Установка серверных компонентов

Система Indeed Certificate Manager доступна к установке на ОС Windows и Linux и состоит из набора сервисов:

- Установка сервера на ОС Windows
  - Установка сервера
  - Аутентификация Windows
  - Настройка аутентификации веб-приложений пользователей
  - Настройка SSL/TLS для веб-приложения
- Установка сервера на ОС Linux
  - Установка сервера
  - Управление веб-приложениями
  - Настройка SSL/TLS для веб-приложения

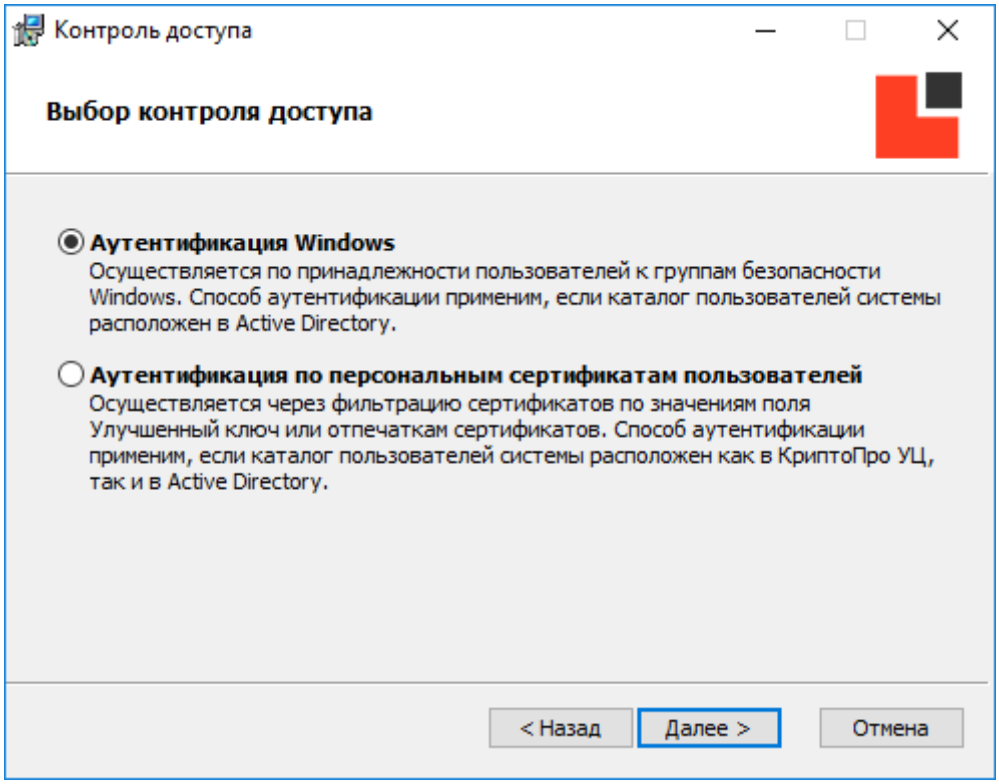
- **Консоль управления** (Management Console) – веб-приложение **mc**.
- **Сервис самообслуживания** (Self-Service) – веб-приложение **ss**.
- **Сервис удаленного самообслуживания за пределами домена** (Remote Self-Service) – веб-приложение **rss**.
- **Сервис разблокировки и выключения устройств** – веб-приложение **credprovapi**.
- **Сервис API** – веб-приложение **api**.
- **Сервер OpenID Connect** – веб-приложение **oidc**.
- **Сервис отслеживания состояния устройств** – **Служба Card Monitor**, не имеет веб-приложения.
- **Сервисы клиентского агента**:
  - **Сервис регистрации агентов** – веб-приложение **agentregistrationapi**.
  - **Сервис агентов для удаленного выполнения задач** – веб-приложение **agentserviceapi**.

> Каждый сервис имеет собственные файлы конфигурации и настройки доступа.

Установка сервера на ОС Windows

Установка сервера

Запустите файл **IndeedCM.Server-<*номер версии*>.x64.ru-ru.msi** из каталога *IndeedCM. Server* дистрибутива системы и выполните установку, следуя указаниям мастера. В процессе установки будет предложено выбрать способ контроля доступа для всех приложений системы.



Аутентификация Windows

При выборе Аутентификации Windows будут заданы следующие параметры контроля доступа:

- **Проверка подлинности** (Authentication):
  - **Проверка подлинности Windows** (Windows Authentication) для веб-приложений: **Консоль управления** (mc), **Сервис самообслуживания** (ss), **Сервис API** (api). Остальные способы отключены.
  - **Анонимная проверка подлинности** (Anonymous Authentication) для веб-приложений: **Сервис удаленного самообслуживания** (rss), **Сервис разблокировки смарт-карт** (credprovapi), **Сервисов клиентских агентов** (agentregistrationapi, agentserviceapi).
- **Параметры SSL** (SSL Settings):
  - **Требовать SSL** (Require SSL) для всех веб-приложений.
  - **Сертификаты клиента** (Client certificates):
    - **Игнорировать** (Ignore) для веб-приложений: **Консоль управления** (mc), **Сервис самообслуживания** (ss), **Сервис удаленного самообслуживания** (rss), **Сервис разблокировки смарт-карт** (credprovapi), **Сервис API** (api), **Сервис регистрации клиентских агентов** (agentregistrationapi).
    - **Требовать** (Require) для веб-приложения: **Сервис агентов** (agentserviceapi).

Аутентификация по персональным сертификатам пользователей

При выборе Аутентификации по персональным сертификатам пользователей будут заданы следующие параметры контроля доступа:

- **Проверка подлинности** (Authentication):
  - **Анонимная проверка подлинности** (Anonymous Authentication) для всех веб-приложений. Остальные способы отключены.
- **Параметры SSL** (SSL Settings):
  - **Требовать SSL** (Require SSL) для всех веб-приложений.
  - **Сертификаты клиента** (Client certificates):
    - **Игнорировать** (Ignore) для веб-приложений: **Сервис удаленного самообслуживания** (rss), **Сервис разблокировки смарт-карт** (credprovapi), **Сервис регистрации клиентских агентов** (agentregistrationapi).
    - **Требовать** (Require) для веб-приложений: **Консоль управления** (mc), **Сервис самообслуживания** (ss), **Сервис API** (api), **Сервис агентов** (agentserviceapi).

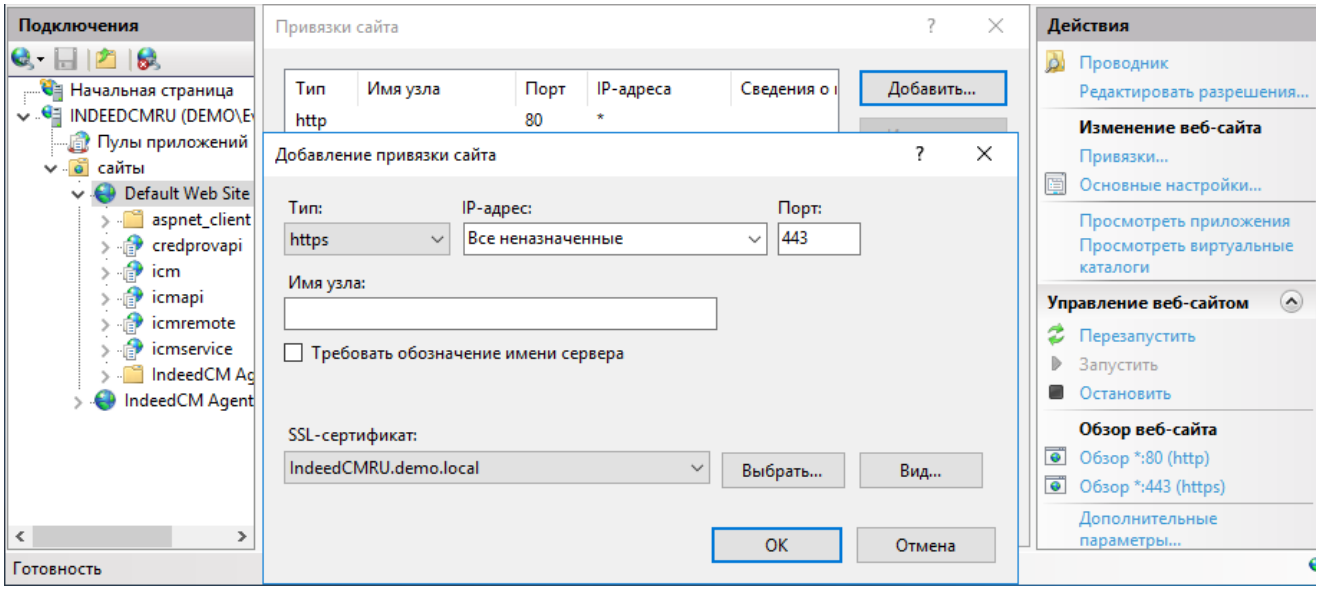
> Если каталог пользователей расположен в Active Directory, то сертификаты, используемые для аутентификации должны содержать **User Principal Name**. Без включенного в сертификат **UPN** вход в web-приложения будет невозможен.

После установки системы **Параметры SSL** для каждого приложения можно изменить вручную в **Диспетчере служб IIS** (IIS Manager).

Привязка SSL/TLS-сертификата

Для настройки защищенного соединения для веб-приложений, необходимо выпустить SSL/TLS-сертификат и **Привязать** (Bindings) его в **Диспетчере служб IIS** (IIS Manager) для сайта **Default Web Site**:

- Запустите **Диспетчер служб IIS** (Internet Information Services (IIS) Manager).
- Выберите сайт **Default Web Site** и перейдите в раздел **Привязки...** (Bindings...).
- Нажмите **Добавить...** (Add...), выберите **Тип:** (Type:) **https** и **Порт:** (Port:) **443**.
- Выберите **SSL-сертификат:** (SSL certificate:) и нажмите **OK**:



Субъект (Subject) сертификата должен содержать атрибут **Общее имя** (Common name) (FQDN сервера Indeed CM).
Дополнительное имя субъекта (Subject Alternative Name) сертификата должно содержать атрибут **DNS-имя** (DNS Name) (FQDN сервера Indeed CM). Например: *indeedcmru.demo.local* или соответствующую запись с подстановочными знаками, например: **. demo.local* (Wildcard certificate).
Улучшенный ключ (Enhanced Key Usage) сертификата должен содержать значение **Проверка подлинности сервера** (Server Authentication).

Установка сервера на ОС Linux

Установка сервера

В зависимости от используемого Linux дистрибутива через соответствующий пакетный менеджер установите DEB или RPM пакет из дистрибутива Indeed Certificate Manager (для использования пакетного менеджера требуются права суперпользователя).

RHEL и производные дистрибутивы:
sudo rpm -i cm.-<номер версии>.x86_64.rpm

Debian и производные дистрибутивы:
sudo dpkg -i cm.-<номер версии>_amd64.deb

После установки системы приложения расположены в каталоге */opt/indeed/cm*.

Владельцем каталога по умолчанию является root.

Для корректной работы **Сервиса удаленного самообслуживания за пределами домена** (Remote Self-Service) требуются установленные TrueType шрифты Windows, установите пакет с шрифтами в зависимости от используемого Linux дистрибутива.

В RHEL и производных дистрибутивах пакет называется *msttcore-fonts-installer*:

```
sudo yum install -y msttcore-fonts-installer
fc-cache -f -v
```

В Debian и производных дистрибутивах пакет называется *ttf-mscorefonts-installer*:

```
wget http://ftp.ru.debian.org/debian/pool/contrib/m/msttcorefonts/ttf-mscorefonts-installer_3.8.1_all.deb
sudo dpkg -i ttf-mscorefonts-installer_3.8.1_all.deb
fc-cache -f -v
```

Управление приложениями

Во время установки сервера для управления приложениями создаются файлы служб systemd. Данная подсистема инициализации и управления службами позволяет запускать приложения автоматически при старте системы и держать их запущенными без участия пользователя.

По умолчанию systemd будет запускать приложения системы от имени учетной записи ***www-data***.

На RHEL-системах и производных дистрибутивах учетная запись *www-data* по умолчанию отсутствует, возможно добавить ее через утилиту *useradd* или заменить используемую учетную запись пользователя (директива *User=<имя пользователя>*) в файлах служб *cm-<имя сервиса>.service*, располагающихся в директории */etc/systemd/system*.

Пример команды создания пользователя *www-data*:

```
useradd -d /var/www -m www-data -s /sbin/nologin
```

Пример файла службы Консоли управления, запускаемой от имени нестандартной учетной записи *cm_adm*:

```
[Unit]
Description=Indeed CM Management Console Application

[Service]
WorkingDirectory=/opt/indeed/cm/mc/
ExecStart=/opt/indeed/cm/mc/Cm.Web.ManagementConsole
Restart=always
RestartSec=10
KillSignal=SIGINT
SyslogIdentifier=cm-mc
User=cm_adm
Environment=ASPNETCORE_URLS="http://localhost:5001"
Environment=ASPNETCORE_ENVIRONMENT=Production
Environment=DOTNET_PRINT_TELEMETRY_MESSAGE=false

[Install]
WantedBy=multi-user.target
```

Для включения автозапуска и немедленного старта приложений выполните файл сценария *start-cm-services.sh* из директории с дистрибутивом Indeed Certificate Manager.

> Для запуска любого файла сценария требуются разрешения на выполнение у данного файла.
> В ходе работы данного сценария потребуются права суперпользователя.

```
chmod +x start-cm-services.sh
sudo ./start-cm-services.sh
```

Далее для корректной работы приложений настройте параметры системы через Мастер Настройки (рекомендуется) или вручную.

Привязка SSL/TLS-сертификата

После установки системы доступ к приложениям осуществляется локально по протоколу HTTP.

Для обеспечения возможности безопасной работы с других машин настройте веб-сервер NGINX или Apache, в соответствующих инструкциях описывается привязка SSL/TLS-сертификатов и настройка подключения по протоколу HTTPS.