

Удостоверяющий центр

Руководство по инсталляции

Версия УЦ 2.2.0

История изменений документа

Версия	Дата	Перечень изменений
1.0	24.05.2018	Первоначальная версия
1.1	22.08.2018	Внесение изменений в пункт 3.4
1.2	11.09.2020	Изменен пункт 3.2, 3.3

Содержание

1. Назначение документа.....	4
2. Подготовка к инсталляции	4
3. Инсталляция	5
3.1. Создание схем (баз данных)	5
3.2. Создание таблиц.....	8
3.3. Настройка параметров	10
3.4. Запуск приложений	11
3.4.1. Запуск через командную строку.....	11
3.4.2. Запуск через создание службы	12

1. Назначение документа

Данный документ описывает процесс установки «Корневого Удостоверяющего центра ИНПАС» и «Удостоверяющего центра хоста удаленной загрузки ключей».

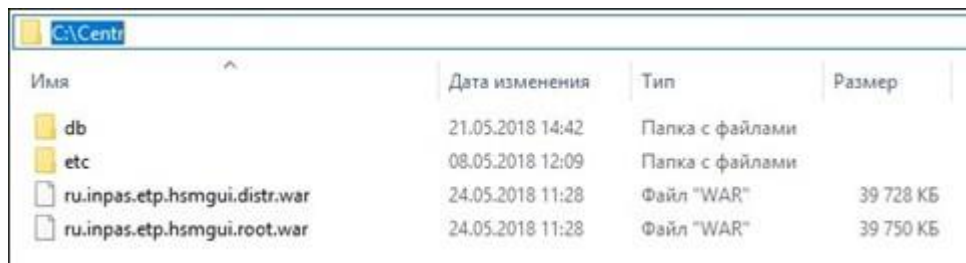
2. Подготовка к установке

Перед началом установки на компьютере с операционной системой «**Windows 7**» должна быть установлена виртуальная машина Java версии 8. Разрядность виртуальной машины Java (32 или 64) не имеет значения. Инструкция по установке Java: https://www.java.com/en/download/help/download_options.xml.

Также должна быть установлена СУБД MySQL версии 5.7.

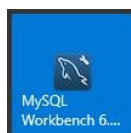
3. Инсталляция

Содержимое поставки (при необходимости надо разархивировать zip-архив) нужно поместить в каталог, например, в C:\Centr.

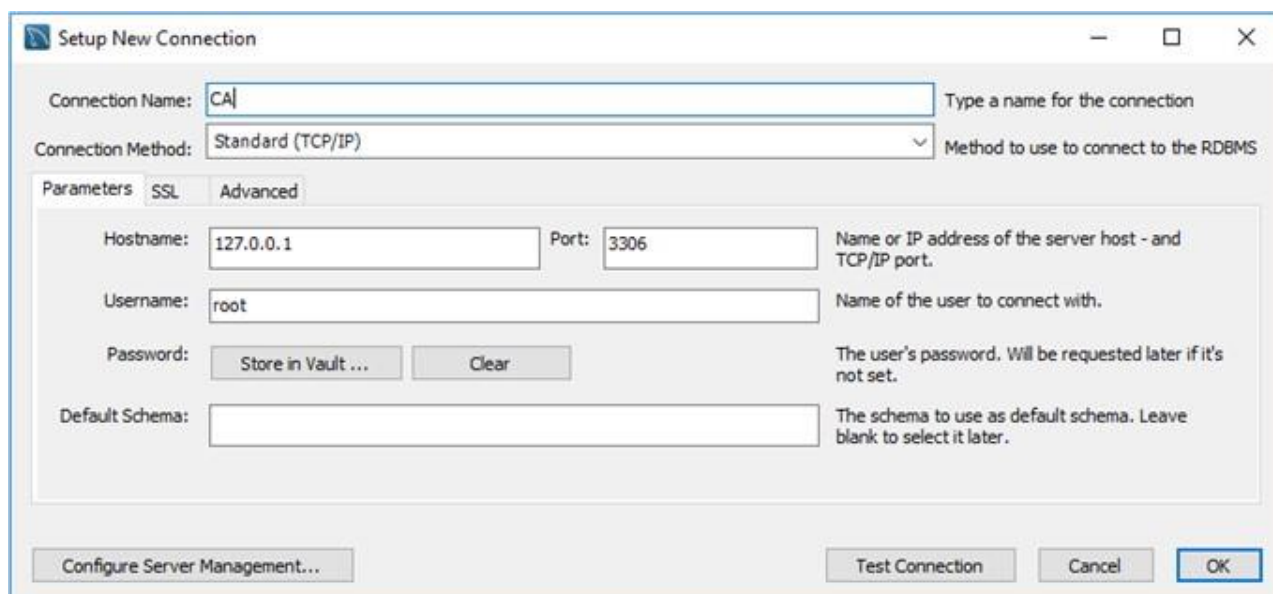


3.1. Создание схем (баз данных)

Запускаем СУБД «MySQL Workbench».



В открывшемся окне создаем новое подключение, для этого нажимаем на значок . Отобразится окно «Setup New Connection», в котором нужно заполнить следующие параметры и нажать кнопку «ОК»:



«**Connection Name**» - указывается название подключения, далее на вкладке «**Parameters**» заполняем параметры:

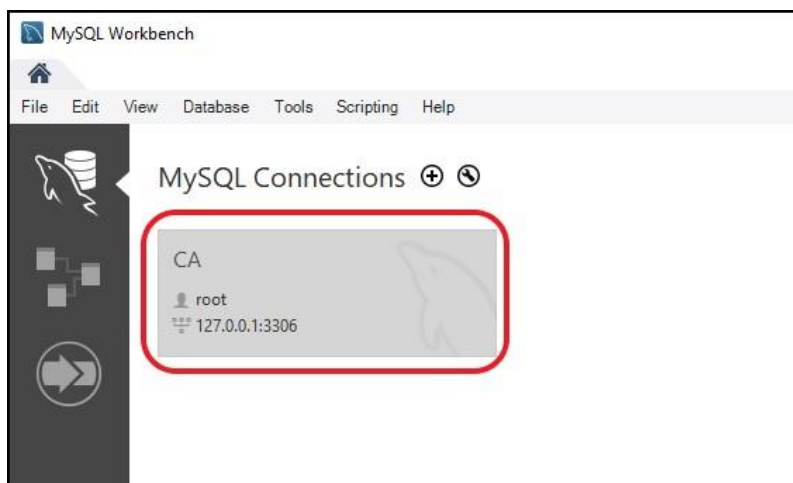
- «**Hostname**» - указывается имя или Ip-адрес компьютера для подключения к базе данных;
- «**Port**» - указывается TCP/IP порт компьютера для подключения к базе данных;
- «**Username**» - указывается имя пользователя (логин) для подключения к базе данных.

В строке «**Password**» отображаются две кнопки: «**Store in Vault...**», «**Clear**».

При нажатии на кнопку «**Store in Vault...**» отобразится окно, где необходимо ввести пароль для подключения к базе данных и нажать кнопку «**ОК**».



При нажатии на кнопку «Clear» система удалит введенный пароль. Далее нажимаем левой клавишей мыши на созданное подключение.



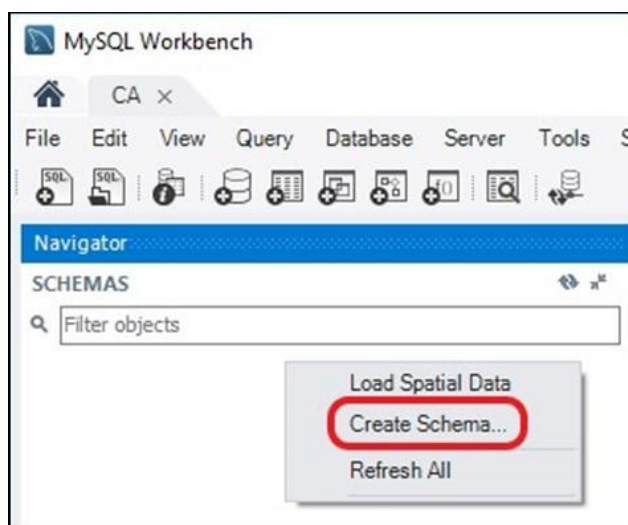
Если при создании подключения был задан пароль, то высветиться окно с запросом ввода пароля.

Если пароль не был задан при создании подключения, то СУБД сразу перейдет к окну управления базами данных (схемами).

Далее в отобразившемся окне в области «SCHEMAS» нажимаем правой клавишей мыши и в отобразившемся контекстном меню выбираем пункт «Create Schema...».

Необходимо создать две схемы (базы данных):

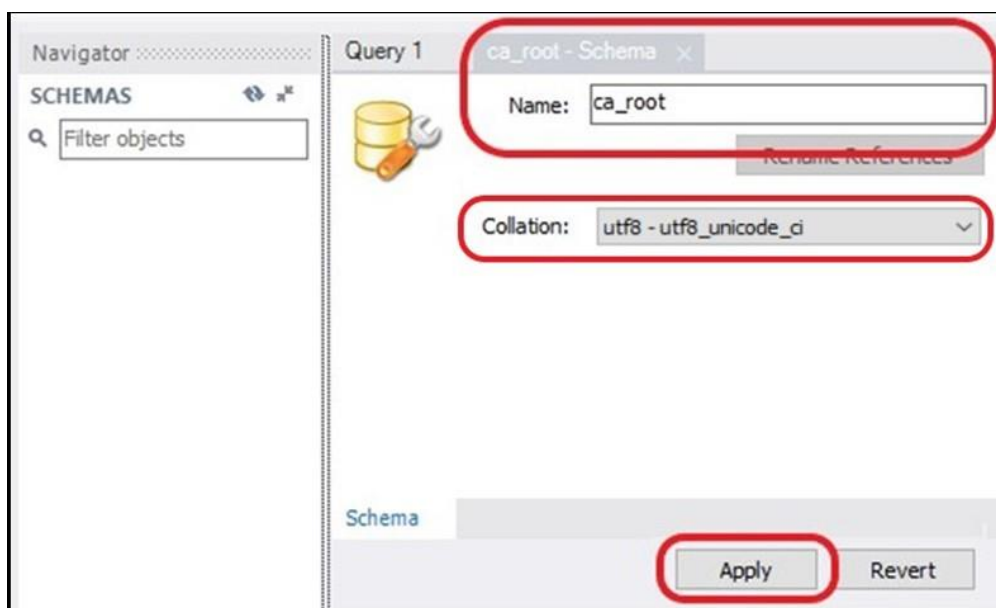
- Корневой Удостоверяющий центр ИНПАС;
- Удостоверяющий центр хоста удаленной загрузки ключей.



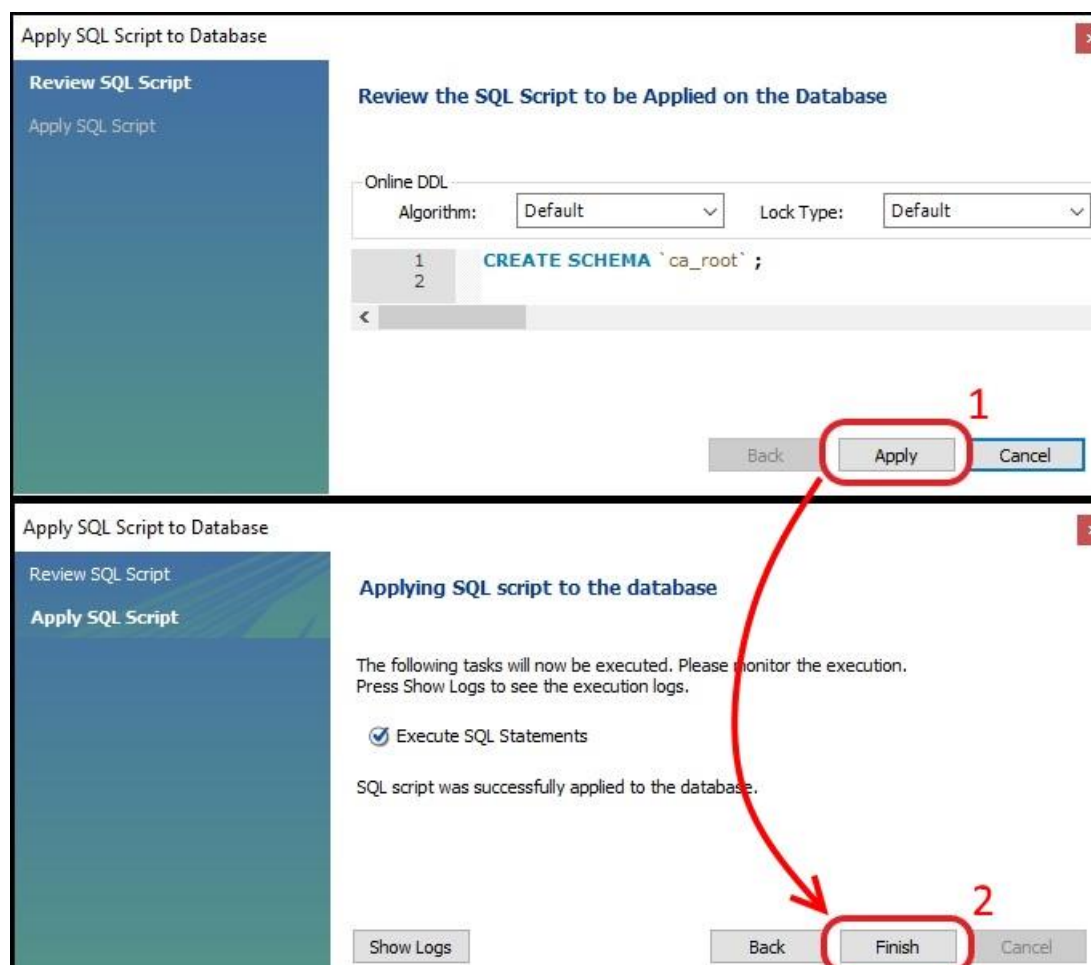
Отобразится вкладка «new_schema – Schema», где необходимо указать название схемы (базы данных) в поле «Name» и в поле «Collation» указать значение «utf8 – utf8_unicode_ci», далее нажать кнопку «Apply».

Значения, которые нужно указать:

- Корневой Удостоверяющий центр ИНПАС – ca_root;
- Удостоверяющий центр хоста удаленной загрузки ключей – ca_distr.



В появившемся окне «**Apply SQL Script to Database**» нужно нажать кнопку «**Apply**» и кнопку «**Finish**».

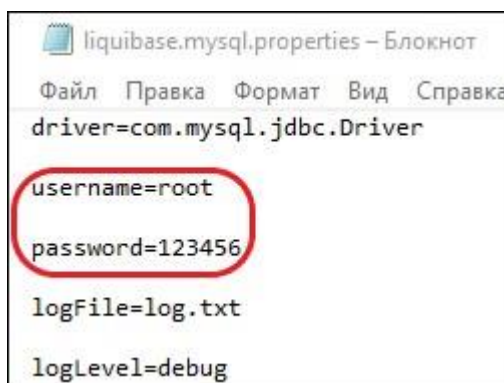


В итоге в главном окне СУБД в области «**SCHEMAS**» должны быть две схемы (базы данных).



3.2. Создание таблиц

Далее в файле «liquibase.mysql.properties», расположенном в «db\bin\liquibase\», нужно указать пароль для пользователя «root». Для сохранения внесенных изменений нужно нажать на кнопку «Файл», выбрать пункт «Сохранить».



Следующим шагом необходимо выполнить два скрипта для создания таблиц в уже созданных схемах (базах данных) «ca_root» и «ca_distr». Для этого запускаем системную консоль под правами администратора. На разных операционных системах это может быть выполнено разными способами.

Windows 7

Нажать сочетание клавиш «Windows+R» и в строку «Выполнить» ввести «cmd.exe», затем нажать кнопку «ОК».

Другой способ – нажать кнопку «Start», набрать в строке поиска «cmd», в результатах поиска в разделе «Programs» нажать правой кнопкой мыши на найденную программу и выбрать пункт «Запуск от имени администратора».

Windows 8.x

Создать ярлык на рабочем столе и в качестве пути к программе указать «c:\windows\system32\cmd». На закладке «Совместимость» поставить флаг «Запуск от имени администратора».

Запустить консоль двойным кликом на созданный ярлык.

Скрипты, указанные ниже необходимо запускать из директории, где они находятся.

В системной консоли ввести «cd C:\Centr\db\bin\liquibase», где «C:\Centr\db\bin\liquibase» - путь до файла «liquibase.mysql.properties».

```
C:\WINDOWS\system32>cd C:\Centr\db\bin\liquibase
C:\Centr\db\bin\liquibase>
```

Далее указываем скрипты:

```
call ./liquibase ^
--defaultsFile=liquibase.mysql.properties ^
--url="jdbc:mysql://localhost:3306/ca_root?useUnicode=true&characterEncoding=utf8" ^
--changeLogFile=../../ca/root/db.ca_root.changelog-master.xml ^
update ^
-Dmain.schema=ca_root

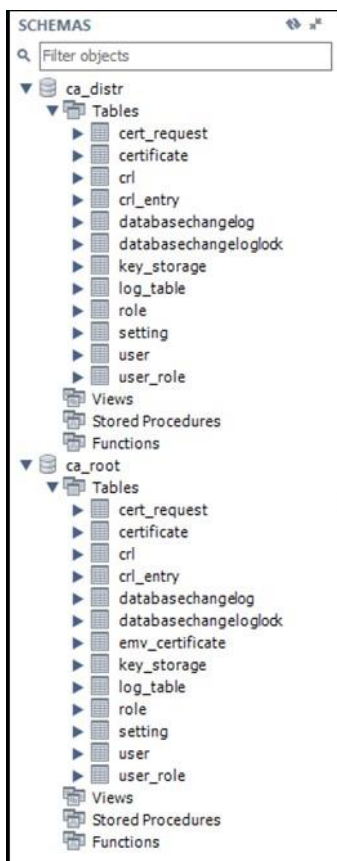
call ./liquibase ^
--defaultsFile=liquibase.mysql.properties ^
--url="jdbc:mysql://localhost:3306/ca_distr?useUnicode=true&characterEncoding=utf8" ^
--changeLogFile=../../ca/distr/db.ca_distr.changelog-master.xml ^
update ^
-Dmain.schema=ca_distr
```

При успешном выполнении скриптов будет отображаться строка «Liquibase: Update has been successful».

```
C:\Centr\db\bin\liquibase>call ./liquibase ^
Продолжить? --defaultsFile=liquibase.mysql.properties ^
Продолжить? --url="jdbc:mysql://localhost:3306/ca_root?useUnicode=true&characterEncoding=utf8" ^
Продолжить? --changeLogFile=../../ca/root/db.ca_root.changelog-master.xml ^
Продолжить? update ^
Продолжить? -Dmain.schema=ca_root
Starting Liquibase at 14:28:28 MSK (version 3.6.1 built at 2018-04-11 08:41:04)
Liquibase: Update has been successful.

C:\Centr\db\bin\liquibase>
C:\Centr\db\bin\liquibase>call ./liquibase ^
Продолжить? --defaultsFile=liquibase.mysql.properties ^
Продолжить? --url="jdbc:mysql://localhost:3306/ca_distr?useUnicode=true&characterEncoding=utf8" ^
Продолжить? --changeLogFile=../../ca/distr/db.ca_distr.changelog-master.xml ^
Продолжить? update ^
Продолжить? -Dmain.schema=ca_distr
Starting Liquibase at 14:28:04 MSK (version 3.6.1 built at 2018-04-11 08:41:04)
Liquibase: Update has been successful.
```

При просмотре схем в СУБД мы увидим, что для каждой из схем (баз данных) были созданы наборы таблиц.



После создания набора таблиц для каждой схемы (базы данных) нужно указать IP-адрес, порт для работы с HSM и указать номер ячейки «**Variant LMK**» на HSM.

Для указания данных IP-адрес, порт HSM и номер ячейки «**Variant LMK**» необходимо в раскрытой группе «**Tables**» выбрать таблицу «**Setting**». Данную таблицу нужно открыть для редактирования и в следующие строки внести изменения (если необходимо), сохранить:

- HSM_ADDRESS – указывается IP-адрес HSM;
- HSM_PORT - указывается порт HSM;
- LMK_ID – указывается номер ячейки «**Variant LMK**» на HSM.

	id	name	setting_value
▶	1	HSM_ADDRESS	10.35.1.100
	2	HSM_PORT	1500
	3	CA_LEVEL	1
	4	OFFICERS_REQUIRED	2
	5	LOG_EXPORT_DIRECTORY	/tmp
	6	LMK_ID	0
•	NULL	NULL	NULL

Примечание.

Номер ячейки «**Variant LMK**» используется при инсталляции апплета на карту. Если номер выставлен неправильно, то будет возникать ошибка привязки карты.

Далее нужно выполнить настройки приложений в файлах параметров.

3.3. Настройка параметров

Файлы параметров располагаются в папке «**etc**»:

- Корневой Удостоверяющий центр ИНПАС – ca_root.user.properties;
- Удостоверяющий центр хоста удаленной загрузки ключей – ca_distr.user.properties.

Пример параметров:

db-url=jdbc:mysql://localhost:3306/ca_root?useUnicode=true&characterEncoding=utf8 - url соединения с БД MYSQL;

Примечание.

Из строки соединения с БД «**db-url**» нужно удалить два символа «**_p**». Как должно получиться указано выше в примере.

db-user=root - пользователь для MySQL;

db-password=gkPcKQHDC0NmNnBXqXe5uQ== - зашифрованный пароль пользователя для MySQL (по умолчанию - 123456);

db-driver=com.mysql.jdbc.Driver – драйвер для работы с СУБД;

db-dialect=org.hibernate.dialect.MySQL5Dialect;

export-path=D:/temp/ca_logs/root - директория, куда будут экспортироваться логи с подписью из БД.

Примечание.

Для создания зашифрованного пароля необходимо выполнить запрос MySQL.

SET @@session.block_encryption_mode = 'aes-128-cbc';

SELECT TO_BASE64(AES_ENCRYPT(PASSWORD,KEY,INIT_VECTOR)), где:

- **PASSWORD** – указывается пароль пользователя для MySQL;
- **KEY** – секретный ключ (предоставляется Inpas Soft);
- **INIT_VECTOR** – случайный набор байтов (предоставляется Inpas Soft).

3.4. Запуск приложений

Последним шагом необходимо выполнить запуск приложений. Запустить приложение возможно двумя способами:

- С использованием командной строки;
- Создание службы

3.4.1. Запуск через командную строку

Для этого запускаем/ открываем системную консоль, указываем путь к корневому каталогу – «**cd C:\Centr**» и нажимаем «**Enter**». Для каждого удостоверяющего центра необходимо запускать персональную системную консоль.

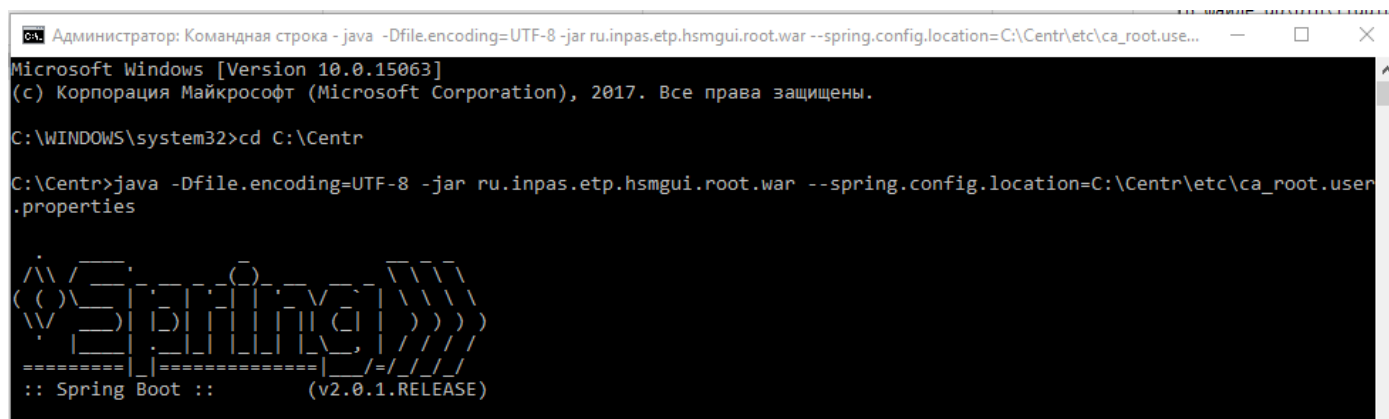
```
C:\WINDOWS\system32>cd C:\Centr
C:\Centr>
```

Далее указываем следующие команды:

- Корневой Удостоверяющий центр ИНПАС

`java -Dfile.encoding=UTF-8 -jar ru.inpas.etp.hsmgui.root.war --spring.config.location=C:\Centr\etc\ca_root.user.properties`

Где «**--spring.config.location=**» путь до файл «**ca_root.user.properties**».



```
Администратор: Командная строка - java -Dfile.encoding=UTF-8 -jar ru.inpas.etp.hsmgui.root.war --spring.config.location=C:\Centr\etc\ca_root.user...
Microsoft Windows [Version 10.0.15063]
(c) Корпорация Майкрософт (Microsoft Corporation), 2017. Все права защищены.

C:\WINDOWS\system32>cd C:\Centr

C:\Centr>java -Dfile.encoding=UTF-8 -jar ru.inpas.etp.hsmgui.root.war --spring.config.location=C:\Centr\etc\ca_root.user...
.properties

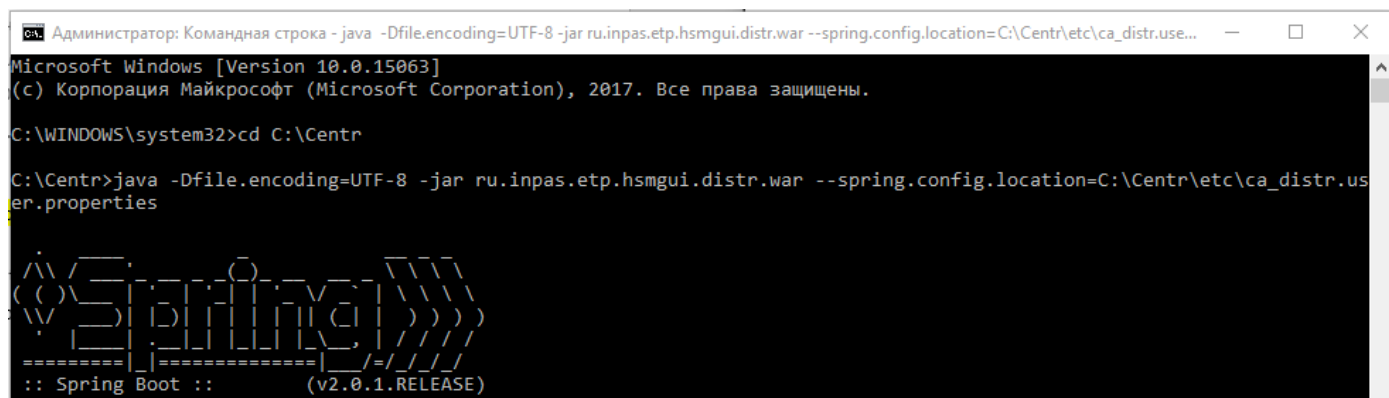
  ____ _
 / ___ \| | | |
 \___ \| |_| |
  ___) | __| |
 |____|_|_|_|

:: Spring Boot ::                (v2.0.1.RELEASE)
```

- Удостоверяющий центр хоста удаленной загрузки ключей

`java -Dfile.encoding=UTF-8 -jar ru.inpas.etp.hsmgui.distr.war --spring.config.location=C:\Centr\etc\ca_distr.user.properties`

Где «**--spring.config.location=**» путь до файл «**ca_distr.user.properties**».



```
Администратор: Командная строка - java -Dfile.encoding=UTF-8 -jar ru.inpas.etp.hsmgui.distr.war --spring.config.location=C:\Centr\etc\ca_distr.use...
Microsoft Windows [Version 10.0.15063]
(c) Корпорация Майкрософт (Microsoft Corporation), 2017. Все права защищены.

C:\WINDOWS\system32>cd C:\Centr

C:\Centr>java -Dfile.encoding=UTF-8 -jar ru.inpas.etp.hsmgui.distr.war --spring.config.location=C:\Centr\etc\ca_distr.us...
er.properties

  ____ _
 / ___ \| | | |
 \___ \| |_| |
  ___) | __| |
 |____|_|_|_|

:: Spring Boot ::                (v2.0.1.RELEASE)
```

Далее запускаем браузер и в адресной строке указываем URL.

- Корневой Удостоверяющий центр ИНПАС – <http://localhost:8080/ca/root>;
- Удостоверяющий центр хоста удалённой загрузки ключей – <http://localhost:8081/ca/distr>.

3.4.2. Запуск через создание службы

- **Создание службы для Корневого Удостоверяющего центра ИНПАС**

Для создания службы необходимо в папке «root» отредактировать файл «ru.inpas.etp.hsmgui.root.xml».

В теге «arguments», после значения «--spring.config.location=», необходимо указать путь к файлу конфигурации «ca_root.user.properties».

```
<?xml version="1.0" encoding="UTF-8"?>
<service>
  <id>ru.inpas.etp.hsmgui.root</id>
  <name>ru.inpas.etp.hsmgui.root</name>
  <description>CA ROOT Windows Service</description>
  <executable>java</executable>
  <arguments>-Dfile.encoding=UTF-8 -jar "ru.inpas.etp.hsmgui.root.war" --spring.config.location=C:\Centr\etc\ca_root.user.properties</arguments>
  <logmode>rotate</logmode>
</service>
```

Далее в папке «root» запускаем файл «install_and_run.bat» с правами администратора, после чего служба «ru.inpas.etp.hsmgui.root» установится и запустится.

Для удаления службы необходимо запустит файл «stop_and_uninstall.bat» с правами администратора.

- **Создание службы для Удостоверяющего центра хоста удаленной загрузки ключей**

Для создания службы необходимо в папке «distr» отредактировать файл «ru.inpas.etp.hsmgui.distr.xml».

В теге «arguments», после значения «--spring.config.location=», необходимо указать путь к файлу конфигурации «ca_distr.user.properties».

```
<?xml version="1.0" encoding="UTF-8"?>
<service>
  <id>ru.inpas.etp.hsmgui.distr</id>
  <name>ru.inpas.etp.hsmgui.distr</name>
  <description>CA DISTR Windows Service</description>
  <executable>java</executable>
  <arguments>-Dfile.encoding=UTF-8 -jar "ru.inpas.etp.hsmgui.distr.war" --spring.config.location=C:\Centr\eto\ca_distr.user.properties</arguments>
  <logmode>rotate</logmode>
</service>
```

Далее в папке «root» запускаем файл «install_and_run.bat» с правами администратора, после чего служба «ru.inpas.etp.hsmgui.root» установится и запустится.

Для удаления службы необходимо запустить файл «stop_and_uninstall.bat» с правами администратора.

Далее запускаем браузер и в адресной строке указываем URL.

- Корневой Удостоверяющий центр ИНПАС – <http://localhost:8080/ca/root>;
- Удостоверяющий центр хоста удаленной загрузки ключей – <http://localhost:8081/ca/distr>.