Требования Indeed AM AirKey Cloud Server

Информация

Сервер поддерживает работу вне домена.

Программные требования

Операционная система:

- Windows Server 2012/2012 R2 x64
- Windows Server 2016 x64
- Windows Server 2019 x64

Internet Information Services 7.0 и выше со следующими модулями:

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

Компоненты Microsoft:

- Microsoft .NET Framework 4.5.2

Microsoft SQL Server:

- Microsoft SQL Server 2012 SP2 всех редакций
- Microsoft SQL Server 2014 всех редакций
- Microsoft SQL Server 2016 всех редакций

Аппаратные требования

- Не менее 8 ГБ оперативной памяти
- Не менее 200 ГБ свободного дискового пространства
- Аппаратные требования совпадают с требованиями, предъявляемыми к операционным системам, на которых функционирует ПО
- Для отправки Push-уведомлений серверу AirKey Cloud требуется внешний доступ к интернету (Для доступа к **fcm.googleapis.com:443**).
- Сервер AirKey Cloud должен быть доступен, по указанному в настройках **dns имени** и **порту,** (Данные параметры задаются при настройке Indeed AK Cloud Server) из внешней сети.

  Информация

  Рекомендуется использовать отличные от 80 и 443 порты. Данные порты используются по умолчанию для приложений IIS.
- DNS имя сервера AirKey Cloud не должно содержать символов нижнего подчеркивания "_".

Требование к сертификатам для iOS устройств

Информация

Сертификат должен быть на устройстве и должно быть доверие со стороны смартфона к внешнему DNS имени сервера Indeed AirKey.

Информация

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

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