  "PartnerCertificates": [  
    {  
      "Thumbprint": "3FD40F59795C9F5977E33E18FCE2D5BB27FDC65C"  
    }  
  ]  
},
```

где:

- в параметре `SingleSignOnServiceUrl` укажите адрес модуля MDP в формате *https://полное\_dns\_имя\_сервера/am/mdp/Account/SLOService*;

- в параметре `PartnerCertificates` укажите отпечаток сертификата MDP, сгенерированный при установке модуля.

Чтобы получить отпечаток сертификата с помощью запроса PowerShell, используйте команду:

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

▼ **Пример**

```

"SAML": {
  "$schema": "https://www.componentspace.com/schemas/saml-
config-schema-v1.0.json",
  "Configurations": [
    {
      "LocalIdentityProviderConfiguration": {
        "Name": "urn:indeedid:saml_idp",
        "SingleSignOnServiceUrl": "https://amcore.indeed-
test.com/am/idp/Account/SsoService",
        "LocalCertificates": [
          {
            "Thumbprint":
"D520DC2E6BEDB1400526842CA88485FFB2F8D757"
          }
        ]
      },
      "PartnerServiceProviderConfigurations": [
        {
          "Name": "urn:indeedid:selfservice",
          "SingleLogoutServiceUrl": "https://amcore.indeed-
test.com/am/uc/Account/SLOService",
          "PartnerCertificates": [
            {
              "Thumbprint":
"DE67FAABC02FC39BB640B99108918481A3C280EC"
            }
          ]
        },
        {
          "Name": "urn:indeedid:emc",
          "SingleLogoutServiceUrl": "https://amcore.indeed-
test.com/am/mc/Account/SLOService",
          "PartnerCertificates": [
            {
              "Thumbprint":
"17BE639E90FA69A5C0F9241E5B0BE6A826604D9C"
            }
          ]
        }
      ]
    }
  ]
}

```

```

    }
  ]
},
{
  "Name": "urn:indeedid:mobiledeviceprovisioning",
  "SingleLogoutServiceUrl": "https://amcore.indeed-
test.com/am/mdp/Account/SLOService",
  "PartnerCertificates": [
    {
      "Thumbprint":
"3FD40F59795C9F5977E33E18FCE2D5BB27FDC65C"
    }
  ]
},

```

## Настроить отображение модуля в User Console

Модуль представляет собой дополнительную вкладку в User Console — Мобильные устройства Exchange, — в которой пользователь может самостоятельно вывести устройство из карантина. По умолчанию модуль Indeed Mobile Device Provisioning не отображается отдельной вкладкой в User Console.

Чтобы настроить отображение модуля:

1. Откройте конфигурационный файл User Console *C:\inetpub\wwwroot\am\uc\Web.config*.

2. Внесите следующие изменения:

- В секцию `configSections` добавьте следующую строку, если ее нет:

```

section name="amMobileDeviceProvisioning"
type="IndeedID.Web.SelfService.Settings.MobileDeviceProvisioningSettin

```

- Найдите строку:

```
amMobileDeviceProvisioning isEnabled="false"  
url="MOBILE_DEVICE_PROVISIONING_URL/device/embed"
```

- в параметре `isEnabled` укажите значение *true*, чтобы настроить отображение вкладки в User Console;
- в параметре `url` укажите адрес сервера с установленным модулем Mobile Device Provisioning в формате *https://полное\_dns\_имя\_сервера/am/mdp/device/embed*.

## ▼ Пример

```
<configuration>
<configSections>
  <section name="amAuthServer"
type="IndeedID.Web.Shared.Utils.ConfigReader.AuthServerSettings,
IndeedID.Web.Shared, Version=1.0.0.0, Culture=neutral" />
  <section name="amCulture"
type="IndeedID.Web.Shared.Utils.ConfigReader.CultureHandler,
IndeedID.Web.Shared, Version=1.0.0.0, Culture=neutral" />
  <section name="amAuthentication"
type="IndeedID.Web.Shared.Utils.ConfigReader.AuthConfigReader" />
  <section name="amProviderImages"
type="IndeedID.Web.Shared.Utils.ConfigReader.ProviderImagesHandler,
IndeedID.Web.Shared, Version=1.0.0.0, Culture=neutral" />
  <section name="amApplicationSettings"
type="IndeedID.Web.Shared.Utils.ConfigReader.ApplicationSettingsHandle
  <section name="amMobileDeviceProvisioning"
type="IndeedID.Web.SelfService.Settings.MobileDeviceProvisioningSettin
</configSections>
<amAuthServer Url="https://amcore.company.com/am/core/" />
<amCulture isEnabled="true" />
<amProviderImages configSource="Config\providerImages.config" />
<amAuthentication mode="Saml" loginUrl="https://amcore.company.com/am/
identityProviderCertificateThumbprint="D520DC2E6BEDB1400526842CA88485F
serviceProviderCertificateThumbprint="DE67FAABC02FC39BB640B99108918481
enableLogout="true" />
<amApplicationSettings configSource="Config\applicationSettings.config
<amMobileDeviceProvisioning isEnabled="true" url="https://amcore.indee
test.com/am/mdp/device/embed" />
<appSettings>
```

### ВАЖНО!

Для аутентификации в модуль MDP используется Identity Provider. Если User Console и Identity Provider находятся на разных машинах и у них разные доменные имена, добавьте в конфигурационный файл Identity Provider *Web.config* в раздел `customHeaders` параметр `Content-Security-Policy`.

#### Пример

```
<customHeaders>
<add name="Content-Security-Policy" value="frame-ancestors 'self'
https://*.domain.local" />
</customHeaders>
```

## Настроить логирование

Как настроить сбор логов для модуля MDP, читайте в разделе [Сбор логов серверных компонентов](#).

В журнале событий Indeed AM отображаются следующие события работы модуля:

- пользователь успешно вывел мобильное устройство из карантина;
- не удалось вывести мобильное устройство из карантина;
- пользователь заблокировал мобильное устройство;
- не удалось заблокировать мобильное устройство.

Подробнее в разделе [События](#).



# Indeed Enterprise Single Sign-On

Indeed AM Enterprise Single Sign-On (ESSO, Enterprise SSO) реализует технологию единого доступа Single Sign On в информационные системы организации. Модуль централизованно хранит пароли пользователя и выполняет автоматическую подстановку пароля в скрытом виде при входе в приложение или других действиях, требующих аутентификации.

Автоматическое заполнение полей данными происходит после подтверждения личности пользователя с помощью аутентификатора. 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 любого компьютера, где установлен компонент.

## Технологии аутентификации

В Enterprise SSO вы можете выполнить аутентификацию по следующим аутентификаторам:

- **мобильное приложение Indeed Key** в режиме отправки одноразовых паролей и push-уведомлений с подтверждением входа,
- **Email OTP,**
- **MFA Provider,**
- **Secured TOTP,**
- **Storage SMS OTP,**
- **SMS OTP,**
- **Software OTP,**
- **Passcode,**
- **Hardware OTP,**
- **Hardware TOTP,**
- **Smart Card Provider,**
- **IronLogic Z2USB Provider,**
- **OMNIKEY Provider,**
- **Futronic Provider.**

## Поддерживаемые приложения

Технология доступа Indeed Enterprise Single Sign-On применяется для win- и веб-приложений и настраивается без программного вмешательства в серверную или клиентскую часть целевого приложения. Для поддержки нового приложения нужно **создать специальный шаблон** в формате XML. В шаблоне указывается, какие формы приложения будут контролироваться. Контроль доступа осуществляется в виде повторного запроса аутентификации, заполнении полей учетными данными, активации нужных элементов управления, записи события в журнал.

О том, как добавить и настроить поддерживаемые приложения в Management Console — в разделе **Модуль ESSO**.

### Часто задаваемые вопросы о работе Indeed Enterprise Single Sign-On

## Предварительная настройка

Чтобы использовать Enterprise SSO:

1. **Установите** модуль ESSO Agent на клиентской машине.
2. **Настройте** подключение к Core Server.
3. Для работы с веб-приложениями **настройте** расширение Indeed ESSO.
4. **Создайте** шаблон целевого приложения с помощью утилиты Indeed-Id ESSO Template Wizard.
5. **Добавьте и настройте** приложение в Management Console.

## Установить ESSO Agent



### ПРИМЕЧАНИЕ

Установить модуль нужно на компьютерах пользователей. Для этого требуются права локального администратора.

Чтобы установить ESSO Agent:

1. Запустите файл для установки *Indeed AM <номер версии>/Indeed AM ESSO Agent/<номер версии>/IndeedID.Enterprise SSO.Agent.msi* и следуйте указаниям Мастера установки.

2. После завершения установки модуля потребуется перезагрузка системы. Нажмите Да, чтобы выполнить перезагрузку сразу, или Нет, чтобы сделать это позднее вручную.

Чтобы установить ESSO Agent на компьютерах пользователей в автоматическом режиме, удобно использовать механизм групповых политик (Microsoft Group Policy) или любой другой инструмент, позволяющий массово распространять и устанавливать MSI-пакеты, например Microsoft System Center Configuration Manager.

Подробнее о способах распространения компонентов системы Indeed AM в автоматическом режиме — в [Руководстве по развертыванию системы](#).

## Настроить ESSO Agent

Настроить Enterprise SSO можно через редактор реестра или с помощью групповых политик.

При этом настройки через групповые политики будут приоритетнее настроек, заданных через реестр вручную. Посмотреть настройки групповых политик в реестре можно по пути `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\SrvLocator2`.

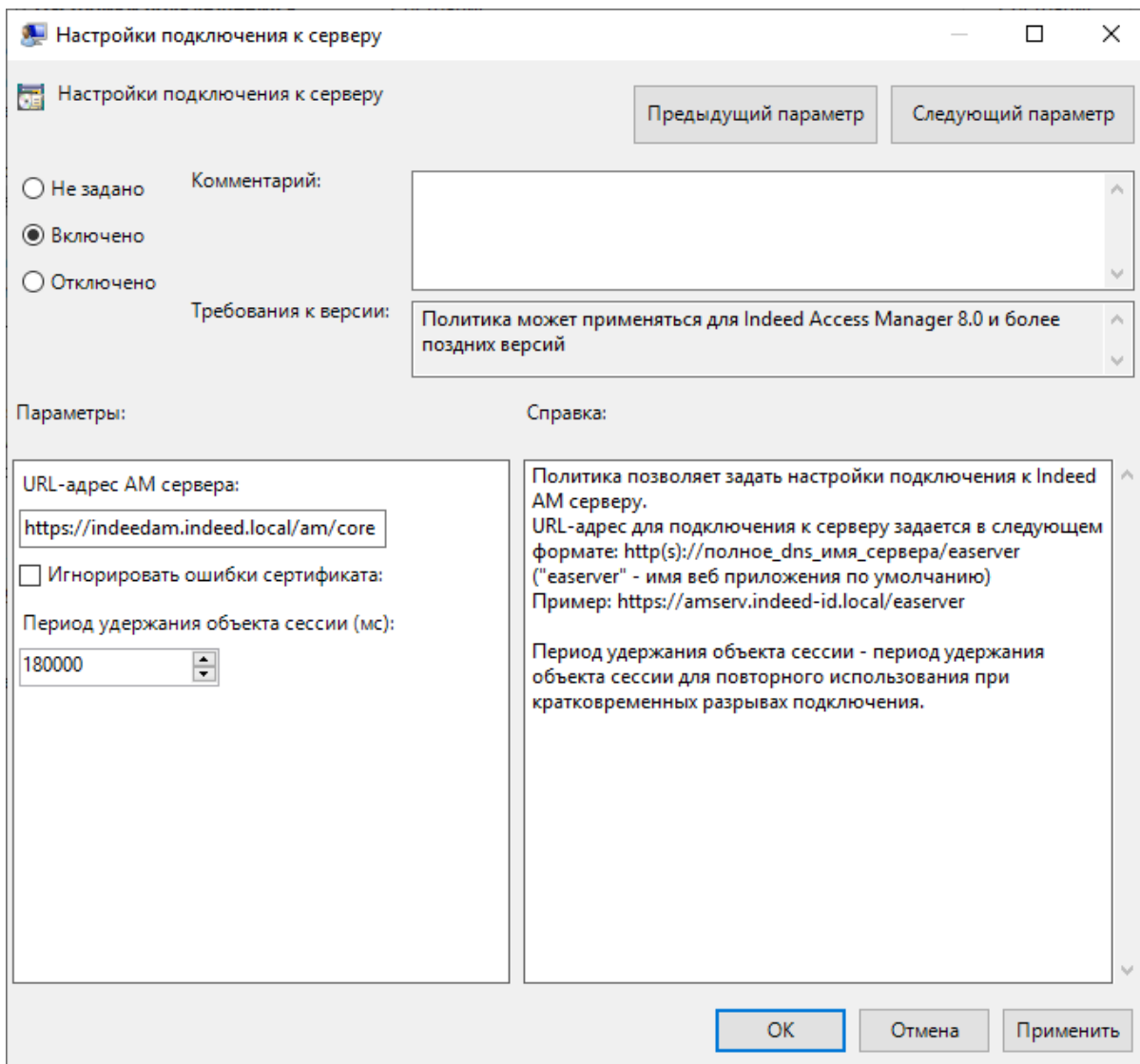
### Через реестр

1. Откройте редактор реестра Windows на компьютере пользователя.
2. Перейдите в раздел `HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\SrvLocator2`.
3. Откройте свойства строкового параметра `ServerUrlBase`.
4. В поле Значение укажите URL вашего Core Server в формате `http(s)://  
полное_dns_имя_сервера/am/core/`.

#### ⚠ ПРИМЕЧАНИЕ

При использовании соединения по протоколу HTTPS установите клиентский сертификат на каждый Core Server.

1. Добавьте политику *IndeedID.ServerUrl.admx* на компьютер с установленным ESSO Agent. Шаблоны групповых политик расположены в папке *Indeed AM <номер версии>\Misc\ADMX Templates*.
2. Откройте редактор GPO.
3. Откройте раздел Конфигурация компьютера → Административные шаблоны → Indeed ID → ClientConnection.
4. Включите политику Настройки подключения к серверу.
5. В поле URL-адрес AM сервера укажите адрес вашего Core Server в формате *http(s)://полное\_dns\_имя\_сервера/am/core/*.



## Настроить расширение Indeed ESSO

При работе с веб-приложениями ESSO использует расширение для браузеров Internet Explorer, Mozilla Firefox и Google Chrome. Для входа в веб-приложение достаточно перейти на страницу сервиса — плагин выполнит аутентификацию автоматически. Запускать ESSO и вручную выбирать приложение для прохождения SSO-аутентификации не требуется.

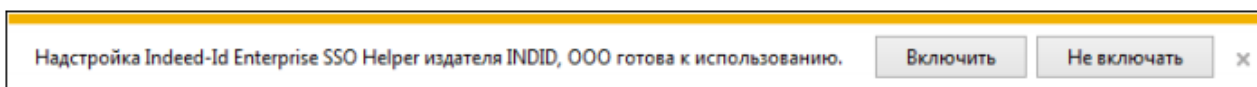
### Internet Explorer

Расширение Indeed AM SSO Helper для Internet Explorer устанавливается вместе с ESSO Agent. Для работы расширения включите его в браузере.

Если после установки расширение ESSO Agent не появилось в браузере, перейдите в Свойства браузера (Internet options)→Дополнительно (Advanced)→раздел Обзор (Browsing)

и включите опцию Разрешение сторонних расширений обозревателя (Enable third-party browser extensions).

Чтобы расширение заработало, включите его в браузере.



 **ПРИМЕЧАНИЕ**

На серверных операционных системах дополнительно 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 расширениями 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)*, чтобы расширение включалось автоматически включения.
2. Чтобы запретить пользователям выключать надстройки, 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 модулем ESSO Agent. Чтобы расширение заработало, включите его в браузере.

Чтобы установить расширение:

1. Перейдите в браузере в раздел Расширения.
2. В правом верхнем углу нажмите  и выберите Установить расширение из файла.

3. Перейдите в папку *C:/Program Files/Indeed-Id/Enterprise SSO/Mozilla FireFox Web Extention/Content/indeed\_id\_esso-vX.X.xpi* и нажмите Открыть.
4. После загрузки расширения нажмите Добавить.

Чтобы расширение заработало, включите его в браузере.



## Google Chrome

Расширение Indeed Id ESSO устанавливается в ручном или автоматическом режиме через механизм групповых политик Microsoft Windows.

При установке вручную из магазина Chrome необходимо загрузить и включить расширение для каждого пользователя компьютера.

Расширение, распространяемое групповыми политиками, устанавливается для всех пользователей компьютера. Для установки не требуется доступ в интернет.

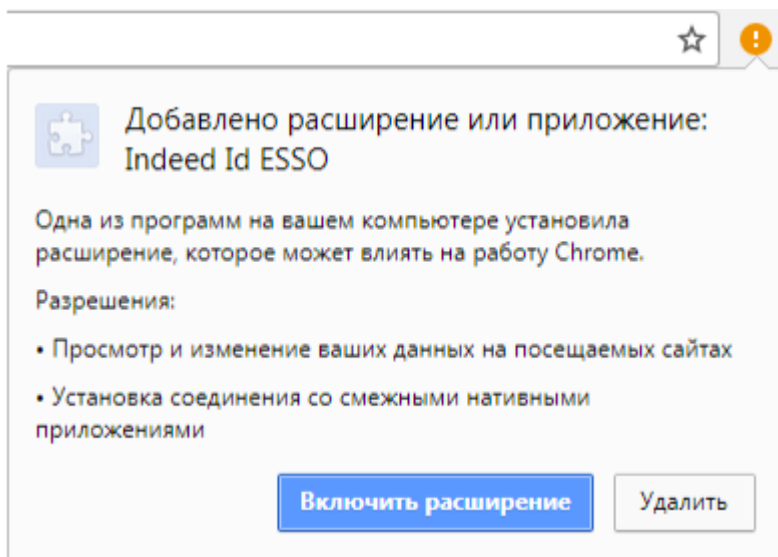
Чтобы установить расширение:

### Из магазина Chrome

1. Установите ESSO Agent на компьютер с доступом в интернет.
2. Запустите Google Chrome.

Расширение загрузится автоматически в течение 1 минуты. После загрузки расширения доступ к интернету не требуется.

Чтобы расширение заработало, включите его в браузере.



**! ПРИМЕЧАНИЕ**

Если расширение было удалено из браузера вручную, то для повторной установки загрузите его из интернет-магазина Chrome.

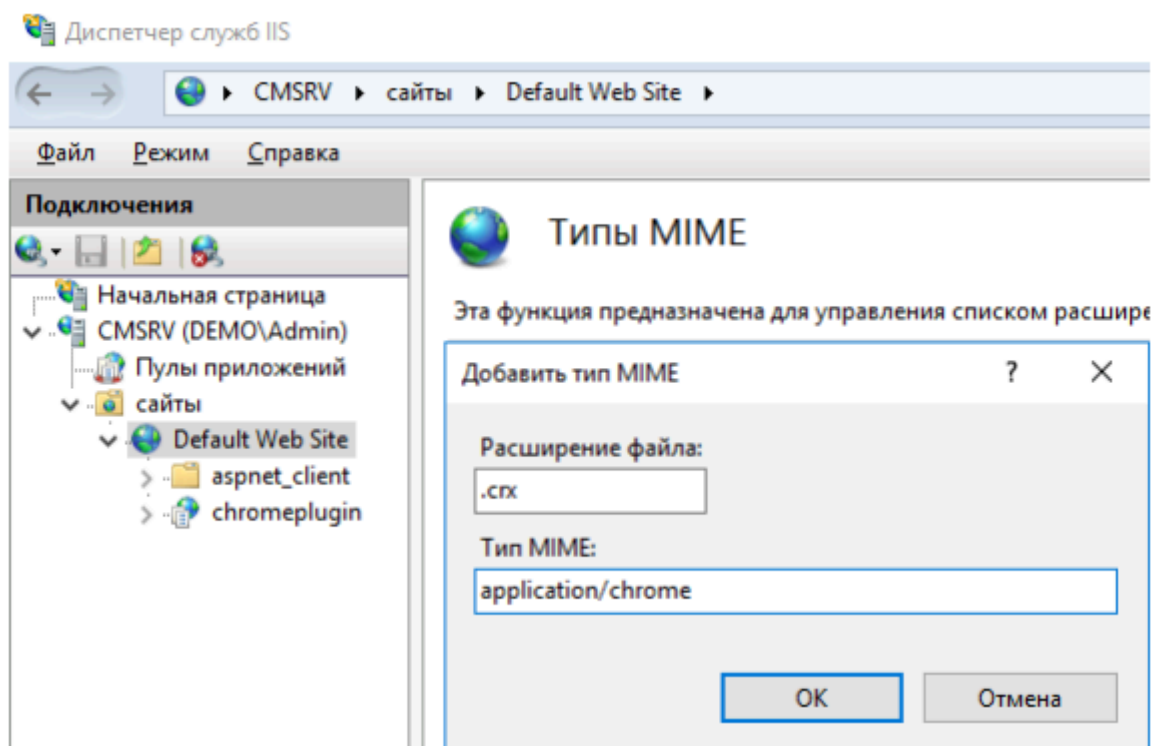
## Через GPO

1. Запустите диспетчер служб IIS (IIS Manager).
2. В области Подключения раскройте узел имя сервера → сайты → Default Web Site.
3. Нажмите правой кнопкой мыши Default Web Site и выберите Добавить приложение.
4. В открывшемся окне задайте следующие настройки:
  - В поле Псевдоним укажите произвольное имя приложения, например *chromeplugin*.
  - Для настройки Пул приложений выберите значение DefaultAppPool.
  - В поле Физический путь выберите каталог для приложения.
5. Нажмите ОК.
6. В настройках приложения откройте Проверка подлинности и включите Анонимную проверку подлинности (Anonymous Authentication).
7. В каталог приложения поместите файлы *lcjenjtmcehnkfkghcflkfialplejjkdj.crx* и *update.xml* из дистрибутива *Indeed AM <номер версии>\Indeed AM ESSO Agent\*



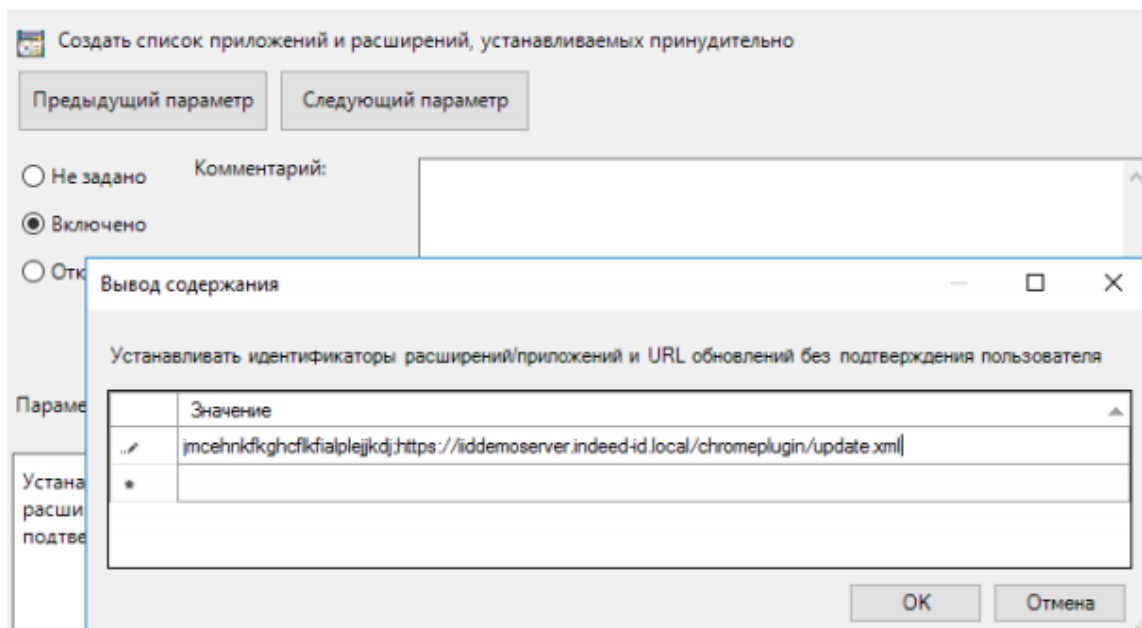
<номер версии>\Misc\Chrome.WebExt.

8. В диспетчере служб IIS перейдите на узел Default Web Site.
9. В разделе настроек Типы MIME (MIME Types) добавьте новый тип с расширением .CRX и описанием *application/chrome*.

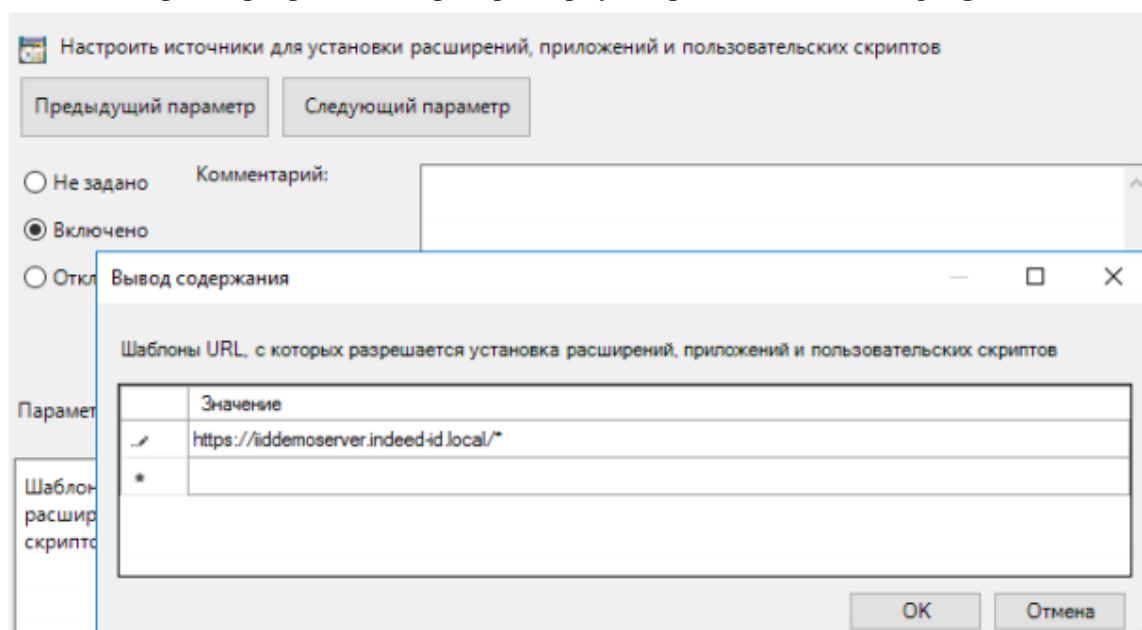


10. Настройте безопасное соединение по протоколу HTTPS для приложения *chromeplugin* и убедитесь, что к нему можно обратиться с компьютеров пользователей.
11. Добавьте шаблоны ADM/ADMX в локальное или центральное хранилище административных шаблонов контроллера домена.
12. Откройте Управление групповой политикой (Group Policy Management) и создайте новый объект групповой политики с произвольным именем.
13. Нажмите правой кнопкой мыши на созданный объект групповой политики и выберите Изменить.
14. В открывшемся окне перейдите в раздел Конфигурация компьютера (Computer Configuration)→Административные шаблоны (Administrative Templates)→Google→Google Chrome→Расширения (Extensions).

15. Включите политику *Создать список приложений и расширений, устанавливаемых принудительно* (*Configure the list of force-installed apps and extensions*).
16. В свойствах политики в разделе Параметры нажмите Показать.
17. В открывшемся окне укажите идентификатор расширения из имени файла CRX и путь к XML-файлу в каталоге *chromeplugin*.



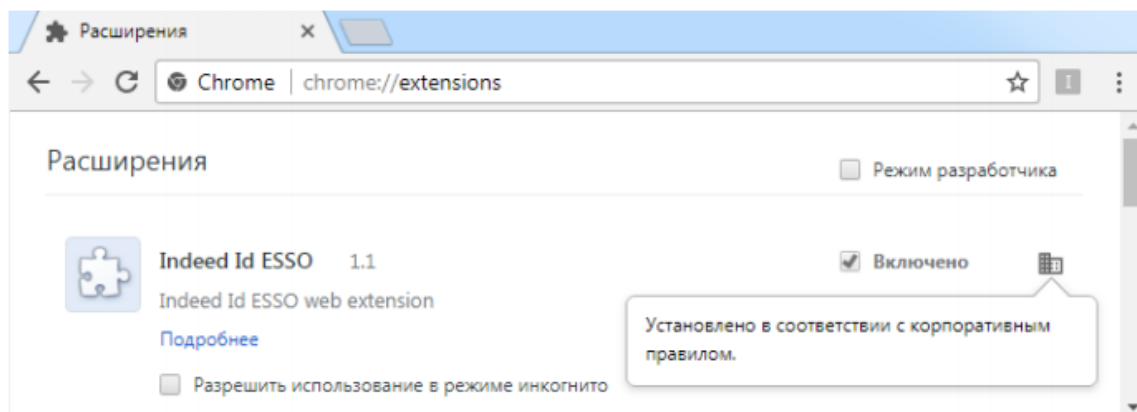
18. Включите политику *Настроить источники для установки расширений, приложений и пользовательских скриптов* (*Configure extension app, and user script install sources*).
19. Укажите адрес сервера, на котором развернуто приложение *chromeplugin*.



20. Добавьте компьютеры пользователей с установленным ESSO Agent в область действия объекта групповой политики.

Расширение автоматически загрузится и установится после применения групповой политики к компьютеру пользователя. Может потребоваться до нескольких минут для того, чтобы оно отобразилось в списке установленных в браузере.

Установленное через групповые политики расширение отмечено соответствующим символом.



# Создание шаблонов приложений

Для подготовки XML-шаблонов win32- и веб-приложений, интегрированных с модулем ESSO Agent, предназначена утилита Indeed-Id ESSO Template Wizard (Мастер шаблонов).

Утилита обрабатывает форму целевого приложения и формирует слепок формы. Это набор данных, описывающий элементы формы, например, имя заголовка, идентификаторы кнопок и полей ввода данных. На основе данных, содержащихся в шаблоне, ESSO Agent отследит запуск целевого приложения на рабочей станции пользователя и, в зависимости от настроек для конкретного пользователя, предоставит или не предоставит доступ.

## ПРИМЕЧАНИЕ

Полученный слепок является заготовкой для создания шаблона приложения. Поэтому после генерации слепка его нужно отредактировать вручную.

## Установить Indeed-Id ESSO Template Wizard

Установите Indeed-Id ESSO Template Wizard на рабочих станциях, где установлены приложения, для которых необходимо подготовить шаблон.

Для этого запустите файл *Indeed AM <номер версии>/Indeed AM Template Wizard/<номер версии>/IndeedID.ESSO.Template.Wizard.msi* и следуйте указаниям мастера установки.

После завершения установки компоненты Indeed-Id ESSO Template Wizard — Web Мастер шаблонов и Win32 Мастер шаблонов — появятся в разделе *Все программы* → *Indeed-Id* → *Enterprise SSO*.

## Собрать информацию о приложении

Прежде чем создавать шаблон приложения, соберите о нем следующую информацию:

1. Набор окон целевого приложения, которые будет обрабатывать ESSO-шаблон. При этом можно ориентироваться на основные операции, которые способен выполнять шаблон:
  - вход в приложение;
  - разблокировка;

- смена пароля в приложении.

В некоторых случаях пользовательский сценарий предполагает отказ от пароля — пользователь не знает свой пароль и использует аутентификатор или прозрачную аутентификацию для работы с целевым приложением. Тогда все окна, в которых пользователю предлагается ввести пароль для приложения, необходимо включить в список обрабатываемых окон. Помимо самих целевых окон важно обратить внимание на контролы (элементы управления интерфейсом), которые должны обрабатываться шаблоном.

2. Набор способов запуска приложения, например через ярлыки, командные или исполняемые файлы. Эта информация необходима для настройки быстрого запуска приложения.
3. Набор исполняемых файлов, создающих процессы, отображающие графический интерфейс приложения — окна, на которые должен реагировать ESSO Agent. Для каждого такого файла необходимо узнать имя, описание и расположение. Если у приложения только один исполняемый файл, то достаточно той информации, которую Мастер шаблонов соберет во время работы.

## Создать шаблон

Определив список необходимых окон и операций, можно приступить к созданию слепка или слепков шаблона. Для одного окна может потребоваться несколько слепков. Также в процессе отладки шаблона может потребоваться создать дополнительные слепки. Поэтому доступ к рабочей станции с установленным целевым приложением и Indeed-Id ESSO Template Wizard необходим на протяжении всего процесса создания шаблона.

### Для win32-приложений

1. Запустите приложение Enterprise SSO — Win 32 Мастер шаблонов.
2. Запустите целевое приложение, шаблон для которого нужно создать, и перейдите на его форму входа.
3. Нажмите комбинацию клавиш Ctr+Shift+T.
4. В мастере шаблонов откроется окно настроек генерации шаблона. Укажите в нем необходимые параметры.

## ▼ Настройки глубины контролов формы

---

- Глубина просмотра контролов формы.

С помощью данного параметра можно задать глубину вложенности элементов управления формы, на основе которой Мастер шаблонов построит шаблон.

Данный параметр задается вручную при создании шаблона. Если параметр равен 0, то Мастер шаблонов соберет информацию только о невложенных элементах управления. Если параметр равен 1, то Мастер шаблонов соберет данные о невложенных элементах управления и об элементах управления первого уровня вложенности и так далее.

- Глубина контролов выбранной формы.

Данный параметр отображает максимальную глубину вложенности элементов управления на выбранной форме — сколько уровней вложенности элементов управления существует на форме. При выборе значения параметра Глубина просмотра контролов формы рекомендуется ориентироваться на данный параметр. Значение глубины контролов для выбранной формы Мастер шаблонов вычисляет индивидуально для каждой формы в момент определения целевой формы приложения.

## ▼ Настройки формы целевого приложения

---

Данный набор настроек позволяет задать совокупность признаков формы приложения, которые будут учитываться Агентом ESSO при поиске целевого окна среди множества окон целевого приложения.

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Заголовок       | <p>При включении данной настройки значение заголовка формы будет учитываться в процессе отслеживания целевой формы целевого приложения. В шаблон будет добавлено фиксированное значение заголовка для сравнения.</p> <p>Если настройка выключена, значение заголовка формы при определении целевой формы приложения учитываться не будет.</p> <p>Рекомендуется использовать данный параметр в шаблоне, кроме случаев, когда заголовок динамически изменяется.</p>                                                                  |
| Имя класса окна | <p>При включении данной настройки в процессе отслеживания целевой формы целевого приложения будет учитываться имя класса окна для данной формы. Имя класса окна задается на этапе разработки приложения. В шаблон будет добавлено фиксированное значение имени класса окна для сравнения.</p> <p>Если настройка выключена, имя класса окна при определении целевой формы приложения учитываться не будет.</p> <p>Рекомендуется использовать данный параметр в шаблоне, кроме случаев, когда имя класса изменяется динамически.</p> |

|         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Размеры | <p>При включении данной настройки в процессе отслеживания целевой формы целевого приложения будут учитываться строго зафиксированные размеры окна — ширина и высота в пикселях. В шаблон будет добавлено фиксированное значение размеров формы для сравнения.</p> <p>Если настройка выключена, размеры окна при определении целевой формы приложения учитываться не будут.</p> <p>Использовать данный параметр следует только в тех случаях, когда остальные параметры не позволяют достаточно точно описать целевую форму приложения.</p> |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|



## ▼ Настройки контролов формы целевого приложения

Данный набор настроек позволяет задать совокупность признаков элементов управления, присутствующих в окне приложения, которые ESSO Agent будет учитывать при поиске целевого окна среди множества окон целевого приложения.

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CtrlId          | <p>Если данная настройка включена, в процессе отслеживания целевой формы целевого приложения будут учитываться идентификаторы всех контролов, которые входят в состав окна. Эти идентификаторы задаются на этапе разработки приложения. Значения всех идентификаторов элементов управления будут зафиксированы в шаблоне.</p> <p>Если настройка выключена, идентификаторы элементов управления при определении целевой формы приложения учитываться не будут.</p> <p>Рекомендуется использовать данный параметр, кроме случаев, когда идентификаторы контролов в целевой форме изменяется динамически.</p> |
| Имя класса окна | <p>Если данная настройка включена, в процессе отслеживания целевой формы целевого приложения будет учитываться имя класса окна для данной формы. Имя класса окна задается на этапе разработки приложения. В шаблон будет добавлено фиксированное значение имени класса окна для сравнения.</p> <p>Если настройка выключена, имя класса окна при определении целевой формы приложения учитываться не будет.</p> <p>Рекомендуется использовать данный параметр в шаблоне, кроме случаев, когда имя класса изменяется динамически.</p>                                                                        |

|         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Текст   | <p>Включение данной настройки позволяет учитывать текст, содержащийся в элементах управления в окне приложения (поля ввода, выпадающие списки и так далее), в процессе отслеживания целевой формы целевого приложения. Параметр учитывается для всех элементов управления, которые входят в состав окна. Значения всех текстовых строк для элементов управления будут зафиксированы в шаблоне.</p> <p>Если настройка выключена, текст элементов управления при определении целевой формы приложения учитываться не будет.</p> <p><b>ВАЖНО:</b></p> <p>При создании шаблона обращайте внимание на изменение текста элементов управления. При различных обстоятельствах — например, при смене языка в системе или в приложении, изменении версии приложения или смене пользователя — текст в элементе управления может измениться. Это может помешать процедуре отслеживания приложения. Не используйте динамически изменяющийся текст в шаблоне либо учитывайте все возможные варианты данного параметра.</p> |
| Размеры | <p>Если данная настройка включена, в процессе отслеживания целевой формы целевого приложения будут учитываться строго зафиксированные размеры всех элементов управления в окне — ширина и высота в пикселях. В шаблон будет добавлено фиксированное значение размеров для сравнения.</p> <p>Если настройка выключена, размеры элементов управления при определении целевой формы приложения учитываться не будут.</p> <p>Используйте данный параметр только в тех случаях, когда остальные параметры не позволяют достаточно точно описать свойства элементов управления целевой формы приложения.</p>                                                                                                                                                                                                                                                                                                                                                                                                       |

|         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Позиция | <p>Если данная настройка включена, в процессе отслеживания целевой формы целевого приложения будет учитываться строго зафиксированная позиция — позиция левого верхнего угла элемента управления относительно левого верхнего угла контейнера, содержащего этот элемент управления, в пикселях — для всех элементов управления в окне. В шаблон будет добавлено фиксированное значение позиции для сравнения.</p> <p>Если настройка выключена, позиция элементов управления при определении целевой формы приложения учитываться не будет.</p> <p>Используйте данный параметр только в тех случаях, когда остальные параметры не позволяют достаточно точно описать свойства элементов управления целевой формы приложения.</p> |
| Visible | <p>Если данная настройка включена, в процессе отслеживания целевой формы целевого приложения учитывается признак видимости — виден ли присутствующий в форме элемент управления для пользователя — всех элементов управления, которые входят в состав окна. Значения свойства видимости для элементов управления будут зафиксированы в шаблоне.</p> <p>Если настройка выключена, видимость элементов управления при определении целевой формы приложения учитываться не будет.</p>                                                                                                                                                                                                                                              |
| Enable  | <p>Если данная настройка включена, в процессе отслеживания целевой формы целевого приложения учитывается признак доступности — доступен ли элемент управления для действий пользователя — всех элементов управления, которые входят в состав окна. Значения свойства доступности для элементов управления будут зафиксированы в шаблоне.</p> <p>Если настройка выключена, доступность элементов управления при определении целевой формы приложения учитываться не будет.</p>                                                                                                                                                                                                                                                   |

## ▼ Настройки алгоритма заполнения

---

В данном разделе задается алгоритм заполнения, который будет использован в процессе подстановки имени пользователя и пароля в целевую форму приложения ESSO.

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Нет                  | Алгоритм заполнения не будет сгенерирован в шаблоне.<br>Автоматическое заполнение формы происходить не будет.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| На основе<br>SetText | После выбора данной настройки Мастер шаблонов сгенерирует команды заполнения поля ввода имени пользователя, заполнения поля ввода пароля и нажатия кнопки ОК. Каждая команда будет содержать данные элемента управления, к которому она должна быть применена. Заполнение элементов управления формы будет производиться стандартным методом SetText.<br><br>Рекомендуется использовать данный алгоритм заполнения.                                                                                                                                                                                                                                                                                           |
| Эмуляция<br>ввода    | Если выбрана эта настройка, Мастер шаблонов сгенерирует команды установки фокуса в поле ввода имени пользователя, заполнения поля ввода имени пользователя, заполнения поля ввода пароля, нажатия кнопки ОК, команды перехода между элементами управления и команды паузы. Само заполнение будет происходить с помощью эмуляции нажатия клавиш клавиатуры. Переход фокуса между элементами управления будет осуществляться эмуляцией нажатия клавиши Tab. В алгоритме заполнения также будут присутствовать команды паузы в 50 миллисекунд командами заполнения и перехода.<br><br>Рекомендуется к использованию в шаблонах для приложений, в которых использование метода SetText невозможно или затруднено. |

❗ **ПРИМЕЧАНИЕ**

При создании шаблона для конкретного приложения задавайте только тот набор настроек, который будет отличать это приложение от других. Перед генерацией шаблона важно понять, по каким признакам будет определяться форма входа в приложение, и какой алгоритм заполнения необходимо применить.

5. Нажмите Генерировать.

6. Откроется окно Определение контрола формы. Перейдите в окно целевого приложения на нужный контрол и нажмите Ctrl+Shift+T. Следуя подсказкам Мастера шаблонов, выполните эти действия для каждого выбранного элемента управления.

После определения контролов будет создан макет шаблона.

7. Включите опцию Сохранять в UTF–16 и нажмите Сохранить.

8. В открывшемся окне выберите место сохранения и укажите имя файла макета шаблона. Нажмите Сохранить.

Макет сохранится в формате XML.

9. В окне Мастера шаблонов нажмите Выход и закройте целевое приложение.

10. Откройте макет в редакторе Блокнот или другом текстовом редакторе, поддерживающем формат XML.

11. Проверьте путь к целевому приложению в разделе **paths**. При необходимости можно добавить дополнительный путь, по которому будет доступно приложение.

Пример

```
<paths>

<path>C:\Users\Admin\Desktop\TestApps\TestApp\TestAppWin\IndeedID.SSO.T
    <path>C:\Users\Admin\Desktop\IndeedID.SSO.Test.App.exe</path>
</paths>
```

12. В параметре `userDescription` укажите название целевого приложения. Именно это название пользователь будет видеть в окне ESSO Agent на своем устройстве.

Пример

```
<userDescription>Test.App.Win</userDescription>
```

13. В параметре `cmdLine` проверьте команду для быстрого запуска приложения. Это должен быть путь до исполняемого файла приложения.

Пример

```
<applicationDetails>  
  
<cmdLine>C:\Users\Admin\Desktop\IndeedID.SSO.Test.App.exe</cmdLine>  
</applicationDetails>
```

14. Если при генерации макета шаблона в качестве алгоритма заполнения была выбрана опция Эмуляция ввода, то проверьте, в каком поле изначально установлен курсор при запуске приложения и в какой последовательности он перемещается по остальным контролам. По результатам этого исследования, если нужно, отредактируйте алгоритм заполнения формы в шаблоне в разделе `fillingAlgorithm`.
15. Сохраните измененный файл шаблона с расширением .APP.

#### Для веб-приложений

1. Запустите Enterprise SSO — Web Мастер шаблонов.
2. Запустите целевое приложение в браузере Internet Explorer.
3. Находясь на целевой странице приложения нажмите Ctrl+Shift+T.

Откроется окно Мастера Определение особенностей формы.

Если комбинация клавиш Ctrl+Shift+T не работает, перейдите в Свойства браузера. В разделе Дополнительно (Advanced)→ Обзор (Browsing) проверьте включена ли опция Разрешение сторонних расширений обозревателя (Enable third-party browser extensions).

4. Перейдите на целевую страницу, выделите небольшой участок, на котором располагаются поля ввода имени пользователя, пароля, кнопки, и нажмите Ctrl+Shift+T.

В этот момент Мастер определяет узлы HTML DOM-дерева. По завершению операции число определенных узлов будет указано в нижней части окна Мастера в строке Определено узлов HTML DOM дерева страницы.



#### **ПРИМЕЧАНИЕ**

Этот шаг может занять некоторое время. Длительность работы Мастера зависит от количества объектов обрабатываемого участка веб-страницы. Не спешите закрывать страницу или окно Мастера.

5. После определения особенностей страницы нажмите Генерировать шаблон и укажите параметры генерации.

## ▼ Настройки формы целевого приложения

Данный набор настроек позволяет задать совокупность признаков веб-страницы приложения, которые ESSO Agent будет учитывать при поиске целевой страницы среди множества загруженных страниц браузера.

|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| URL<br>страницы       | <p>Если данная настройка включена, в процессе отслеживания отслеживания целевой веб-страницы приложения ESSO будет учитываться URL страницы. В шаблон будет добавлено фиксированное значение URL для сравнения.</p> <p>Если настройка выключена, URL при определении целевой веб-страницы учитываться не будет.</p> <p>Рекомендуется использовать данный параметр в шаблоне, кроме случаев, когда URL динамически изменяется. Для таких страниц либо откажитесь от использования данного параметра, либо используйте регулярное выражение.</p>                              |
| Заголовок<br>страницы | <p>Если данная настройка включена, в процессе отслеживания целевой веб-страницы приложения ESSO будет учитываться значение заголовка страницы. В шаблон будет добавлено фиксированное значение заголовка для сравнения.</p> <p>Если настройка выключена, значение заголовка при определении целевой веб-страницы учитываться не будет.</p> <p>Рекомендуется использовать данный параметр в шаблоне, кроме случаев, когда заголовок динамически изменяется. Для таких страниц либо откажитесь от использования данного параметра, либо используйте регулярное выражение.</p> |



## ▼ Настройки контролов формы целевого приложения

Данный набор настроек позволяет задать совокупность признаков веб-элементов управления, присутствующих на странице, которые ESSO Agent будет учитывать при поиске целевой страницы среди множества загруженных страниц браузера.

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Имя тега | <p>Если данная настройка включена, в процессе отслеживания целевой веб-страницы приложения ESSO будет учитываться имя тега для каждого веб-элемента, входящего в состав DOM-дерева фрагмента страницы, выделенного на этапе подготовки к генерации шаблона. В шаблон будет добавлено фиксированное значение имени тега для сравнения.</p> <p>Если настройка выключена, имя тега для веб-элементов при определении целевой формы приложения учитываться не будет.</p> <p>Рекомендуется использовать данный параметр в шаблоне, кроме случаев, когда имя тега изменяется динамически.</p>                                                                                                                                          |
| Текст    | <p>Если данная настройка включена, в процессе отслеживания целевой веб-страницы приложения ESSO будет учитываться текст для каждого веб-элемента, входящего в состав DOM-дерева фрагмента страницы, выделенного на этапе подготовки к генерации шаблона. В шаблон будет добавлено фиксированное значение текста для сравнения.</p> <p>Если настройка выключена, значение текстовой составляющей для веб-элементов при определении целевой формы приложения учитываться не будет.</p> <p>При использовании данного параметра рекомендуется проверить получившийся шаблон — массив текста в шаблоне может превышать ожидаемый, что приведет к проблеме с отслеживанием целевой веб-страницы и усложнит редактирование шаблона.</p> |

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Атрибут id      | <p>Если данная настройка включена, в процессе отслеживания целевой веб-страницы приложения ESSO будет учитываться значение атрибута id для каждого веб-элемента, входящего в состав DOM-дерева фрагмента страницы, выделенного на этапе подготовки к генерации шаблона. В шаблон будет добавлено фиксированное значение атрибутов id для сравнения.</p> <p>Если настройка выключена, значение атрибута id для веб-элементов при определении целевой формы приложения учитываться не будет.</p> <p>Рекомендуется к использованию.</p>                                                                                        |
| Атрибут name    | <p>Если данная настройка включена, в процессе отслеживания целевой веб-страницы приложения ESSO будет учитываться значение атрибута name для каждого веб-элемента, входящего в состав DOM-дерева фрагмента страницы, выделенного на этапе подготовки к генерации шаблона. В шаблон будет добавлено фиксированное значение атрибутов name для сравнения.</p> <p>Если настройка выключена, значение атрибута name для web-элементов при определении целевой формы приложения учитываться не будет.</p> <p>Рекомендуется к использованию.</p>                                                                                  |
| Другие атрибуты | <p>Если данная настройка включена, в процессе отслеживания целевой веб-страницы приложения ESSO будет учитываться набор значений для указанного списка атрибутов для каждого веб-элемента, входящего в состав DOM-дерева фрагмента страницы, выделенного на этапе подготовки к генерации шаблона. Атрибуты для отслеживания необходимо выбрать из раскрывающегося списка. Чтобы открыть список, нажмите .... В шаблон будут добавлены фиксированные значения указанных атрибутов для сравнения.</p> <p>Данный параметр рекомендуется использовать, когда остальные параметры не могут однозначно описать элемент формы.</p> |

|                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Стилевые атрибуты                           | <p>Если данная настройка включена, в процессе отслеживания целевой веб-страницы приложения ESSO будет учитываться набор значений для указанного списка стиливых атрибутов для каждого веб-элемента, входящего в состав DOM-дерева фрагмента страницы, выделенного на этапе подготовки к генерации шаблона. Стиливые атрибуты для отслеживания необходимо выбрать из раскрывающегося списка. Чтобы открыть список, нажмите .... В шаблон будут добавлены фиксированные значения указанных стиливых атрибутов для сравнения.</p> <p>Данный параметр рекомендуется использовать, когда остальные параметры не могут однозначно описать элемент формы.</p> |
| Если есть id, подставлять все остальное     | <p>Если у веб-элемента есть атрибут id, все другие атрибуты для данного элемента не будут использованы в шаблоне. Данную настройку можно применять, если атрибут id — основной параметр, по которому будет происходить определение целевой страницы.</p>                                                                                                                                                                                                                                                                                                                                                                                               |
| Использовать текст, только когда нет других | <p>Атрибут text будет использован, если никаких других указанных атрибутов для данного элемента не будет найдено. В противном случае, атрибут text не будет использован в шаблоне.</p> <p>Рекомендуется к использованию.</p>                                                                                                                                                                                                                                                                                                                                                                                                                           |

## ▼ Настройки алгоритма заполнения

В данном разделе производится выбор алгоритма заполнения, который будет использован в процессе подстановки имени пользователя и пароля в целевую веб-страницу приложения ESSO.

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Нет                      | Алгоритм заполнения не будет сгенерирован в шаблоне.<br>Автоматическое заполнение формы происходить не будет.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| На основе<br>fillWebCtrl | <p>Если выбрана данная настройка, Мастер шаблонов запросит у пользователя указать 3 контрола на веб-странице с помощью сочетания клавиш Ctrl+Shift+T и сгенерирует 3 команды в алгоритме заполнения для данных элементов:</p> <ul style="list-style-type: none"><li>• первая команда — заполнение веб-контрола значением логина пользователя;</li><li>• вторая команда — заполнение веб-контрола значением пароля учетной записи ESSO;</li><li>• третья команда — нажатие на кнопку ОК.</li></ul> <p>В каждой команде содержится данные об элементе на странице, с которым данная команда работает. Аналог алгоритма SetText для Win32 приложений.</p> |

### ⓘ ПРИМЕЧАНИЕ

При создании шаблона для конкретного приложения задайте только тот набор настроек, который будет отличать это приложение от других. Перед генерацией шаблона важно понять, какие контролы будут задействованы в определении формы входа веб-приложения.

6. Нажмите Генерировать.

Если при настройке генерации шаблона был задан алгоритм заполнения, откроется окно Определение контрола формы.

7. Перейдите на странице целевого приложения на нужный контрол и нажмите Ctrl+Shift+T. Следуя подсказкам Мастера шаблонов, выполните эти действия для каждого выбранного элемента управления.
8. Включите опцию Сохранять в UTF-16 и нажмите Сохранить.
9. В открывшемся окне выберите место сохранения и укажите имя файла макета шаблона. Нажмите Сохранить.
10. Макет сохранится в формате XML. В окне Мастера шаблонов нажмите Выход и закройте целевое приложение.
11. Откройте макет в редакторе Блокнот или другом текстовом редакторе, поддерживающем формат XML.
12. Если в начале файла есть следующая строка, удалите ее:

```
<?xml version="1.0" encoding="UTF-16"?>
```

13. Проверьте адрес целевого приложения в параметре `url`.

#### Пример

```
<componentWeb>  
  <url>https://amcore.indeed.com/TestAppWeb/logon.html</url>  
</componentWeb>
```

Значение адреса может быть задано в виде текста или регулярного выражения. Если адрес целевого приложения динамически меняется, используйте регулярное выражение. В этом случае параметр `url` должен содержать использовать атрибут `isRegex` со значением `1`. При значении `0` адрес приложения определяется текстом.

#### Пример регулярного выражения

```
<componentWeb>
  <url
isRegex="1">https:\\\\amcore\\.indeed\\.com\\TestAppWeb\\logon\\.html(.*)
</url>
</componentWeb>
```

14. В параметре `userDescription` пропишите название целевого приложения. Именно это название пользователь будет видеть в окне ESSO Agent на своем устройстве.

Пример

```
<userDescription>Test.App.Web</userDescription>
```

15. В параметре `cmdLine` проверьте команду для быстрого запуска приложения. Это должна быть команда запуска браузера и адрес страницы приложения.

Пример

```
<applicationDetails>
  <cmdLine>"%ProgramFiles%\\Internet Explorer\\iexplore.exe"
"https://amcore.indeed.com/TestAppWeb/logon.html"
</cmdLine>
</applicationDetails>
```

16. Сохраните измененный файл шаблона с расширением .APP.

## Полезные ссылки

- [Шаблоны Enterprise SSO](#)
- [Шаблонизация Enterprise SSO](#)
- [Подготовка шаблона SSO к работе в Firefox](#)
- [Регулярное выражения в шаблонах SSO](#)
- [Задержки при переходе между контролами при эмуляции ввода](#)

- Шаблонизатор не реагирует на страницы в IE

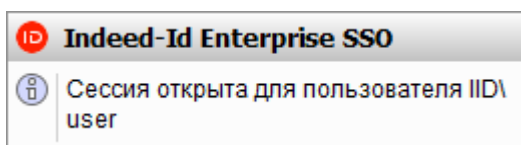
# Работа с ESSO Agent

Чтобы получить доступ в приложения через Enterprise SSO с использованием аутентификатора, обязательно:

- **настройте учетную запись** приложения;
- убедитесь, что пользователь, для которого нужен доступ, **добавлен в политику** с целевым приложением;
- **зарегистрируйте аутентификатор**.

## Запустить ESSO Agent

1. Выполните вход на рабочую станцию. В панели задач отобразится всплывающее сообщение об открытии сессии Single Sign-On.

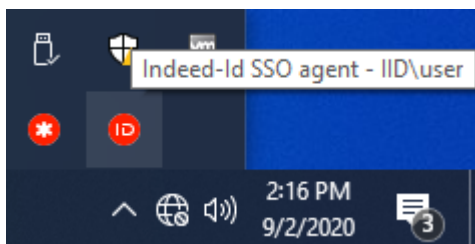


2. ESSO Agent запускается автоматически при входе в операционную систему. Для запуска вручную выберите пункт Indeed Id→Enterprise SSO-Агент в меню Пуск.

## Выбрать целевое приложение

1. Откройте приложение Indeed Id SSO Agent одним из способов:

- Нажмите [Ctrl]+[Alt]+[Q].
- Дважды щелкните левой кнопкой мыши по значку приложения в области уведомлений Windows.



- Правой кнопки мыши нажмите значок в области уведомлений Windows и выберите пункт Быстрый запуск в контекстном меню приложения.

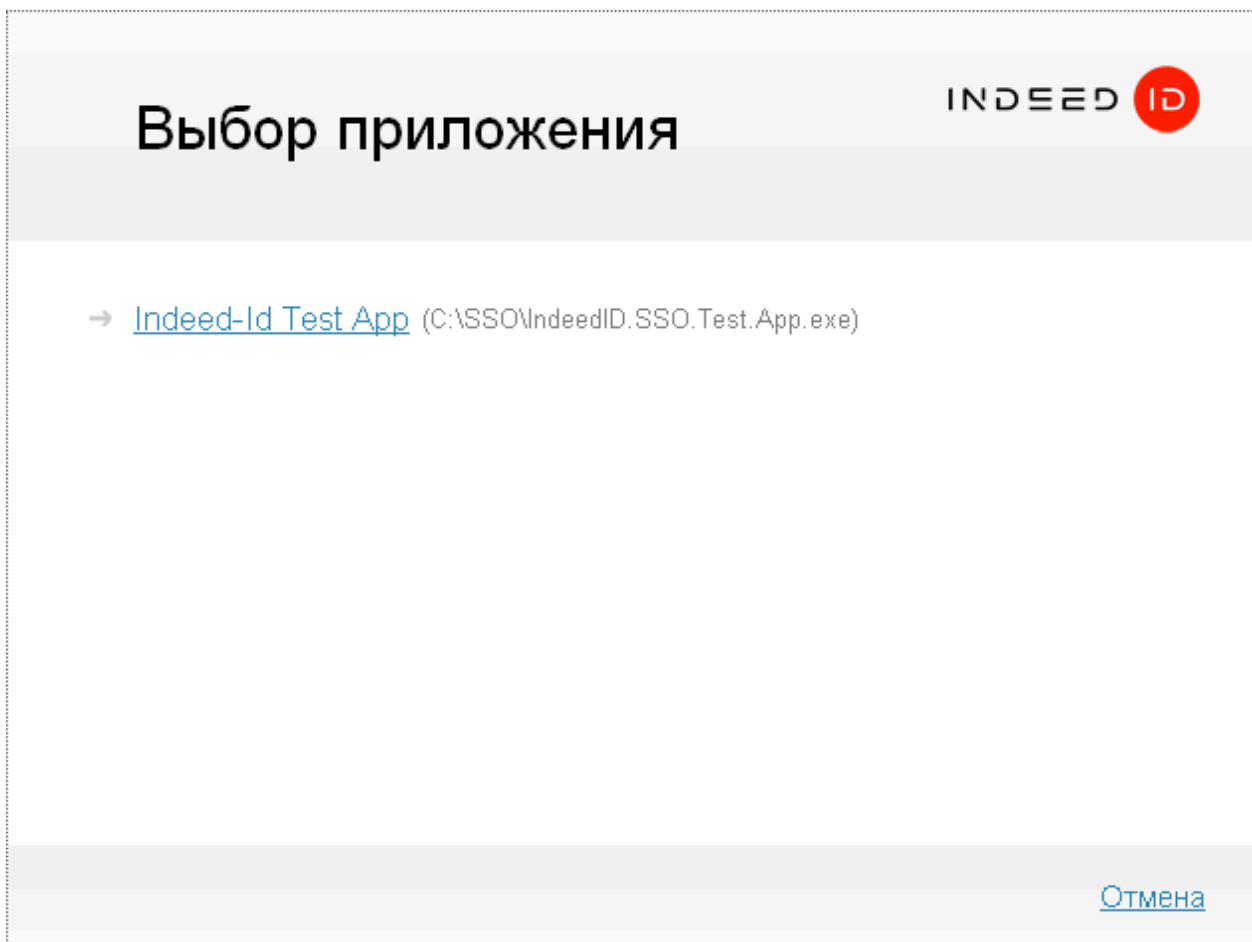


2. В окне Выбор приложения отображаются приложения, разрешенные для запуска с помощью ESSO Agent. Вид окна определяется настройками ESSO-приложений. Выберите нужное приложение.



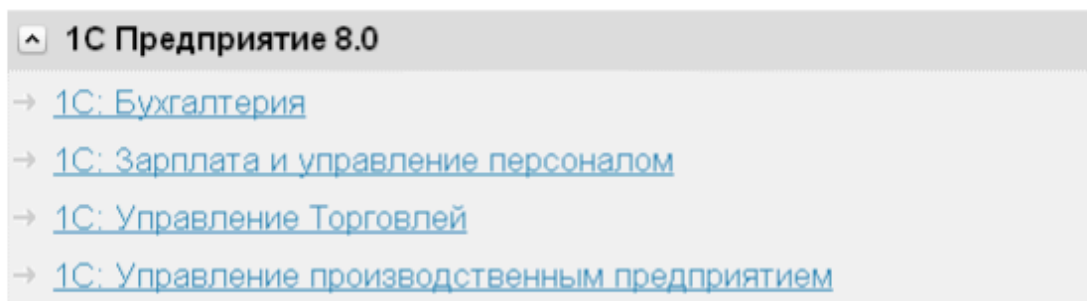
#### ПРИМЕЧАНИЕ

Приложение не отображается в списке, если ESSO Agent не может найти его исполняемый файл на рабочей станции пользователя.



Если приложение содержит в себе несколько компонентов, то исполняемые файлы каждого компонента группируются для удобства выбора в панели быстрого запуска под одним именем.

## Выбор приложения



[Отмена](#)

3. Если для одного целевого приложения настроено несколько учетных записей SSO, то после выбора приложения выберите **учетную запись**.

## Войти в приложение с помощью аутентификатора

Чтобы войти в приложение с помощью аутентификатора:

1. Выберите имя пользователя и способ входа. По умолчанию операционная система предлагает последний использованный способ. Следуйте подсказкам на экране. При наличии нескольких обученных аутентификаторов используйте любой из них.
2. Если зарегистрировано несколько аутентификаторов, выберите любой из них. Чтобы выбрать аутентификатор, нажмите Сменить способ входа.

**SSO: Indeed-Id Test App** **INDEED ID**

**user** (IID\user)

Введите пароль Passcode

\*\*\*\*

Вход

→ [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 выбран запуск приложения только с помощью ESSO Agent и настроено требование аутентификации при входе в приложение, то при отмене аутентификации отобразится сообщение об ошибке.

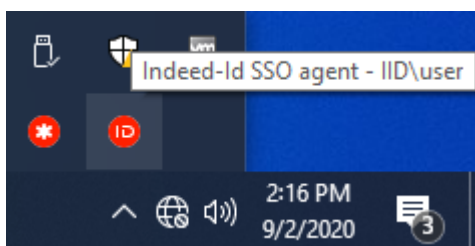
Доступ к целевым приложениям регулируется административными настройками. Некоторые приложения могут быть запрещены для запуска администратором ESSO. Запрещенные приложения недоступны в окне Выбор приложения. При попытке запуска запрещенного приложения отображается сообщение об ошибке *A device attached to the system is not functioning*.

## Сменить пользователя

При использовании ESSO Agent можно выбрать другого пользователя, чтобы получить доступ в приложение.

Чтобы сменить пользователя:

1. Войдите в операционную систему.
2. Правой кнопкой мыши нажмите значок Indeed AM SSO Agent в области уведомлений Windows.



3. В контекстном меню приложения выберите Сменить пользователя...
4. В окне Вход в SSO введите имя учетной записи, под которой требуется выполнить вход в приложение.

# Вход в SSO

INDEED ID

→ Введите имя пользователя

Пользователь:

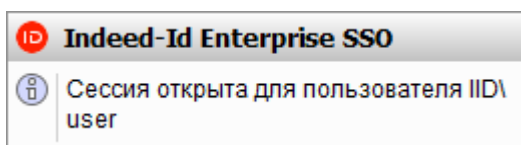
Домен: 

IID

Далее

[Отмена](#)

5. Выполните аутентификацию по имеющимся у выбранного пользователя аутентификаторам. В случае успешной аутентификации ESSO Agent откроет сессию SSO выбранного пользователя.



## Обновить данные

При изменении данных профиля SSO, необходимо загрузить изменения в ESSO Agent. Для этого:

1. Нажмите правой кнопкой мыши по значку приложения Indeed ESSO Agent в панели уведомлений Windows.
2. В открывшемся контекстном меню выберите Обновить данные.

Статус обновления данных отобразится во всплывающих окнах.

▼ Примеры всплывающих окон

---

- Обновление данных:

**Indeed-Id Enterprise SSO**

 Идет обновление данных...

**Indeed-Id Enterprise SSO**

 Обновление завершено.  
Не обнаружено изменений в данных  
профиля

- Новые данные получены:

**Indeed-Id Enterprise SSO**

 Данные профиля были изменены  
администратором

- Ошибка обновления данных:

**Indeed-Id Enterprise SSO**

 Ошибка при обновлении данных.  
Используются прежние данные

## Отключить быстрые клавиши

При необходимости можно отключить использование быстрых клавиш.

По умолчанию включены следующие комбинации клавиш:

- [CTRL]+[ALT]+[Q] — вызов окна быстрого запуска;
- [CTRL]+[ALT]+[U] — обновление данных ESSO;
- [CTRL]+[ALT]+[R] — принудительная обработка формы приложения (рематчинг).

Чтобы отключить быстрые клавиши:

1. Нажмите правой кнопкой мыши по значку приложения Indeed ESSO Agent в панели уведомлений Windows.
2. В открывшемся контекстном меню выберите Отключить быстрые клавиши.

# Вход при отсутствии сети

Войти в приложение по аутентификатору можно даже при отсутствии физического подключения к сети. Вход по кешированному аутентификатору аналогичен входу по аутентификатору при доступной сети.

Чтобы настроить вход при отсутствии сети:

1. Настройте кеширование сессии с помощью **групповых политик или реестра**.
2. Включите кеширование и настройте срок действия аутентификаторов в **Management Console**.
3. Настройте **срок хранения сессии в кеше**.

## Предварительная настройка

Вход при отсутствии сети доступен, если:

- для вашей учетной записи было установлено **разрешение на кеширование аутентификаторов**;
- было выполнено кеширование аутентификаторов при первом входе в приложение по аутентификатору;
- был выполнен вход в систему по кешированному аутентификатору при доступной сети.

## Настроить кеширование сессии

В случаях, когда отсутствует соединение с Core Server, пользователи могут пройти аутентификацию в ESSO Agent в офлайн-режиме. Для этого используется сессия, закешированная на компьютере пользователя.

Чтобы настроить вход по закешированной сессии, используйте политику Настройки публичного ключа сеанса в GPO:

1. Добавьте файл политики *IndeedID.SessionPublicKey.admx* из папки *indeed AM <номер версии> \Misc\ADMX Templates* на компьютер с Core Server.
2. Откройте редактор GPO.
3. Откройте раздел Конфигурация компьютера → Административные шаблоны → Indeed ID → Cache server.



4. Включите политику Настройки публичного ключа сеанса.
5. В свойствах политики в поле Публичный ключ сессии введите значение публичного ключа, сгенерированного **при установке Core Server**. Значение публичного ключа можно найти в файле *SessionPublicKey.pub* либо в конфигурационном файле Core Server *Web.config* в разделе `sessionEncryptionSettings` в параметре `publicKey`.
6. Перейдите в раздел Конфигурация компьютера → Административные шаблоны → Indeed ID → Client Connection.
7. Включите политику Проверка доступности сервера Indeed EA\ESSO.
8. В параметрах политики задайте значения для настроек Таймаут ожидания результата проверки (мс) и Время жизни результата проверки (мс).

## Включить кеширование и настроить срок действия аутентификаторов

**Включить кеширование и задать срок действия кешированных аутентификаторов** можно в настройках приложения политики или пользователя в Management Console. Если сроки действия не указаны, кеширование действует бессрочно.

Если для кешированных аутентификаторов задан параметр Количество дней, то срок их действия отсчитывается со времени последнего входа через Enterprise SSO с использованием сети по любому аутентификатору, кроме Windows Password.

Например, при установленном сроке 10 дней и выполнении входа в приложение в 10:00 12.04.2025 кешированные аутентификаторы будут действительны с 10:00 12.04.2025 до 10:00 22.04.2025.

Если срок действия кешированных аутентификаторов истек и Core Server недоступен, при попытке входа в приложение отображается сообщение *Ошибка входа в систему. Период кеширования данных пользователя закончился*.

## Настроить срок хранения сессии в кеше

При кратковременных разрывах подключения к Core Sever можно настроить период, в течение которого сессию можно будет использовать повторно.

В течение заданного периода сессия хранится в кеше и может быть повторно использована при запросе на новое соединение с сервером. При этом проверка работоспособности сервера повторно не происходит, вместо этого используется закешированный результат проверки.

По истечении периода хранения сессия завершается. По новому запросу на соединение с сервером создается новая сессия.

Чтобы настроить срок хранения сессии в кеше:

#### Через GPO

1. Откройте редактор GPO.
2. Откройте раздел Конфигурация компьютера → Административные шаблоны → Indeed ID → Client Connection.
3. Включите политику Настройки подключения к серверу.
4. В свойствах политики задайте нужное значение для параметра Период удержания объекта сессии (мс). Значение по умолчанию — 180000 мс (3 минуты).

#### Через реестр

1. Откройте редактор реестра.
2. Откройте раздел Компьютер\HKEY\_LOCAL\_MACHINE\SOFTWARE\Indeed-ID\SrvLocator2.
3. Для параметра `SessionHoldPeriodMs` типа *DWORD* установите нужное значение. Значение по умолчанию — 180000 мс (3 минуты).

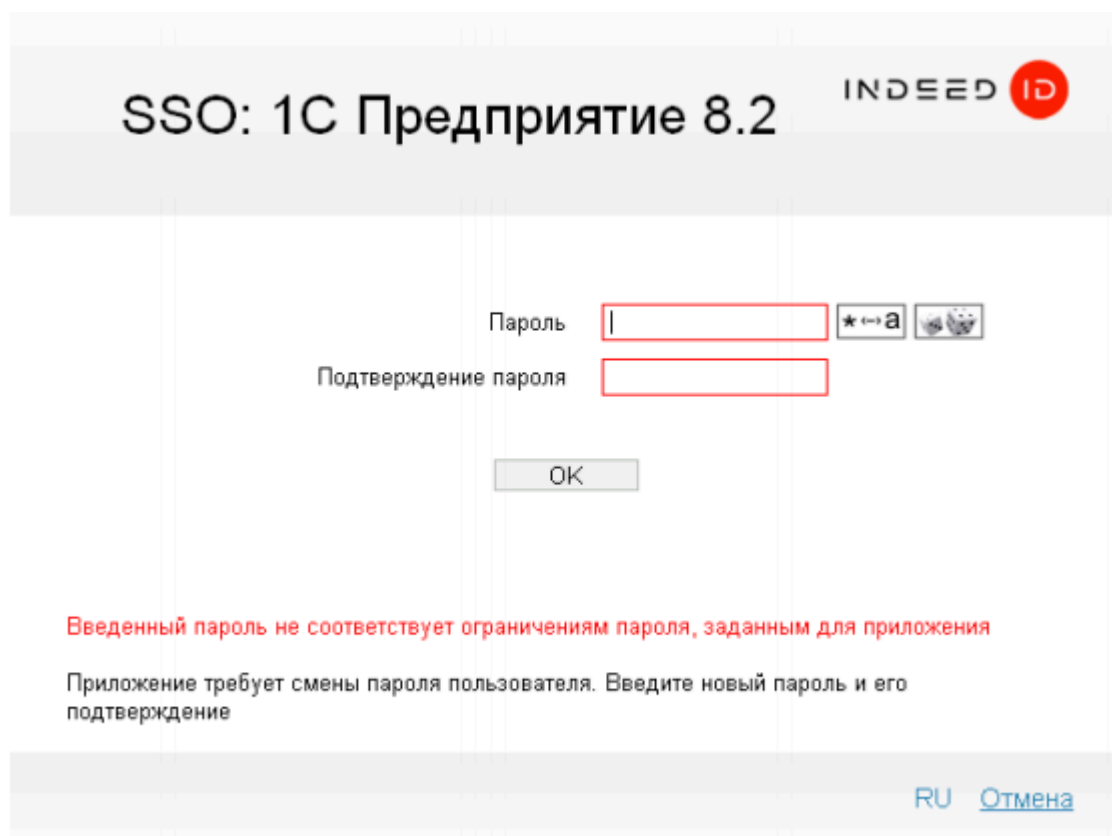
# Управление паролем

ESSO Agent предусматривает регулярную смену пароля в приложениях. Как правило, пароль меняется автоматически.

Можно настроить ручную смену пароля пользователем. 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.

Если включена ручная смена пароля пользователем, то при смене пароля отобразится следующее окно:



SSO: 1C Предприятие 8.2

INDEED ID

Пароль

Подтверждение пароля

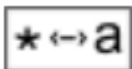
OK

Введенный пароль не соответствует ограничениям пароля, заданным для приложения

Приложение требует смены пароля пользователя. Введите новый пароль и его подтверждение

RU [Отмена](#)

Введите новый пароль и подтвердите его.

- Кнопка Открыть пароль  регулирует режим ввода пароля — скрытый пароль/открытый ввод символов.

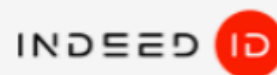
- Кнопка Генерировать случайный пароль  позволяет автоматически сгенерировать пароль с учетом ограничений для данного приложения.

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 ESSO относится к типу *Учетные данные Active Directory*, при смене пароля отображается следующее сообщение:

## SSO: ошибка в 1C 8.2



**Операция смены пароля для приложения 1С 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

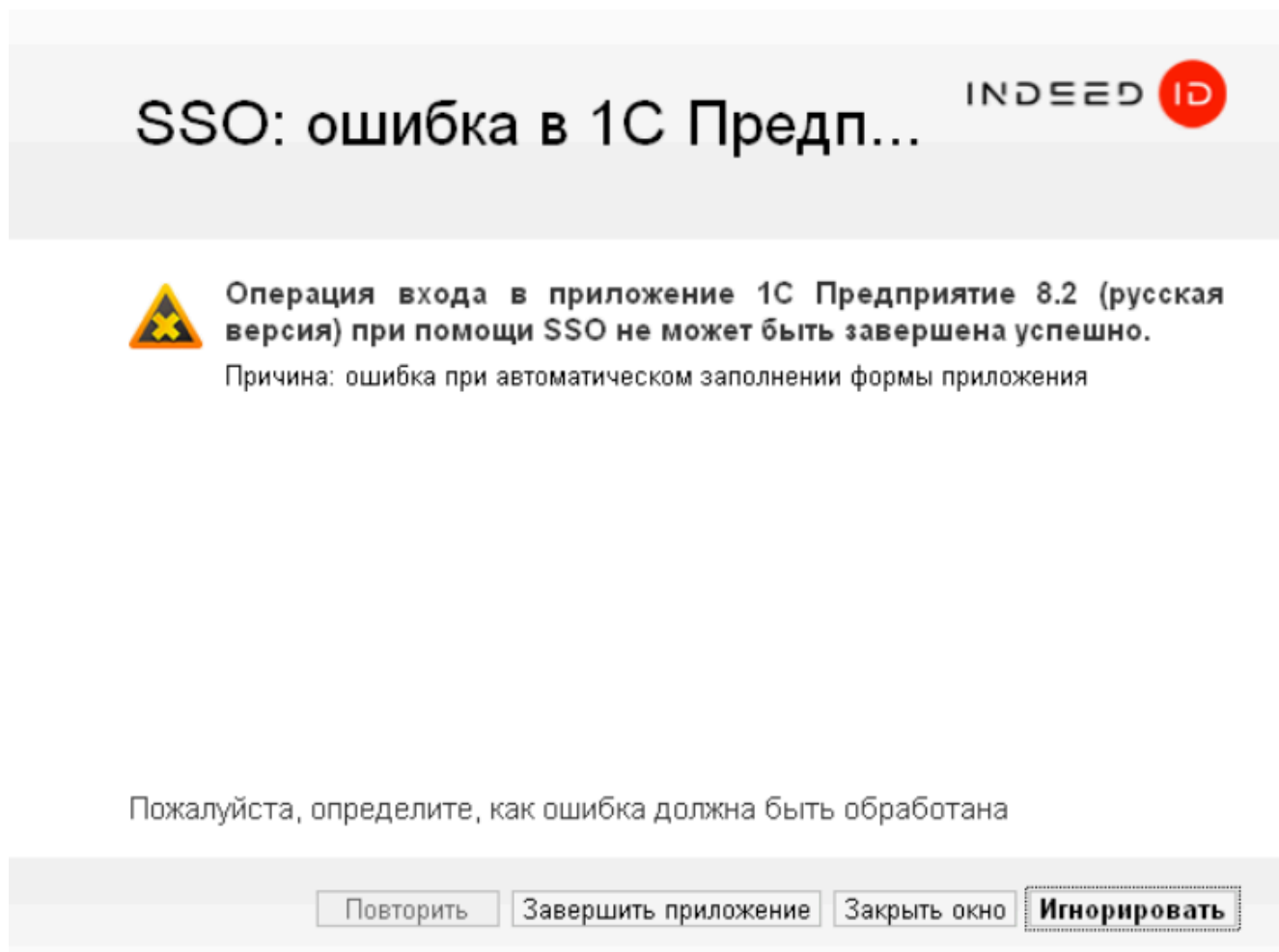
Завершить приложение

Закрыть окно

Игнорировать

# Обработка ошибок

При возникновении ошибок во время работы целевого приложения ESSO Agent позволяет выбрать действие для обработки ошибки. В таких случаях отображается окно Обработка ошибки.



В окне Обработка ошибки выберите действие:

- **Повторить** — операция, в ходе которой возникла ошибка, будет выполнена повторно.
- **Завершить приложение** — приложение, при работе с которым возникла ошибка, будет завершено. Несохранные данные будут потеряны.
- **Заккрыть окно** — будет закрыто текущее окно или форма приложения. При закрытии главного окна приложение может быть завершено.
- **Игнорировать** — не будет предпринято никаких действий.

После выбора действия окно закроется автоматически.

# Прозрачный вход для группы пользователей

Модуль Enterprise SSO позволяет настроить прозрачный вход для отдельной группы пользователей таким образом, чтобы учетные данные подставлялись автоматически без использования аутентификатора.

Чтобы настроить прозрачный вход без использования аутентификатора для отдельной группы пользователей:

1. В **шаблоне** целевого приложения для параметра `forceReauthentication` задайте значение `0`.

В Management Console в карточке приложения на вкладке Общая информация будет отображаться значение Входить прозрачно для настройки Аутентификация при входе в приложение.

2. Убедитесь, что целевое приложение добавлено в политику.
3. В настройках политики в Management Console **создайте** для целевого приложения учетную запись со значением Запрашивать каждый раз для настройки Аутентификация при входе в приложение. Это нужно, чтобы для всех пользователей по умолчанию запрос второго фактора был обязателен.
4. Для тех пользователей, которым нужен прозрачный вход, в карточке пользователя на вкладке Приложения перейдите в настройки целевого приложения и **создайте** учетную запись со значением Входить прозрачно для настройки Аутентификация при входе в приложение.

Пользователи, для которых настроен прозрачный вход, в окне Выбор учетной записи ESSO Agent смогут выбрать вариант без ввода аутентификатора.

# Indeed Windows Logon

Indeed Windows Logon (Windows Logon) предоставляет пользователям:

- доступ в операционную систему по паролю учетной записи;
- доступ в операционную систему с применением доступных технологий аутентификации;
- доступ к удаленному рабочему столу с применением доступных технологий аутентификации;
- доступ в операционную систему по кешированному аутентификатору при отсутствии связи с Core Server.

Windows Logon поддерживает двухфакторную аутентификацию, сертификаты, бесконтактные карты, одноразовые пароли по SMS, электронной почте и другие.

В Windows Logon вы можете выполнить аутентификацию по следующим аутентификаторам:

- Email OTP,
- Futronic Provider,
- Hardware OTP,
- Hardware TOTP,
- мобильное приложение **Indeed Key** в режиме отправки одноразовых паролей и push-уведомлений с подтверждением входа,
- IronLogic Z2USB Provider,
- MFA Provider,
- OMNIKEY Provider,
- Passcode,
- Secured TOTP,
- Smart Card Provider,
- SMS OTP,
- Software TOTP,
- Storage SMS OTP,
- Windows Password.

Для безопасности данных при отсутствии пользователя на рабочем месте Windows Logon поддерживает ручную и автоматическую блокировку рабочей станции — при извлечении устройства аутентификации или включении экранной заставки. Независимо от способа

блокировки для разблокирования рабочей станции всегда требуется повторное подтверждение личности пользователя с помощью аутентификатора.

Часто задаваемые вопросы о работе Windows Logon

## Предварительная настройка

Чтобы использовать Windows Logon для входа в систему:

1. **Установите и настройте** модуль Windows Logon.
2. **Зарегистрируйте лицензию модуля** в Management Console.
3. **Установите и настройте** провайдеры аутентификации.
4. При необходимости установите аппаратное устройство аутентификации.

Войти в систему по аутентификатору и управлять аутентификаторами можно только при **разрешении**, выданном администратором системы.

## Установить

1. Запустите файл для установки, расположенный по пути *Indeed AM <номер версии>/Indeed AM Windows Logon/<номер версии>*.
2. После завершения установки компонента нужно перезагрузить систему. В окне мастера установки нажмите Да, чтобы выполнить перезагрузку сразу, или Нет, чтобы сделать это позднее вручную.

### ПРИМЕЧАНИЕ

Развернуть Windows Logon на рабочих станциях пользователей в автоматическом режиме можно с помощью механизма групповых политик (Microsoft Group Policy) или любого другого инструмента, который позволяет массово распространять и устанавливать MSI-пакеты на рабочие станции пользователей (например, Microsoft System Center Configuration Manager).

## Настроить

Настроить Windows Logon можно через редактор реестра или с помощью групповых политик.



При этом настройки через групповые политики будут приоритетнее настроек, заданных через реестр вручную. Посмотреть настройки групповых политик в реестре можно по пути *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Indeed-ID\SrvLocator2*.

Подробнее о групповых политиках модуля — в разделе **Windows Logon**.

#### Через реестр

1. Откройте редактор реестра Windows.
2. Перейдите в раздел *HKEY\_LOCAL\_MACHINE\SOFTWARE\Indeed-ID\SrvLocator2*.
3. Откройте свойства строкового параметра `ServerUrlBase`.
4. В поле Значение укажите URL вашего Core Server в формате *http(s)://  
полное\_dns\_имя\_сервера/am/core*.

#### ⚠ ПРИМЕЧАНИЕ

При использовании соединения по протоколу HTTPS установите клиентский сертификат на каждый Core Server.

#### Через GPO

#### ⚠ ПРИМЕЧАНИЕ

Шаблоны групповых политик расположены в папке *Indeed AM <номер версии>\Misc\ADMX Templates*.

1. Добавьте политику *IndeedID.ServerUrl.admx* на устройство с установленным Indeed AM Windows Logon.
2. Откройте редактор GPO.
3. Откройте раздел Конфигурация компьютера → Административные шаблоны → Indeed ID → ClientConnection.
4. Включите политику Настройки подключения к серверу.

5. В поле URL-адрес AM сервера укажите адрес вашего Core Server в формате *http(s)://полное\_dns\_имя\_сервера/am/core*.

## Дополнительные возможности

Дополнительные возможности Windows Logon:

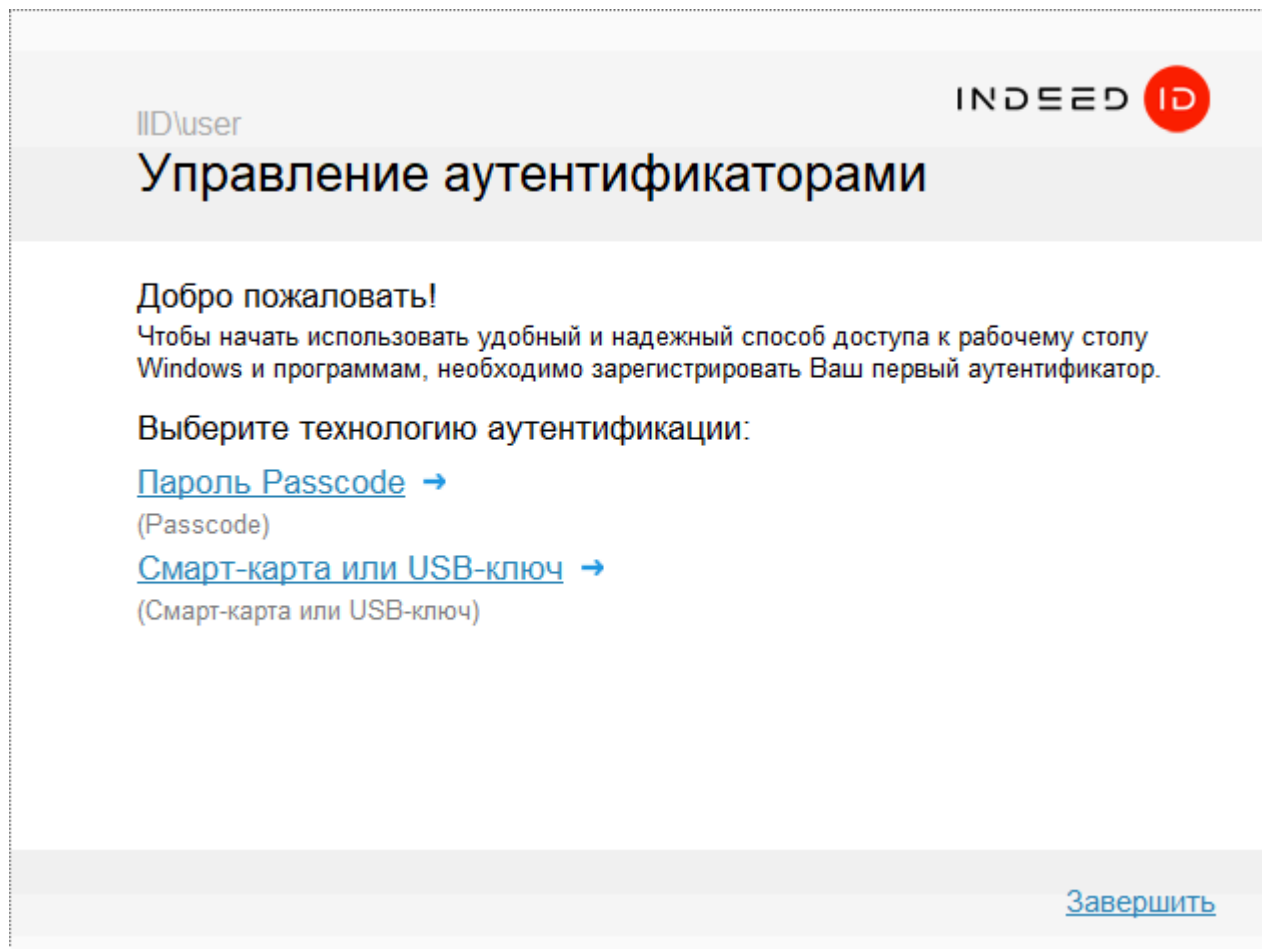
- Самостоятельная регистрация и управления аутентификаторами с помощью **утилиты управления**.
- Генерация **случайного пароля** для пользователя в Active Directory.
- Функция **Indeed AM Paste**, которая позволяет автоматически подставить пароль в скрытом виде при нажатии определенной комбинации клавиш.
- **Одновременная работа** модуля с Indeed RDP Windows Logon.

- Аутентификация средствами Indeed AM при запуске приложения **от имени администратора.**

# Первый вход в систему

Если у пользователя нет зарегистрированных аутентификаторов, для первого входа в систему нужно использовать доменный пароль.

Если пользователю **разрешено регистрировать аутентификаторы**, то при входе в систему запустится *Мастер первого входа* и предложит зарегистрировать **первый аутентификатор**.



ИД\user **INDEED ID**

## Управление аутентификаторами

Добро пожаловать!

Чтобы начать использовать удобный и надежный способ доступа к рабочему столу Windows и программам, необходимо зарегистрировать Ваш первый аутентификатор.

Выберите технологию аутентификации:

[Пароль Passcode](#) →  
(Passcode)

[Смарт-карта или USB-ключ](#) →  
(Смарт-карта или USB-ключ)

[Завершить](#)

Можно зарегистрировать аутентификатор сразу или позднее в любое удобное время.

- Чтобы зарегистрировать аутентификатор, в окне Управление аутентификаторами выберите один из доступных способов аутентификации.
- Чтобы войти в систему без регистрации аутентификатора, нажмите Завершить. В этом случае *Мастер первого входа* будет отображаться при каждом следующем входе в систему до регистрации первого аутентификатора.

Если на рабочей станции не обнаружены провайдеры аутентификации, зарегистрировать аутентификаторы будет невозможно. Отобразится ошибка *В системе не обнаружено ни одного*

провайдера аутентификации. Необходимо установить провайдер и повторно выполнить настройку защищенного входа в систему.

Если у пользователя настроена аутентификация по SMS OTP или Email OTP, то вход систему будет выполнен по настроенному аутентификатору, после чего появится сообщение о **рассинхронизации пароля**.

## Зарегистрировать первый аутентификатор

Чтобы зарегистрировать первый аутентификатор:

1. В окне мастера выберите способ аутентификации. В окне мастера отображаются установленные аутентификаторы, которые включены в свойства Windows Logon в карточке политики.
2. Выполните необходимые действия, следуя подсказкам в окне Управление аутентификаторами. Внешний вид окна и действия зависят от выбранного способа аутентификации.

Если вы хотите вернуться на предыдущую страницу и изменить настройки или выбрать другой способ входа, нажмите Вернуться.

3. После регистрации аутентификатора в окне Управление аутентификаторами отображается сообщение *Новый аутентификатор успешно обучен*. Можно добавить произвольный текстовый комментарий к зарегистрированному аутентификатору, если данное действие разрешено администратором системы.

Чтобы завершить регистрацию аутентификатора, нажмите Сохранить.

IID\user

INDEED ID

## Управление аутентификаторами



### Новый аутентификатор успешно обучен

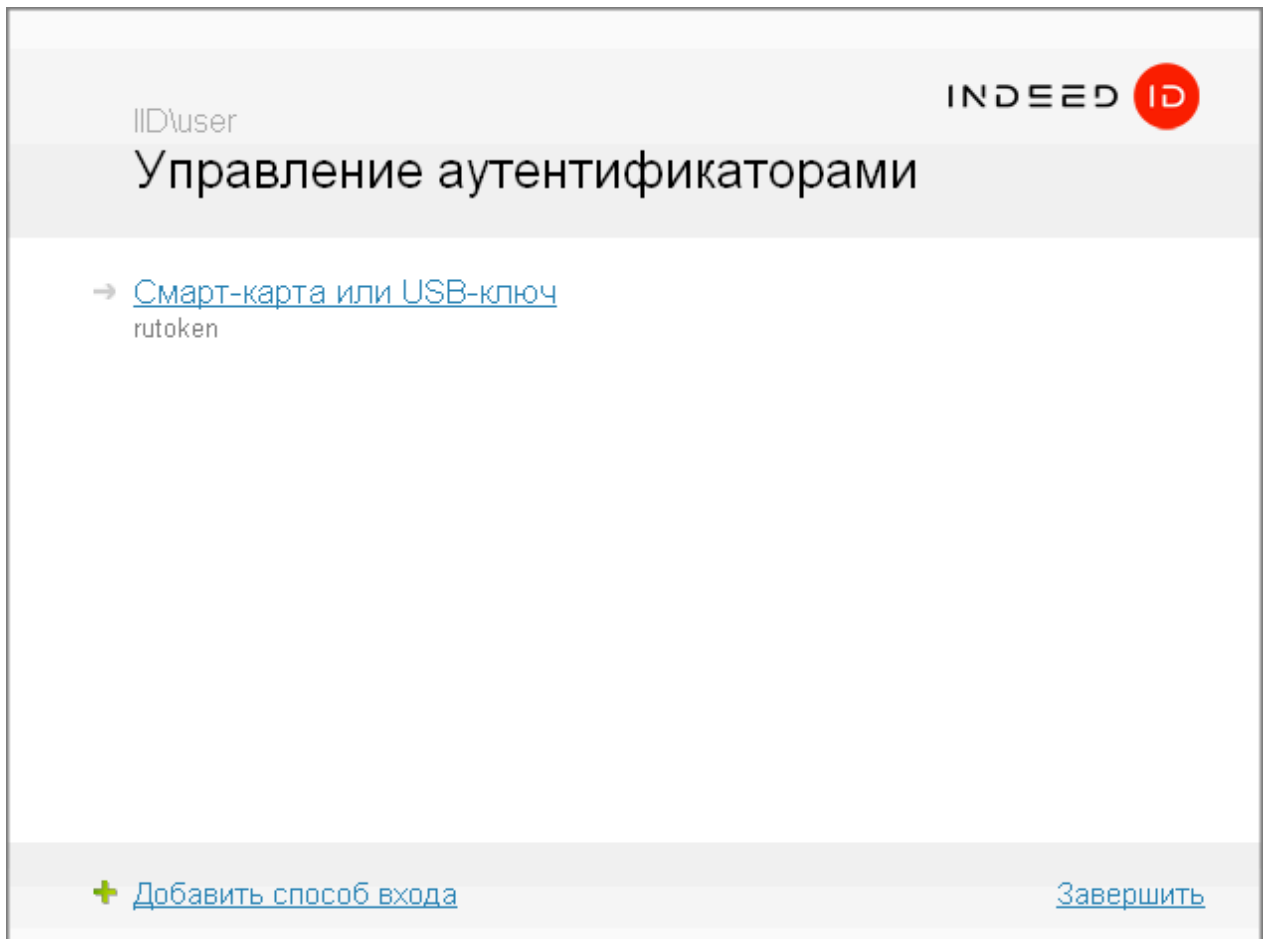
Все готово для регистрации аутентификатора в системе.  
Перед сохранением вы можете задать комментарий к аутентификатору:

Сохранить

[Завершить](#)

Тип зарегистрированного аутентификатора и комментарий к нему отобразятся в окне Управление аутентификаторами.

4. Если для пользователю разрешено добавление нескольких аутентификаторов, можно перейти к их регистрации, нажав Добавить способ входа. В зависимости от **выданных разрешений**, можно также изменить, проверить или удалить зарегистрированный аутентификатор.



При следующем входе в систему будет доступен способ входа по зарегистрированному аутентификатору.

# Вход в систему по аутентификатору

Этот способ входа доступен только если:

- вы являетесь **лицензированным пользователем** Indeed AM,
- для вашей учетной записи **разрешена регистрация аутентификаторов**,
- вы уже зарегистрировали **хотя бы один аутентификатор**.

Чтобы войти в систему:

1. После загрузки операционной системы выберите нужного пользователя.
2. В открывшемся окне Вход в Windows отобразится имя пользователя, выполнявшего вход в систему последним и используемый им способ входа.



**Вход в Windows**

user (IID\user)

Введите свой пароль Windows

→ [Сменить способ входа](#)

[Отмена](#)

Если вы хотите сменить пользователя, нажмите Отмена и выберите учетную запись нужного пользователя.



Если вы хотите выбрать другой способ входа, нажмите Сменить способ входа и выберите один из способов входа, соответствующий зарегистрированному аутентификатору.

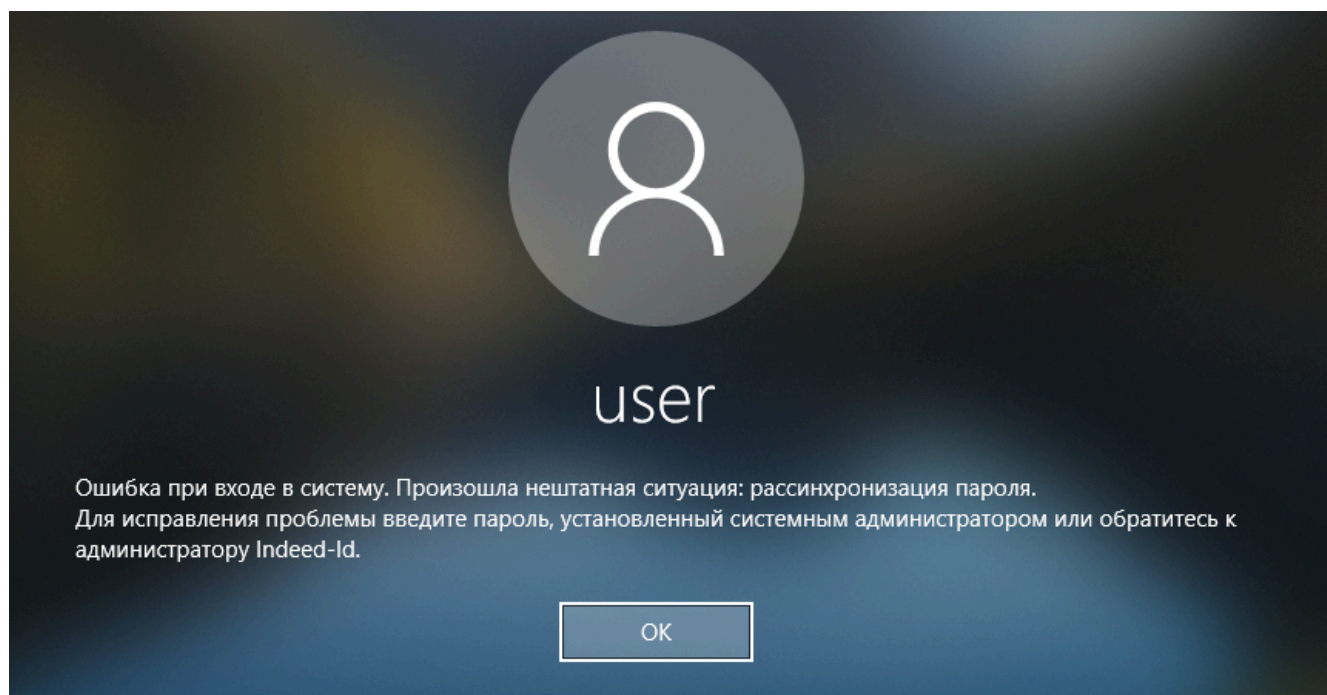
3. После выбора способа входа следуйте подсказкам в окне аутентификации. Внешний вид окна аутентификации и требуемые действия зависят от выбранного типа аутентификатора.

# Рассинхронизация пароля

В ряде случаев может произойти рассинхронизация пароля:

- Если доменный пароль сброшен администратором системы, а у пользователя зарегистрирован хотя бы один зарегистрированный аутентификатор.
- Если при запросе на изменение пароля недоступен ни один Core Server, но доступен хотя бы один контроллер домена. В этом случае отображается сообщение *Ошибка связи с сервером. Сервер не найден. Если Вы продолжите, произойдет рассинхронизация пароля.*
- При первом входе в систему, если для пользователя настроена аутентификация по SMS OTP или Email OTP.

Это происходит, когда новый пароль невозможно синхронизировать с базой данных Core Server.



Чтобы синхронизировать пароль:

1. В окне с предупреждением о рассинхронизации нажмите ОК.
2. Введите новый пароль.

Если рассинхронизация произошла из-за недоступности Core Server, выполните эти действия, когда доступен хотя бы один сервер.

Актуальный пароль из Active Directory синхронизируется с паролем в базе данных Core Server.  
После успешной синхронизации будет выполнен вход в систему.

# Доступ к удаленному рабочему столу

Для доступа к удаленному рабочему столу по аутентификатору требуются:

- стандартная утилита Windows *Подключение к удаленному рабочему столу* (mstsc.exe/Remote Desktop) на устройстве, с которого происходит подключение (терминальный клиент);
- модуль **Indeed AM Windows Logon**, установленный на устройстве, к которому требуется удаленный доступ (терминальный сервер);
- соответствующий **провайдер аутентификации**, установленный на устройстве, к которому требуется удаленный доступ;
- при использовании Hardware OTP Provider аппаратное устройство аутентификации, подключенное к устройству, с которого происходит подключение;
- отключенная аутентификация на сетевом уровне на устройстве, к которому требуется получить доступ.

## ▼ Как отключить аутентификацию на сетевом уровне

### Через GPO

1. Откройте редактор GPO.
2. Откройте раздел Конфигурация компьютера → Административные шаблоны → Компоненты Windows → Службы удаленных рабочих столов → Узел сеансов удаленных рабочих столов → Безопасность.
3. Отключите политику Требовать проверку подлинности пользователя для удаленных подключений путем проверки подлинности на уровне сети.
4. Включите политику Установить уровень шифрования для клиентских подключений.
5. В параметрах политики для настройки Уровень шифрования выберите значение Высокий уровень.
6. Включите политику Требовать использования специального уровня безопасности для удаленных подключений по протоколу RDP.
7. В параметрах политики для настройки Уровень безопасности выберите значение RDP.

### Через реестр

1. Откройте редактор реестра.
2. Откройте раздел  
Компьютер\HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services.
3. Для параметра `UserAuthentication` типа *DWORD* установите значение 0.
4. Для параметра `MinEncryptionLevel` типа *DWORD* установите значение 3.
5. Для параметра `SecurityLayer` типа *DWORD* установите значение 0.



#### ПРЕДУПРЕЖДЕНИЕ

Если Аутентификация на сетевом уровне (Network Level Authentication, NLA) отключена, снижается уровень безопасности. Поэтому для подключения к удаленному рабочему столу рекомендуется использовать модуль RDP Windows Logon.

Можно также настроить одновременную работу Windows Logon и RDP Windows Logon.

Чтобы подключиться к удаленному рабочему столу по аутентификатору:

1. Запустите Подключение к удаленному рабочему столу.
2. Введите имя или адрес устройства, к которому нужно получить доступ, и нажмите Подключить.
3. В окне Безопасность Windows введите пароль учетной записи и дождитесь подключения.
4. В отобразившемся окне Вход в Windows выберите учетную запись, способ входа (тип аутентификатора) и пройдите аутентификацию.



#### ПРИМЕЧАНИЕ

Если для учетной записи не включена генерация случайного пароля, можно получить доступ к удаленному рабочему столу по доменному паролю.

Чтобы при подключении к удаленному рабочему столу не запрашивались логин и пароль пользователя, нужно изменить системные настройки. Подробнее — в статье [Отключение запроса логина и пароля на стороне терминального клиента](#).

# Вход при отсутствии сети

Войти в систему по аутентификатору можно даже при отсутствии физического подключения к сети. Вход по кешированному аутентификатору аналогичен входу по аутентификатору при доступной сети.

Чтобы настроить вход при отсутствии сети:

1. Настройте кеширование сессии с помощью **групповых политик или реестра**.
2. Включите кеширование и настройте срок действия аутентификаторов в **Management Console**.
3. Настройте **срок хранения сессии в кеше**.

## Предварительная настройка

Вход при отсутствии сети доступен, если:

- для вашей учетной записи было установлено **разрешение на кеширование аутентификаторов**;
- было выполнено кеширование аутентификаторов при первом входе в систему по аутентификатору;
- был выполнен вход в систему по кешированному аутентификатору при доступной сети.

## Настроить кеширование сессии

В случаях, когда отсутствует соединение с Core Server, пользователи могут пройти аутентификацию в Windows Logon в офлайн-режиме. Для этого используется сессия, закешированная на компьютере пользователя.

Чтобы настроить вход по закешированной сессии, используйте политику Настройки публичного ключа сеанса в GPO:

1. Добавьте файл политики *IndeedID.SessionPublicKey.admx* из папки *indeed AM <номер версии> \Misc\ADMX Templates* на компьютер с Core Server и установленным Windows Logon.
2. Откройте редактор GPO.

3. Откройте раздел Конфигурация компьютера → Административные шаблоны → Indeed ID → Cache server.
4. Включите политику Настройки публичного ключа сеанса.
5. В свойствах политики в поле Публичный ключ сессии введите значение публичного ключа, сгенерированного **при установке Core Server**. Значение публичного ключа можно найти в файле *SessionPublicKey.pub* либо в конфигурационном файле Core Server *Web.config* в разделе `sessionEncryptionSettings` в параметре `publicKey`.
6. Перейдите в раздел Конфигурация компьютера → Административные шаблоны → Indeed ID → Client Connection.
7. Включите политику Проверка доступности сервера Indeed EA\ESSO.
8. В параметрах политики задайте значения для настроек Таймаут ожидания результата проверки (мс) и Время жизни результата проверки (мс).

## Включить кеширование и настроить срок действия аутентификаторов

**Включить кеширование и задать срок действия кешированных аутентификаторов** можно в настройках приложения политики или пользователя в Management Console. Если сроки действия не указаны, кеширование действует бессрочно.

Если для кешированных аутентификаторов задан параметр Количество дней, то срок их действия отсчитывается со времени последнего входа в Windows Logon с использованием сети по любому аутентификатору, кроме Windows Password.

Например, при установленном сроке 10 дней и выполнении входа в приложение в 10:00 12.04.2025 кешированные аутентификаторы будут действительны с 10:00 12.04.2025 до 10:00 22.04.2025.

Если срок действия кешированных аутентификаторов истек и Core Server недоступен, при попытке входа в приложение отображается сообщение *Ошибка входа в систему. Период кеширования данных пользователя закончился*.

## Настроить срок хранения сессии в кеше

При кратковременных разрывах подключения к Core Sever можно настроить период, в течение которого сессию можно будет использовать повторно.



В течение заданного периода сессия хранится в кеше и может быть повторно использована при запросе на новое соединение с сервером. При этом проверка работоспособности сервера повторно не происходит, вместо этого используется закешированный результат проверки.

По истечении периода хранения сессия завершается. По новому запросу на соединение с сервером создается новая сессия.

Чтобы настроить срок хранения сессии в кеше:

#### Через GPO

1. Откройте редактор GPO.
2. Откройте раздел Конфигурация компьютера → Административные шаблоны → Indeed ID → Client Connection.
3. Включите политику Настройки подключения к серверу.
4. В свойствах политики задайте нужное значение для параметра Период удержания объекта сессии (мс). Значение по умолчанию — 180000 мс (3 минуты).

#### Через реестр

1. Откройте редактор реестра.
2. Откройте раздел Компьютер\HKEY\_LOCAL\_MACHINE\SOFTWARE\Indeed-ID\SrvLocator2.
3. Для параметра `SessionHoldPeriodMs` типа *DWORD* установите нужное значение. Значение по умолчанию — 180000 мс (3 минуты).

# Опциональные настройки

С помощью Windows Logon вы можете:

## ▼ Включить генерацию случайного пароля

---

При использовании модуля Windows Logon можно задать генерацию случайного пароля для пользователя в Active Directory. Для работы этой настройки в свойствах пользователя в Active Directory отключите опции Запретить смену пароля пользователя и Срок действия пароля не ограничен.

Случайный пароль для учетной записи будет сгенерирован по истечении срока действия текущего пароля. Если для учетной записи был сгенерирован случайный пароль, то следующий вход в систему возможен только с использованием аутентификатора.

Чтобы включить генерацию случайного пароля:

1. На боковой панели Management Console перейдите в раздел Политики.
2. Откройте нужную политику.
3. На вкладке Приложения нажмите Windows Logon.
4. Для настройки Пароль учетной записи Active Directory выберите Генерировать случайный.
5. Нажмите Сохранить.

Пароли для всех пользователей в данной политике будут изменены, если это не противоречит их свойствам в Active Directory.

В журнале событий Management Console отобразится событие 1091 Пароль пользователя был успешно сменен автоматически. Пользователи смогут войти в систему только с помощью добавленных аутентификаторов, не используя доменный пароль.

Если у пользователя нет зарегистрированных аутентификаторов, то при первом входе в систему после ввода доменного пароля откроется утилита управления аутентификаторами и предложит зарегистрировать **первый аутентификатор**.

После регистрации аутентификатора происходит генерация и смена пароля пользователя.

Если доменный пароль изменен администратором, при входе в систему появится сообщение о рассинхронизации пароля. Нажмите ОК и введите пароль, заданный администратором. После этого пароль будет автоматически изменен.

## ❗ ИНФОРМАЦИЯ

Если для учетной записи разрешено кэширование аутентификаторов, то при последующем входе в систему по аутентификатору будет выполнено сохранение данных в локальную память компьютера. Тогда при отсутствии подключения к Core Server войти в систему можно будет с помощью кэшированных данных аутентификатора.

### ▼ Если для пользователя включено требование на смену пароля

Если в свойствах пользователя в Active Directory включено требование на смену доменного пароля и разрешена генерация случайного пароля, то при следующей аутентификации с помощью технологии Indeed будет сгенерирован случайный пароль. При этом отобразится сообщение об успешной автоматической смене пароля.

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

## ▼ Настроить автоматическую подстановку скрытого пароля с помощью Indeed AM Paste

---

Когда для входа в приложение требуется ввести пароль, можно сделать это безопасно с помощью функции Indeed AM Paste. Она позволяет автоматически подставлять скрытый пароль в поле ввода, используя определенную комбинацию клавиш. По умолчанию это *[CTRL] + [ALT] + [V]*.

Включить и отключить функцию Indeed AM Paste можно в приложении Indeed-Id Paste Tool. Для этого:

1. Нажмите правой кнопкой мыши  в области уведомлений Windows.
2. Выберите нужный пункт контекстного меню:
  - Разрешить Indeed-Id Paste, чтобы включить или отключить функцию. Функция по умолчанию включена.
  - Запускать при загрузке, чтобы Indeed-Id Paste Tool запускалась при загрузке Windows. Эта настройка по умолчанию включена.
  - Выход.

Чтобы подставить пароль в скрытом виде:

1. В окне приложения установите курсор в поле ввода пароля.
2. Нажмите комбинацию клавиш для подстановки пароля.
3. Откроется окно Аутентификация. Подтвердите свою личность любым доступным способом.

После успешной аутентификации в поле ввода отображается скрытый пароль.

## ▼ Настроить одновременную работу с Indeed RDP Windows Logon

---

Если модули Windows Logon и RDP Windows Logon установлены на одном устройстве, настройте политику для Windows Logon.

### Через GPO

1. Перейдите на устройство, на котором установлены модули RDP Windows Logon и Windows Logon.
2. Откройте редактор GPO.
3. Откройте раздел Конфигурация компьютера → Административные шаблоны → Indeed ID → Windows Logon.
4. Включите политику Настройки Credential Provider.
5. Для параметра Отображение способов входа выберите значение Все, кроме пароля.

### Через реестр

1. Перейдите на устройство, на котором установлены модули RDP Windows Logon и Windows Logon.
2. Откройте редактор реестра.
3. Откройте раздел  
Компьютер\HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Indeed-ID\Logon for Windows.
4. Создайте параметр типа *DWORD* с именем **CredProvFilter** и установите ему значение 2.

## ▼ Использовать аутентификацию при запуске от имени администратора

На устройствах под управлением Windows 7 модуль Windows Logon выполняет запрос на аутентификацию при использовании команды Запуск от имени администратора. После запуска этой команды отображается диалог выбора учетной записи, затем окно Аутентификация системы Indeed AM. В зависимости от версии операционной системы окно выбора учетной записи может иметь разный вид.

# Аутентификация



→ Введите имя пользователя

Пользователь:

Домен:  

[EN](#) [Отмена](#)

# Утилита управления аутентификаторами

## ВАЖНО!

Утилита управления аутентификаторами работает только в сценариях с модулями Enterprise SSO и Windows Logon.

Утилита устанавливается автоматически при установке этих модулей.

Вы можете управлять аутентификаторами с помощью приложения Indeed AM Управление аутентификаторами. Данное приложение позволяет добавлять новые аутентификаторы, редактировать, проверять и удалять существующие.

## ПРИМЕЧАНИЕ

Возможности управления аутентификаторами доступны при наличии разрешения, установленного администратором системы.

Для перехода к управлению аутентификаторами выполните следующие действия:

1. Откройте приложение Indeed AM Управление аутентификаторами (Пуск→Indeed AM→Indeed AM Управление аутентификаторами).
2. В окне Аутентификация выберите свою учетную запись и способ входа (тип аутентификатора). По умолчанию автоматически выбирается последний использованный способ входа.

## ИНФОРМАЦИЯ

Для входа в приложение Управление аутентификаторами следует использовать ранее зарегистрированный аутентификатор. При использовании пароля для доступа к приложению будут недоступны функции изменения, удаления и добавления аутентификаторов.

3. Выполните требуемые действия (в зависимости от выбранного способа входа).





#### ПРИМЕЧАНИЕ

Возможности добавления, редактирования и удаления аутентификаторов доступны после авторизации с использованием аутентификатора. Возможность проверки аутентификаторов доступна как после авторизации с использованием аутентификатора, так и после авторизации с использованием пароля.

4. После успешной аутентификации отображается окно Управление аутентификаторами.

# Добавление аутентификатора

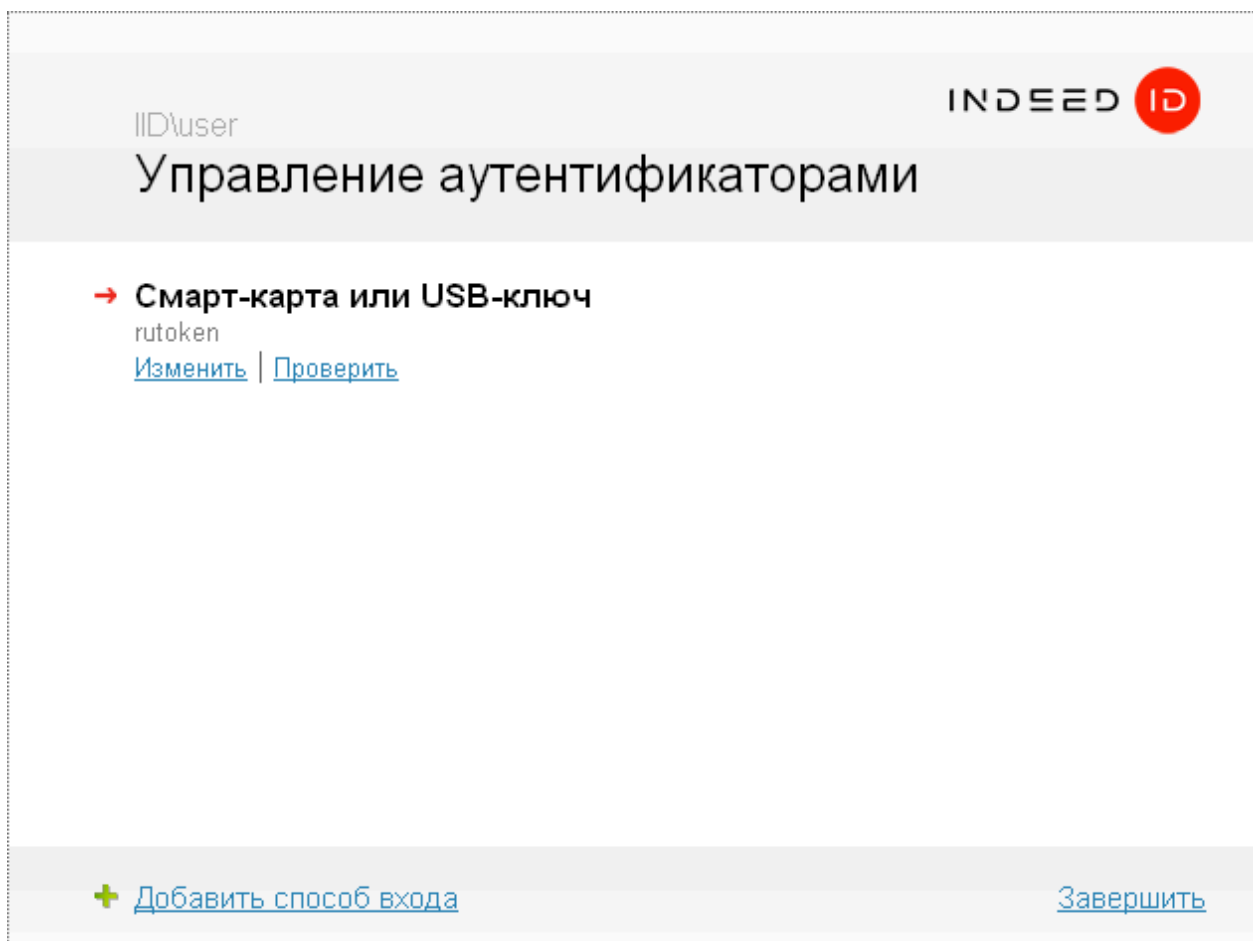
## ВАЖНО!

Перед регистрацией аутентификаторов необходимо создать политику и распространить на целевых пользователей

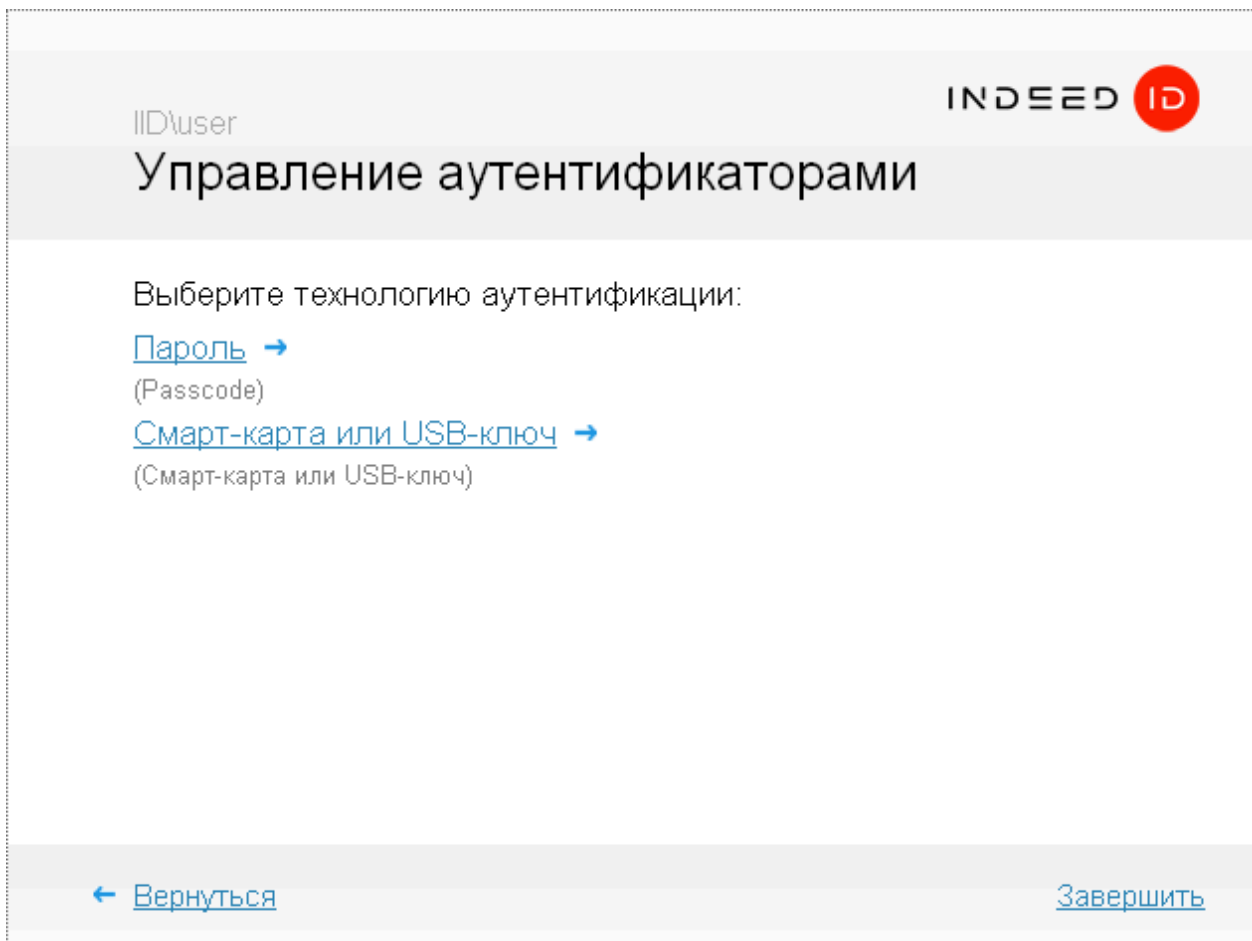
Количество аутентификаторов, которое вы можете добавить, устанавливается администратором системы. После достижения максимального количества аутентификаторов кнопка **Добавить** способ входа в окне Управление аутентификаторами становится неактивна.

Для добавления аутентификатора выполните следующие действия:

1. В окне Управление аутентификаторами нажмите **Добавить** способ входа



2. Выберите технологию аутентификации.



3. Следуйте инструкциям по регистрации аутентификатора. Внешний вид окна и текст подсказок зависят от выбранного типа аутентификатора.

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\userINDEED ID

Управление аутентификаторами

\*\*\*\*



Новый аутентификатор успешно обучен

Все готово для регистрации аутентификатора в системе. Перед сохранением вы можете задать комментарий к аутентификатору:

Сохранить

[← Вернуться](#)

[Завершить](#)

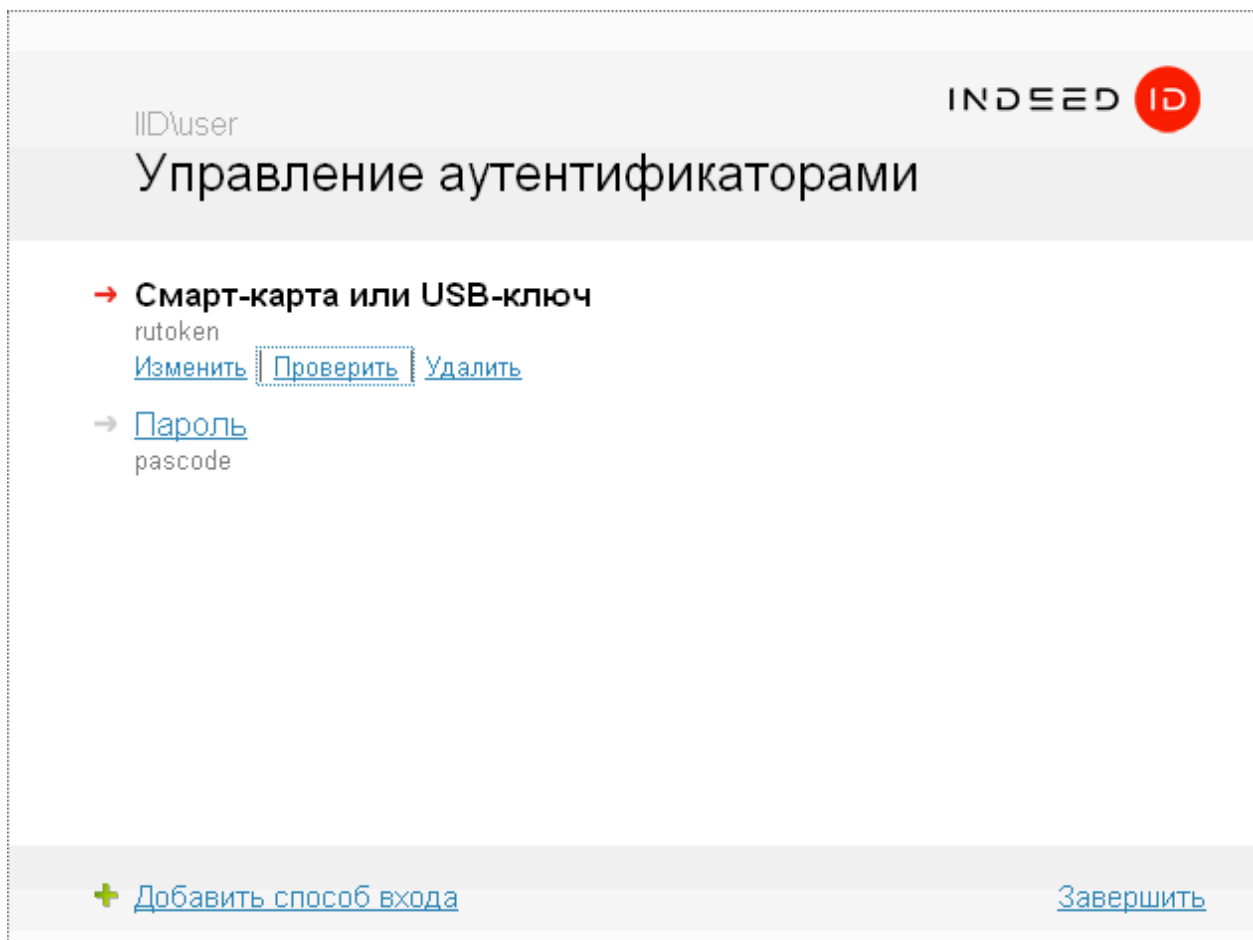
4. Вы можете добавить произвольный текстовый комментарий к зарегистрированному аутентификатору (если данное действие разрешено администратором системы). Для завершения регистрации аутентификатора нажмите Сохранить.

Тип зарегистрированного аутентификатора и комментарий к нему отображаются в окне Управление аутентификаторами. Если для вашей учетной записи разрешено добавление нескольких аутентификаторов, вы можете перейти к их регистрации, нажав кнопку Добавить аутентификатор.

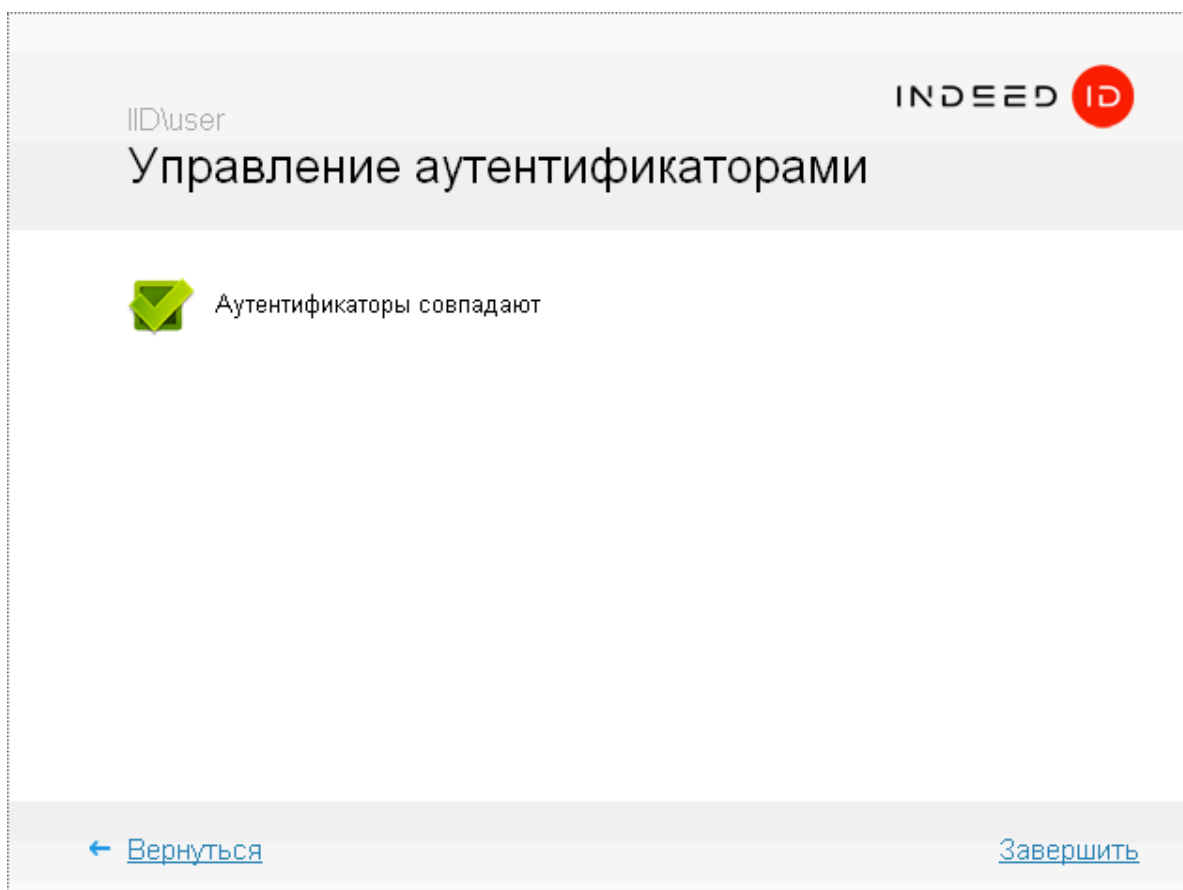
# Проверка аутентификатора

Для проверки аутентификатора выполните следующие действия:

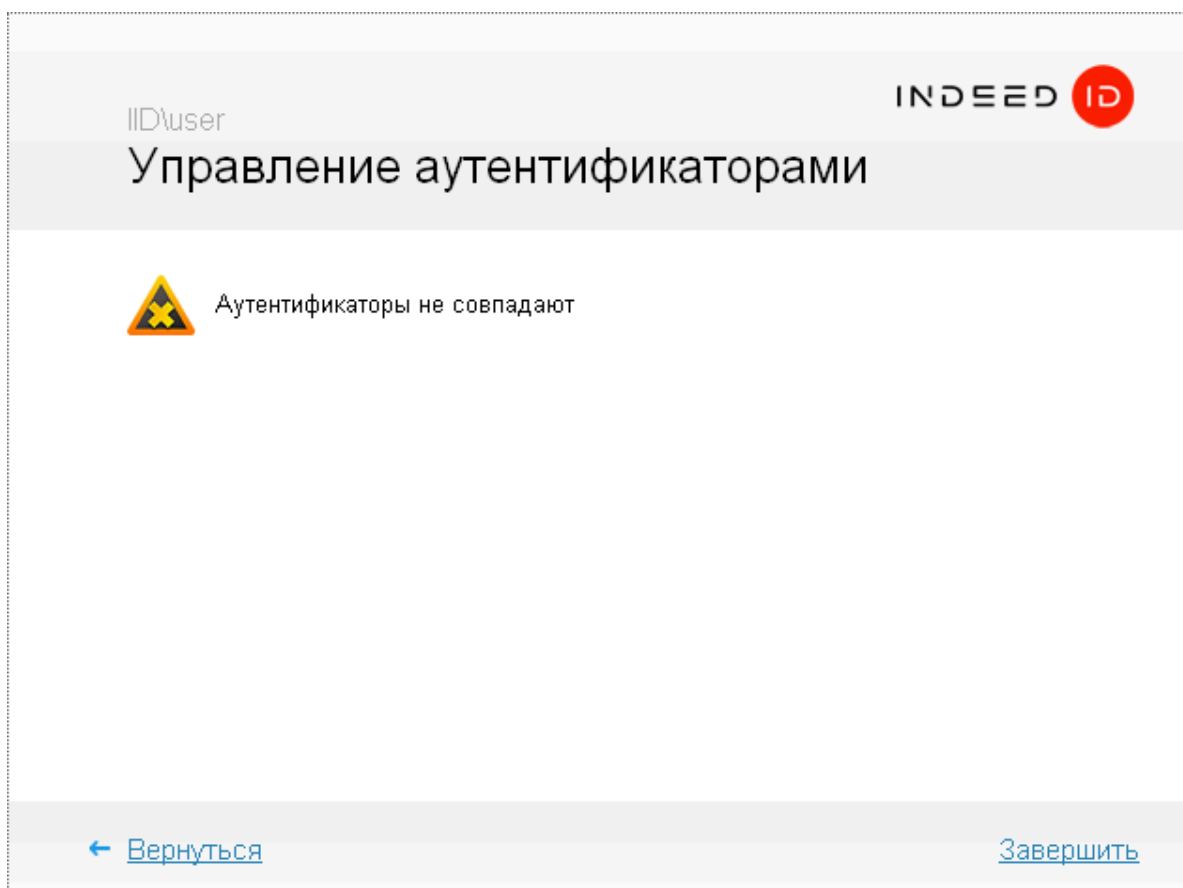
1. В окне Управление аутентификаторами выберите аутентификатор и нажмите Проверить.



2. Далее в окне Управление аутентификаторами отображаются инструкции по регистрации аутентификатора. Внешний вид окна и текст подсказок зависят от выбранного типа аутентификатора. Выполните требуемые действия.
3. После завершения проверки в окне Управление аутентификаторами отображается сообщение о результате.
  - Если аутентификаторы совпадают;



- Если аутентификаторы не совпадают;



4. Если аутентификаторы не совпадают, нажмите Вернуться и повторите процедуру проверки или заново обучите аутентификатор.



# Редактирование аутентификатора

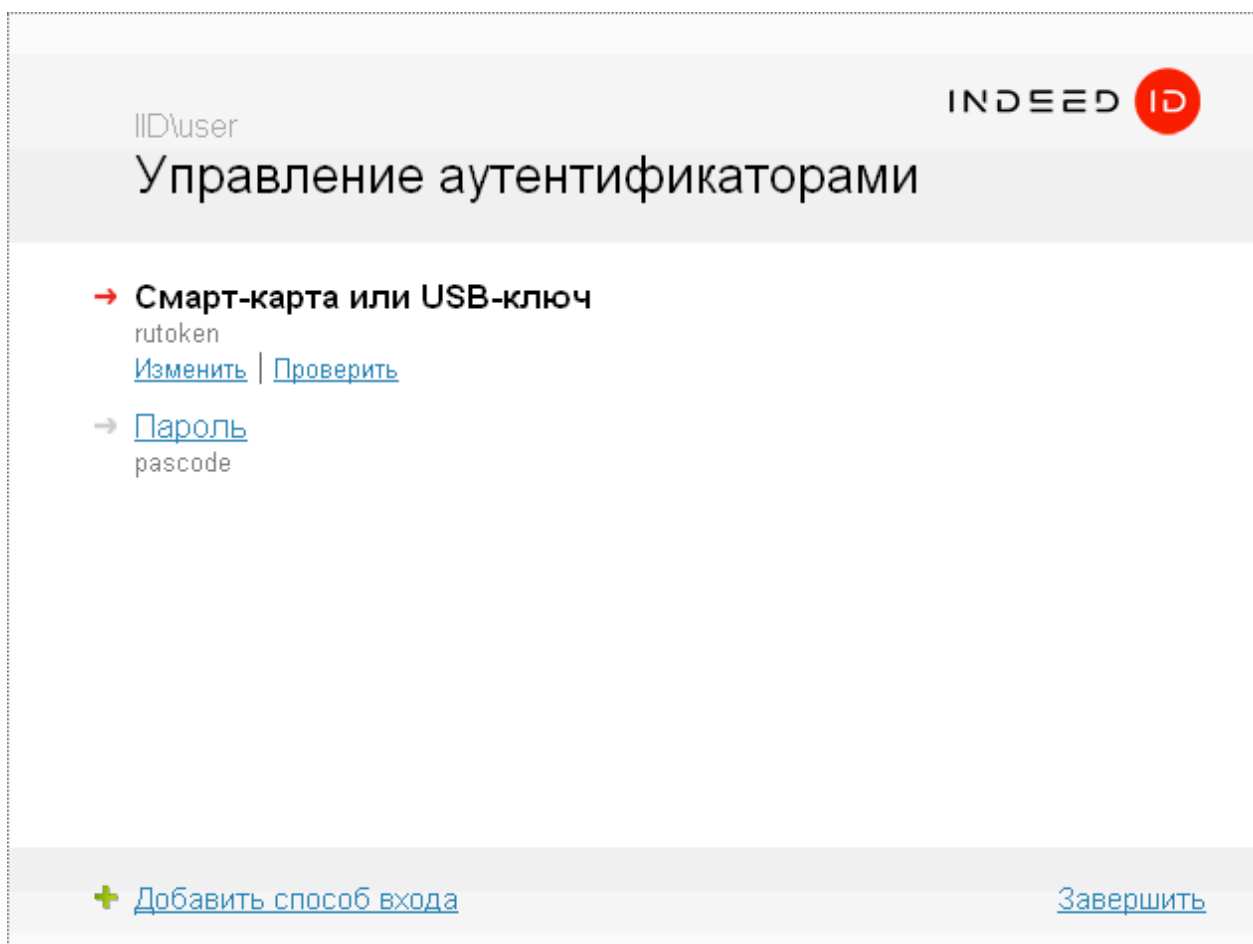
## ВАЖНО!

Доступные действия:

- отредактировать (повторно зарегистрировать) аутентификатор;
- изменить только комментарий к аутентификатору (если это действие разрешено администратором системы).

Для редактирования аутентификатора выполните следующие действия:

1. В окне Управление аутентификаторами выберите аутентификатор и нажмите Изменить.



2. Выполните одно из указанных действий:

- Чтобы отредактировать только комментарий к аутентификатору, введите комментарий в соответствующее поле и нажмите Сохранить.

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. Далее 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

INDEED ID

## Управление аутентификаторами



[Задать заново](#) →

Вы можете изменить комментарий к аутентификатору:

rutoken

Сохранить

← [Вернуться](#)

[Завершить](#)

IID\user

INDEED ID

## Управление аутентификаторами



Выберите смарт-карту или токен

Rutoken S : 0783311828

▼

Ok

[← Вернуться](#)[Завершить](#)

3. После успешной регистрации аутентификатора нажмите Сохранить.

IID\user

INDEED ID

## Управление аутентификаторами



[Задать заново](#) →

Вы можете изменить комментарий к аутентификатору:

rutoken

Сохранить

[← Вернуться](#)[Завершить](#)



# Удаление аутентификатора

Для удаления аутентификатора в окне Управление аутентификаторами выберите аутентификатор и нажмите Удалить. Для подтверждения действия нажмите Да.

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](#)



#### СОВЕТ

Если вы удалили все аутентификаторы и не можете выполнить вход в систему по паролю, обратитесь к администратору системы. После сброса пароля вы снова сможете выполнить вход в систему и зарегистрировать новые аутентификаторы.

После удаления всех аутентификаторов вход в систему может быть выполнен только по паролю. Если для вашей учетной записи был сгенерирован случайный пароль, вход в систему станет невозможен.

# Установка и настройка провайдеров аутентификации



## Indeed Key Provider

Одноразовый пароль и push-уведомления в приложении Indeed Key



## Indeed AM Telegram Provider

Одноразовый пароль и push-уведомления в приложении Telegram



## Indeed AM Secured TOTP Provider

Одноразовый пароль на основе идентификатора устройства



## Indeed AM Software OTP Provider

Одноразовый пароль в дополнение к своему логину и паролю



## Indeed AM Hardware OTP Provider

Аутентификация по Hardware OTP от eToken PASS



## Indeed AM Hardware TOTP Provider

Аутентификация по TOTP от eToken PASS



## Indeed AM SMS OTP Provider

Количество глав: 2





## Indeed AM Storage SMS OTP Provider

Аутентификация по номерам телефонов из базы Microsoft SQL



## Indeed AM Email OTP Provider

Одноразовый пароль по электронной почте



## Indeed AM Windows Password Provider

Аутентификация по паролю Windows



## Indeed AM Passcode Provider

Аутентификация по заданному паролю



## Indeed AM MFA Provider

Многофакторная аутентификация



## Indeed AM Smart Card Provider

Аутентификация по смарт-картам и USB-ключам



## Indeed AM IronLogic Z2USB Provider

Аутентификация с помощью считывателя IronLogic Z-2 USB



## Indeed AM OMNIKEY Provider

Аутентификация с помощью смарт-карт HID OMNIKEY



## Indeed AM Futronic Provider

Аутентификация с помощью биометрического сканера



## Миграция настроек провайдеров

Перенос настроек провайдеров в Management Console

# Indeed Key Provider

Для аутентификации с помощью push-уведомлений есть следующие требования:

- В сетевой инфраструктуре:
  - **Установка сервера Indeed Key Server.** Данный сервер выполняет отправку уведомлений на смартфон пользователя с помощью сервисов API Google.
  - Установка провайдера аутентификации Indeed Key. Установка провайдера позволит использовать данную технологию аутентификации в целевых сценариях.
- На стороне клиента:
  - Установка приложения Indeed Key. Приложение необходимо для получения уведомлений об аутентификации в целевых приложениях с помощью компонентов Indeed Access Manager.

Без установки Indeed Key Server, Indeed Key Provider и приложения Indeed Key аутентификация с помощью push-уведомлений невозможна.

Indeed Key Provider может быть использован для аутентификации в следующих модулях:

- **Identity Provider,**
- **Windows Logon,**
- **Enterprise SSO,**
- **ADFS Extension,**
- **NPS Radius Extension** (только в режиме отправки push-уведомлений с подтверждением входа),
- **IIS Extension** (только в режиме отправки push-уведомлений с подтверждением входа),
- **RDP Windows Logon** (только в режиме отправки push-уведомлений с подтверждением входа).

Идентификатор провайдера

{DEEF0CB8-AD2F-4B89-964A-B6C7ECA80C68}

# Установка провайдера Indeed Key

Чтобы установить провайдер:

1. Запустите файл для установки, расположенный по пути *Indeed AM <номер версии>/Indeed AM Providers/Indeed AM Providers/Indeed Key Provider*, и следуйте шагам мастера установки. Установить провайдер нужно как на компьютере с установленным Core Server, так и на клиентском компьютере.



## ВАЖНО

Если в инфраструктуре используется несколько Core Server, то установку провайдера необходимо выполнить на всех серверах инфраструктуры.

При использовании провайдера в клиентских сценариях с Indeed AM Windowsl Logon и ESSO Agent выполните 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 Indeed Key в Management Console

Для настройки Indeed Key в Management Console в разделе Конфигурация→Аутентификаторы выберите аутентификатор Indeed Key.

### Права доступа

Чтобы выдать или отозвать права на использование аутентификатора, выполните следующее:

1. В секции Основные настройки выполните следующие настройки:
  - В настройке Запретить использовать укажите, может ли пользователь использовать или регистрировать выбранный аутентификатор.
2. В секции Доступные пользователю действия выполните следующие настройки:
  - В настройке Регистрация новых аутентификаторов укажите, может ли пользователь регистрировать новые аутентификаторы;

- В настройке Редактирование имеющихся аутентификаторов укажите, может ли пользователь изменять уже зарегистрированные аутентификаторы;
- В настройке Удаление имеющихся аутентификаторов укажите, может ли пользователь удалять уже зарегистрированные аутентификаторы;
- В настройке Разрешить редактирование комментария к аутентификатору укажите, в какой момент пользователь может редактировать комментарии к уже зарегистрированным аутентификаторам.

## Блокировка аутентификатора

Чтобы заблокировать аутентификатор, в секции Настройки блокировки аутентификатора выполните следующие настройки:

1. Разрешите или заблокируйте использование Indeed Key в случае серии неудачных попыток аутентификации.
2. В поле Количество попыток аутентификации до блокировки укажите, сколько раз пользователь может совершить неудачную аутентификацию до блокировки способа аутентификации.
3. В поле Сброс счетчика блокировки укажите, сколько минут должно пройти после неудачной попытки аутентификации, прежде чем сбросится счетчик.
4. В поле Таймаут до разблокировки способа входа укажите, через сколько минут заблокированный способ аутентификации станет вновь доступным.

## Настройки мобильного приложения

Чтобы настроить мобильное приложение Indeed Key, в секции Настройки мобильного приложения выполните следующие настройки:

1. В поле Отображаемое имя сервера укажите название сервера Indeed Key, которое будет отображаться в мобильном приложении.
2. В настройке Способ подтверждения Push выберите, как у пользователя будет запрашиваться подтверждение входа:
  - Подтверждение не требуется — у пользователя не будет запрашиваться дополнительная аутентификация на устройстве;
  - Подтверждение биометрическими средствами — у пользователя будет запрашиваться дополнительная аутентификация на устройстве с помощью биометрии;

- Подтверждение любыми средствами, доступными на устройстве — у пользователя будет запрашиваться дополнительная аутентификация на устройстве с помощью любого доступного на устройстве метода;
3. В настройке Отображать одноразовый пароль в мобильном приложении для новых аутентификаторов укажите, будет ли отображаться одноразовый код в карточке аутентификатора в приложении. По умолчанию одноразовый код скрыт.
  4. В настройке Способ подтверждения для отображения ОТР выберите, как пользователь будет подтверждать право просматривать одноразовые коды:
    - Подтверждение не требуется — у пользователя не будет запрашиваться дополнительная аутентификация на устройстве;
    - Подтверждение биометрическими средствами — у пользователя будет запрашиваться дополнительная аутентификация на устройстве с помощью биометрии;
    - Подтверждение любыми средствами, доступными на устройстве — у пользователя будет запрашиваться дополнительная аутентификация на устройстве с помощью любого доступного на устройстве метода;
  5. В поле Время отображения ОТР укажите, в течение какого времени будет актуален одноразовый пароль. Значение указывается в секундах.
  6. В настройке Режим работы Indeed Key выберите, какой способ подтверждения входа будет использоваться в приложении:
    - Push — пользователь будет получать push-уведомления с возможностью отклонить или подтвердить вход.
    - ОТР — вместо push-уведомлений пользователь получит одноразовый код.

## Серверные настройки

Чтобы настроить сервер, к которому обращается приложение Indeed Key, в секции Серверные настройки выполните следующие настройки:

1. В поле URL-адрес Indeed Key Server укажите адрес, по которому сервер Indeed Key доступен с машины Indeed AM;
2. В поле Доверенный ID Indeed Key Server укажите произвольный уникальный идентификатор. Этот идентификатор необходим для подтверждения удаления аутентификатора. Значение идентификатора должно совпадать со значением, указанным в конфигурационном файле Indeed Key Server (тег `trustedClients`).

## Настройки одноразового пароля

Чтобы настроить генерацию одноразового пароля, в секции Настройки OTP выполните следующие настройки:

1. В поле Период обновления OTP укажите, на протяжении какого времени будет актуален одноразовый пароль.
2. В настройке Окно сравнения укажите, сколько периодов обновления должно пройти, пока одноразовый пароль не будет считаться недействительным.
3. В настройке Формат имени пользователя выберите, в каком формате будет отображаться имя пользователя в приложении. Значение по умолчанию — *Name*.
4. В настройке Алгоритм генерации OTP-кода выберите, по какому алгоритму будет генерироваться одноразовый пароль.
5. В настройке Количество цифр в OTP-коде выберите, сколько цифр будет содержать одноразовый пароль.

## Регистрация аутентификатора Indeed Key по ссылке

Для регистрации аутентификатора Indeed Key по ссылке из письма необходимы следующие условия:

- установленный и настроенный провайдер Email OTP,
- заполненный email пользователя в каталоге Active Directory.

Ссылка отправляется на электронный адрес, указанный для пользователя в каталоге Active Directory.

Чтобы зарегистрировать Indeed Key по ссылке:

1. В разделе Конфигурация→Аутентификаторы, в секции Настройки регистрации выполните следующие настройки:
  - а. В настройке Способ регистрации аутентификатора выберите способ регистрации по ссылке из электронного письма.
  - б. Далее укажите следующее:
    - В поле Тема уведомления укажите заголовок письма для регистрации.
    - В поле Сообщение укажите тело письма.
    - В поле Текст ссылки укажите текст для ссылки, по которой перейдет пользователь для регистрации аутентификатора.

- При необходимости **укажите адрес сервера, участвующий в формировании ссылки.**

Если поле оставить пустым, используется ссылка по умолчанию в зависимости от локали Indeed AM.

2. Далее перейдите в раздел Пользователи, выберите пользователя, затем выберите вкладку Аутентификаторы.

3. Нажмите кнопку Зарегистрировать и выберите из списка Indeed Key.

После этого пользователю отправляется письмо со ссылкой на регистрацию аутентификатора. Как только письмо отправлено, в Management Console и User Console добавляется аутентификатор Indeed Key в статусе *Ожидает*. По ссылке пользователь перейдет в приложение Indeed Key, где начнется регистрация аутентификатора.

После того как пользователь успешно прошел регистрацию в приложении, администратор в Management Console должен нажать на значок обновления статуса и далее нажать Сохранить. Статус *Ожидает* поменяется на *Действующий*, а аутентификатор будет готов к использованию.

Если у пользователя возникли ошибки во время регистрации Indeed Key, то после обновления статуса в Management Console статус *Ожидает* поменяется на *Ошибка*. Удалите аутентификатор и снова пройдите процедуру регистрации.

## Регистрация аутентификатора Indeed Key по QR-коду

Чтобы зарегистрировать Indeed Key по QR-коду:

1. В разделе Доступные пользователю действия разрешите пользователю регистрировать новые аутентификаторы.
2. В настройке Способ регистрации аутентификатора выберите способ регистрации аутентификатора по QR-коду.

В User Console у пользователя в списке доступных аутентификаторов появится Indeed Key.

Пользователю нужно выполнить следующие действия:

1. Нажать значок шестеренки.
2. Нажать кнопку Зарегистрировать.
3. Откройте приложение Indeed Key, нажмите значок +.
4. Сканируйте появившийся QR-код.



## Конфигурация ссылки на регистрацию и скачивание Indeed Key

Ссылку на регистрацию аутентификатора и скачивание приложения Indeed Key можно задать вручную. Для этого:

1. Перейдите в раздел Конфигурация→Аутентификаторы в секцию Настройки регистрации.
2. В настройке Адрес сервера, участвующий в формировании ссылки на регистрацию аутентификатора (диплинк) укажите ссылку для регистрации, отправляемую по email.

Доступны следующие ссылки для регистрации (в скобках указано местонахождение сервера):

- <https://indeedkey.drru.agconnect.link> (Россия)
- <https://indeedkey.dre.agconnect.link> (Германия)
- <https://indeedkey.drcn.agconnect.link> (Китай)
- <https://indeedkey.dra.agconnect.link> (Сингапур)

3. В секции Дополнительные настройки укажите ссылку для скачивания Indeed Key.

Доступны следующие ссылки для скачивания (в скобках указано местонахождение сервера):

- <https://indeedkey.drru.agconnect.link/XwZr> (Россия)
- <https://indeedkey.dre.agconnect.link/MJyW> (Германия)
- <https://indeedkey.drcn.agconnect.link/NDbK> (Китай)
- <https://indeedkey.dra.agconnect.link/i1RD> (Сингапур)

## Защита от спама

Механизм защиты от спама основан на расчете процента успешных аутентификаций относительно всех отправленных сообщений за указанный интервал времени. При этом расчет запускается, только если количество отправленных сообщений превышает количество, заданное вами в настройке Окно оценки.

При обнаружении спам-атаки дальнейшая отправка сообщений блокируется на заданный период времени, а при попытке входа возникает ошибка *Potential spam attack detected*.

Отправка сообщений возобновляется либо по истечении заданного периода, либо по достижении определенного количества (в процентном отношении) успешных аутентификаций.

Чтобы настроить защиту от спама, выполните следующее:

1. В Management Console в разделе Конфигурация→Аутентификаторы выберите аутентификатор.
2. В секции Настройки защиты от спама выполните следующие настройки:
  - включите или отключите защиту от спама;
  - в поле Окно оценки попыток аутентификации укажите, в течение какого времени будет выполняться расчет процента успешных попыток входа;
  - в поле Пороговое окно попыток аутентификации укажите, сколько попыток входа должно производиться за время, указанное в окне оценки попыток аутентификации;
  - в поле Процент успешных попыток аутентификации укажите минимальный процент успешных входов относительно всех отправленных сообщений.

#### ▼ Пример

Настройка включена со следующими значениями:

- Окно оценки попыток аутентификации — 600
- Пороговое окно попыток аутентификации — 20
- Процент успешных попыток аутентификации — 85

Защита от спама включится, если произойдет 21 попытка входа (отправлено 21 сообщение). Произойдет блокировка аутентификатора на 600 секунд.

Аутентификатор разблокируется в одном из случаев:

- процент успешных входов (пользователь успешно ввел одноразовый пароль из сообщения) достигнет значения 85;
- прошло 600 секунд с момента блокировки.

#### ⓘ ИНФОРМАЦИЯ

События лог-сервера:

- 2090: Обнаружена потенциальная спам-атака. Отправка сообщений приостановлена.
- 1118: Отправка сообщений пользователям возобновлена.

# Настройка доверенного идентификатора для Indeed Key Server

По умолчанию при удалении аутентификатора в User Console, в утилите управления аутентификаторами или в консоли администратора аутентификатор будет удален из системы без уведомлений и продолжит отображаться в приложении.

Чтобы настроить push-уведомления с информацией об удалении аутентификатора и удалением в приложении:

1. Откройте конфигурационный файл Indeed Key Server *Web.config* из папки *C:\inetpub\wwwroot\airkeycloud*.
2. Добавьте в файл следующие теги после блока `appSettings`:

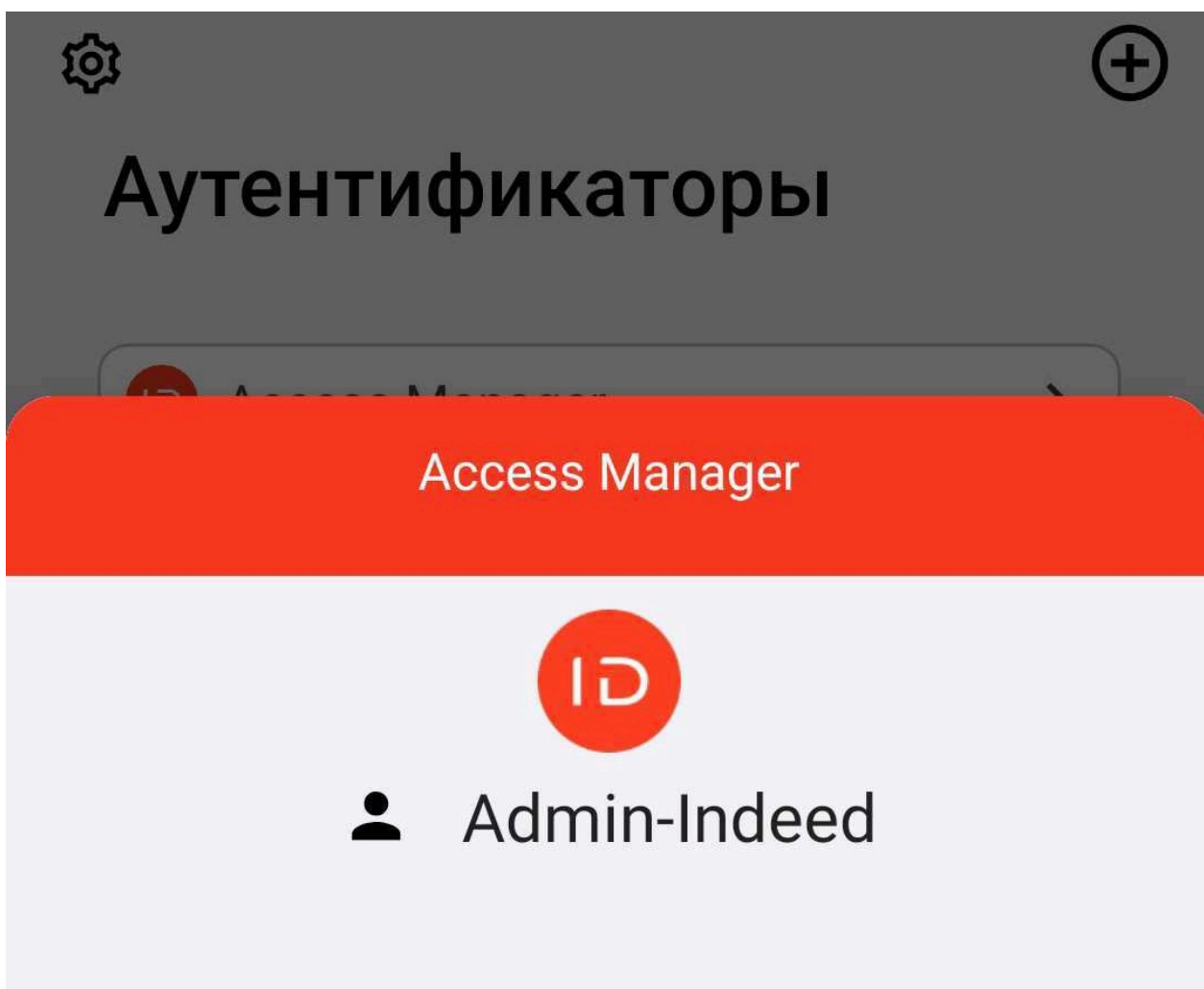
## ⚠ ПРИМЕЧАНИЕ

В параметре `id` тега `add` введите уникальный идентификатор, указанный в пункте Доверенный ID Indeed Key Server в Management Console.

### Пример

```
<trustedClientsSettings>
  <trustedClients>
    <add id="уникальный идентификатор, заданный при
конфигурировании Indeed Key Server" />
  </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 Indeed Key на смартфоне

Приложение Indeed Key доступно для смартфонов с iOS 13.0 и выше, Android 7.0 и выше.

Корректная работа приложения Indeed Key гарантируется, только если оно скачано из официальных магазинов приложений. Чтобы скачать или обновить приложение, воспользуйтесь следующими ссылками:

- [App Store](#)
- [Google Play](#)
- [Huawei AppGallery](#)
- [RuStore](#)



## ВАЖНО!

Чтобы обновить приложение, скачивайте обновление в том же магазине, где вы устанавливали предыдущую версию.

### ▼ Примечание для владельцев Android-устройств

Для корректной работы push-уведомлений на Android-устройствах убедитесь, что выполнены следующие обязательные требования:

- Вы разрешили приложению отправку уведомлений;
- На устройствах с Android 9 и выше отключите режим энергосбережения.

Примечание: корректная работа push-уведомлений возможна не на всех модификациях Android.

1. Откройте приложение. В панели Аутентификаторы нажмите значок + для добавления аутентификатора.
2. Разрешите приложению доступ к камере и отсканируйте QR-код.
3. Подтвердите регистрацию аутентификатора, нажав кнопку Подтвердить.
4. После успешной регистрации аутентификатор будет отображаться на главном окне программы.

Для удаления выберите необходимый аутентификатор и нажмите Удалить аутентификатор.

#### ⓘ ДОПОЛНИТЕЛЬНЫЕ НАСТРОЙКИ

Для машин с установленными компонентами Indeed AM Windows Logon и Indeed AM ESSO Agent выполните настройку параметров аутентификации с помощью групповых политик.

# Indeed AM Telegram Provider

Indeed AM Telegram Provider предназначен для аутентификации пользователей с помощью следующих технологий:

- одноразовые пароли;
- push-уведомления с запросом подтвердить или отклонить вход.

Одноразовые пароли и push-уведомления пользователи получают через бота в мессенджере Telegram.

Telegram Provider может быть использован для аутентификации в следующих модулях:

- **Identity Provider**,
- **ADFS Extension**,
- **NPS Radius Extension** (только в режиме отправки одноразовых паролей),
- **IIS Extension** (только в режиме отправки одноразовых паролей),
- **Windows Logon** (только в режиме отправки одноразовых паролей).



## ПРИМЕЧАНИЕ

Для работы компонента требуется доступ к серверам Telegram для сервисной службы и для провайдера.

Идентификатор провайдера

{CA4645CC-5896-485E-A6CA-011FCC20DF1D}

## Предварительная настройка

Чтобы настроить Telegram Provider:

1. **Установите** провайдер.
2. **Установите** сервисную службу.
3. **Настройте** атрибут с номером телефона.
4. **Создайте** бот в приложении Telegram.

5. **Настройте** сервисную службу.
6. **Задайте** настройки в Management Console.
7. **Зарегистрируйте** аутентификатор.

## Установить провайдер

1. Запустите файл для установки, расположенный по пути *Indeed AM <номер версии>/Indeed AM Providers/Indeed AM Telegram OTP Provider/<номер версии>*.

### ВАЖНО

Если в инфраструктуре используется несколько Core Server, установите провайдер на всех серверах инфраструктуры.

2. После завершения установки компонента нужно перезагрузить систему. В окне мастера установки нажмите Да, чтобы выполнить перезагрузку сразу, или Нет, чтобы сделать это позднее вручную.

## Установить сервисную службу

1. Запустите файл *IndeedId.Telegram.Service-<номер версии>.x86.ru-ru.msi*, расположенный по пути *Indeed AM <номер версии>/Indeed AM Providers/Indeed AM Telegram OTP Provider/*.
2. После завершения установки компонента нужно перезагрузить систему. В окне мастера установки нажмите Да, чтобы выполнить перезагрузку сразу, или Нет, чтобы сделать это позднее вручную.

## Настроить атрибут с номером телефона

Чтобы использовать провайдер, задайте номер телефона в атрибуте пользователя Active Directory. По умолчанию это атрибут `telephoneNumber`. Также можно настроить любой другой атрибут. Если номер не задан, использовать провайдер будет невозможно.





## ВАЖНО

Прежде чем приступить к настройке атрибута, обязательно расшифруйте и создайте резервную копию конфигурационного файла Core Server `inetpub/wwwroot/am/core/Web.config`.

Чтобы настроить атрибут с номером телефона:

### Через мастер конфигурации

1. Запустите мастер конфигурации на компьютере с установленным Core Server: *Пуск → Indeed Identity → Мастер конфигурации Indeed AM*.
2. Перейдите на вкладку Каталоги пользователей.
3. Выберите каталог.
4. Нажмите Изменить.
5. Появится предупреждение, что если уменьшить область действия каталога или изменить домен, данные пользователей станут недоступны. Если вы уже расшифровали и сделали резервную копию файла `inetpub/wwwroot/am/core/Web.config`, нажмите ОК.
6. В мастере конфигурации нажмите Настроить соответствие атрибутов.
7. В поле Phone введите название атрибута пользователя в Active Directory, в котором указан номер телефона, например атрибут *mobile*.
8. Дважды нажмите Сохранить.
9. Перейдите на вкладку Подтверждение и нажмите Применить.
10. После завершения настройки конфигурационного файла и проверки работоспособности закройте мастер.

### Через конфигурационный файл

1. Откройте конфигурационный файл Core Server `inetpub/wwwroot/am/core/Web.config`.
2. В раздел `adUserCatalogProvider` добавьте:

```

        <userMapRules>
            <adObjectMapRule attribute="Phone"
adAttribute="название_атрибута_в_Active_Directory"/>
            <objectTypeSettings>
                <objectSetting category="person"
class="user"></objectSetting>
            </objectTypeSettings>
        </userMapRules>

```

где:

- `attribute="Phone"` — название атрибута в Access Manager;
- `adAttribute="название_атрибута_в_Active_Directory"` — название соответствующего атрибута в Active Directory, откуда будет браться значение номера телефона.

#### Пример

```

<adUserCatalogProvider id="userId" serverName="ind.loc"
containerPath="DC=ind,DC=loc" userName="userAdmin"
password="Q1q2E3e4">
    <userMapRules>
        <adObjectMapRule attribute="Phone"
adAttribute="mobile"/>
        <objectTypeSettings>
            <objectSetting category="person"
class="user"></objectSetting>
        </objectTypeSettings>
    </userMapRules>
</adUserCatalogProvider>

```

## Создать бот

1. Откройте приложение Telegram, найдите специального бота @botfather и откройте диалог с ботом.
2. Нажмите Start и отправьте команду `/newbot`.
3. Укажите имя создаваемого бота. Данное название будет отображаться в окне диалога с ботом. Введите любое имя, например *IndeedOTP*.
4. Укажите имя пользователя для аккаунта с ботом с *bot* в конце, например *IndeedOTP\_bot*. Данное имя пользователя используется для ссылок на бота.
5. При успешной регистрации отобразится токен для доступа к API. Данный токен потребуется для настройки **службы AM Telegram Service** и **бота в Management Console**.

## Настроить сервисную службу

Для настройки службы нужен сервисный пользователь с правами **глобального администратора** Indeed AM. От имени этого пользователя будут регистрироваться аутентификаторы. В целях безопасности рекомендуется создать в Active Directory отдельного пользователя для регистрации Telegram Provider.

Чтобы настроить службу Telegram Service:

1. Откройте конфигурационный файл службы *AM.Telegram.Service.exe.config*, расположенный по пути *C:\Program Files(x86)\Indeed-Id\Indeed-Id Telegram Service*.

Чтобы сохранить изменения в конфигурационном файле, запустите редактор с правами администратора.

2. В разделе `appSettings` задайте значения в параметрах `value` для соответствующих параметров `key`:

|                          |                                                                                               |
|--------------------------|-----------------------------------------------------------------------------------------------|
| <code>culture</code>     | Язык локализации, поддерживается русский и английский. Значение по умолчанию — <i>ru-RU</i> . |
| <code>EAWebAPIURL</code> | URL-адрес Core Server                                                                         |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| username | Имя сервисного пользователя с правами глобального администратора, от имени которого будут регистрироваться аутентификаторы.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| password | Пароль сервисного пользователя.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| lognames | <p>Формат логирования имен пользователей. Значение по умолчанию — <i>Name</i>.</p> <div> <p>▼ Поддерживаемые форматы</p> <hr/> <ul style="list-style-type: none"> <li>• <b>Id</b> — идентификатор пользователя в системе Indeed AM в формате <i>rootUserCatalogProviderId_Guid</i>;</li> <li>• <b>Name</b> — значение атрибута <b>name</b> из Active Directory;</li> <li>• <b>CanonicalName</b> — имя пользователя в формате <i>CanonicalName(myserver.demo.local/users/UserName)</i>;</li> <li>• <b>PrincipalName</b> — значение атрибута <b>userPrincipalName</b> из Active Directory;</li> <li>• <b>SamCompatibleName</b> — имя пользователя в формате <i>domainName\UserName</i>;</li> <li>• <b>DistinguishedName</b> — значение атрибута <b>distinguishedName</b> из Active Directory;</li> <li>• <b>Sid</b> — значение атрибута <b>objectSid</b> из Active Directory;</li> <li>• <b>Email</b> — значение атрибута <b>mail</b> из Active Directory или значение, указанное в конфигурационном файле Core Server;</li> <li>• <b>Phone</b> — значение атрибута <b>telephoneNumber</b> из Active Directory или значение, указанное в конфигурационном файле сервера.</li> </ul> </div> <p>Пример:</p> <pre>add key="lognames" value="PrincipalName,Sid"</pre> |
| botId    | Токен, полученный <b>при создании бота в Telegram</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

trustedId

Произвольный уникальный идентификатор. Значение идентификатора должно совпадать с тем, что указано в настройке *Доверенный ID Telegram Service* в **Management Console**.

▼ Пример отредактированного раздела **appSettings**

```
<appSettings>
  <add key="culture" value="ru-RU" />
  <add key="EWebAPIURL "
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_feYYQ0fbPddK_2Z_JDiKQ" />
  <add key="trustedId" value="уникальный идентификатор,
заданный при конфигурировании Telegram Service" />
</appSettings>
```

3. В разделе **logServer** укажите значения следующих параметров:

- в параметре **URL** укажите URL для подключения к Log Server в формате *http(s)://полноеднsumя\_сервера/ls/api*;
- если закрытый ключ в реестре, а сертификат в хранилище компьютера, укажите отпечаток сертификата в параметре **CertificateThumbprint**;
- если ключевая пара в pfx, укажите путь в параметре **CertificateFilePath** и пароль от pfx в параметре **CertificateFilePassword**.

Пример

```
<logServer Url="https://logserver.indeed.local/ls/api/"
CertificateThumbprint="ВАШ_ОТПЕЧАТОК_СЕРТИФИКАТА"
CertificateFilePath="ПУТЬ_К_PFX"
CertificateFilePassword="ПАРОЛЬ_ОТ_PFX" />
```

4. Сохраните изменения.

5. Запустите службу AM Telegram Service.

#### ▼ Как запустить службу

1. Запустите диспетчер задач.
2. В открывшемся окне нажмите Подробнее и перейдите на вкладку Службы.
3. Найдите в списке AM Telegram Service, нажмите правой кнопкой мыши и выберите Запустить.



#### ПРИМЕЧАНИЕ

Если вы используете несколько Core Server, одновременно можно запустить службу только на одном из серверов.

## Задать настройки в Management Console

Для корректной работы провайдера задайте остальные настройки в Management Console. Для этого:

1. На боковой панели Management Console откройте раздел Конфигурация
2. Перейдите на вкладку Аутентификаторы.
3. Выберите аутентификатор Telegram.
4. При необходимости задайте **общие настройки**.
5. В секции Настройки Telegram Service укажите произвольный уникальный идентификатор. **Значение идентификатора** должно совпадать с тем, что указано в конфигурационном файле

службы *AM.Telegram.Service.exe.config*.

6. В секции Режим работы выберите режим работы провайдера — *Push* или *OTP*.

7. В секции Настройки бота:

- В поле Идентификатор бота укажите токен, полученный **при создании бота в Telegram**.
- В поле Шаблон для сообщения настройте вид сообщения. Сообщение может содержать одноразовый код для входа в приложение, название приложения, имя пользователя, дата и время входа, IP-адрес компьютера, с которого выполняется вход.

8. Если планируется использовать Telegram Provider в режиме отправки одноразовых паролей, в секции Настройки генерации одноразового пароля:

- В поле Длина одноразового пароля укажите, сколько символов будет содержать одноразовый пароль.
- В настройке Цифры укажите, будет ли одноразовый пароль содержать цифры.
- В настройке Строчные латинские буквы укажите, будет ли одноразовый пароль содержать строчные латинские буквы;
- В настройке Прописные латинские буквы укажите, будет ли одноразовый пароль содержать прописные латинские буквы;
- В настройке Специальные символы укажите, будет ли одноразовый пароль содержать специальные символы.

9. При необходимости выполните следующие настройки:

#### ▼ Настройте работу Telegram Provider через прокси

---

В секции Настройки бота:

- В настройке Использовать прокси выберите *Да*. По умолчанию выбрано *Нет*.
- В поле Адрес прокси укажите адрес прокси-сервера.

## ▼ Настройте защиту от спама

---

Механизм защиты от спама основан на расчете процента успешных аутентификаций относительно всех отправленных сообщений за указанный интервал времени. При этом расчет запускается, только если количество отправленных сообщений превышает количество, заданное вами в настройке Окно оценки.

При обнаружении спам-атаки дальнейшая отправка сообщений блокируется на заданный период времени, а при попытке входа возникает ошибка *Potential spam attack detected*.

Отправка сообщений возобновляется либо по истечении заданного периода, либо по достижении определенного количества (в процентном отношении) успешных аутентификаций.

Чтобы настроить защиту от спама, выполните следующее:

1. В Management Console в разделе Конфигурация→Аутентификаторы выберите аутентификатор.
2. В секции Настройки защиты от спама выполните следующие настройки:
  - включите или отключите защиту от спама;
  - в поле Окно оценки попыток аутентификации укажите, в течение какого времени будет выполняться расчет процента успешных попыток входа;
  - в поле Пороговое окно попыток аутентификации укажите, сколько попыток входа должно производиться за время, указанное в окне оценки попыток аутентификации;
  - в поле Процент успешных попыток аутентификации укажите минимальный процент успешных входов относительно всех отправленных сообщений.



### ▼ Пример

Настройка включена со следующими значениями:

- Окно оценки попыток аутентификации — 600
- Пороговое окно попыток аутентификации — 20
- Процент успешных попыток аутентификации — 85

Защита от спама включится, если произойдет 21 попытка входа (отправлено 21 сообщение). Произойдет блокировка аутентификатора на 600 секунд.

Аутентификатор разблокируется в одном из случаев:

- процент успешных входов (пользователь успешно ввел одноразовый пароль из сообщения) достигнет значения 85;
- прошло 600 секунд с момента блокировки.

### ⓘ ИНФОРМАЦИЯ

События лог-сервера:

- 2090: Обнаружена потенциальная спам-атака. Отправка сообщений приостановлена.
- 1118: Отправка сообщений пользователям возобновлена.

## Зарегистрировать аутентификатор

### ⓘ ПРИМЕЧАНИЕ

При регистрации провайдера пользователь получит запрос номера телефона из аккаунта Telegram. Необходимо, чтобы номер телефона пользователя в Active Directory полностью совпадал и был одного формата. Поддерживаемые форматы: +7xxxxxxxxxx или 8xxxxxxxxxx.

1. Откройте чат с созданным ботом. Для этого введите в поисковой строке мессенджера имя вашего бота либо перейдите по ссылке из сообщения BotFather.
2. Нажмите Start.
3. Введите команду `/register`.
4. Введите номер телефона аккаунта Telegram.
5. При успешной регистрации аутентификатора отобразится сообщение *Вы были успешно зарегистрированы*.

# Indeed AM Secured TOTP Provider

Indeed AM Secured TOTP — это провайдер с привязкой к идентификатору устройства пользователя.

Секретный ключ для генерации одноразового кода зашифрован и расшифровывается только ключом на основе идентификатора устройства. Таким образом, регистрация конкретного аутентификатора возможна лишь на одном устройстве.

Secured TOTP может быть использован для аутентификации в следующих модулях:

- [Identity Provider](#),
- [ADFS Extension](#),
- [NPS RADIUS Extension](#),
- [RDP Windows Logon](#),
- [Windows Logon](#),
- [Enterprise SSO](#).

## Предварительные требования

Для работы провайдера необходимы следующие условия:

- установлен провайдер Secured TOTP,
- установлено мобильное приложение Indeed Key версии 2.6 и выше,
- для регистрации Secured TOTP по ссылке из письма необходимы:
  - установленный и настроенный провайдер Email OTP,
  - заполненный email пользователя в каталоге Active Directory.

Идентификаторы провайдера для интеграции с модулем NPS Radius Extension

{F15FD7EC-19EA-4384-846E-A2D0BE149FA2} — Secured TOTP

{882C1787-FD32-44A2-BA89-F1F529FBE7AB} — Passcode + Secured TOTP

{7F3DE86F-59D1-4476-AA5D-F277E5DD5938} — Windows Password + Secured TOTP

## Установка провайдера

Выполните установку Indeed AM Secured TOTP через запуск пакета

*IndeedAM.AuthProviders.SecuredTOTP-<номер версии>.<разрядность>.ru-ru.msi* из папки *indeed AM <Номер версии>\Indeed AM Providers\Indeed AM Secured TOTP Provider\<Номер версии>*.



### ВАЖНО

Если в инфраструктуре используется несколько Core Server, то установку провайдера необходимо выполнить на всех серверах инфраструктуры.

После завершения установки может потребоваться перезагрузка системы. Если программа установки предлагает выполнить перезагрузку, подтвердите данное действие.

Удаление/Восстановление продукта осуществляется стандартным для поддерживаемых ОС способом, через меню Панель управления.

## Права доступа

Чтобы выдать или отозвать права на использование аутентификатора, выполните следующее:

1. В Management Console в разделе Конфигурация→Аутентификаторы из списка выберите аутентификатор Secured TOTP.
2. В секции Основные настройки выполните следующие настройки:
  - В настройке Запретить использовать укажите, может ли пользователь использовать или регистрировать выбранный аутентификатор.
3. В секции Доступные пользователю действия выполните следующие настройки:
  - В настройке Регистрация новых аутентификаторов укажите, может ли пользователь регистрировать новые аутентификаторы.
  - В настройке Редактирование имеющихся аутентификаторов укажите, может ли пользователь изменять уже зарегистрированные аутентификаторы.
  - В настройке Удаление имеющихся аутентификаторов укажите, может ли пользователь удалять уже зарегистрированные аутентификаторы.
  - В настройке Разрешить редактирование комментария к аутентификатору укажите, в какой момент пользователь может редактировать комментарии к уже зарегистрированным аутентификаторам.

## Блокировка аутентификатора

Чтобы заблокировать аутентификатор, выполните следующее:

1. В Management Console в разделе Конфигурация→Аутентификаторы из списка выберите аутентификатор Secured TOTP.
2. В секции Настройки блокировки аутентификатора выполните следующие настройки:
  - Разрешите или заблокируйте использование Secured TOTP в случае серии неудачных попыток аутентификации;
  - В поле Количество попыток аутентификации до блокировки укажите, сколько раз пользователь может совершить неудачную аутентификацию до блокировки способа аутентификации;
  - В поле Сброс счетчика блокировки укажите, сколько минут должно пройти после неудачной попытки аутентификации, прежде чем сбросится счетчик;
  - В поле Таймаут до разблокировки способа входа укажите, через сколько минут заблокированный способ аутентификации станет вновь доступным.

## Настройки одноразового пароля

Настройки применяются к серверам Indeed AM и позволяет задать длину и вхождение групп символов при генерации одноразового пароля.

Чтобы настроить генерацию одноразового пароля, выполните следующее:

1. В Management Console в разделе Конфигурация→Аутентификаторы из списка выберите аутентификатор Secured TOTP.
2. В секции Настройки генерации одноразового пароля выполните следующие настройки:
  - В поле Длина одноразового пароля укажите, сколько символов будет содержать одноразовый пароль;
  - В настройке Цифры укажите, будет ли одноразовый пароль содержать цифры;
  - В настройке Строчные латинские буквы укажите, будет ли одноразовый пароль содержать строчные латинские буквы;
  - В настройке Прописные латинские буквы укажите, будет ли одноразовый пароль содержать прописные латинские буквы;
  - В настройке Специальные символы укажите, будет ли одноразовый пароль содержать специальные символы.

# Регистрация в Management Console

Secured TOTP можно зарегистрировать по ссылке из письма или по QR-коду. В Management Console доступны оба способа регистрации.

Для регистрации по ссылке из письма необходимы следующие условия:

- установленный и настроенный провайдер Email OTP,
- установлено мобильное приложение Indeed Key версии 2.6 и выше,
- заполненный email пользователя в каталоге Active Directory.

Ссылка отправляется на электронный адрес, указанный для пользователя в каталоге Active Directory. Опционально вы можете продублировать ссылку на другой электронный адрес, например руководителю сотрудника.

Чтобы зарегистрировать аутентификатор по email, выполните следующее:

1. В Management Console в настройке Способ регистрации аутентификатора в Management Console выберите способ регистрации аутентификатора по email.
2. Укажите текст темы электронного письма.
3. Укажите текст сообщения электронного письма. Ссылка на регистрацию указывается специальным тегом `<regLink>`.
4. Укажите текст ссылки, чтобы заменить написание в явном виде.
5. Далее перейдите в раздел Пользователи, выберите пользователя, выберите вкладку Аутентификаторы.
6. Нажмите кнопку Зарегистрировать и выберите из списка *Secured TOTP*.
7. В открывшемся окне введите идентификатор устройства пользователя. Его можно получить в настройках приложения Indeed Key и скопировать или отправить кнопкой Поделиться. Опционально на этом шаге вы можете указать дополнительные электронные адреса через запятую.
8. Нажмите кнопку Далее. После этого пользователю придет письмо со ссылкой на регистрацию аутентификатора. По ссылке пользователь перейдет в приложение Indeed Key, где начнется регистрация аутентификатора.
9. В Management Console нажмите кнопку Сохранить.

## Конфигурация ссылки на регистрацию Secured TOTP (и скачивание Indeed Key)

Ссылку на регистрацию аутентификатора Secured TOTP и скачивание приложения Indeed Key можно задать вручную.

1. Перейдите в раздел Конфигурация→Аутентификаторы в секцию Настройки регистрации.
2. В настройке Адрес сервера, участвующий в формировании ссылки на регистрацию аутентификатора (диплинк) укажите ссылку для регистрации, отправляемую по email.

Доступны следующие ссылки для регистрации (в скобках указано местонахождение сервера):

- <https://indeedkey.drru.agconnect.link> (Россия)
- <https://indeedkey.dre.agconnect.link> (Германия)
- <https://indeedkey.drcn.agconnect.link> (Китай)
- <https://indeedkey.dra.agconnect.link> (Сингапур)

3. В секции Дополнительные настройки укажите ссылку для скачивания Indeed Key.

Доступны следующие ссылки для скачивания (в скобках указано местонахождение сервера):

- <https://indeedkey.drru.agconnect.link/XwZr> (Россия)
- <https://indeedkey.dre.agconnect.link/MJyW> (Германия)
- <https://indeedkey.drcn.agconnect.link/NDbK> (Китай)
- <https://indeedkey.dra.agconnect.link/i1RD> (Сингапур)

## Принудительная проверка аутентификатора

Для регистрации аутентификатора можно настроить принудительную проверку аутентификатора.

1. Перейдите в раздел Конфигурация→Аутентификаторы и выберите из списка Secured TOTP.
2. В разделе Основные настройки включите принудительную проверку. При регистрации появится дополнительное окно подтверждения для ввода данных аутентификации.
3. Введите полученные данные аутентификации и нажмите Подтвердить.

## Регистрация в User Console

Пользователь может зарегистрировать новый аутентификатор в User Console, если администратор разрешил пользователю регистрировать новые аутентификаторы в настройках Secured TOTP в Management Console.

На устройстве пользователя должно быть установлено приложение Indeed Key 2.6 и выше.

Чтобы зарегистрировать аутентификатор по QR-коду, выполните следующее:

1. В Management Console в разделе Доступные пользователю действия разрешите пользователю регистрировать новые аутентификаторы Secured TOTP.
2. В настройке Способ регистрации аутентификатора в User Console выберите способ регистрации аутентификатора по QR-коду.
3. В User Console у пользователя в списке доступных аутентификаторов появится Secured TOTP.

Пользователю нужно выполнить следующие действия:

1. Нажать значок шестеренки.
2. Нажать кнопку Зарегистрировать.
3. Указать ID устройства. Чтобы получить ID, пользователю нужно зайти в приложение Indeed Key, нажать значок шестеренки и скопировать значение из поля ID устройства.
4. Отсканировать появившийся код устройством с открытым приложением Indeed Key.
5. Если настроена **принудительная проверка аутентификатора**, дополнительно ввести полученный одноразовый пароль.



# Indeed AM Software OTP Provider

С помощью Software OTP Provider вы можете реализовать двухфакторную аутентификацию, основанную на программном обеспечении. Аутентификатор представляет собой одноразовый пароль, который пользователь должен предоставить в дополнение к своему логину и паролю, чтобы получить доступ к приложению.

Одноразовый пароль генерируется автономно на мобильном устройстве (телефон, смартфон, планшет) с использованием специализированного приложения (например, Indeed Key, Google Authenticator, Яндекс.Ключ). Генерация одноразового пароля производится на основе двух параметров: секретного ключа, задаваемого на этапе регистрации аутентификатора, и текущего времени.

Технология аутентификации основана на системе, где для заданного секретного ключа пользователя в каждый момент времени существует единственный верный одноразовый пароль. Таким образом, имея информацию о секретном ключе, сервер может проверить переданный пользователем одноразовый пароль. Для правильного функционирования технологии время на мобильном устройстве и сервере аутентификации должно совпадать (при этом допускается погрешность, величина которой может регулироваться администратором).

|                                        |
|----------------------------------------|
| Идентификатор провайдера               |
| {0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0} |

|                                                             |
|-------------------------------------------------------------|
| Идентификатор провайдера для Indeed AM NPS RADIUS Extension |
| {B772829C-4076-482B-B9BD-53B55EA1A302}                      |

## Предварительные требования

Для работы провайдера требуется установка Indeed AM Bsp Broker на сервере Indeed AM.

Файлы для Indeed Bsp Broker расположены в папке *Indeed AM <номер версии>/Indeed AM Providers/Indeed AM Bsp Broker/<номер версии>*.

- *IndeedEA.AuthProviders.BspBroker-<номер версии>.x64.ru-ru.msi* — пакет для установки Indeed Bsp Broker на 64-битных ОС.
- *IndeedEA.AuthProviders.BspBroker-<номер версии>.x86.ru-ru.msi* — пакет для установки Indeed Bsp Broker на 32-битных ОС.

## Установка провайдера

1. Запустите файл для установки *IndeedAM.AuthProviders.SoftwareTOTP.Provider-<номер версии>.<разрядность>.ru-ru.msi*, расположенный по пути *Indeed AM <Номер версии> \Indeed AM Providers \Indeed AM Software OTP Provider \<Номер версии>*, и следуйте шагам мастера установки.



### ВАЖНО

Если в инфраструктуре используется несколько Core Server, 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.

Файлы шаблонов политик расположены в папке *Indeed AM <номер версии> \Misc \ADMX Templates*.

## Принудительная проверка аутентификатора

Для регистрации аутентификатора можно настроить принудительную проверку аутентификатора.

1. Перейдите в раздел Конфигурация→Аутентификаторы и выберите из списка Software TOTP.
2. В разделе Основные настройки включите принудительную проверку. При регистрации появится дополнительное окно подтверждения для ввода данных аутентификации.
3. Введите полученные данные аутентификации и нажмите Подтвердить.

# Indeed AM Hardware OTP Provider

Автономный генератор одноразовых паролей eToken PASS можно использовать для аутентификации в любых приложениях и службах, поддерживающих протокол аутентификации RADIUS: VPN, Microsoft ISA, Microsoft IIS, Outlook Web Access и др. Подробную информацию об устройстве eToken PASS вы можете получить на [официальном сайте компании Aladdin](#).

В eToken PASS реализован алгоритм генерации одноразовых паролей (One-Time Password – OTP). Этот алгоритм основан на алгоритме HMAC и хеш-функции SHA-1. Для расчета значения OTP принимаются два входных параметра – секретный ключ (начальное значение для генератора) и текущее значение счетчика (количество необходимых циклов генерации). Начальное значение хранится как в самом устройстве, так и на сервере в системе Indeed. Счетчик в устройстве увеличивается при каждой генерации OTP, на сервере – при каждой удачной аутентификации по OTP.

Провайдер Indeed AM Hardware OTP может быть использован для аутентификации в следующих модулях:

- [Identity Provider](#),
- [ADFS Extension](#),
- [NPS Radius Extension](#),
- [IIS Extension](#),
- [RDP Windows Logon](#),
- [Windows Logon](#),
- [Enterprise SSO](#).

| Идентификатор провайдера               |
|----------------------------------------|
| {AD3FBA95-AE99-4773-93A3-6530A29C7556} |

## Установка провайдера

1. Запустите файл для установки, расположенный по пути *Indeed AM <номер версии>/Indeed AM Providers/Indeed AM HOTP Provider/Server/<номер версии>*, и следуйте шагам мастера 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.

## Добавление устройства

### ❗ ИНФОРМАЦИЯ

Одно устройство может быть зарегистрировано только для одного пользователя

Для добавления устройства необходимо выполнить следующее:

1. Откройте консоль управления Management Console.
2. Перейдите на вкладку Устройства.
3. Нажмите Добавить или Добавить из файла.

### ❗ ПРИМЕЧАНИЕ

Вы можете добавить устройство, выбрав файл с параметрами устройства (Добавить из файла), либо указать параметры вручную (Добавить).

## Устройства

[+ Добавить](#) [📁 Добавить из файла](#) [🗑 Удалить](#) [📁 Удалить из файла](#) [🔒 Заблокировать](#) [🔓 Разблокировать](#)

| Модель                                                    | Серийный номер       | Комментарий          | Провайдер аутентификации |
|-----------------------------------------------------------|----------------------|----------------------|--------------------------|
| Не выбрана ▾                                              | <input type="text"/> | <input type="text"/> | Не выбран ▾              |
| <div><a href="#">Поиск</a> <a href="#">Сбросить</a></div> |                      |                      |                          |

Нет информации о зарегистрированных устройствах

## Добавление из файла

1. Нажмите Добавить из файла.
2. Выберите файл формата XML с параметрами устройства и нажмите Добавить.

## Пример конфигурации устройства

```
<Tokens xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">
  <Token serial="000200071927">
    <CaseModel>5</CaseModel>
    <Model>109</Model>
    <ProductionDate>11/4/2008</ProductionDate>
    <ProductName>Aladdin OTPD v1.0</ProductName>
    <Applications>
      <Application ConnectorID="{a61c4073-2fc8-4170-
99d1-9f5b70a2cec6}">

<Seed>884f20ce4b2c406e0b6199338990bb6cc3fabac403eaa7f8</Seed>
      <MovingFactor>1</MovingFactor>
    </Application>
  </Applications>
</Token>
</Tokens>
```



## Добавление вручную

1. Нажмите Добавить.
2. В поле Серийный номер укажите серийный номер устройства.
3. В поле Секретный ключ укажите seed устройства.

4. Поле Комментарий — необязательный параметр.

5. Нажмите Добавить.

## Добавить устройство



Модель

eToken PASS (HOTP): Aladdin OTPD v1.0

Серийный номер

000200071927

Секретный ключ

884f20ce4b2c406e0b6199338990bb6cc3fabac403eaa7f8

Комментарий

eToken 000200071927

Отмена

Добавить

## Редактирование устройства

Для редактирования устройства выполните следующие действия:

1. Откройте консоль управления Management Console.
2. Перейдите на вкладку Устройства.
3. Нажмите серийный номер устройства.



### ИНФОРМАЦИЯ

При необходимости можно выполнить поиск, используя фильтры в верхней части страницы.

## 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         |
|-------------------------------------------|---------------------|--------------------------|--------------|---------------------|
| <input type="checkbox"/> 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 нажмите 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 выполните следующие действия:

1. Откройте консоль управления Management Console.
2. Перейдите на вкладку Устройства.
3. Выберите устройство и нажмите Удалить.



### ИНФОРМАЦИЯ

При необходимости можно выполнить поиск, используя фильтры в верхней части страницы.

## 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         |
|------------------------------------------------------|----------------|--------------------------|--------------|---------------------|
| <input checked="" type="checkbox"/> Aladdin OTP v1.0 | 000200071927   | Hardware HOTP            |              | eToken 000200071927 |

### Удаление из файла

1. Для удаления устройства по информации из файла нажмите Удалить из файла.
2. Выберите файл конфигурации устройства.
3. Нажмите Удалить.

## Удалить устройство



Тип устройства

eToken PASS (HOTP)

Файл устройств

etoken.xml

Выбрать файл

Отмена

Удалить

## Синхронизация устройства

Для синхронизации устройства выполните следующие действия:

1. Откройте консоль управления Management Console.
2. Перейдите на вкладку Устройства.
3. Нажмите серийный номер устройства.
4. Выберите Синхронизировать OTP.



5. В поле Одноразовый пароль 1 и Одноразовый пароль 2 укажите пароли с устройства и нажмите Синхронизировать.

**INDEED** 

## 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

# Indeed AM Hardware TOTP Provider

Провайдер Indeed AM Hardware TOTP может быть использован для аутентификации в следующих модулях:

- Identity Provider,
- ADFS Extension,
- NPS Radius Extension,
- IIS Extension,
- RDP Windows Logon,
- Windows Logon,
- Enterprise SSO.

Hardware TOTP позволяет получать одноразовые пароли с помощью следующих устройств:

- Автономный генератор одноразовых паролей **eToken PASS**. Его можно использовать для аутентификации в любых приложениях и службах, в том числе поддерживающих протокол аутентификации RADIUS — VPN, Microsoft ISA, Microsoft IIS, Outlook Web Access и других.
- Токен для надежной защиты доступа к данным аккаунтов **Рутокен OTP**. Он используется для аутентификации в корпоративных сервисах и порталах, сервисах аутентификации, приложениях и сервисах управления паролями, а также в других сервисах, поддерживающих технологию OATH TOTP.

Таблица сравнения характеристик устройств

| Устройство  | Формат файла | Алгоритм     | Период обновления |
|-------------|--------------|--------------|-------------------|
| eToken Pass | XML          | SHA1         | 30 секунд         |
| Рутокен OTP | CSV          | SHA1, SHA256 | 30, 60 секунд     |

Идентификатор провайдера

{CEB3FEAF-86ED-4A5A-BD3F-6A7B6E60CA05}

## Установка провайдера

1. Запустите файл для установки, расположенный по пути *Indeed AM <номер версии>/Indeed AM Providers/Indeed AM Hardware TOTP Provider/<номер версии>*, и следуйте шагам мастера 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.

## Добавление устройства

Вы можете добавить устройство вручную или через загрузку файла с параметрами устройства.

Устройство может быть зарегистрировано только для одного пользователя

### Добавление вручную

#### Устройство Рутокен ОТР

Для добавления устройства Рутокен ОТР выполните следующие действия:

1. Откройте консоль управления Management Console.
2. В меню слева выберите Устройства.
3. Нажмите Добавить устройство.
4. В открывшемся окне выберите *Rutoken OTP*.
5. Заполните поля Серийный номер, Секретный ключ, Период обновления и Комментарий (это необязательное поле) и нажмите Добавить.



#### ВАЖНО

При добавлении Рутокен ОТР вручную вы можете указать секретный ключ в двух форматах — HEX и Base32.

## Устройство eToken PASS

Для добавления устройства eToken PASS выполните следующие действия:

1. Откройте консоль управления Management Console.
2. В меню слева выберите Устройства.
3. Нажмите Добавить устройство.
4. В открывшемся окне выберите модель eToken PASS.
5. Заполните поля Серийный номер, Секретный ключ и Комментарий (это необязательное поле) и нажмите Добавить.

## Добавление из файла

### Устройство Рутокен ОТР

Для добавления устройства Рутокен ОТР выполните следующие действия:



#### ВАЖНО

При добавлении Рутокен ОТР через файл вы можете указать секретный ключ только в одном формате — Base32.

1. Откройте консоль управления Management Console.
2. В меню слева выберите Устройства.
3. Нажмите Добавить из файла.
4. В открывшемся окне выберите *Rutoken OTP* и нажмите Выбрать файл.
5. В открывшемся окне выберите файл формата CSV с параметрами устройства и нажмите Добавить.



#### СОВЕТ

Подробную информацию по настройке устройства вы можете найти [в руководстве по использованию Рутокен ОТР](#).

## Устройство eToken PASS

Для добавления устройства eToken PASS выполните следующие действия:

1. Откройте консоль управления Management Console.
2. В меню слева выберите Устройства.
3. Нажмите Добавить из файла.
4. В открывшемся окне выберите модель eToken PASS.
5. В открывшемся окне выберите файл формата XML с параметрами устройства и нажмите Добавить.

## Синхронизация устройства

Для синхронизации устройства выполните следующие действия:

1. Откройте консоль управления Management Console.
2. В меню слева выберите Устройства.
3. Из списка выберите устройство и нажмите Синхронизировать.
4. В открывшемся новом окне в поле Одноразовый пароль 1 и Одноразовый пароль 2 укажите пароли с устройства и нажмите Синхронизировать.

## Изменение серийного номера и отключение устройства

Для редактирования устройства выполните следующие действия:

1. Откройте консоль управления Management Console.
2. В меню слева выберите Устройства.
3. В выпадающем списке Провайдер аутентификации выберите *Hardware TOTP*, в поле Серийный номер, если известно, укажите серийный номер устройства и нажмите Поиск.
4. Выберите найденное устройство и нажмите значок редактирования.

### ▼ Пример

Устройства

[✕ Удалить устройства](#)

| <input checked="" type="checkbox"/> | Серийный номер | Провайдер     | Модель      | Комментарий | Пользователь |
|-------------------------------------|----------------|---------------|-------------|-------------|--------------|
| <input checked="" type="checkbox"/> | AP578201       | Hardware TOTP | eTPass 6.20 |             |              |



5. В окне редактирования можно изменить серийный номер устройства, комментарий или отключить устройство. После внесения изменений нажмите Сохранить.

### ▼ Пример

**Серийный номер**

AP578201

**Комментарий**

Hardware TOTP

**Время последней синхронизации**

Нет данных

☒ Устройство отключено

Сохранить

Отмена

## Удаление устройства

Вы можете удалить устройство вручную или через загрузку файла с параметрами устройства.

### Удаление вручную

Для удаления устройства выполните следующие действия:

1. Откройте консоль управления Management Console.

2. В меню слева выберите Устройства.
3. В выпадающем списке Провайдер аутентификации выберите *Hardware TOTP*, в поле Серийный номер, если известно, укажите серийный номер устройства и нажмите Поиск.
4. Выберите найденное устройство и нажмите Удалить устройство.
5. В открывшемся окне подтвердите удаление.

## Удаление из файла

### Устройство Рутокен ОТР

Для удаления устройства Рутокен ОТР выполните следующие действия:

1. Откройте консоль управления Management Console.
2. В меню слева выберите Устройства.
3. Нажмите Удалить из файла.
4. В открывшемся окне выберите *Rutoken OTP* и нажмите Выбрать файл.
5. В открывшемся окне выберите файл формата CSV с параметрами устройства и нажмите Удалить.



#### СОВЕТ

Подробную информацию по настройке устройства вы можете найти [в руководстве по использованию Рутокен ОТР](#).

### Устройство eToken PASS

Для удаления устройства eToken PASS выполните следующие действия:

1. Откройте консоль управления Management Console.
2. В меню слева выберите Устройства.
3. Нажмите Удалить из файла.
4. В открывшемся окне выберите модель eToken PASS.
5. В открывшемся окне выберите файл формата XML с параметрами устройства и нажмите Удалить.

# Indeed AM SMS OTP Provider

Компонент Indeed AM SMS OTP Provider предназначен для аутентификации пользователей с применением технологии одноразовых паролей, доставляемых пользователям по СМС.

Одноразовый пароль представляет собой набор случайных символов (цифр, специальных символов и латинских букв). Генерация пароля происходит на сервере Indeed AM, затем пароль передается на СМС-шлюз, имеющийся в инфраструктуре клиента, после одноразовый код отправляется на номер телефона пользователя. Передача данных происходит по протоколу SMPP (Short Message Peer-to-Peer).

Идентификатор провайдера

{EBB6F3FA-A400-45F4-853A-D517D89AC2A3}

## Предварительные требования

Для использования Indeed AM SMS OTP Provider необходимо наличие СМС- шлюза. Данный шлюз должен быть доступен с каждого сервера Indeed AM, на котором предполагается установка SMS OTP Provider.

Для использования провайдера у пользователя должен быть задан номер телефона в атрибуте по умолчанию `telephoneNumber` или в другом настроенном атрибуте, иначе провайдер будет недоступен для использования.

Регистрация аутентификатора в User Console не требуется.

## Установка провайдера

1. Запустите файл для установки, расположенный по пути *Indeed AM <номер версии>/Indeed AM Providers/Indeed AM SMS OTP Provider/Server/<номер версии>*, и следуйте шагам мастера установки.



### ВАЖНО

Если в инфраструктуре используется несколько Core Server, то установку провайдера необходимо выполнить на всех серверах инфраструктуры.

Если провайдер используется в клиентских сценариях с Indeed AM Windows Logon и ESSO Agent, установите провайдер на клиентские машины с помощью файла *Indeed AM* <номер версии>/*Indeed AM Providers/Indeed AM SMS OTP Provider/Server/<номер версии>/Client/<Номер версии>/IndeedID.SMSOTP.Provider.msi*.

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 номером телефона

Для смены атрибута по умолчанию добавьте следующие параметры в конфигурационный файл сервера *C:\inetpub\wwwroot\am\core\Web.config*:

- тег `userMapRules` в теге `adUserCatalogProvider`;
- тег `adObjectMapRule` в теге `userMapRules` с следующими параметрами:
  - `attribute="Phone"` — указывает на изменяемый параметр;
  - `adAttribute="mobile"` — указывает, из какого атрибута Active Directory брать значение;
- тег `objectTypeSettings`;
- 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"/>
    <objectTypeSettings>
        <objectSetting category="person" class="user">
</objectSetting>
    </objectTypeSettings>
</userMapRules>
</adUserCatalogProvider>

```

## Защита от спама

Механизм защиты от спама основан на расчете процента успешных аутентификаций относительно всех отправленных сообщений за указанный интервал времени. При этом расчет запускается, только если количество отправленных сообщений превышает количество, заданное вами в настройке Окно оценки.

При обнаружении спам-атаки дальнейшая отправка сообщений блокируется на заданный период времени, а при попытке входа возникает ошибка *Potential spam attack detected*.

Отправка сообщений возобновляется либо по истечении заданного периода, либо по достижении определенного количества (в процентном отношении) успешных аутентификаций.

Чтобы настроить защиту от спама, выполните следующее:

1. В Management Console в разделе Конфигурация→Аутентификаторы выберите аутентификатор.
2. В секции Настройки защиты от спама выполните следующие настройки:
  - включите или отключите защиту от спама;
  - в поле Окно оценки попыток аутентификации укажите, в течение какого времени будет выполняться расчет процента успешных попыток входа;
  - в поле Пороговое окно попыток аутентификации укажите, сколько попыток входа должно производиться за время, указанное в окне оценки попыток аутентификации;
  - в поле Процент успешных попыток аутентификации укажите минимальный процент успешных входов относительно всех отправленных сообщений.

### ▼ Пример

---

Настройка включена со следующими значениями:

- Окно оценки попыток аутентификации — 600
- Пороговое окно попыток аутентификации — 20
- Процент успешных попыток аутентификации — 85

Защита от спама включится, если произойдет 21 попытка входа (отправлено 21 сообщение). Произойдет блокировка аутентификатора на 600 секунд.

Аутентификатор разблокируется в одном из случаев:

- процент успешных входов (пользователь успешно ввел одноразовый пароль из сообщения) достигнет значения 85;
- прошло 600 секунд с момента блокировки.

### ❗ ИНФОРМАЦИЯ

События лог-сервера:

- 2090: Обнаружена потенциальная спам-атака. Отправка сообщений приостановлена.
- 1118: Отправка сообщений пользователям возобновлена.

### ❗ ДОПОЛНИТЕЛЬНЫЕ НАСТРОЙКИ

Чтобы выбрать и настроить тип подключения, выполнить настройки формата сообщения и телефонного номера, а также настройки одноразового пароля, перейдите в раздел с настройками групповых политик.

# Indeed AM Messages Proxy

Indeed AM Messages Proxy (Messages Proxy) — это веб-приложение, которое работает на базе IIS. Messages Proxy предоставляет Web API для отправки OTP при помощи запуска внешних модулей (скрипты, бинарные исполняемые модули). В отличие от SMS Proxy, Messages Proxy не подключается к SMPP-шлюзу, а только запускает скрипты (любой исполняемый файл).

## Системные требования

- Windows Server 2012 R2 и выше;
- Internet Information Services 7.5 и выше со следующими модулями:
  - Веб-сервер (Web server);
  - Сжатие статического содержимого (Static Content Compression);
  - Ошибки HTTP (HTTP Errors);
  - Перенаправление HTTP (HTTP Redirection);
  - Проверка подлинности Windows (Windows Authentication);
  - Публикация WebDAV (WebDAV Publishing);
  - ASP.NET;
  - ASP;
  - Расширения ISAPI (ISAPI Extensions);
  - Фильтры ISAPI (ISAPI Filters);
  - Консоль управления службами IIS (IIS Management Console);
  - Сценарии и средства управления IIS (IIS Management Scripts and Tools);
  - Служба управления (Management Service).

## Предварительная настройка

1. Установите роль IIS на сервере, на котором вы планируете устанавливать Messages Proxy, одним из следующих способов:
  - откройте Диспетчер серверов, выберите Локальный сервер и во вкладке Управление нажмите Добавить роли и компоненты;
  - запустите скрипт `\Misc\IISScripts\Indeed.Main.IIS.Install.MSServer.ps1`.
2. Установите .NET 6 через запуск `dotnet-hosting-6.0.10-win.exe` из папки *Indeed AM <номер версии>/Indeed AM Idp* дистрибутива.

## Установка

1. Запустите файл для установки, расположенный по пути *Indeed AM <номер версии>/Indeed AM Messages Proxy/<номер версии>*, и следуйте шагам мастера 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.

## Подготовка сертификатов для Messages Proxy и Core Server

В процессе установки модуля Indeed AM Messages Proxy по умолчанию включается требование SSL-сертификата, что, в свою очередь, требует настройки HTTPS.

На сервере Indeed AM Messages Proxy (сервер)

Для запроса сертификата от доменного центра сертификации Windows выполните следующие действия:

1. Откройте диспетчер сертификатов `certlm.msc`.
2. В каталоге Личное нажмите правой кнопкой мыши на Сертификаты и выберите Все задачи→Запросить новый сертификат.
3. В окне Регистрация сертификатов нажмите Далее→Далее, выберите созданный ранее шаблон сертификата веб-сервера и нажмите Требуется больше данных для подачи заявки на этот сертификат.
4. В появившемся окне Свойства сертификата добавьте следующие значения и нажмите ОК:
  - Имя субъекта: в поле Тип укажите значение *Общее имя*, а в поле Значение — полное имя компьютера (*Srv01.indeed.local*) или сокращенное (*Srv01*).
  - Дополнительное имя: в поле Тип укажите значение *Служба DNS*, а в поле Значение — полное имя компьютера (*Srv01.indeed.local*).
5. Запустите Диспетчер служб IIS.
6. Перейдите на страницу `Srv01(INDEED\Admin-indeed)`→Сайты→Default Web Site и в разделе Действия нажмите Привязки.

7. Выберите строчку с https 443 и нажмите Изменить. В открывшемся окне Изменение привязки сайта в выпадающем списке SSL-сертификат выберите ваш сертификат и нажмите ОК.

8. Выберите строчку с http 80 и нажмите Удалить.

### ❗ ИНФОРМАЦИЯ

Теперь в браузере можно открыть стартовую страницу IIS по адресу <https://Srv01.indeed.local/> (соединение безопасное).

На Core Server (клиент)

Сгенерируйте сертификат клиентской аутентификации. За основу можно взять шаблон *Компьютер* в доменном центре сертификации Windows. Для этого на машине с Core Server:

1. Откройте диспетчер сертификатов certlm.msc.
2. В каталоге Личное нажмите правой кнопкой мыши на Сертификаты и выберите Все задачи→Запросить новый сертификат.
3. В окне Регистрация сертификатов нажмите Далее→Далее, выберите созданный ранее шаблон сертификата *Компьютер*.

## Редактирование конфигурационного файла

1. Откройте на сервере Messages Proxy конфигурационный файл *app-settings.Production.json* из папки *C:\inetpub\wwwroot\am\proxies\messages*.
2. В поле **Scripts** укажите следующие значения:
  - **Path** — путь к программе, через которую запускается **скрипт**,
  - **Arguments** — параметры запуска скрипта, включая путь к скрипту,
  - **Timeout** — время, по истечении которого Messages Proxy вернет ошибку, если скрипт не выполнится. Значение по умолчанию — 00:00:20 (20 секунд).

### ❗ ИНФОРМАЦИЯ

В поле `Scripts` можно добавить более одного скрипта, для этого нужно через запятую указать несколько блоков с параметрами для каждого скрипта. Также можно задать очередность запуска скриптов — последовательный (`Sequential`) и одновременный (`Parallel`) запуск. Если этот параметр не задан, то используется значение по умолчанию — `Sequential`.

3. В поле `LoggingPermissions` укажите параметры, которые определяют информацию для логирования. Возможные параметры:

- `Source` — отправитель сообщения,
- `Destination` — получатель сообщения,
- `Error` — ошибки выполнения скрипта,
- `Output` — сообщения при выполнении скрипта,
- `None` (значение по умолчанию) — скрываются значения всех логируемых полей,
- `All` — показываются значения всех логируемых полей.

Например, если в `LoggingPermissions` указан параметр `Source`, то *отправитель сообщения* логируется (не скрывается). Все остальные параметры скрываются и заменяются на `***`. *Логи находятся в папке C:\inetpub\wwwroot\am\proxies\messages\Logs\<папка с датой>\**.

4. Поле `Publication` включает опциональный параметр `DefaultSource`, содержащий имя отправителя SMS по умолчанию.

5. Опционально можно настроить параметр для включения Swagger. В поле `Documentation` для параметра `Enabled` укажите значение `true`. Swagger будет доступен по адресу `/am/proxies/messages/documentation`.

6. В поле `Authentication": { "Certificate": { "Thumbprint": "" } }` укажите отпечаток сертификата (**клиента**), по которому провайдер (SMS или Storage SMS) может быть аутентифицирован в Messages Proxu для отправки сообщений. Можно использовать несколько сертификатов от нескольких клиентов, в таком случае поле будет называться `"Thumbprints"`.

## ▼ Пример конфигурационного файла



```

{
  "MessagesProxy": {
    "Scripts": [
      {
        "Path":
"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe",
        "Arguments":
[
          "/c",
"C:\\inetpub\\wwwroot\\am\\proxies\\messages\\script.bat",
          "{0:Source}",
          "{0:Content}",
          "{0:Phone}",
          "{0:RawObjectId}",
          "{0:Sid}",
          "{0:DistinguishedName}",
          "{0:PrincipalName}",
          "{0:SamCompatibleName}",
          "{0:Email}",
          "{0:CustomParameter}"
        ],
        "Timeout": "00:00:10"
      }
    ],
    "LoggingPermissions": "Source"
  },
  "Publication": {
    "DefaultSource": "Indeed sender"
  },
  "Documentation": {
    "Enabled": false
  },
  "Debug": {
    "ExceptionResponsesEnabled": false
  },
  "Authentication": {

```

```
"Certificate": {  
  "Thumbprint": "124b3c62f4da3ce8bb271dc4990e354d118daa0g"  
},  
"ReverseProxyIntegration": {  
  "BasePath": "/am/proxies/messages"  
},  
"Localization": {  
  "DefaultCulture": "en-US"  
}  
}
```

## Скрипт

В файле со скриптом происходит чтение параметров, переданных из Messages Proxy. Параметры записываются в файл *C:\distr\ps.json* (параметр `fileName` из примера скрипта Powershell). При использовании Messages Proxy через SMS-провайдер OTP будет передаваться в параметре `Content`.

### ▼ Пример скрипта Powershell

---

```
$body = @(
@{
Source = $args[0]
Content = $args[1]
Phone = $args[2]
RawObjectId = $args[3]
Sid = $args[4]
DistinguishedName = $args[5]
PrincipalName = $args[6]
SamCompatibleName = $args[7]
Email = $args[8]
CustomParameter = "I am PS"
}
)

$body | ConvertTo-Json | Out-File "C:\distr\ps.json"

Invoke-WebRequest -Method Post -Uri
'http://Srv01.indeed.local:82/api/sms' -Body ($body|ConvertTo-Json)
-ContentType 'application/json'

Start-Sleep -Seconds 5
```

## Настройка провайдера SMS OTP/Storage SMS OTP

С помощью групповых политик выполните настройку провайдера SMS OTP или Storage SMS OTP для отправки OTP через Messages Proxy. Перед настройкой групповых политик добавьте шаблоны политик Indeed AM в список административных шаблонов. Файлы шаблонов политик входят в состав дистрибутива Messages Proxy и расположены в каталоге Misc.

## Выбор типа подключения

### Через GPO

Политика *Выбор типа подключения для провайдера* применяется к серверам Indeed AM и предназначена для выбора типа подключения Core Server (с помощью провайдера SMS OTP или Storage SMS OTP) к SMS-шлюзу.

1. Откройте политику *Выбор типа подключения для провайдера*. Политика расположена по следующему пути: *Административные шаблоны*→*Indeed-ID*→*Id Providers*→*SMS OTP*.
2. Установите значение политики *Включено*.
3. В параметрах выберите опцию Прокси сообщений для Messages Proxy.

### В реестре

1. Откройте редактор реестра на сервере Indeed AM.
2. Откройте раздел *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Indeed-ID\BSPs\SMSOTP*.
3. Создайте параметр *SmsSenderType* с типом DWORD со значением 6.

## Настройки типа подключения

### Через GPO

Политика *Настройки прокси сообщений* применяется к серверам Indeed AM и определяет настройки типа подключения.

1. Откройте политику *Настройки прокси сообщений*. Политика расположена по следующему пути: *Административные шаблоны*→*Indeed-ID*→*Id Providers*→*SMS OTP*.
2. Установите значение политики *Включено*.
3. Задайте следующие параметры:

- *URL* — адрес подключения к серверу;
- *Отправитель* — имя отправителя, которое будет отображаться при получении сообщения;
- *Дополнительный текст перед отправкой OTP* — произвольный текст сообщения, предшествующий одноразовому паролю;
- *Отпечаток сертификата клиента* — сертификат провайдера, указанный в настройках конфигурационного файла Messages Proxy *app-settings.Production.json* (поле `"Authentication": { "Certificate": { "Thumbprint": "" } }`);
- *Отпечаток сертификата сервера* — сертификат Messages Proxy для работы по протоколу HTTPS (настраивается в IIS).

## В реестре

1. Откройте редактор реестра на сервере Indeed AM.
2. Откройте раздел *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Indeed-ID\BSPs\SMSOTP\MessagesProxy*.
3. Создайте следующие параметры:
  - *ServerUrl* — адрес подключения к серверу;
  - *From* (REG\_SZ) — имя отправителя, которое будет отображаться при получении сообщения;
  - *messageOTP* (REG\_SZ) — произвольный текст сообщения, предшествующий одноразовому паролю;
  - *ClientCertificateThumbprint* (REG\_SZ) — сертификат провайдера, указанный в настройках конфигурационного файла Messages Proxy *app-settings.Production.json* (поле `"Authentication": { "Certificate": { "Thumbprint": "" } }`);
  - *ServerCertificateThumbprint* (REG-SZ) — сертификат Messages Proxy для работы по протоколу HTTPS (настраивается в IIS).

# Indeed AM SMS Proxy

Indeed AM SMS Proxy (SMS Proxy) — это веб-приложение, которое работает на базе IIS. SMS Proxy напрямую подключается к SMPP-шлюзу и отправляет SMS, при этом Indeed AM Server не производит разрыв сессии с SMPP-шлюзом, и запросы отправляются в рамках одного подключения, а не в отдельных для каждого запроса.

## Системные требования

- Windows Server 2012 R2 и выше;
- Internet Information Services 7.5 и выше со следующими модулями:
  - Веб-сервер (Web server);
  - Сжатие статического содержимого (Static Content Compression);
  - Ошибки HTTP (HTTP Errors);
  - Перенаправление HTTP (HTTP Redirection);
  - Проверка подлинности Windows (Windows Authentication);
  - Публикация WebDAV (WebDAV Publishing);
  - ASP.NET;
  - ASP;
  - Расширения ISAPI (ISAPI Extensions);
  - Фильтры ISAPI (ISAPI Filters);
  - Консоль управления службами IIS (IIS Management Console);
  - Сценарии и средства управления IIS (IIS Management Scripts and Tools);
  - Служба управления (Management Service).

## Предварительная настройка

1. Установите роль IIS на сервере, на котором вы планируете устанавливать SMS Proxy, одним из следующих способов:
  - откройте Диспетчер серверов, выберите Локальный сервер и во вкладке Управление нажмите Добавить роли и компоненты;
  - запустите скрипт `\Misc\IISScripts\Indeed.Main.IIS.Install.MSServer.ps1`.
2. Установите .NET 6 через запуск `dotnet-hosting-6.0.10-win.exe` из папки *Indeed AM <номер версии>/Indeed AM Idp* дистрибутива.

## Установка

1. Запустите файл для установки, расположенный по пути *Indeed AM <номер версии>/Indeed AM SMS Proxy/<номер версии>*, и следуйте шагам мастера 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.

## Подготовка сертификата для SMS Proxy

В процессе установки модуля Indeed AM SMS Proxy по умолчанию включается требование SSL-сертификата, что, в свою очередь, требует настройки HTTPS.

Для запроса сертификата от доменного центра сертификации Windows на сервере Indeed AM SMS Proxy:

1. Откройте диспетчер сертификатов certlm.msc.
2. В каталоге Личное нажмите правой кнопкой мыши на Сертификаты и выберите Все задачи→Запросить новый сертификат.
3. В окне Регистрация сертификатов нажмите Далее→Далее, выберите созданный ранее шаблон сертификата веб-сервера и нажмите Требуется больше данных для подачи заявки на этот сертификат.
4. В появившемся окне Свойства сертификата добавьте следующие значения и нажмите ОК:
  - Имя субъекта: в поле Тип укажите значение *Общее имя*, а в поле Значение — полное имя компьютера (*Srv01.indeed.local*) или сокращенное *Srv01*.
  - Дополнительное имя: в поле Тип укажите значение *Служба DNS*, а в поле Значение — полное имя компьютера (*Srv01.indeed.local*).
5. Запустите Диспетчер служб IIS.
6. Перейдите на страницу Srv01(INDEED\Admin-indeed)→Сайты→Default Web Site и в разделе Действия нажмите Привязки.
7. Выберите строчку с https 443 и нажмите Изменить. В открывшемся окне Изменение привязки сайта в выпадающем списке SSL-сертификат выберите ваш сертификат и

нажмите ОК.

8. Выберите строчку с http 80 и нажмите Удалить.

### ❗ ИНФОРМАЦИЯ

Теперь в браузере можно открыть стартовую страницу IIS по адресу:

<https://Srv01.indeed.local/>

## Редактирование конфигурационного файла

1. Откройте конфигурационный файл *app-settings.Production.json* из папки

*C:\inetpub\wwwroot\am\proxies\sms*.

2. В секции **Smpp** заполните следующие параметры:

- **SystemId** и **Password** — укажите данные аутентификации для подключения к серверу SMPP;
- **Host** — укажите адрес подключения к серверу SMPP;
- **Port** — укажите заданный порт для подключения к серверу SMPP;
- **SystemType** — опциональный параметр входа в систему со стороны сервера SMPP, например, S1;
- **EsmeAddressTon** — возможные значения: Unknown, International, National, NetworkSpecific, SubscriberNumber, Alphanumeric, Abbreviated;
- **EsmeAddressNpi** — возможные значения: Unknown, ISDN, Data, Telex, LandMobile, National, Private, ERMES, IP;
- **LoggingPermissions** — укажите параметр, отвечающий за отображение в логах информации об отправителе и получателе. Можно указать значения через запятую.

Возможные параметры:

- **Source** — отправитель сообщения,
- **Destination** — получатель сообщения,
- **None** (значение по умолчанию) — скрываются значения всех логируемых полей,
- **All** — показываются значения всех логируемых полей.

3. Поле **Publication** включает опциональный параметр **DefaultSource**, содержащий имя отправителя в запросах, например, Indeed-AM.



4. В поле `Authentication": {"Certificate":}` укажите отпечаток сертификата, по которому провайдер (SMS или Storage SMS) может быть аутентифицирован в SMS Proxy для отправки сообщений. По умолчанию используется конфигурация для аутентификации без сертификата `"Certificate": {"Enabled": false, "Thumbprint": "" }`.



#### ПРИМЕЧАНИЕ

Чтобы исключить возможные проблемы при работе сертификатов, сначала настройте систему без их использования — то есть без установки двустороннего TLS-соединения:

- При настройке политики SMS прокси оставьте значения отпечатков сертификатов пустыми, как в настройках по умолчанию.
- В версии AM 8.2.6 и выше дополнительно добавьте в поле `Authentication": {"Certificate":}` значение `"NetworkAddress": { "Enabled": false }`.

5. Чтобы применить изменения в файле `app-settings.Production.json`, перезапустите сервер `IndeedAM.Core.proxies.sms`.

## ▼ Пример конфигурационного файла

```

{
  "Smpp": {
    "SystemId": "smppclient1",
    "Password": "password",
    "Host": "am1.indeed.local",
    "Port": "2776",
    "EsmeAddressTon": "International",
    "EsmeAddressNpi": "ISDN",
    "ReconnectionDelay": "00:02:00",
    "LoggingPermissions": "Source"
  },
  "Publication": {
    "DefaultSource": "Indeed-Id"
  },
  "Documentation": {
    "Enabled": false
  },
  "Debug": {
    "ExceptionResponsesEnabled": false
  },
  "Authentication": {
    "Certificate": {
      "Enabled": false,
      "Thumbprint": "",
      "ForwardingHeader": "Proxy-Client-Certificate"
    },
    "NetworkAddress": {
      "Enabled": false
    }
  },
  "ReverseProxyIntegration": {
    "BasePath": "/am/proxies/sms"
  },
  "Localization": {
    "DefaultCulture": "ru-RU"
  }
}

```

```
}  
  
}
```

## Выбор типа подключения

### ❗ ИНФОРМАЦИЯ

Перед настройкой групповой политики добавьте шаблоны политик Indeed AM в список административных шаблонов. Файлы шаблонов политик входят в состав дистрибутива SMS Proxy и расположены в каталоге Misc.

### Через GPO

Политика *Выбор типа подключения для провайдера* применяется к серверам Indeed AM и предназначена для выбора Sender провайдера SMS OTP.

1. Откройте политику *Выбор типа подключения для провайдера*. Политика расположена по следующему пути: *Административные шаблоны*→*Indeed-ID*→*Id Providers*→*SMS OTP*.
2. Установите значение политики *Включено*.
3. В параметрах выберите опцию SMS Прокси для SMS Proxy.

### В реестре

1. Откройте редактор реестра на сервере Indeed AM.
2. Откройте раздел *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Indeed-ID\BSPs\SMSOTP*.
3. Создайте параметр *SmsSenderType* с типом DWORD со значением 5.

# Настройки SMS прокси

## Через GPO

Политика применяется к серверам Indeed AM и определяет настройки для сервиса отправки SMS.

Включите политику *Настройки SMS прокси* и укажите необходимые параметры:

- *URL* — адрес подключения к SMS Proxy. Например:  
<https://am1.indeed.local/am/proxies/sms>.
- *Отправитель* — имя отправителя, которое будет отображаться при получении SMS.
- *Дополнительный текст перед отправкой OTP* — произвольный текст сообщения, предшествующий одноразовому паролю.
- *Отпечаток сертификата клиента* (необязательный параметр) — сертификат провайдера, указанный в настройках конфигурационного файла SMS Proxy *app-settings.Production.json* (поле `Authentication": {"Certificate": {"Thumbprint": "" } }`). Этот сертификат будет добавлен в список сертификатов клиента при запросе к SMS Proxy.
- *Отпечаток сертификата сервера* — сертификат SMS Proxy для работы по протоколу HTTPS (настраивается в IIS).

## В реестре

1. Откройте редактор реестра на сервере Indeed AM.
2. Откройте раздел *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Indeed-ID\BSPs\SMSOTP\SMSProxy*.
3. Создайте следующие параметры:
  - *ServerUrl* — адрес подключения к SMS Proxy. Например:  
<https://am1.indeed.local/am/proxies/sms>.
  - *From* (REG\_SZ) — имя отправителя, которое будет отображаться при получении сообщения.
  - *messageOTP* (REG\_SZ) — произвольный текст сообщения, предшествующий одноразовому паролю.
  - *ClientCertificateThumbprint* (REG\_SZ) — сертификат провайдера, указанный в настройках конфигурационного файла SMS Proxy *app-settings.Production.json*

(поле `Authentication": {"Certificate": {"Thumbprint": "" } }`).

- `ServerCertificateThumbprint` (REG-SZ) — сертификат SMS Proxy для работы по протоколу HTTPS (настраивается в IIS).

## Двустороннее TLS-соединение

Чтобы установить двустороннее TLS-соединение между серверами Indeed Core Server и Indeed AM SMS Proxy, выполните следующие действия:

1. Для сервера SMS Proxy (сервер) сгенерируйте **сертификат** серверной аутентификации (по шаблону *Веб-сервер*).
2. Для Core Server (клиент) сгенерируйте сертификат клиентской аутентификации (например, по шаблону *Компьютер* в доменном центре сертификации Windows).

Для этого на машине с Core Server:

- а. Откройте диспетчер сертификатов `certlm.msc`.
  - б. В каталоге Личное нажмите правой кнопкой мыши на Сертификаты и выберите Все задачи→Запросить новый сертификат.
  - в. В окне Регистрация сертификатов нажмите Далее→Далее, выберите созданный ранее шаблон сертификата *Компьютер*.
3. Экпортируйте в файл сертификат клиента и установите его на сервере SMS Proxy в Сертификаты компьютера→Личные.
  4. В конфигурационном файле SMS Proxy укажите следующие параметры.

```
"Authentication": {  
  "Certificate": {  
    "Enabled": true,  
    "Thumbprint": "отпечаток_сертификата_клиента"  
  }  
}
```

В таблице приведены возможные параметры для поля `"Authentication":`  
`{"Certificate":}`.

| Параметр                                                       |                                                                                                        |
|----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| <code>Authentication:Certificate:Enabled</code>                | По умолчанию true. Вкл. двустороннего TLS-сое                                                          |
| <code>Authentication:Certificate:ForwardingEnabled</code>      | По умолчанию true. Вкл. сертификата клиента от заголовке<br><code>Authentication:Certificate</code>    |
| <code>Authentication:Certificate:ForwardingHeader</code>       | Ожидается закодирован интеграции с IIS вне пр MS-ASPNETCORE-CL автоматически использ Certificate       |
| <code>Authentication:Certificate:Thumbprint</code>             | Пример:<br>380854EA27F2BAED04                                                                          |
| <code>Authentication:Certificate:RevocationMode</code>         | По умолчанию <code>NoCheck</code><br><code>NoCheck</code> , <code>Online</code> , <code>Offline</code> |
| <code>Authentication:Certificate:ValidateCertificateUse</code> | По умолчанию <code>true</code> . С проверки ЕКУ.                                                       |
| <code>Authentication:Certificate:ValidateValidityPeriod</code> | По умолчанию <code>true</code> . С проверки времени дейс                                               |

5. Добавьте отпечаток сертификата в политику *Настройки SMS прокси* на Core Sever.

# Indeed AM Storage SMS OTP Provider

Если в качестве хранилища данных Indeed AM вы используете Microsoft SQL, вы можете использовать провайдер Indeed AM Storage SMS OTP. Этот провайдер предоставляет возможность хранения, получения и обновления телефонных номеров пользователей системы Indeed AM в базе данных. Номера телефонов хранятся в зашифрованном виде.

Storage SMS OTP Provider может быть использован для аутентификации в следующих модулях:

- Identity Provider,
- Windows Logon,
- Enterprise SSO,
- ADFS Extension,
- NPS RADIUS Extension.

Идентификатор провайдера

{3F2C1156-B5AF-4643-BFCB-9816012F3F34}

## Предварительные требования

Для использования Storage SMS OTP Provider необходимо наличие СМС-шлюза. Данный шлюз должен быть доступен с каждого сервера Indeed AM, на котором предполагается установка Storage SMS OTP Provider.

## Установка провайдера

1. Запустите файл для установки, расположенный по пути *Indeed AM <номер версии>/Indeed AM Providers/Indeed AM Storage SMS OTP Provider/Server/<номер версии>*, и следуйте шагам мастера установки.



### ❗ ПРИМЕЧАНИЕ

При использовании провайдера в клиентских сценариях с Indeed AM Windows Logon и ESSO Agent выполните установку провайдера с помощью файла *Indeed AM <номер версии>/Indeed AM Providers/Indeed AM Storage SMS OTP Provider/Client/<номер версии>/IndeedID.SMSOTP.Provider.msi* 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

Рекомендуется регистрировать провайдер через облегченную версию API компонента **Indeed AM Phone Management Server**, предназначенную специально для работы с провайдером Storage SMS OTP, также возможно использование основного API системы Indeed.

## Защита от спама

Механизм защиты от спама основан на расчете процента успешных аутентификаций относительно всех отправленных сообщений за указанный интервал времени. При этом расчет запускается, только если количество отправленных сообщений превышает количество, заданное вами в настройке Окно оценки.

При обнаружении спам-атаки дальнейшая отправка сообщений блокируется на заданный период времени, а при попытке входа возникает ошибка *Potential spam attack detected*.

Отправка сообщений возобновляется либо по истечении заданного периода, либо по достижении определенного количества (в процентном отношении) успешных аутентификаций.

Чтобы настроить защиту от спама, выполните следующее:

1. В Management Console в разделе Конфигурация→Аутентификаторы выберите аутентификатор.
2. В секции Настройки защиты от спама выполните следующие настройки:
  - включите или отключите защиту от спама;

- в поле Окно оценки попыток аутентификации укажите, в течение какого времени будет выполняться расчет процента успешных попыток входа;
- в поле Пороговое окно попыток аутентификации укажите, сколько попыток входа должно производиться за время, указанное в окне оценки попыток аутентификации;
- в поле Процент успешных попыток аутентификации укажите минимальный процент успешных входов относительно всех отправленных сообщений.

### ▼ Пример

Настройка включена со следующими значениями:

- Окно оценки попыток аутентификации — 600
- Пороговое окно попыток аутентификации — 20
- Процент успешных попыток аутентификации — 85

Защита от спама включится, если произойдет 21 попытка входа (отправлено 21 сообщение). Произойдет блокировка аутентификатора на 600 секунд.

Аутентификатор разблокируется в одном из случаев:

- процент успешных входов (пользователь успешно ввел одноразовый пароль из сообщения) достигнет значения 85;
- прошло 600 секунд с момента блокировки.

### ❗ ИНФОРМАЦИЯ

События лог-сервера:

- 2090: Обнаружена потенциальная спам-атака. Отправка сообщений приостановлена.
- 1118: Отправка сообщений пользователям возобновлена.

### ❗ ДОПОЛНИТЕЛЬНЫЕ НАСТРОЙКИ

Чтобы настроить сервис отправки СМС, а также формат сообщения и одноразового пароля, перейдите в раздел с настройками групповых политик.

# Indeed AM Email OTP Provider

Компонент Email OTP Provider предназначен для аутентификации пользователей с применением технологии одноразовых паролей, доставляемых пользователям по электронной почте.

Одноразовый пароль представляет собой набор случайных символов (цифр, специальных символов и латинских букв). Генерация пароля происходит на сервере Indeed AM, затем пароль передается на сервис рассылки электронной почты, который пересылает его пользователю в виде письма. Передача данных происходит по протоколу SMTP (Simple Mail Transfer Protocol).

Идентификатор провайдера

{093F612B-727E-44E7-9C95-095F07CBB94B}

## Предварительные требования

Для использования Email OTP Provider необходимо наличие сервера электронной почты. Данный сервер должен быть доступен с каждого сервера Indeed Access Manager, на котором предполагается установка Email OTP Provider.

Для использования аутентификатора у пользователя должен быть задан адрес электронной почты в атрибуте `mail`, иначе аутентификатор будет не доступен для использования.

Регистрация аутентификатора в User Console не требуется.

## Установка провайдера

1. Запустите файл для установки, расположенный по пути *Indeed AM <номер версии>/Indeed AM Providers/Indeed AM Email OTP Provider/Server/<номер версии>*, и следуйте шагам мастера 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 следующие параметры в конфигурационный файл сервера *C:\inetpub\wwwroot\am\core\Web.config*:

- добавьте тег `userMapRules` в теге `adUserCatalogProvider`;
- добавьте тег `adObjectMapRule` в теге `userMapRules` с параметрами:
  - `attribute="Email"` — указывает на изменяемый параметр;
  - `adAttribute="otherMailbox"` — указывает, из какого атрибута Active Directory брать значение;
- добавьте тег `objectTypeSettings`;
- добавьте 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"/>
  <objectTypeSettings>
    <objectSetting category="person" class="user">
</objectSetting>
  </objectTypeSettings>
</userMapRules>
</adUserCatalogProvider>
```

## Настройки SMTP-сервера

Для работы с SMTP-сервером необходимо настроить **групповую политику**

## Блокировка аутентификатора

Чтобы заблокировать аутентификатор, выполните следующее:

1. В Management Console в разделе Конфигурация→Аутентификаторы из списка выберите аутентификатор Email OTP.
2. В секции Настройки блокировки аутентификатора выполните следующие настройки:
  - Разрешите или заблокируйте использование Email OTP в случае серии неудачных попыток аутентификации;
  - В поле Количество попыток аутентификации до блокировки укажите, сколько раз пользователь может совершить неудачную аутентификацию до блокировки способа аутентификации;
  - В поле Сброс счетчика блокировки укажите, сколько минут должно пройти после неудачной попытки аутентификации, прежде чем сбросится счетчик;
  - В поле Таймаут до разблокировки способа входа укажите, через сколько минут заблокированный способ аутентификации станет вновь доступным.

## Настройка одноразового пароля

Настройки применяются к серверам Indeed AM и позволяет задать длину и вхождение групп символов при генерации одноразового пароля.

Чтобы настроить генерацию одноразового пароля, выполните следующее:

1. В Management Console в разделе Конфигурация→Аутентификаторы из списка выберите аутентификатор Email OTP.
2. В секции Настройки генерации одноразового пароля выполните следующие настройки:
  - В поле Длина одноразового пароля укажите, сколько символов будет содержать одноразовый пароль;
  - В настройке Цифры укажите, будет ли одноразовый пароль содержать цифры;
  - В настройке Строчные латинские буквы укажите, будет ли одноразовый пароль содержать строчные латинские буквы;
  - В настройке Прописные латинские буквы укажите, будет ли одноразовый пароль содержать прописные латинские буквы;
  - В настройке Специальные символы укажите, будет ли одноразовый пароль содержать специальные символы.

## Защита от спама

Механизм защиты от спама основан на расчете процента успешных аутентификаций относительно всех отправленных сообщений за указанный интервал времени. При этом расчет запускается, только если количество отправленных сообщений превышает количество, заданное вами в настройке Окно оценки.

При обнаружении спам-атаки дальнейшая отправка сообщений блокируется на заданный период времени, а при попытке входа возникает ошибка *Potential spam attack detected*.

Отправка сообщений возобновляется либо по истечении заданного периода, либо по достижении определенного количества (в процентном отношении) успешных аутентификаций.

Чтобы настроить защиту от спама, выполните следующее:

1. В Management Console в разделе Конфигурация→Аутентификаторы выберите аутентификатор.
2. В секции Настройки защиты от спама выполните следующие настройки:
  - включите или отключите защиту от спама;
  - в поле Окно оценки попыток аутентификации укажите, в течение какого времени будет выполняться расчет процента успешных попыток входа;
  - в поле Пороговое окно попыток аутентификации укажите, сколько попыток входа должно производиться за время, указанное в окне оценки попыток аутентификации;
  - в поле Процент успешных попыток аутентификации укажите минимальный процент успешных входов относительно всех отправленных сообщений.

### ▼ Пример

---

Настройка включена со следующими значениями:

- Окно оценки попыток аутентификации — 600
- Пороговое окно попыток аутентификации — 20
- Процент успешных попыток аутентификации — 85

Защита от спама включится, если произойдет 21 попытка входа (отправлено 21 сообщение). Произойдет блокировка аутентификатора на 600 секунд.

Аутентификатор разблокируется в одном из случаев:

- процент успешных входов (пользователь успешно ввел одноразовый пароль из сообщения) достигнет значения 85;
- прошло 600 секунд с момента блокировки.



### ИНФОРМАЦИЯ

События лог-сервера:

- 2090: Обнаружена потенциальная спам-атака. Отправка сообщений приостановлена.
- 1118: Отправка сообщений пользователям возобновлена.

# Indeed AM Windows Password Provider

Провайдер Indeed AM Windows Password может быть использован для аутентификации в следующих модулях:

- Identity Provider,
- Windows Logon.

|                                        |
|----------------------------------------|
| Идентификатор провайдера               |
| {CF189AF5-01C5-469D-A859-A8F2F41ED153} |

## Установка провайдера

1. Запустите файл для установки, расположенный по пути *Indeed AM <номер версии>/Indeed AM Providers/Indeed AM Windows Password Provider/<номер версии>*, и следуйте шагам мастера 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.

## Проверка учетных данных

При аутентификации через провайдер Windows Password можно настроить проверку учетных данных на контроллере домена. Для этого выполните следующие действия:

1. В Management Console перейдите в раздел Конфигурация→Аутентификаторы и выберите из списка Пароль Windows.
2. В разделе Основные настройки выберите приоритетный способ проверки учетных данных:
  - Logon User (значение по умолчанию) — используется только для Windows на машинах внутри домена, либо на машинах из другого домена, если между доменами настроены доверительные отношения. Если выбран LogonUser, но использовать его невозможно, то далее используется способ проверки пароля Ldap Bind.



- Ldap Bind — используется, если Core Server на Windows развернут вне домена, либо если Core Server развернут на Linux.



#### **ПРИМЕЧАНИЕ**

Если вы выбрали Ldap Bind, то пользователь при попытке входа с истекшим паролем Windows не будет получать уведомление *Срок действия пароля истек*.

# Indeed AM Passcode Provider

Indeed AM Passcode Provider предназначен для аутентификации пользователей по самостоятельно заданному паролю и совместного использования с продуктами Indeed AM.

Идентификатор провайдера

{F696F05D-5466-42b4-BF52-21BEE1CB9529}

## Предварительные требования

Для работы провайдера требуется установка Indeed AM Bsp Broker на сервере Indeed AM.

Файлы для Indeed Bsp Broker расположены в папке *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-битных ОС.
- *IndeedEA.AuthProviders.BspBroker-<номер версии>.x86.ru-ru.msi* — пакет для установки Indeed Bsp Broker на 32-битных ОС.

## Установка провайдера

1. Запустите файл для установки, расположенный по пути *Indeed AM <номер версии>/Indeed AM Providers/Indeed AM Passcode Provider/<номер версии>*, и следуйте шагам мастера установки.



### ВАЖНО

Если в инфраструктуре используется несколько Core Server, 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.

### ⓘ ДОПОЛНИТЕЛЬНЫЕ НАСТРОЙКИ

Чтобы настроить требования к паролю, перейдите в раздел с настройками групповых политик для Passcode.

# Indeed AM MFA Provider

Провайдер Indeed AM MFA Provider позволяет задать последовательность провайдеров в цепочке многофакторной аутентификации.

MFA Provider может быть использован для аутентификации в следующих модулях:

- **Windows Logon,**
- **Enterprise SSO,**
- **NPS RADIUS Extension.**

Идентификатор провайдера

{070719BA-EB57-4EA8-BB4D-D15A33E7363D}

## Установка провайдера

1. Установите MFA Provider и провайдеры, которые будут использованы в цепочке, компьютере с установленным Core Server и на клиентском компьютере.

Чтобы установить MFA Provider, запустите файл, расположенный по пути *Indeed AM <номер версии>/Indeed AM Providers/Indeed AM MFA Provider*, и следуйте шагам мастера установки.



### ВАЖНО

Если в инфраструктуре используется несколько Core Server, то установку провайдера необходимо выполнить на всех серверах инфраструктуры.

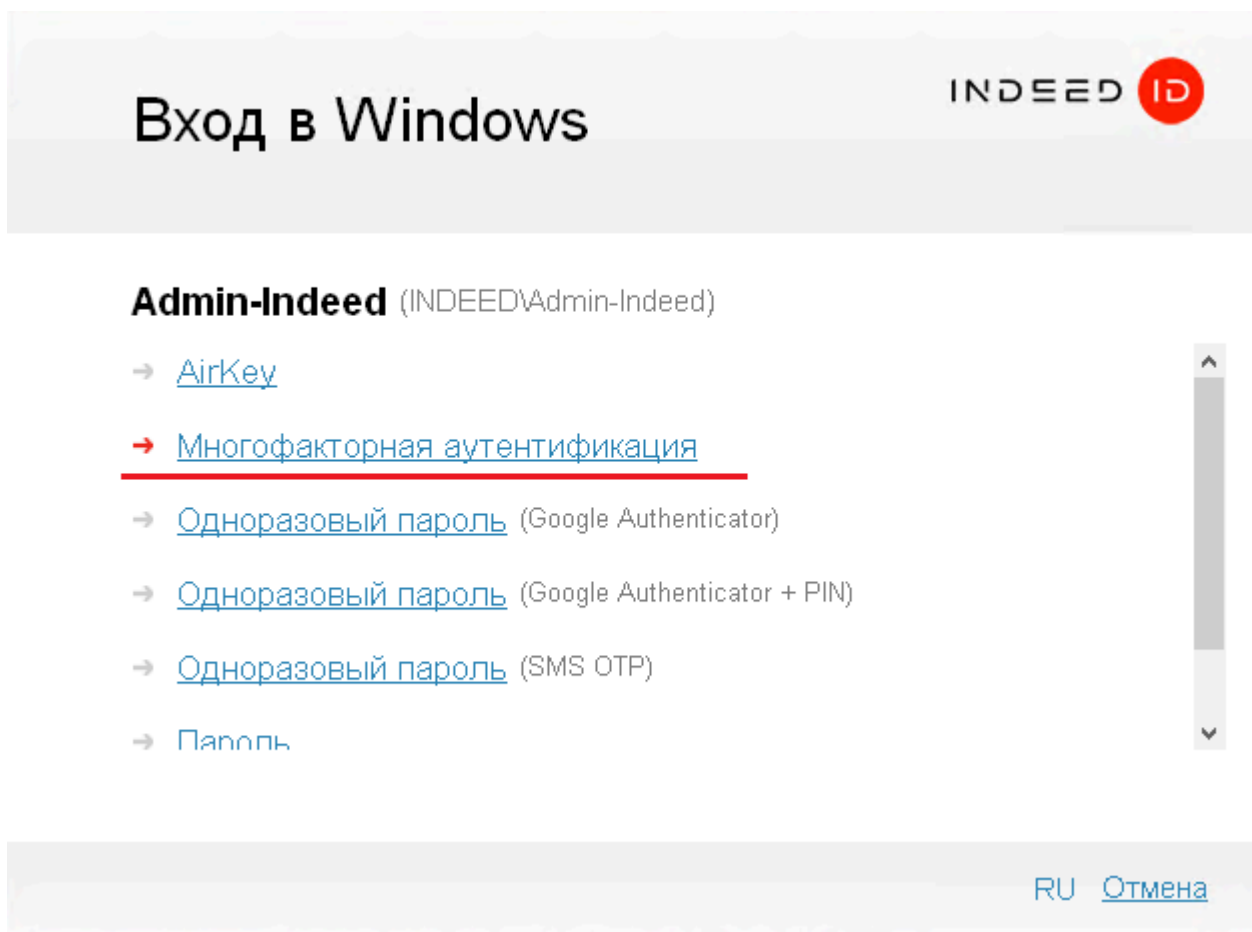
2. После завершения установки может потребоваться перезагрузка системы. Если программа установки предлагает выполнить перезагрузку, подтвердите данное действие.
3. Удаление/Восстановление продукта осуществляется стандартным для поддерживаемых ОС способом, через меню Панель управления.

## Пример аутентификации

В примере используется компонент Indeed AM Windows Logon и цепочка провайдеров Indeed AM Passcode + Indeed AM SMS OTP.

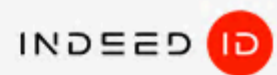
Чтобы выполнить вход с помощью MFA Provider, выполните следующее:

1. Выберите провайдер аутентификации Многофакторная аутентификация.



2. Введите данные для первого провайдера в цепочке.

# 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 и выполните вход.

# Вход в Windows



## Admin-Indeed (INDEED\Admin-Indeed)

Введите одноразовый пароль, полученный в SMS



Вход

→ [Сменить способ входа](#)

EN [Отмена](#)

### ⓘ ДОПОЛНИТЕЛЬНЫЕ НАСТРОЙКИ

Чтобы настроить параметры аутентификации, перейдите в раздел с настройками групповых политик для MFA.

# Indeed AM Smart Card Provider

Компонент Indeed AM Smart Card Provider предназначен для аутентификации пользователей по персональным устройствам (смарт-картам, USB-ключам).



## ПРИМЕЧАНИЕ

Этот тип аутентификаторов можно зарегистрировать только с помощью утилиты управления аутентификаторами.

Этот способ аутентификации поддерживается в следующих модулях:

- **Windows Logon,**
- **Enterprise SSO.**

Поддерживаются следующие устройства:

### ▼ Устройства Рутокен

---

- Рутокен S,
- Рутокен ЭЦП,
- Рутокен ЭЦП 2.0,
- Рутокен Lite.

### ▼ Устройства eToken

---

- eToken Pro 32k,
- eToken Pro 64k,
- eToken Pro Java 72k.



#### ▼ **Устройства ESMART**

---

- Token 64k,
- Token SC 64k,
- Token USB 64k.

#### ▼ **Устройства Avest**

---

- Avest Key 256A.

#### ▼ **Устройства SafeNet**

---

- iKey 1000,
- iKey 1032.

#### ▼ **Устройства JaCarta**

---

- JaCarta PKI.

#### ▼ **Устройства Gemalto**

---

- IDPrime MD.

Возможны варианты использования одного и того же устройства аутентификации как с запросом PIN-кода, так и без него:

- компонент Indeed AM Smart Card Provider позволяет пользователю пройти аутентификацию с помощью карты, PIN-код запрашиваться не будет;
- компонент Indeed AM Smart Card Provider + PIN требует ввод PIN-кода при каждой аутентификации пользователя.

### ПРИМЕЧАНИЕ

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.

Идентификатор провайдера

Smartcard {0AF65AD8-DB77-4B64-B489-958D9B36E28C}

Smartcard + PIN {42456525-8EC1-4AB1-97B8-45AF8635D10F}

## Предварительные требования

Для работы провайдера требуется установка Indeed AM Bsp Broker на сервере Indeed AM.

Файлы для Indeed AM Bsp Broker расположены в папке *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-битных ОС.
- *IndeedAM.AuthProviders.BspBroker-<номер версии>.x86.ru-ru.msi* — пакет для установки Indeed Bsp Broker на 32-битных ОС.

## Установка провайдера

1. Запустите файл для установки, расположенный по пути *Indeed AM <номер версии>/Indeed AM Providers/Indeed AM SmartCard Provider/<номер версии>*, и следуйте шагам мастера установки. Установить провайдер нужно как на компьютере с установленным Core Server, так и на клиентском компьютере.

### ВАЖНО

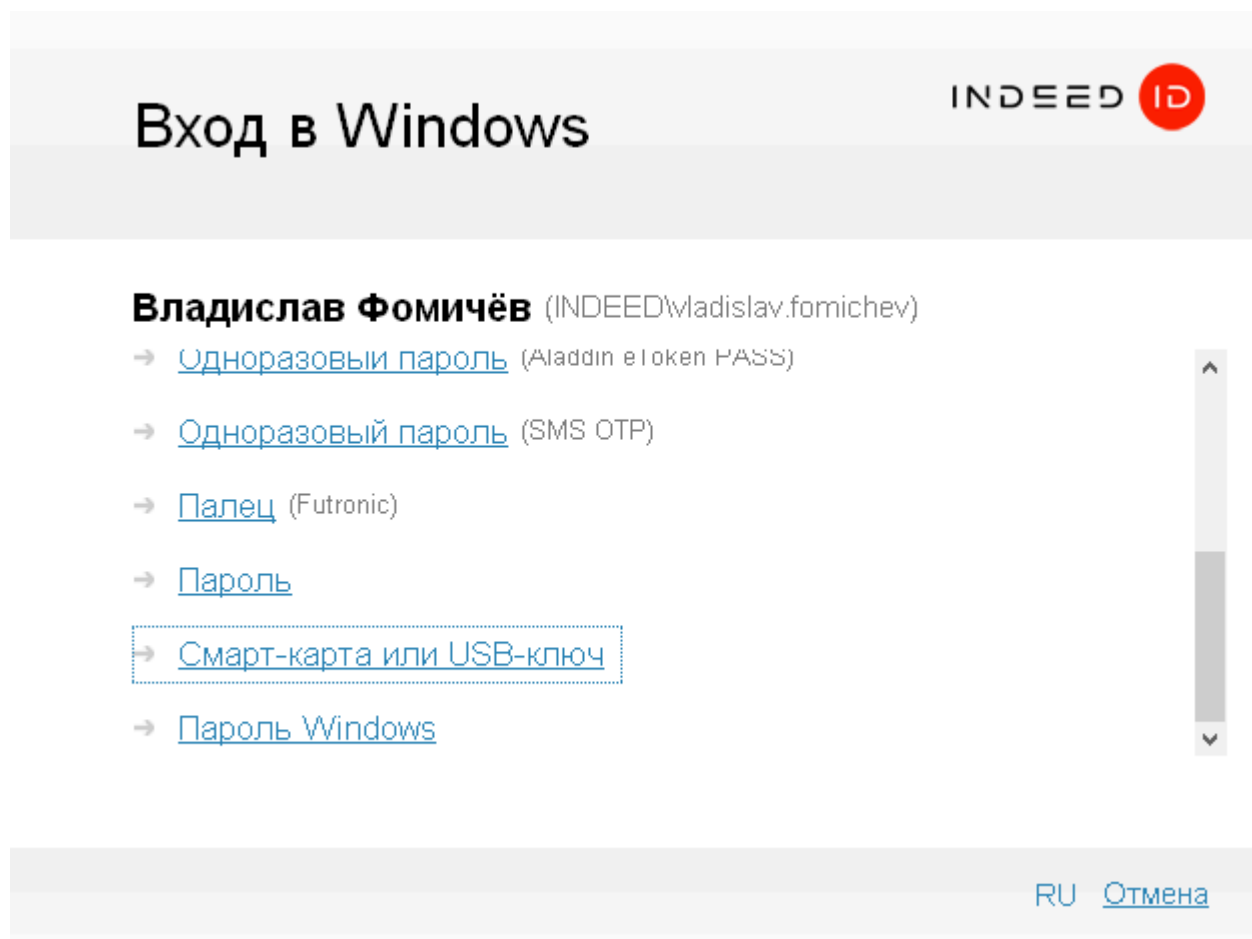
Если в инфраструктуре используется несколько Core Server, то установку провайдера необходимо выполнить на всех серверах инфраструктуры.

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.

## Пример аутентификации

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** 

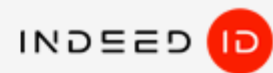
**Владислав Фомичёв** (INDEEDwladislav.fomichev)

- [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 способ входа Indeed AM Smart Card Provider + PIN, введите PIN-код и нажмите кнопку Вход.

# Вход в Windows



**Владислав Фомичёв** (INDEED\vladislav.fomichev)



Выберите смарт-карту или токен

Token: 0641367757

Ok

→ [Сменить способ входа](#)

RU [Отмена](#)

- 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

Indeed AM IronLogic Z2USB Provider необходим для аутентификации пользователей с применением считывателей IronLogic.



## ВАЖНО

Для корректной работы провайдера требуется специализированная версия считывателя IronLogic Z-2 USB (мод. Indeed). Работа других версий Z-2 USB с Indeed Access Manager не гарантирована.

Подробную информацию о считывателях и метках IronLogic вы можете получить на [сайте компании-производителя](#).



## ПРИМЕЧАНИЕ

Этот тип аутентификаторов можно зарегистрировать только с помощью [утилиты управления аутентификаторами](#).

Indeed AM IronLogic Z-2 USB Provider поддерживается в следующих модулях:

- **Windows Logon,**
- **Enterprise SSO.**

Идентификатор провайдера

Z-2 USB {CB5109DA-B575-422C-8805-524FE12B02F5}

Z-2 USB + PIN {1EDFD6E1-FD66-4A5B-971A-CBA0C611BA9B}

## Предварительные требования

Для работы провайдера требуется установка Indeed AM Bsp Broker на сервере Indeed AM.

Файлы для Indeed Bsp Broker расположены в папке *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-битные ОС;
- *IndeedEA.AuthProviders.BspBroker-<номер версии>.x86.ru-ru.msi* — пакет для установки Indeed Bsp Broker на 32-битные ОС.

## Установка провайдера

1. Запустите файл для установки, расположенный по пути *Indeed AM <номер версии>/Indeed AM Providers/Indeed AM IronLogic Z2USB Provider/<номер версии>*, и следуйте шагам мастера установки. Установить провайдер нужно как на компьютере с установленным Core Server, так и на клиентском компьютере.



### ВАЖНО

Если в инфраструктуре используется несколько Core Server, то установку провайдера необходимо выполнить на всех серверах инфраструктуры.

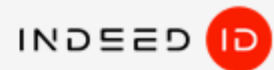
2. После завершения установки может потребоваться перезагрузка системы. Если программа установки предлагает выполнить перезагрузку, подтвердите данное действие.
3. Удаление/Восстановление продукта осуществляется стандартным для поддерживаемых ОС способом, через меню Панель управления.

## Пример аутентификации

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



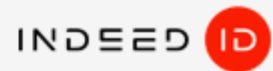
**Владислав Фомичёв** (INDEED\vladislav.fomichev)

- [AirKey](#)
- [Карта](#) (HID OMNIKEY Smart Card Reader)
- [Карта](#) (Z2 USB Card Reader)
- [Карта + PIN](#) (HID OMNIKEY Smart Card Reader)
- [Многофакторная аутентификация](#)
- [Одноразовый пароль](#) (Google Authenticator)

RU [Отмена](#)

2. Подключите считыватель карт Z-2 USB и положите на считыватель зарегистрированную карту.

# Вход в Windows



**Владислав Фомичёв** (INDEED\vladislav.fomichev)



Пожалуйста, положите карту на считыватель Z2-USB для аутентификации

→ [Сменить способ входа](#)

RU [Отмена](#)

- 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



**Владислав Фомичёв** (INDEEDwladislav.fomichev)



Идентификационные данные получены. Идет обработка...

→ [Сменить способ входа](#)

RU [Отмена](#)

## ⓘ ДОПОЛНИТЕЛЬНЫЕ НАСТРОЙКИ

Чтобы определить поведение при извлечении смарт-карты, настроить таймаут выполнения действия при извлечении смарт-карты и указать формат хранения идентификаторов карт в базе данных Indeed AM, перейдите в раздел с настройками групповых политик для IronLogic Z2USB Provider.

# Indeed AM OMNIKEY Provider

Компонент обеспечивает работу считывателей смарт-карт HID OMNIKEY с модулями Indeed Access Management. Подробную информацию о считывателях и картах OMNIKEY вы можете получить на [сайте компании-производителя](#).

## ⚠ ПРИМЕЧАНИЕ

Этот тип аутентификаторов можно зарегистрировать только с помощью [утилиты управления аутентификаторами](#).

Indeed AM OMNIKEY Provider поддерживается в следующих модулях:

- [Windows Logon](#),
- [Enterprise SSO](#).

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.

Идентификатор провайдера

OMNIKEY {4B15AF52-A795-4CA6-B7CD-CDB8ABF2D2C2}

OMNIKEY + PIN {199B8FA8-FA9D-4ED8-941D-F86A5C681E0C}

## Предварительные требования

Для работы провайдера требуется установка Indeed AM Bsp Broker на сервере Indeed AM.

Файлы для Indeed Bsp Broker расположены в папке *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-битные ОС;
- *IndeedEA.AuthProviders.BspBroker-<номер версии>.x86.ru-ru.msi* — пакет для установки Indeed Bsp Broker на 32-битные ОС.

## Установка провайдера

1. Запустите файл для установки, расположенный по пути *Indeed AM <номер версии>/Indeed AM Providers/Indeed AM OMNIKEY Provider/<номер версии>*, и следуйте шагам мастера установки. Установить провайдер нужно как на компьютере с установленным Core Server, так и на клиентском компьютере.



### ВАЖНО

Если в инфраструктуре используется несколько Core Server, 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.

## Пример аутентификации

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 (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 считыватель зарегистрированную карту.

# Вход в Windows



**Владислав Фомичёв** (INDEED\vladislav.fomichev)



Пожалуйста, положите карту на считыватель OMNIKEY для аутентификации

→ [Сменить способ входа](#)

RU [Отмена](#)

- 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.

## ⓘ ДОПОЛНИТЕЛЬНЫЕ НАСТРОЙКИ

Чтобы определить поведение при извлечении смарт-карты, настроить таймаут выполнения действия при извлечении смарт-карты и разрешить/запретить использовать данные PACS, перейдите в раздел с настройками групповых политик для OMNIKEY Provider.

# Indeed AM Futronic Provider

Indeed AM Futronic Provider необходим для аутентификации пользователей с применением биометрического сканера Futronic FS80. Подробную информацию об устройствах Futronic вы можете получить на официальном [сайте компании Futronic Technologies](#).



## ПРИМЕЧАНИЕ

Этот тип аутентификаторов можно зарегистрировать только с помощью [утилиты управления аутентификаторами](#).

Indeed AM Futronic Provider поддерживается в следующих модулях:

- [Windows Logon](#),
- [Enterprise SSO](#).

Идентификатор провайдера

{A0EF00AD-1EEB-4D48-8BCF-06E19CD5585F}

## Предварительные требования

Для работы провайдера требуется установка Indeed AM Bsp Broker на сервере Indeed AM.

Файлы для Indeed Bsp Broker расположены в папке *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-битные ОС;
- *IndeedEA.AuthProviders.BspBroker-<номер версии>.x86.ru-ru.msi* — пакет для установки Indeed Bsp Broker на 32-битные ОС.

## Установка провайдера

1. Запустите файл для установки, расположенный по пути *Indeed AM <номер версии>/Indeed AM Providers/Indeed AM Futronic Provider/<номер версии>*, и следуйте шагам мастера

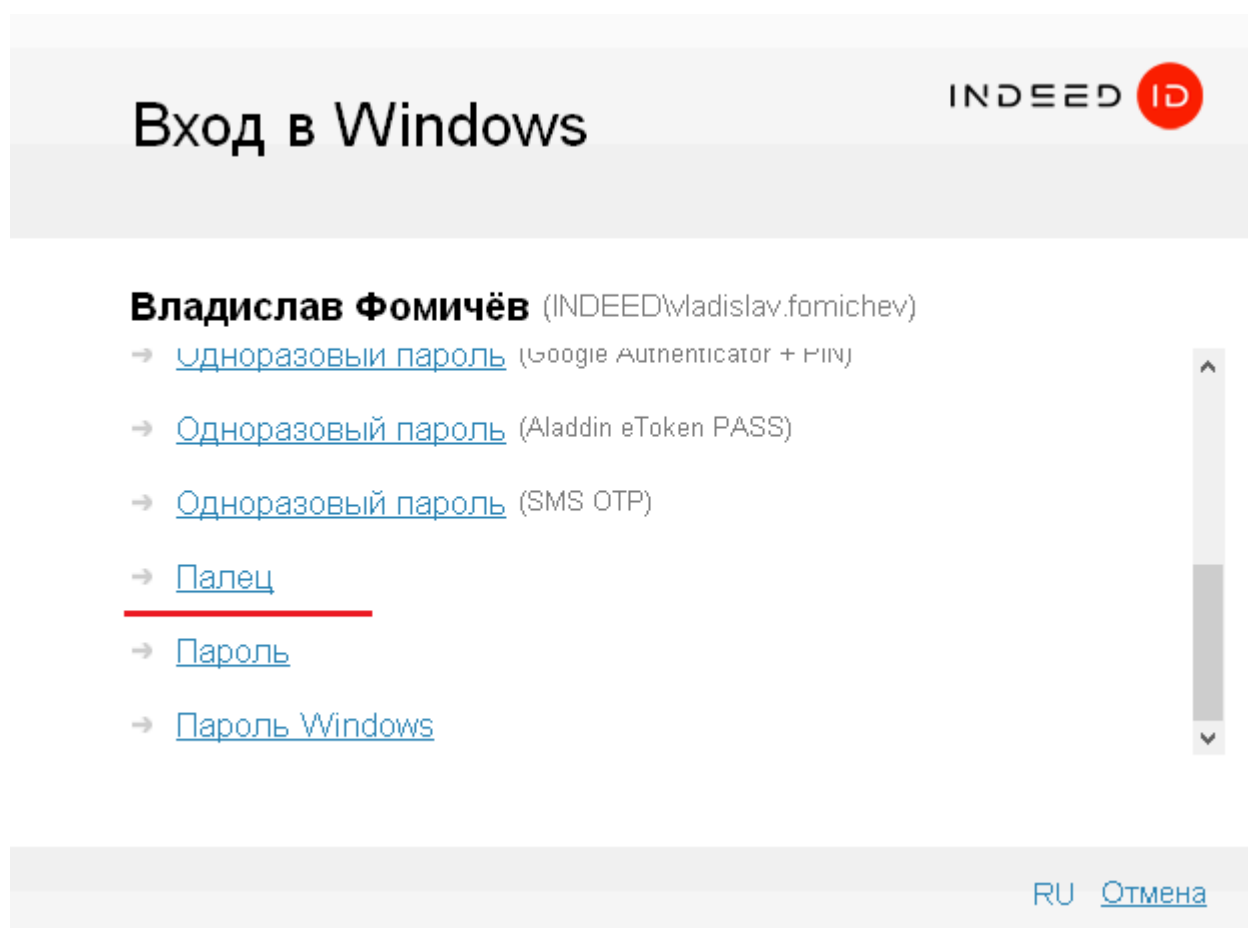
установки. Установить провайдер нужно как на компьютере с установленным Core Server, так и на клиентском компьютере.

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.

## Пример аутентификации

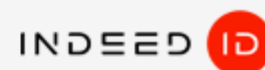
1. При первом входе в систему или приложение с использованием технологии аутентификации Indeed AM необходимо выбрать способ входа.

Для этого нажмите Сменить способ входа в окне Вход в Windows. Выберите способ аутентификации *Палец*.



2. Подключите биометрический сканер к компьютеру и приложите к сканеру палец.

# Вход в Windows



**Владислав Фомичёв** (INDEED\vladislav.fomichev)



Приложите палец к сканеру

→ [Сменить способ входа](#)

RU [Отмена](#)

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.



# Миграция настроек провайдеров

В Indeed AM, начиная с версии 8.2, настройки провайдеров аутентификации располагаются в Management Console. При обновлении с более ранних версий можно перенести настройки провайдеров, уже заданные ранее в политиках и реестре, с помощью утилиты *EA.Settings.Migration.Tool*. Эта утилита также позволяет настроить отображение настройки принудительной проверки аутентификаторов OTP.

При миграции настроек из политик переносятся настройки аутентификаторов самой приоритетной политики.

Можно перенести настройки следующих провайдеров:

- **Indeed Key;**
- **Telegram;**
- **Email OTP;**
- **SMS OTP;**
- **Storage SMS OTP.**

В результате будут перенесены следующие настройки:

- доступные пользователю действия с аутентификаторами, которые требуют регистрации;
- заданное в приоритетной политике максимальное количество аутентификаторов, которые требуют регистрации;
- заданные в приоритетной политике настройки опции Запретить использовать для всех установленных аутентификаторов.

## Подготовка

Перед тем, как провести миграцию настроек:

1. Расшифруйте конфигурационный файл Core Server *C:\inetpub\wwwroot\am\core\Web.config* одним из способов:
  - С помощью мастера конфигурации. Откройте файл *C:\inetpub\wwwroot\am\core\Web.config*, пройдите заново все шаги и на шаге Шифрование файла отключите опцию Шифровать конфигурационный файл (рекомендуется).

- С помощью скрипта *decryptConfigs.bat*. Подробнее — в [Indeed Core Server](#).
2. **Создайте резервную копию** базы данных.
  3. **Создайте резервные копии** конфигурационных файлов и реестра серверных компонентов вручную или с помощью **утилиты UpdateHelper**.
  4. При миграции настроек из реестра убедитесь, что на сервере с установленным Core Server действует групповая политика с настройками реестра.
  5. При миграции настроек из политики сделайте резервную копию папки *C:/inetpub/wwwroot/am/core* для версии Access Manager 8.1.x перед обновлением сервера до версии 8.2.x. Эта папка будет использована как источник данных.

## Миграция

Чтобы перенести настройки с помощью утилиты:

1. Запустите файл *Indeed AM 8.2.x\Indeed Access Manager Server\8.2.x\Misc\EA.Settings.Migration.Tool\EA.Settings.Migration.Tool.exe*.
2. Подтвердите, что создали резервную копию БД.
3. Введите адрес Core Server в формате *http(s)://полноеднsumя\_сервера/am/core/*.
4. При необходимости введите учетные данные для доступа к Core Server.
5. Укажите путь до конфигурационного файла Core Server.
6. Стрелками на клавиатуре выберите одну из опций и выполните необходимые для нее действия:
  - Auth method settings — миграция настроек из реестра. После выбора этой опции отметьте провайдеры, настройки которых нужно перенести, с помощью пробела или сочетания клавиш *Ctrl+A* (чтобы выбрать все провайдеры).
  - Policy settings — миграция настроек из политики. После выбора этой опции введите путь к резервной копии конфигурационного файла Core Server *Web.config*. Затем выберите политику для переноса настроек.
  - Forced Authenticator Verification policy — для отображения настройки принудительной проверки аутентификатора в Management Console.

 **ПРИМЕЧАНИЕ**

Отображение настройки принудительной проверки аутентификатора выполняется только для уже установленных провайдеров аутентификации по одноразовым паролям. После установки новых провайдеров миграцию нужно проводить повторно.

7. Нажмите Enter.

8. В отобразившемся логге убедитесь, что миграция настроек прошла успешно.

 **ВАЖНО**

После переноса настроек проверьте количество аутентификаторов в настройке Максимальное количество для каждого провайдера в Management Console.

# Административные шаблоны групповых политик (ADMX)

Некоторые настройки Indeed AM задаются групповыми политиками Microsoft.

## ⓘ ПРИМЕЧАНИЕ

Перед настройкой групповых политик добавьте шаблоны политик Indeed AM в список административных шаблонов. Файлы шаблонов политик входят в состав дистрибутива Indeed AM и расположены в каталоге *Misc\ADMX Templates*.

Действие политики представляет из себя добавление определенных ключей в реестр, при необходимости значения политик можно добавить в реестр вручную. При добавлении вручную создайте недостающие разделы реестра.

## Добавление административных шаблонов

1. Скопируйте файлы шаблонов групповых политик из каталога дистрибутива *C:\Indeed\Indeed AM <номер версии>\Misc\ADMX Templates* в один из следующих каталогов:
  - *C:\Windows\PolicyDefinitions* — локальное хранилище ADMX-файлов.
  - *C:\Windows\SYSVOL\sysvol\ИМЯ\_ДОМЕНА\Policies\PolicyDefinitions* — хранилище ADMX-файлов на контроллере домена.

Если каталог *PolicyDefinitions* отсутствует, создайте его.
2. Скопируйте файл *IndeedID.BaseFile.admx* и все необходимые ADMX-файлы в каталог *\PolicyDefinitions*.
3. Скопируйте файл *IndeedID.BaseFile.adml* и все ADML-файлы, аналогичные скопированным ADMX-файлам, из каталога *\Indeed AM <номер версии>\Misc\ADMX Templates\<en-US или ru-RU>* в каталог *\PolicyDefinitions\en-US* (для англоязычной локализации сервера) или *\PolicyDefinitions\ru-RU* (для русскоязычной локализации сервера).
4. Скопируйте шаблоны из папки *ADMX Templates\BSPs* в корневую папку *PolicyDefinitions* рядом с остальными ADMX-файлами.

5. Добавьте шаблоны политик и провайдеров аутентификации в раздел Конфигурация компьютера (Computer Configuration). Добавьте шаблоны политик Indeed AM Paste в раздел Конфигурация пользователя (User Configuration).

После загрузки групповые политики Indeed ID станут доступны в Редакторе локальных групповых политик (Group Policy Management Editor в разделе ADMX files).

## Настройка с помощью Редактора локальной групповой политики

При настройке политик можно использовать консоль редактора групповой политики gredit.msc для управления параметрами в реестре.

## Настройка с помощью Редактор реестра

При настройке политик вручную откройте Редактор реестра:

1. В поле поиска на панели задач введите regedit, затем выберите Редактор реестра.
2. Перейдите в необходимый раздел в зависимости от провайдера, который вы настраиваете, или создайте этот раздел. Например,  
*Компьютер\HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Indeed-ID.*



### ВАЖНО

Будьте осторожны при использовании Редактора реестра. Если вы неправильно отредактируете реестр, могут возникнуть серьезные проблемы, требующие полной переустановки операционной системы или приводящие к потере данных.

# Провайдеры аутентификации



## Indeed Key

Политики распространяются на машины с установленными компонентами Indeed



## Telegram

Таймаут операции для приложения Telegram



## Software OTP

Настройка параметров аутентификации



## HOTP

Настройки синхронизации и проверки одноразового пароля



## Hardware TOTP

Настройки синхронизации и проверки одноразового пароля



## SMS OTP

Выбор типа подключения



## Storage SMS OTP

Сервис отправки СМС



## Email OTP

Настройки SMTP-сервера



## Passcode

Настройка хранения пароля



## MFA

Настройка параметров аутентификации



## Smart Card

Поведение при извлечении смарт-карты



## IronLogic Z2USB

Поведение при извлечении смарт-карты



## Omnikey

Поведение при извлечении смарт-карты



## Futronic

Минимально допустимое качество шаблона при обучении

# Indeed Key

## ⓘ ПРИМЕЧАНИЕ

Политики распространяются на машины с установленными компонентами Indeed AM Windows Logon и Indeed AM ESSO Agent.

## Таймаут операции для приложения Indeed Key

Политика определяет время ожидания операции для приложения Indeed Key.

## Требовать команды от пользователя

Политика указывает ждать команды от пользователя для активации процедуры входа.



# Telegram

## Таймаут операции для приложения Telegram

Политика определяет время ожидания операции для приложения Indeed Key.

## Требовать команды от пользователя

Политика указывает ждать команды от пользователя для активации процедуры входа.

# Software OTP

## Настройка параметров аутентификации

Перед настройкой групповой политики добавьте шаблоны политик Indeed AM в список административных шаблонов. Файлы шаблонов политик входят в состав дистрибутива провайдера и расположены в папке *Misc*.

### ПРИМЕЧАНИЕ

Настройка политик необходима для повышения уровня безопасности. Однако полноценная работа Software OTP Provider возможна и со значениями политик, определенными по умолчанию.

- Длина одноразового пароля — политика определяет количество цифр в одноразовом пароле. Возможно задать значение 6 или 8. Если политика не определена, по умолчанию используется значение 6.

### ВАЖНО

При использовании провайдера Software OTP в сценариях с модулями Indeed Enterprise Single Sign-On и Indeed Windows Logon в настоящее время поддерживается использование только шестизначного пароля.

- 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 — политика позволяет задать параметр пользователя в качестве имени OTP-аккаунта, который будет передаваться в QR-коде. Возможные параметры:
  - CanonicalName,
  - CN,

- DistinguishedName,
- FullName,
- Mail,
- PrincipalName,
- SamCompatibleName.

**ПРИМЕЧАНИЕ**

Политика применяется к серверам с установленной Management Console. Если политика не была применена, в качестве имени OTP-аккаунта будет использоваться имя пользователя.

Формат имени

Формат имени

Предыдущий параметр Следующий параметр

☐ Не задано
 ☒ Включено
 ☐ Отключено

Комментарий:

Требования к версии: Windows XP и более поздние версии

Параметры: Справка:

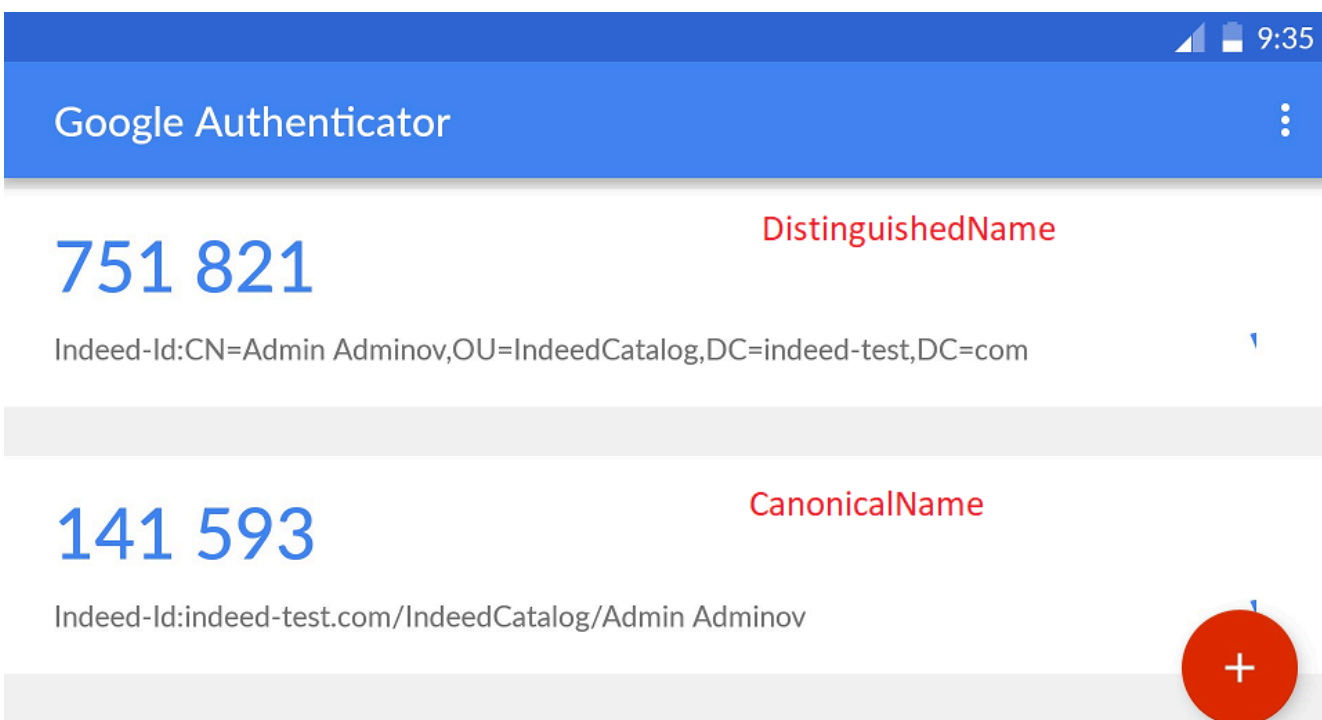
Формат имени: CanonicalName

CanonicalName  
 CN  
 DistinguishedName  
 FullName  
 Mail  
 PrincipalName  
 SamCompatibleName

Формат имени. Возможные значения:

- CanonicalName,
- PrincipalName,
- SamCompatibleName,
- DistinguishedName,
- FullName,
- CN,
- Mail.

OK Отмена Применить



## Настройка алгоритма шифрования

В Indeed Access Manager 8.2 и выше вы можете задать алгоритм шифрования для Software OTP Provider. Если алгоритм шифрования не задан, по умолчанию используется значение SHA1. Настройку можно выполнить через GPO или редактор реестра Windows.

### Через GPO

1. Откройте редактор GPO.
2. Перейдите к Конфигурация компьютера→Административные шаблоны→ Indeed ID→Id Providers→SoftwareTOTP.
3. Включите политику Длина секрета и выберите необходимое значение.

### В реестре

1. Откройте редактор реестра на машине, где развернуты **Management Console** и **User Console**.

2. Откройте раздел *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Indeed-ID\BSPs* и выберите или создайте раздел *GoogleOTP*.
3. Создайте параметр **SecretLength** типа DWORD и укажите одно из следующих значений в десятичной системе исчисления:
  - 20 — для алгоритма SHA1,
  - 32 — для алгоритма SHA256,
  - 64 — для алгоритма SHA512.

# НОТР

## Настройки синхронизации и проверки одноразового пароля

Задаёт интервал значений счетчика при синхронизации и при проверке одноразового пароля.

Значения по умолчанию:

- Окно синхронизации — 2000;
- Окно проверки одноразового пароля — 5.

Настройки синхронизации и проверки одноразового пароля

Предыдущий параметр    Следующий параметр

☐ Не задано    Комментарий:

☒ Включено

☐ Отключено

Требования к версии: Windows XP и более поздние версии

Параметры:    Справка:

Окно синхронизации: 1000

Окно проверки одноразового пароля: 5

Задаёт интервал значений счетчика при синхронизации и при проверке одноразового пароля.

ОК    Отмена    Применить

# Hardware TOTP

## Настройки синхронизации и проверки одноразового пароля

Задаёт интервал значений счетчика при синхронизации и при проверке одноразового пароля.

Значения по умолчанию:

- Окно синхронизации — 100;
- Окно проверки одноразового пароля — 1.

Настройки синхронизации и проверки одноразового пароля

Предыдущий параметр    Следующий параметр

☐ Не задано    Комментарий:

☒ Включено

☐ Отключено

Требования к версии: Windows XP и более поздние версии

Параметры:    Справка:

Окно синхронизации: 100

Окно проверки одноразового пароля: 1

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

## 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.

Настройки времени устройства

Настройки времени устройства

Предыдущий параметр Следующий параметр

☐ Не задано ☒ Включено ☐ Отключено

Комментарий:

Требования к версии: Windows XP и более поздние версии

Параметры: Справка:

Соответствие модели устройства и начального времени:

Показать...

Задаёт соответствие модели и начального времени устройства.

Введите в поле "Value Name" модель устройства, в поле "Value" начальное время устройства, шаг времени и длину одноразового пароля через точку с запятой.

Например:  
Value Name=eTPass 6.20  
Value=1/1/2000;30;6

OK Отмена Применить



❗ **ИНФОРМАЦИЯ**

В поле Имя значения указывается имя устройства, в поле Значение указываются параметры: *Начальное время, Шаг, Длина пина*.

Вывод содержания

Соответствие модели устройства и начального времени:

|   | Имя значения | Значение      |
|---|--------------|---------------|
| ▶ | eTPass 6.20  | 1/1/2000;30;6 |
| * |              |               |

OK Отмена

# SMS OTP

## Выбор типа подключения

### Через GPO

Политика применяется к серверам Indeed AM и предназначена для выбора Sender провайдера SMS OTP.

*Не задан (Not Configured) или Отключен (Disabled)* — будет использоваться подключение по SMPP.

*Включен (Enabled)* — будет использоваться подключение по заданному провайдеру.

### В реестре

1. Откройте редактор реестра на сервере Indeed AM.
2. Откройте раздел `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\BSPs\SMSOTP`.
3. Создайте параметр `SmsSenderType` с типом `DWORD` со следующими значениями:
  - 0 — Smpp;
  - 1 — Megafon;
  - 2 — OneGate;
  - 3 — Kafka;
  - 4 — MFM Solutions;
  - 5 — SMS Прокси,
  - 6 — Прокси сообщений.

## ▼ Настройки сервиса SMPP (Service Configurations SMPP)

### Настройки сервиса SMPP (Service Configurations SMPP)

#### Через GPO

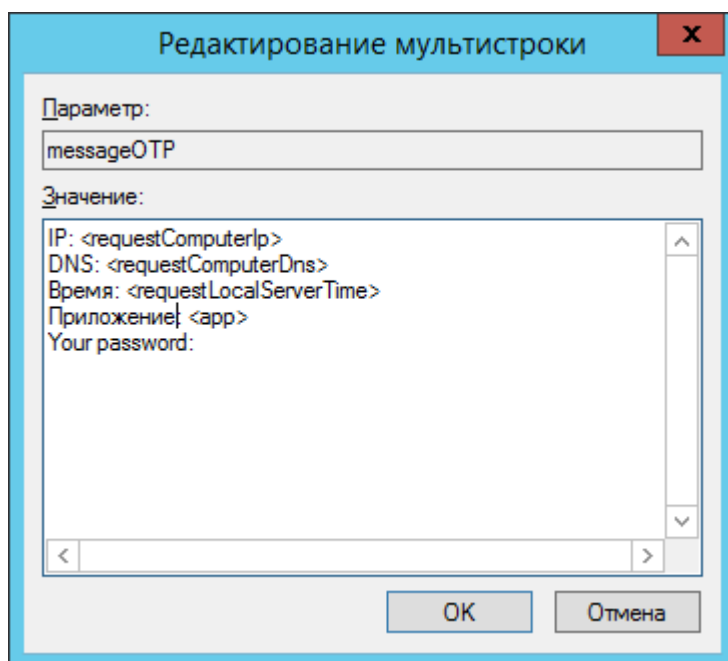
Политика применяется к серверам Indeed AM и определяет следующие настройки для сервиса SMPP:

- *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 СМС;
- *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;

 **ВАЖНО**

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 СМС 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;

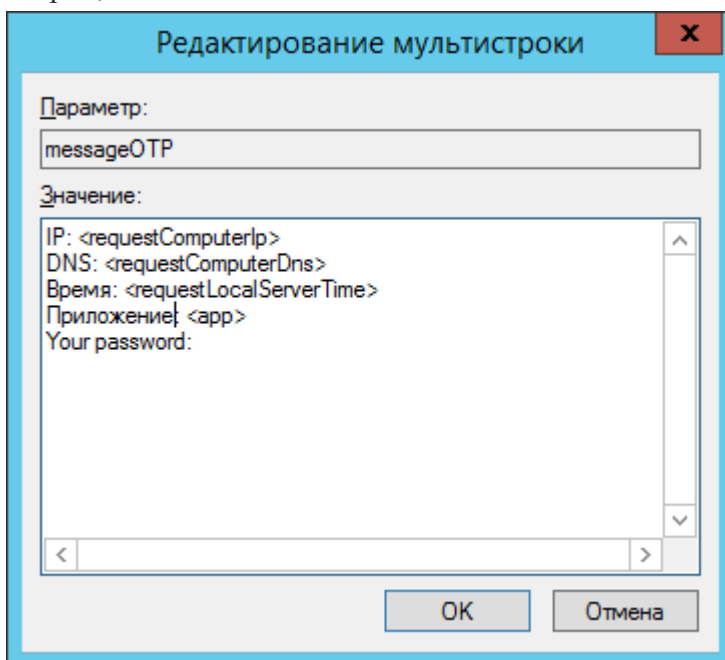
В случае подключения как Transmitter сервер присылает статус отправленного СМС-сообщения только в пакете `SUBMIT_SM_RESP`.

- *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 СМС или подтверждение SME.
- *data\_coding* — определяет схему кодировки пользовательских данных короткого сообщения.



- `srvSystemId` (REG\_SZ) — имя учетной записи для подключения к серверу;
- `srvPassword` (REG\_SZ) — пароль учетной записи для подключения к серверу;
- `srvSysType` (REG\_SZ) — поле PDU операции BIND\_TRANSCEIVER протокола SMPP;
- `senderName` (REG\_SZ) — имя отправителя, которое будет отображаться при получении CMC;
- `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;
  - `&lt;requestLocalServerTime&gt;` — локальное серверное время получения запроса;
  - `&lt;requestComputerDns&gt;` — DNS-имя компьютера отправившего запрос;
  - `&lt;requestComputerIp&gt;` — IP-адрес компьютера отправившего запрос;



- `SMPPServerTimeoutSec` (DWORD) — время ожидания получения статуса отправленного CMC с сервера;
- `MessageStatusPDU` (DWORD) — PDU, в котором сервер присылает статус отправленного сообщения. 0 — SUBMIT\_SM\_RESP; 1 — DELIVER\_SM.

- `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 СМС-сообщения только в пакете `SUBMIT_SM_RESP`;
- `sourceAddrTon` (DWORD) — тип номера (Type of Number) для исходного адреса;
- `sourceAddrNpi` (DWORD) — индикатор схемы присвоения номеров (Numbering Plan Indicator) для исходного адреса;
- `destAddrTon` (DWORD) — тип номера (Type of Number) для адресата;
- `destAddrNpi` (DWORD) — индикатор схемы присвоения номеров (Numbering Plan Indicator) для адресата;
- `esmClass` — указывает Message Mode & Message Type;
- `registeredDelivery` — индикатор для того, чтобы обозначить, что запрашивается расписка о получении СМС или подтверждение SME;
- `dataCoding` — определяет схему кодировки пользовательских данных короткого сообщения.



## ▼ Настройки резервного сервиса SMPP

---

### Настройки 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 Server 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 Server получает следующие ошибки:

- *SMS sending service address unavailable,*
- *SMPP Error Bind,*
- *SMPP Error SubmitS.*

Политика резервного сервиса SMPP настраивается аналогично основного сервиса SMPP.

При наличии настроенного резервного сервиса переход к нему при недоступности основного сервиса происходит автоматически.

## ▼ Настройки сервиса Megafon (Service Configurations Megafon)

### Настройки сервиса Megafon (Service Configurations Megafon)

#### Через GPO

Политика применяется к серверам Indeed AM и определяет настройки для Megafon — сервиса отправки СМС:

- *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 СМС;
- *Дополнительный текст перед OTP* — произвольный текст сообщения, предшествующий одноразовому паролю.

#### Настройки сервиса Megafon

 Настройки сервиса Megafon

Предыдущий параметр

Следующий па

☐ Не задано

Комментарий:

☒ Включено

☐ Отключено

Требования к версии:

Windows XP и более поздние версии

Параметры:

URL:

Логин:

Пароль:

Отправитель:

Дополнительный текст перед отправкой OTP:

## В реестре

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:
  - *ServerUrl* (REG\_SZ) — адрес подключения к серверу;
  - *Login* (REG\_SZ) — имя учетной записи для подключения к серверу;
  - *Password* (REG\_SZ) — пароль учетной записи для подключения к серверу;
  - *From* (REG\_SZ) — имя отправителя, которое будет отображаться при получении СМС;
  - *messageOTP* (REG\_SZ) — произвольный текст сообщения, предшествующий одноразовому паролю.

## ▼ Настройки сервиса OneGate (Service Configurations OneGate)

### Настройки сервиса OneGate (Service Configurations OneGate)

#### Через GPO

Политика применяется к серверам Indeed AM и определяет настройки для OneGate — сервиса отправки СМС:

- *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

Предыдущий параметр

Следующий параметр

☒ 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:

## В реестре

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:
  - *ServerUrl* (REG\_SZ) — адрес подключения к серверу;
  - *Login* (REG\_SZ) — имя учетной записи для подключения к серверу;
  - *Password* (REG\_SZ) — пароль учетной записи для подключения к серверу;
  - *NameSender* (REG\_SZ) — отображается как имя отправителя в устройстве получателя;
  - *NameSystem* (REG\_SZ) — сочетание *Имя системы отправителя* и *Имя отправителя* определяет логин, под которым обращаемся в сепаратор;
  - *messageOTP* (REG\_SZ) — произвольный текст сообщения, предшествующий одноразовому паролю.

## ▼ Настройки сервиса MFMSolution (Service Configurations MFMSolution)

---

### Настройки сервиса MFMSolution (Service Configurations MFMSolution)

#### Через GPO

Политика применяется к серверам Indeed AM и определяет настройки для MFMSolution — сервиса отправки СМС:

- *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

Настройки сервиса MFMSolution

☐ Не задано    Комментарий:

☒ Включено

☐ Отключено

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.

OK    Отмена    Применить

## В реестре

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:
  - *ServerUrl* (REG\_SZ) — адрес подключения к серверу;
  - *Login* (REG\_SZ) — имя учетной записи для подключения к серверу;
  - *Password* (REG\_SZ) — пароль учетной записи для подключения к серверу;
  - *From* (REG\_SZ) — отображается как имя отправителя в устройстве получателя;

- *MessageOTP* (REG\_SZ) — произвольный текст сообщения, предшествующий одноразовому паролю.



## Настройки сервиса Apache Kafka

### Через GPO

Политика применяется к серверам Indeed AM и определяет настройки для Apache Kafka — сервиса отправки СМС:

- *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

☐ Отключено

Требования к версии: Windows XP and later versions

Параметры:

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:

Справка:

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

## В реестре

1. Откройте редактор реестра на сервере Indeed AM.
2. Откройте раздел *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Indeed-ID\BSPs\SMSOTP*.
3. Создайте следующие параметры:
  - *SmsSenderType* (DWORD) — тип отправителя СМС (для Apache Kafka установите значение 3);
  - *ParsePhone* (DWORD) — включение парсинга телефонного номера;

- *PhonePrefix* (REG\_SZ) — префикс номера телефона (если вы включили парсинг телефонного номера);
- *PhoneLength* (DWORD) — длина номера телефона (если вы включили парсинг телефонного номера);

4. В разделе *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Indeed-ID\BSPs\SMSOTP\Kafka* создайте следующие параметры:

- *messageOTP* (REG\_SZ) — произвольный текст сообщения, предшествующий одноразовому паролю;
- *MessageFormatPath* (REG\_SZ) — путь к файлу json с форматом сообщения;
- *MessageDateFormat* (REG\_SZ) — формат даты в полях сообщения;
- *ServerUrl* (REG\_SZ) — адрес сервера Apache Kafka;
- *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;
- *TopicName* (REG\_SZ) — имя темы Apache Kafka, в которую будут публиковаться сообщения;
- *UseSerialization* (REG\_DWORD) — включение или отключение сериализации;
- *SchemaRegistryUrl* — адрес подключения к *Schema registry*;
- *RecordSchemaPath* (REG\_SZ) — путь к файлу json со схемой сериализации;

Если вы используете авторизацию в Apache Kafka, добавьте следующие параметры;

- *SecurityProtocol* (REG\_SZ) — протокол, используемый для связи с брокерами;
- *SaslMechanism* (REG\_SZ) — механизм SASL для аутентификации;

## ▼ Настройки SMS прокси (SMS Proxy)

### Настройки SMS прокси (SMS Proxy)

#### Через GPO

Политика применяется к серверам Indeed AM:

- *URL* — адрес подключения к SMS Proxy;
- *Отправитель* — имя отправителя, которое будет отображаться при получении SMS;
- *Дополнительный текст перед отправкой OTP* — произвольный текст сообщения, предшествующий одноразовому паролю;
- *Отпечаток сертификата клиента* — определяет сертификат, который будет добавлен в список сертификатов клиента при запросе к SMS Proxy (сам сертификат должен находиться в хранилище сертификатов LocalMachine/LocalComputer и удовлетворять требованиям SMS Proxy);
- *Отпечаток сертификата сервера* — определяет сертификат сервера, который будет признан валидным.

#### В реестре

1. Откройте редактор реестра на сервере Indeed AM.
2. Откройте раздел *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Indeed-ID\BSPs\SMSOTP\Proxy*.
3. Создайте следующие параметры:
  - *ServerUrl* — адрес подключения к SMS Proxy;
  - *From* (REG\_SZ) — имя отправителя, которое будет отображаться при получении сообщения;
  - *messageOTP* (REG\_SZ) — произвольный текст сообщения, предшествующий одноразовому паролю;
  - *ClientCertificateThumbprint* (REG\_SZ) — определяет сертификат, который будет добавлен в список сертификатов клиента при запросе к SMS Proxy (сам сертификат должен находиться в хранилище сертификатов LocalMachine/LocalComputer и удовлетворять требованиям SMS Proxy);

- *ServerCertificateThumbprint* (REG-SZ) — определяет сертификат сервера, который будет признан валидным.

## ▼ Настройки прокси сообщений (Messages Proxy)

### Настройки прокси сообщений (Messages Proxy)

#### Через GPO

Политика применяется к серверам Indeed AM:

- *URL* — адрес подключения к серверу;
- *Отправитель* — имя отправителя, которое будет отображаться при получении сообщения;
- *Дополнительный текст перед отправкой OTP* — произвольный текст сообщения, предшествующий одноразовому паролю;
- *Отпечаток сертификата клиента* — определяет сертификат, который будет добавлен в список сертификатов клиента при запросе к Messages Proxy (сам сертификат должен находиться в хранилище сертификатов LocalMachine/LocalComputer и удовлетворять требованиям Messages Proxy);
- *Отпечаток сертификата сервера* — определяет сертификат сервера, который будет признан валидным.

#### В реестре

1. Откройте редактор реестра на сервере Indeed AM.
2. Откройте раздел *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Indeed-ID\BSPs\SMSOTP\MessagesProxy*.
3. Создайте следующие параметры:
  - *ServerUrl* — адрес подключения к серверу;
  - *From* (REG\_SZ) — имя отправителя, которое будет отображаться при получении сообщения;
  - *messageOTP* (REG\_SZ) — произвольный текст сообщения, предшествующий одноразовому паролю;
  - *ClientCertificateThumbprint* (REG\_SZ) — определяет сертификат, который будет добавлен в список сертификатов клиента при запросе к Messages Proxy (сам

сертификат должен находиться в хранилище сертификатов

LocalMachine/LocalComputer и удовлетворять требованиям Messages Proxy);

- *ServerCertificateThumbprint* (REG-SZ) — определяет сертификат сервера, который будет признан валидным.

## Настройка формата сообщения

### Через GPO

Политика позволяет задать настройки формата отображения даты. Примеры форматов можно посмотреть [в статье Microsoft](#).

*Включен (Enabled)* — дата будет отображаться согласно заданной в политике формата.

|                                           |              |                                   |
|-------------------------------------------|--------------|-----------------------------------|
| <input type="radio"/> Не задано           | Комментарий: |                                   |
| <input checked="" type="radio"/> Включено |              |                                   |
| <input type="radio"/> Отключено           |              |                                   |
| Требования к версии:                      |              | Windows XP и более поздние версии |
| Параметры:                                |              |                                   |
| Формат даты:                              |              | d                                 |

## В реестре

1. Откройте редактор реестра на сервере Indeed AM.
2. Откройте раздел `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\BSPs\SMSOTP`.
3. Создайте следующие параметры:
  - `SMSOTP` (DWORD) со значением 1;
  - `dateFormat` (REG\_SZ) — позволяет задать настройки формата отображения даты. Примеры форматов можно посмотреть [в статье Microsoft](#).

## Настройка одноразового пароля

### Через GPO

Политика применяется к серверам Indeed AM и позволяет задать длину и вхождение групп символов при генерации одноразового пароля.

- *Не задано (Not Configured)* — одноразовый пароль будет состоять из цифр, строчных латинских букв и иметь длину в 6 символов.
- *Включено (Enabled)* — одноразовый пароль будет генерироваться согласно заданным в политике правилам. Длина пароля должна быть не менее 4 и не более 24 символов.
- *Отключено (Disabled)* — одноразовый пароль будет состоять из цифр, строчных латинских букв и иметь длину в 6 символов.

### В реестре

1. Откройте редактор реестра на сервере Indeed AM.
2. Откройте раздел `HKEY\LOCAL\MACHINE\SOFTWARE\Policies\Indeed-ID\BSPs\SMSOTP`.
3. Создайте следующие параметры:
  - `OTPGeerator` (DWORD) — включает данную настройку;
  - `OneTimePasswordLength` (DWORD) — длина одноразового пароля;
  - `AllowDigitsChGr` (DWORD) — использовать цифры в OTP;



- *AllowLatinsLowerChGr* (DWORD) — использовать строчные латинские буквы в OTP;
- *AllowLatinsUpperChGr* (DWORD) — использовать прописные латинские буквы в OTP;
- *AllowSpecialChGr* (DWORD) — использовать специальные символы в OTP.

## Настройка формата телефонного номера

### Через GPO

Политика применяется к серверам Indeed AM и позволяет настраивать формат телефонного номера. При включении данной политики включается нормализация телефонного номера.

Это означает следующее:

- пробелы, табуляция, скобочки, дефисы будут удаляться;
- если в строке записаны несколько номеров и разделены запятой или точкой с запятой, будет браться первый номер в строке до разделителя;
- 8 будет заменяться на +7;
- если в номере не хватает +7 или 8 в начале строки, то будет добавляться +7 перед номером;
- в номерах могут быть символы O вместо цифры 0, они будут заменяться обратно на цифры.



#### ПРИМЕЧАНИЕ

MegaFon по требованию формата REST запроса номер телефона должен иметь тип long. При нормализации + не учитывается.

Настройки формата телефонного номера

Настройки формата телефонного номера

☐ Не задано
 ☒ Включено
 ☐ Отключено

Комментарий:

Требования к версии: Windows XP и более поздние версии

Параметры:
   
Префикс телефонного номера: +7
   
Размер телефонного номера: 10

Справка: Политика позволяет настраивать формат телефонного номера.

OK
 Отмена
 Применить

## В реестре

1. Откройте редактор реестра на сервере Indeed AM.
2. Откройте раздел `HKEY\LOCAL\MACHINE\SOFTWARE\Policies\Indeed-ID\BSPs\SMSOTP`.
3. Создайте следующие параметры:
  - `ParsePhone` (DWORD) — включает парсинг телефонного номера;
  - `PhoneLength` (DWORD) — размер телефонного номера;
  - `PhonePrefix` (строковый параметр) — префикс телефонного номера.

## Настройка 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.

# Storage SMS OTP

## Сервис отправки СМС

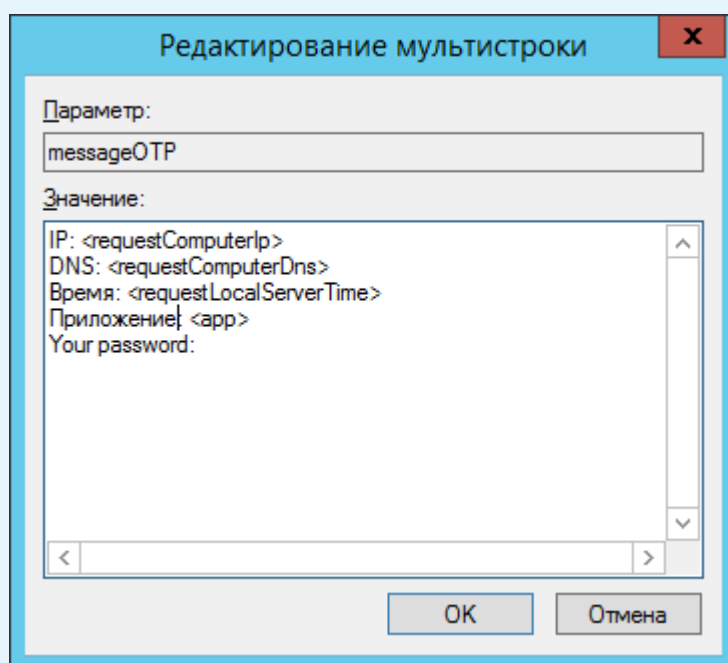
Политика применяется к серверам Indeed AM и определяет следующие настройки для сервера отправки СМС:

- *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_TRANSCIVER` протокола SMPP;
- *Отправитель* — имя отправителя, которое будет отображаться при получении СМС;
- *Дополнительный текст перед OTP* — произвольный текст сообщения, предшествующий одноразовому паролю. По умолчанию отправляется только одноразовый пароль, 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 одноразового пароля не настраивается, пароль всегда отображается в конце сообщения.

Для переноса строк отправляемого сообщения внесите 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 СМС 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 указывает на то, что запрашивается расписка о получении СМС или подтверждение SME;
- *data\_coding* — определяет схему кодировки пользовательских данных короткого сообщения.


Сервис отправки SMS

Предыдущий параметр

Следующий параметр

☐ Не задано

Комментарий:

☒ Включено

☐ Отключено

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 [в статье Microsoft](#).

*Включен (Enabled)* — дата будет отображаться согласно заданного в политике формата.

☐ Не задано      Комментарий:

☒ Включено

☐ Отключено

Требования к версии: Windows XP и более поздние версии

Параметры:

Формат даты: d

## Настройка одноразового пароля

Политика применяется к серверам Indeed AM и позволяет задать длину и вхождение групп символов при генерации одноразового пароля.

- *Не задано (Not Configured)* — одноразовый пароль будет состоять из цифр, строчных латинских букв и иметь длину в 6 символов.
- *Включено (Enabled)* — одноразовый пароль будет генерироваться согласно заданным в политике правилам. Длина пароля должна быть не менее 4 и не более 24 символов.
- *Отключено (Disabled)* — одноразовый пароль будет состоять из цифр, строчных латинских букв и иметь длину в 6 символов.

## Настройка одновременного подключения к серверу SMPP

Политика применяется к серверам Indeed AM и определяет порядок обработки запросов к серверу SMPP. Включение политики может быть необходимо, если сервер SMPP не поддерживает несколько подключений от одного пользователя (учетной записи, указанной в политике *Сервис отправки СМС*) 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.



# Email OTP

## 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 отображаться в теме письма, в противном случае в самом тексте письма.
- *Текст письма* — имя и почта отправителя, тема и текст письма.

### ⚠ ПРИМЕЧАНИЕ

В тексте письма необходимо указать место вставки одноразового пароля с помощью тега `<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 согласно определенных в политике параметров.

Настройки SMTP-сервера

Предыдущий параметр

Следующий параметр

☐ Не задано
 ☒ Включено
 ☐ Отключено

Комментарий:

Требования к версии: Windows XP и более поздние версии

Параметры:

Справка:

Сервер (DNS-имя, IP-адрес): smtp.gmail.com

Порт: 587

Таймаут сервера (сек): 30

Тип соединения: Незащищенное

Логин: MyEmail@indeed-id.com

Пароль: MyPassword

Имя отправителя(необязательно): Indeed-Id

E-Mail отправителя: Indeed-id@test.com

☐ Одноразовый пароль в теме письма

Тема письма: Ваш пароль

Текст письма: Ваш пароль <отр>

Данная политика позволяет задать 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 включено, то одноразовый пароль будет подставлен в тему письма, в противном случае в сам текст письма.
- Параметры письма - имя и почта отправителя, тема и текст письма.

В тексте письма необходимо указать место вставки одноразового пароля с помощью "<отр>".  
 Например: "Ваш одноразовый пароль: <отр>".  
 Если выставлена опция "Одноразовый пароль в теме письма", то аналогичное место вставки одноразового пароля необходимо указать в теме письма.

OK

Отмена

Применить

# Passcode

## Настройка хранения пароля

Политика включает хранение хеш-суммы пароля Passcode вместо хранения его значения.

Хеширование происходит по алгоритму SHA-1.

Если политика не определена или выключена, то пароль будет сохранен в оригинальном виде.

## Настройка 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.

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 содержать не менее 6 символов.

# MFA

## Настройка параметров аутентификации



### ВАЖНО

Политика должна распространяться на все серверы Indeed AM и на все клиентские машины.

### Через GPO

1. Откройте политику Настройки цепочки многофакторной аутентификации. Политика расположена по следующему пути: *Административные шаблоны→Indeed-ID→Id Providers→MFA*.
2. Установите значение политики *Включено*.
3. В параметре *Цепочка многофакторной аутентификации* укажите идентификаторы провайдеров аутентификации, которые будут использоваться в цепочке. Каждый идентификатор указывайте в фигурных скобках и с новой строки без пробелов и других символов.



### ПРИМЕЧАНИЕ

Запрещенный для использования провайдер может быть использован в цепочке провайдера MFA.

Список поддерживаемых провайдеров для Windows Logon и Enterprise SSO

SMS OTP {EBB6F3FA-A400-45F4-853A-D517D89AC2A3}  
Passcode {F696F05D-5466-42b4-BF52-21BEE1CB9529}  
Software OTP {0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0}  
Windows Password {CF189AF5-01C5-469D-A859-A8F2F41ED153}  
Z2 USB {CB5109DA-B575-422C-8805-524FE12B02F5}  
Futronic {A0EF00AD-1EEB-4D48-8BCF-06E19CD5585F}  
смарт-карта или USB-ключ {0AF65AD8-DB77-4B64-B489-958D9B36E28C}  
HID OMNIKEY {4B15AF52-A795-4CA6-B7CD-CDB8ABF2D2C2}  
Indeed Key {DEEF0CB8-AD2F-4B89-964A-B6C7ECA80C68}  
Hardware OTP {AD3FBA95-AE99-4773-93A3-6530A29C7556}  
Hardware TOTP {CEB3FEAF-86ED-4A5A-BD3F-6A7B6E60CA05}  
Secured TOTP {F15FD7EC-19EA-4384-846E-A2D0BE149FA2}

#### Список поддерживаемых провайдеров для NPS Radius Extension

Hardware OTP {AD3FBA95-AE99-4773-93A3-6530A29C7556}  
Hardware TOTP {CEB3FEAF-86ED-4A5A-BD3F-6A7B6E60CA05}  
Secured TOTP {F15FD7EC-19EA-4384-846E-A2D0BE149FA2}  
Software TOTP {0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0}  
Windows Password {CF189AF5-01C5-469D-A859-A8F2F41ED153}  
Passcode {F696F05D-5466-42b4-BF52-21BEE1CB9529}

#### ▼ Пример цепочки Indeed AM Passcode + Indeed AM SMS OTP

{F696F05D-5466-42b4-BF52-21BEE1CB9529}  
  
{EBB6F3FA-A400-45F4-853A-D517D89AC2A3}

4. В параметре *Имя устройства* указывается имя для созданной цепочки. Значение по умолчанию — *MFA*.

## ❗ ИНФОРМАЦИЯ

Данное значение будет отображаться в названии устройства MFA для пользователя и в событиях системы.

Настройки цепочки многофакторной аутентификации

Настройки цепочки многофакторной аутентификации

Предыдущий параметр Следующий параметр

☐ Не задано ☒ Включено ☐ Отключено

Комментарий:

Требования к версии: Windows XP и более поздние версии

Параметры:

Цепочка многофакторной аутентификации:

{F696F05D-5466-42b4-BF52-21BEE1CB9529}  
{EBB6F3FA-A400-45F4-853A-D517D89AC2A3}

Имя устройства:

Passcode+SMS OTP

Справка:

Задаёт последовательность методов аутентификации в цепочке многофакторной аутентификации. Id используемых провайдеров записываются в фигурных скобках, 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 OTP
- {DEEF0CB8-AD2F-4B89-964A-B6C7ECA80C68} - AirKeyProvider
- {CF189AF5-01C5-469D-A859-A8F2F41ED153} - Windows Password
- {CB5109DA-B575-422C-8805-524FE12B02F5} - Z2 USB

OK Отмена Применить

## В реестре

1. Откройте редактор реестра.
2. Откройте раздел `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\BSPs\MFA`.
3. Создайте параметр `BSPChain` типа `REG_MULTI_SZ` и укажите идентификаторы провайдеров аутентификации, которые будут использоваться в цепочке. Каждый идентификатор указывайте в фигурных скобках и с новой строки без пробелов и других символов.

Список поддерживаемых провайдеров для Windows Logon и Enterprise SSO

SMS OTP {EBB6F3FA-A400-45F4-853A-D517D89AC2A3}  
Passcode {F696F05D-5466-42b4-BF52-21BEE1CB9529}  
Software OTP {0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0}  
Windows Password {CF189AF5-01C5-469D-A859-A8F2F41ED153}  
Z2 USB {CB5109DA-B575-422C-8805-524FE12B02F5}  
Futronic {A0EF00AD-1EEB-4D48-8BCF-06E19CD5585F}  
смарт-карта или USB-ключ {0AF65AD8-DB77-4B64-B489-958D9B36E28C}  
HID OMNIKEY {4B15AF52-A795-4CA6-B7CD-CDB8ABF2D2C2}  
Indeed Key {DEEF0CB8-AD2F-4B89-964A-B6C7ECA80C68}  
Hardware OTP {AD3FBA95-AE99-4773-93A3-6530A29C7556}  
Secured TOTP {F15FD7EC-19EA-4384-846E-A2D0BE149FA2}

#### Список поддерживаемых провайдеров для NPS Radius Extension

Hardware OTP {AD3FBA95-AE99-4773-93A3-6530A29C7556}  
Hardware TOTP {CEB3FEAF-86ED-4A5A-BD3F-6A7B6E60CA05}  
Secured TOTP {F15FD7EC-19EA-4384-846E-A2D0BE149FA2}  
Software TOTP {0FA7FDB4-3652-4B55-B0C0-469A1E9D31F0}  
Windows Password {CF189AF5-01C5-469D-A859-A8F2F41ED153}  
Passcode {F696F05D-5466-42b4-BF52-21BEE1CB9529}

#### Edit Multi-String



Value name:

BSPChain

Value data:

{F696F05D-5466-42B4-BF52-21BEE1CB9529}  
{CF189AF5-01C5-469D-A859-A8F2F41ED153}

OK

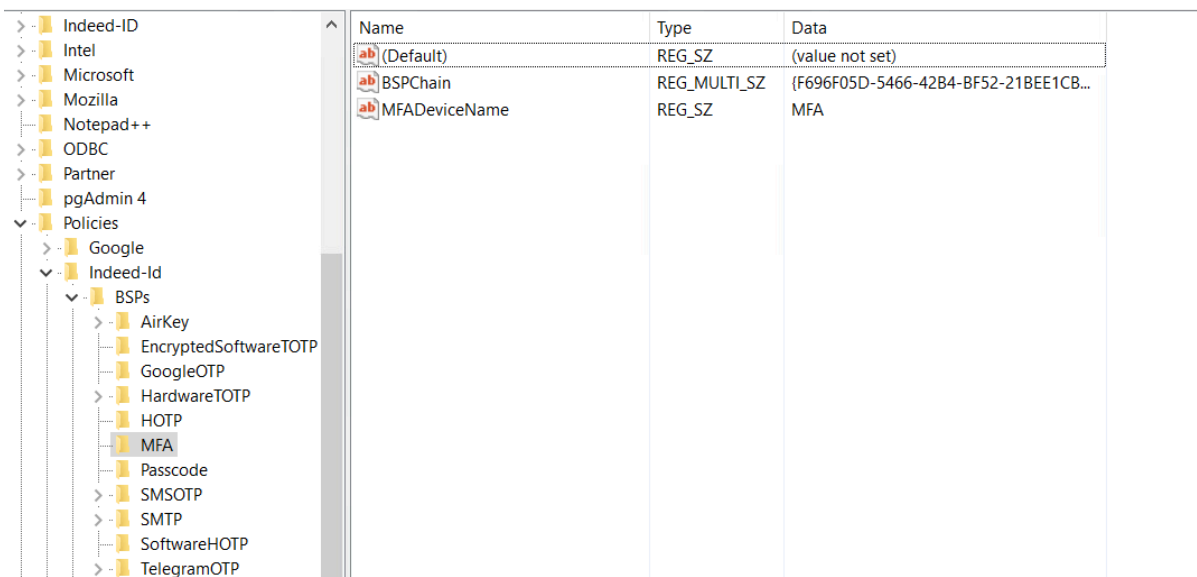
Cancel



4. Создайте параметр `MFADeviceName` типа `REG_SZ` и укажите имя для созданной цепочки.

#### ❗ ИНФОРМАЦИЯ

Данное значение будет отображаться в названии устройства MFA для пользователя и в событиях системы.



| Name          | Type         | Data                                 |
|---------------|--------------|--------------------------------------|
| (Default)     | REG_SZ       | (value not set)                      |
| BSPChain      | REG_MULTI_SZ | {F696F05D-5466-42B4-BF52-21BEE1CB... |
| MFADeviceName | REG_SZ       | MFA                                  |

## Настройка политик RADIUS Extension

При интеграции с модулем RADIUS Extension способ аутентификации MFA называется *One-string authenticator*. При таком способе многофакторной аутентификации для пользователей предусмотрено одно поле для ввода всех факторов. Каждый фактор аутентификации вписывается в поле ввода в одну строку с разделителем или без него.

### Длина OTP

Позволяет задать длину одноразового пароля, если в цепочке провайдеров не используется разделитель. Если политика включена, одноразовый пароль отделяется от постоянного пароля с помощью определения количества символов в пароле. Заданная длина применяется ко всем провайдерам одноразовых паролей в цепочке.

## Через GPO

1. Откройте политику *Длина OTP*. Политика расположена по следующему пути:  
*Административные шаблоны*→*RADIUS*→*MFA*.
2. Установите значение политики *Включено*.
3. Задайте значение, которое совпадает со значением в политике *Длина одноразового пароля* (значение 6 или 8).

## В реестре

1. Откройте редактор реестра.
2. Откройте или создайте раздел `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius\MFA`.
3. Создайте параметр `OTPLen` типа `REG_DWORD` и укажите значение, которое совпадает со значением в политике *Длина одноразового пароля* (значение 6 или 8).

## Символ разделителя

Позволяет задать символ, которым разделяются аутентификаторы. В качестве разделителя можно использовать любой одиночный символ: цифры, строчные и прописные буквы латиницы и кириллицы, специальные символы (включая пробел).



### ВАЖНО

Если аутентификатор уже содержит символ разделителя, при вводе в форму пользователь должен продублировать символ разделителя. Например, аутентификатор `password\example`, одноразовый пароль `395816`. В форму ввода нужно ввести `password\\example\395816`.



### ИНФОРМАЦИЯ

Если включены обе политики *Длина OTP* и *Символ разделителя*, приоритетнее политика *Символ разделителя*.

### Через GPO

1. Откройте политику *Символ разделителя*. Политика расположена по следующему пути:  
*Административные шаблоны*→*RADIUS*→*MFA*.
2. Установите значение политики *Включено*.
3. Задайте символ, которым разделяются постоянный пароль и одноразовый пароль.

### В реестре

1. Откройте редактор реестра.
2. Откройте или создайте раздел `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius\MFA`.
3. Создайте параметр `Separator` типа `REG_SZ` и укажите символ, которым разделяются постоянный пароль и одноразовый пароль.

## Поддержка политик для смарт-карт

Если в цепочке присутствуют такие провайдеры как **Smart Card Provider**, **IronLogic Z2USB Provider**, **OMNIKEY Provider**, поддерживаются политики *Поведение при извлечении смарт-карты* и *Таймаут выполнения действия при извлечении смарт-карты*.

# Smart Card

## Поведение при извлечении смарт-карты

Smart Card Provider поддерживает политику безопасности Windows *Интерактивный вход в систему: поведение при извлечении смарт-карты*.

С помощью этой политики вы можете определить действие, которое будет выполняться при извлечении смарт-карты с рабочей станции пользователя.

## 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 политики Windows *Интерактивный вход: поведение при извлечении смарт-карты (Interactive logon: Smart-card enhanced removal behavior)*.

### ИНФОРМАЦИЯ

Административный файл шаблона политики *IndeedID.Client.admx* входит в состав дистрибутива и расположен в каталоге *Misc*.

Наличие стандартного таймаута предотвращает автоматическую блокировку компьютера при случайном извлечении устройства аутентификации.

Наличие сервисного таймаута 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 таймаута перед извлечением устройства нажмите и удерживайте комбинацию клавиш +  
.

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".

## Использование дополнительных данных

Политика 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.

### ИНФОРМАЦИЯ

Административный файл шаблона политики *IndeedID.Smartcard.Provider.admx* входит в состав дистрибутива и расположен в каталоге *Misc*.

Дополнительные данные – это 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 случае некорректной работы PKCS смарт-карты.

The screenshot shows a Windows Group Policy configuration window titled "Ожидание смарт-карты после входа в терминальную сессию". The window has a standard Windows interface with minimize, maximize, and close buttons in the title bar. Inside, there are navigation buttons "Предыдущий параметр" and "Следующий параметр". The policy is currently set to "Включено" (Enabled), indicated by a selected radio button. To the right of the radio buttons is a "Комментарий:" (Comment) text box. Below the radio buttons is a "Требования к версии:" (Version requirements) dropdown menu, which is currently set to "Windows XP и более поздние версии". At the bottom left, under the "Параметры:" (Parameters) section, there is a numeric input field labeled "Ожидание смарт-карты после входа в терминальную сессию в секундах:" (Waiting for smart card after login to terminal session in seconds:), with the value "10" entered. To the right of the parameters is a "Справка:" (Help) section containing the text: "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." At the bottom right of the window are three buttons: "ОК", "Отмена", and "Применить".

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:

Ожидание смарт-карты после входа в терминальную сессию в секундах:

10

Справка:

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

# IronLogic Z2USB

## Поведение при извлечении смарт-карты

IronLogic Z-2 USB Provider поддерживает политику безопасности Microsoft *Интерактивный вход в систему: поведение при извлечении смарт-карты*.

С помощью этой политики вы можете определить действие, которое будет выполняться при извлечении смарт-карты с рабочей станции пользователя.

## Таймаут выполнения действия при извлечении смарт-карты

### ПРИМЕЧАНИЕ

Настройка политик необходима для повышения уровня безопасности, однако полноценная работа Indeed AM IronLogic Z-2 USB Provider возможна и со значениями политик, определенными по умолчанию.

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 политики 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 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): 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".

## Использование идентификатора 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:

Справка:

Программное обеспечение SKUD:

Perco/Gate

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

# Omnikey

## Поведение при извлечении смарт-карты

OMNIKEY Provider поддерживает политику безопасности Windows *Интерактивный вход в систему: поведение при извлечении смарт-карты*.

С помощью этой политики вы можете определить действие, которое будет выполняться при извлечении смарт-карты с рабочей станции пользователя.

## 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 политики 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 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): 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".

## Использование данных PACS

### ❗ ИНФОРМАЦИЯ

Политика применяется к рабочим станциям пользователя.

При включении данная политика позволяет использовать данные PACS вместо идентификатора карты.

Не требует настройки.

Использовать данные PACS

Использовать данные PACS

Предыдущий параметр

Следующий параметр

☐ Не задано

☒ Включено

☐ Отключено

Комментарий:

Требования к версии:

Windows XP и более поздние версии

Параметры:

Справка:

Политика позволяет использовать данные PACS вместо идентификатора карты.

OK

Отмена

Применить

# Futronic

## Минимально допустимое качество шаблона при обучении

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.



### ПРИМЕЧАНИЕ

Политика должна быть определена на рабочих станциях пользователей, на которых установлены клиентские компоненты системы. Если политика не определена, по умолчанию используется значение 3.

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

☐ Не задано
 ☒ Включено
 ☐ Отключено

Комментарий:

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

Политика определяет максимально допустимое значение FAR (False Acceptance Rate) при сравнении шаблонов отпечатков.

### ⓘ ПРИМЕЧАНИЕ

Политика должна быть определена на всех серверах Indeed AM. Если политика не определена, значением по умолчанию является 250.

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 задать слишком большое значение параметра, это может привести к частым ошибкам, связанным с отказом легитимным пользователям.

Максимально допустимый FAR

Максимально допустимый FAR

Предыдущий параметр Следующий параметр

☐ Не задано Комментарий:

☒ Включено

☐ Отключено

Требования к версии: Windows XP и более поздние версии

Параметры: Справка:

Максимальный FAR 400

Численное представление максимально допустимого значения FAR (False Acceptance Rate) при сравнении шаблонов отпечатков. Задается целым числом от 1 до 1000. Значение 1 соответствует самому "мягкому" сравнению, когда максимальна вероятность сравнить разные шаблоны и получить положительный результат, значение 1000 соответствует самому "жесткому" сравнению, когда такая вероятность минимальна.

Если значение параметра будет слишком большим, это приведет к частым ошибкам, связанным с отказом легитимным пользователям.

Политика применяется к серверам Indeed EA\ESSO.

Если политика не определена, в качестве значения по умолчанию используется 250.

ОК Отмена Применить

## 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

☒ Включено

☐ Отключено

Комментарий:

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

# RADIUS Extension

Политики применяются к серверам с развернутой ролью NPS (Network Policy Server) и позволяют 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.

## Настройка таймаута сессии Challenge\Response

Позволяет задать таймаут сессии при использовании провайдера аутентификации, поддерживающего Challenge\Response.

### Через GPO

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. В поле Таймаут сессии в секундах укажите необходимое значение.

Настройки таймута сессии Challenge\Response

Настройки таймута сессии Challenge\Response

☐ Не задано
 ☒ Включено
 ☐ Отключено

Комментарий:

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

## В реестре

1. Откройте редактор реестра на сервере NPS.
2. Откройте или создайте раздел `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius`.
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.

### Через GPO

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. В поле Сообщение пользователю введите необходимый текст.

Challenge\Response: сообщение пользователю

Challenge\Response: сообщение пользователю

Предыдущий параметр Следующий параметр

☐ Не задано
 ☒ Включено
 ☐ Отключено

Комментарий:

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

## В реестре

1. Откройте редактор реестра на сервере NPS.
2. Откройте или создайте раздел *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius*.
3. Создайте раздел с именем необходимого провайдера: *EmailOTP*, *HardwareHOTP*, *GoogleOTP*, *SMSOTP*.
4. Создайте строковый параметр с именем формата *<имя используемого провайдера>ChallengeResponseReplyMessage*, например *HardwareHOTPChallengeResponseReplyMessage*.
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\HardwareHOTP]  
"HardwareHOTPChallengeResponseReplyMessage"="HardwareHOTP: "
```

```
[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: "
```

## Определение IP-адреса клиента Radius

Политика позволяет задать атрибуты для определения IP-адреса клиента RADIUS, по которому будет выполняться поиск Radius-приложения в Access Manager. Если значение не присвоено, значение по умолчанию соответствует 265 (SrcIPAddress), 278 (SrcIPv6Address).

#### Через GPO

1. Откройте редактор GPO.
2. Перейдите в раздел Конфигурация компьютера→Административные шаблоны→Indeed ID→Radius.
3. Откройте политику *Определение IP-адреса клиента Radius*.
4. Включите политику. В поле Атрибуты укажите необходимое значение. Можно указать несколько значений через запятую.

## В реестре

1. Откройте редактор реестра на сервере NPS.
2. Откройте или создайте раздел *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius*.
3. Создайте параметр типа REG\_SZ с именем **ClientIPAttributes** и задайте необходимое значение (можно указать несколько значений через запятую):
  - 4 — NASIPAddress
  - 95 — NASIPv6Address
  - 265 — SrcIPAddress
  - 278 — SrcIPv6Address

## Кеширование групп пользователей

Политика включает кеширование групп пользователей при RADIUS-аутентификации и позволяет задать период обновления кеша.

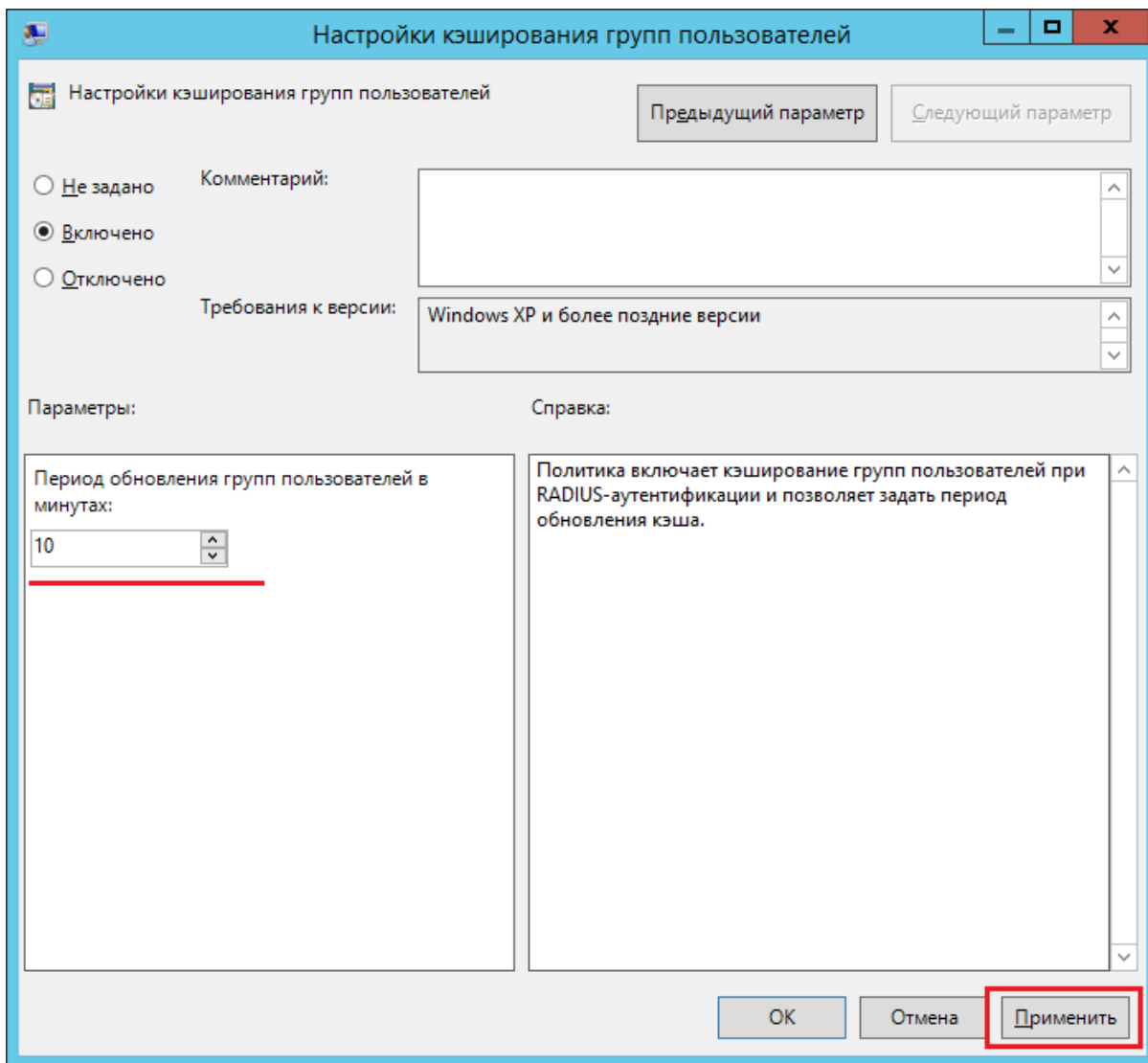


### ПРИМЕЧАНИЕ

Если NPS RADIUS Extension или Indeed AM Server долго отвечают во время работы под нагрузкой с большим количеством пользователей, необходимо отключить данную настройку.

## Через GPO

1. Откройте редактор GPO.
2. Перейдите в раздел Конфигурация компьютера→Административные шаблоны→Indeed ID→Radius.
3. Откройте политику Настройки кеширования групп пользователей.
4. Включите политику. В поле Период обновления групп пользователей в минутах укажите требуемое значение в минутах.



## В реестре

1. Откройте редактор реестра на сервере NPS.
2. Откройте или создайте раздел `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius`.
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
```

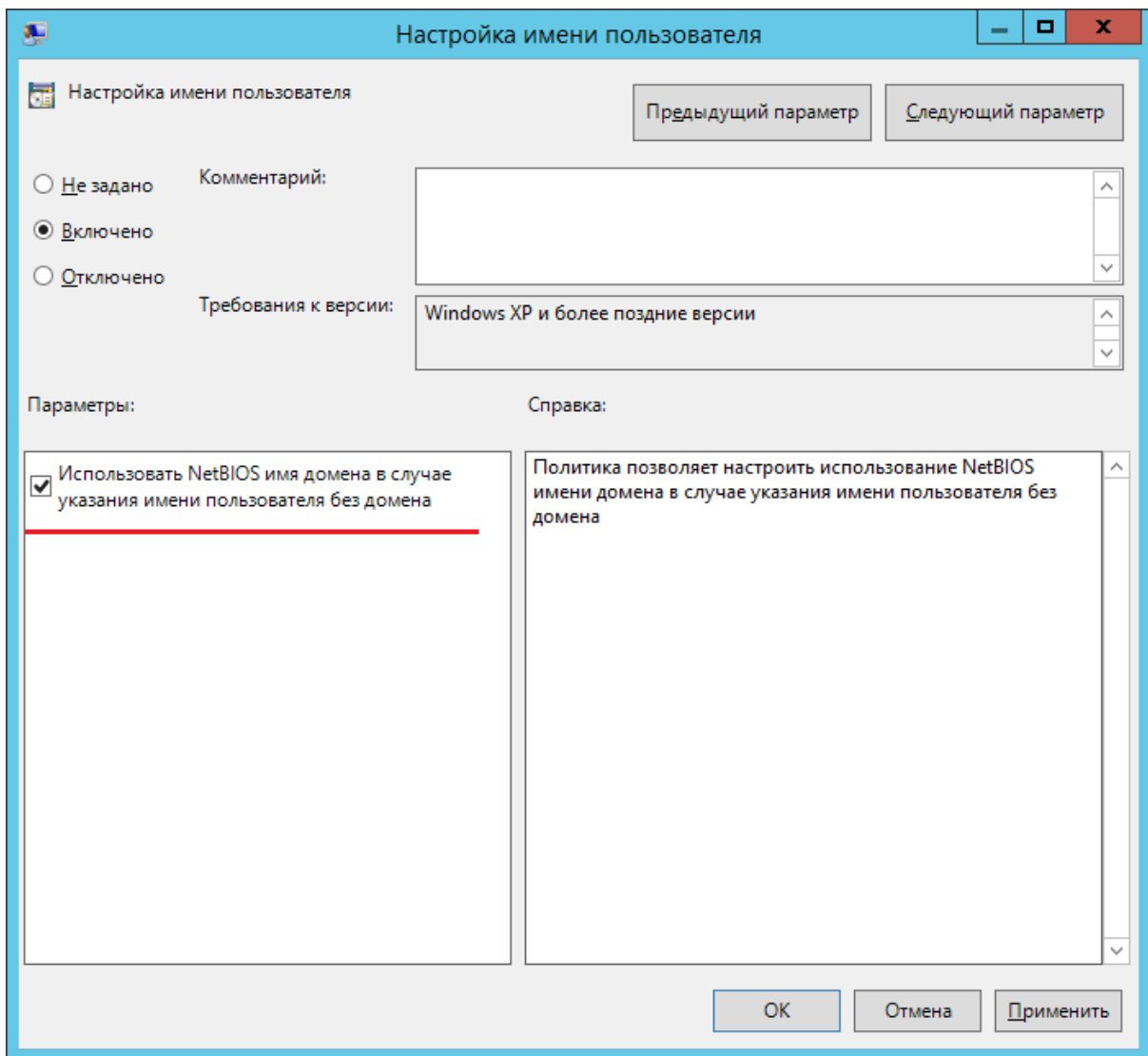
```
"UserGroupsCacheUpdateMin"=dword:00000021
```

## Настройка имени пользователя

Политика позволяет настроить использование NetBIOS имени домена в случае указания имени пользователя без домена.

### Через GPO

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.



## В реестре

1. Откройте редактор реестра на сервере NPS.
2. Откройте или создайте раздел *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius*.
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]
```

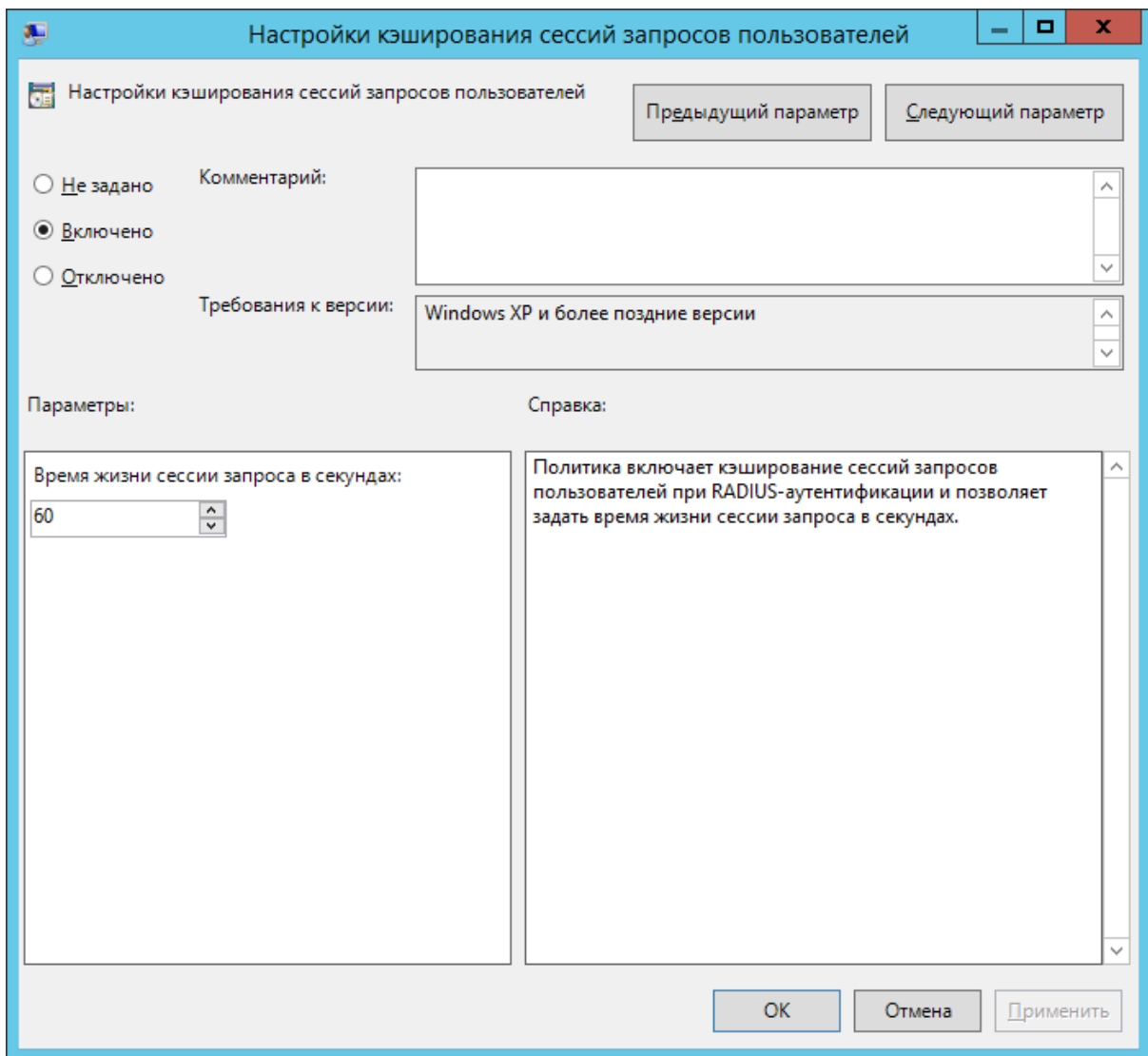
```
"UseNetBiosDomainName"=dword:00000001
```

## Настройка кеширования сессий запросов пользователей

Политика включает кеширование сессий запросов пользователей при RADIUS-аутентификации и позволяет задать время жизни сессии запроса в секундах.

### Через GPO

1. Откройте редактор GPO.
2. Перейдите в раздел Конфигурация компьютера→Административные шаблоны→Indeed ID→Radius.
3. Откройте политику *Настройка кеширования сессий запросов пользователей*.
4. Включите политику. В поле Время жизни сессии запроса в секундах укажите значение.



## В реестре

1. Откройте редактор реестра на сервере NPS.
2. Откройте или создайте раздел `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius`.
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

## Отключить использование настроек способа входа в Management Console

В версии Indeed Access Manager 8.2 и выше вы можете настраивать способ входа **через приложение Management Console**. В версиях **Indeed Access Manager 8.1** и ранее способ входа настраивался через политики *Настройка способов входа для групп пользователей* и *Общая настройка способа входа*.

Вы можете использовать ваши существующие настройки способа входа в текущей версии Access Manager. Для этого настройте политику *Отключить использование политик Access Manager*.

### Через GPO

1. Откройте редактор GPO.
2. Перейдите в раздел Конфигурация компьютера→Административные шаблоны→Indeed ID→Radius.
3. Откройте политику *Отключить использование политик Access Manager*.
4. Включите политику.

Отключить использование политик Access Manager

Отключить использование политик Access Manager

Предыдущий параметр Следующий параметр

☐ Не задано      Комментарий:

☒ Включено

☐ Отключено

Требования к версии: Windows XP и более поздние версии

Параметры:

Справка:

Настройка отключает использование политик Access Manager для определения способа аутентификации пользователя. В этом случае настройки должны быть заданы с помощью групповой политики "Настройка способов входа для групп пользователей". По умолчанию настройка отключена и применяются настройки из политик Access Manager.

OK Отмена Применить

## В реестре

1. Откройте редактор реестра на сервере NPS.
2. Откройте или создайте раздел `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\Radius`.
3. Создайте параметр типа DWORD с именем `DisableAccessManagerPolicies`, в значении параметра укажите `1`.

| Имя                          | Тип       | Значение                |
|------------------------------|-----------|-------------------------|
| (По умолчанию)               | REG_SZ    | (значение не присвоено) |
| DisableAccessManagerPolicies | REG_DWORD | 0x00000001 (1)          |

# RDP Windows Logon

## Настройка одновременной работы с модулем Indeed Windows Logon

При условии, что используется сценарий с установкой на одной машине RDP Windows Logon и **Windows Logon**, необходимо настроить политику для Windows Logon.

### Через GPO

1. Перейдите на машину, на которой установлены модули RDP Windows Logon и Windows Logon.
2. Откройте редактор GPO.
3. Перейдите к Конфигурация компьютера→Административные шаблоны→ Indeed ID→Windows Logon.
4. Включите политику Настройки Credential Provider и установите параметр Отображение способов входа на *Все, кроме пароля*.

### В реестре

1. Перейдите на машину, на которой установлены компоненты RDP Windows Logon и Windows Logon.
2. Откройте редактор реестра.
3. Перейдите к Компьютер\HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Indeed-ID\Logon for Windows.
4. Создайте параметр **DWORD** с именем **CredProvFilter** и установите значение 2.



# Enterprise Single Sign-On

## Настройка подключения к Core Server

### Через GPO

Если вы настраиваете подключение к серверу 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 ESSO Agent.
2. Через *gpedit.msc* пройдите по пути: Конфигурация компьютера→Административные шаблоны→Indeed ID→ClientConnection→Настройки подключения к серверу и включите политику.
3. В поле URL-адрес AM сервера укажите URL вашего сервера Indeed, например *http(s)://dc.indeed-id.local/am/core/*.

### В реестре

1. Откройте редактор реестра Windows.
2. Перейдите в раздел *HKEY\_LOCAL\_MACHINE\SOFTWARE\Indeed-ID\SrvLocator2*.
3. Измените строковый параметр **ServerUrlBase** и укажите URL вашего сервера Indeed, например *http(s)://dc.indeed-id.local/am/core/*.



#### ПРИМЕЧАНИЕ

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

## Проверка доступности Core Server

Для клиентских компьютеров можно включить проверку доступности Core Server, а также настроить время, по истечении которого Core Server считается недоступным и клиентский компьютер начинает использовать кешированные данные.

По умолчанию и при выключенной политике проверки доступности Core Server отключены и не производятся, время определения недоступности сервера не ограничено.

При настройке через политики значения будут указаны по пути реестра: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Indeed-ID\AM\ServerAvailability* и будут приоритетнее ручной настройки.

Чтобы настроить проверку доступности Core Server:

### Через GPO

1. Перейдите на машину с установленными Core Server и модулем ESSO Agent.
2. Откройте редактор GPO.
3. Перейдите в раздел Конфигурация компьютера→Административные шаблоны→Indeed ID→Client Connection.
4. Включите политику Проверка доступности сервера Indeed EA\ESSO.
5. Задайте значения следующих параметров:
  - Для параметра Таймаут ожидания результата проверки задайте период, в течении которого клиентский модуль Indeed ожидает результат проверки доступности сервера, по истечении которого сервер считается недоступным. Значение по умолчанию — 5000 мс.
  - Для параметра Время жизни результата проверки задайте время, в течение которого результат предыдущей проверки остается валидным и используется вместо проведения новых проверок. Значение по умолчанию — 6000 мс.

1. Перейдите на клиентскую машину с установленным ESSO Agent.
2. Откройте редактор реестра.
3. Перейдите Компьютер\HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Indeed-ID\AM\ServerAvailability.
4. Задайте значения следующих параметров:
  - Для параметра `IsEnabled` установите значение `1`, чтобы включить проверку.
  - Для параметра `CheckWaitTimeoutMs` задайте период, в течении которого клиентский модуль Indeed ожидает результат проверки доступности сервера, по истечении которого сервер считается недоступным. Значение по умолчанию — 5000 мс.
  - Для параметра `CheckResultTtlMs` задайте время, в течение которого результат предыдущей проверки остается валидным и используется вместо проведения новых проверок. Значение по умолчанию — 6000 мс.

# Windows Logon

## Настройка Windows Logon

### Через GPO

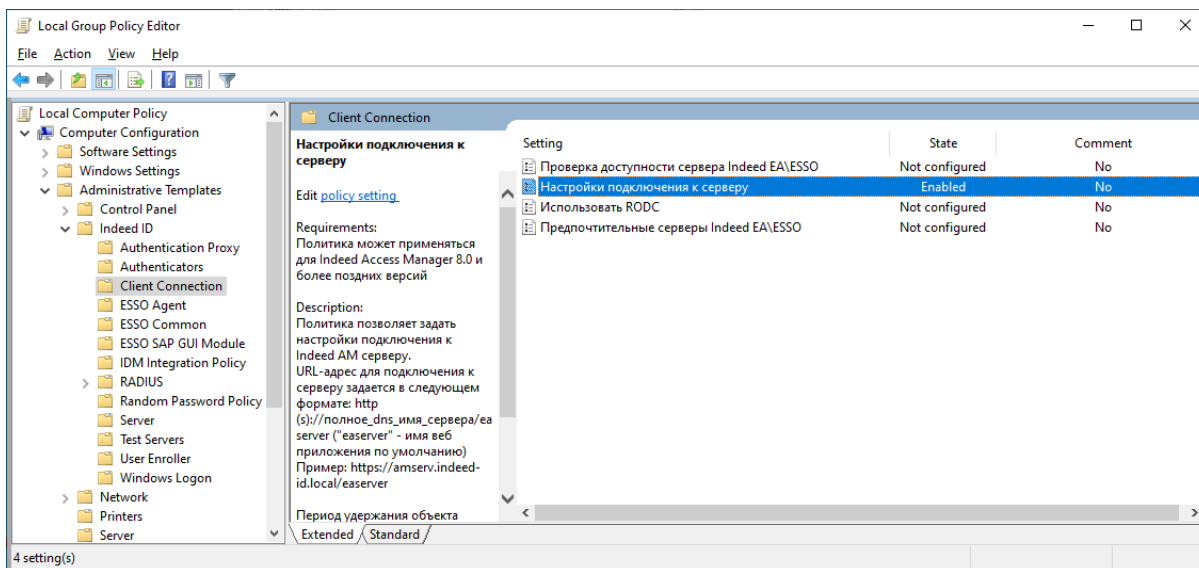


#### ВАЖНО!

При настройке через политики значения будут указаны по пути реестра: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Indeed-ID\SrvLocator2` и будут приоритетнее ручной настройки.

1. Добавьте политику `IndeedID.ServerUrl.admx` на рабочее место с установленным Indeed AM Windows Logon.
2. Через `gpedit.msc` пройдите по пути Конфигурация компьютера→Административные шаблоны→Indeed ID→ClientConnection→Настройки подключения к серверу.

Включите политику.



3. В поле URL-адрес AM сервера укажите URL вашего Indeed Access Manager Server, например `http(s)://dc.indeed-id.local/am/core/`.

Настройки подключения к серверу

Настройки подключения к серверу

Предыдущий параметр Следующий параметр

☐ 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:

☐ Игнорировать ошибки сертификата:

Период удержания объекта сессии (мс):

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.

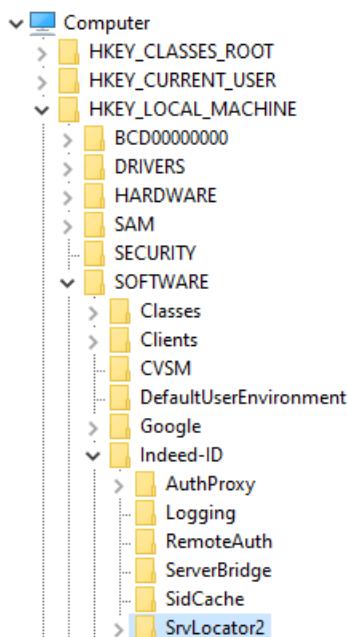
OK Отмена Применить

## В реестре

1. Откройте редактор реестра Windows.
2. Перейдите в раздел `HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\SrvLocator2`.
3. Измените строковый параметр `ServerUrlBase` и укажите URL вашего Indeed Access Manager Server, например `http(s)://dc.indeed-id.local/am/core/`.

### ⚠ ПРИМЕЧАНИЕ

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



| Name                 | Type       | Data                                |
|----------------------|------------|-------------------------------------|
| (Default)            | REG_SZ     | (value not set)                     |
| IsIgnoreCertErrors   | REG_DWORD  | 0x00000001 (1)                      |
| ServerCertThumbprint | REG_BINARY | (zero-length binary value)          |
| ServerUrlBase        | REG_SZ     | https://dc.indeed-id.local/am/core/ |
| SessionHoldPeriodMs  | REG_DWORD  | 0x0002bf20 (180000)                 |

## Настройка одновременной работы с Indeed RDP Windows Logon

Если используется сценарий с установкой Windows Logon и RDP Windows Logon на одной машине, необходимо настроить политику для Windows Logon.

### Через GPO

1. Перейдите на машину, на которой установлены модули RDP Windows Logon и Windows Logon.
2. Откройте редактор GPO.
3. Перейдите в раздел Конфигурация компьютера→Административные шаблоны→Indeed ID→Windows Logon.
4. Включите политику *Настройка Credential Provider* и установите параметр Отображение способов входа на Все, кроме пароля.

### Через реестр

1. Перейдите на машину, на которой установлены модули RDP Windows Logon и Windows Logon.
2. Откройте редактор реестра.

3. Перейдите в раздел  
Компьютер\HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Indeed-ID\Logon for Windows.
4. Создайте параметр типа *DWORD* с именем **CredProvFilter** и установите ему значение 2.

## Проверка доступности Core Server

Для клиентских компьютеров можно включить проверку доступности Core Server, а также настроить время, по истечении которого Core Server считается недоступным и клиентский компьютер начинает использовать кешированные данные.

По умолчанию и при выключенной политике проверки доступности Core Server отключены и не производятся, время определения недоступности сервера не ограничено.

При настройке через политики значения будут указаны по пути реестра: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Indeed-ID\AM\ServerAvailability* и будут приоритетнее ручной настройки.

Чтобы настроить проверку доступности Core Server:

### Через GPO

1. Перейдите на машину с установленными Core Server и модулем Indeed AM Windows Logon.
2. Откройте редактор GPO.
3. Перейдите в раздел Конфигурация компьютера→Административные шаблоны→Indeed ID→Client Connection.
4. Включите политику Проверка доступности сервера Indeed EA\ESSO.
5. Задайте значения следующих параметров:
  - Для параметра Таймаут ожидания результата проверки задайте период, в течении которого клиентский модуль Indeed ожидает результат проверки доступности сервера, по истечении которого сервер считается недоступным. Значение по умолчанию — 5000 мс.

- Для параметра Время жизни результата проверки задайте время, в течение которого результат предыдущей проверки остается валидным и используется вместо проведения новых проверок. Значение по умолчанию — 6000 мс.

## Через реестр

1. Перейдите на клиентскую машину с установленным Indeed AM Windows Logon.
2. Откройте редактор реестра.
3. Перейдите Компьютер\HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Indeed-ID\AM\ServerAvailability.
4. Задайте значения следующих параметров:
  - Для параметра `IsEnabled` установите значение `1`, чтобы включить проверку.
  - Для параметра `CheckWaitTimeoutMs` задайте период, в течении которого клиентский модуль Indeed ожидает результат проверки доступности сервера, по истечении которого сервер считается недоступным. Значение по умолчанию — 5000 мс.
  - Для параметра `CheckResultTtlMs` задайте время, в течение которого результат предыдущей проверки остается валидным и используется вместо проведения новых проверок. Значение по умолчанию — 6000 мс.



# Резервное копирование

Рекомендуется подготовить резервные копии базы данных, конфигурационных файлов и настройки реестра после того, как вы развернули Indeed Access Manager и проверили его работоспособность.

Периодичность создания резервных копий зависит от того, как вы эксплуатируете Access Manager. Например, резервные копии конфигурационных файлов рекомендуется создавать, если проводились изменения параметров в файлах конфигурации, а далее каждый месяц.

Резервные копии базы данных Access Manager рекомендуется создавать после периода внедрения и отладки. В период, когда пользователи регистрируют аутентификаторы, рекомендуется создавать резервные копии базы данных ежедневно, так как база данных меняется, когда вносятся изменения политик, настройки аутентификаторов, и при регистрации или изменении аутентификаторов пользователями.

Рекомендуется создавать резервные копии следующих компонентов:

## ▼ Базы данных

---

- база данных Core Server;
- база данных Key Server (при наличии);
- база событий Log Server (при наличии).

## ▼ Конфигурационные файлы компонентов

- конфигурационные файлы Log Server:
  - *C:\inetpub\wwwroot\ls\clientApps.config*;
  - *C:\inetpub\wwwroot\ls\targetConfigs\sampleDb.config*, если логи хранятся в Microsoft SQL;
  - *C:\inetpub\wwwroot\ls\targetConfigs\postgresDb.config*, если логи хранятся в PostgreSQL;
  - *C:\inetpub\wwwroot\ls\targetConfigs\sampleSyslog.config*, если логи хранятся в SysLog.



### ПРИМЕЧАНИЕ

Перед созданием резервной копии расшифруйте файл конфигурации с помощью утилиты *EA.Config.Encryptor.exe* (расположена в каталоге дистрибутива *Indeed Access Manager Server*/*<номер версии>/Misc/EA.Config.Encryptor*). Подробную информацию по расшифрованию вы найдете в разделе Ручная настройка Core Server. Если использовались резервные базы для логов, сохраните все настроенные файлы.

- конфигурационный файл консоли администратора  
*C:\inetpub\wwwroot\am\mc\Web.config*;
- конфигурационный файл User Console (при наличии)  
*C:\inetpub\wwwroot\am\uc\Web.config*;
- конфигурационный файл Identity Provider (при наличии):
  - для Indeed Access Manager 8.1.5 и ниже файл для резервной копии —  
*C:\inetpub\wwwroot\am\idp\Web.config*;
  - для Indeed Access Manager 8.1.5 и выше файл для резервной копии —  
*C:\inetpub\wwwroot\am\idp\app-settings.json*;
- конфигурационный файл Key Server (при наличии):
  - для Indeed Access Manager 8.2 и ниже файл для резервной копии —  
*C:\inetpub\wwwroot\airkeycloud\Web.config*;
  - для Indeed Access Manager 8.2 и выше файл для резервной копии —  
*C:\inetpub\wwwroot\indeedkey\Web.config\**.

### ▼ Настройки реестра

---

- настройки реестра с Core Server, расположенные в разделе *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Indeed-ID*;
- настройки реестра с серверов, где установлены модули интеграции, расположенные в разделе *HKEY\_LOCAL\_MACHINE\SOFTWARE\Indeed-ID* , *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Indeed-ID*;
- настройки реестра с клиентских машин, где используются модули Windows Logon и/или ESSO Agent, расположенные в разделе *HKEY\_LOCAL\_MACHINE\SOFTWARE\Indeed-ID*, *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Indeed-ID*.

### ▼ Настройки мастера конфигурации

---

Чтобы создать резервную копию настроек мастера конфигурации, запустите мастер конфигурации (расположен в каталоге дистрибутива *Indeed Access Manager Server/<номер версии>/Misc/EA.Server.Wizard.exe*). Перейдите на шаг Подтверждение, убедитесь, что вы выбрали опцию Сохранить резервную копию параметров конфигурации, и нажмите Применить. Сохраните созданную резервную копию.

# Руководство администратора



## Приложения

Количество глав: 3



## Лицензии

Операции с лицензиями



## Аутентификаторы

Общие настройки аутентификаторов в Management Console



## Пользователи

Управление пользователями Indeed Access Manager



## Политики

Управление доступами и правами пользователей



## Устройства

Управление устройствами аутентификации



## События

Управление событиями пользователей



## Конфигурация

Настройки аутентификаторов и прав доступа

# Приложения

Данный раздел содержит приложения и модули, для которых в Indeed AM **зарегистрированы лицензии**. Модули интеграции автоматически отображаются в разделе Приложения после регистрации лицензии.

Для каждого приложения в этом разделе доступны настройки:

- разрешить или запретить использование аутентификаторов;
- сгенерировать случайный пароль для учетной записи Active Directory;
- включить, отключить и настроить **кеширование данных**.

Также в этом разделе можно вручную добавить приложения, интегрированные с модулями **ESSO Agent** и **NPS Radius Extension**, в систему Indeed AM.

# Модуль Enterprise SSO

В разделе Приложения можно добавить и настроить приложения, интегрированные с модулем ESSO, а также при необходимости задать их дополнительные настройки.

## Предварительная настройка

Перед добавлением приложения:

1. **Настройте модуль** Indeed Enterprise Single Sign-On.
2. **Зарегистрируйте лицензию** в Management Console.
3. **Подготовьте шаблон** для приложения.

## Добавить приложение

1. На боковой панели в Management Console в блоке Настройки выберите Приложения.
2. Нажмите Добавить приложение.
3. В окне Добавить приложение выберите модуль интеграции *Enterprise SSO*, выберите файл шаблона для приложения и нажмите Создать.

После успешной загрузки шаблона откроется страница с настройками приложения.

## Добавить в политику

Чтобы настройки приложения были применены для пользователей, добавьте приложение в политику. Сделать это можно только при наличии зарегистрированной лицензии для данного модуля.

Чтобы добавить приложение в политику:

1. Перейдите в раздел Политики.
2. Выберите политику из списка.
3. В карточке политики перейдите на вкладку Приложения.
4. Нажмите Добавить приложение.
5. Из выпадающего списка выберите приложение.

6. Нажмите Добавить.

Приложение отобразится в списке добавленных приложений.

## Добавить учетную запись

Чтобы задать, данные какого пользователя будут подставляться при входе в приложение ESSO, добавьте учетную запись. Для этого:

1. На боковой панели Management Console откройте раздел Политики.
2. Выберите политику.
3. Перейдите на вкладку Приложения
4. Откройте приложение, интегрированное с модулем ESSO нажав на его название.
5. Нажмите Добавить учетную запись.
6. В поле Тип учетных данных выберите тип:
  - Индивидуальные — у каждого пользователя своя учетная запись для входа в приложение.
  - Active Directory — для входа используются данные пользователя из Active Directory.
  - Связанные — создается учетная запись, связанная с одной из уже сохраненных. В рамках одной политики можно сделать связку с учетными записями разных приложений. Это полезно, когда есть несколько приложений с одинаковыми учетными данными для входа. Если учетные записи связаны, достаточно будет внести изменения в учетную запись только корневого приложения, а не редактировать каждую запись отдельно.
  - Общие для всех — для входа в приложение все пользователи используют одну учетную запись.
7. В поле Описание введите описание учетной записи, которое будет отображаться в Management Console.
8. Задайте остальные настройки в зависимости от выбранного типа учетных данных. Если настройки уже заданы в шаблоне приложения, они отобразятся в Management Console автоматически, но их нельзя будет отредактировать.
9. Нажмите Сохранить.

Добавленная учетная запись отобразится в списке учетных записей для приложения.



## Задать метод аутентификации

1. На боковой панели Management Console откройте раздел Политики.
2. Выберите политику.
3. Перейдите на вкладку Приложения
4. Откройте приложение, интегрированное с модулем ESSO, нажав на его название.
5. В разделе Доступные методы аутентификации выберите, какие методы могут использоваться для входа в интегрированное приложение.
6. Нажмите Сохранить.

## Опциональные настройки

### ▼ Изменить общую информацию

---

1. В карточке приложения на вкладке Общая информация нажмите Редактировать.
2. Измените название или описание приложения.
3. Нажмите Сохранить.

### ▼ Загрузить логотип

---

1. В карточке приложения на вкладке Общая информация в блоке Логотип нажмите Загрузить. Поддерживаются изображения формата JPG и PNG, максимальный размер — 512KB.
2. Выберите файл.
3. Нажмите Загрузить.

### ▼ Загрузить/выгрузить шаблон

---

1. В карточке приложения на вкладке ESSO шаблон нажмите Загрузить шаблон.
2. В окне ESSO шаблон нажмите Выбрать файл.
3. Выберите файл.
4. Нажмите Загрузить шаблон.

Чтобы выгрузить использующийся в данный момент шаблон, нажмите Выгрузить шаблон. Шаблон будет доступен в папке Загрузки вашего компьютера.

### ▼ Добавить администратора

---

Можно назначить администратора, которому будут доступны только ограниченные настройки приложения. Такой пользователь будет иметь права:

- просматривать все настройки приложения в разделе Приложения;
- добавлять учетные записи для приложения в карточке политики;
- добавлять учетные записи для приложения в карточке пользователя.

Чтобы добавить администратора:

1. Перейдите на вкладку Администраторы.
2. В поле Тип объекта выберите тип — Пользователь или Группа.
3. В поле Расположение выберите расположение объекта. Это может быть весь пользовательский каталог или отдельное подразделение.
4. В поле Имя введите полное имя или часть имени для поиска.
5. Нажмите Поиск.
6. Выберите объект и нажмите Добавить.

## ▼ Создать ярлык для быстрого запуска

Для быстрого запуска приложения можно создать ярлык, который будет доступен в контекстном меню ESSO Agent в системном трее.

Чтобы создать ярлык:

1. Перейдите на вкладку Ярлыки.
2. Нажмите Добавить ярлык.
3. В открывшемся окне выполните настройки:
  - В поле Описание укажите дополнительную информацию для создаваемого ярлыка.
  - В поле Тип выберите Командная строка.
  - В поле Адрес укажите полный путь до исполняемого файла для десктоп-приложения или путь до исполняемого файла браузера и URL для веб-приложения.

Пример для десктоп-приложения

```
C:\TestFolder\Test.App.exe
```

Пример для веб-приложения

```
"%ProgramFiles%\Internet Explorer\iexplore.exe" "https://  
полное\_dns\_имя\_сервера/am/core/testapps/login.html"
```

4. Нажмите Добавить.



### ИНФОРМАЦИЯ

Если при создании шаблона были указаны параметры ярлыка, то они автоматически отобразятся на вкладке Ярлыки.

## ▼ Настроить парольную политику

---

Можно также настроить политику для генерации пароля при его смене в приложении.

Чтобы задать парольную политику:

1. Перейдите на вкладку Парольная политика.
2. В поле Минимальная длина пароля укажите минимальное количество символов пароля.
3. В поле Максимальное количество вхождений каждого символа укажите количество вхождений символов из группы символов. Для работы этого параметра необходимо создать группу символов.
4. Нажмите Добавить группу.
5. В поле Тип группы выберите предлагаемые типы символов или пользовательскую группу. При добавлении пользовательской группы укажите свою группу символов в поле Символы группы.
6. В поле Число символов укажите количество символов.
7. Нажмите Добавить. Добавленная группа символов отображается в списке групп.
8. Нажмите Сохранить.

## ▼ Изменить клиентский модуль

---

В разделе Клиентские модули указывается целевой URL приложения или путь к исполняемому файлу. Значение этого параметра содержится в шаблоне приложения. При необходимости это значение можно изменить.

Чтобы изменить клиентский модуль:

1. Выберите клиентский модуль и нажмите Редактировать.
2. Измените URL или путь к исполняемому файлу.
3. Если нужно использовать регулярное выражение, выберите Да в опции Использовать регулярное выражение.
4. Нажмите Сохранить.

## ▼ Настроить кеширование данных пользователя

---

Данная настройка позволяет включить кеширование данных пользователя на локальном компьютере для компонента Windows Logon и приложений, интегрированных с модулем Indeed AM Enterprise Single Sign-On.

Если данная настройка включена 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.

Включить кеширование данных пользователя можно в настройках политики или отдельного пользователя.

Если на пользователя распространяется действие политики, изменить настройки кеширования отдельно для него невозможно.

Подробнее о том, как включить эту настройку — в разделе [Кеширование данных пользователя](#).

# Модуль NPS Radius Extension

В разделе Приложения можно добавить приложения, интегрированные с модулем NPS Radius Extension, а также при необходимости задать их дополнительные настройки.

## Предварительная настройка

Перед добавлением интегрированного приложения:

1. **Настройте модуль NPS Radius Extension.**
2. **Зарегистрируйте лицензию** в Management Console.
3. **Установите и настройте провайдеры аутентификации.**
4. Интегрируйте бизнес-приложение с NPS Radius Extension.

Примеры интеграции бизнес-приложений:

- **Cisco ASA**
- **FortiGate-VM**
- **Citrix Netscaler**



### ВАЖНО

Если приложения работают через NPS (Network Policy Server) с установленным RADIUS Extension, но аутентификация для них будет осуществляться не через Access Manager, настройте для них доступ в Management Console в разделе Конфигурация. В противном случае вход в эти приложения будет невозможен.

## Добавить приложение

Чтобы добавить приложение, интегрированное с NPS RADIUS Extension:

1. На боковой панели Management Console откройте раздел Приложения.
2. Нажмите Добавить приложение.
3. В открывшемся окне выберите NPS Radius Extension и введите название приложения. Название должно быть уникальным.

4. Нажмите Создать.



#### ПРИМЕЧАНИЕ

Нельзя добавить еще одно приложение, если вы не изменили IP-адрес по умолчанию у ранее добавленного приложения.

5. В открывшемся окне приложения перейдите на вкладку RADIUS.

6. Измените значение поля IP-адрес сервера приложений. Можно указать несколько значений через запятую. Поддерживаются форматы IPv4 и IPv6. Также можно использовать маску или префикс для указания подсети.

#### ▼ Примеры адресов

##### Корректные адреса

- 192.168.0.1/24
- 172.16.3.251
- 10.0.0.1
- 21:db8:58:74:1c60:2c18::4/64

##### Некорректные адреса

- 192.168.0.300 — некорректный IPv4;
- 172.16.3.251/33 — некорректная маска сети;
- fe80::1%eth0 — некорректный IPv6;
- 21:db8:58:74:1c60:2c18:0:4/129 — некорректная маска сети;
- example.com — не является IP-адресом.

## Добавить в политику

Чтобы настройки приложения были применены для пользователей, добавьте приложение в политику. Сделать это можно только при наличии зарегистрированной лицензии для данного модуля.

Чтобы добавить приложение в политику:

1. Перейдите в раздел Политики.
2. Выберите политику из списка.
3. В карточке политики перейдите на вкладку Приложения.
4. Нажмите Добавить приложение.
5. Из выпадающего списка выберите приложение.
6. Нажмите Добавить.

Приложение отобразится в списке добавленных приложений.

## Настроить аутентификатор

Для приложений, интегрированных с Radius Extension, можно выбрать только один способ входа. При добавлении приложения в политику по умолчанию включается первый способ входа из доступных.

В списке доступных методов аутентификации отображаются провайдеры, установленные на Core Server и поддерживаемые RADIUS-приложениями.

Поддерживается как однофакторная, так и двухфакторная аутентификация.

### Предварительная настройка

Прежде чем настроить однофакторную или двухфакторную аутентификацию, установите провайдеры из каталога *Indeed AM <номер версии> \Indeed AM Providers\Indeed AM Radius Providers\<номер версии>* на Core Server.

### Однофакторная аутентификация

Чтобы настроить однофакторную аутентификацию:

1. На боковой панели Management Console откройте раздел Политики.
2. Выберите политику.
3. Перейдите на вкладку Приложения
4. Выберите приложение, интегрированное с NPS Radius Extension.
5. В списке Метод аутентификации выберите провайдер с префиксом 1FA.
6. Нажмите Сохранить.

Доступные способы входа по однофакторной аутентификации:



- Secured TOTP;
- Hardware OTP;
- Passcode;
- Software TOTP;
- Hardware TOTP.

## Двухфакторная аутентификация

Чтобы настроить двухфакторную аутентификацию:

1. На боковой панели Management Console откройте раздел Политики.
2. Выберите политику.
3. Перейдите на вкладку Приложения
4. Выберите приложение, интегрированное с NPS Radius Extension.
5. В списке Метод аутентификации выберите провайдер с префиксом 2FA.
6. Нажмите Сохранить.

Доступные способы входа по двухфакторной аутентификации:

- Passcode + Secured TOTP;
- Passcode + SMS OTP;
- Passcode + Software TOTP;
- Passcode + Indeed Key (только в режиме отправки push-уведомлений с подтверждением входа);
- Windows Password + Hardware HOTP;
- Windows Password + Hardware TOTP;
- Windows Password + Secured TOTP;
- Windows Password + Software TOTP;
- Windows Password + Storage SMS OTP;
- Windows Password + Indeed Key (только в режиме отправки push-уведомлений с подтверждением входа);
- Windows Password + Email OTP;
- Windows Password + SMS OTP;
- Windows Password + Telegram (только в режиме отправки одноразовых паролей);

- One-string authenticator (аутентификаторы вводятся в одну строку).

## Опциональные настройки

### ▼ Изменить общую информацию

---

1. В карточке приложения на вкладке Общая информация нажмите Редактировать.
2. Измените название или описание приложения.
3. Нажмите Сохранить.

### ▼ Загрузить логотип

---

1. На вкладке Общая информация в разделе Логотип нажмите Загрузить.  
Поддерживаются изображения формата JPG и PNG, максимальный размер — 512KB.
2. Выберите файл.
3. Нажмите Загрузить.

### ▼ Настроить доступ к приложениям для пользователей вне политик доступа

---

При необходимости можно разрешить или запретить доступ в приложения для тех пользователей, на которых не распространяются политики доступа Access Manager (например, для пользователей из другого домена). Для этого:

1. В карточке приложения перейдите на вкладку RADIUS.
2. В настройке Если для пользователя не заданы параметры доступа в приложение разрешите или запретите доступ.
3. Нажмите Сохранить.

## ▼ Настроить обработку повторных запросов на аутентификацию

---

При необходимости можно настроить обнаружение и обработку дубликатов запросов на аутентификацию. Эта необязательная настройка может быть полезна, когда наблюдаются повторные запросы. Например, если пользователь не успевает подтвердить вход через push-уведомление и получает его повторно.

Чтобы настроить обработку повторных запросов на аутентификацию:

1. В карточке приложения на вкладке RADIUS включите опцию Включить обнаружение и обработку дубликатов запросов на аутентификацию.
2. В поле Атрибуты запроса для поиска дубликатов введите значения атрибутов Radius. Можно указать несколько значений через запятую. Значения по умолчанию — *1* (User-Name) и *264* (Request authenticator).

В качестве атрибутов могут выступать имя пользователя, пароль, IP-адрес, с которого отправляется запрос на аутентификацию, и другие параметры. Запрос считается повторным, если значения всех указанных атрибутов в настройке совпадают со значениями в кешированном запросе. Подробнее о поддерживаемых атрибутах RADIUS — в [официальной документации Cisco](#).

3. Выберите тип ответа на дубликаты запросов:
  - Discard — проигнорировать. В этом случае сервер RADIUS не отправляет ответ на повторный запрос;
  - Reject — отклонить. В этом случае при повторном запросе сервер RADIUS отправляет ответ *Access-Reject* (Доступ отклонен).
4. Нажмите Сохранить.

# Кеширование данных пользователя

Данная настройка позволяет включить кеширование данных пользователя на локальном компьютере для компонента Windows Logon и приложений, интегрированных с модулем Indeed AM Enterprise Single Sign-On.

Если данная настройка включена 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.

Включить кеширование данных пользователя можно в настройках политики или отдельного пользователя.

Если на пользователя распространяется действие политики, изменить настройки кеширования отдельно для него невозможно.

## Для пользователей внутри политики

1. На боковой панели Management Console откройте раздел Политики.
2. В списке политик откройте нужную политику.
3. Откройте вкладку Приложения и выберите приложение ESSO или компонент Windows Logon, для которого необходимо включить кеширование данных.



### ПРИМЕЧАНИЕ

При включении кеширования для одного приложения ESSO настройки кеширования будут применены для всех ESSO приложений, добавленных в политику.

4. Нажмите Кеширование данных.
5. Для настройки Разрешить кешировать учетные данные на ПК пользователя выберите *Да*.
6. При необходимости настройте срок жизни кешированных данных:

- В полях Начальная дата и Конечная дата укажите срок действия кешированных аутентификаторов.
- В поле Количество дней с последнего входа в онлайн режим укажите срок действия кешированных аутентификаторов, отсчитывая срок от последнего входа в систему с подключением к сети.

Если срок действия кешированных аутентификаторов истек и Core Server недоступен, при попытке входа в систему отображается сообщение *Ошибка входа в систему. Период кеширования данных пользователя закончился.*

7. Нажмите Сохранить.

| main - Test.App.Win |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                       |          |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|----------|
| Информация          |  Сохранить  Отмена  Добавить учетную запись  Удалить  Кеширование данных |                       |          |
| Приложения          |  Для приложения включено кеширование данных на ПК пользователей                                                                                                                                                                                                                                                                                                                                                  |                       |          |
| Область действия    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                       |          |
| Администраторы      | УЧЕТНАЯ<br>ЗАПИСЬ                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | ТИП УЧЕТНЫХ<br>ДАННЫХ | ОПИСАНИЕ |

#### Для отдельного пользователя

1. На боковой панели Management Console откройте раздел Пользователи.
2. Найдите пользователя, для которого нужно включить кеширование.
3. Откройте вкладку Приложения и выберите приложение ESSO или компонент Windows Logon, для которого необходимо включить кеширование данных.

#### ПРИМЕЧАНИЕ

При включении кеширования для одного приложения ESSO настройки кеширования будут применены для всех ESSO приложений пользователя.

4. Нажмите Кеширование данных.
5. Для настройки Разрешить кешировать учетные данные на ПК пользователя выберите *Да*.
6. При необходимости настройте срок жизни кешированных данных:

- В полях Начальная дата и Конечная дата укажите срок действия кешированных аутентификаторов.
- В поле Количество дней с последнего входа в онлайн режим укажите срок действия кешированных аутентификаторов, отсчитывая срок от последнего входа в систему с подключением к сети.

Если срок действия кешированных аутентификаторов истек и Core Server недоступен, при попытке входа в систему отображается сообщение *Ошибка входа в систему.*

*Период кеширования данных пользователя закончился.*

7. Нажмите Сохранить.

Подробнее о настройках входа при отсутствии сети — в разделах [Enterprise SSO](#) и [Indeed Windows Logon](#).

# Лицензии

В Indeed Access Manager используется два типа лицензий:

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

Подробнее о лицензировании — в [Лицензирование](#).

## Получить

Лицензии генерируются на основе идентификатора инсталляции. Чтобы найти его и получить лицензии:

1. На боковой панели Management Console в блоке Настройки выберите Лицензии.
2. На вкладке Файлы лицензий скопируйте значение из поля Идентификатор инсталляции.
3. Отправьте скопированное значение закреплённому за вашей организацией менеджеру или в службу технической поддержки [support@indeed-id.com](mailto:support@indeed-id.com).

## Зарегистрировать

После получения лицензию нужно зарегистрировать. Для этого:

1. На боковой панели Management Console в блоке Настройки выберите Лицензии.
2. На вкладке Файлы лицензий нажмите Загрузить лицензию.
3. Нажмите Выбрать файл.
4. Выберите файл с лицензией и нажмите Зарегистрировать.

После успешной регистрации лицензии отображаются в таблице.

## Выдать лицензию пользователю

Для всех пользователей, которые включены в [политики доступа](#), выдача лицензий происходит автоматически. Лицензия закрепляется за пользователем после успешной аутентификации в

соответствующем модуле.

## Отозвать лицензию у пользователя

Для отзыва лицензий используется механизм автоматического освобождения лицензий. Этот механизм включен по умолчанию.

Лицензия отзывается у пользователя, если:

- пользователь удален из политики;
- пользователь отключен или перемещен из области действия политики;
- пользователь заблокирован/удален из Active Directory.

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

В Indeed Access Manager также можно настроить время, по истечении которого лицензия будет отозвана, и перезапустить механизм отзыва, если лицензии не освобождаются автоматически.

Для этого нужно отредактировать конфигурационный файл сервера

*C:\inetpub\wwwroot\am\core\Web.config*. Подробнее — в [Настройка механизма отзыва лицензий](#).

## Распределить по политикам (отделам)

Чтобы ограничить количество используемых лицензий для подразделения, вы можете задать доступное количество лицензий для определенной политики.

Чтобы задать доступное количество лицензий для политики:

1. На боковой панели Management Console перейдите в раздел Политики.
2. Выберите в списке политику.
3. На странице политики перейдите на вкладку Лицензии.
4. Выберите лицензии.
5. Нажмите Доступное количество.
6. В открывшемся окне введите количество доступных лицензий для политики и нажмите Сохранить.

В разделе Распределение лицензий по политикам отобразится количество используемых лицензий в рамках каждой политики.



На странице политики вы можете просмотреть количество используемых лицензий в этой политике и общее доступное количество лицензий для этой политики.

## Обновить

Чтобы обновить лицензии:

1. Обратитесь к закрепленному за вашей организацией менеджеру или в службу технической поддержки [support@indeed-id.com](mailto:support@indeed-id.com) с запросом на генерацию новых лицензий.
2. **Зарегистрируйте** новые лицензии в Management Console.

После окончания срока действия старых лицензий новые вступят в силу согласно заданным дате и времени.

Отслеживать срок действия лицензий можно в Management Console в разделе Лицензии.

# Аутентификаторы

Настроить аутентификаторы можно в следующих разделах Indeed Access Manager:

- Конфигурация→Аутентификаторы;
- Вкладка Приложения карточки политики;
- Вкладка Аутентификаторы карточки пользователя.

## Общие настройки

Раздел Конфигурация→Аутентификаторы содержит общие для всех пользователей настройки всех аутентификаторов, **установленных на сервере Indeed AM**. Настройки могут отличаться в зависимости от аутентификатора.

## Настроить автоматическую блокировку

Для аутентификаторов можно настроить автоматическую блокировку и разблокировку в случае неудачных попыток входа.

### ПРИМЕЧАНИЕ

Настройка блокировки аутентификаторов в Management Console не поддерживается для двухфакторной аутентификации для приложений RADIUS Extension.

Чтобы настроить автоматическую блокировку в Management Console:

1. Выберите аутентификатор.
2. Для параметра Блокировать способ аутентификации в случае серии неудачных попыток установите значение *Да*.
3. Задайте значения для следующих параметров:
  - Количество попыток аутентификации до блокировки. Этот параметр определяет количество неудачных попыток аутентификации до блокировки способа входа. Способ входа остается заблокированным до момента разблокировки администратором или до истечения таймаута до разблокировки. Значение параметра по умолчанию — 5. Заданное значение должно быть больше или равно 1.
  - Сброс счетчика блокировки через (минут). Этот параметр определяет, сколько минут должно пройти после неудачной попытки входа, прежде чем счетчик неудачных

попыток будет обнулен. Значение параметра по умолчанию — 5. Заданное значение должно быть больше или равно 1. Интервал сброса счетчика блокировки не должен быть больше таймаута до разблокировки способа входа, только если значение последнего не равно 0.

- Таймаут до разблокировки способа входа (минут). Этот параметр определяет период, на который заданный способ входа будет заблокирован. По истечении таймаута способ входа будет автоматически разблокирован. Значение параметра по умолчанию — 5. Если установлено значение 0, способ входа остается недоступным для пользователя, пока администратор не разблокирует его в Management Console.

4. Нажмите Сохранить.

## Настроить принудительную проверку

Для регистрации аутентификаторов Software TOTP, Secured TOTP и Software HOTP можно настроить принудительную проверку аутентификатора.

Если принудительная проверка аутентификатора включена, при регистрации появится дополнительное окно подтверждения для ввода данных аутентификации.

### Предварительные требования

Данная настройка работает в версии Management Console 8.2.6 или выше. Если установлена более старая версия, необходимо обновление. Посмотреть номер установленной версии можно в разделе Помощь и поддержка боковой панели Management Console.

Чтобы настройка принудительной проверки стала доступна в Management Console, настройте ее отображение с помощью утилиты *EA.Settings.Migration.Tool*. Подробнее об использовании утилиты — в [Миграция настроек провайдеров](#).

Чтобы включить принудительную проверку:

1. В разделе Конфигурация→Аутентификаторы выберите аутентификатор Software TOTP, Secured TOTP или Software HOTP.
2. В разделе Основные настройки включите принудительную проверку.

Для подтверждения регистрации введите полученные данные аутентификации и нажмите Подтвердить.

 **ПРИМЕЧАНИЕ**

При регистрации Storage SMS принудительная проверка выполняется по умолчанию.

## Настройки для политик

Можно также задать настройки аутентификаторов, которые распространяются на всех пользователей, включенных в политику. Эти настройки доступны в карточке политики в Management Console.

Чтобы задать настройки аутентификаторов для пользователей, включенных в политику:

1. На боковой панели Management Console выберите Политики.
2. Выберите политику.
3. Перейдите на вкладку Приложения. Эта вкладка содержит информацию о приложениях и модулях интеграции, добавленных в политику. Подробнее о настройках политик — в **Политики**.
4. Выберите приложение.
5. В секции Доступные методы аутентификации разрешите/запретите использование аутентификаторов.
6. Для модулей **Identity Provider**, **Windows Logon**, **ESSO Agent**, **ADFS Extension** выберите режим работы Indeed Key Provider.
7. Для модулей **Identity Provider**, **ADFS Extension** и **IIS Extension** выберите режим работы Telegram Provider.

## Настройки для отдельного пользователя

Задать настройки аутентификаторов для отдельного пользователя можно в его карточке в Management Console.

Чтобы открыть карточку пользователя:

1. На боковой панели Management Console выберите Пользователи.
2. Найдите пользователя. Подробнее о настройках поиска — в **Пользователи**.
3. В карточке пользователя перейдите на вкладку Аутентификаторы. Эта вкладка содержит информацию о количестве зарегистрированных аутентификаторов пользователя и их параметры.

## Зарегистрировать

Перед регистрацией аутентификаторов **создайте политику и распространите** ее на целевых пользователей.

### ⓘ ПРИМЕЧАНИЕ

Провайдеры Email OTP и SMS OTP не требуют регистрации и могут использоваться, если у пользователя задан email или номер телефона соответственно. Если параметры не заданы, то аутентификаторы не отображаются в списке доступных для пользователя.

Чтобы зарегистрировать аутентификатор:

1. Нажмите Зарегистрировать и выберите метод аутентификации из выпадающего списка.

Если у пользователя зарегистрировано максимальное количество аутентификаторов для определенного метода, то данный метод аутентификации отображаться не будет.

2. Выполните дополнительные настройки для регистрации аутентификатора. Для различных аутентификаторов отличаются окна и действия для регистрации.
3. После успешной регистрации статус аутентификатора — *Действующий*.
4. Если был удален провайдер, имеющий зарегистрированные аутентификаторы, то статус аутентификатора — *Не установлен*.

Аутентификатор появится в списке зарегистрированных для пользователя аутентификаторов.

## Запретить

Пользователю можно запретить использовать аутентификатор.

### ⓘ ПРИМЕЧАНИЕ

Способ аутентификации Windows Password не может быть запрещен. Рекомендуем отключить учетную запись пользователя в Active Directory, если нужно заблокировать доменный пароль.

Чтобы запретить пользователю использовать аутентификатор:

1. Выберите аутентификатор.

## 2. Нажмите Запретить.

После отключения аутентификатора пользователь не сможет использовать данный способ входа.

Статус аутентификатора — *Запрещен*.

В карточке пользователя можно запретить использовать аутентификатор только для одного пользователя. Запретить использовать аутентификатор всем пользователям можно в разделе [Конфигурация→Аутентификаторы](#).

## Разрешить

Чтобы разрешить пользователю использовать аутентификатор:

1. Выберите аутентификатор.
2. Нажмите Разрешить использовать.

После включения аутентификатора пользователь сможет использовать данный способ входа.

Статус аутентификатора — *Действующий*.



### ПРИМЕЧАНИЕ

В карточке пользователя можно разрешить использовать аутентификатор, только если запрет был установлен для отдельного пользователя. Снять запрет на использование аутентификатора для всех пользователей можно только в разделе [Конфигурация→Аутентификаторы](#).

## Разблокировать

Если для аутентификатора отключена автоматическая разблокировка после неудачных попыток входа, его нужно разблокировать вручную в карточке пользователя. Для этого:

1. Выберите заблокированный аутентификатор.
2. Нажмите Разблокировать.

Способ входа снова будет доступен для пользователя.

## Удалить

1. Выберите аутентификатор.

2. Нажмите Удалить.

3. Подтвердите удаление.

Аутентификатор исчезнет из списка зарегистрированных для пользователя аутентификаторов.

# Пользователи

В карточке пользователя содержится информация о пользователе из Active Directory (AD) и настройки для пользователя в системе Indeed.

## Найти пользователя

1. На боковой панели Management Console откройте раздел Пользователи.
2. В поле Имя введите имя пользователя, часть имени или UserPrincipalName (UPN, имя пользователя в формате адреса электронной почты, например `username@domain.com`).
3. В поле Контейнер выберите место поиска — весь контейнер или отдельное подразделение. Если оставить поле Имя пустым, в результате поиска отобразятся все пользователи в выбранном контейнере.
4. Нажмите Поиск.

В окне отобразится список пользователей, попадающих под критерии поиска.

Варианты поиска пользователей можно настроить. Для этого откройте файл `C:\inetpub\wwwroot\am\mc\Config\userSearchSettings.config` и установите значения `true` или `false` в строках:

- `searchByGivenName` — поиск в Active Directory по атрибуту `GivenName` (имя);
- `searchBySn` — поиск по фамилии;
- `searchByUpn` — поиск по атрибуту `UPN` (User Principal Name);
- `searchByGivenNameAndSn` — поиск по имени и фамилии;
- `searchByName` — поиск в Active Directory по атрибуту `Name`.

В строке `searchTemplate` можно задать шаблон для поиска. Например, значение `searchTemplate="*(*)"` означает, что поиск будет вестись по всем значениям объекта.

## Просмотреть общую информацию

1. Найдите пользователя.
2. Откройте карточку пользователя, нажав на его имя.
3. Вкладка Общая информация содержит следующие данные:



- Информация о пользователе из Active Directory:
  - Фото — атрибут `jpegPhoto` или `thumbnailPhoto`. Если атрибуты пустые, то используется изображение-заглушка.
  - Учетная запись — атрибут `userPrincipalName`.
  - Email — атрибут `mail`.
  - Телефон — атрибут `telephoneNumber`.
  - Путь в каталоге — расположение пользователя в каталоге Active Directory.
- Данные из системы Indeed AM:
  - Политика — название политики, которая распространяется на пользователя. Чтобы перейти в карточку политики, нажмите ее название.
  - Количество приложений — число приложений, которые доступны пользователю.
  - Количество аутентификаторов — общее число зарегистрированных аутентификаторов для пользователя.
  - События — пять последних событий, связанных с данным пользователем. Чтобы просмотреть все события, связанные с пользователем, нажмите Все события пользователя.

МС / Пользователи / Admin-indeed

## Admin-indeed - Общая информация

Общая информация

Приложения

Аутентификаторы

История входов

Лицензии



Учётная запись

Admin-indeed@company.local

Email

test@company.local

Телефон

+79123456789

Путь в каталоге

company.local/Indeed/Admins/Admin-indeed



С целью обеспечения безопасности пароля учетной записи, включена автоматическая генерация случайного пароля. Для изменения настроек перейдите в приложение "Windows Logon" в политике.

Политика

main 

Количество приложений

Количество аутентификаторов

5

2

| СОБЫТИЕ                                                                                                                                                       | ДАТА                | ИНИЦИАТОР    |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|--------------|
|  Пользователь был аутентифицирован по предоставленному аутентификатору.      | 2025.03.18 11:48:02 | Admin-indeed |
|  Настройки кэширования данных пользователя в политике были успешно изменены: | 2025.03.17 18:07:40 | Admin-indeed |
|  Пользователь был аутентифицирован по предоставленному аутентификатору.      | 2025.03.17 12:52:00 | Admin-indeed |
|  Пользователь был аутентифицирован по предоставленному аутентификатору.      | 2025.03.12 17:56:08 | Admin-indeed |
|  Пользователь был аутентифицирован для целевого приложения.                | 2025.03.10 11:34:17 | Admin-indeed |

Все события пользователя 

## Добавить в политику

Чтобы распространить настройки политики на пользователя, нужно добавить его в область действия политики. Подробнее — в разделе **Политики**.

## Просмотреть информацию о приложениях

Если пользователь попадает в область действия более одной политики, он получает доступ ко всем приложениям и модулям, добавленным в эти политики. Подробнее о политиках и их приоритетах — в разделе **Политики доступа**. Узнать, как управлять политиками в Management Console, можно в разделе **Политики**.

Чтобы просмотреть список доступных пользователю приложений и модулей:

1. В карточке пользователя перейдите на вкладку Приложения.
2. В открывшемся окне отобразится таблица со списком приложений и модулей, доступных пользователю.

614

3. Чтобы просмотреть более подробную информацию о методах аутентификации, настроенных для модуля или приложения, нажмите на его название.

## Настроить кеширование данных

Для пользователя можно включить кеширование данных на локальном компьютере для компонента Windows Logon и приложений, интегрированных с модулем Indeed AM Enterprise Single Sign-On. Это позволяет войти в систему по аутентификатору даже при отсутствии физического подключения к сети. Подробнее о включении данной настройки — в разделе [Кеширование данных пользователя](#)

## Настроить аутентификаторы

В карточке пользователя также можно управлять настройками аутентификаторов для целевого пользователя. Подробнее — в статье [Аутентификаторы](#).

## Просмотреть историю входов

В карточке пользователя можно просмотреть историю входов пользователя в модули Indeed AM, а также выгрузить эту информацию в файл в форматах CSV, XLSX или PDF.

Чтобы просмотреть историю входов пользователя:

1. В карточке пользователя перейдите на вкладку История входов.
2. При необходимости задайте фильтры для выборочного поиска записей о входах:
  - Укажите начальную и конечную даты периода, за который хотите посмотреть историю входов.
  - Выберите приложение или модуль.
  - Выберите тип аутентификатора, используемый для входа.
  - Выберите статус события — Успешный вход, Не удалось войти или Не задано.
3. Нажмите Применить.
4. Чтобы выгрузить историю входов, нажмите Экспортировать и выберите формат файла — CSV, XLSX или PDF.

## Просмотреть лицензии

Для всех пользователей, которые включены в политики доступа, выдача лицензий происходит автоматически. Лицензия закрепляется за пользователем после успешной аутентификации в соответствующем модуле.

Чтобы просмотреть доступные пользователю лицензии, в карточке пользователя перейдите на вкладку Лицензии.

# Политики

Политики позволяют задать настройки доступа для определенной группы пользователей.

Подробнее о применении настроек политики — в разделе [Политики доступа](#).

## Создать

1. На боковой панели Management Console откройте раздел Политики.
2. Нажмите Создать политику.
3. Укажите значения для следующих параметров:
  - Приоритет. Чем больше значение, тем выше приоритет. Подробнее о приоритетах — в разделе [Политики доступа](#).
  - Имя.
  - Описание (необязательно).

Создать политику

Приоритет\*

999

Имя\*

Общая политика

Описание

Общая политика для всех пользователей системы

Отмена

Создать

## Настроить

В карточке политики можно настроить параметры политики. Для этого:

1. На боковой панели Management Console откройте раздел Политики.

2. Откройте политику, нажав на ее название.
3. Перейдите на нужную вкладку и выполните соответствующие настройки.

## Изменить информацию

В карточке политики можно изменить заданные ранее имя, приоритет и описание политики. Для этого:

1. На вкладке Информация нажмите Редактировать.
2. Внесите изменения.
3. Нажмите Сохранить.

## Добавить/удалить приложение

Чтобы настроить политику, нужно добавить приложения, на которые будет распространяться ее действие. Для этого:

1. В карточке политики перейдите на вкладку Приложения.
2. Нажмите Добавить приложение.
3. В окне Добавить приложение выберите приложение и нажмите Добавить.

Приложение отобразится в таблице добавленных приложений.



### ПРИМЕЧАНИЕ

Добавить приложение можно только при наличии зарегистрированной лицензии для данного модуля.

Чтобы удалить приложение:

1. В карточке политики перейдите на вкладку Приложения.
2. Выберите приложение.
3. Нажмите Удалить.
4. Подтвердите удаление.

Приложение будет удалено из списка добавленных приложений.

Подробнее о настройках приложений — в разделе [Приложения](#).

## Добавить/удалить объекты в области действия

Чтобы распространить настройки политики на определенных пользователей, нужно добавить объекты в области действия. В качестве таких объектов можно добавить отдельных пользователей, группы или подразделения.

Чтобы добавить объект в области действия:

1. В карточке политики перейдите на вкладку Область действия.
2. Нажмите Добавить.
3. В поле Тип объекта выберите тип — Пользователь, Группа или Подразделение.
4. В поле Расположение выберите расположение объекта. Это может быть весь пользовательский каталог или отдельное подразделение.
5. В поле Название укажите полное или часть имени объекта и нажмите Поиск.

Если оставить поле Название пустым, в результате поиска отобразятся все объекты заданного типа, имеющие выбранное расположение.

6. Выберите объект.
7. Нажмите Добавить.

Объект отобразится в списке объектов области действия.

**Глобальный администратор** может также искать и удалять объекты из области действия политики.

Для поиска объектов можно использовать шаблоны, заданные **в конфигурационном файле Management Console**.

Чтобы удалить объект область действия:

1. В карточке политики перейдите на вкладку Область действия.
2. Выберите объект.
3. Нажмите Удалить.
4. Подтвердите удаление. Объект будет удален из списка объектов в области действия.

Глобальный администратор может также воспользоваться функцией поиска объекта.

Чтобы найти и удалить объект в области действия политики: {#search-remove}

1. В карточке политики перейдите на вкладку Область действия.
2. Нажмите Поиск. Откроется страница поиска.
3. В поле Тип объекта выберите тип — Пользователь, Группа или Подразделение. Выберите тип объекта и расположение.
4. В поле Расположение выберите расположение объекта. Это может быть весь пользовательский каталог или отдельное подразделение.
5. В поле Название укажите полное или часть имени объекта и нажмите Поиск.

Если оставить поле Название пустым, в результате поиска отобразятся все объекты заданного типа, имеющие выбранное расположение.

6. Выберите объект в результатах поиска и нажмите кнопку Удалить.
7. Подтвердите удаление. Объект будет удален из списка объектов в области действия.

## Задать роли

Для политики также можно назначить пользователей, которые смогут выполнять роль администратора, оператора или инспектора относительно этой политики. Назначить роль можно отдельным пользователям или группе пользователей. Каждая роль имеет свой набор прав.

Чтобы назначить роль:

1. В карточке политики перейдите на вкладку Администраторы.
2. Нажмите Добавить.
3. Выберите роль — Администратор, Оператор или Инспектор.
4. В поле Тип объекта выберите тип — Пользователь или Группа.
5. В поле Расположение выберите расположение объекта. Это может быть весь пользовательский каталог или отдельное подразделение.
6. В поле Название укажите полное или часть имени объекта и нажмите Поиск. Если оставить поле Название пустым, в результате поиска отобразятся все объекты заданного типа, имеющие выбранное расположение.
7. Выберите объект.
8. Нажмите Добавить.

После добавления объект отобразится в списке на вкладке Администраторы.



## Распределить лицензии

Можно задать доступное количество лицензий для определенной политики, чтобы ограничить количество используемых лицензий для подразделения. О том, как это сделать — в разделе [Лицензии](#).

## Удалить политику

Чтобы удалить политику:

1. На боковой панели Management Console откройте раздел Политики.
2. В списке политик выберите нужную политику.
3. Нажмите Удалить.
4. Подтвердите удаление.

Удаленная политика исчезнет из списка политик.

Также удалить политику можно в карточке политики. Для этого:

1. В карточке политики перейдите на вкладку Информация.
2. Нажмите Удалить.
3. Подтвердите удаление.

## Кеширование данных пользователя

Данная настройка позволяет включить кеширование данных пользователя на локальном компьютере для компонента Windows Logon и приложений, интегрированных с модулем Indeed AM Enterprise Single Sign-On.

Если данная настройка включена 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.

Включить кеширование данных пользователя можно в настройках политики или отдельного пользователя.

Если на пользователя распространяется действие политики, изменить настройки кеширование отдельно для него невозможно.

Подробнее о том, как включить эту настройку — в разделе [Кеширование данных пользователя](#).

# Устройства

В данном разделе можно управлять общими настройками устройств Software HOTP, Hardware OTP и TOTP. Детали о частных настройках устройств можно узнать в разделе [Установка и настройка провайдеров аутентификации](#).

## Добавить

Чтобы добавить устройство:

1. На боковой панели Management Console откройте раздел Устройства.
2. Нажмите Добавить из файла, чтобы загрузить информацию из файла с параметрами устройства, или Добавить, чтобы задать параметры устройства вручную.

### Добавить из файла

1. Нажмите Добавить из файла.
2. Выберите файл с параметрами устройства и нажмите Добавить.
3. В окне Результат отобразится количество добавленных устройств.
4. Нажмите Заккрыть.

Добавленное устройство отобразится в списке доступных устройств.

### Добавить вручную

1. Нажмите Добавить.
2. В поле Серийный номер укажите серийный номер устройства.
3. В поле Секретный ключ укажите ключ устройства (значение параметра `Seed`).
4. При необходимости укажите дополнительную информацию в поле Комментарий.
5. Нажмите Добавить.

Добавленное устройство отобразится в списке доступных устройств.

## Удалить

Чтобы удалить устройство:

1. На боковой панели Management Console откройте раздел Устройства.
2. Чтобы удалить устройство вручную, выберите его из списка и нажмите Удалить.

При необходимости можно выполнить поиск, используя фильтры в верхней части страницы.

3. Чтобы удалить устройство по информации из файла:

1. Нажмите Удалить из файла.
2. Выберите XML-файл с параметрами устройства и нажмите Удалить.
3. В окне Результат отобразится количество удаленных устройств.
4. Нажмите Заккрыть.

## Синхронизировать

Чтобы синхронизировать устройство в случае рассинхронизации счетчиков на устройстве и сервере:

1. На боковой панели Management Console откройте раздел Устройства.
2. Нажмите серийный номер устройства.
3. На верхней панели нажмите Синхронизировать ОТР.
4. В открывшемся окне введите два последовательно сгенерированных на устройстве одноразовых пароля и нажмите Синхронизировать.

## Заблокировать/разблокировать

В Management Console можно как отключить возможность использовать добавленное устройство, так и разблокировать ранее заблокированное.

Чтобы заблокировать устройство:

1. В разделе Устройства Management Console выберите устройство из списка добавленных.
2. Нажмите Заблокировать

Статус устройства сменится с Активно на Заблокировано.

Чтобы разблокировать устройство:

1. В разделе Устройства Management Console выберите заблокированное устройство.
2. Нажмите Разблокировать.

Статус устройства сменится с Заблокировано на Активно.

# События

Записи обо всех операциях Indeed AM отражаются в журнале событий на каждом сервере Indeed AM.

В Indeed AM ведется учет событий следующих типов:

- ошибка;
- информация;
- предупреждение.

Чтобы открыть журнал событий, в левом меню в блоке Аудит выберите События.

Для более узкого поиска событий используйте параметры фильтра:

- *Пользователь или инициатор* — в поле требуется выбрать учетную запись, от имени которой было совершено событие;
- *Приложение* — фильтрация событий по выбранному компоненту Indeed AM.
- *Начальная\Конечная дата* — в полях указывается временной интервал, в котором будет выполнена выборка событий.
- *Тип аутентификатора* — фильтрация событий по выбранному методу аутентификации Indeed AM.
- *Модуль* — фильтрация событий по выбранному модулю системы Indeed AM.

## ПРИМЕЧАНИЕ

При поиске событий будут отображены события для конкретного модуля системы, в отличие от параметра *Приложение*, где события отображаются для конкретного приложения системы, но могут присутствовать различные модули.

- *Описание содержит* — в поле указывается полное значение атрибута события (приложение, администратор, компьютер и др.).

## ❗ ИНФОРМАЦИЯ

Поиск по части запроса с использованием символа \* невозможен: это связано с ограничениями хранилища EventLog Microsoft. Возможности поиска с использованием остальных поддерживаемых методов хранения ограничены по возможностям самого ограниченного источника — EventLog.

- *Тип события* — в поле указывается тип события: ошибка, информация, предупреждение. Если выбран параметр *Не задано*, осуществляется выборка всех событий.
- *Код события* — в поле можно выбрать конкретное событие системы Indeed AM.

### Выберите события

☐

|                          |                                                                                          |       |                                                                                                                                                                                                                                                                                                               |
|--------------------------|------------------------------------------------------------------------------------------|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> |  1000   | Info  | Пользователь был аутентифицирован по предоставленному аутентификатору. Приложение: {requestApplication}. Инициатор: {requestUser}. Компьютер: {requestComputer}. Способ аутентификации: {authMode}. Комментарий аутентификатора: {authComment}. Имя бизнес приложения: {businessApplication}.                 |
| <input type="checkbox"/> |  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}. |
| <input type="checkbox"/> |  1001 | Info  | Сервер Indeed-Id был запущен. Компьютер: {computer}.                                                                                                                                                                                                                                                          |

Отмена

Выбрать

## События

 Экспортировать

|                                                                 |                                            |                                                          |                                                  |
|-----------------------------------------------------------------|--------------------------------------------|----------------------------------------------------------|--------------------------------------------------|
| Пользователь или инициатор<br>Admin-Indeed <span>Выбрать</span> | Приложение<br>Windows Logon <span>▼</span> | Начальная дата<br>2020/08/26 00:00 <span>📅</span>        | Конечная дата<br>2020/08/30 00:00 <span>📅</span> |
| Тип аутентификатора<br>AirKey Cloud <span>▼</span>              | Модуль<br>Не задано <span>▼</span>         | Описание содержит <span>ℹ</span><br><input type="text"/> | Тип события<br>Информация <span>▼</span>         |
| Код события<br>1000 <span>Выбрать</span>                        |                                            |                                                          |                                                  |
| <span>Применить</span> <span>Сбросить</span>                    |                                            |                                                          |                                                  |

| СОБЫТИЕ                                                                                 | ДАТА                | МОДУЛЬ        | ИНИЦИАТОР    | КОД  |
|-----------------------------------------------------------------------------------------|---------------------|---------------|--------------|------|
| ▶ <span>ℹ</span> Пользователь был аутентифицирован по предоставленному аутентификатору. | 2020.08.28 21:49:41 | Windows Logon | Admin-Indeed | 1000 |
| ▶ <span>ℹ</span> Пользователь был аутентифицирован по предоставленному аутентификатору. | 2020.08.28 21:49:26 | Windows Logon | Admin-Indeed | 1000 |
| ▶ <span>ℹ</span> Пользователь был аутентифицирован по предоставленному аутентификатору. | 2020.08.28 13:21:36 | Windows Logon | Admin-Indeed | 1000 |
| ▶ <span>ℹ</span> Пользователь был аутентифицирован по предоставленному аутентификатору. | 2020.08.28 13:16:19 | Windows Logon | Admin-Indeed | 1000 |
| ▶ <span>ℹ</span> Пользователь был аутентифицирован по предоставленному аутентификатору. | 2020.08.28 13:15:19 | Windows Logon | Admin-Indeed | 1000 |

Для экспорта событий нажмите кнопку Экспортировать в верхней части страницы. Экспорт возможен в форматах csv, xlsx, pdf.

Список событий Indeed AM Server и Indeed Key Server вы можете просмотреть в [Справочнике](#).



# Конфигурация

В данном разделе Management Console можно настроить аутентификаторы и задать права доступа.

## Права доступа

### Роли

В разделе Роли можно посмотреть права ролей относительно всей системы Indeed AM — глобальный администратор, оператор или инспектор. Каждая роль имеет свой набор прав. Подробнее о ролях — в разделе [Роли](#).

### Глобальные администраторы

В разделе Глобальные администраторы можно посмотреть и добавить пользователей с ролями глобальный администратор, оператор или инспектор, которые имеют права на администрирование всей системы Indeed AM.

Чтобы назначить роль:

1. Перейдите на вкладку Глобальные администраторы.
2. Нажмите Добавить и выберите необходимую роль.
3. В поле Имя введите имя пользователя, часть имени или UPN.
4. В поле Тип объекта выберите тип — Пользователь или Группа.
5. В поле Расположение выберите расположение объекта. Это может быть весь пользовательский каталог или отдельное подразделение. Если оставить поле Имя пустым, в результате поиска отобразятся все объекты заданного типа, имеющие выбранное расположение.
6. Выберите объект.
7. Нажмите Добавить.

Пользователь с назначенной ролью отобразится в списке на вкладке Глобальные администраторы.

| Конфигурация - Глобальные администраторы |                                                    |                     |              |                                              |
|------------------------------------------|----------------------------------------------------|---------------------|--------------|----------------------------------------------|
| Права доступа                            | <a href="#">+ Добавить</a> <a href="#">Удалить</a> |                     |              |                                              |
| Роли                                     |                                                    |                     |              |                                              |
| Глобальные администраторы                | ИМЯ                                                | ГРУППА БЕЗОПАСНОСТИ | ТИП ОБЪЕКТА  | РАСПОЛОЖЕНИЕ                                 |
| Аутентификаторы                          | Администратор                                      |                     |              |                                              |
| Multi-factor authentication              | <input type="checkbox"/> Admin-Indeed              | Администратор       | Пользователь | indeed.local/Indeed/UsersIndeed/Admin-Indeed |
| Push-аутентификация                      | Оператор                                           |                     |              |                                              |
| Одноразовый пароль по SMS                | <input type="checkbox"/> Operator                  | Оператор            | Пользователь | indeed.local/Indeed/UsersIndeed/Operator     |
| Пароль Passcode                          | Инспектор                                          |                     |              |                                              |
| Пароль Windows                           | <input type="checkbox"/> Inspector                 | Инспектор           | Пользователь | indeed.local/Indeed/UsersIndeed/Inspector    |

Также можно назначить пользователю **роль в рамках одной политики**.

## Аутентификаторы

В разделе можно посмотреть и настроить аутентификаторы, которые установлены на данном сервере.

## Разрешить/Запретить использование и редактирование

Чтобы настроить использование и редактирование аутентификаторов:

1. Выберите аутентификатор.
2. В секции Основные настройки:
  - В настройке Запретить использовать укажите, могут ли пользователи использовать или регистрировать выбранный аутентификатор.
  - Задайте другие настройки в зависимости от типа аутентификатора.
3. Для аутентификаторов, которые требуют регистрации, в секции Доступные пользователю действия:
  - В настройке Регистрация новых аутентификаторов укажите, могут ли пользователи регистрировать новые аутентификаторы.
  - В настройке Редактирование имеющихся аутентификаторов укажите, могут ли пользователи изменять уже зарегистрированные аутентификаторы.
  - В настройке Удаление имеющихся аутентификаторов укажите, могут ли пользователи удалять уже зарегистрированные аутентификаторы.
  - В настройке Разрешить редактирование комментария к аутентификатору укажите, в какой момент пользователи могут редактировать комментарии к уже

зарегистрированным аутентификаторам.

## Изменить максимальное количество

В данном разделе можно определить, сколько аутентификаторов может максимально зарегистрировать для себя один пользователь. Эта настройка доступна для следующих аутентификаторов:

- **IronLogic Z2USB Provider**
- **Passcode Provider**
- **OMNIKEY Provider**
- **Smart Card Provider**

Чтобы задать максимальное количество:

1. Выберите аутентификатор.
2. В поле Максимальное количество введите значение.
3. Нажмите Сохранить.

# Руководство пользователя



## Карточка пользователя

Информация о пользователе



## Управление аутентификаторами

Управление аутентификаторами пользователя



## Локализация

Смена языка в консоли пользователя



## Управление Windows Password

Изменить или зарегистрировать доменный пароль

# Карточка пользователя

В карточке пользователя содержится следующая информация:

- Данные из профиля Active Directory:
  - Имя учетной записи — атрибут *userPrincipalName*;
  - Путь — путь к учетной записи пользователя в каталоге;
  - E-mail — атрибут *mail*;
  - Телефон — атрибут *telephoneNumber*;
  - Фото — атрибут *jpegPhoto* или *thumbnailPhoto*. Если атрибуты пустые, то используется изображение-заглушка;
  - История входов — последние события в системе Indeed AM, инициатором которых был пользователь;
  - Сведения о зарегистрированных аутентификаторах на вкладке Аутентификаторы.

# Управление аутентификаторами

В карточке пользователя на вкладке Аутентификаторы содержится информация о количестве зарегистрированных аутентификаторов пользователя и их параметры. По умолчанию пользователи могут только регистрировать аутентификаторы. Для остальных действий с аутентификаторами запросите права у администратора.

## Зарегистрировать



### ПРИМЕЧАНИЕ

Провайдеры Email OTP и SMS OTP регистрируются автоматически, если у пользователя задан email или номер телефона в Active Directory.

Чтобы зарегистрировать аутентификатор:

1. Выберите аутентификатор.
2. Нажмите .
3. Выберите Зарегистрировать.
4. Введите запрашиваемые данные и нажмите Сохранить. Запрашиваемые данные и действия при регистрации могут отличаться в зависимости от аутентификатора.
5. При необходимости введите данные аутентификации, чтобы подтвердить регистрацию.

После успешной регистрации аутентификатор отобразится как зарегистрированный.

Если у пользователя зарегистрировано максимальное количество аутентификаторов, регистрация завершится ошибкой *Доступ запрещен: Достигнуто максимальное количество аутентификаторов*.

Если зарегистрированный аутентификатор удален администратором, он перестанет отображаться в карточке пользователя.

## Изменить

Чтобы изменить аутентификатор:

1. Выберите аутентификатор.
2. Нажмите .
3. Выберите Изменить.
4. Введите новые данные для аутентификатора.
5. Нажмите Сохранить. При необходимости введите данные аутентификации, чтобы подтвердить регистрацию.

## Удалить

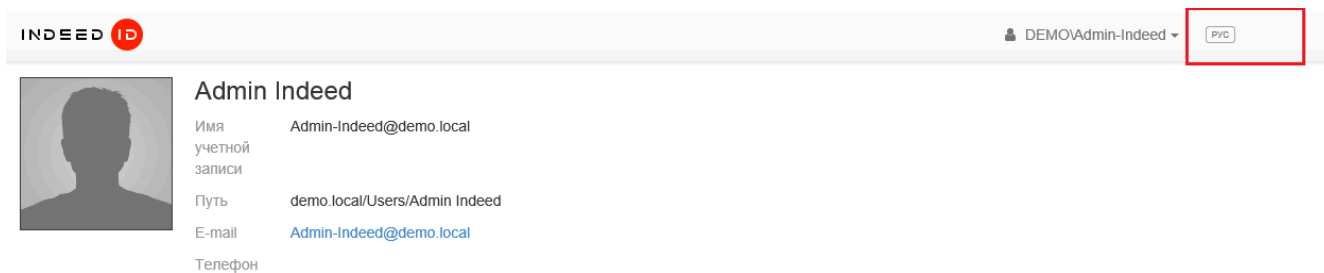
Чтобы удалить аутентификатор:

1. Выберите аутентификатор.
2. Нажмите .
3. Выберите Удалить.
4. Подтвердите удаление.

# Локализация

Чтобы сменить язык:

1. Нажмите кнопку с названием языка в правом верхнем углу.
2. В выпадающем списке выберите нужный язык.





# Управление Windows Password

В User Console можно зарегистрировать или изменить доменный пароль.

## Зарегистрировать

Чтобы зарегистрировать доменный пароль:

1. Откройте User Console.
2. Перейдите на вкладку Аутентификаторы.
3. В списке аутентификаторов выберите Windows Password.
4. Нажмите .
5. Выберите Зарегистрировать пароль.
6. В открывшемся окне введите пароль и нажмите Сохранить.

## Изменить

Чтобы сменить доменный пароль:

1. Откройте User Console.
2. Перейдите на вкладку Аутентификаторы.
3. В списке аутентификаторов выберите Windows Password.
4. Нажмите .
5. Выберите Изменить пароль.
6. В появившемся окне введите текущий пароль, новый пароль, подтвердите новый пароль и нажмите Сохранить.

# API



## Общая информация

Общая информация



## Быстрый старт

Быстрый старт



## Методы API

Количество глав: 8



## Сценарии использования

Количество глав: 6

# Общая информация

Вы можете использовать API Indeed AM для интеграции с приложениями.

В данном разделе описаны основные моменты и общие параметры, которые необходимы для использования API Indeed.

## Запрос к API

Для обращения к методу необходимо выполнить запрос `POST` или для некоторых методов запрос `GET` по `http(s)://<dns_indeedam_server>/am/core/<url_api_method>`, где:

- `dns_indeedam_server` — полное DNS-имя сервера, где развернут Indeed AM Server;
- `url_api_method` — адрес соответствующего метода; адреса указаны в документации к методу, либо в Swagger.

Пример для метода `authenticateByWindowsToken`, где DNS-имя сервера Indeed AM: `indeedam.indeed.local`:

```
https://indeedam.indeed.local/am/core/api/v5/logon/authenticateByWindowsTo
```



### ВАЖНО!

При использовании протокола HTTPS загрузите на сервер Indeed AM действующий сертификат.

## UserId

В данном параметре указывается уникальный идентификатор пользователя из системы Indeed.

Идентификатор состоит из строкового ID, указанного в `web.config` AM в параметре `userId`, и `objectGuid` пользователя из Active Directory.

Например, в параметре `userId` указано значение GUID пользователя `10efa04f-7ba9-47d8-89db-56e166f1679f`. UserId пользователя будет `UserId\_10efa04f-7ba9-47d8-89db-56e166f1679f`.

Для получения `userId` можно воспользоваться методом `[POST]/api/v5/user/searchUserId`.

## modeId

Уникальный идентификатор 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 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}

Чтобы получить все установленные способы аутентификации на сервере Indeed AM, вы можете воспользоваться методом `[GET]/api/v5/authenticationProvider/getAll`.

# ApplicationId

## Внутренний модуль

### **ВАЖНО!**

Для работы с внутренним модулем не требуется лицензия, достаточно иметь права на операции, предоставляемые внутренними модулями.

Функциональность Access Manager разбита на группы, за которые отвечают внутренние модули. Они реализуют внутреннюю бизнес-логику решения. Их строковые идентификаторы используются для обращения к разным частям API Core Server.

Внутренние модули Core Server:

- User Profile Setting Management,
- User Access Control Management,
- Hardware Devices Management,
- License Management,
- Authenticator Management,
- Authenticator Enrollment,
- User Accounts Management,
- Policy Management,
- User Cache Management,
- Business Applications Management.

Кроме того, есть еще набор внутренних приложений:

- Enterprise Management Console,
- Self Service,
- Native Enroller.

## Модуль интеграции

### **ВАЖНО!**

Для работы с модулями интеграции требуется лицензия для соответствующего модуля.

Это модуль, реализующий взаимосвязь Access Manager и внешних систем, с которыми выполняется интеграция. К ним относятся:

- Windows Logon,
- Enterprise SSO,
- IIS Extension,
- NPS RADIUS Extension,
- 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 или удалять, например модуль Enterprise SSO. Он предоставляет возможности интеграции с разными типами приложений пользователя (desktopными или веб-приложениями) и для каждого нужно создавать отдельное бизнес-приложение ESSO: 1C, Lotus Notes и так далее.

## Идентификатор политики

Чтобы узнать идентификатор политик, выполните следующее:

1. Откройте Management Concole.
2. Перейдите на вкладку Политики.
3. Выберите целевую политику.
4. Скопируйте идентификатор политики из параметра `policyId` в URL.

# Быстрый старт

Для вызова методов API, тестирования запросов вы можете использовать интерфейс Swagger, который встроен в Core Server.

Для включения доступа к интерфейсу выполните следующие действия:

1. Откройте конфигурационный файл Core Server *web.config* (расположен в папке *C:\inetpub\wwwroot\am\core*).
2. Для параметра `enableSwagger` установите значение *true*.

Интерфейс Swagger будет доступен по ссылке  
*http(s)://<DNS\_IndeedAM\_Server>/am/core/swagger/*

 **swagger**

**Explore**

## EA.Server API

Created by Indeed Id  
[Contact the developer](#)

|                               |           |                 |                   |
|-------------------------------|-----------|-----------------|-------------------|
| <b>AccessControl</b>          | Show/Hide | List Operations | Expand Operations |
| <b>AuthenticationMethod</b>   | Show/Hide | List Operations | Expand Operations |
| <b>AuthenticationProvider</b> | Show/Hide | List Operations | Expand Operations |
| <b>Authenticator</b>          | Show/Hide | List Operations | Expand Operations |
| <b>BusinessApplication</b>    | Show/Hide | List Operations | Expand Operations |
| <b>ESSO</b>                   | Show/Hide | List Operations | Expand Operations |
| <b>HardwareDevice</b>         | Show/Hide | List Operations | Expand Operations |
| <b>HealthCheck</b>            | Show/Hide | List Operations | Expand Operations |
| <b>Identification</b>         | Show/Hide | List Operations | Expand Operations |
| <b>InstanceInfo</b>           | Show/Hide | List Operations | Expand Operations |
| <b>License</b>                | Show/Hide | List Operations | Expand Operations |
| <b>Logon</b>                  | Show/Hide | List Operations | Expand Operations |
| <b>Module</b>                 | Show/Hide | List Operations | Expand Operations |

## Токен администратора запроса

Для выполнения большинства запросов API требуются определенные права в системе Indeed. Для успешного выполнения таких запросов необходимо выполнить аутентификации в API под

пользователем с требуемым набором прав. После выполнения аутентификации будет получен токен сессии, который используется в запросах API.

Получение токена с помощью `authenticate ByWindowsToken`

### Описание метода

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 при запросе необходимо использовать дополнительный параметр `UseDefaultCredentials` (пример функции `postRequestForWin` в Powershell).

В качестве идентификатора приложения может быть указано любое приложение из [списка Indeed](#).



#### ВАЖНО!

Используемое приложение будет указываться в событиях аутентификации.

#### Response Body

```
{
  "ValidPropertiesMask": 5,
  "Token": ""
  "LogonResult": null,
  "UserId": ""
}
```

Получение токена с помощью `authenticate`

### Описание метода

В данном способе получения токена можно использовать методы аутентификации, которые доступны пользователю.

В результате аутентификации будет получен аналогичный токен.



# Методы API



## Authenticator

getUserAuth, findByUserIds



## License

getAllLicenses, getCatalogObjectLicenses



## Logon

isAvailable, authenticate, getAvailableMethods, authenticateByWindowsToken



## Policy

get



## TemplateSession

createTemplate, openEnrollSession, openVerifySession, openIdentifySession, prepareTemplateData



## User

searchUserId



## UserCatalog

getObjects, searchUsers, searchGroups, searchContainers



## UserProfile

findLogonInfoByUser

# Authenticator

## ❗ ИНФОРМАЦИЯ

Пример функций на PowerShell: [ССЫЛКА](#)

## getUserAuth

Возвращает все обученные аутентификаторы пользователя по внутреннему идентификатору в Indeed Access Manager.

POST /api/v5/authenticator/getUserAuth

Объект запроса

```
{
  "Id": "00000000-0000-0000-0000-000000000000",
  "UserId": "string",
  "AccessToken": "string",
  "ApplicationId": "string"
}
```

в объекте запроса:

- **Id** — обязательный параметр. Внутренний идентификатор Indeed Access Manager.
- **UserId** — обязательный параметр. Внутренний идентификатор пользователя в Indeed Access Manager.
- **AccessToken** — обязательный параметр. Токен администратора, от имени которого выполняется запрос к API.
- **ApplicationId** — обязательный параметр. Строковый идентификатор модуля Indeed AM.

Объект ответа

```

{
  "AuthenticationCountLimit": 0,
  "CreatedOn": "2022-10-26T07:23:08.550Z",
  "Description": "string",
  "ExpirationDate": "2022-10-26T07:23:08.550Z",
  "Flags": 1,
  "Id": "00000000-0000-0000-0000-000000000000",
  "IsDisabled": true,
  "IsLocked": true,
  "ModeDeviceName": "string",
  "ModeId": "00000000-0000-0000-0000-000000000000",
  "ModeType": 0,
  "ModeTypeName": "string",
  "UserId": "string",
  "SerialNumber": "string",
  "Device": {
    "Id": "00000000-0000-0000-0000-000000000000",
    "AuthType": "00000000-0000-0000-0000-000000000000",
    "SerialNumber": "string",
    "RegistrationDate": "2022-10-26T07:23:08.550Z",
    "IsEnabled": true,
    "LastUserId": "string",
    "Comment": "string",
    "Model": "string"
  },
  "CreatedBy": "string"
}

```

## findByUserIds

Возвращает внутренний идентификатор пользователя в Indeed Access Manager.

POST /api/v5/authenticator/findByUserIds

#### Объект запроса

```
{  
  "UserId": "string",  
  "AccessToken": "string",  
  "ApplicationId": "string"  
}
```

В объекте запроса:

- **UserId** — обязательный параметр. Внутренний идентификатор пользователя в Indeed Access Manager.
- **AccessToken** — обязательный параметр. Токен администратора, от имени которого выполняется запрос к API.
- **ApplicationId** — обязательный параметр. Строковый идентификатор модуля Indeed AM.

#### Объект ответа

```
[  
  "00000000-0000-0000-0000-000000000000"  
]
```

# License

## getAllLicenses

Возвращает все зарегистрированные в Indeed Access Manager лицензии.

POST /api/v5/license/getAllLicenses

Объект запроса

```
{
  "AccessToken": "string",
  "ApplicationId": "string"
}
```

в объекте запроса:

- **AccessToken** — обязательный параметр. Токен администратора, от имени которого выполняется запрос к API.
- **ApplicationId** — обязательный параметр. Строковый идентификатор модуля Indeed AM.

Объект ответа

```
{
  "LicenseUid": "string",
  "InstanceId": "string",
  "Type": "string",
  "Amount": 0,
  "BeginDate": "2022-10-26T08:43:22.406Z",
  "EndDate": "2022-10-26T08:43:22.406Z",
  "Description": "string",
  "Issuer": "string",
  "IssuedTo": "string",
  "IssueDate": "2022-10-26T08:43:22.406Z",
  "Id": "00000000-0000-0000-0000-000000000000",
  "ControlValue": "string"
}
```

## getCatalogObjectLicenses

Возвращает зарегистрированные лицензии для конкретного объекта каталога.

POST /api/v5/license/getCatalogObjectLicenses

Объект запроса

```
{
  "ObjectId": "string",
  "AccessToken": "string",
  "ApplicationId": "string"
}
```

в объекте запроса:

- **ObjectId** — идентификатор каталога, для которого будут получены зарегистрированные лицензии.
- **AccessToken** — обязательный параметр. Токен администратора, от имени которого выполняется запрос к API.

- **ApplicationId** — обязательный параметр. Строковый идентификатор модуля Indeed AM.

Объект ответа

```
{
  "ApplicationId": "string",
  "CatalogObjectId": "string",
  "PolicyId": "00000000-0000-0000-0000-000000000000"
}
```

## getAcquiredLicenseCount

Возвращает количество используемых лицензий указанного типа в выбранной политике.

POST /api/v6/license/getAcquiredLicenseCount

Объект запроса

```
{
  "LicenseType": "string",
  "PolicyId": "00000000-0000-0000-0000-000000000000",
  "AccessToken": "string",
  "ApplicationId": "string"
}
```

в объекте запроса:

- **LicenseType** — тип **лицензии**.
- **PolicyId** — идентификатор политики. Идентификатор можно получить в URL-адресе политики в **Management Console** или с помощью метода **/api/v6/policy/getAll**.
- **AccessToken** — обязательный параметр. Токен администратора, от имени которого выполняется запрос к API.
- **ApplicationId** — обязательный параметр. Строковый идентификатор модуля Indeed AM.



|               |
|---------------|
| Объект ответа |
| "0"           |

# Logon

## ❗ ИНФОРМАЦИЯ

Пример функций на PowerShell: [ссылка](#)

## isAvailable

Выполняет проверку доступности аутентификации пользователя в приложении.

- В параметре `ApplicationId` указывается идентификатор приложения.
- В параметре `UserId` указывается идентификатор целевого пользователя.
- В параметре `ExcludeWindowsPassword` указывается *true/false*:
  - Если указано *true*, значит из проверки исключается возможность аутентификации по доменному паролю. В таком случае пользователю должен быть доступен любой другой метод аутентификации, иначе запрос вернет *false*.
  - Если указано *false*, доменный пароль не исключается из возможных способов аутентификации в сценарии.

[POST] /api/v5/logon/isAvailable

Объект запроса

```
{
  "ApplicationId": "string",
  "UserId": "string",
  "ExcludeWindowsPassword": true
}
```

в объекте запроса:

- `ApplicationId` — обязательный параметр. Строковый идентификатор модуля Indeed AM.
- `UserId` — обязательный параметр. Идентификатор пользователя в Indeed AM.

- `ExcludeWindowsPassword` — опциональный параметр. Значение по умолчанию *true*.

Объект ответа

`true\false`

## authenticate

Выполняет аутентификацию пользователя в приложении *BusinessApplication* по зарегистрированному шаблону *TemplateId*.

[POST] /api/v5/logon/authenticate

Объект запроса

```
{
  "TemplateId": "00000000-0000-0000-0000-000000000000",
  "BusinessApplication": "string"
}
```

Объект ответа

```
{
  "Token": "string",
  "LogonResult": {
    "Result": "string"
  },
  "UserId": "string"
}
```

Пример успешного объекта ответа

```
{
  "ValidPropertiesMask": 5,
  "Token": "eyJ0e----.eyJleH----",
  "LogonResult": {
    "ValidPropertiesMask": 0,
    "Result": null
  },
  "UserId": "UserId_b1cfaa29-6368-4c50-9868-06dbbe21fe23"
}
```

## getAvailableMethods

Возвращает массив доступных способов аутентификации для пользователя *UserId* в указанном в *ApplicationId* приложении.

[POST] /api/v5/logon/getAvailableMethods

Объект запроса

```
{
  "ApplicationId": "string",
  "UserId": "string",
  "IncludeModeIds": [
    "00000000-0000-0000-0000-000000000000"
  ],
  "ExcludeModeIds": [
    "00000000-0000-0000-0000-000000000000"
  ]
}
```

в объекте запроса:

- **ApplicationId** — обязательный параметр. Строковый идентификатор модуля Indeed AM.
- **UserId** — обязательный параметр. Идентификатор пользователя в Indeed AM.

- `IncludeModeIds` — опциональный параметр. GUID методов аутентификации Indeed, которые будут учитываться при проверке возможности аутентификации.
- `ExcludeModeIds` — опциональный параметр. GUID методов аутентификации Indeed, которые будут исключаться при проверке возможности аутентификации.

Объект ответа

```
{
  "AutheticationMethods": [
    "00000000-0000-0000-0000-000000000000"
  ]
}
```

#### ▼ Примеры ответов

Нет доступных методов

```
{
  "ValidPropertiesMask": 1,
  "AutheticationMethods": []
}
```

Доступен доменный пароль

```
{
  "ValidPropertiesMask": 1,
  "AutheticationMethods": [
    "cf189af5-01c5-469d-a859-a8f2f41ed153"
  ]
}
```

## authenticateByWindowsToken

Аутентификация пользователя с использованием токена сессии Windows. Токен передается в запрос посредством аутентификации Windows и билетов Kerberos.

[POST] /api/v5/logon/authenticateByWindowsToken

### Объект запроса

```
{
  "ApplicationId": "string",
  "BusinessApplication": "string"
}
```

в объекте запроса:

- **ApplicationId** — обязательный параметр. Строковый идентификатор модуля Indeed AM.
- **BusinessApplication** — опциональный параметр. Имя бизнес-приложения Indeed AM.

### Объект ответа

```
{
  "Token": "string",
  "LogonResult": {
    "Result": "string"
  },
  "UserId": "string"
}
```

### Пример успешного объекта ответа

```
{
  "ValidPropertiesMask": 5,
  "Token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJleHAiOj.....",
  "LogonResult": null,
  "UserId": "UserId_10efa04f-7ba9-47d8-89db-56e166f1679f"
}
```

# Policy

## ❗ ИНФОРМАЦИЯ

Пример функций на PowerShell: [ссылка](#)

## get

Возвращает информацию и настройки политик по идентификатору.

POST /api/v5/policy/get

Объект запроса

```
{
  "Id": "00000000-0000-0000-0000-000000000000",
  "AccessToken": "string",
  "ApplicationId": "string"
}
```

в объекте запроса:

- **Id** — обязательный параметр. Идентификатор политики.
- **AccessToken** — обязательный параметр. Токен администратора, от имени которого выполняется запрос к API.
- **ApplicationId** — обязательный параметр. Строковый идентификатор модуля Indeed AM.

Объект ответа



```
{
  "Id": "00000000-0000-0000-0000-000000000000",
  "Name": "string",
  "Description": "string",
  "Settings": \[
    {
      "Id": "00000000-0000-0000-0000-000000000000",
      "SettingType": 0,
      "Value": {},
      "ParentId": "00000000-0000-0000-0000-000000000000"
    }
  \],
  "CreatedById": "string",
  "CreatedTime": "2022-10-26T07:23:08.768Z",
  "LastEditedById": "string",
  "LastEditedTime": "2022-10-26T07:23:08.768Z"
}
```

в объекте ответа:

- **SettingType:**
  - 0 — область действия политики. Возвращается внутренний GUID объектов области действия.
  - 1 — приложения политики.
  - 2 — приоритет политики.

# TemplateSession

## ❗ ИНФОРМАЦИЯ

Пример функций на PowerShell: [ссылка](#)

## createTemplate

Создает шаблон для аутентификации по идентификатору открытой сессии.

```
[POST] /api/v5/templateSession/createTemplate
```

Объект запроса

```
{  
  "SessionId": "00000000-0000-0000-0000-000000000000"  
}
```

в объекте запроса:

- **SessionId** — обязательный параметр. Указывается GUID открытой сессии, полученный из метода **openVerifySession**.

Объект ответа

```
"00000000-0000-0000-0000-000000000000"
```

## openEnrollSession

```
[POST] /api/v5/templateSession/openEnrollSession
```

# openVerifySession

Открывает сессию для аутентификации пользователя, указанного в `UserSearchParams` в приложении `ApplicationId`, с использованием способа аутентификации `ModeId`.

[POST] /api/v5/templateSession/openVerifySession

Объект запроса

```
{
  "UserSearchParams": {
    "Id": "string",
    "Email": "string",
    "Phone": "string",
    "NameFormat": 0,
    "Name": "string",
    "ApplicationId": "string"
  },
  "ModeId": "00000000-0000-0000-0000-000000000000",
  "ApplicationId": "string"
}
```

в объекте запроса:

- `UserSearchParams` — массив параметров для поиска пользователя;
  - `Id` — внутренний идентификатор пользователя в Indeed AM;
  - `Email` — email пользователя из каталога Active Directory;
  - `Phone` — номер телефона пользователя из каталога Active Directory;
  - `NameFormat` — числовое значение формата имени, которое будет указано в `Name`.

Поддерживаются следующие форматы:

- 0 — Undefined;
- 1 — CanonicalName;
- 2 — PrincipalName: *name@domain.name*;
- 3 — SamCompatibleName: *domain\logon-name*;
- 4 — DistinguishedName;

- 5 — Sid;
- ModeId** — обязательный параметр. Строковый идентификатор используемого способа аутентификации.
- ApplicationId** — обязательный параметр. Строковый идентификатор модуля Indeed AM.

Объект ответа

GUID открытой сессии

"00000000-0000-0000-0000-000000000000"

## openIdentifySession

[POST] /api/v5/templateSession/openIdentifySession

## prepareTemplateData

Добавляет информацию о шаблоне пользователя.

[POST] /api/v5/templateSession/prepareTemplateData

Объект запроса

```
{
  "Data": {},
  "SessionId": "00000000-0000-0000-0000-000000000000"
}
```

в объекте запроса:

- Data** — аутентификационные данные пользователя (одноразовый код или пароль или другие данные в зависимости от используемого способа аутентификации);
- SessionId** — идентификатор открытой сессии, полученный в **openVerifySession**.

#### Объект ответа

```
{
  "EnoughData": true,
  "BinaryData": "string",
  "StringData": "string"
}
```

в объекте ответа:

- **EnoughData** — признак того, что данных от клиента для формирования шаблона достаточно.

#### Пример объекта ответа

```
{
  "ValidPropertiesMask": 1,
  "EnoughData": true,
  "BinaryData": null,
  "StringData": null
}
```

# User

## ❗ ИНФОРМАЦИЯ

Пример функций на PowerShell: [ССЫЛКА](#)

## searchUserId

Возвращает **UserId** по входным параметрам.

POST /api/v5/user/searchUserId

### Объект запроса

```
{
  "Id": "string",
  "Email": "string",
  "Phone": "string",
  "NameFormat": 0,
  "Name": "string",
  "ApplicationId": "string"
}
```

в объекте запроса:

- **NameFormat**:
  - 0 — Undefined,
  - 1 — CanonicalName,
  - 2 — PrincipalName,
  - 3 — SamCompatibleName,
  - 4 — DistinguishedName,
  - 5 — Sid.

### Объект ответа

"xxx\\_\\_0000000-0000-0000-0000-000000000000"

# UserCatalog

## ❗ ИНФОРМАЦИЯ

Пример функций на PowerShell: [ссылка](#)

## getObjects

Возвращает данные объекта каталога пользователя Indeed AM по внутреннему идентификатору.

POST /api/v5/userCatalog/getObjects

Объект запроса

```
{
  "Ids": [
    "string"
  ],
  "AccessToken": "string",
  "ApplicationId": "string"
}
```

в объекте запроса:

- **Ids** — массив внутренних идентификаторов.
- **AccessToken** — обязательный параметр. Токен администратора, от имени которого выполняется запрос к API.
- **ApplicationId** — обязательный параметр. Строковый идентификатор модуля Indeed AM.

Объект ответа



```
{
  "Id": "string",
  "RawObjectId": "string",
  "Name": "string",
  "CanonicalName": "string",
  "PrincipalName": "string",
  "SamCompatibleName": "string",
  "DistinguishedName": "string",
  "Sid": "string",
  "IsGroup": true,
  "IsContainer": true,
  "IsRemoved": true,
  "GroupsIds": [
    "string"
  ],
  "ContainerId": "string"
}
```

## searchUsers

Поиск пользователя по входным параметрам.

POST /api/v5/userCatalog/searchUsers

Объект запроса

```
{
  "Operation": 0,
  "Filters": [
    {
      "AttributeName": "string",
      "Value": {},
      "Negation": true
    }
  ],
  "Limit": 0,
  "LoadParentObjects": true,
  "AccessToken": "string",
  "ApplicationId": "string"
}
```

в объекте запроса:

- **Operation:**
  - 0 — ИЛИ;
  - 1 — И;
- **Filters** - массив фильтров для поиска:
  - **AttributeName** — имя атрибута Active Directory для поиска;
  - **Value** — значение атрибута Active Directory для поиска;
  - **Negation** — отрицание заданного фильтра. Значения *true/false*.

Объект ответа

```
[
  {
    "FirstName": "string",
    "MiddleName": "string",
    "LastName": "string",
    "Email": "string",
    "Phone": "string",
    "IsDisabled": true,
    "IsLocked": true,
    "Id": "string",
    "RawObjectId": "string",
    "Name": "string",
    "CanonicalName": "string",
    "PrincipalName": "string",
    "SamCompatibleName": "string",
    "DistinguishedName": "string",
    "Sid": "string",
    "IsGroup": true,
    "IsContainer": true,
    "IsRemoved": true,
    "GroupsIds": [
      "string"
    ],
    "ContainerId": "string"
  }
]
```

## searchGroups

Поиск группы по входным параметрам.

POST /api/v5/userCatalog/searchGroups

Объект запроса

```
{
  "Operation": 0,
  "Filters": [
    {
      "AttributeName": "string",
      "Value": {},
      "Negation": true
    }
  ],
  "Limit": 0,
  "LoadParentObjects": true,
  "AccessToken": "string",
  "ApplicationId": "string"
}
```

в объекте запроса:

- **Operation**:
  - 0 — ИЛИ;
  - 1 — И;
- **Filters** — массив фильтров для поиска:
  - **AttributeName** — имя атрибута Active Directory для поиска;
  - **Value** — значение атрибута Active Directory для поиска;
  - **Negation** — отрицание заданного фильтра. Значения *true/false*.

Объект ответа

```
[
  {
    "FirstName": "string",
    "MiddleName": "string",
    "LastName": "string",
    "Email": "string",
    "Phone": "string",
    "IsDisabled": true,
    "IsLocked": true,
    "Id": "string",
    "RawObjectId": "string",
    "Name": "string",
    "CanonicalName": "string",
    "PrincipalName": "string",
    "SamCompatibleName": "string",
    "DistinguishedName": "string",
    "Sid": "string",
    "IsGroup": true,
    "IsContainer": true,
    "IsRemoved": true,
    "GroupsIds": [
      "string"
    ],
    "ContainerId": "string"
  }
]
```

## searchContainers

Поиск подразделения по входным параметрам.

POST /api/v5/userCatalog/searchContainers

Объект запроса

```
{
  "Operation": 0,
  "Filters": [
    {
      "AttributeName": "string",
      "Value": {},
      "Negation": true
    }
  ],
  "Limit": 0,
  "LoadParentObjects": true,
  "AccessToken": "string",
  "ApplicationId": "string"
}
```

в объекте запроса:

- **Operation**:
  - 0 — ИЛИ;
  - 1 — И;
- **Filters** — массив фильтров для поиска:
  - **AttributeName** — имя атрибута Active Directory для поиска;
  - **Value** — значение атрибута Active Directory для поиска;
  - **Negation** — отрицание заданного фильтра. Значения *true/false*.

Объект ответа

```
[
  {
    "FirstName": "string",
    "MiddleName": "string",
    "LastName": "string",
    "Email": "string",
    "Phone": "string",
    "IsDisabled": true,
    "IsLocked": true,
    "Id": "string",
    "RawObjectId": "string",
    "Name": "string",
    "CanonicalName": "string",
    "PrincipalName": "string",
    "SamCompatibleName": "string",
    "DistinguishedName": "string",
    "Sid": "string",
    "IsGroup": true,
    "IsContainer": true,
    "IsRemoved": true,
    "GroupsIds": [
      "string"
    ],
    "ContainerId": "string"
  }
]
```

# UserProfile

## ❗ ИНФОРМАЦИЯ

Пример функций на PowerShell: [ССЫЛКА](#)

## findLogonInfoByUser

Возвращает информацию об аутентификациях пользователя.

POST /api/v5/userProfile/findLogonInfoByUser

### Объект запроса

```
{
  "UserId": "string",
  "AccessToken": "string",
  "ApplicationId": "string"
}
```

### Объект ответа

```
{
  "UserId": "xxxx\_000000-0000-0000-0000-000000000000",
  "ApplicationId": "Native Enroller",
  "LogonDate": "2022-05-04T10:54:05.821+03:00",
  "ModeId": "000000-0000-0000-0000-000000000000"
}
```

В объекте ответа:

- **UserId** — внутренний идентификатор пользователя;
- **ApplicationId** — идентификатор приложения, в которое был выполнен вход;
- **LogonDate** — дата и время входа;



- `ModeId` — идентификатор способа входа.

# Сценарии использования



## Создание отчетов

Создание отчетов



## Сбор статистики по обученным аутентификаторам пользователей

Сбор статистики по обученным аутентификаторам пользователей



## Получение списка пользователей с лицензиями

Получение списка пользователей с лицензиями



## Двухфакторная аутентификация в API

Настройка двухфакторной аутентификации через API



## Удаление пользователей из политики

Удаление пользователей из политики



## Получение списка пользователей из политики

Получение списка пользователей из политики

# Создание отчетов

## ❗ ИНФОРМАЦИЯ

Скрипт для создания отчетов вы можете скачать [по этой ссылке](#).

## Предварительные требования

- Установленный модуль Active Directory для PowerShell в Windows Server.
- Работоспособный сервер Indeed AM.
- Пользователь, от имени которого будет запускаться скрипт, должен обладать минимальными глобальными правами *Инспектор* в системе Indeed AM.

## Как работает скрипт

Скрипт формирует отчеты по подготовленным сценариям. Для создания отчетов используется API Indeed AM Core и Indeed AM Log Server.

Скрипт поддерживает настройку фильтрации для формирования отчета:

- выборка из контейнера пользовательского каталога,
- выборка по конкретному пользователю,
- выборка по дате.

## Фильтры

### Поле *Container*

Поле предназначено для выбора подразделений, в домене в которых будет выполняться поиск пользователей. Значение *Entire Catalog* означает, что выбран корневой каталог с каталогом пользователей, который используется сервером Indeed AM.

Поиск подразделений из пользовательского каталога выполняется с использованием метода `searchContainers` в соответствующей функции в файле *Base/AMAPI/UserCatalog.ps1*.

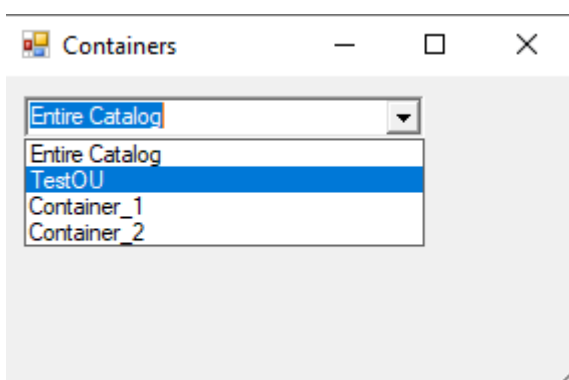
### ⓘ ПРИМЕЧАНИЕ

Выгрузка контейнеров выполняется из пользовательского каталога. Значение в поле не редактируемое.

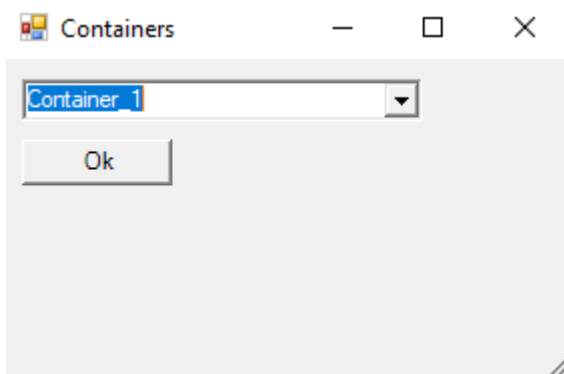
Имя корневых каталогов пользователей, заданных в конфигурационном файле Core Server, не отображается.

Для выбора необходимого подразделения из каталога выполните следующие действия:

1. Нажмите кнопку Select.



2. В выпадающем списке окна Containers выберите контейнер и нажмите Ok.



## Поле *Groups*

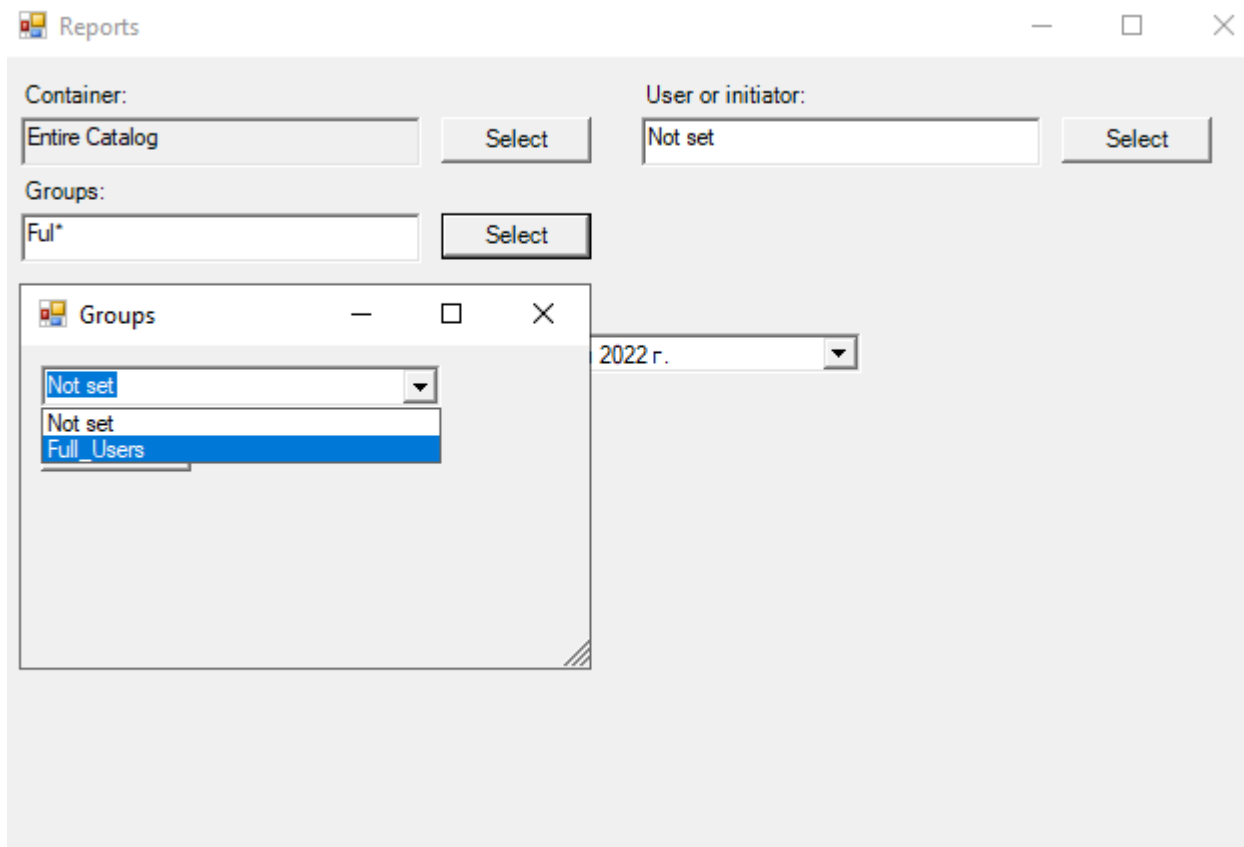
Поле предназначено для поиска групп в домене или в подразделении, которое было выбрано в поле *Container*. Значение по умолчанию *Not set*.

Поиск пользователя выполняется с использованием метода `searchGroups` в соответствующей функции в файле *Base/AMAPI/UserCatalog.ps1*.

Подготовка запроса с использованием заданных фильтров выполняется в функции `searchGropsUseFilters` в файле *Scenarios/Reports/SearchUseFilters.ps1*.

В поиске учитывается параметр Active Directory `Name`.

Для поиска группы при необходимости выберите контейнер и введите имя группы. Если данные не указаны, то будут найдены все группы из каталога пользователя.



### Поле *User or initiator*

Поле предназначено для поиска пользователя в домене; в подразделении, которое было выбрано в поле *Container*; группе из поля *Groups*. Значение по умолчанию *Not set*.

Поиск пользователя выполняется с использованием метода `searchUsers` в соответствующей функции в файле *Base/AMAPI/UserCatalog.ps1*.

Подготовка запроса с использованием заданных фильтров выполняется в функции `searchUsersUseFilters` в файле *Scenarios/Reports/SearchUseFilters.ps1*.

В поиске учитываются следующие параметры:

- **ContainerId** — идентификатор контейнера, в котором будет выполнен поиск пользователя. Параметр используется, если было выбрано подразделение в поле *Container*.
- **FirstName**, **MiddleName**, **LastName**, **PrincipalName**, **Name** — соответствующие значения атрибутов пользователя из Active Directory.

#### ⚠ ПРИМЕЧАНИЕ

Все параметры используются с логической операцией *OR*.

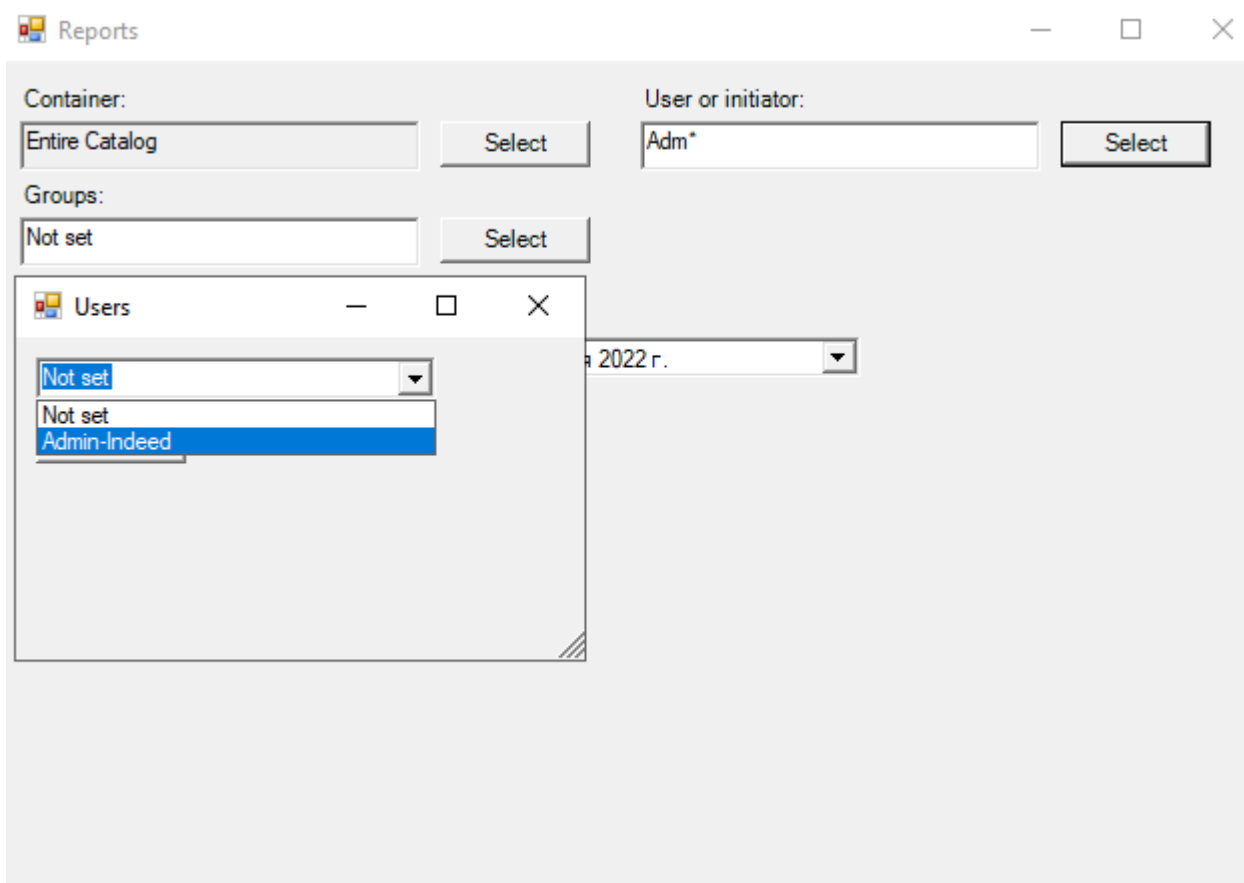
Для поиска пользователей можно нажать кнопку **Select** и выбрать всех найденных пользователей.

The screenshot shows the 'Reports' application window. It contains several input fields and buttons for searching users:

- Container:** A text box containing 'Entire Catalog' with a 'Select' button next to it.
- User or initiator:** A text box containing 'Not set' with a 'Select' button next to it.
- Groups:** A text box containing 'Not set' with a 'Select' button next to it.

Overlaid on the bottom left is a smaller 'Users' dialog box with a dropdown menu showing 'Not set' and an 'Ok' button. To the right of the dialog, a date dropdown menu shows 'я 2022 г.'.

Для поиска пользователя можно указать часть имени, в конце указанной части добавьте символ \*.



## Настройка

Для работы скрипта необходимо сконфигурировать файл *Config.ps1*, который находится в корне папки со скриптом.

### ВАЖНО!

В данном разделе описана общая настройка скрипта. Для отдельных отчетов может потребоваться дополнительная настройка.

В файле:

- `$domainName` — указывается имя домена. Обязательный параметр.
- `$eventsCount` — ограничение по выгрузке событий. Опциональный параметр. По умолчанию количество получаемых событий не ограничено, параметр закомментирован.
- `$serverUrl` — URL сервера Indeed AM. Обязательный параметр.
- `$logServerUrl` — URL Indeed AM Log Server. Обязательный параметр.
- `$logsOnFile` — включение\отключение логирования в файл. Обязательный параметр. По умолчанию включено.

- `$logsOnConsole` — включение\отключение логирования в консоль. Обязательный параметр. По умолчанию отключено.
- `$apiVersion` — версия API, используемая в скрипте. Обязательный параметр.

## Создание отчета с количеством аутентификаций по указанным провайдерам

В данном отчете формируется таблица с количеством аутентификаций пользователя по массиву аутентификаторов в конкретном приложении Indeed, указанному в файле *Config.ps1*.

Создание отчета выполняется в функции `createLogonsByProviderReport` в файле *Create-reports/Scenarios/Reports/CreateReports.ps1*.

## Настройка



### ВАЖНО!

В разделе описаны настройки для конкретного отчета. Перед началом работы необходимо выполнить базовую настройку, описанную в разделе [Настройка](#).

Для настройки откройте файл *Config.ps1* и выполните следующее:

1. В переменной `AuthForReport` задайте идентификатор провайдера Indeed и наименование для отчета:
  - Значения должны задаваться в формате *GUID провайдера Indeed=Наименование для отчета*.
  - Значения GUID провайдеров можно найти в разделе [Идентификаторы способов аутентификации](#).
  - Наименование для отчета может быть произвольным. Данное наименование будет использовано при создании таблицы.

Пример настройки с доменным паролем и отпечатком пальца



```
$AuthForReport          = @{  
    'CF189AF5-01C5-469D-A859-A8F2F41ED153' = 'Пароль'  
    'A0EF00AD-1EEB-4D48-8BCF-06E19CD5585F' = 'Отпечаток пальца'  
}
```

2. В переменной `ApplicationId` указывается наименование модуля интеграции Indeed. Список модулей можно найти в разделе [Идентификаторы приложений](#).

Пример настройки для приложения Windows Logon

```
$ApplicationId="Windows Logon"
```

3. Вы можете указать, в каком формате будет выгружаться отчет. Поддерживаются форматы CSV и HTML. Можно выгружать отчет в двух форматах одновременно. Если обе переменные не определены, это приведет к ошибке выгрузки.

Чтобы отчет выгружался в CSV, задайте переменной `CsvReport` значение *true*.

```
$CsvReport = 'true'
```

Чтобы отчет выгружался в HTML задайте переменной `HtmlReport` значение *true*.

```
$HtmlReport = 'true'
```

4. В переменной `pathReportLogonsByProvider` указывается путь до папки, где будет сохранен отчет. По умолчанию используется корень папки со скриптом.

```
$pathReportLogonsByProvider="$ScriptDirectory\Reports\LogonsByProvider"
```

## Пример работы

1. Для начала работы со скриптом откройте оснастку PowerShell, перейдите в папку со скриптом и запустите файл *Start.ps1* через команду `.\Start.ps1`.

2. При необходимости настройте фильтры скрипта и нажмите кнопку Report of number of logins by providers.
3. После завершения работы скрипта будет сформирована таблица формата HTML по указанному при настройке пути.

| Имя пользователя                | Приложение    | Дата и время последнего входа                                | Палец | Пароль |
|---------------------------------|---------------|--------------------------------------------------------------|-------|--------|
| who_i@indeed.local              | Windows Logon | 22.09.2022 14:11:03                                          | 0     | 0      |
| Ivan_I@indeed.local             | Windows Logon | 22.09.2022 14:13:06                                          | 0     | 0      |
| vf-adm@indeed.local             | Windows Logon | 28.09.2022 11:21:16                                          | 2     | 1      |
| ii@indeed.local                 | Windows Logon | The user:ii@indeed.local is not logged in to any application | 0     | 0      |
| vf@indeed.local                 | Windows Logon | The user:vf@indeed.local is not logged in to any application | 0     | 0      |
| rdp@indeed.local                | Windows Logon | 06.05.2022 14:31:41                                          | 0     | 0      |
| Admin-Indeed@indeed.local       | Windows Logon | 28.09.2022 11:09:44                                          | 1     | 1      |
| Number of users: 7              |               |                                                              |       |        |
| Number of logons by 'Палец': 3  |               |                                                              |       |        |
| Number of logons by 'Пароль': 2 |               |                                                              |       |        |

# Сбор статистики по обученным аутентификаторам пользователей

## ❗ ИНФОРМАЦИЯ

Скрипт для сбора статистики вы можете скачать [по этой ссылке](#).

## Предварительные требования

- Установленный модуль Active Directory для PowerShell в Windows Server.
- Работоспособный сервер Indeed AM.
- Пользователь, от имени которого будет запускаться скрипт, должен обладать минимальными глобальными правами *Инспектор* в системе Indeed AM.

## Как работает скрипт

Работа скрипта состоит из нескольких этапов:

1. Скрипт перебирает идентификаторы политик из массива конфигурационного файла *Config.ps1*.
2. С помощью метода `/api/v5/policy/get` запрашивается информация о политике.
3. Из свойства области действия запрашивается информация по настроенным объектам с помощью метода `/api/v5/userCatalog/getObjects`.
4. Из полученных объектов запрашиваются пользователи:
  - С помощью командлета PowerShell `Get-ADGroup` в функции `getUsersCN` файла *Base/AdditionalFunctions/GetUsers.ps1* для группы Active Directory.
  - С помощью командлета PowerShell `Get-ADUser` в функции `getUsersOU` файла *Base/AdditionalFunctions/GetUsers.ps1* для подразделения Active Directory.
5. По полученным пользователям составляется отчет по состоянию аутентификаторов, которые указаны в переменной `AuthForReport` файла *Config.ps1*.
  - С помощью метода `/api/v5/authenticator/findByUserIds` запрашивается информация со всеми внутренними GUID аутентификаторов пользователя.
  - С помощью метода `/api/v5/authenticator/getUserAuth` запрашивается информация по конкретному GUID.

6. С помощью функции `addDataToCSV` файла *Base/AdditionalFunctions/CsvReport.ps1* собирается таблица в формате CSV.

## Настройка

Для работы скрипта необходимо сконфигурировать файл *Config.ps1*, который находится в корне папки со скриптом.

В файле:

- `$serverUrl` — URL сервера Indeed AM. Обязательный параметр.
- `$logsOnFile` — включение\отключение логирования в файл. Обязательный параметр. По умолчанию включено.
- `$logsOnConsole` — включение\отключение логирования в консоль. Обязательный параметр. По умолчанию отключено.
- `$apiVersion` — версия API, используемая в скрипте. Обязательный параметр. Значение по умолчанию: v5.
- `$policyIds` — идентификаторы политик, из области действия которых запрашиваются пользователи.
- `$AuthForReport` — в переменной указываются GUID аутентификаторов Indeed и их название для отчета. Название может быть произвольным. Значения указываются в следующем формате: `'GUID' = "Наименование"`.

Пример настройки для Indeed Key и Passcode

```
$AuthForReport      = @{  
    'F696F05D-5466-42b4-BF52-21BEE1CB9529' = 'Passcode'  
    'DEEF0CB8-AD2F-4B89-964A-B6C7ECA80C68' = 'Push-уведомление в  
Indeed Key'  
}
```

- `$csvPathToReport` — путь до CSV-файла отчета. По умолчанию файл создается в папке скрипта по пути *Reports\Statistics*.

## Пример работы

1. Для запуска скрипта запустите файл *main.ps1*.
2. В процессе работы скрипта по пути из переменной `$csvPathToReport` будет создан файл формата CSV.



### ПРИМЕЧАНИЕ

Пользователи добавляются в отчет последовательно.

```
26.10.2022_9.39.csv 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
```

# Получение списка пользователей с лицензиями

## ❗ ИНФОРМАЦИЯ

Скрипт для получения списка пользователей вы можете скачать [по этой ссылке](#).

## Предварительные требования

- Установленный модуль Active Directory для PowerShell в Windows Server.
- Работоспособный сервер Indeed AM.
- Пользователь, от имени которого будет запускаться скрипт, должен обладать минимальными глобальными правами *Инспектор* в системе Indeed AM.

## Как работает скрипт

Скрипт формирует таблицу формата CSV со следующими столбцами:

- <UserName>,
- <true>,
- <false>,

где *true/false* — это столбцы с соответствующим названием лицензии.

Массив лицензий, наличие которых проверяется у пользователя, — это список всех зарегистрированных лицензий.

Работа скрипта состоит из нескольких этапов:

1. Формируется массив загруженных в систему лицензий с помощью метода `/license/getAllLicenses`.
2. С помощью метода `/api/v5/policy/get` запрашивается информация о политике.
3. Из свойства области действия запрашивается информация по настроенным объектам с помощью метода `/api/v5/userCatalog/getObjects`.
4. Из полученных объектов запрашиваются пользователи:

- С помощью командлета PowerShell `Get-ADGroup` в функции `getUsersCN` файла *Base/AdditionalFunctions/GetUsers.ps1* для группы Active Directory.
  - С помощью командлета PowerShell `Get-ADUser` в функции `getUsersOU` файла *Base/AdditionalFunctions/GetUsers.ps1* для подразделения Active Directory.
5. С помощью метода `license/getCatalogObjectLicenses` запрашивается наличие лицензий пользователя и сопоставляется с общим массивом лицензий.
  6. С помощью функции `addDataToCSV` файла *Base/AdditionalFunctions/CsvReport.ps1* собирается таблица в формате CSV.

## Настройка

Для работы скрипта необходимо сконфигурировать файл *Config.ps1*, который находится в корне папки со скриптом.

В файле:

- `$serverUrl` — URL сервера Indeed AM. Обязательный параметр.
- `$logsOnFile` — включение\отключение логирования в файл. Обязательный параметр. По умолчанию включено.
- `$logsOnConsole` — включение\отключение логирования в консоль. Обязательный параметр. По умолчанию отключено.
- `$apiVersion` — версия API, используемая в скрипте. Обязательный параметр. Значение по умолчанию: v5.
- `$policyIds` — идентификаторы политик, из области действия которых запрашиваются пользователи.
- `$csvPathToReport` — путь до CSV-файла отчета. По умолчанию файл создается в папке скрипта по пути *Reports\Statistics*.

## Пример работы

1. Для запуска скрипта запустите файл *main.ps1*.
2. В процессе работы скрипта по пути из переменной `$csvPathToReport` будет создан файл формата CSV.

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;Authentication_API;
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;

```



# Двухфакторная аутентификация в API

## ❗ ИНФОРМАЦИЯ

Скрипт для выполнения двухфакторной аутентификации через API вы можете скачать [по этой ссылке](#).

## Как работает скрипт

Скрипт выполняет аутентификацию через стандартное API Core Server. В качестве провайдеров аутентификации поддерживаются провайдеры с одноразовым паролем, Passcode, Windows Password.

Чтобы выполнить аутентификацию через API, выполните следующее:

1. Вызовите метод `/api/v5/templateSession/openVerifySession`. При успешном выполнении метода вернется идентификатор сессии — переменная `$SessionId` в скрипте.

## ❗ ПРИМЕЧАНИЕ

В качестве примера в скрипте используется формат имени *PrincipalName*.

2. Следующие шаги отличаются в зависимости от используемого провайдера аутентификации:

### Если одноразовый код известен

Если одноразовый код известен и его не нужно отправлять, то аутентификация выполняется по следующему алгоритму (функция `SimpleLogon` в скрипте):

1. Запрашивается ввод одноразового кода.
2. Подготовка шаблона аутентификации — вызывается метод `/api/v5/templateSession/prepareTemplateData`.

В качестве `Data` строкой передается одноразовый код (строка №12 в скрипте). Если подготовка прошла успешно, то создается шаблон, вызывается метод `/api/v5/templateSession/createTemplate`.

Завершающий шаг — это аутентификация пользователя с помощью метода `/api/v5/logon/authenticate`.

При успешной аутентификации возвращается токен в формате JSON.

#### Если одноразовый код не известен

Если одноразовый код не известен, то сначала нужно инициировать его отправку с помощью функции `'LogonByOtp'` в скрипте.

1. Вызовите метод `/api/v5/templateSession/prepareTemplateData`.

Первоначально в качестве `Data` передается значение *Null*.

Первый вызов необходим для того, чтобы сервер выполнил отправку одноразового кода, например отправку СМС. Также при первоначальном запросе значение параметра `EnoughData` будет содержать *false*.

2. Запрашивается ввод одноразового кода.

3. Подготовка шаблона аутентификации — вызывается метод

`/api/v5/templateSession/prepareTemplateData`.

В качестве `Data` строкой передается одноразовый код (строка №12 в скрипте). Запрос вернет объект, где значение параметра `EnoughData` будет содержать *true*. Если подготовка прошла успешно, то создается шаблон, вызывается метод `/api/v5/templateSession/createTemplate`.

Завершающий шаг — это аутентификация пользователя с помощью метода `/api/v5/logon/authenticate`. При успешной аутентификации возвращается токен в формате JSON.



# Удаление пользователей из политики

## ❗ ИНФОРМАЦИЯ

Скрипт для сбора статистики вы можете скачать [по этой ссылке](#).

## Предварительные требования

- Работоспособный сервер Indeed AM.
- Наличие **лицензии Authentication API**.

## Как работает скрипт

Скрипт удаляет пользователя из указанной политики, используя стандартное API Indeed AM Core.

## Настройка

| Параметр        | За что отвечает                            | Требование            | Настройки по умолчанию     |
|-----------------|--------------------------------------------|-----------------------|----------------------------|
| \$serverUrl     | Содержит URL сервера Indeed AM             | Обязательный параметр | Отсутствуют                |
| \$logsOnFile    | Включение\отключение логирования в файл    | Обязательный параметр | По умолчанию включено      |
| \$logsOnConsole | Включение\отключение логирования в консоль | Обязательный параметр | По умолчанию отключено     |
| \$apiVersion    | Версия API, используемая в скрипте         | Обязательный параметр | Значение по умолчанию — v6 |

## Пример работы

1. Запустите скрипт *main.ps1*.
2. Введите имя пользователя в формате *UPN*. Сформируется список номеров всех политик, в которые входит пользователь.
3. Введите номера политик, из которых вы хотите удалить пользователя, через запятую (или укажите только одну политику).

### Пример

```
Enter UPN: Admin-Indeed@indeed.local
User is in scope of the following policies:
0. Radius
1. Main
2. WL + ESS0
Choose policies to remove user from (e.g. 0,1,2): 0,2
User successfully removed from Radius
User successfully removed from WL + ESS0
```

# Получение списка пользователей из политики

## ❗ ИНФОРМАЦИЯ

Скрипт для получения списка пользователей из политики Indeed вы можете скачать [по этой ссылке](#).

## Предварительные требования

- Установленный модуль Active Directory для PowerShell в Windows Server.
- Работоспособный сервер Indeed AM.
- Пользователь, от имени которого будет запускаться скрипт, должен обладать **минимальными глобальными правами Инспектор**.

## Как работает скрипт

Скрипт выгружает список пользователей из указанной политики в формате CSV. Выгружаются атрибуты пользователя *UserPrincipalName* и *displayName*.

1. Скрипт перебирает идентификаторы политик из массива конфигурационного файла *Config.ps1*.
2. С помощью метода `/api/v5/policy/get` запрашивается информация о политике.
3. Из свойства области действия запрашивается информация по настроенным объектам с помощью метода `/api/v5/userCatalog/getObjects`.
4. Из полученных объектов запрашиваются пользователи:
  - С помощью командлета `Get-ADGroup` в функции `getUsersCN` файла *Base/AdditionalFunctions/GetUsers.ps1* для группы Active Directory.
  - С помощью командлета `Get-ADUser` в функции `getUsersOU` файла *Base/AdditionalFunctions/GetUsers.ps1* для подразделения Active Directory.
  - С помощью командлета `Get-ADUser` в функции `getADUser` файла *Base/AdditionalFunctions/GetUsers.ps1* для пользователя Active Directory.
5. С помощью функции `addDataForUserInPolicyReportCsv` файла *Scenarios/Reports/CsvReport.ps1* собирается таблица в формате CSV.

## Настройка

1. В файле *Config.ps1* в переменной `$serverUrl` укажите адрес Indeed AM сервера в формате `https://indeedam.indeed.local/`.
2. В переменной `$logServerUrl` укажите адрес Log Server в формате `https://indeedam.indeed.local/`.
3. В переменной `$policyIds` укажите идентификатор целевой политики в формате `@('2fc7eeec-5adf-4a50-bad3-ba04585c76cd')`. Можно указать несколько через запятую `@('2fc7eeec-5adf-4a50-bad3-ba04585c76cd','7436daa7-abf7-437b-991f-0e89cc9f1b9b')`.



### СОВЕТ

Вы можете найти идентификатор политики в Management Console. Откройте нужную политику, идентификатор содержится в адресной строке браузера в переменной `policyId`.

Файл с выгруженными пользователями сохраняется в каталоге `$ScriptDirectory\Reports\UserInPolicyReport`. Если вы хотите сохранить файл в другом месте, укажите путь в переменной `$pathReportUserInPolicyReport` в файле *Config.ps1*.

Чтобы запустить скрипт, выполните файл *Start.ps1* с помощью PowerShell.

# Миграция с Indeed AM 7.x на Indeed AM 8.x



## Подготовка к миграции

Подготовка к миграции



## Миграция MS SQL

Миграция MS SQL



## Миграция хранилища Active Directory

Миграция хранилища Active Directory



# Подготовка к миграции

Перед началом процедуры миграции и/или обновления, требуется выполнить следующие действия:

## Расшифровка файлов конфигурации

- Расшифровка конфигурационного файла `easerver`  
(`C:\inetpub\wwwroot\easerver\Web.config`);
- Расшифровка конфигурационного файла  
`airkeycloud` (`C:\inetpub\wwwroot\airkeycloud\Web.config`);
- Расшифровка конфигурационных файлов `ils`  
(`C:\inetpub\wwwroot\ils\targetConfigs\sampleDb.config` и  
`C:\inetpub\wwwroot\ils\targetConfigs\akcSqlTarget.config`).

## Резервное копирование конфигурационных файлов

- `easerver` (`C:\inetpub\wwwroot\easerver\Web.config`);
- `airkeycloud` (`C:\inetpub\wwwroot\airkeycloud\Web.config`);
- `iidemc` (`C:\inetpub\wwwroot\iidemc\Web.config`);
- `iidsamlidp` (`C:\inetpub\wwwroot\iidsamlidp\Web.config` и  
`C:\inetpub\wwwroot\iidsamlidp\saml.config`);
- `iidselfservice` (`C:\inetpub\wwwroot\iidselfservice\Web.config`);
- `ils` (`C:\inetpub\wwwroot\ils\clientApps.config` и  
каталога `C:\inetpub\wwwroot\ils\targetConfigs\`)

## Резервное копирование веток реестра

- Настроек модулей интеграции Indeed ветка реестра

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID]
```

- Политик модулей и провайдеров Indeed ветка реестра

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Indeed-ID]

## Резервное копирование баз данных

- Полная резервная копия базы данных хранилища Indeed AM 7.x;
- Полная резервная копия базы данных Indeed AM AirKey Cloud Server;
- Полная резервная копия базы данных логов Indeed AM 7.x;
- 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 инстансов должны совпадать.

## ИНФОРМАЦИЯ

Используется штатный набор инструментов SQL Server (SSMS).

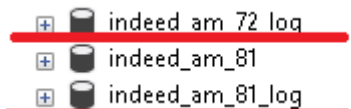
Миграция осуществляется по шагам, интерактивно, прозрачно для DBA.

Используется инструментарий экспорта данных БД Export Wizard.

## Миграция базы данных логов системы Indeed AM 7.x

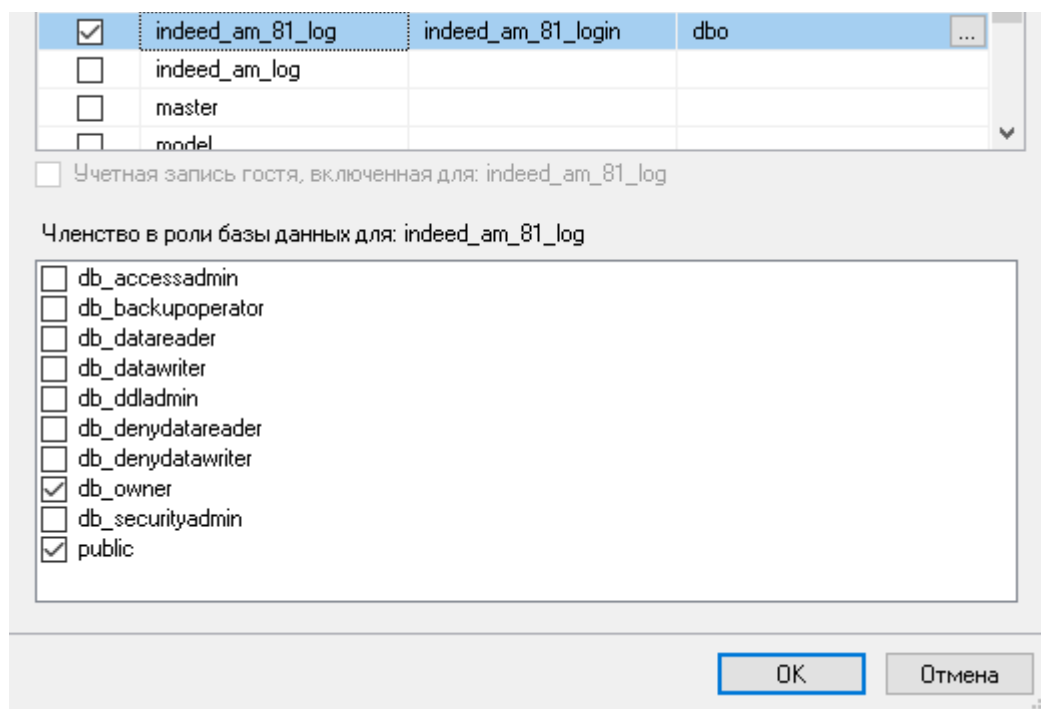
Скопируйте базу данных логов системы с новым именем (например: *indeed\_am\_81\_log*) одним из следующих способов:

- Через Мастер копирования базы данных. Подробнее можно узнать [в статье Microsoft](#).
- Через копирование баз данных путем создания и восстановления резервных копий. Подробнее можно узнать [в статье Microsoft](#).
- Через Мастер импорта и экспорта данных SQL Server. Подробнее можно узнать [в статье Microsoft](#).



indeed am 72 log  
indeed\_am\_81  
indeed\_am\_81\_log

По завершении копирования укажите для новой БД логин сервера MS SQL с правами владельца.

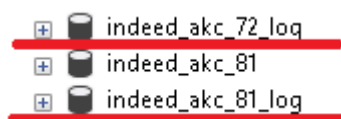


Далее при настройке Log server для Indeed AM 8.1 для событий системы укажите данную БД (например, *indeed\_am\_81\_log*) и учетную запись сервера MS SQL.

## Миграция базы данных логов AM AirKey Cloud Server версии 7.x

Скопируйте базу данных логов AM AirKey Cloud Server с новым именем (например, *indeed\_akc\_81\_log*) одним из следующих способов:

- Через Мастер копирования базы данных. Подробнее можно узнать [в статье Microsoft](#).
- Через копирование баз данных путем создания и восстановления резервных копий. Подробнее можно узнать [в статье Microsoft](#).
- Через мастер импорта и экспорта данных SQL Server. Подробнее можно узнать [в статье Microsoft](#).



По завершении копирования укажите для новой БД логин сервера MS SQL с правами владельца.

|                                     |                   |                     |     |     |
|-------------------------------------|-------------------|---------------------|-----|-----|
| <input checked="" type="checkbox"/> | indeed_akc_81_log | indeed_akc_81_login | dbo | ... |
| <input type="checkbox"/>            | indeed_akc_log    |                     |     |     |
| <input type="checkbox"/>            | indeed_am         |                     |     |     |
| <input type="checkbox"/>            | indeed_am_72      |                     |     |     |
| <input type="checkbox"/>            | indeed_am_72_log  |                     |     |     |
| <input type="checkbox"/>            | indeed_am_81      |                     |     |     |
| <input type="checkbox"/>            | indeed_am_81_log  |                     |     |     |
| <input type="checkbox"/>            | indeed_am_log     |                     |     |     |
| <input type="checkbox"/>            | master            |                     |     |     |
| <input type="checkbox"/>            | model             |                     |     |     |

☐ Учетная запись гостя, включенная для: indeed\_akc\_81\_log

Членство в роли базы данных для: indeed\_akc\_81\_log

|                                     |                   |
|-------------------------------------|-------------------|
| <input type="checkbox"/>            | db_accessadmin    |
| <input type="checkbox"/>            | db_backupoperator |
| <input type="checkbox"/>            | db_datareader     |
| <input type="checkbox"/>            | db_datawriter     |
| <input type="checkbox"/>            | db_ddladmin       |
| <input type="checkbox"/>            | db_denydatareader |
| <input type="checkbox"/>            | db_denydatawriter |
| <input checked="" type="checkbox"/> | db_owner          |
| <input type="checkbox"/>            | db_securityadmin  |
| <input checked="" type="checkbox"/> | public            |

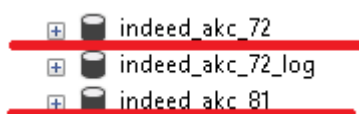
OK Отмена

Далее при настройке Log Server для Indeed AM 8.1 для AM Key Server укажите данную БД (например, *indeed\_akc\_81\_log*) и учетную запись сервера MS SQL Indeed Key Server.

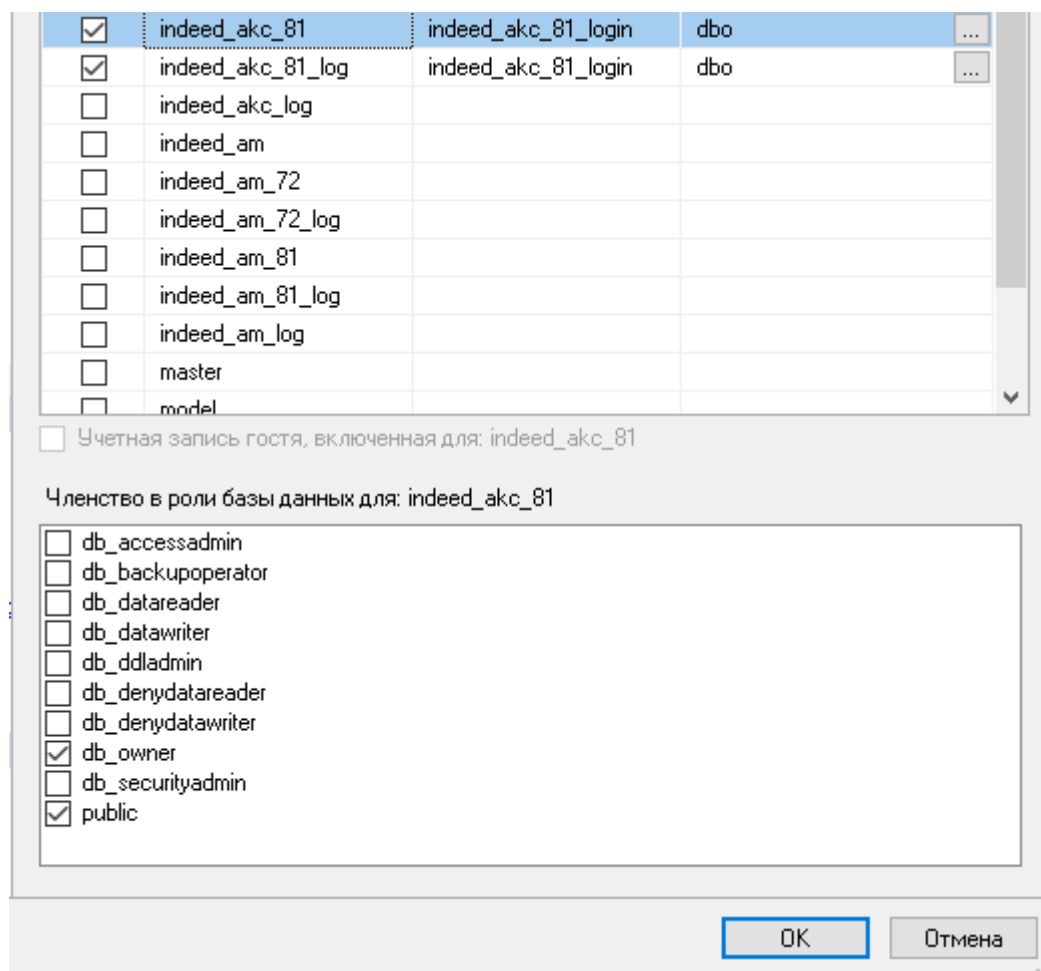
## Миграция базы данных хранилища Key Server версии 7.x

Скопируйте базу данных логов Key Server с новым именем (например, *indeed\_akc\_81*) одним из следующих способов:

- Через Мастер копирования базы данных. Подробнее можно узнать [в статье Microsoft](#).
- Через копирование баз данных путем создания и восстановления резервных копий. Подробнее можно узнать [в статье Microsoft](#).
- Через Мастер импорта и экспорта данных SQL Server. Подробнее можно узнать [в статье Microsoft](#).



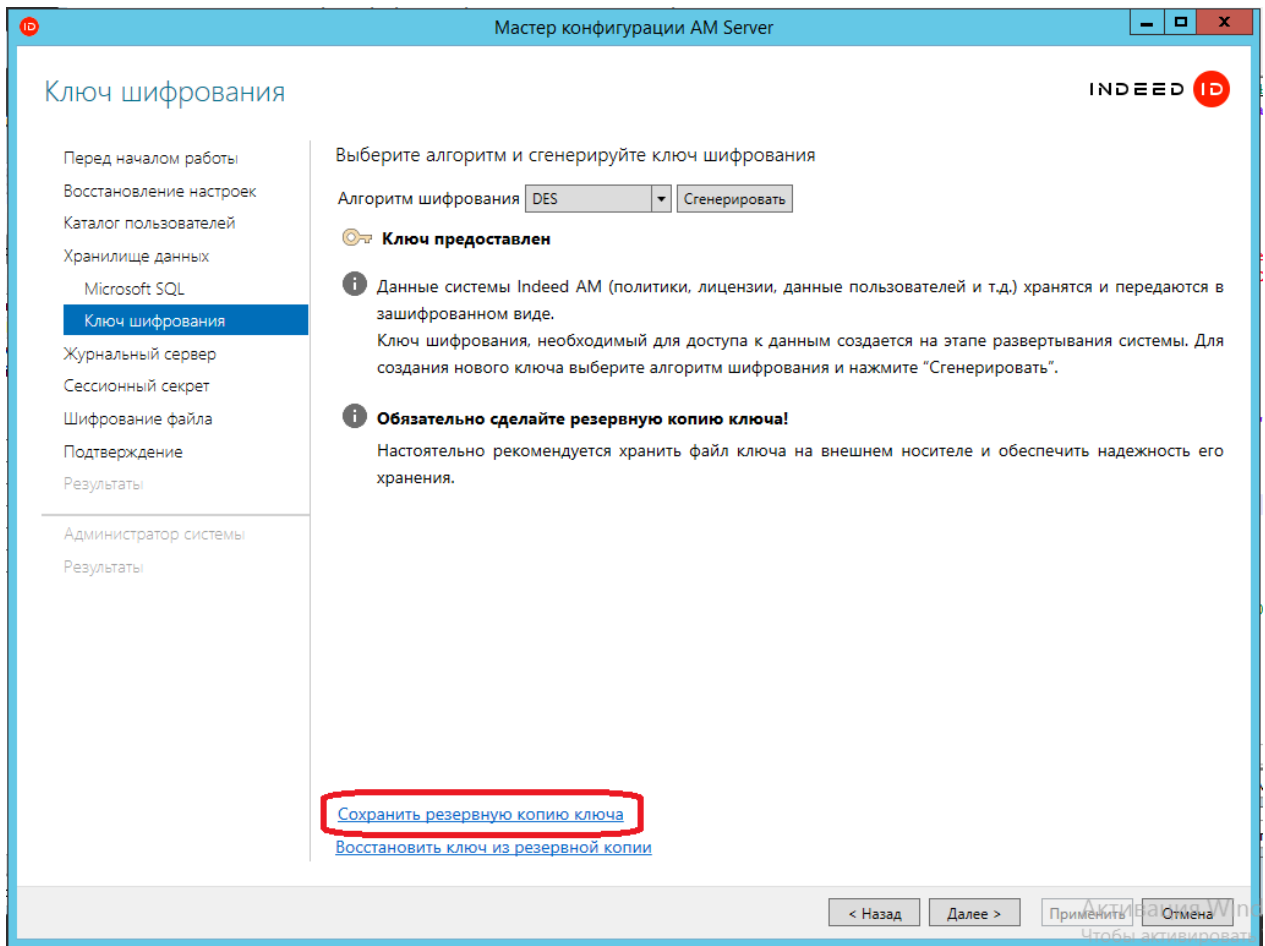
По завершении копирования укажите для новой БД логин сервера MS SQL с правами владельца.



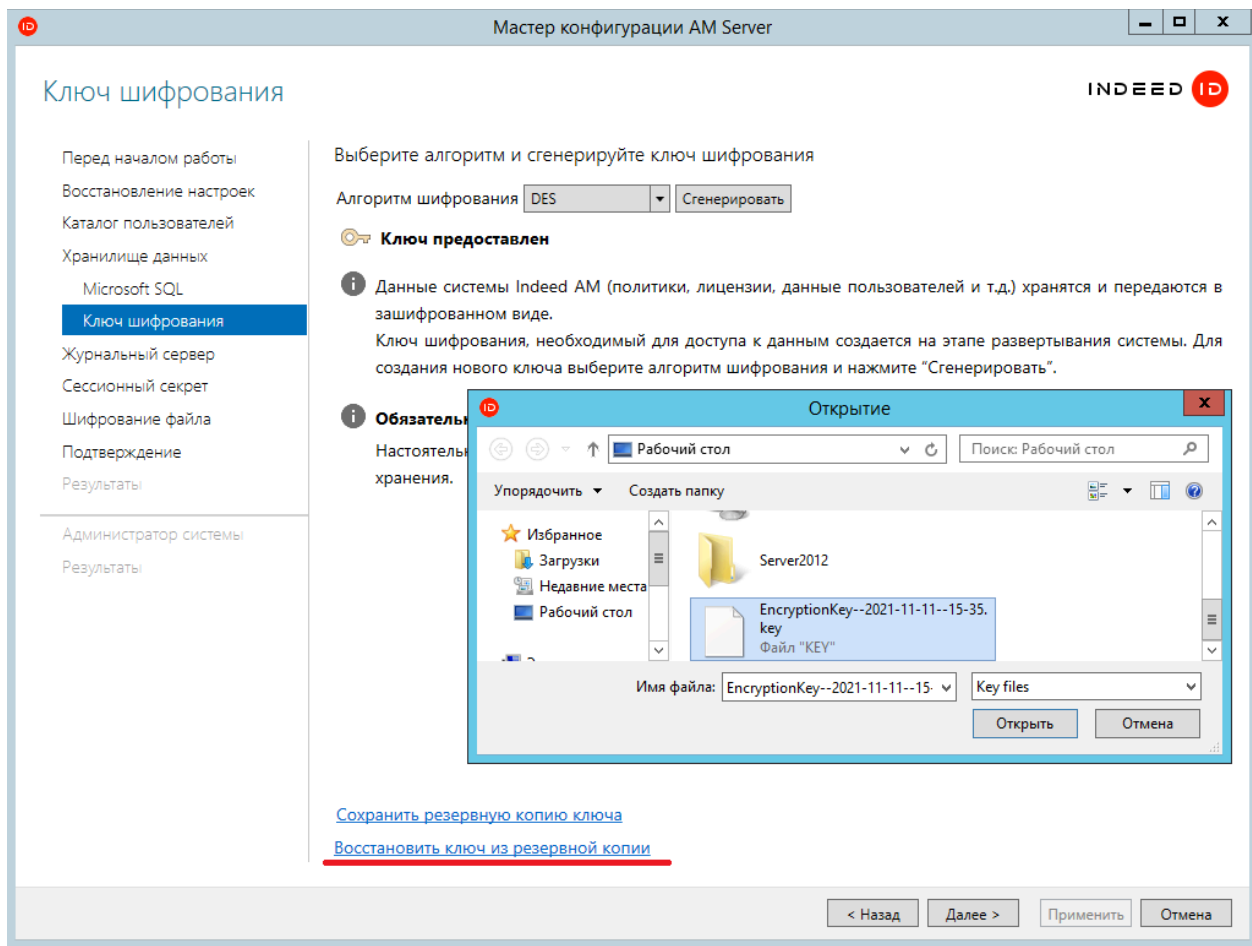
Далее при настройке Log Server для Indeed AM 8.1 для Key Server укажите данную БД (например, *indeed\_akc\_81*) и учетную запись сервера MS SQL.

## Подготовка базы данных хранилища Indeed AM 8.1

1. Запустите Мастер конфигурации на сервере Indeed AM 7.x.
2. Пройдите в нем 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, при создании используйте полученный ключ шифрования с Indeed AM 7.x



6. Остановите сервер IIS с Indeed AM server 8.1.

## Миграция базы данных хранилища Indeed AM 7.x

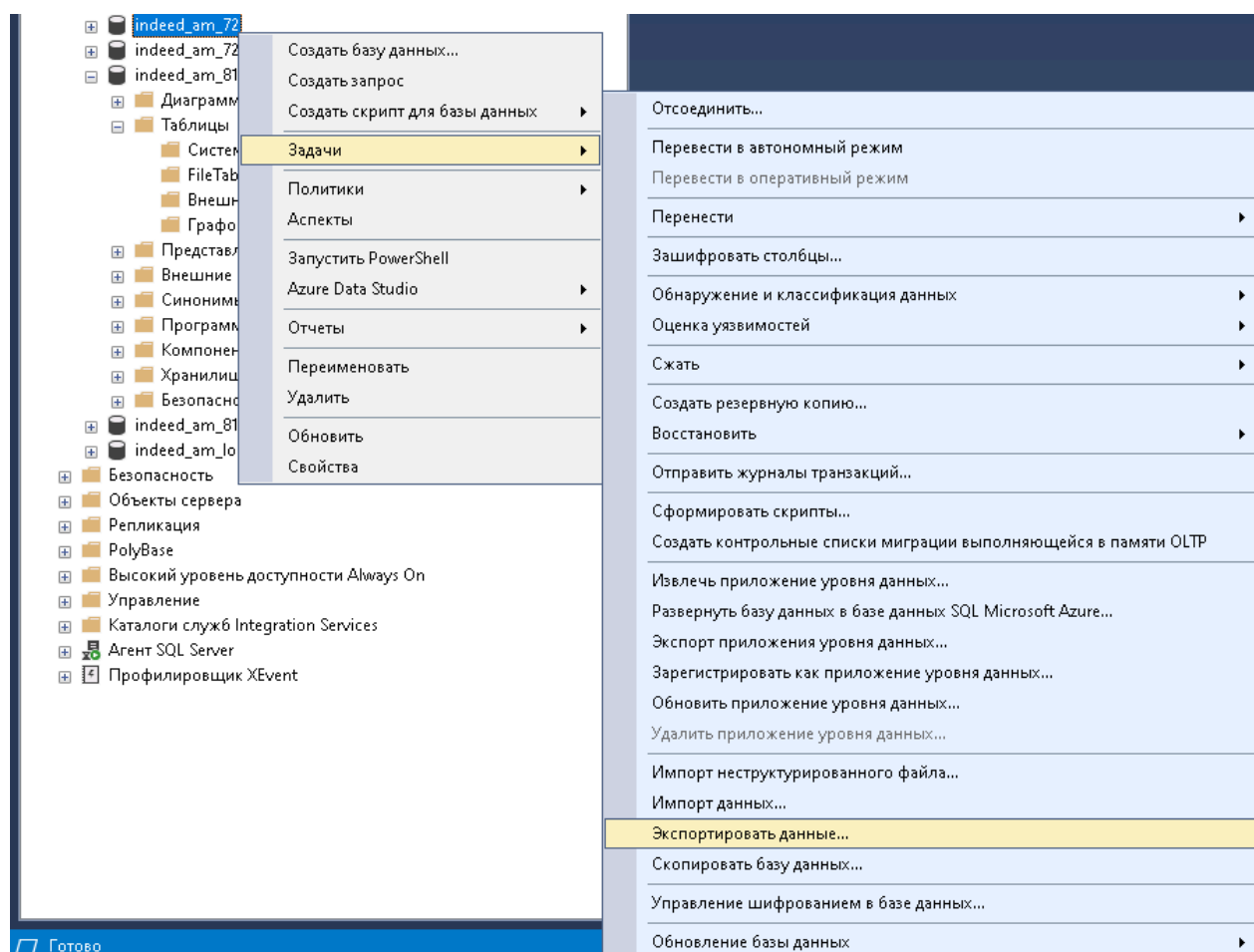
Список таблиц для миграции:

- DbInstanceProperties;
- DbLicenses;
- DbUserAuthenticators;
- DbHardwareDevices;
- DbHardwareDeviceProperties.

Все шаги повторяются для каждой мигрируемой таблицы.

1. Запустите экспорт данных БД Export Wizard.





2. Выберите источник данных — базу данных хранилища 7.x.

Мастер импорта и экспорта SQL Server

### Выбор источника данных

Выберите источник, из которого необходимо скопировать данные.

Источник данных: SQL Server Native Client 11.0

Имя сервера: 192.168.88.35

Проверка подлинности

☐ Использовать проверку подлинности Windows

☒ Использовать проверку подлинности SQL Server

Имя пользователя: sa

Пароль: xxxxxxxx

База данных: indeed\_am\_72 Обновить

Help < Back Next > Finish >> Cancel

3. Выберите приемник — базу данных хранилища 8.1.

Мастер импорта и экспорта SQL Server

**Выбор назначения**  
Укажите, куда копировать данные.

Назначение: SQL Server Native Client 11.0

Имя сервера: 192.168.88.35

Проверка подлинности

☐ Использовать проверку подлинности Windows

☒ Использовать проверку подлинности SQL Server

Имя пользователя: sa

Пароль: xxxxxxxx

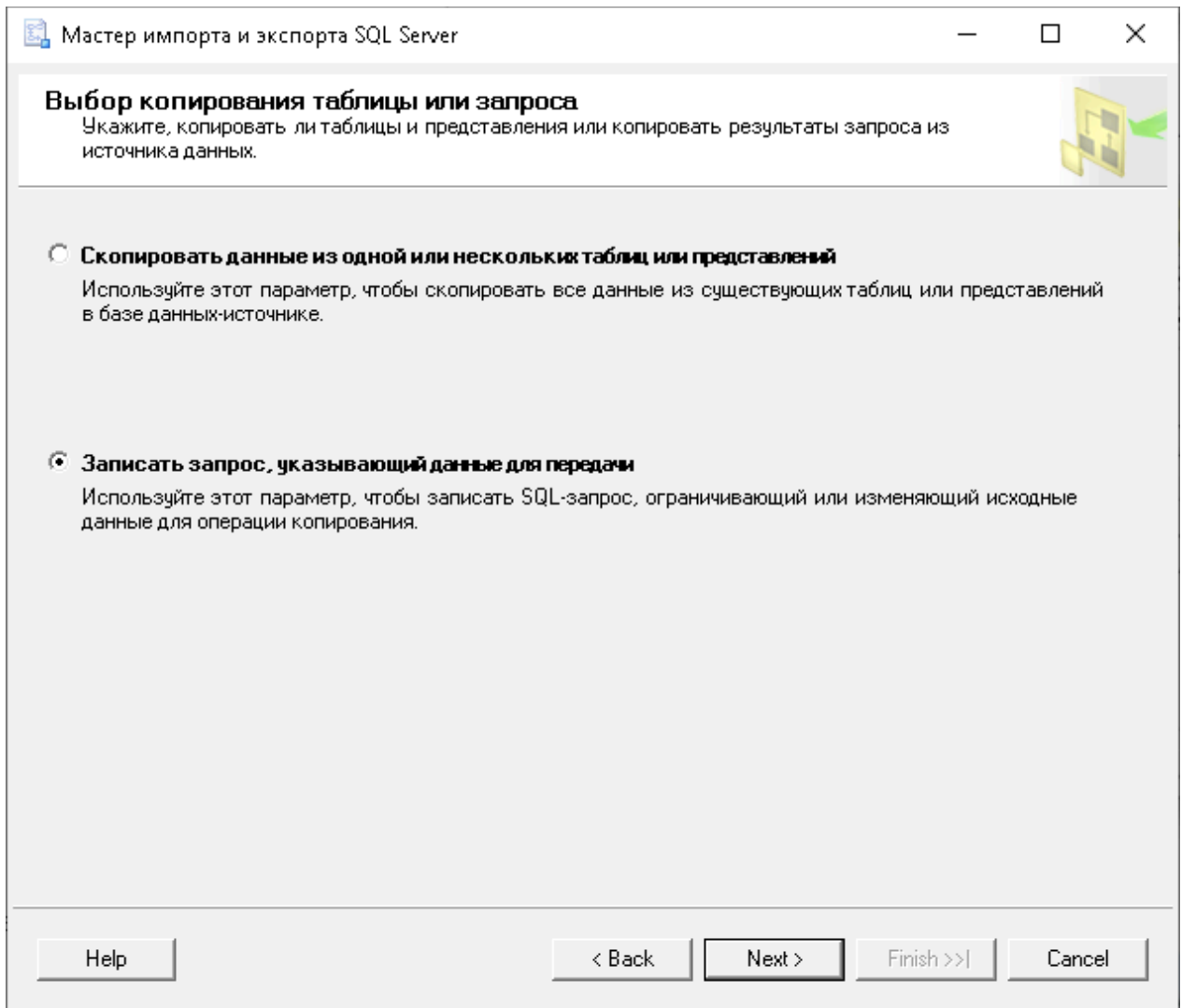
База данных: indeed\_am\_81

Обновить

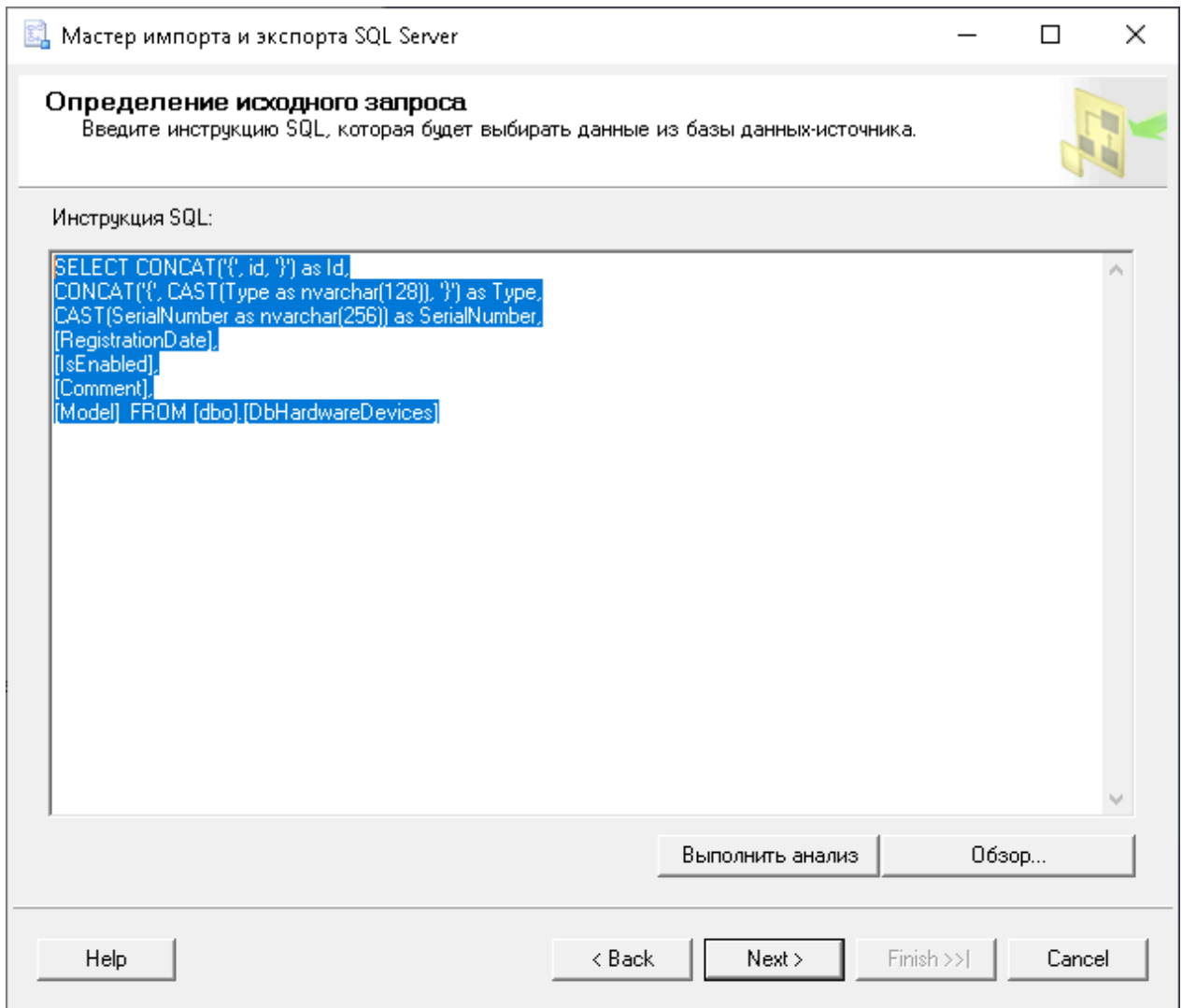
Создать...

Help < Back Next > Finish >> Cancel

4. Выберите получение данных для экспорта пользовательским запросом.



5. Укажите запрос для выборки данных (список всех запросов приведен в пункте Запросы получения данных из хранилища 7.х).



### ❗ 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 сервера sql не сможет обработать строковое значение.

6. Далее выберите таблицы для экспорта и импорта.

Мастер импорта и экспорта SQL Server

**Выбор исходных таблиц и представлений**  
Выберите одну или несколько таблиц или представлений для копирования.

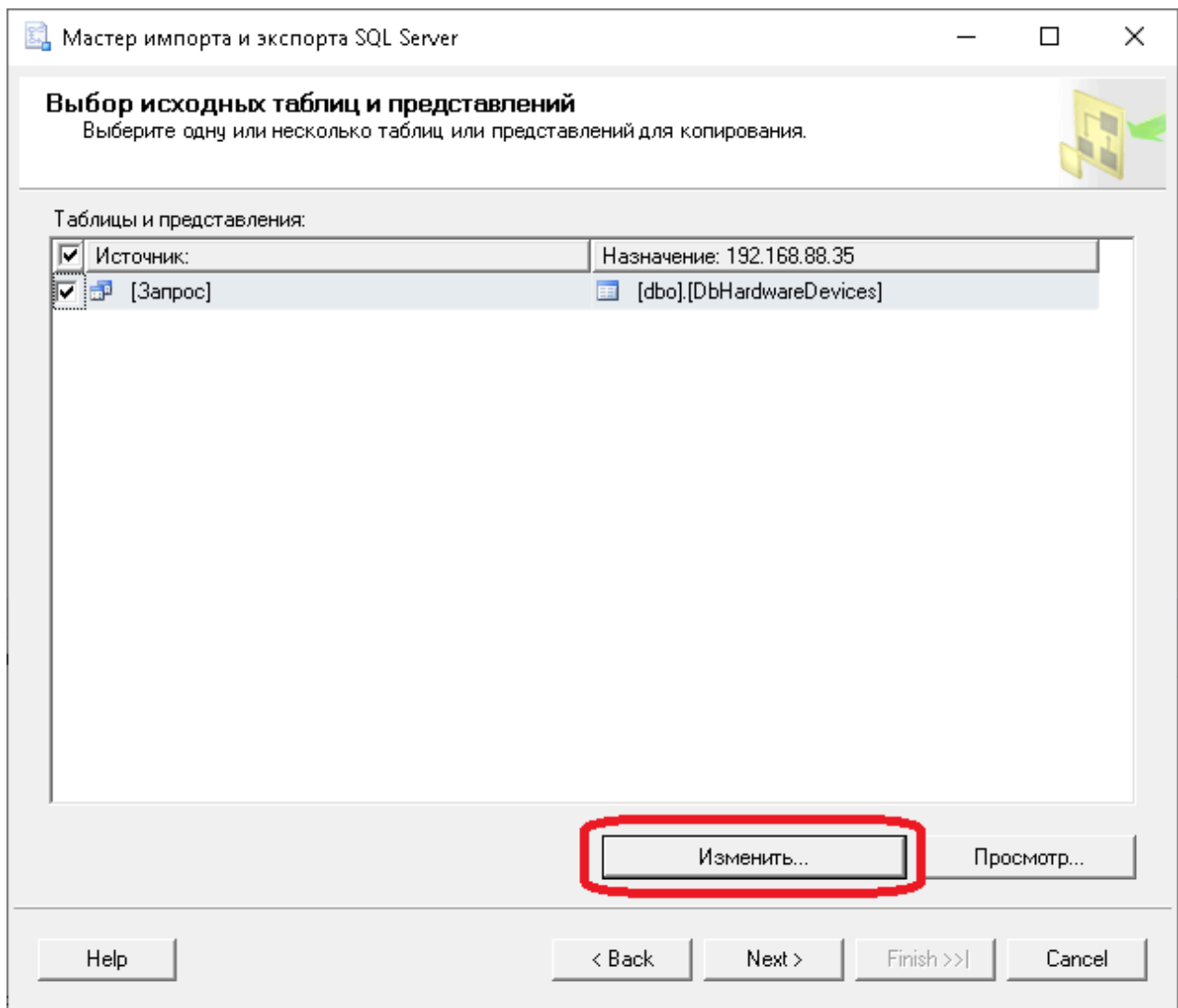
Таблицы и представления:

|                                               |                           |
|-----------------------------------------------|---------------------------|
| <input checked="" type="checkbox"/> Источник: | Назначение: 192.168.88.35 |
| <input checked="" type="checkbox"/> [Запрос]  | [dbo].[Запрос]            |

- [dbo].[DbAccessGroupMembers]
- [dbo].[DbCacheSettings]
- [dbo].[DbHardwareDeviceProperties]
- [dbo].[DbHardwareDevices]
- [dbo].[DbInstanceProperties]
- [dbo].[DbLicenseObjects]
- [dbo].[DbLicenses]
- [dbo].[DbStorageProperties]

Изменить...    Просмотр...

Help    < Back    Next >    Finish >>    Cancel



7. В настройках маппинга на этом же экране укажите, 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 | <input type="checkbox"/>            |        |           |        |
| Type             | Type             | uniqueidentifier | <input type="checkbox"/>            |        |           |        |
| SerialNumber     | SerialNumber     | nvarchar         | <input checked="" type="checkbox"/> | 256    |           |        |
| RegistrationDate | RegistrationDate | datetime2        | <input type="checkbox"/>            |        |           | 7      |
| IsEnabled        | IsEnabled        | bit              | <input type="checkbox"/>            |        |           |        |
| Comment          | Comment          | nvarchar         | <input checked="" type="checkbox"/> | max    |           |        |
| Model            | Model            | nvarchar         | <input checked="" type="checkbox"/> | max    |           |        |

Исходный столбец: Id nvarchar (130) NOT NULL

8. Далее проверьте набор полей. Вы увидите 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 утраты данных           |
|---|------------------|--------------|------------------|------------------|-------------------------------------|----------------------------------|----------------------------------|
| ⚠ | Id               | nvarchar     | Id               | uniqueidentifier | <input checked="" type="checkbox"/> | Использовать глобальное значение | Использовать глобальное значение |
| ⚠ | Type             | nvarchar     | Type             | uniqueidentifier | <input checked="" type="checkbox"/> | Использовать глобальное значение | Использовать глобальное значение |
| ✓ | 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 утраты данных (используется глобально)

9. Запустите 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

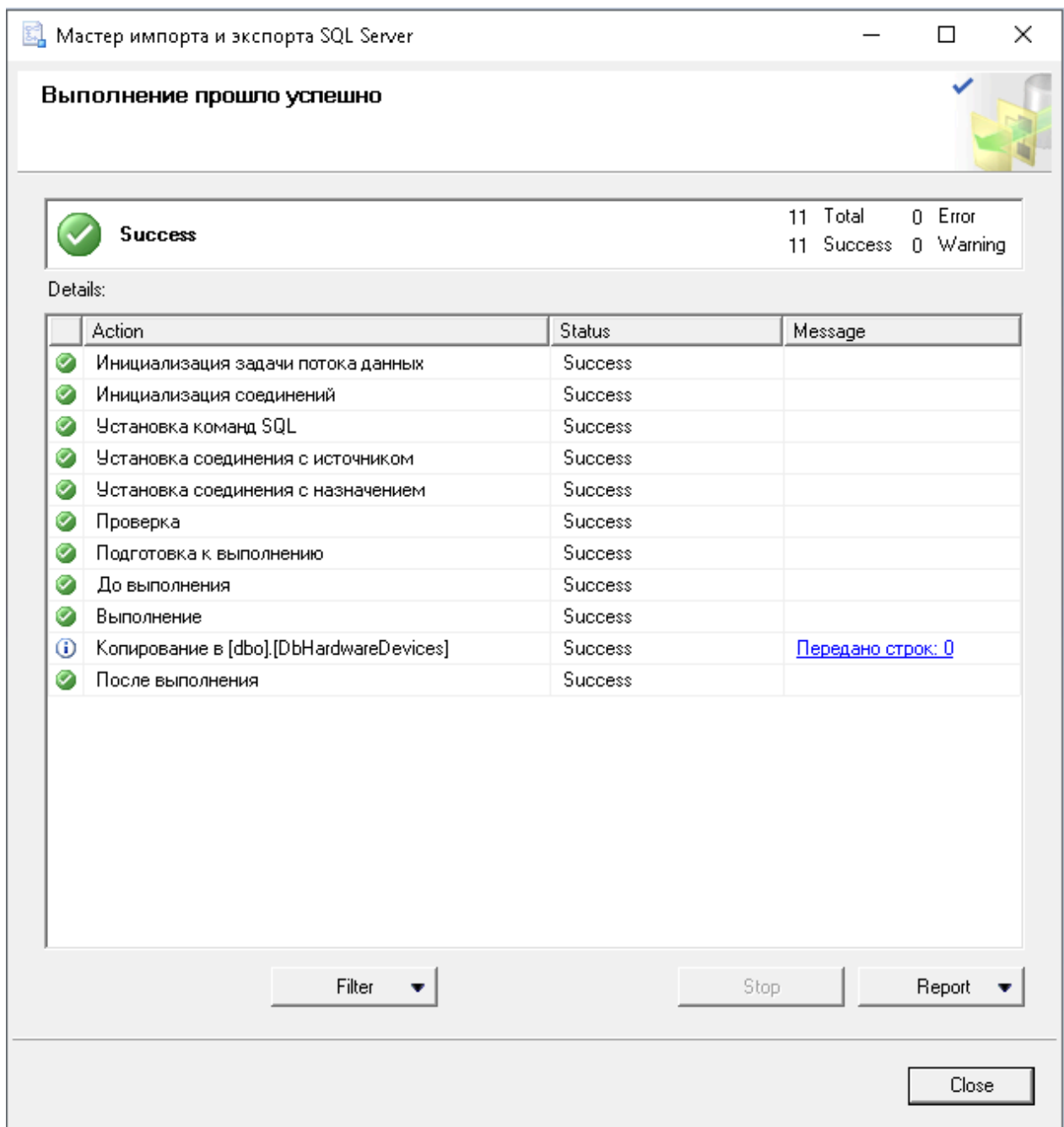
Уровень защиты пакета:

Шифровать конфиденциальные данные пользовательским ключом

Пароль:

Подтверждение:

Help < Back Next > Finish >>| Cancel



10. После миграции всех таблиц запустите сервер IIS 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('{', ModeId, '}') as ModeId
      ,[ModeTypeName]
      ,[ModeDeviceName]
      ,[ModeType]
      ,[CreatedOn]
      ,[TemplateRawData]
      ,[Description]
      ,[IsDisabled]
      ,[ExpirationDate]
      ,[AuthenticationCountLimitValue]
      ,[Flags]
      ,[IsLocked]
      ,[SerialNumber]
FROM [dbo].[DbUserAuthenticators]
```

4. Запрос к таблице *DbHardwareDevices*. Текст запроса:

```
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]
```

5. Запрос к таблице *DbHardwareDeviceProperties*. Текст запроса:

```
SELECT CONCAT('{', id, '}') as Id
      ,CONCAT('{', CAST(HardwareDeviceId as nvarchar(128)), '}') as
HardwareDeviceId
      ,[PropertyId]
      ,[Value]
FROM [dbo].[DbHardwareDeviceProperties]
```

# Миграция хранилища Active Directory



## ВАЖНО

Обязательное условие: ключи шифрования хранилища и структура пользовательских каталогов (их идентификаторы) обоих инстансов должны совпадать.



## ИНФОРМАЦИЯ

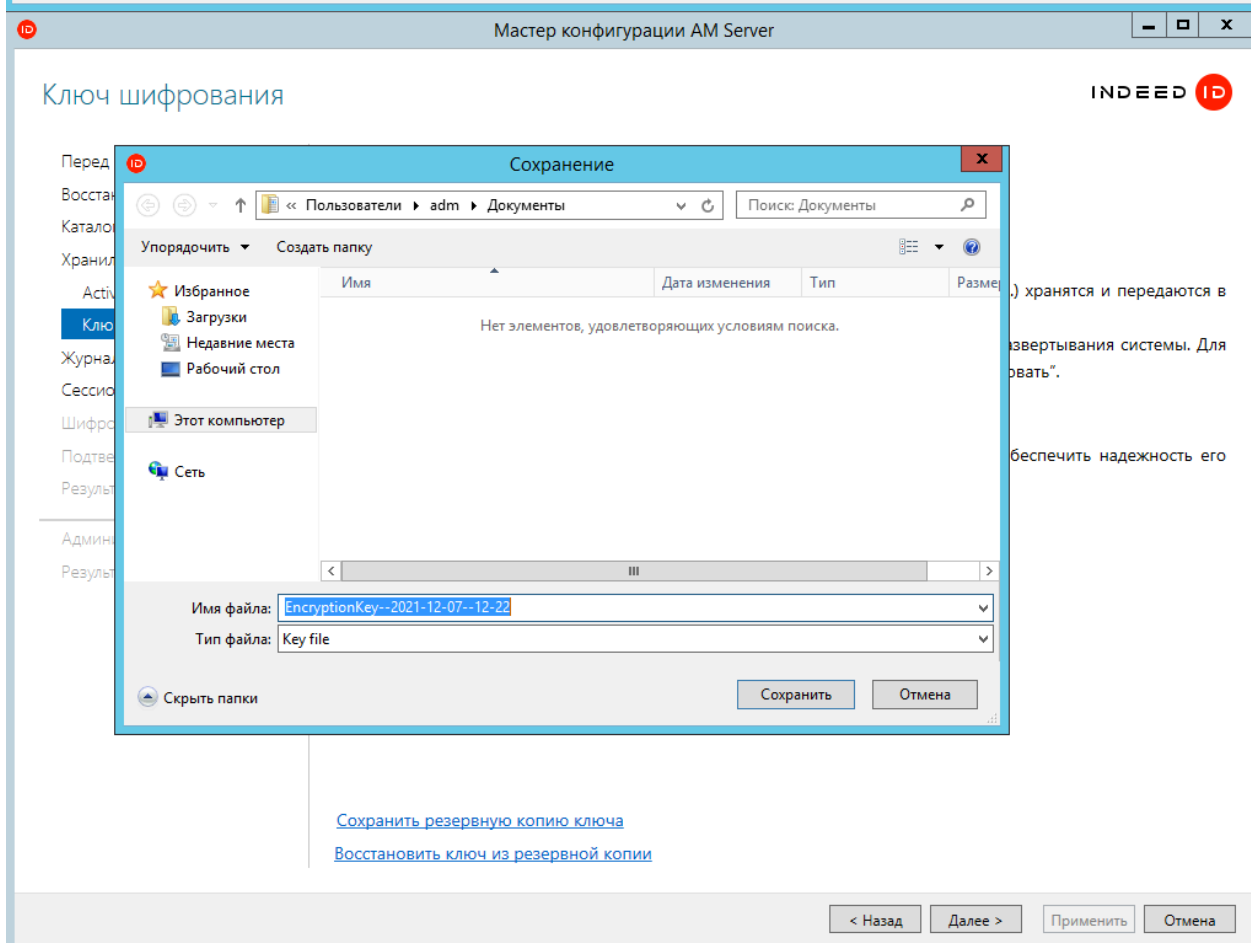
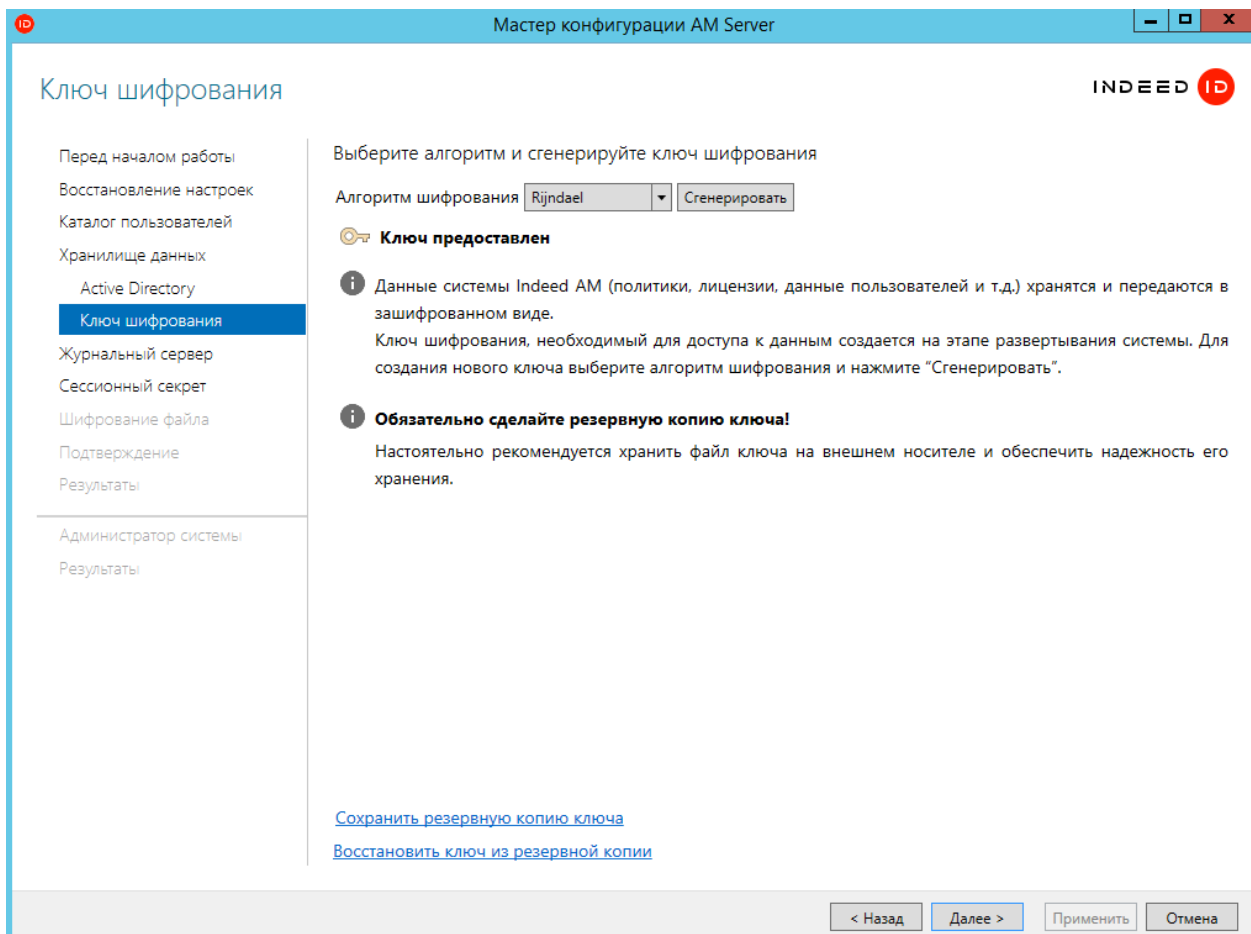
Используется инструмент ADUC.

Миграция осуществляется по шагам, интерактивно, прозрачно для администратора AD.

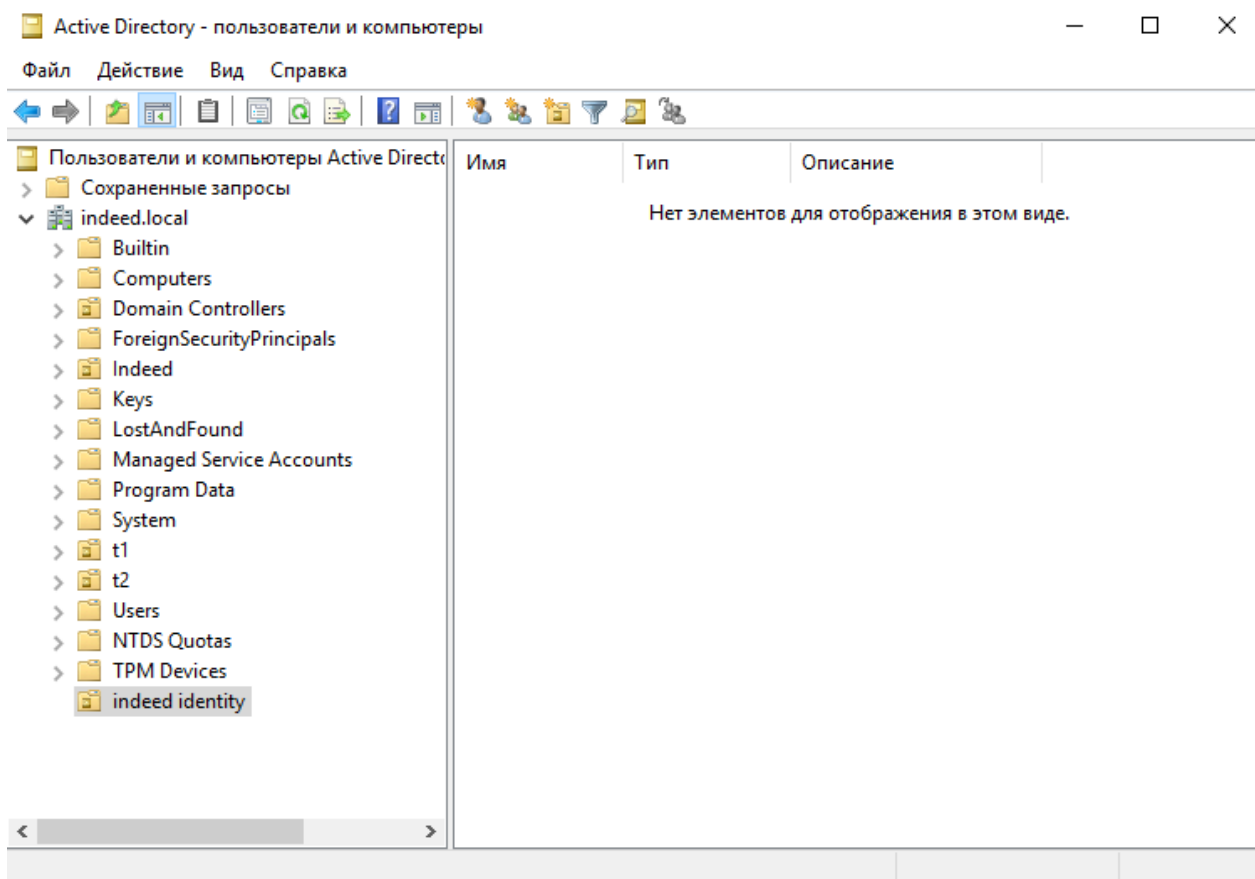
Миграция производится путем перемещения объектов с данными АМ из контейнера хранилища ЕА 7 в хранилище АМ 8.

## Подготовка AD хранилища Indeed AM 8.1

1. Запустите Мастер конфигурации на сервере Indeed AM 7.x
2. Пройдите в нем 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.



## Ключ шифрования

- Перед началом работы
  - Восстановление настроек
  - Каталог пользователей
  - Хранилище данных
  - Active Directory
  - Ключ шифрования**
  - Журнальный сервер
  - Сессионный секрет
  - Шифрование файла
  - Подтверждение
  - Результаты
- 
- Администратор системы
  - Результаты

Выберите алгоритм и сгенерируйте ключ шифрования

Алгоритм шифрования Aes Сгенерировать

### Ключ не предоставлен

**i** Данные системы Indeed AM (политики, лицензии, данные пользователей и т.д.) хранятся и передаются в зашифрованном виде. Ключ шифрования, необходимый для доступа к данным создается на этапе развертывания системы. Для создания нового ключа выберите алгоритм шифрования и нажмите "Сгенерировать".

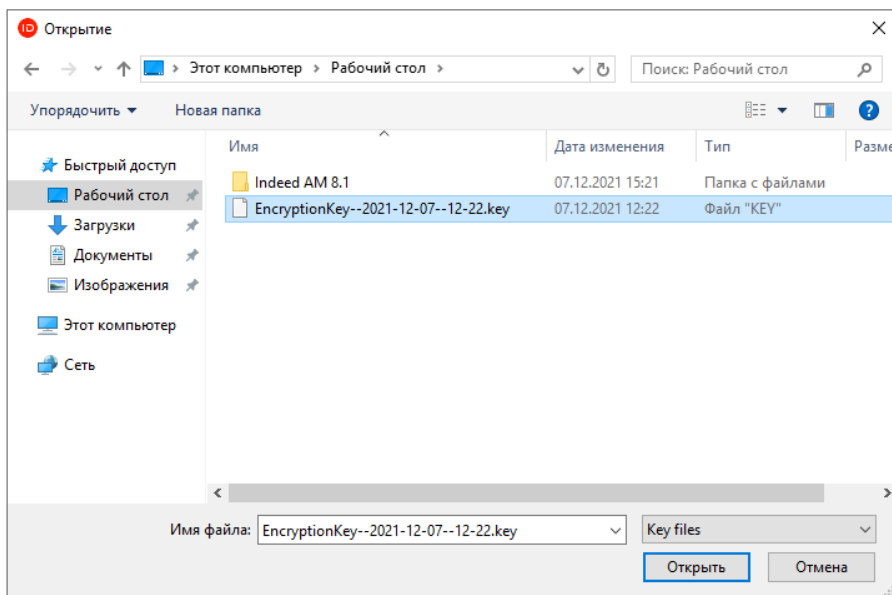
### **i** Обязательно сделайте резервную копию ключа!

Настоятельно рекомендуется хранить файл ключа на внешнем носителе и обеспечить надежность его хранения.

[Сохранить резервную копию ключа](#)

[Восстановить ключ из резервной копии](#)

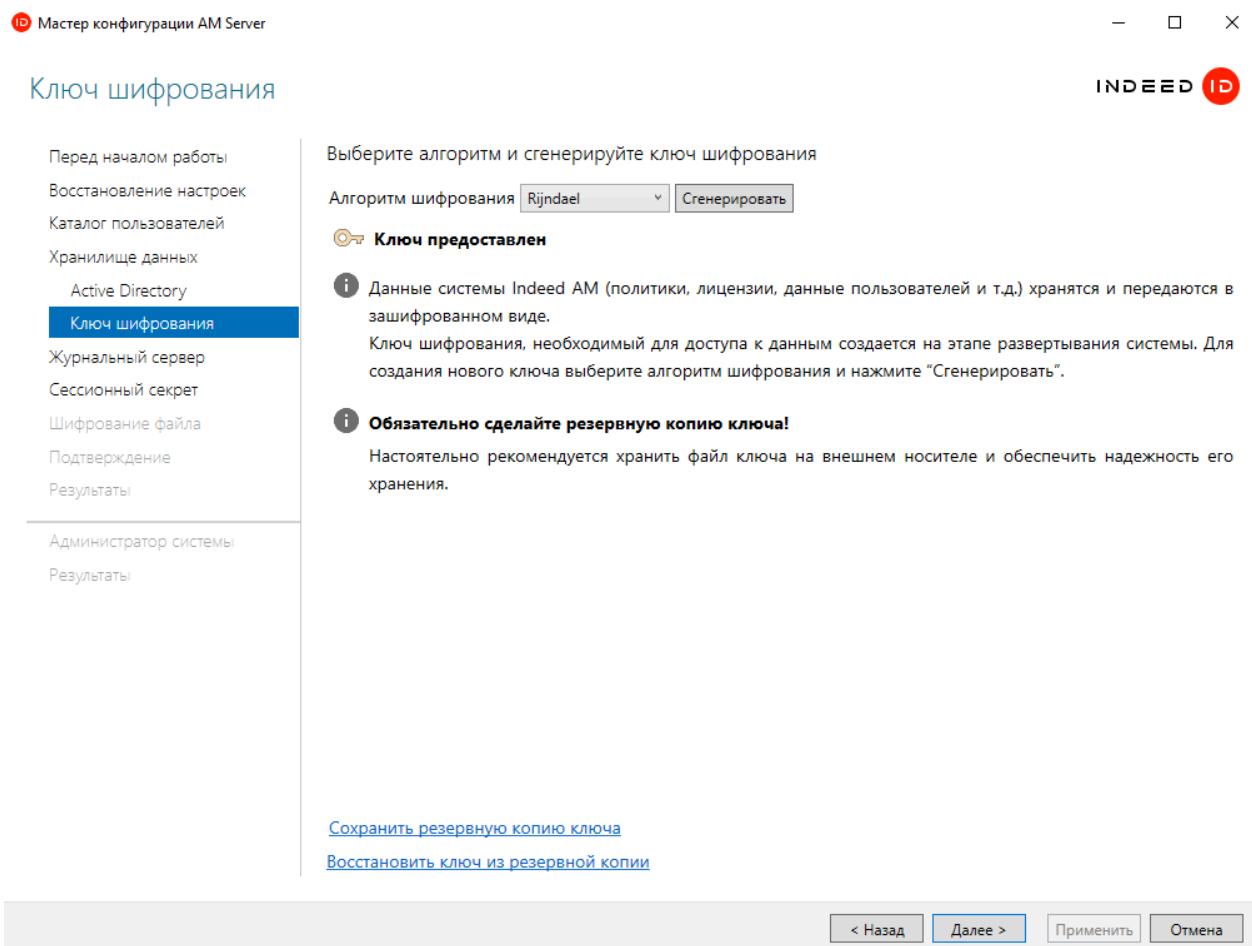
< Назад Далее > Применить Отмена



[Сохранить резервную копию ключа](#)

[Восстановить ключ из резервной копии](#)

< Назад Далее > Применить Отмена



6. Остановите сервер IIS 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.

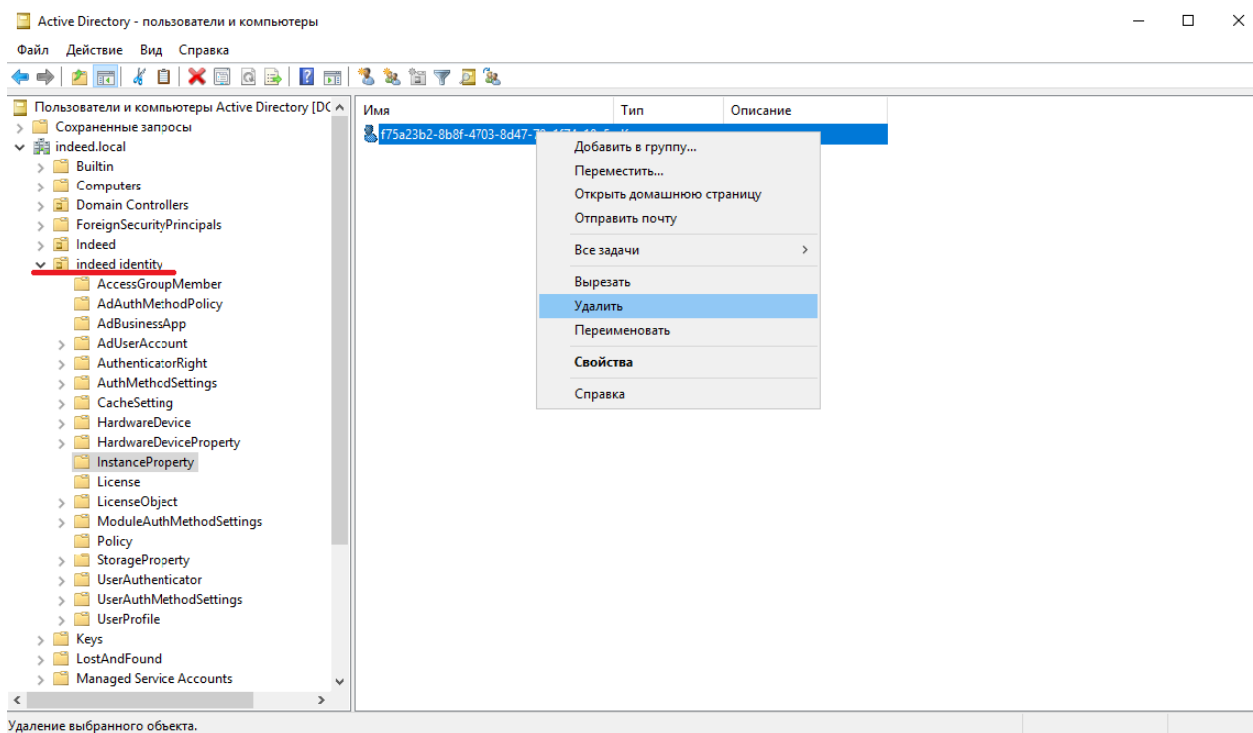


## СОВЕТ

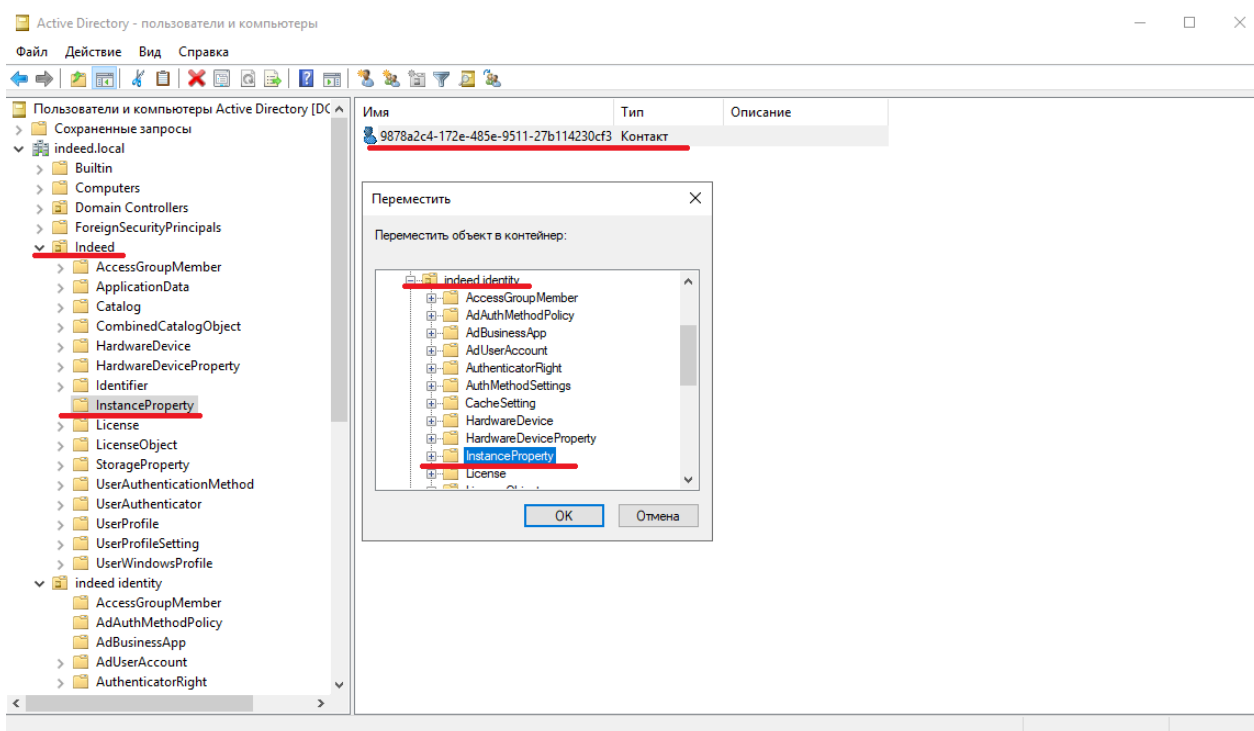
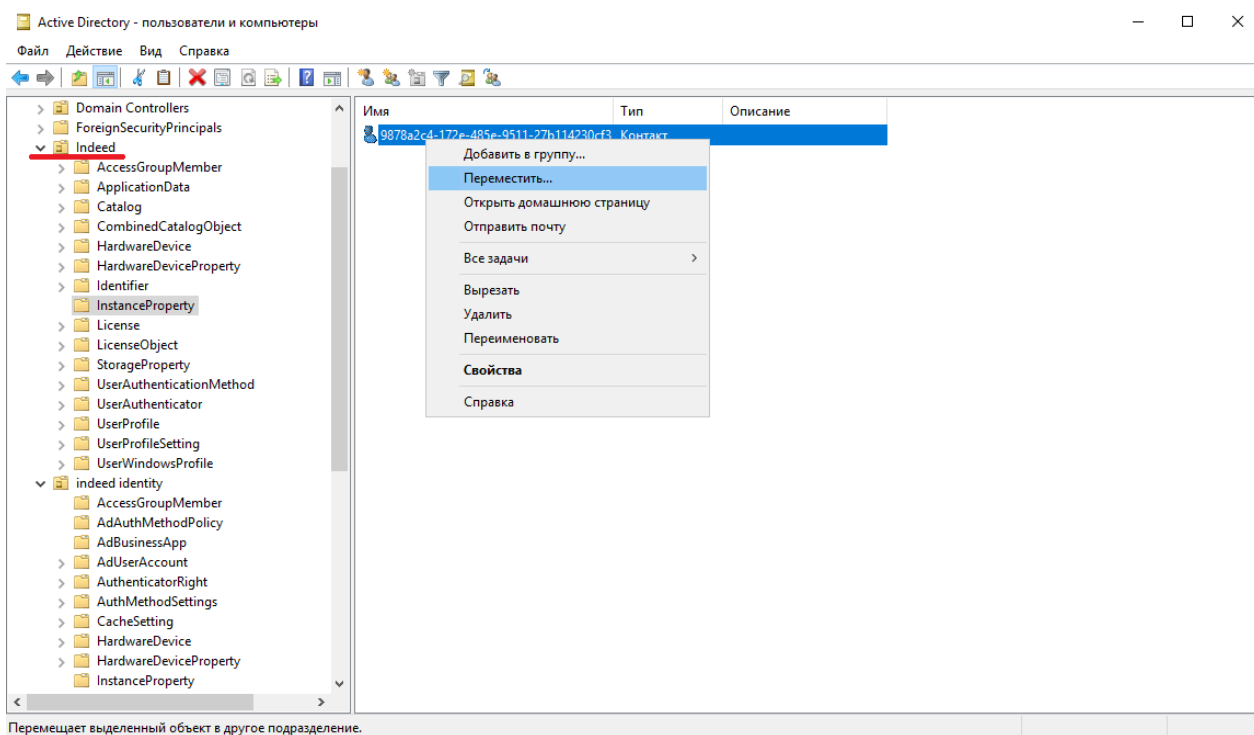
При необходимости объемных групповых перемещений, можно использовать скрипт PowerShell и командлет `Move-ADObject`. Подробнее об этом командлете можно узнать в [статье Microsoft](#).

## Миграция InstanceProperty

1. Удалите содержимое каталога *indeed identity* — *InstanceProperty*.

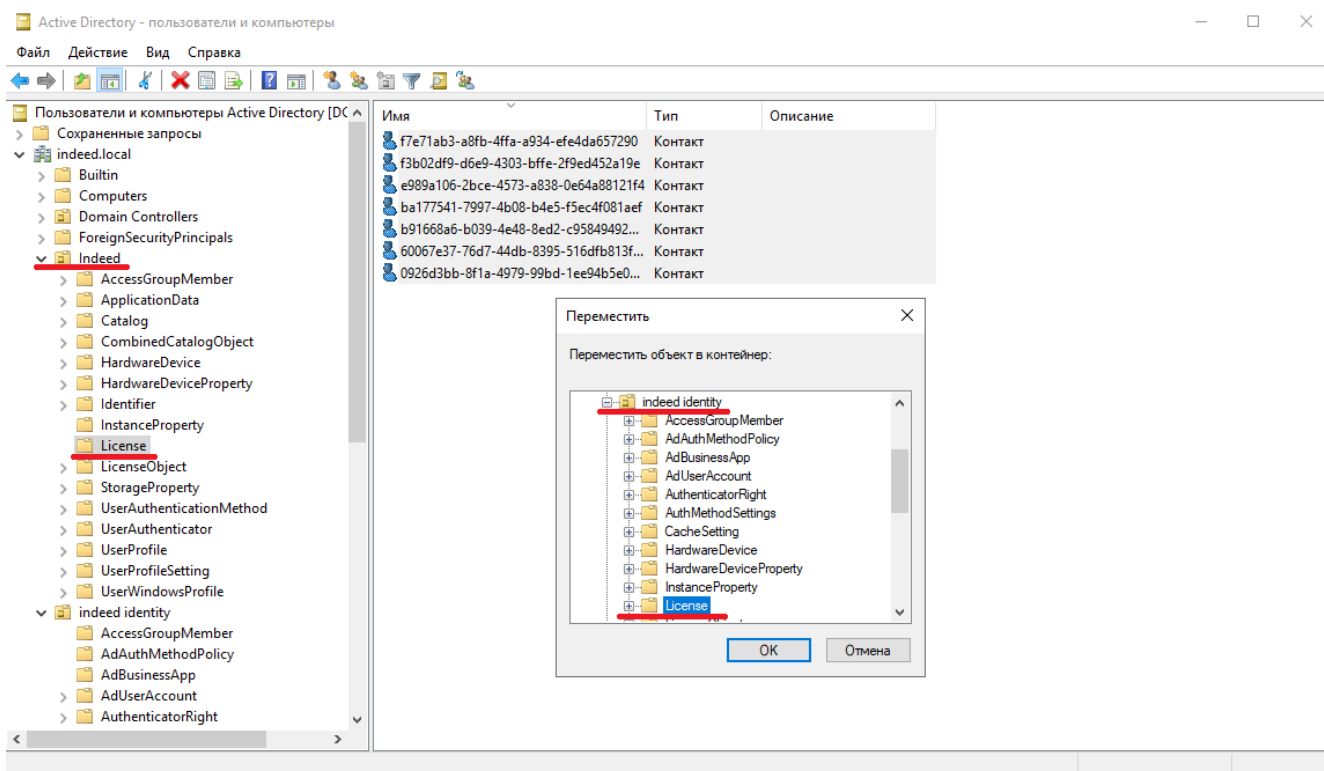
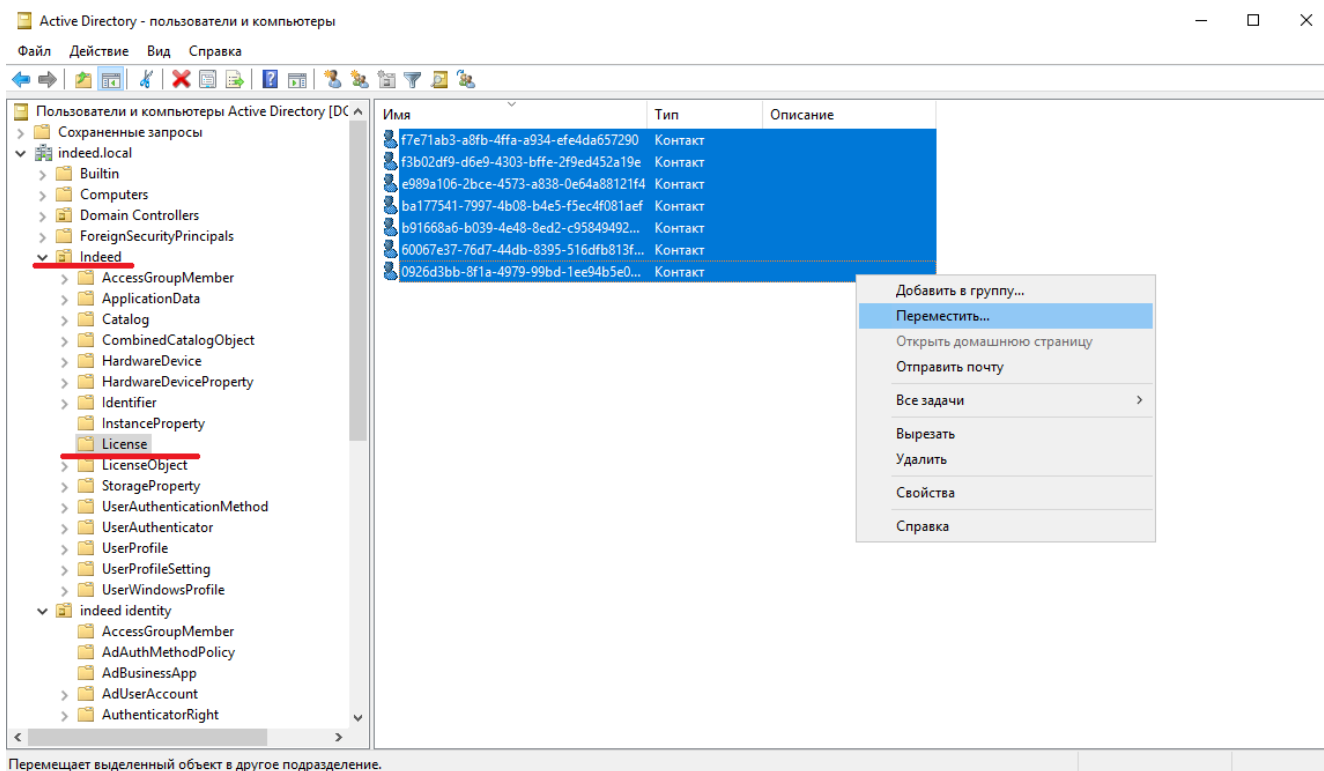


2. Переместите содержимое каталога *indeed* — *InstanceProperty* в *indeed identity* — *InstanceProperty*.



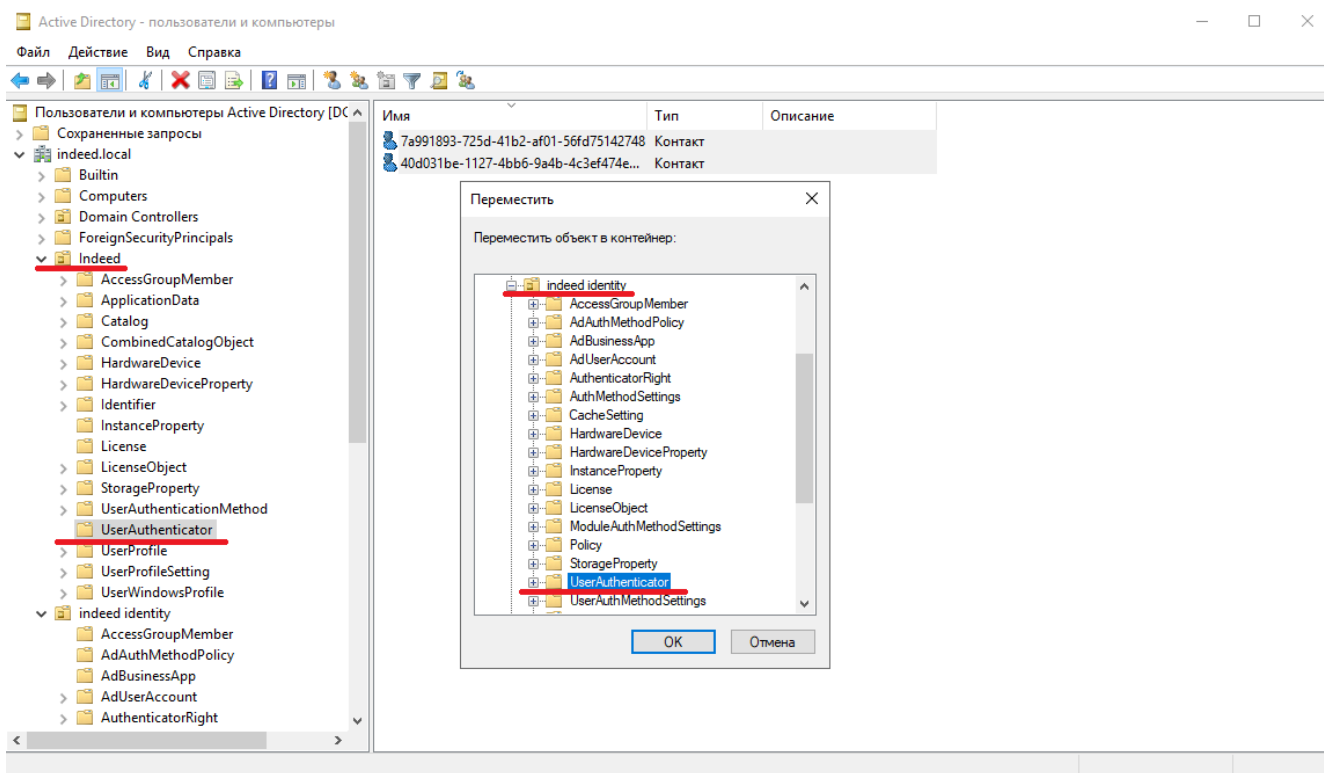
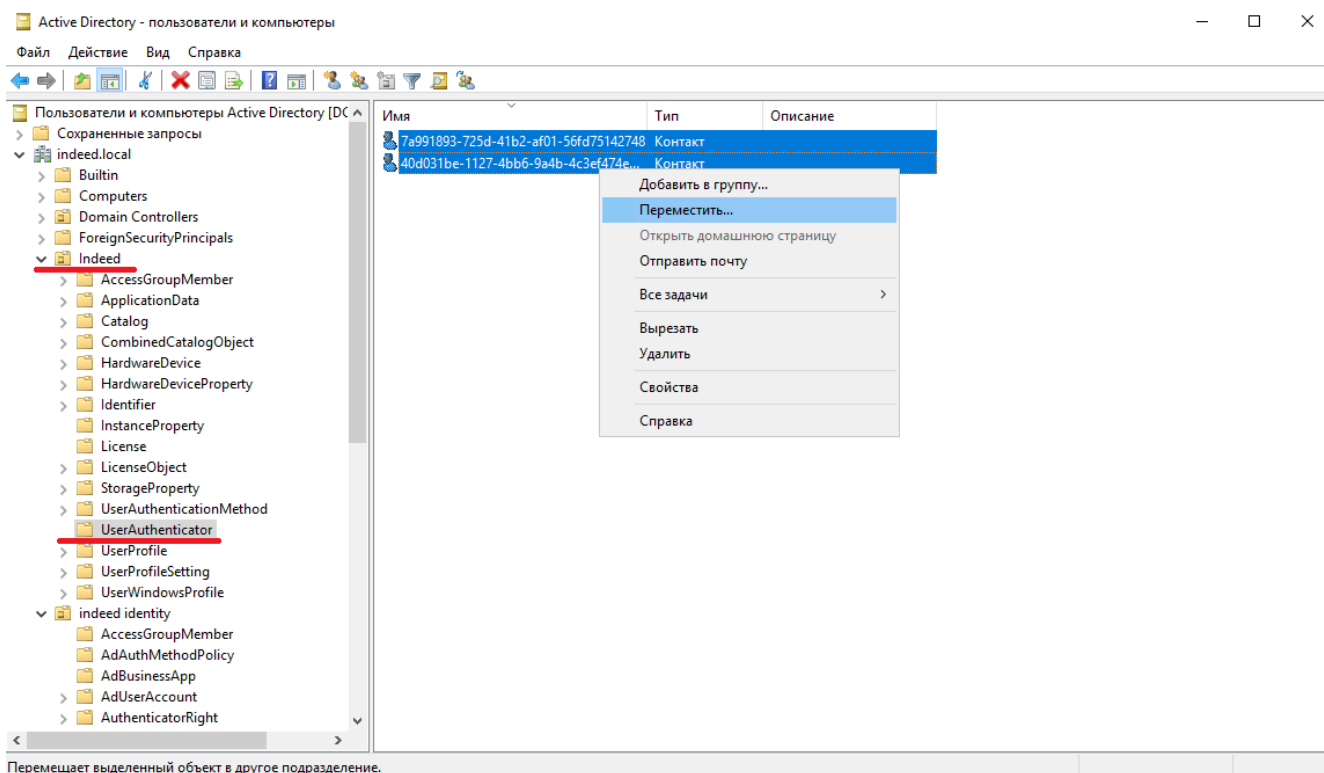
## Миграция License

Переместите содержимое каталога *indeed* — *License* в *indeed identity* — *License*.



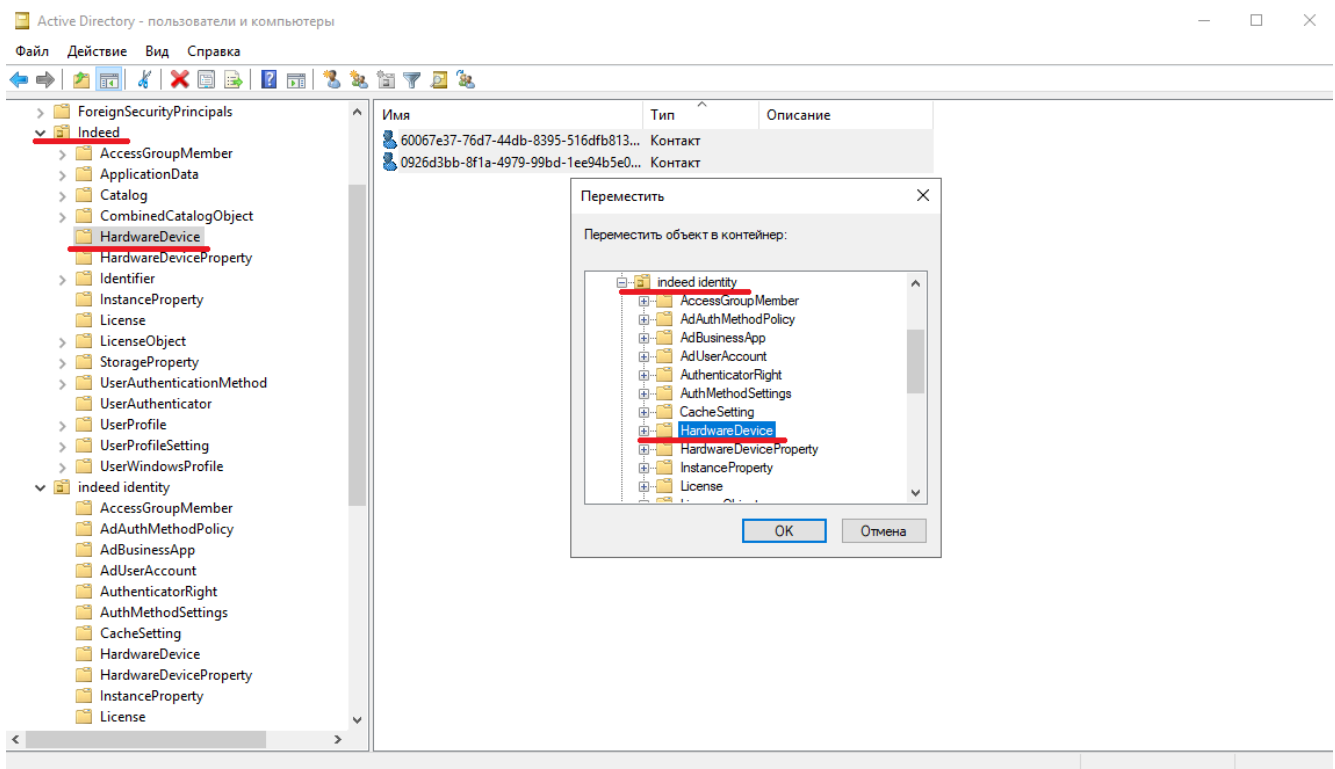
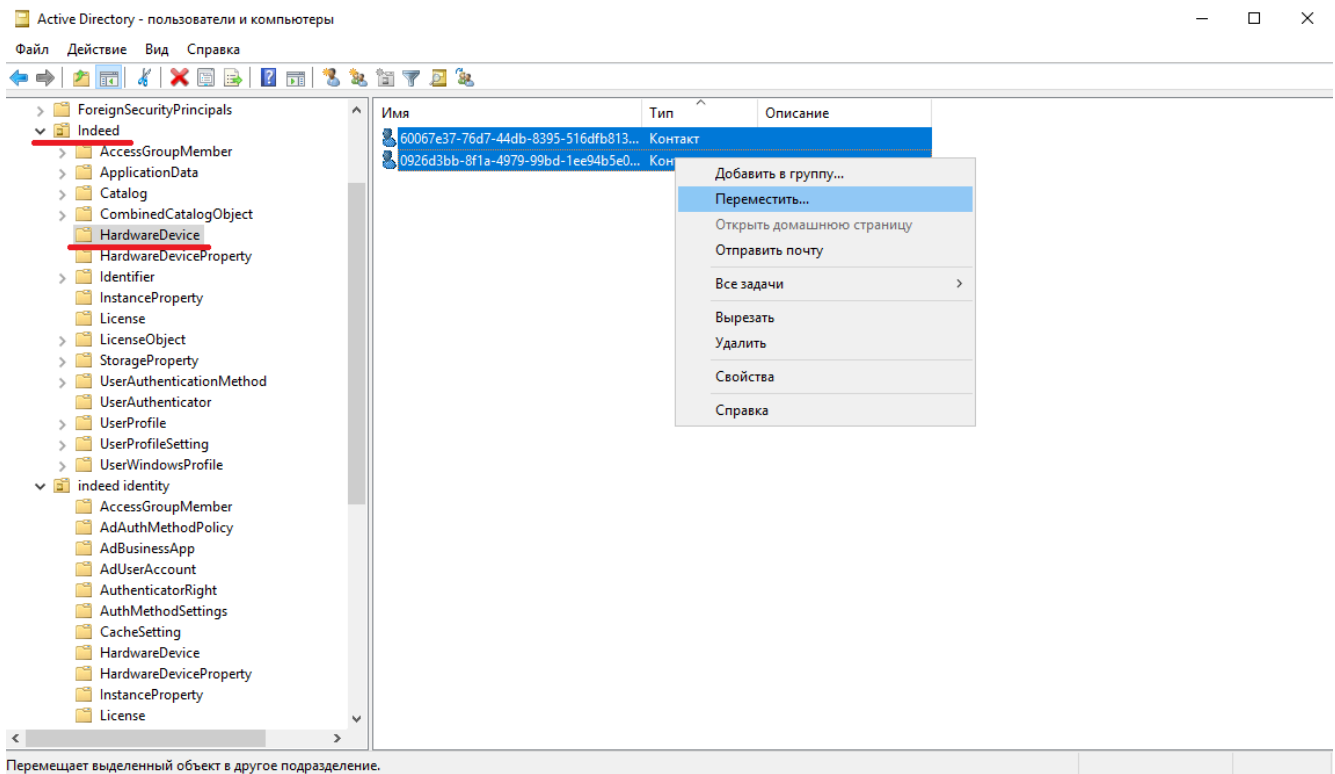
## Миграция UserAuthenticator

Переместите содержимое каталога *indeed* — *UserAuthenticator* в *indeed identity* — *UserAuthenticator*.



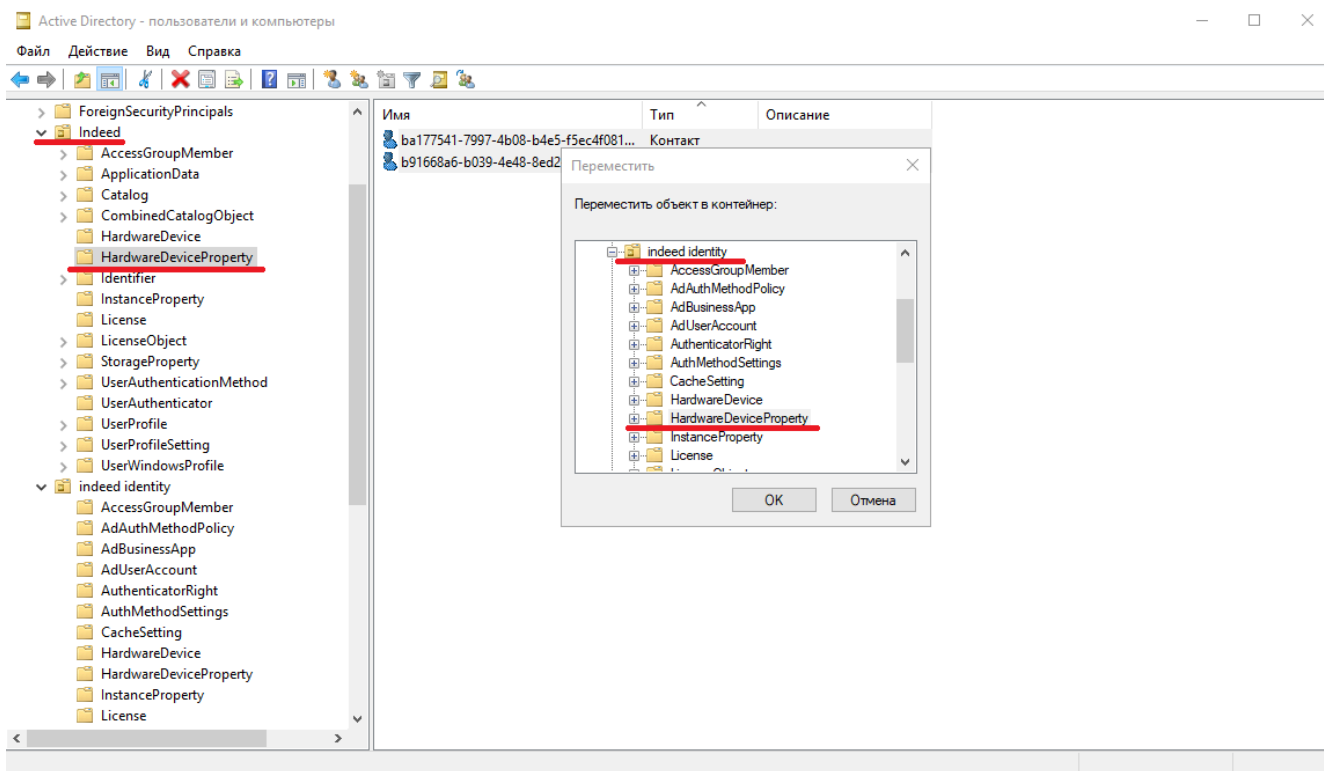
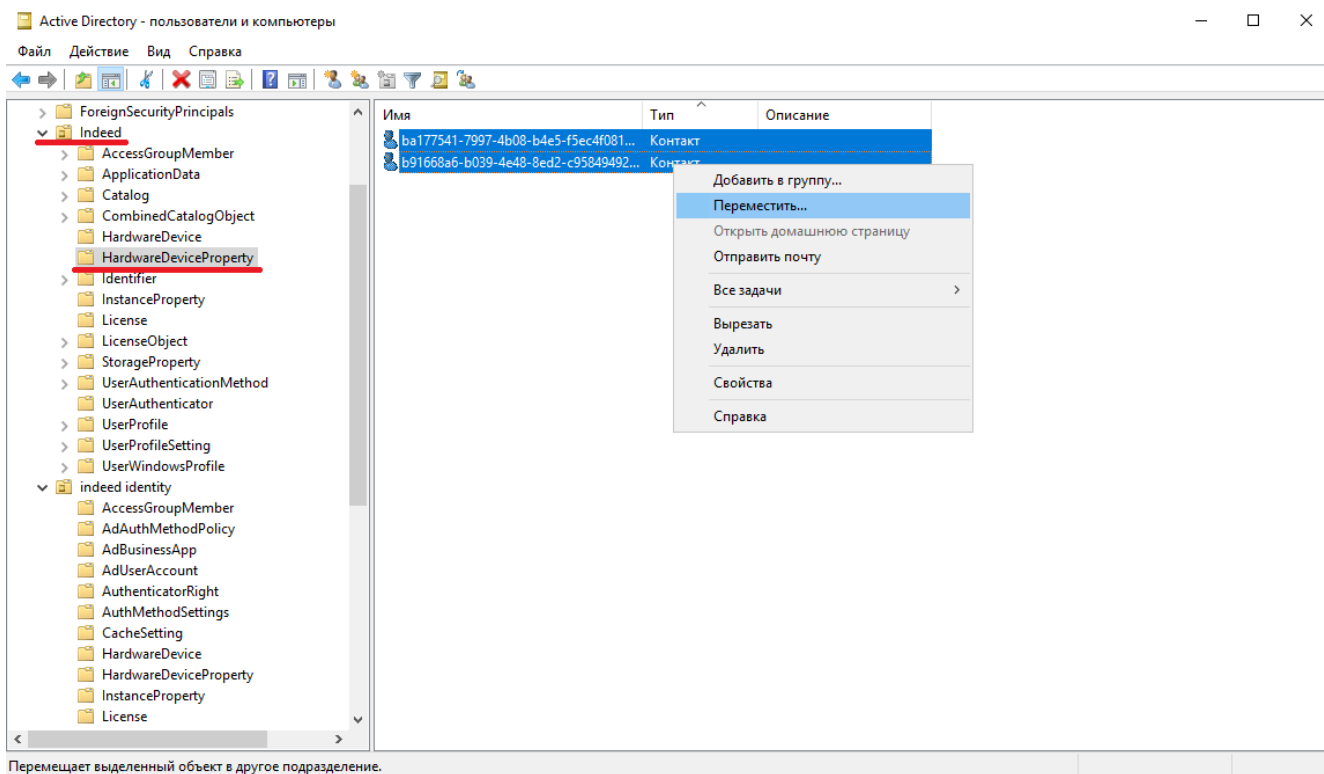
## Миграция HardwareDevice

Переместите содержимое каталога *indeed* — *HardwareDevice* в *indeed identity* — *HardwareDevice*.\*.



## Миграция HardwareDeviceProperty

Переместите содержимое каталога *indeed* — *HardwareDeviceProperty* в *indeed identity* — *HardwareDeviceProperty*.



При завершении миграции запустите сервер IIS с Indeed AM server 8.1.



# Решение проблем



## Сбор программных логов

Логи IIS Extension, Radius Extension, RDP Windows Logon, Windows Logon и ESSO



## Сбор логов серверных компонентов

Логи Core Server, Log Server, Key Server, Management Console, User Console и IDP



## База знаний

Часто задаваемые вопросы и их решения



## Техническая поддержка

Как создать обращение в поддержку

# Сбор программных логов

Приложение Indeed AM GetLog предназначено для локального и удаленного сбора программных логов следующих компонентов:

- IIS Extension,
- Radius Extension,
- RDP Windows Logon,
- Windows Logon,
- Enterprise Single Sign-On.

## Подключение к компьютеру

Чтобы подключиться к компьютеру, логи которого нужно получить:

1. Запустите утилиту GetLog от имени локального администратора. Файл запуска расположен в *Indeed AM <номер версии>\logging\IndeedAM.GetLog.exe*.
2. В поле Computer введите имя или IP-адрес удаленного компьютера. Чтобы подключиться к локальному компьютеру, введите *localhost* или *127.0.0.1*.
3. Нажмите Connect. После установки соединения станут доступны:
  - кнопка включения/отключения логов Enable Log/Disable Log;
  - кнопка получения логов Get Log;
  - кнопка перехода к дополнительным настройкам Advanced Settings;
  - кнопка отключения Disconnect.



### ПОДСКАЗКА

Чтобы подключиться к удаленному компьютеру под управлением Windows 7 и выше, убедитесь в том, что на удаленном компьютере запущена и не заблокирована служба Инструментарий управления Windows (WMI) (Windows Management Instrumentation).

# Основные действия

## Работа с утилитой

Чтобы включить или отключить логирование и получить логи:

1. Подключитесь к компьютеру.
2. Для включения записи логов нажмите Enable Log.
3. Если сбор логов требуется для выявления причин проблемной ситуации, выполните действия для воспроизведения проблемы.
4. Для отключения записи логов нажмите Disable Log.
5. Для получения логов нажмите Get Log....
6. Укажите каталог для сохранения ZIP-архива и нажмите Сохранить.
7. Для отключения от компьютера нажмите Disconnect и закройте приложение.

## Работа с реестром

В некоторых случаях может потребоваться включить/отключить логирование вручную. Для этого:

1. Откройте редактор реестра.
2. Перейдите в каталог `HKEY_LOCAL_MACHINE\SOFTWARE\Indeed-ID\Logging`.
3. Задайте значение параметра **Enabled**:
  - 0, чтобы отключить логирование;
  - 1, чтобы включить логирование.

### ❗ ПРИМЕЧАНИЕ

По умолчанию логи записываются в каталог `\WINDOWS\System32\LogFiles\Indeed-Id`. Для доступа к логам удаленного компьютера по умолчанию используется сетевой каталог `ADMIN$\System32\LogFiles\Indeed-Id`. Каталог для записи логов можно задать в разделе `Advanced Settings > Use alternative location`.

Если при попытке сохранить логи появляется ошибка *The system cannot find the file specified*, убедитесь, что папка `C:\Windows\System32\LogFiles\Indeed-ID` существует. Создайте папку вручную, если она отсутствует.

## Дополнительные настройки

### Настройки в утилите

Чтобы перейти к дополнительным настройкам, нажмите `Advanced Settings` в главном окне `Indeed AM GetLog`. В окне `Advanced Settings` доступны следующие настройки:

- `Max. log size (bytes)` — максимальный размер в байтах всех файлов в каталоге. Значение по умолчанию — 1ГБ. При достижении указанного значения из каталога будут удалены все файлы, дата изменения которых старше значения поля *Max.log file age*.
- `Max. log file age (s)` — возраст файла лога в секундах. Если размер логов в каталоге превысил значение *Max. log size*, то из каталога будут удалены все файлы, дата изменения которых старше значения этого поля.
- `Cleaner interval (s)` — интервал проверки размера каталога с логами в секундах. Значение по умолчанию – 1 час (3600 секунд).
- `Activity checking period (ms)` — интервал проверки активности логирования в миллисекундах. Прежде чем начать запись логов, компонент `Indeed AM` проверит, включено ли на рабочей станции логирование. По умолчанию интервал проверки составляет 1 минуту (60 000 миллисекунд).
- `Enable log cycling` — режим циклической записи логов. Если опция включена, то логи каждого процесса будут записываться согласно заданным настройкам по количеству файлов и размеру.

- Max. size of a log file (bytes) — максимальный размер лога в байтах. Значение по умолчанию — 10Мб (1000000 байт). При достижении заданного размера содержимое файла перезапишется новыми данными.
  - Max. number of saved log files — максимальное количество сохраняемых логов. Значение по умолчанию — 5, без учета текущего записываемого файла. Если установленное количество файлов превышено, самый ранний удалится, а запись продолжится во вновь созданный файл.
- Use alternative location — альтернативный каталог записи логов. Если опция выключена, логи записываются в каталоги по умолчанию:
  - ADMIN\$\System32\LogFiles\Indeed-Id — сетевой путь;
  - \WINDOWS\System32\LogFiles\Indeed-Id — локальный путь.

## Настройки в реестре

Чтобы перейти к дополнительным настройкам в реестре, откройте редактор реестра и перейдите в каталог *HKEY\_LOCAL\_MACHINE\SOFTWARE\Indeed-ID\Logging*. В реестре доступны следующие параметры:

- **CycleLogsFileCountMax** — максимальное количество сохраняемых логов. Значение по умолчанию — 5, без учета текущего записываемого файла. Если установленное количество файлов превышено, самый ранний удалится, а запись продолжится во вновь созданный файл.
- **CycleLogsFileSizeMaxBytes** — максимальный размер лога в байтах. Значение по умолчанию — 10Мб (1000000 байт). При достижении заданного размера содержимое файла перезапишется новыми данными.
- **EnabledRecheckPeriodMs** — интервал проверки активности логирования в миллисекундах. Прежде чем начать запись логов, компонент Indeed АМ проверит, включено ли на рабочей станции логирование. По умолчанию интервал проверки составляет 1 минуту (60 000 миллисекунд).
- **MaxLogFileAge** — возраст файла лога в секундах. Если размер логов в каталоге превысил значение **MaxlogSize**, то из каталога будут удалены все файлы, дата изменения которых старше значения этого параметра.

- **MaxLogSize** — максимальный размер в байтах всех файлов в каталоге. Значение по умолчанию — 1ГБ. При достижении указанного значения из каталога будут удалены все файлы, дата изменения которых старше значения параметра **MaxlogFileAge**.
- **RootLogPath** — альтернативный каталог записи логов. Если параметр отключен, логи записываются в каталоги по умолчанию:
  - *ADMIN\$\System32\LogFiles\Indeed-Id* — сетевой путь;
  - *\WINDOWS\System32\LogFiles\Indeed-Id* — локальный путь.

# Сбор логов серверных компонентов

## Уровни логирования

В зависимости от того, насколько подробную информацию о работе компонента нужно получить, можно задать разные уровни логирования. Они определяют, насколько важная и подробная информация будет записываться в лог-файлы. Это позволяет фильтровать и анализировать логи более эффективно.

Рекомендуется использовать уровень логирования *Trace*, как наиболее информативный.

## ▼ Уровни логирования

|       |                                                                                                                                                                                                                                                                                                                                                |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Trace | Наиболее подробный уровень. Логи с уровнем Trace содержат всю информацию о процессах работы компонента, включая детали о вызовах методов API.                                                                                                                                                                                                  |
| Debug | При этом уровне логирования записи содержат подробности о ходе работы компонента, значимые переменные и другие данные, которые могут быть полезными при обнаружении и исправлении ошибок.                                                                                                                                                      |
| Info  | При этом уровне логирования записываются информационные сообщения, которые уведомляют о нормальном функционировании компонента. Они могут включать такие события, как запуск или завершение процессов, редактирование профиля пользователя и другие.                                                                                           |
| Warn  | Логирование этого уровня используется, чтобы записывать предупреждения и уведомления о потенциальных ошибках и внештатных ситуациях. События не являются критическими, но требуют внимания. При этом компонент может продолжать работу.                                                                                                        |
| Error | Уровень логирования, используемый для записи ошибок, повлекших за собой некорректную работу компонента или возникновение серьезных проблем. Логи с уровнем Error указывают на проблемы, которые требуют вмешательства и исправления.                                                                                                           |
| Fatal | Наименее подробный уровень логирования. Если задан этот уровень, будут записываться только самые критические ошибки и проблемы, которые приводят к немедленному завершению работы компонента или другим серьезным последствиям. Логи с уровнем Fatal обычно означают серьезные сбои, которые требуют немедленного вмешательства и исправления. |

## 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 отправьте в поддержку с подробным описанием действий пользователя и указанием точного времени воспроизведения проблемы.

## 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 отправьте в поддержку с подробным описанием действий пользователя и указанием точного времени воспроизведения проблемы.

## 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="file" 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 отправьте в поддержку с подробным описанием действий пользователя и указанием точного времени воспроизведения проблемы.

## Сбор логов Indeed Key Server

### Включение логирования

1. Откройте с правами администратора файл *C:\inetpub\wwwroot\indeedkey\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 Key в папке *C:\inetpub\wwwroot\indeedkey\logs*.
2. Воспроизведите проблему.
3. Соберите архив с логами и отправьте в поддержку с подробным описанием действий пользователя и указанием точного времени воспроизведения проблемы.

## 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 отправьте в поддержку с подробным описанием действий пользователя и указанием точного времени воспроизведения проблемы.

## 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 отправьте в поддержку с подробным описанием действий пользователя и указанием точного времени воспроизведения проблемы.

## Сбор логов Indeed AM Mobile Device Provisioning

#### Включение логирования

1. Откройте конфигурационный файл *C:\inetpub\wwwroot\am\mdp\nlog.config*.
2. В разделе `rules`:
  - в параметре `minlevel` укажите значение `Trace`;
  - в параметре `enabled` введите значение `true`.

#### Пример

```
<rules>
  <logger name="*" writeTo="f1" minlevel="Trace" enabled="true"
/>
</rules>
```

3. Сохраните изменения.

#### Сбор логов

1. Очистите существующие логи Indeed AM Mobile Device Provisioning в папке `C:\inetpub\wwwroot\am\mdp\logs`.
2. Воспроизведите проблему.
3. Соберите архив с логами и отправьте в поддержку с подробным описанием действий пользователя и указанием точного времени воспроизведения проблемы.

## Сбор логов кеш-сервера Indeed AM

### ❗ ИНФОРМАЦИЯ

Сбор логов кеш-сервера выполняется на клиентских машинах с установленными компонентами 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 64-разрядных машин или `C:\Program Files\Common Files\Indeed-Id\AM\CacheServer\NLog.config` для 86-разрядных машин.
2. Для тегов `logger` в параметре `enabled` установите `true`.

#### Пример

```

<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 кеш-сервера в папке *C:\Windows\System32\LogFiles\Indeed-ID Cache*.
2. Воспроизведите проблему.
3. Соберите архив с логами и отправьте в поддержку с подробным описанием действий пользователя и указанием точного времени воспроизведения проблемы.

## 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="file" 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 отправьте в поддержку с подробным описанием действий пользователя и указанием точного времени воспроизведения проблемы.

## Сбор логов Telegram Service

#### Включение логирования

1. Откройте с правами администратора файл *C:\Program Files (x86)\Indeed-Id\Indeed-Id Telegram Service\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" encoding="Unicode"
enabled="true">
  </logger>
</rules>
```

3. Сохраните изменения в файле и перезапустите службу Telegram Service.



## Сбор логов

1. Очистите существующие логи Telegram Service в папке *C:\Program Files (x86)\Indeed-Id\Indeed-Id Telegram Service\Logs*.
2. Воспроизведите проблему.
3. Соберите архив с логами и отправьте в поддержку с подробным описанием действий пользователя и указанием точного времени воспроизведения проблемы.

# База знаний

В **базе знаний** вы можете найти ответы на часто задаваемые вопросы, познакомиться с примерами внедрения Access Manager с бизнес-приложениями, оставить запрос на доработку, отправить заявку в службу поддержки.

Главы базы знаний разделены по версиям продукта Access Manager:

- [Access Manager 8](#),
- [Access Manager 7](#),
- [Access Manager 6](#).

В базе знаний для Access Manager 8 вы найдете:

- [ответы на общие технические вопросы](#);
- [решения проблем, возникающих при эксплуатации продукта](#);
- [примеры интеграции Access Manager 8 с бизнес-приложениями](#);
- [ответы на вопросы про Indeed Windows Logon](#).

# Техническая поддержка

Если вы не нашли ответ на ваш вопрос в документации или **базе знаний**, вы можете обратиться за помощью в службу поддержки.

Если вы обращаетесь в поддержку для решения проблемы, предоставьте как можно больше информации, включая файлы, скриншоты, логи. Это поможет решить проблему оперативно.

Чтобы отправить обращение в поддержку, выполните следующее:

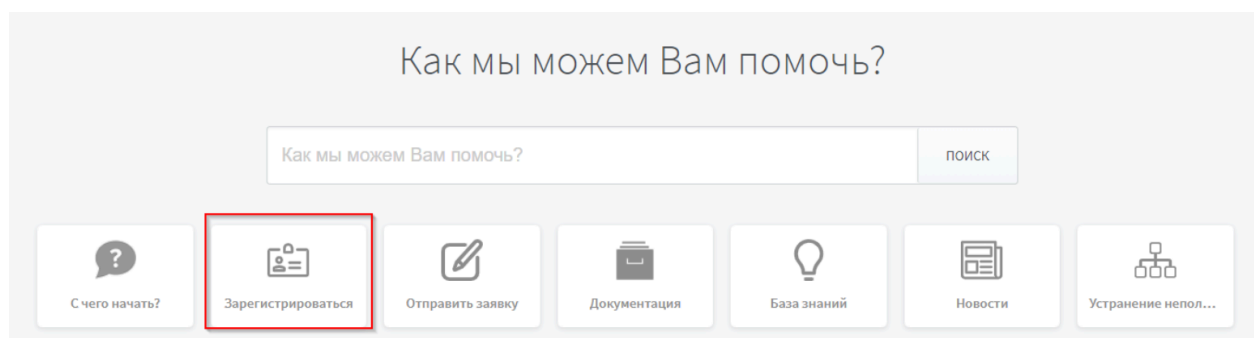
1. Откройте **портал технической поддержки**.
2. Введите ваш электронный адрес и пароль и нажмите Вход.

## ▼ Если у вас нет логина и пароля

Вы можете зарегистрироваться на портале поддержки самостоятельно или отправить заявку на регистрацию.

Чтобы зарегистрироваться самостоятельно:

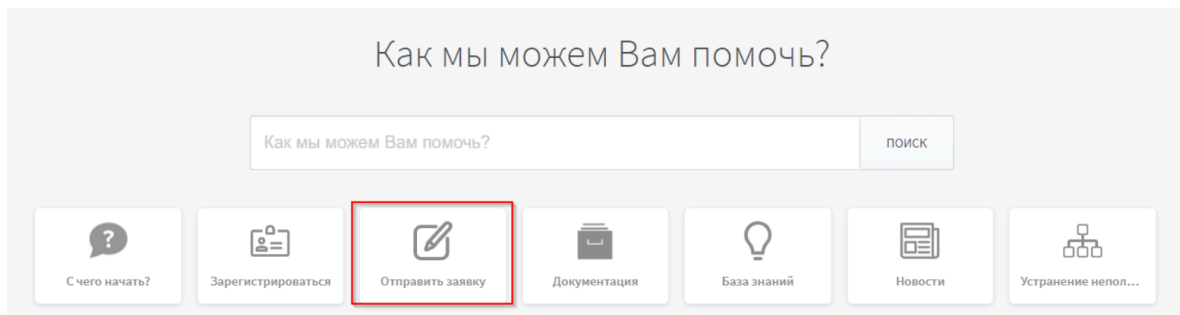
1. Нажмите Зарегистрироваться.



2. Откроется форма регистрации. Заполните поля и нажмите Зарегистрироваться.
3. На указанный электронный адрес вы получите письмо со ссылкой для активации аккаунта. Пройдите по ссылке.

Чтобы отправить заявку на регистрацию

1. Нажмите Отправить заявку.



2. Откроется форма заявки. Укажите, что это заявка на создание учетной записи.
3. На указанный электронный адрес вы получите письмо со ссылкой для активации аккаунта. Пройдите по ссылке.

3. Нажмите Отправить заявку.
4. Выберите департамент и нажмите Вперед.

5. Заполните форму заявки и нажмите Отправить.

Также вы можете связаться с командой поддержки по следующим телефонам:

- 8 800 333 09-06,
- +7 (495) 640 06-09,
- +7 (812) 640 06-09.

# История версий

В этом разделе содержится краткое описание изменений и улучшений в продукте Indeed Access Manager по версиям.

## 8.2.9–8.2.11

Минорные улучшения и исправления ошибок.

## 8.2.8

- Оптимизирована работа Management Console версии Access Manager 8 на базе данных Access Manager 9.
- Для провайдера SMS OTP устранены ошибки при работе со шлюзом МегаФон.
- Для провайдера Secured TOTP добавлена поддержка кеширования.
- Устранен дефект, препятствовавший успешной установке Windows Logon при отсутствии интернета.
- Исправлена ошибка при регистрации и смене пароля Active Directory в User Console.

## 8.2.7

- Обновлен состав дистрибутива (Indeed AM Telegram Provider).
- Устранены ошибки в подписях некоторых MSI-пакетов.

## 8.2.6

- Появилась возможность отправки OTP с помощью скрипта через веб-приложение **Messages Proxy**.
- Для провайдера Windows Password добавлен функционал, позволяющий настроить способ **проверки учетных данных** на контроллере домена.
- В Radius Extension появилась возможность записывать цепочку провайдеров в одну строку – **One-string authenticator**.
- Добавлен новый способ аутентификации для Radius – Passcode + SMS.
- Добавлена поддержка Secured TOTP в Windows Logon и RDP Windows Logon.

- Появилась настройка, с помощью которой можно поменять ссылку (диплинк) на регистрацию **Indeed Key** и **Secured TOTP** и скачивание приложения Indeed Key.
- Изменен процесс **регистрации аутентификатора Indeed Key по ссылке** из письма.
- Появилась возможность копировать в буфер обмена шестизначный код из мобильного приложения Indeed Key.
- Изменен формат времени начала и окончания срока действия лицензии.
- Оптимизирована установка MSI-пакетов в изолированной среде.
- Расширены возможности взаимодействия приложений по протоколу OpenID Connect.

## 8.2.4

- Добавлена утилита, с помощью которой можно генерировать ключи для шифрования токена пользователя при **ручной настройке** Indeed AM Core Server.
- В политики добавлена функциональность, с помощью которой можно **искать и удалять объекты из области действия**.
- Добавлена поддержка политики безопасности Windows «**Интерактивный вход в систему: поведение при извлечении смарт-карты**» в многофакторной аутентификации, где в качестве второго фактора используются смарт-карты.
- Оптимизирована работа Indeed AM NPS Radius Extension при включенном логировании.
- Устранена ошибка в работе повторных аутентификаций через Indeed AM NPS Radius Extension.

## 8.2.3

- Добавлена поддержка устройства **Рутокен**, с помощью которого можно получать одноразовые пароли.
- Устранена ошибка аутентификации, которая возникала из-за того, что поиск пользователя в каталоге занимал много времени.
- Устранено несколько ошибок в работе дубликатов запросов в NPS Radius Extension.
- Устранена ошибка аутентификации в NPS Radius Extension, при которой было невозможно выполнить вход через Remote Desktop Gateway (RDG) по двухфакторной аутентификации.
- Устранена ошибка в NPS Radius Extension, при которой время ожидания запроса второго фактора аутентификации всегда было разным.

# Справочник



## Журнал событий

Список событий Indeed AM Server и Indeed Key Server



## Роли

Права доступа администратора, оператора и инспектора



# Журнал событий

Данный раздел содержит списки событий **Indeed AM Server** и **Indeed Key Server**.

## События Indeed AM Server

В Indeed AM ведется учет событий следующих типов:

- **информация** (информационное сообщение, нет проблем или ошибок),
- **ошибка** (проблемы или ошибки, которые требуют вмешательства пользователя),
- **предупреждение** (возможны проблемы или ошибки).

## Информация

| Код  | Текст сообщения                                                               | Атрибуты события                                                                                                |
|------|-------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| 1000 | Пользователь был аутентифицирован по предоставленному аутентификатору.        | Приложение, Пользователь, Компьютер, Способ аутентификации, Комментарий аутентификатора.                        |
| 1001 | Сервер Indeed-Id был запущен.                                                 | Компьютер.                                                                                                      |
| 1002 | Сервер Indeed-Id был остановлен.                                              | Компьютер.                                                                                                      |
| 1003 | Пользователь был идентифицирован по предоставленному способу аутентификации.  | Приложение, Пользователь, Компьютер, Способ аутентификации.                                                     |
| 1004 | Аутентификатор для целевого пользователя был зарегистрирован администратором. | Приложение, Целевой пользователь, Администратор, Компьютер, Способ аутентификации, Комментарий аутентификатора. |

| Код  | Текст сообщения                                                                                                                     | Атрибуты события                                                                 |
|------|-------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| 1005 | Настройка 'Максимальное количество аутентификаторов' для целевого пользователя была изменена администратором.                       | Администратор, Компьютер, Целевой пользователь, Старое значение, Новое значение. |
| 1006 | Настройка 'Право на регистрацию аутентификатора' для целевого пользователя была изменена администратором.                           | Администратор, Компьютер, Целевой пользователь, Старое значение, Новое значение. |
| 1007 | Настройка 'Право на изменение аутентификатора' для целевого пользователя была изменена администратором.                             | Администратор, Компьютер, Целевой пользователь, Старое значение, Новое значение. |
| 1008 | Настройка 'Право на удаление аутентификатора' для целевого пользователя была изменена администратором.                              | Администратор, Компьютер, Целевой пользователь, Старое значение, Новое значение. |
| 1009 | Настройка 'Право на изменение комментария аутентификатора при регистрации' для целевого пользователя была изменена администратором. | Администратор, Компьютер, Целевой пользователь, Старое значение, Новое значение. |
| 1010 | Настройка 'Право на изменение комментария аутентификатора' для целевого пользователя была изменена администратором                  | Администратор, Компьютер, Целевой пользователь, Старое значение, Новое значение. |
| 1011 | Настройка 'Кэширование данных начиная с' для целевого пользователя была изменена администратором.                                   | Администратор, Компьютер, Целевой пользователь, Старое значение, Новое значение. |

| Код  | Текст сообщения                                                                                            | Атрибуты события                                                                           |
|------|------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| 1012 | Настройка 'Кэширование данных вплоть до' для целевого пользователя была изменена администратором.          | Администратор, Компьютер, Целевой пользователь, Старое значение, Новое значение.           |
| 1014 | Настройка 'Кэширование данных в период' для целевого пользователя была изменена администратором.           | Администратор, Компьютер, Целевой пользователь, Старое значение, Новое значение.           |
| 1015 | Настройка 'Начальная дата замещения пользователя' для целевого пользователя была изменена администратором. | Администратор, Компьютер, Целевой пользователь, Старое значение, Новое значение.           |
| 1016 | Настройка 'Конечная дата замещения пользователя' для целевого пользователя была изменена администратором.  | Администратор, Компьютер, Целевой пользователь, Старое значение, Новое значение.           |
| 1017 | Настройка 'Список заместителей' для целевого пользователя была изменена администратором.                   | Администратор, Компьютер, Целевой пользователь, Старое значение, Новое значение.           |
| 1018 | Настройка 'Разрешить кэширование' для целевого пользователя была изменена администратором.                 | Администратор, Компьютер, Целевой пользователь, Старое значение, Новое значение.           |
| 1019 | Настройка 'Разрешить замещение' для целевого пользователя была изменена администратором.                   | Администратор, Компьютер, Целевой пользователь, Старое значение, Новое значение.           |
| 1020 | Лицензия была выдана целевому объекту каталога администратором.                                            | Компьютер, Администратор, Идентификатор приложения, Целевой объект каталога, Тип лицензии. |

| Код  | Текст сообщения                                                                | Атрибуты события                                                                                                                                          |
|------|--------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1021 | Лицензия была добавлена пользователем.                                         | Идентификатор лицензии, Дата начала, Дата окончания, Количество, Описание, Пользователь, Компьютер.                                                       |
| 1022 | Лицензия была удалена пользователем.                                           | Идентификатор лицензии, Дата начала, Дата окончания, Количество, Описание, Пользователь, Компьютер.                                                       |
| 1023 | Лицензия целевого объекта каталога была удалена администратором.               | Идентификатор лицензии, Компьютер, Администратор, Идентификатор приложения, Целевой объект каталога, Тип лицензии.                                        |
| 1024 | Аутентификатор целевого пользователя был изменен администратором.              | Приложение, Целевой пользователь, Администратор, Компьютер, Способ аутентификации, Комментарий аутентификатора.                                           |
| 1025 | Комментарий аутентификатора целевого пользователя был изменен администратором. | Приложение, Целевой пользователь, Администратор, Компьютер, Способ аутентификации, Старый комментарий аутентификатора, Новый комментарий аутентификатора. |
| 1026 | Аутентификатор целевого пользователя был удален администратором.               | Приложение, Целевой пользователь, Администратор, Компьютер, Способ аутентификации, Комментарий аутентификатора.                                           |
| 1027 | Лицензия целевого пользователя была удалена сервером.                          | Идентификатор лицензии, Идентификатор приложения, Целевой пользователь.                                                                                   |

| Код  | Текст сообщения                                                                               | Атрибуты события                                                                                                           |
|------|-----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| 1028 | 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. |
| 1029 | 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. |
| 1030 | Устройство было добавлено пользователем.                                                      | Приложение, Пользователь, Компьютер, Устройство, Комментарий, Серийный номер.                                              |
| 1031 | Устройство было удалено пользователем.                                                        | Приложение, Пользователь, Компьютер, Устройство, Комментарий, Серийный номер, Идентификатор устройства.                    |
| 1032 | Способ аутентификации для целевого пользователя был запрещен администратором.                 | Приложение, Администратор, Компьютер, Целевой пользователь, Способ аутентификации.                                         |
| 1033 | Способ аутентификации для целевого пользователя был разрешен администратором.                 | Приложение, Администратор, Компьютер, Целевой пользователь, Способ аутентификации.                                         |
| 1034 | Аутентификатор целевого пользователя был заблокирован администратором.                        | Приложение, Администратор, Компьютер, Целевой пользователь, Способ аутентификации, Комментарий аутентификатора.            |
| 1035 | Аутентификатор целевого пользователя был разблокирован администратором.                       | Приложение, Администратор, Компьютер, Целевой пользователь, Способ аутентификации, Комментарий аутентификатора.            |

| Код  | Текст сообщения                                                                    | Атрибуты события                                                                                                                   |
|------|------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| 1036 | Способ аутентификации был заблокирован пользователем.                              | Приложение, Пользователь, Компьютер, Способ аутентификации.                                                                        |
| 1037 | Способ аутентификации для целевого пользователя был разблокирован администратором. | Приложение, Администратор, Компьютер, Целевой пользователь, Способ аутентификации.                                                 |
| 1038 | SMS-сообщение отправлено пользователем.                                            | Приложение, Инициатор, Компьютер, Способ аутентификации, Телефон, Время отправки, Параметры отправки, Идентификатор сообщения.     |
| 1039 | Email-сообщение отправлено пользователем.                                          | Приложение, Пользователь, Компьютер, Способ аутентификации, Email.                                                                 |
| 1040 | Часть каталогов сервера недоступна.                                                | Компьютер, Описание ошибки.                                                                                                        |
| 1041 | Аутентификатор был изменен пользователем.                                          | Приложение, Пользователь, Компьютер, Способ аутентификации, Комментарий аутентификатора.                                           |
| 1042 | Аутентификатор был зарегистрирован пользователем.                                  | Приложение, Пользователь, Компьютер, Способ аутентификации, Комментарий аутентификатора.                                           |
| 1043 | Комментарий аутентификатора был изменен пользователем.                             | Приложение, Пользователь, Компьютер, Способ аутентификации, Старый комментарий аутентификатора, Новый комментарий аутентификатора. |
| 1044 | Аутентификатор был удален пользователем.                                           | Приложение, Пользователь, Компьютер, Способ аутентификации, Комментарий аутентификатора.                                           |

| Код  | Текст сообщения                                                    | Атрибуты события                                                                                                              |
|------|--------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| 1045 | Аутентификатор целевого пользователя был отключен администратором. | Приложение, Администратор, Компьютер, Целевой пользователь, Способ аутентификации, Комментарий аутентификатора.               |
| 1046 | Аутентификатор целевого пользователя был включен администратором.  | Приложение, Администратор, Компьютер, Целевой пользователь, Способ аутентификации, Комментарий аутентификатора.               |
| 1047 | Лицензия целевого объекта каталога была удалена администратором.   | Компьютер, Администратор, Идентификатор приложения, Целевой объект каталога, Тип лицензии.                                    |
| 1048 | Лицензия была добавлена пользователем.                             | Идентификатор лицензии, Дата начала, Дата окончания, Количество, Описание, Пользователь, Компьютер, Идентификатор приложения. |
| 1049 | Лицензия была удалена пользователем.                               | Идентификатор лицензии, Дата начала, Дата окончания, Количество, Описание, Пользователь, Компьютер, Идентификатор приложения. |
| 1050 | Лицензия целевого пользователя была удалена сервером.              | Идентификатор приложения, Целевой пользователь.                                                                               |
| 1051 | Политика успешно создана.                                          | Идентификатор, Имя, Описание, Приоритет, Новые объекты каталога, Новые приложения, Приложение, Инициатор, Компьютер.          |

| Код  | Текст сообщения                                                         | Атрибуты события                                                                                                                                                       |
|------|-------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1052 | Политика удалена.                                                       | Идентификатор, Имя, Описание, Приоритет, Удаленные объекты каталога, Удаленные приложения, Приложение, Инициатор, Компьютер.                                           |
| 1053 | Политика изменена.                                                      | Идентификатор, Имя, Описание, Приоритет, Новые объекты каталога, Новые приложения, Удаленные объекты каталога, Удаленные приложения, Приложение, Инициатор, Компьютер. |
| 1054 | Пароль пользователя был успешно синхронизирован.                        | Инициатор, Компьютер, Клиентский пользователь, Клиентский компьютер.                                                                                                   |
| 1055 | Пользователь успешно выполнил вход по предоставленному паролю.          | Инициатор, Компьютер, Клиентский пользователь, Клиентский компьютер.                                                                                                   |
| 1056 | Пользователь успешно выполнил вход по кэшированному аутентификатору.    | Инициатор, Способ входа, Комментарий аутентификатора, Компьютер, Клиентский пользователь, Клиентский компьютер.                                                        |
| 1057 | Пользователь успешно выполнил вход по предоставленному аутентификатору. | Инициатор, Способ входа, Комментарий аутентификатора, Компьютер, Клиентский пользователь, Клиентский компьютер.                                                        |
| 1058 | Пользователь убрал устройство входа. Сессия завершена.                  | Инициатор, Комментарий аутентификатора, Компьютер, Клиентский пользователь, Клиентский компьютер.                                                                      |
| 1059 | Пользователь вышел из системы.                                          | Инициатор, Комментарий аутентификатора, Компьютер, Клиентский пользователь, Клиентский компьютер.                                                                      |



| Код  | Текст сообщения                                                                 | Атрибуты события                                                                                                      |
|------|---------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| 1060 | Пользователь убрал устройство входа.<br>Компьютер заблокирован.                 | Инициатор, Комментарий<br>аутентификатора, Компьютер, Клиентский<br>пользователь, Клиентский компьютер.               |
| 1061 | Пользователь заблокировал компьютер.                                            | Инициатор, Комментарий<br>аутентификатора, Компьютер, Клиентский<br>пользователь, Клиентский компьютер.               |
| 1062 | Пользователь разблокировал<br>компьютер по предоставленному<br>паролю.          | Инициатор, Компьютер, Клиентский<br>пользователь, Клиентский компьютер.                                               |
| 1063 | Пользователь разблокировал<br>компьютер по кэшированному<br>аутентификатору.    | Инициатор, Способ входа, Комментарий<br>аутентификатора, Компьютер, Клиентский<br>пользователь, Клиентский компьютер. |
| 1064 | Пользователь разблокировал<br>компьютер по предоставленному<br>аутентификатору. | Инициатор, Способ входа, Комментарий<br>аутентификатора, Компьютер, Клиентский<br>пользователь, Клиентский компьютер. |
| 1065 | Пользователь снова подключился к<br>своему терминальному сеансу.                | Инициатор, Комментарий<br>аутентификатора, Компьютер, Клиентский<br>пользователь, Клиентский компьютер.               |
| 1067 | Пароль пользователя был успешно<br>сменен автоматически.                        | Инициатор, Компьютер, Клиентский<br>пользователь, Клиентский компьютер.                                               |
| 1068 | Пароль пользователя был успешно<br>сменен.                                      | Инициатор, Компьютер, Клиентский<br>пользователь, Клиентский компьютер.                                               |
| 1069 | Пароль пользователя<br>рассинхронизирован.                                      | Инициатор, Компьютер, Клиентский<br>пользователь, Клиентский компьютер.                                               |
| 1070 | Пользователь был аутентифицирован<br>для целевого приложения.                   | Приложение, Инициатор, Компьютер,<br>Целевой пользователь.                                                            |

| Код  | Текст сообщения                                     | Атрибуты события                                                                                                                                                                                                                                                                        |
|------|-----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1073 | Изменение настроек метода аутентификации:           | Приложение, Инициатор, Компьютер, Провайдер, Настройки.                                                                                                                                                                                                                                 |
| 1076 | Изменение настройки прав аутентификатора - Успешно: | Политика, Пользователь, Обучение, Переобучение, Удаление, Изменение комментария только при обучении, Изменение комментария, Приложение, Инициатор, Компьютер.                                                                                                                           |
| 1077 | Создание настройки учетной 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. |
| 1078 | Удаление настройки учетной 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. |
| 1079 | Изменение настройки учетной 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. |

| Код  | Текст сообщения                                                             | Атрибуты события                                                                                             |
|------|-----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| 1082 | Изменение настроек метода аутентификации для пользователя:                  | Целевой пользователь, Провайдер, Приложение, Инициатор, Компьютер, Настройки.                                |
| 1085 | Изменение настроек метода аутентификации для модуля:                        | Модуль, Провайдер, Политика, Id политики, Приложение, Инициатор, Компьютер, Настройки.                       |
| 1086 | Настройки кэширования данных пользователя были успешно изменены:            | Целевое приложение, Целевой пользователь, Старые значения, Новые значения, Приложение, Инициатор, Компьютер. |
| 1087 | Настройки кэширования данных пользователя в политике были успешно изменены: | Целевое приложение, Политика, Старые значения, Новые значения, Приложение, Инициатор, Компьютер.             |
| 1088 | Телефонный номер успешно зарегистрирован.                                   | Пользователь, Инициатор, Пользователь API, Телефон.                                                          |
| 1089 | Телефонный номер успешно изменен.                                           | Пользователь, Инициатор, Пользователь API, Телефон.                                                          |
| 1090 | Телефонный номер успешно удален.                                            | Пользователь, Инициатор, Пользователь API.                                                                   |
| 1091 | Пароль пользователя был успешно сменен автоматически.                       | Целевой пользователь, Приложение, Инициатор, Компьютер.                                                      |
| 1092 | Пароль пользователя был успешно сменен.                                     | Целевой пользователь, Приложение, Инициатор, Компьютер.                                                      |
| 1093 | Изменение политики метода аутентификации:                                   | Провайдер, Политика, Id политики, Приложение, Инициатор, Компьютер, Настройки.                               |

| Код  | Текст сообщения                                                                                                                                                                                          | Атрибуты события                                                                                                       |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| 1094 | Сервис отзыва лицензий завершил работу. Завершен отзыв лицензий в связи с удалением пользователя, политики, приложения политики или исключением пользователя из политики в которой была выдана лицензия. | Отозвано лицензий, Не удалось отозвать.                                                                                |
| 1095 | Лицензия целевого пользователя была удалена сервером в связи с превышением периода неактивности пользователя.                                                                                            | Идентификатор приложения, Целевой пользователь.                                                                        |
| 1096 | Сервис отзыва лицензий завершил работу. Завершен отзыв лицензий в связи с неактивностью пользователей.                                                                                                   | Отозвано лицензий, Не удалось отозвать.                                                                                |
| 1097 | Indeed-Id ESSO Agent успешно инициализировался и начал работу                                                                                                                                            | Инициатор, Компьютер, Идентификатор процесса, Компьютер.                                                               |
| 1098 | Indeed-Id ESSO Agent завершает работу                                                                                                                                                                    | Инициатор, Компьютер, Идентификатор процесса, Компьютер.                                                               |
| 1099 | Приложение было принудительно завершено                                                                                                                                                                  | Инициатор, Компьютер, Описание приложения, Путь исполняемого файла приложения, Компьютер, Командная строка.            |
| 1100 | Форма приложения была принудительно закрыта                                                                                                                                                              | Инициатор, Компьютер, Описание приложения, Путь исполняемого файла приложения, Тип формы, Компьютер, Командная строка. |
| 1101 | Пользователь аутентифицировался в Indeed-Id ESSO                                                                                                                                                         | Инициатор, Компьютер, Имя пользователя, Компьютер.                                                                     |

| Код  | Текст сообщения                                                          | Атрибуты события                                                                                                                                                                                         |
|------|--------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1102 | Пользователь реаутентифицировался в Indeed-Id ESSO                       | Инициатор, Компьютер, Имя пользователя, Компьютер.                                                                                                                                                       |
| 1103 | 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, Командная строка. |
| 1104 | 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.       |
| 1105 | Добавлено сетевое подключение для пользователя Indeed-Id ESSO            | Инициатор, Компьютер, Имя пользователя, Диск подключения, Путь подключения, Компьютер.                                                                                                                   |
| 1106 | Удалено сетевое подключение для пользователя Indeed-Id ESSO              | Инициатор, Компьютер, Имя пользователя, Диск подключения, Компьютер.                                                                                                                                     |
| 1107 | Ошибка при удалении сетевого подключения для пользователя Indeed-Id ESSO | Инициатор, Компьютер, Имя пользователя, Диск подключения, Компьютер.                                                                                                                                     |
| 1108 | 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.       |

| Код  | Текст сообщения                                                      | Атрибуты события                                                                                                                                                                                   |
|------|----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1109 | Замещающий пользователь аутентифицировался в Indeed-Id ESSO          | Инициатор, Компьютер, Имя пользователя, Замещающий пользователь, Компьютер.                                                                                                                        |
| 1110 | Замещающий пользователь реаутентифицировался в Indeed-Id ESSO        | Инициатор, Компьютер, Имя пользователя, Замещающий пользователь, Компьютер.                                                                                                                        |
| 1111 | 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. |
| 1112 | Добавлено новое приложение.                                          | Название, Описание, Модуль интеграции, Приложение, Инициатор, Компьютер.                                                                                                                           |
| 1113 | Приложение удалено.                                                  | Название, Описание, Модуль интеграции, Приложение, Инициатор, Компьютер.                                                                                                                           |
| 1114 | Параметры приложения изменены.                                       | Название приложения, Описание, Список изменений, Модуль, Инициатор, Компьютер.                                                                                                                     |
| 1115 | Сообщение Telegram отправлено пользователю.                          | Модуль интеграции, Инициатор, Компьютер, Способ аутентификации.                                                                                                                                    |
| 1116 | Контакт Telegram успешно зарегистрирован.                            | Пользователь, Инициатор, Телефон.                                                                                                                                                                  |
| 1117 | Пользователь был аутентифицирован в целях формирования ПЭП.          | Ключ проверки ПЭП, Имя бизнес-приложения, Идентификатор устройства, Пользователь API, Пользователь.                                                                                                |

| Код  | Текст сообщения                                                        | Атрибуты события                                                                                                                      |
|------|------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| 1118 | Отправка сообщений пользователям возобновлена.                         | Компьютер, Способ аутентификации.                                                                                                     |
| 1119 | Пользователь был аутентифицирован на устройстве.                       | Предъявленный аутентификатор, Ключ операции, Имя бизнес-приложения, Идентификатор устройства, Метод аутентификации, Пользователь API. |
| 1120 | Пользователь был аутентифицирован для подписания ЭД.                   | Предъявленный идентификатор, Ключ проверки ПЭП, Имя бизнес-приложения, Идентификатор ЭД, Метод аутентификации, Пользователь API.      |
| 1121 | Инициирован процесс регистрации аутентификатора.                       | Приложение, Инициатор, Компьютер, Способ аутентификации.                                                                              |
| 1122 | Инициирована аутентификация пользователя.                              | Модуль интеграции, Инициатор, Компьютер, Способ аутентификации, Приложение.                                                           |
| 1123 | Пользователь успешно вывел мобильное устройство из карантина Exchange. | Инициатор, Идентификатор устройства.                                                                                                  |

## Ошибка

| Код  | Текст сообщения                                                                               | Атрибуты события                                                             | Причины возникновения                                                                                                                                                                                                            |
|------|-----------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2000 | Ошибка при попытке аутентифицировать пользователя по предоставленному способу аутентификации. | Приложение, Пользователь, Компьютер, Способ аутентификации, Описание ошибки. | Неверный аутентификатор. Аутентификатор считается неверным, если:<br>Аутентификатор указанного типа не обучен для пользователя.<br>Аутентификатор не найден в списке аутентификаторов пользователя. Хранилище данных повреждено. |
| 2001 | Ошибка при попытке запустить сервер Indeed-Id                                                 | Компьютер, Описание ошибки.                                                  | Неуспешная попытка запуска Indeed AM Server вручную. Возможные причины: Ошибка в конфигурационном файле сервера. Сервер уже запущен. Повреждено хранилище данных. Ошибка IIS.                                                    |
| 2002 | Ошибка при попытке остановить сервер Indeed-Id                                                | Компьютер, Описание ошибки.                                                  | Неуспешная попытка остановки Indeed AM Server вручную. Возможные причины: Недостаточно прав для выполнения операции. Indeed AM Server уже остановлен.                                                                            |



| Код  | Текст сообщения                                                                              | Атрибуты события                                                                                                                 | Причины возникновения                                                                                                                                                                                                                                                             |
|------|----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2003 | Ошибка при попытке идентифицировать пользователя по предоставленному способу аутентификации. | Приложение, Компьютер, Способ аутентификации, Описание ошибки.                                                                   | Неуспешная попытка идентификации пользователя по выбранному способу аутентификации.<br>Возможные причины:<br>Пользователю отключен/заблокирован выбранный способ аутентификации.<br>Аутентификатор не найден в списке аутентификаторов пользователя. Хранилище данных повреждено. |
| 2004 | 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.<br>Возможные причины:<br>Провайдер аутентификатора удален.<br>Повреждено хранилище данных. Нет прав на управление аутентификаторами.                                                                              |

| Код  | Текст сообщения                                                                  | Атрибуты события                                                                                                                                                           | Причины возникновения                                                                                                                                                                                            |
|------|----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2005 | 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.<br>Возможные причины:<br>Провайдер аутентификатора удален.<br>Повреждено хранилище данных. Нет прав на изменение аутентификатора.                  |
| 2006 | 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 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.<br>Возможные причины:<br>Ошибка в файле лицензии.<br>Сервер Indeed AM неактивен. Повреждено хранилище данных. |

| Код  | Текст сообщения                                                               | Атрибуты события                                                                              | Причины возникновения                                                                                                                                                                             |
|------|-------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2008 | 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 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 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.      |

| Код  | Текст сообщения                                                                                                            | Атрибуты события                                                                                  | Причины возникновения                                                                                                                                                                                                           |
|------|----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2011 | Ошибка при попытке сервера удалить лицензию целевого пользователя.                                                         | Идентификатор лицензии,<br>Идентификатор приложения, Целевой пользователь,<br>Описание ошибки.    | Неуспешная попытка сервера удалить лицензию целевого пользователя.<br>Возможные причины:<br>Лицензия уже удалена.<br>Повреждено хранилище данных.                                                                               |
| 2012 | 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.<br>Возможные причины:<br>Недостаточно прав. Сервер Indeed AM неактивен.<br>Повреждено хранилище данных. |
| 2013 | 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.<br>Возможные причины:<br>Недостаточно прав. Сервер Indeed AM неактивен.<br>Повреждено хранилище данных.     |

| Код  | Текст сообщения                                                                                                                                  | Атрибуты события                                                                                  | Причины возникновения                                                                                                                                                                                                                        |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2014 | 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 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 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. |

| Код  | Текст сообщения                                                                                                                  | Атрибуты события                                                                                  | Причины возникновения                                                                                                                                                                                                        |
|------|----------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2017 | 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 АМ неактивен. Повреждено хранилище данных. |
| 2018 | 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 АМ неактивен. Повреждено хранилище данных.                   |
| 2019 | 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 АМ неактивен. Повреждено хранилище данных.                   |

| Код  | Текст сообщения                                                                                                         | Атрибуты события                                                                                  | Причины возникновения                                                                                                                                                                                               |
|------|-------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2020 | 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 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 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.  |

| Код  | Текст сообщения                                                                                         | Атрибуты события                                                                                  | Причины возникновения                                                                                                                                                                               |
|------|---------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2023 | 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 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 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.   |



| Код  | Текст сообщения                                                                                              | Атрибуты события                                                                                                                            | Причины возникновения                                                                                                                                                                            |
|------|--------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2026 | 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 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 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.                               |

| Код  | Текст сообщения                                                                              | Атрибуты события                                                                                                                           | Причины возникновения                                                                                                                                                                                                                     |
|------|----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2029 | Ошибка при попытке пользователя удалить устройство.                                          | Приложение,<br>Пользователь,<br>Компьютер,<br>Устройство,<br>Комментарий,<br>Серийный номер,<br>Идентификатор устройства, Описание ошибки. | Неуспешная попытка при удалении устройства пользователем системы.<br>Возможные причины:<br>Устройство уже удалено.<br>Недостаточно прав. Сервер Indeed AM неактивен.<br>Повреждено хранилище данных.                                      |
| 2030 | Ошибка при попытке администратора запретить способ аутентификации для целевого пользователя. | Приложение,<br>Администратор,<br>Компьютер, Целевой пользователь, Способ аутентификации,<br>Описание ошибки.                               | Неуспешная попытка при запрете способа аутентификации для целевого пользователя администратором системы.<br>Возможные причины:<br>Данный способ уже запрещен. Недостаточно прав. Сервер Indeed AM неактивен. Повреждено хранилище данных. |
| 2031 | Ошибка при попытке администратора разрешить способ аутентификации для целевого пользователя. | Приложение,<br>Администратор,<br>Компьютер, Целевой пользователь, Способ аутентификации,<br>Описание ошибки.                               | Неуспешная попытка при разрешении способа аутентификации для целевого пользователя администратором системы.<br>Возможные причины:<br>Недостаточно прав. Сервер Indeed AM неактивен.<br>Повреждено хранилище данных.                       |

| Код  | Текст сообщения                                                                        | Атрибуты события                                                                                                                                   | Причины возникновения                                                                                                                                                                                                                           |
|------|----------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2032 | Ошибка при попытке администратора заблокировать аутентификатор целевого пользователя.  | Приложение,<br>Администратор,<br>Компьютер, Целевой объект каталога,<br>Способ аутентификации,<br>Комментарий аутентификатора,<br>Описание ошибки. | Неуспешная попытка при блокировке аутентификатора целевого пользователя администратором системы.<br>Возможные причины:<br>Аутентификатор уже заблокирован.<br>Недостаточно прав. Сервер Indeed AM неактивен.<br>Повреждено хранилище данных.    |
| 2033 | Ошибка при попытке администратора разблокировать аутентификатор целевого пользователя. | Приложение,<br>Администратор,<br>Компьютер, Целевой пользователь, Способ аутентификации,<br>Комментарий аутентификатора,<br>Описание ошибки.       | Неуспешная попытка при разблокировке аутентификатора целевого пользователя администратором системы.<br>Возможные причины:<br>Аутентификатор уже заблокирован.<br>Недостаточно прав. Сервер Indeed AM неактивен.<br>Повреждено хранилище данных. |

| Код  | Текст сообщения                                                                                   | Атрибуты события                                                                                                                                            | Причины возникновения                                                                                                                                                                                                    |
|------|---------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2034 | Ошибка при попытке пользователя заблокировать способ аутентификации.                              | Приложение,<br>Пользователь,<br>Компьютер, Способ аутентификации,<br>Описание ошибки.                                                                       | Неуспешная попытка при блокировке способа аутентификации пользователем. Возможные причины: Способ аутентификации уже заблокирован.<br>Недостаточно прав. Сервер Indeed AM неактивен.<br>Повреждено хранилище данных.     |
| 2035 | Ошибка при попытке администратора разблокировать способ аутентификации для целевого пользователя. | Приложение,<br>Администратор,<br>Компьютер, Целевой пользователь, Способ аутентификации,<br>Описание ошибки.                                                | Неуспешная попытка при разблокировке способа аутентификации пользователем. Возможные причины: Способ аутентификации уже разблокирован.<br>Недостаточно прав. Сервер Indeed AM неактивен.<br>Повреждено хранилище данных. |
| 2036 | Ошибка при попытке отправить SMS-сообщение.                                                       | Приложение,<br>Инициатор,<br>Компьютер, Способ аутентификации,<br>Телефон, Описание ошибки, Время отправки, Параметры отправки,<br>Идентификатор сообщения. | Неуспешная попытка при отправке SMS. Возможные причины: Ошибка при подключении к SMPP серверу. Не задан номер телефона.                                                                                                  |

| Код  | Текст сообщения                                            | Атрибуты события                                                                                                                                    | Причины возникновения                                                                                                                                          |
|------|------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2037 | Ошибка при попытке пользователя отправить Email-сообщение. | Приложение, Пользователь, Компьютер, Способ аутентификации, Email.                                                                                  | Неуспешная попытка при отправке Email-сообщения. Возможные причины: Ошибка при подключении к SMTP серверу. Не задан email пользователя.                        |
| 2038 | Хранилище сервера недоступно.                              | Компьютер, Описание ошибки.                                                                                                                         | Неуспешная попытка при соединении с сервером Indeed. Возможные причины: Сервер Indeed АМ неактивен. Повреждено хранилище данных.                               |
| 2039 | Каталоги сервера недоступны.                               | Компьютер, Описание ошибки.                                                                                                                         |                                                                                                                                                                |
| 2040 | Сервер не был запущен.                                     | Компьютер, Описание ошибки.                                                                                                                         | Неуспешная попытка при запуске сервера indeed. Возможные причины: Сервер Indeed АМ уже запущен. Ошибка в конфигурационном файле. Повреждено хранилище данных.  |
| 2041 | 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 АМ неактивен. Повреждено хранилище данных. |

| Код  | Текст сообщения                                                                   | Атрибуты события                                                                                                                                   | Причины возникновения                                                                                                                                                                                                        |
|------|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2042 | Ошибка при попытке пользователя зарегистрировать аутентификатор.                  | Приложение,<br>Пользователь,<br>Компьютер, Способ аутентификации,<br>Комментарий аутентификатора,<br>Описание ошибки.                              | Неуспешная попытка при регистрации аутентификатора пользователем. Возможные причины: Недостаточно прав. Сервер Indeed AM неактивен. Повреждено хранилище данных.                                                             |
| 2043 | Ошибка при попытке пользователя удалить аутентификатор.                           | Приложение,<br>Пользователь,<br>Компьютер, Способ аутентификации,<br>Комментарий аутентификатора,<br>Описание ошибки.                              | Неуспешная попытка при удалении аутентификатора пользователем. Возможные причины: Аутентификатор уже удален. Недостаточно прав. Сервер Indeed AM неактивен. Повреждено хранилище данных.                                     |
| 2044 | Ошибка при попытке администратора отключить аутентификатор целевого пользователя. | Приложение,<br>Администратор,<br>Компьютер, Целевой объект каталога,<br>Способ аутентификации,<br>Комментарий аутентификатора,<br>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. |

| Код  | Текст сообщения                                                                  | Атрибуты события                                                                                                                             | Причины возникновения                                                                                                                                                                                                      |
|------|----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2045 | Ошибка при попытке администратора включить аутентификатор целевого пользователя. | Приложение,<br>Администратор,<br>Компьютер, Целевой пользователь, Способ аутентификации,<br>Комментарий аутентификатора,<br>Описание ошибки. | Неуспешная попытка при включении аутентификатора целевого пользователя администратором системы. Возможные причины: Аутентификатор уже включен. Недостаточно прав. Сервер Indeed AM неактивен. Повреждено хранилище данных. |
| 2046 | Ошибка при попытке пользователя добавить лицензию.                               | Идентификатор лицензии,<br>Пользователь,<br>Компьютер,<br>Идентификатор приложения,<br>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 при попытке пользователя удалить лицензию.                                | Идентификатор лицензии,<br>Пользователь,<br>Компьютер,<br>Идентификатор приложения,<br>Описание ошибки.                                      | Неуспешная попытка при удалении лицензии пользователем. Возможные причины: Недостаточно прав. Сервер Indeed AM неактивен. Повреждено хранилище данных.                                                                     |
| 2048 | Ошибка при попытке сервера удалить лицензию целевого пользователя.               | Идентификатор приложения, Целевой пользователь,<br>Описание ошибки.                                                                          | Неуспешная попытка при удалении лицензии сервером.                                                                                                                                                                         |

| Код  | Текст сообщения                | Атрибуты события                                                                                                                                                               | Причины возникновения                                                                    |
|------|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| 2049 | Ошибка при создании политики.  | Идентификатор, Имя, Описание, Приоритет, Новые объекты каталога, Новые приложения, Ошибка, Приложение, Инициатор, Компьютер.                                                   | Неуспешное создание политики.                                                            |
| 2050 | Ошибка при удалении политики.  | Идентификатор, Имя, Описание, Приоритет, Удаленные объекты каталога, Удаленные приложения, Ошибка, Приложение, Инициатор, Компьютер.                                           | Неуспешное удаление политики.                                                            |
| 2051 | Ошибка при изменении политики. | Идентификатор, Имя, Описание, Приоритет, Новые объекты каталога, Новые приложения, Удаленные объекты каталога, Удаленные приложения, Ошибка, Приложение, Инициатор, Компьютер. | Неуспешное изменение политики.                                                           |
| 2052 | Сервер Indeed-Id не найден.    | Компьютер, Описание ошибки, Код ошибки.                                                                                                                                        | Ошибка при попытке подключения к серверу Indeed AM. Указан неверный URL. Проблема в DNS. |



| Код  | Текст сообщения                                             | Атрибуты события                                                                                                    | Причины возникновения                                                                                                                                                           |
|------|-------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2053 | Не удалось сменить пароль пользователя.                     | Инициатор,<br>Компьютер,<br>Клиентский<br>пользователь,<br>Клиентский<br>компьютер, Описание<br>ошибки, Код ошибки. | Неуспешная смена пароля<br>пользователя.                                                                                                                                        |
| 2054 | Не удалось сменить пароль<br>пользователя<br>автоматически. | Инициатор,<br>Компьютер,<br>Клиентский<br>пользователь,<br>Клиентский<br>компьютер, Описание<br>ошибки, Код ошибки. | Неуспешная смена пароля<br>пользователя<br>автоматически.                                                                                                                       |
| 2055 | Не удалось<br>синхронизировать пароль<br>пользователя.      | Инициатор,<br>Компьютер,<br>Клиентский<br>пользователь,<br>Клиентский<br>компьютер, Описание<br>ошибки, Код ошибки. | Ошибка синхронизации<br>доменного пароля<br>пользователя с паролем в<br>хранилище Indeed.<br>Возможные причины:<br>Сервер Indeed недоступен.<br>Повреждено хранилище<br>данных. |
| 2058 | Изменение настроек метода<br>аутентификации:                | Приложение,<br>Инициатор,<br>Компьютер,<br>Провайдер,<br>Настройки, Описание<br>ошибки.                             | Неуспешное изменение<br>настроек метода<br>аутентификации.                                                                                                                      |

| Код  | Текст сообщения                                  | Атрибуты события                                                                                                                                                                                                                                                                                | Причины возникновения                                |
|------|--------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|
| 2061 | Изменение настройки прав аутентификатора - Сбой: | Политика,<br>Пользователь,<br>Обучение,<br>Переобучение,<br>Удаление, Изменение комментария только при обучении,<br>Изменение комментария,<br>Приложение,<br>Инициатор,<br>Компьютер, Ошибка.                                                                                                   | Неуспешное изменение настройки прав аутентификатора. |
| 2062 | Ошибка создания настройки учетной 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 учетной записи         |

| Код  | Текст сообщения                              | Атрибуты события                                                                                                                                                                                                                                                                                                                                | Причины возникновения                            |
|------|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------|
| 2063 | Ошибка удаления<br>настройки учетной записи. | Политика, Целевой<br>пользователь, Роль,<br>Связанная учетная<br>запись, Приложение,<br>Имя, Пароль задан,<br>Пароль случайный,<br>Учетная запись<br>выключена, Требовать<br>аутентификацию при<br>входе, Использовать<br>учетные данные ОС,<br>Формат<br>преобразования<br>имени, Описание,<br>Приложение,<br>Инициатор,<br>Компьютер, Ошибка. | Неуспешное удаление<br>настройки учетной записи. |

| Код  | Текст сообщения                                                  | Атрибуты события                                                                                                                                                                                                                                                                                                                                | Причины возникновения                                                          |
|------|------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| 2064 | Ошибка изменения<br>настройки учетной записи.                    | Политика, Целевой<br>пользователь, Роль,<br>Связанная учетная<br>запись, Приложение,<br>Имя, Пароль задан,<br>Пароль случайный,<br>Учетная запись<br>выключена, Требовать<br>аутентификацию при<br>входе, Использовать<br>учетные данные ОС,<br>Формат<br>преобразования<br>имени, Описание,<br>Приложение,<br>Инициатор,<br>Компьютер, Ошибка. | Неуспешное изменение<br>настройки учетной записи.                              |
| 2067 | Изменение настроек метода<br>аутентификации для<br>пользователя: | Целевой пользователь,<br>Провайдер,<br>Приложение,<br>Инициатор,<br>Компьютер,<br>Настройки, Описание<br>ошибки.                                                                                                                                                                                                                                | Неуспешное изменение<br>настроек метода<br>аутентификации для<br>пользователя. |
| 2070 | Изменение настроек метода<br>аутентификации для<br>модуля:       | Модуль, Провайдер,<br>Политика, Id<br>политики,<br>Приложение,<br>Инициатор,<br>Компьютер,<br>Настройки, Описание<br>ошибки.                                                                                                                                                                                                                    | Неуспешное изменение<br>настроек метода<br>аутентификации для модуля           |

| Код  | Текст сообщения                                                                   | Атрибуты события                                                                                                              | Причины возникновения                                                                                                                                                                                                  |
|------|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2071 | Ошибка при попытке изменить настройки кэширования данных пользователя:            | Целевое приложение, Целевой пользователь, Старые значения, Новые значения, Приложение, Инициатор, Компьютер, Описание ошибки. | Неуспешная попытка изменить настройки кэширования данных пользователя. Возможные причины: Недостаточно прав для выполнения операции. Повреждено хранилище данных.                                                      |
| 2072 | Ошибка при попытке изменить настройки кэширования данных пользователя в политике: | Целевое приложение, Политика, Старые значения, Новые значения, Приложение, Инициатор, Компьютер, Описание ошибки.             | Неуспешная попытка изменить настройки кэширования данных пользователя в политике. Возможные причины: Недостаточно прав для выполнения операции. Повреждено хранилище данных.                                           |
| 2073 | Ошибка регистрации телефонного номера.                                            | Пользователь, Инициатор, Пользователь API, Описание ошибки, Инициатор ошибки, Телефон.                                        | Неуспешная попытка регистрации телефонного номера. Возможные причины: Недостаточно прав для выполнения операции. Не доступен компонент EAPhoneServer. Указан несуществующий пользователь. Повреждено хранилище данных. |

| Код  | Текст сообщения                                       | Атрибуты события                                                                                      | Причины возникновения                                                                                                                                                                                                |
|------|-------------------------------------------------------|-------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2074 | Ошибка изменения телефонного номера.                  | Пользователь,<br>Инициатор,<br>Пользователь API,<br>Описание ошибки,<br>Инициатор ошибки,<br>Телефон. | Неуспешная попытка изменения телефонного номера. Возможные причины: Недостаточно прав для выполнения операции. Не доступен компонент EAPhoneServer. Указан несуществующий пользователь. Повреждено хранилище данных. |
| 2075 | Ошибка удаления телефонного номера.                   | Пользователь,<br>Инициатор,<br>Пользователь API,<br>Описание ошибки,<br>Инициатор ошибки.             | Неуспешная попытка удаления телефонного номера. Возможные причины: Недостаточно прав для выполнения операции. Не доступен компонент EAPhoneServer. Указан несуществующий пользователь. Повреждено хранилище данных.  |
| 2076 | Не удалось сменить пароль пользователя автоматически. | Целевой пользователь,<br>Приложение,<br>Инициатор,<br>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.      |

| Код  | Текст сообщения                                                         | Атрибуты события                                                                                                                                                                                         | Причины возникновения                                                                                                                                       |
|------|-------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2077 | Не удалось сменить пароль пользователя.                                 | Целевой пользователь, Приложение, Инициатор, Компьютер, Описание ошибки.                                                                                                                                 | Неуспешная попытка смены пароля пользователем вручную (при первом входе, в окне «Безопасность Windows» после нажатия комбинации клавиш [Ctrl]+[Alt]+[Del]). |
| 2078 | Ошибка изменения политики метода аутентификации:                        | Провайдер, Политика, Id политики, Приложение, Инициатор, Компьютер, Настройки, Описание ошибки.                                                                                                          | Неуспешное изменение политики метода аутентификации.                                                                                                        |
| 2079 | Ошибка при сохранении пароля пользователя в базе данных 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 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.                    |

| Код  | Текст сообщения                                                   | Атрибуты события                                                                                                                      | Причины возникновения                                                                                                                                    |
|------|-------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2081 | Обнаружен сбой в Indeed-Id ESSO Agent                             | Инициатор,<br>Компьютер,<br>Компьютер, Описание<br>ошибки, Код ошибки.                                                                | Не удалось завершить<br>процесс приложения.                                                                                                              |
| 2082 | Ошибка при добавлении<br>сетевого подключения для<br>пользователя | Инициатор,<br>Компьютер, Имя<br>пользователя, Диск<br>подключения, Путь<br>подключения,<br>Компьютер, Описание<br>ошибки, Код ошибки. | Сетевой диск заполнен.<br>Отсутствует связь с<br>сервером Indeed.                                                                                        |
| 2083 | Ошибка при добавлении<br>нового приложения.                       | Название, Описание,<br>Модуль интеграции,<br>Приложение,<br>Инициатор,<br>Компьютер, Описание<br>ошибки.                              | Неуспешная попытка<br>добавления нового<br>приложения: Недостаточно<br>прав для выполнения<br>операции. Отсутствует<br>связь с сервером Indeed<br>AM.    |
| 2084 | Ошибка при удалении<br>приложения.                                | Название, Описание,<br>Модуль интеграции,<br>Приложение,<br>Инициатор,<br>Компьютер, Описание<br>ошибки.                              | Неуспешная попытка<br>удаления приложения:<br>Недостаточно прав для<br>выполнения операции.<br>Отсутствует связь с<br>сервером Indeed AM.                |
| 2085 | Ошибка при изменении<br>параметров приложения.                    | Название, Описание,<br>Список изменений,<br>Приложение,<br>Инициатор,<br>Компьютер, Описание<br>ошибки.                               | Неуспешная попытка<br>изменения параметров<br>приложения: Недостаточно<br>прав для выполнения<br>операции. Отсутствует<br>связь с сервером Indeed<br>AM. |



| Код  | Текст сообщения                                                             | Атрибуты события                                                                    | Причины возникновения                                                                                                                                                                                                                                                               |
|------|-----------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2086 | Не удалось доставить сообщение на центральный лог-сервер.                   | Приложение, Инициатор, Компьютер, Тип, Категория, ID сообщения, Описание.           | Неуспешная попытка отправки сообщения на центральный лог-сервер: Отсутствует связь с лог сервером Indeed AM.                                                                                                                                                                        |
| 2087 | Ошибка при попытке отправить сообщение Telegram.                            | 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 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: ReadUserAuthenticators для приложения Authenticator Management: сервисная УЗ Telegram не добавлена в глобальные администраторы Management Console. |
| 2089 | Ошибка при попытке аутентифицировать пользователя в целях формирования ПЭП. | Описание ошибки, Имя бизнес-приложения, Пользователь API, Идентификатор устройства. | Произошла ошибка аутентификации пользователя при формировании простой электронной подписи.                                                                                                                                                                                          |

| Код  | Текст сообщения                                                         | Атрибуты события                                                                                                                                             | Причины возникновения                                                                                                |
|------|-------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|
| 2090 | Обнаружена потенциальная спам-атака. Отправка сообщений приостановлена. | Компьютер, Способ аутентификации, Начало временного интервала, Конец временного интервала, Кол-во отправок, Кол-во успешных входов, Процент успешных входов. | Неуспешная попытка отправки сообщения из-за обнаружения подозрительной активности при данном способе аутентификации. |
| 2091 | Ошибка при попытке аутентифицировать пользователя на устройстве.        | Описание ошибки, Предъявленный идентификатор, Ключ операции, Имя бизнес-приложения, Идентификатор устройства, Метод аутентификации, Пользователь API.        | Неуспешный ввод кода на устройстве.                                                                                  |
| 2092 | Ошибка при попытке аутентифицировать пользователя для подписания ЭД.    | Описание ошибки, Предъявленный идентификатор, Ключ проверки ПЭП, Имя бизнес-приложения, Идентификатор ЭД, Метод аутентификации, Пользователь API.            | Неуспешная попытка входа. Возможные причины: Неверный логин. Неверный пароль.                                        |

| Код  | Текст сообщения                                                                                            | Атрибуты события                                                                         | Причины возникновения                                                              |
|------|------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| 2093 | Пользователь ввел ОТР, длина которого не совпадает с настройками провайдера аутентификации.                | Способ аутентификации, Целевой пользователь, Значение при регистрации, Текущее значение. | Несоответствие фактической длины введенного ОТР и заданной длины ОТР провайдера.   |
| 2094 | Период обновления ОТР в аутентификаторе пользователя не совпадает с настройками провайдера аутентификации. | Способ аутентификации, Целевой пользователь, Значение при регистрации, Текущее значение. | Несоответствие фактического периода обновления ОТР с заданным периодом обновления. |
| 2095 | Алгоритм ОТР в аутентификаторе пользователя не совпадает с настройками провайдера аутентификации.          | Способ аутентификации, Целевой пользователь, Значение при регистрации, Текущее значение. | Неуспешная попытка вывести устройство из карантина.                                |
| 2096 | Не удалось вывести мобильное устройство из карантина Exchange.                                             | Инициатор, Идентификатор устройства.                                                     | Несоответствие фактического алгоритма ОТР с заданным алгоритмом.                   |
| 2097 | Не удалось заблокировать мобильное устройство на сервере Exchange.                                         | Инициатор, Идентификатор устройства.                                                     | Неуспешная попытка заблокировать мобильное устройство.                             |

## Предупреждение

| Код  | Текст сообщения                                                                                             | Атрибуты события                                                                         | Причины возникновения                                                              |
|------|-------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| 3000 | Окно сравнения OTP в аутентификаторе пользователя не совпадает с настройками провайдера аутентификации.     | Способ аутентификации, Целевой пользователь, Значение при регистрации, Текущее значение. | Несоответствие фактического окна сравнения OTP с заданным окном сравнения.         |
| 3001 | Окно синхронизации OTP в аутентификаторе пользователя не совпадает с настройками провайдера аутентификации. | Способ аутентификации, Целевой пользователь, Значение при регистрации, Текущее значение. | Несоответствие фактического окна синхронизации OTP с заданным окном синхронизации. |
| 3002 | Пользователь заблокировал мобильное устройство на сервере Exchange.                                         | Инициатор, Идентификатор устройства.                                                     | Успешная попытка заблокировать устройство.                                         |

## События Indeed Key Server

### ❗ ИНФОРМАЦИЯ

Просмотр журнала событий возможен через просмотр EventLog Windows (при использовании хранилища Windows) или сторонними средствами через SQL (при использовании хранилища SQL).

| Код  | Категория  | Сервис     | Текст сообщения                                                                  |
|------|------------|------------|----------------------------------------------------------------------------------|
| 1000 | Информация | Indeed Key | Запрос на аутентификацию пользователя {userLogin} отправлен. Приложение: {appId} |
| 1001 | Информация | Indeed Key | Запрос на регистрацию пользователя {userLogin} отправлен. Приложение: {appId}    |

| Код  | Категория  | Сервис     | Текст сообщения                                                                                                                  |
|------|------------|------------|----------------------------------------------------------------------------------------------------------------------------------|
| 1002 | Информация | Indeed Key | Обработан ответ пользователя {userLogin} на запрос аутентификации. Приложение: {appId}. Результат: {state}. Сообщение: {message} |
| 1003 | Информация | Indeed Key | Запрос на установку сертификата пользователю {userLogin} отправлен. Приложение: {appId}                                          |
| 1004 | Информация | Indeed Key | Регистрация пользователя {userLogin} успешно завершена. Приложение: {appId}                                                      |
| 1005 | Информация | Indeed Key | Удаление пользователя {userLogin} успешно завершено. Приложение: {appId}                                                         |
| 2000 | Ошибка     | Indeed Key | Ошибка при отправке запроса на аутентификацию пользователя {userLogin}. Приложение: {appId}. Ошибка:                             |
| 2001 | Ошибка     | Indeed Key | Ошибка при отправке запроса на регистрацию пользователя {userLogin}. Приложение: {appId}. Ошибка:                                |
| 2002 | Ошибка     | Indeed Key | Ошибка при отправке запроса на установку сертификата пользователю {userLogin}. Приложение: {appId}. Ошибка:                      |
| 2003 | Ошибка     | Indeed Key | Ошибка при регистрации пользователя {userLogin}. Приложение: {appId}. Ошибка:                                                    |
| 2004 | Ошибка     | Indeed Key | Ошибка при удалении пользователя {userLogin}. Приложение: {appId}. Ошибка:                                                       |

# Роли

Данный раздел содержит таблицы ролей и прав следующих пользователей:

- Администратор — полный доступ ко всем функциям и настройкам системы,
- Оператор — права только на изменение настроек пользователей и устройств аутентификации,
- Инспектор — доступ на чтение всех данных и настроек системы.

## Регистрация аутентификаторов

| Операция                            | Администратор | Оператор | Инспектор |
|-------------------------------------|---------------|----------|-----------|
| Регистрация первого аутентификатора | ✓             | ✓        | ✗         |
| Регистрация любого аутентификатора  | ✓             | ✓        | ✗         |

## Аутентификаторы пользователя

| Операция                                            | Администратор | Оператор | Инспектор |
|-----------------------------------------------------|---------------|----------|-----------|
| Просмотр аутентификаторов пользователя              | ✓             | ✓        | ✓         |
| Отключение аутентификаторов пользователя            | ✓             | ✓        | ✗         |
| Включение аутентификаторов пользователя             | ✓             | ✓        | ✗         |
| Удаление аутентификаторов пользователя              | ✓             | ✓        | ✗         |
| Разблокирование методов аутентификации пользователя | ✓             | ✓        | ✗         |
| Получение методов аутентификации пользователя       | ✓             | ✓        | ✓         |

| Операция                                              | Администратор | Оператор | Инспектор |
|-------------------------------------------------------|---------------|----------|-----------|
| 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

| Операция                             | Администратор | Оператор | Инспектор |
|--------------------------------------|---------------|----------|-----------|
| Регистрация лицензий                 | ✓             | ✗        | ✗         |
| Отмена регистрации лицензий          | ✓             | ✗        | ✗         |
| Просмотр зарегистрированных лицензий | ✓             | ✓        | ✓         |
| Выдача лицензий пользователю         | ✓             | ✓        | ✗         |
| Отзыв лицензии у пользователя        | ✓             | ✓        | ✗         |
| Просмотр лицензий пользователя       | ✓             | ✓        | ✓         |

## Административный доступ

| Операция                                     | Администратор | Оператор | Инспектор |
|----------------------------------------------|---------------|----------|-----------|
| Добавление объекта каталога в группу доступа | ✓             | ✗        | ✗         |
| Удаление объекта каталога из группы доступа  | ✓             | ✗        | ✗         |
| Просмотр членов группы доступа               | ✓             | ✓        | ✓         |

## Устройства аутентификации

| Операция               | Администратор | Оператор | Инспектор |
|------------------------|---------------|----------|-----------|
| Регистрация устройства | ✓             | ✗        | ✗         |
| Обновление устройства  | ✓             | ✗        | ✗         |



| Операция                  | Администратор | Оператор | Инспектор |
|---------------------------|---------------|----------|-----------|
| Просмотр списка устройств | ✓             | ✓        | ✓         |
| Удаление устройства       | ✓             | ✗        | ✗         |

## Политики

| Операция                                | Администратор | Оператор | Инспектор |
|-----------------------------------------|---------------|----------|-----------|
| 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           | ✓             | ✗        | ✗         |

## Кеширование данных пользователя на ПК

| Операция                       | Администратор | Оператор | Инспектор |
|--------------------------------|---------------|----------|-----------|
| Включение кеширования          | ✓             | ✓        | ✗         |
| Отключение кеширования         | ✓             | ✓        | ✗         |
| Проверка состояния кеша        | ✓             | ✓        | ✗         |
| Изменение настроек кеширования | ✓             | ✗        | ✗         |
| Просмотр настроек кеширования  | ✓             | ✓        | ✓         |

## Учетные записи ESSO

| Операция                                        | Администратор | Оператор | Инспектор |
|-------------------------------------------------|---------------|----------|-----------|
| Добавление учетной записи                       | ✓             | ✗        | ✗         |
| Удаление учетной записи                         | ✓             | ✗        | ✗         |
| Просмотр учетных записей пользователя           | ✓             | ✓        | ✓         |
| Чтение состояния учетных записей пользователя   | ✓             | ✓        | ✗         |
| Изменение пароля учетных записей пользователя   | ✓             | ✗        | ✗         |
| Просмотр состояния пароля аккаунта пользователя | ✓             | ✓        | ✓         |
| Изменение имени учетной записи пользователя     | ✓             | ✓        | ✗         |

| Операция                                                    | Администратор | Оператор | Инспектор |
|-------------------------------------------------------------|---------------|----------|-----------|
| 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

| Операция                          | Администратор | Оператор | Инспектор |
|-----------------------------------|---------------|----------|-----------|
| Просмотр списка бизнес-приложений | ✓             | ✓        | ✓         |
| Создание бизнес-приложения        | ✓             | ✗        | ✗         |
| Изменение бизнес-приложения       | ✓             | ✓        | ✗         |
| Удаление бизнес-приложения        | ✓             | ✗        | ✗         |