Indeed AM

Indeed Certificate Manager может быть интегрирован с продуктами компании Индид – Indeed Access Manager и Indeed AM Enterprise Single Sign-On. Интеграция позволит объединить операции выпуска устройства, запроса сертификата, записи сертификата и регистрации аутентификатора в единый процесс.

Выпущенное подобным образом устройство может быть использовано пользователем как для аутентификации в домене и SSO-приложениях, так и для цифровой подписи или доступа к ресурсам, требующих наличие персональных сертификатов. Интеграция между системами возможна на любом этапе, независимо от того, какой из продуктов был развернут раньше.

Настройка интеграции систем Indeed CM и Indeed AM состоит из двух этапов:

- Установка и настройка необходимого ПО
- Конфигурирование параметров интеграции

На первом этапе необходимо выполнить установку следующих компонентов:

- **Indeed Administration Tools** (или Indeed Admin Pack) на каждый сервер Indeed CM
- **Indeed Extended Security Provider** на каждый сервер Indeed AM
- **Indeed SmartCard + PIN Provider** на каждый сервер Indeed AM

> **Indeed Administration Tools** поставляется в дистрибутиве системы Indeed Access Manager.
> **Indeed Extended Security Provider** и **Indeed SmartCard + PIN Provider** поставляется по запросу **службой технической поддержки компании Indeed Identity**.

А также выполнить настройку Extended Security Provider:

- Создать группу безопасности Indeed-ID Enrollment Admins согласно Руководству по установке и эксплуатации Indeed Extended Security Provider.
- Добавить сервисную учетную запись (‘**servicecm**’) в группы безопасности Indeed-ID User Admins и Indeed-ID Enrollment Admins.

На втором этапе необходимо задать параметры интеграции в политике использования устройств в Indeed Certificate Manager. Перейдите в раздел **Indeed AM** в конфигурации выбранной политики и определите параметры работы с Indeed AM (Таблица 3).

Таблица 3 – Параметры интеграции с Indeed AM.

Параметр	Описание
Включить интеграцию с Indeed AM	Если опция включена, то при выпуске устройства в системе Indeed CM будет выпускаться и аутентификатор «Смарт-карта или USB-ключ + PIN» в системе Indeed AM.
Использовать прокси-сервер Indeed AM	Если опция включена, то Indeed CM будет обращаться к прокси-серверу Indeed AM, который направит запрос на серверы Indeed AM. Использование прокси-сервера необходимо, если серверы Indeed CM располагаются за пределами домена, в котором установлена система Indeed AM.
URL-адрес прокси-сервера	Адрес, по которому доступен Indeed AM Proxy Server.
Имя пользователя Пароль	Учетные данные пользователя (логин и доменный пароль), входящего в группы безопасности Indeed-ID User Admins и Indeed-ID Enrollment Admins.
Разрешить использование Indeed AM Windows Logon	Если опция включена, то при выпуске устройства в Indeed CM пользователю будет разрешено использование технологии Indeed для аутентификации в домене при помощи компонента Indeed AM Windows Logon.
Разрешить использование Indeed AM Enterprise Single Sign-On	Если опция включена, то при выпуске устройства в Indeed CM пользователю будет разрешено использование технологии Indeed для аутентификации в приложениях при помощи компонента Indeed AM Enterprise SSO Agent.
Генерировать случайный пароль учетной записи Windows	Если опция включена, то при выпуске устройства в Indeed CM для пользователя будет установлена опция генерации случайного доменного пароля. В этом случае при истечении срока действия пароля новый пароль будет сгенерирован случайным образом и будет известен только системе Indeed AM.

Разрешения на использование Indeed AM Windows Logon, Indeed AM Enterprise Single Sign-On и генерацию случайного пароля будут выключены в случае удаления последнего зарегистрированного аутентификатора пользователя.

Например:

Если у пользователя не было ни одного аутентификатора в системе Indeed AM и ни одного устройства в системе Indeed CM, то после выпуска устройства с настроенными параметрами интеграции у пользователя появится один аутентификатор («Смарт-карта или USB-ключ + PIN») в системе Indeed AM и одно устройство (например, eToken) в системе Indeed CM.

В случае удаления устройства в Indeed CM, удалится и аутентификатор в Indeed AM, а если других обученных аутентификаторов нет, отключатся и разрешения на использование Indeed AM Windows Logon, Indeed AM Enterprise Single Sign-On и генерация случайного пароля (если хотя бы одна из этих опций была активна на момент отзыва).