# SP5000 интеллектуальная облачная платформа интернета вещей "IoT SP5000 "Элемент"

Руководство пользователя

**Екатеринбург 2018**

# Оглавление

# 1. Руководство пользователя интерфейса IAPE GUI (ORIN)

## 1.1. Общие сведения

Графический интерфейс пользователя **ORIN** является центром управления платформы IAPE. Для разработки всех клиентских приложений была использована технология **Angular**, для создания визуального оформления компонентов платформы была использована библиотека **Angular Material**.

Интерфейс Composite UI является частью платформы IAPE, где пользователь может настроить вид приложений. Глубина настройки зависит от администратора, который может добавлять или удалять приложения.

Существует два типа пользователей, которые могут подключиться к интерфейсу Composite UI, это *user* и *admin*, у них различные пользовательские интерфейсы. Администратор (*admin*) может добавлять приложения, которые будут использоваться обычными пользователями (*user*). Пользователи, в свою очередь, могут настраивать вид своего интерфейса путем выбора отображаемых приложений.

Интерфейс Composite UI соединен с бэкенд-сервисом, который содержит всю информацию о добавляемых, удаляемых приложениях и о соответствующем пользователе.

## 1.2. Доступ

Для доступа к интерфейсу ORIN сначала необходимо настроить SDP-клиент (см. Главу 2).

## 1.3. Клиентское приложение Composite User Interface (ORIN)

Интерфейс Composite User Interface (другое название – ORIN) представляет собой шлюз для интерфейсов платформы IAPE, а также других продуктов Искра Технологии. С помощью технологии *microfrontends* в приложении была реализована архитектура микросервисов, ранее использовавшаяся в бэкенд-приложениях. Доступ ко всем веб-приложениям осуществляется посредством технологии iframe из приложения ORIN.

Пользовательский интерфейс состоит из двух экранов:

- **User operations Dashboard** – панель мониторинга пользовательских операций;
- **User Dashboard –** панель мониторинга пользователей.

Оба экрана доступны в зависимости от разрешений и ролей, назначенных пользователю.

Каждый клиент с ролью **ENGINEER** после входа в систему перенаправляется на экран **User operations**, каждый клиент с ролью **OPERATOR** после входа в систему перенаправляется на экран **User Dashboard.**

### 1.3.1. Экран User operations Dashboard

Экран **User operations dashboard** представляет собой конфигурацию экрана **User dashboard.** На этом экране открывается страница **Register IAPE Platform components**, где можно изменять (добавлять, удалять, редактировать) вид интерфейсов всех существующих и будущих модулей **IAPE** или **Искра Технологии**.

Кроме того, на этом экране осуществляется перенаправление на некоторые программные приложения платформы IAPE: система управления ключами (FreeIpa), система поставщика идентичности (Keycloak), панель управления периметром SDP (описывается в данной документации) и панель управления компонентом Ingestor (Hawtio).

### 1.3.2. Экран User Dashboard

Этот экран используется для доступа пользователя к компонентам платформы. После выбора элемента **Menu** открывается окно, где пользователь может просмотреть зарегистрированные компоненты платформы и после этого при необходимости добавить их в свой интерфейс. Таким образом, каждый пользователь может настроить свой собственный интерфейс по своим нуждам. После добавления какого-либо зарегистрированного компонента платформы в интерфейсе пользователя появляется кнопка доступа, которая перенаправляет пользователя на экран соответствующего компонента посредством технологии iframe.

## 1.4. Защита приложений и ролевое управление доступом

Защита приложения обеспечивается с помощью двухфакторной аутентификации (**Two Factor Authentication**, **2FA**), при которой при попытке доступа к веб-приложению пользователь перенаправляется в поставщик идентичности (**IAPE IdP - Identity provider**), где ему требуется предоставить сертификаты, выданные системой KMS (**IAPE Key Management system**), а затем ввести имя пользователя и пароль, чтобы войти в приложение. Также реализовано ролевое управление доступом (**Role based access control, RBAC**), что означает, что некоторые части приложения ограничены для пользователей, которые не имеют прав на их использование или не принадлежат к группе, которая имеет доступ к соответствующим данным или функциональностям.

## 1.5. Интерфейс администратора Composite UI

Интерфейс Composite UI для администратора представлен на скриншоте ниже. Администратор имеет роль Engineer.

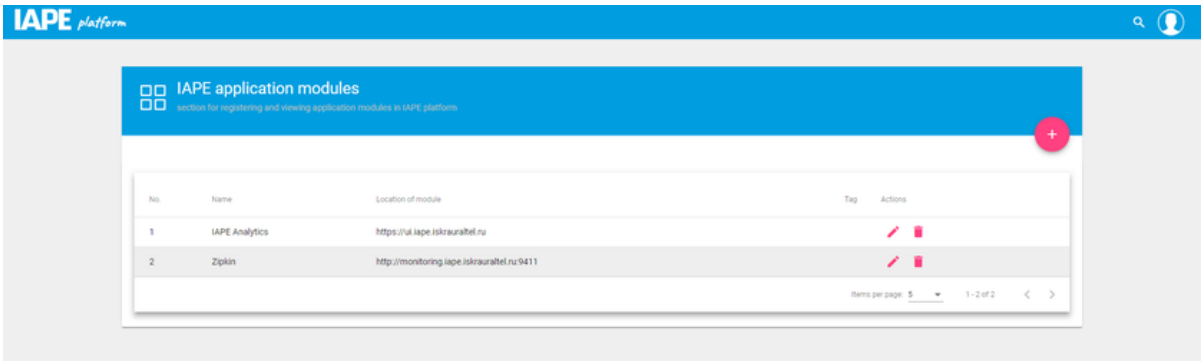


Рис. 1 – Интерфейс администратора Composite UI

В интерфейсе Composite UI, администратор может контролировать компоненты платформы, управлять пользователями и их привилегиями, управлять безопасностью и приложениями. В следующих разделах будут описаны основные выполняемые им операции.

### 1.5.1. Добавление приложений

Щелчком по значку **плюса (+)** можно добавить приложения, которые будут отображаться в интерфейсах пользователей.

Откроется всплывающее меню, в котором можно ввести имя приложения, его описание, задать URL-адрес для приложения, выбрать рисунок, который будет представлять приложение, назначить уровень приоритета и опционально выбрать группу, к которой будет принадлежать приложение (добавить тег).

### 1.5.2. Редактирование приложений

После добавления приложение будет отображаться в списке в интерфейсе администратора, как показано на скриншоте выше. Щелчком по значку **карандаша** можно отредактировать приложение.

Откроется окно, в котором можно изменить все параметры, перечисленные выше, кроме идентификатора модуля.

### 1.5.3. Удаление приложений

Щелчком по значку **корзины** можно удалить приложение.

### 1.5.4. Список Items per page

В списке **Items per page** можно выбрать максимальное количество приложений, отображаемых на одной странице.

## 1.6. Интерфейс пользователя Composite UI

Интерфейс Composite UI для пользователя показан на скриншоте ниже. Пользователь имеет роль Operator.


Рис. 2 – Интерфейс пользователя Composite UI

### 1.6.1. Добавление приложений

Пользователь может добавлять приложения, щелкнув красную кнопку в правом нижнем углу и щелкнув значок **плюса (+)**.

Откроется всплывающее меню со всеми доступными приложениями и их описанием, в котором можно выбрать приложения, которые нужно добавить, после чего нужно щелкнуть кнопку сохранения.

### 1.6.2. Удаление приложений

Пользователь может удалять приложения, щелкнув красную кнопку в правом нижнем углу и щелкнув значок **редактирования.** После этого нужно выбрать приложения, которые нужно удалить, и снова щелкнуть значок редактирования.

### 1.6.3. Просмотр приложений

Пользователь может перейти в то или иное приложение, щелкнув кнопку соответствующего приложения.

### 1.6.4. Выход из системы

Пользователь может выйти из системы, щелкнув значок пользователя в правом верхнем углу и щелкнув кнопку **Log Out**.

## 1.7. Приложение IAPE Analytics

Пользователь может перейти на экран приложения **IAPE Analytics**, щелкнув кнопку данного приложения в интерфейсе Composite UI.

Интерфейс пользователя был разработан для поставщиков и производителей энергии, поэтому его основной идеей является просмотр и контроль данных умных счетчиков по заданному источнику энергии посредством графиков в реальном времени, а также исторических данных. Таким образом, источники энергии включают: Уголь (**Coal**), Ядерная (**Nuclear**), Гидро (**Hydro**), Ветер (**Wind**) и Солнечная (**Solar**).

После входа в приложение пользователь переходит на главный экран, который содержит **боковую панель**, **навигационную панель** и **область просмотра**. Навигационная панель содержит кнопку **Language** (язык), значок **Notifications** (уведомления) и значок **Profile** (профиль). Боковая панель содержит меню со следующими функциональными элементами:

- **Dashboard** – панель мониторинга
- **Historic Measurements** – исторические измерения
- **Real time Measurements** – измерения в реальном времени
- **GeoMap** – географическая карта
- **System Analytics** – системная аналитика
- **User Manual** – руководство пользователя

Отображаемые функциональные элементы зависят от роли, которую имеет пользователь.

На экране **Dashboard** пользователь может создавать виджеты (Widgets) для нужных узлов и параметров, а также просматривать уведомления, если тот или иной узел инициирует аварийный сигнал.

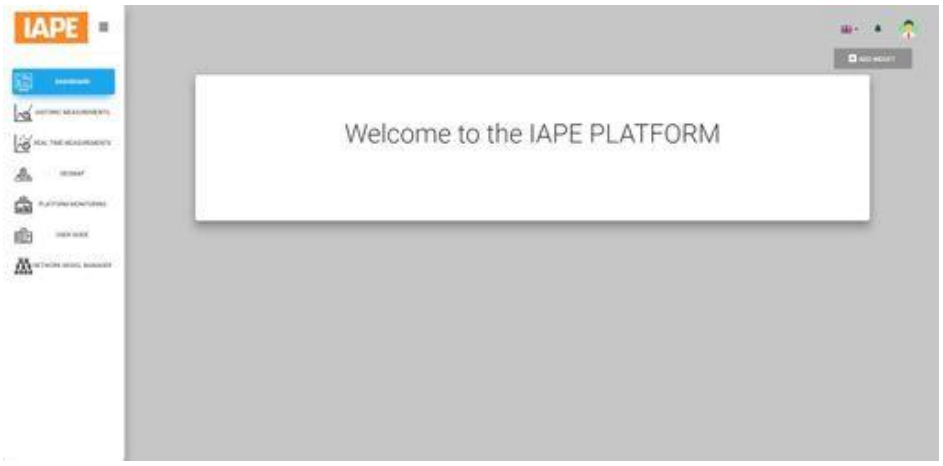


Рис. 3 – IAPE Analytics – экран **Dashboard**

### 1.7.1. Добавление виджета

Виджеты являются неотъемлемой частью главного экрана. Пользователь может перемещать виджеты по главному экрану и изменять их размер в рамках сетки главного экрана. Виджеты сбора (Collection) предназначены для отображения нескольких элементов одного типа, например, набор линейных графиков по историческим данным или данным в реальном времени, получаемым от умных счетчиков. В зависимости от роли и разрешений, пользователь может создать и настроить свою собственную панель мониторинга, заполнив поля специальной формы: измерение, источник, параметр, время, идентификатор узла.

Администратор может добавить виджет, щелкнув кнопку **Add Widget**. Откроется окно с настраиваемыми параметрами: измерения, источник энергии, наблюдаемые параметры, временной период и идентификатор счетчика. Опционально администратор может выбрать группу, к которой будет принадлежать этот виджет, т.е. предоставить доступ к виджету согласно разрешениям групп пользователей. Виджет можно сохранить, щелкнув кнопку **Submit**.


Рис. 4 – Экран Dashboard – добавление виджета

На рисунке ниже показан настроенный пользователем виджет.

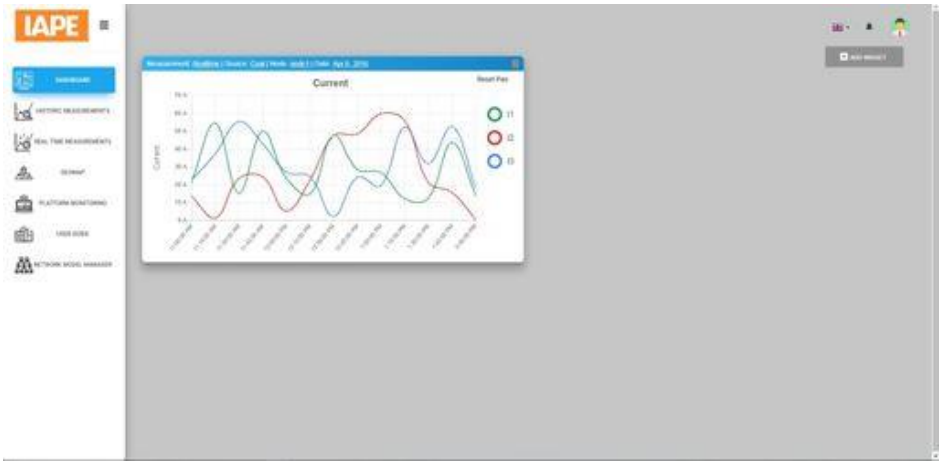


Рис. 5 – Экран Dashboard с настроенным виджетом

### 1.7.2. Экран Historic measurements

Назначением этого экрана является просмотр всех исторических данных по измерениям, собранным умными счетчиками.

На экране **Historic Measurements** пользователь может просмотреть все доступные источники энергии, такие как Уголь (**Coal**), Ядерная (**Nuclear**), Гидро (**Hydro**), Ветер (**Wind**), Солнечная (**Solar**) и т.д. Щелкнув по каждому из источников энергии, можно просмотреть более подробные данные и круговую диаграмму с собранными и просуммированными данными за 24 часа. Кроме того, отображаются данные по соотношению сгенерированная энергия/потребленная энергия на каждый источник энергии. Также можно отфильтровать данные по суммарному объему, по конкретной станции или умному счетчику.

На первой вкладке экрана (**Summarized measurement data)** показаны суммарные данные измерений за 24-часовой период в виде круговой диаграммы и такие показатели, как генерируемая энергия (**Generated Power**) и средняя генерируемая энергия (**Average Generated Power**) на источник энергии.

Все источники энергии разделены по категориям. Экраны категорий различаются только списками умных счетчиков и типом данных, получаемых от этих умных счетчиков.

Щелчком по какому-либо источнику энергии пользователь переходит на экран соответствующего поставщика энергии. Этот экран содержит таблицу со списком умных счетчиков, гистограмму со всеми данными за 24 часа по сгенерированной энергии каждым из узлов конкретного источника энергии, а также отображается коэффициент мощности (**cosFi)**, который обновляется в реальном времени. Его значение может быть от -1 до 1 и в зависимости от этого значения выделяется шкала (от хорошего до плохого показателя – зеленым, желтым или красным).

В этой таблице пользователь может просмотреть подробную информацию о том или ином счетчике, щелкнув кнопку **Details** в строке нужного умного счетчика.


Рис. 6 – Экран Historic Measurements

После выбора какого-либо источника энергии появляется список всех соответствующих ему станций или умных счетчиков, а также гистограмма с историческими данными, собранными за последние 24 часа (показано на рисунке ниже).

На вкладке **View smart meters** пользователю предоставляется меню, в котором можно выбрать конкретный параметр умного счетчика: электрический ток (**electrical current**), мощность (**power**), напряжение (**voltage**) и реактивная мощность (**reactive power**). После выбора параметра нужно ввести период времени сбора исторических данных. Появится линейный график, на котором каждое значение выбранного параметра выделяется цветом на линиях графика. Кроме того, пользователь может выбрать один из двух типов графика: линейный график или гистограмма. В правом верхнем углу графика находится область с переключателями для скрытия или отображения каждого из

параметров. Также при наведении указателя на конкретную точку графика появляется окно с данными соответствующего параметра в этот момент времени.

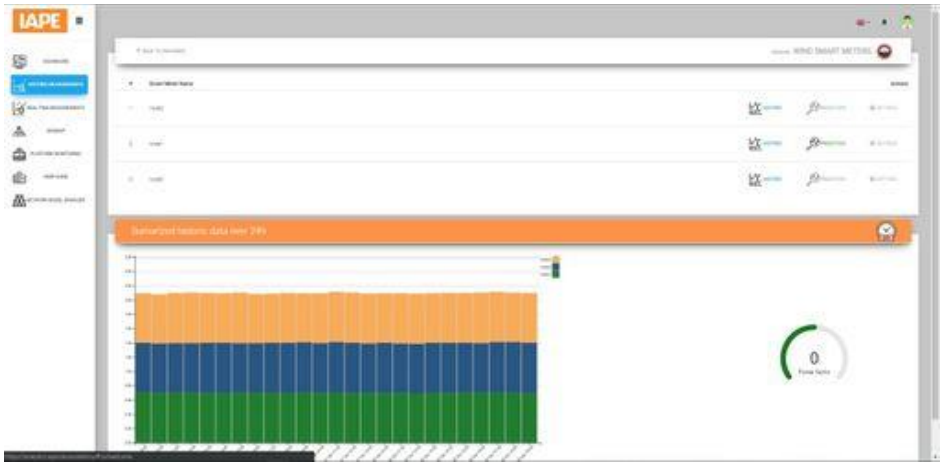

Рис. 7 – Экран **Historic measurements** – **View smart meters**

Если выбран тот или иной умный счетчик или узел, пользователь может просмотреть его параметры, такие как ток (**Current**), напряжение (**Voltage**), мощность (**Power**), коэффициент мощности (**Power factor**) и т.д. в числовом или графическом выражении. Например, если выбран параметр «электрический ток» (**Electrical Current**), пользователь может выбрать режим просмотра всех токов i1, i2, i3 одновременно или по выбору, как показано на рисунке ниже.

Рис. 8 – Экран **Historic measurements** – **View Smart Meters – View node** (линейный график)

Та же информация может отображаться в виде гистограммы по необходимости.

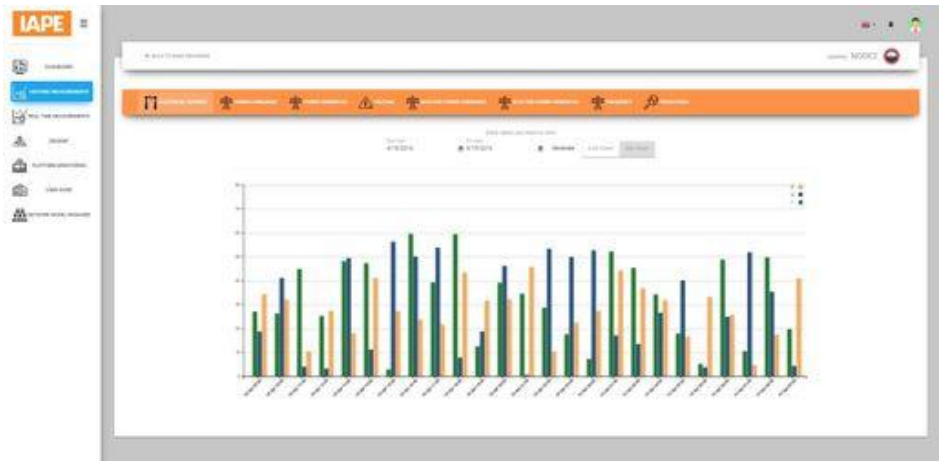

Рис. 9 – Экран **Historic measurements** – **View Smart Meters** – **View node** (гистограмма)

### 1.7.3. Прогнозирование и аналитика

Прогнозирование лежит в основе множества ключевых сценариев использования в секторе энергетики. В частности, помочь решить критические проблемы может прогнозирование по запросу. С помощью модуля аналитики был сформирован узкий сценарий использования, основным назначением которого является прогнозирование распределения вероятностей генерирования энергии ветра одной или нескольких ветряных установок.

Необходимо открыть представление **Wind Power Forecasting.** Данные по предсказанию можно увидеть в категории **Wind**, экран которой имеет схожую структуру с экранами других источников энергии. Он так же содержит таблицу со списком умных счетчиков и доступных действий, различие только в том, что в столбце действий есть кнопка **Historic** для просмотра исторических данных каждого счетчика и кнопка **Prediction** для просмотра прогнозов для конкретного счетчика. На данный момент прогнозы доступны только для одного умного счетчика (**node1**).

После нажатия на кнопку **Prediction** пользователь переходит на экран с линейным графиком, который показывает прогнозируемое значение мощности по предварительно заданному периоду времени. Этот линейный график имеет те же функциональные возможности, что и другие графики на экране **Historic measurements**.

После нажатия на кнопку **Historic** пользователь переходит на экран, содержащий список параметров: электрический ток (**electrical current**), напряжение (**voltage**) и реактивная мощность (**reactive power**), а также кнопку **Predictions**, которая может быть активна или нет в зависимости от наличия прогнозов для конкретного счетчика. При наличии прогнозов для счетчика на графике «мощность» (**power**) будут отображаться прогнозируемое значение и реально измеренное значение.

### 1.7.4. Экран Real Time Measurements

Экран **Real Time Measurements** похож по структуре на экран **Historic Measurements**, с отличием в том, что на данном экране на графиках отображаются данные, обновляемые в реальном времени.

В первую очередь эти линейные графики показывают исторические данные умных счетчиков по источникам Уголь (**Coal**) и Гидро (**Hydro**) с параметрами: электрический ток (**current**), напряжение (**voltage**), активная мощность (**active power**), реактивная мощность (**reactive power**), (**current, voltage, active power, reactive power**) за заданный период времени.

При получении с сервера новых данных, графики автоматически обновляются и отображают новые данные счетчиков. Каждый линейный график имеет легенду с переключателями для скрытия или отображения той или иной линии.

При наведении указателя на ту или иную точку графика, появляется окно с подробностями. С помощью колесика мыши можно приблизить график. Также можно переместить график по временной шкале, перетащив его указателем.

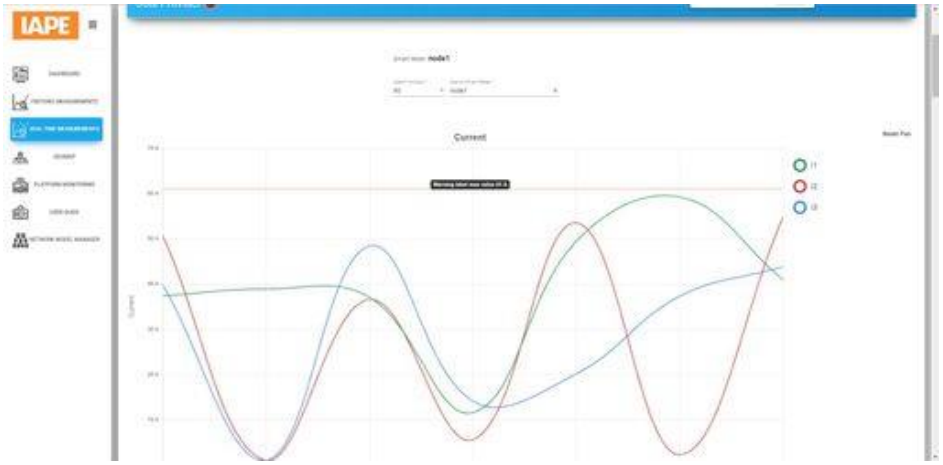


Рис. 10 – Экран **Real Time Measurements**

### 1.7.5. Экран GeoMap

Экран **GeoMap** обеспечивает географическую визуализацию сети умных счетчиков и станций. На карте можно увидеть точное местоположение каждого счетчика, его состояние (активный или неактивный) и тип источника энергии, который он отслеживает.

При наведении указателя на значок конкретного счетчика появляется окно с данными этого счетчика: имя, состояние (активный или неактивный). Щелкнув по значку счетчика, можно перейти на экран с более подробными данными счетчика. Кроме того, вся карта поделена на регионы, пользователь может приблизить тот или иной регион, щелкнув по нему на карте.

Возможные состояния станций: ON (работает нормально) или OFF (отключена или активен аварийный сигнал). Если на той или иной станции активен аварийный сигнал, значок этой станции мигает синим цветом на карте. Щелком по значку станции на карте пользователь может перейти на экран с более подробными данными станции.

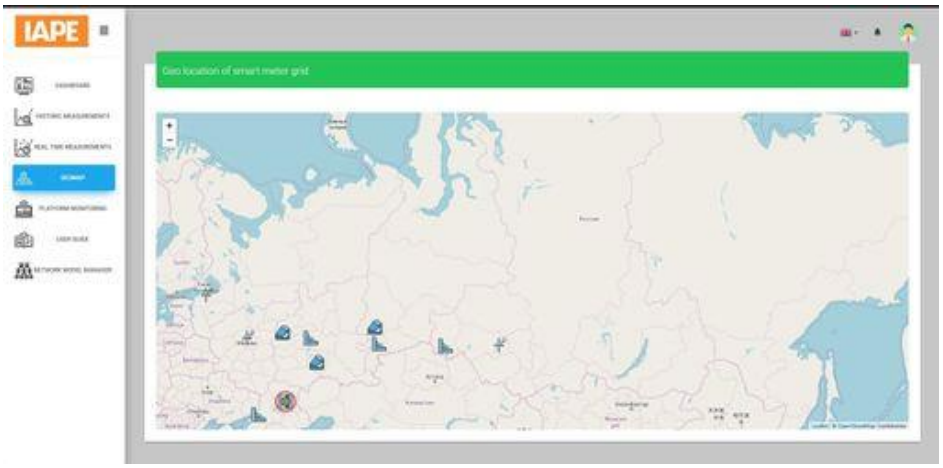


Рис. 11 – Экран GeoMap

### 1.7.6. Уведомления

Уведомление – это системное сообщение, которое появляется в интерфейсе пользователя. Когда активен экран **Real time measurements** и какой-либо график имеет значение выше ожидаемого, этот факт отображается в виде значка в области уведомлений.

Чтобы просмотреть подробности уведомления, пользователь может открыть уведомление в модальном режиме. Все данные будут представлены в виде таблиц, и каждый параметр будет разделен табуляцией. Данные могут быть отсортированы щелком по названию параметра или названию значения.

Пользователь может просмотреть область уведомлений в любое время.

### 1.7.7. Всплывающие уведомления

**Всплывающее уведомление** – это немодальное, небольшое системное сообщение которое появляется в интерфейсе пользователя и в течение нескольких секунд исчезает. В данном приложении оно используется для показа пользователю информации о запросе приложения к платформе. Например, об обнаруженной ошибке

Все сообщения выделяются цветом в зависимости от типа и наличия ошибок:

- Зеленый – для успешных транзакций и запросов к платформе.
- Красный – для ошибок при запросе данных к платформе.
- Желтый – для оповещений о том или ином типе информации.

## 1.8. Мониторинг платформы IAPE

Мониторинг платформы IAPE осуществляется на всех компонентах платформы с целью обеспечения визуального контроля функциональности и рабочего состояния компонентов. Экран **IAPE Management** содержит несколько вкладок, таких как: **Register Platform Components** (регистрация компонентов платформы), **SDP Management** (управление программно-управляемым периметром), **IDP Management** (управление поставщиком идентичности), **Key Management** (управление ключами)**, Ingestor Management** (управление компонентом Ingestor).

### 1.8.1. Вкладка Register Platform Components

На данной вкладке администратор может добавлять настраиваемые модули.

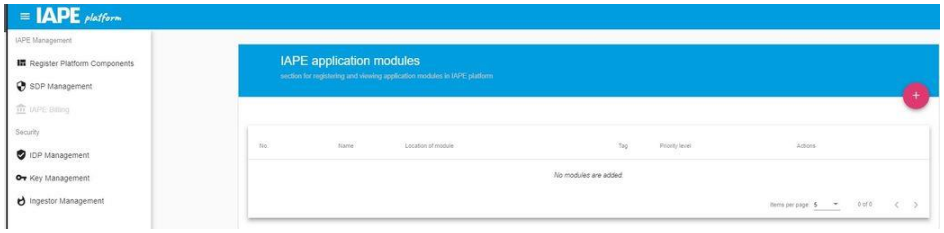


Рис. 12 – Вкладка **Register Platform Components**

# 2. Руководство пользователя Software Defined Perimeter (SDP)

## 2.1. Общие сведения

Программно-управляемый периметр (Software Defined Perimeter, SDP) является набором спецификаций для технологии контроля доступа следующего поколения. Ключевыми концепциями SDP являются концепции предварительной авторизации доступа и предварительной аутентификации запросов на подключение. Основная идея заключается в том, что периметр защищает и изолирует сеть и устройства от любого типа доступа со стороны неавторизованных пользователей, предоставляя доступ только при прохождении проверок на ограниченный период времени.

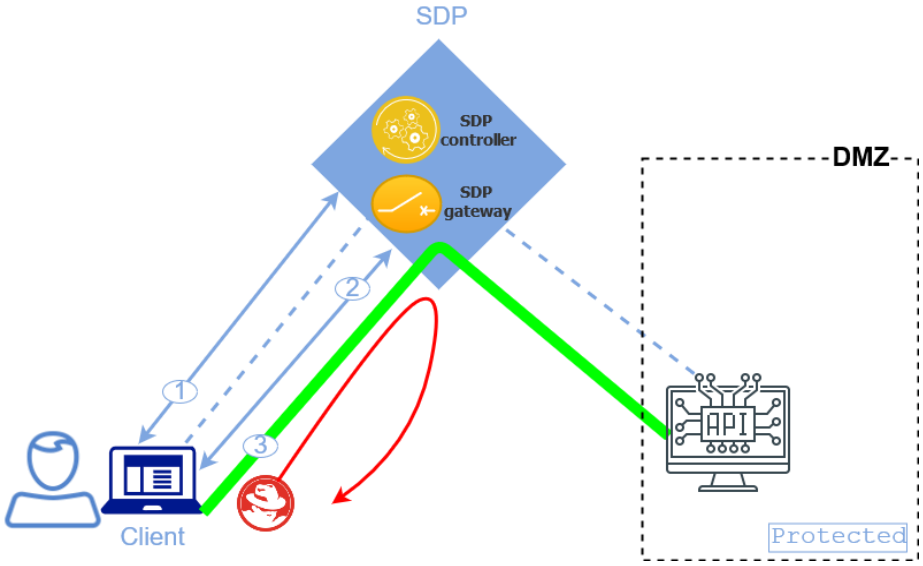


Рис. 13 – Архитектура SDP

## 2.2. Доступ

Для доступа к SDP в приложении **IAPE Platform Monitoring** нужно выбрать элемент **SDP Management.** В загрузившемся приложении надо нажать на элемент **Toggle sidebar** в правом верхнем углу страницы – в результате в левом верхнем углу появятся основные меню: **Manage** и **Monitoring**.

## 2.3. Управление

Элементы меню **Manage** предназначены для обеспечения доступа к функциям управления архитектурой SDP.

## 2.4. Экран Clients

Экран **Clients** содержит список всех существующих в системе клиентов, при этом функция создания клиента, **Create**, на этом экране отсутствует. Отображаемые свойства для каждого клиента: **ID** (идентификатор), **Name** (имя), **Valid** (валидность), **Encrypt key** (ключ шифрования), **Hmac key** (ключ HMAC).

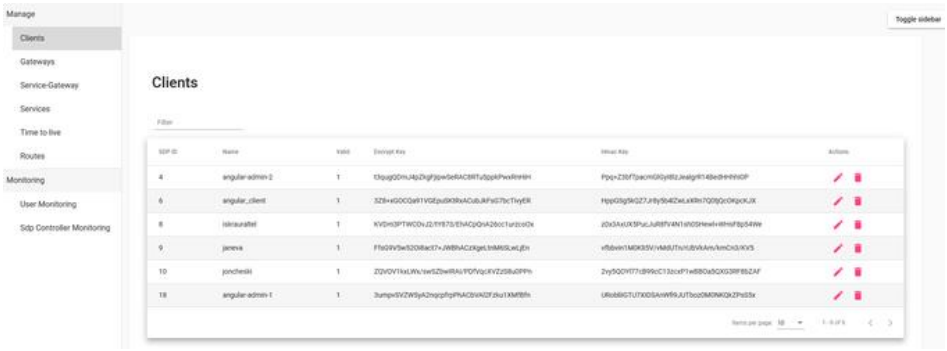


Рис. 14 – Экран **Manage → Clients**

## 2.5. Экран Gateways

Экран **Gateways** содержит список всех существующих в системе шлюзов, при этом функция создания шлюза, **Create**, на этом экране отсутствует.

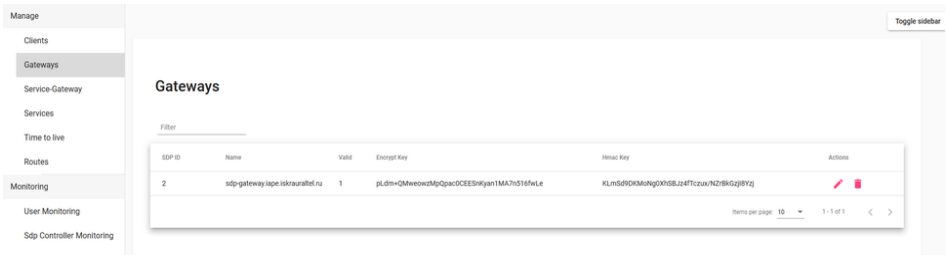


Рис. 15 – Экран **Manage → Gateway**

## 2.6. Экран Service Gateways

Тому или иному сервису должен быть назначен определенный шлюз, протокол и порт (все клиенты этого сервиса будут иметь соответствующие права). Поэтому для этого необходимо сначала создать сервисный шлюз на экране **Service Gateways**. Все порты, добавленные на данном экране, являются сервисами, доступными для клиентов. Они должны быть настроены на экране **Routes**.

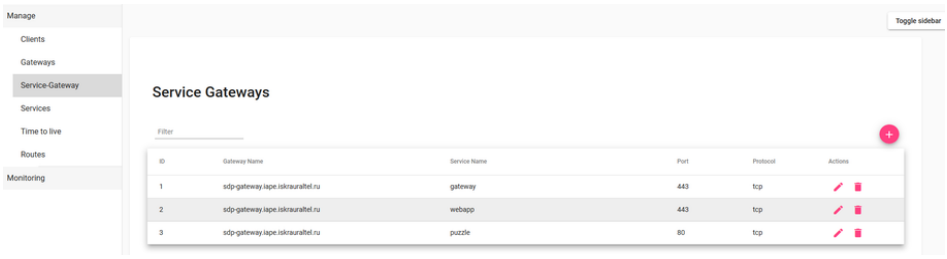


Рис. 16 – Экран **Manage → Service Gateways**

## 2.7. Экран Services

Сервис в рамках архитектуры SDP представляет собой кластер с заданным именем. Если один сервис связан с несколькими клиентами, каждый клиент получает соответствующие сервису права. На экране **Services** можно просмотреть все существующие сервисы, а также все связанные с ними клиенты.

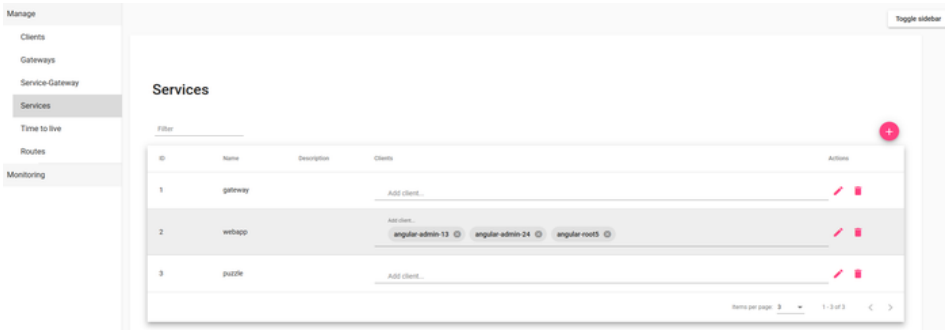


Рис. 17 – Экран **Manage → Services**

## 2.8. Экран Time to live

На экране Time to live можно изменить параметр «временя жизни» (Time To Live, TTL) SDP-шлюза.

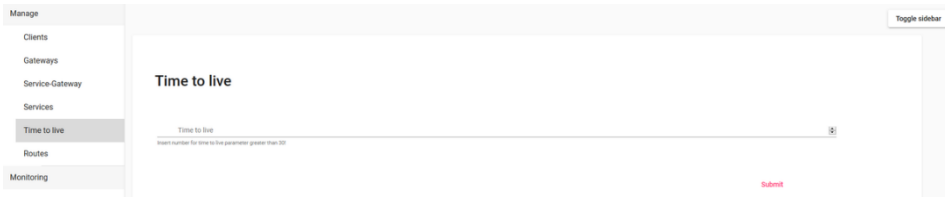


Рис. 18 – Экран **Manage → Time to live**

## 2.9. Экран Routes

На экране **Routes** применяются настройки, выполненные на экране **Service Gateways**. Основным назначением этого экрана является создание и контроля местоположения (*location*) и назначения его серверному блоку (*server block*). В сущности, здесь задаются правила обработки запросов сервером.

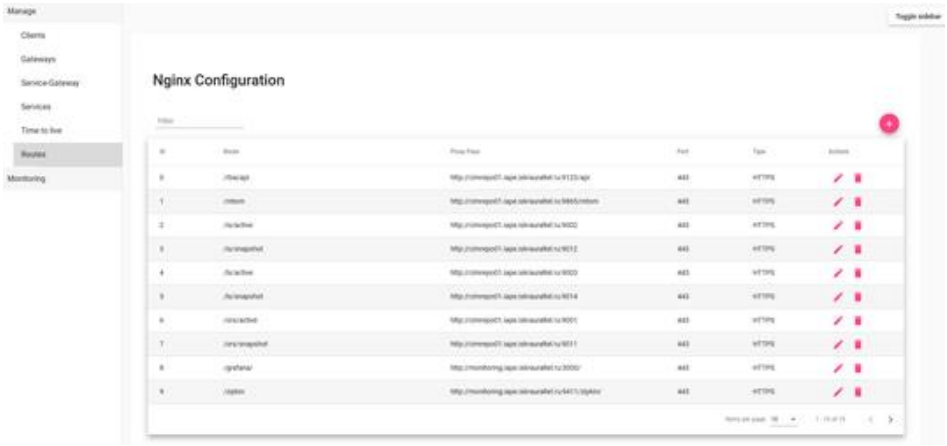


Рис. 19 – Экран **Manage → Routes**

## 2.10. Мониторинг

Элементы меню **Monitoring** предназначена для обеспечения доступа к функциям мониторинга SDP-клиентов.

## 2.11. Экран User Monitoring

Основным назначением экрана **User Monitoring** является мониторинг всех клиентов, попытавшихся получить доступ к SDP-шлюзу. Причем соединение может быть как успешным, так и неуспешным. Также для каждого соединения отображается его тип: **open** (открытое) или **closed** (закрытое). Если его тип **closed**, то отображается время установки соединения и время его завершения. В противном случае данное поле пустое. Кроме того, на данном экране отображаются параметры: **Client ID** (идентификатор клиента), **Source IP** (IP-адрес источника), **IP Allow** (разрешенный IP-адрес), **Destination IP** (IP-адрес назначения), **Destination Port** (порт назначения), а также **Success** (успешное), который показывает, было ли соединение успешным или неуспешным.

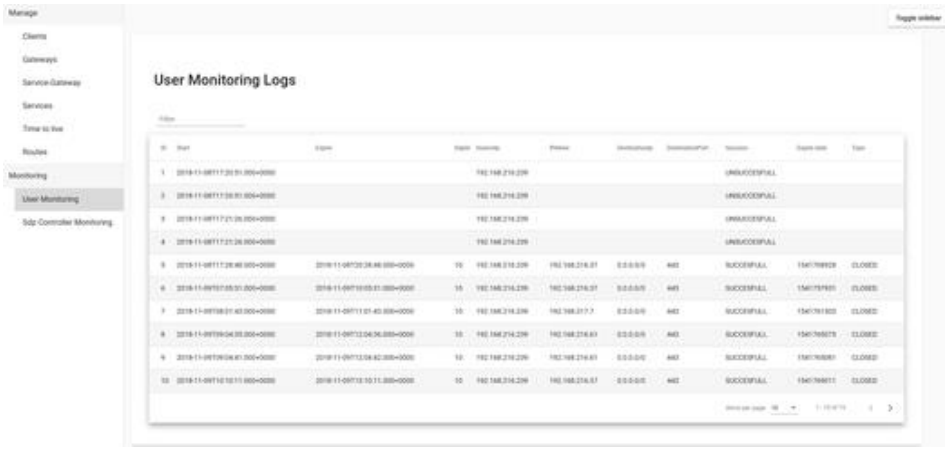


Рис. 20 – Экран **Monitoring → User Monitoring**

## 2.12. Экран SDP Controller Monitoring

Основным назначением экрана **SDP Controller Monitoring** является журналирование попыток подключения к SDP-контроллеру. На данном экране отображаются параметры: **Time** (время исходящего запроса на соединение), **Client ID** (идентификатор клиента) и **Connection ID** (идентификатор соединения).

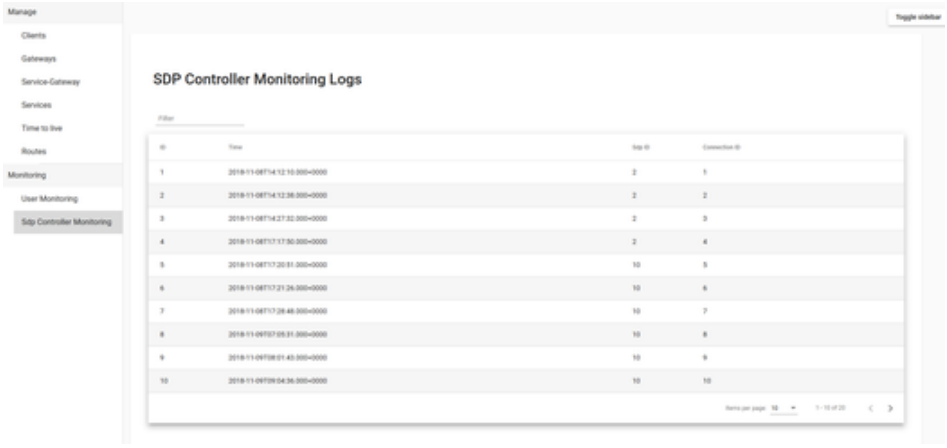


Рис. 21 – Экран **Monitoring → SDP Controller Monitoring**

# 3. Руководство пользователя системы управления ключами FreeIPA

## 3.1. Общие сведения

FreeIPA (Free Identity, Policy and Audit) — открытый проект для создания централизованной системы для идентификации пользователей, задания политик доступа и аудита, система обеспечения безопасности в виртуализированных средах. Он является контроллером домена для машин на ОС Linux и Unix и задает домен с помощью управляющих серверов и зарегистрированных клиентских машин по тому же принципу, что и продукт Microsoft Active Directory. Таким образом обеспечивается централизованная структура в средах Linux/Unix. FreeIPA является решением для управления пользователями, группами, хостами, сервисами и т.д. FreeIPA был разработан на базе нескольких проектов с открытым исходным кодом, включая 389 Directory Server, MIT Kerberos, а для управления сертификатами используется Dogtag.

Для обнаружения машин и соединения с другими клиентами в домене используется DNS. Для синхронизации всех часов в домене, что обеспечивает правильную работу журналирования, сертификатов и операций, используется NTP. Для Kerberos-сервисов сертификаты предоставляются сервисом сертификатов. Все эти дополнительные сервисы работают совместно под контролем сервера FreeIPA.

Сервер FreeIPA также имеет набор инструментов, которые используются для управления всеми связанными с FreeIPA сервисами. Вместо того, чтобы управлять сервером LDAP, настройками KDC или DNS по отдельности, с помощью разных инструментов на локальных машинах, FreeIPA имеет единый набор инструментов управления (CLI и web UI), который обеспечивает централизованное и целостное администрирование домена.

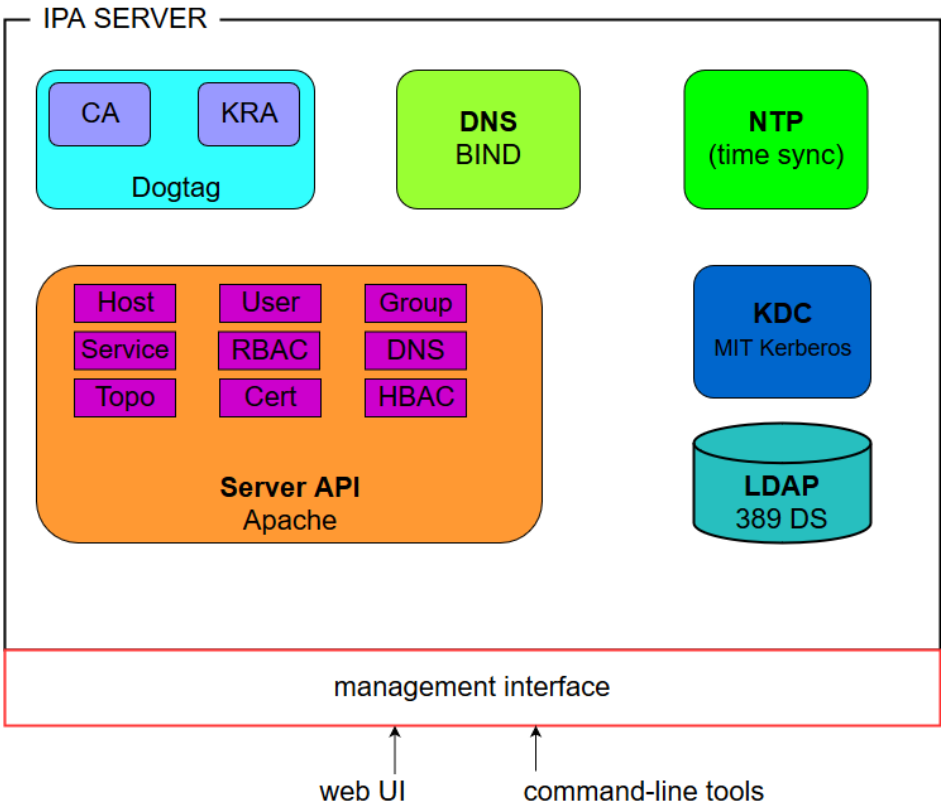


Рис. 22 – Сервер FreeIPA: унификация сервисов

## 3.2. Доступ

Для доступа к FreeIPA в приложении **IAPE Platform Monitoring** нужно выбрать элемент **Key Management**:

## 3.3. Импортирование сертификата FreeIPA в хранилище доверенных корневых сертификатов

1. Перейдите на веб-сайт FreeIPA, https://<*ipa.hostname*>/*ipa/ui*, и войдите в систему в роли администратора.
2. Перейдите на вкладку **Authentication → Certificates → Certificates**.

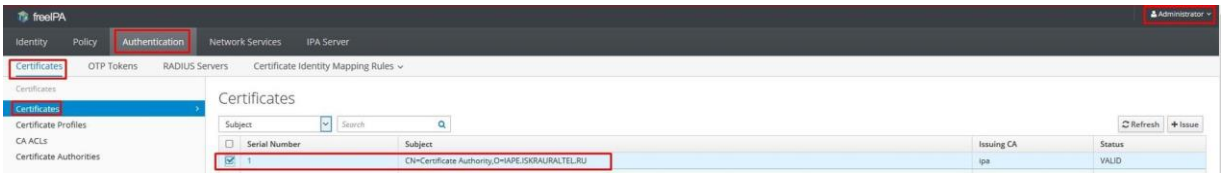


Рис. 23 – Выбор сертификата FreeIPA

Обычно первым сертификатом является корневой сертификат центра сертификации rootCA FreeIPA.

3. Загрузите сертификат FreeIPA.

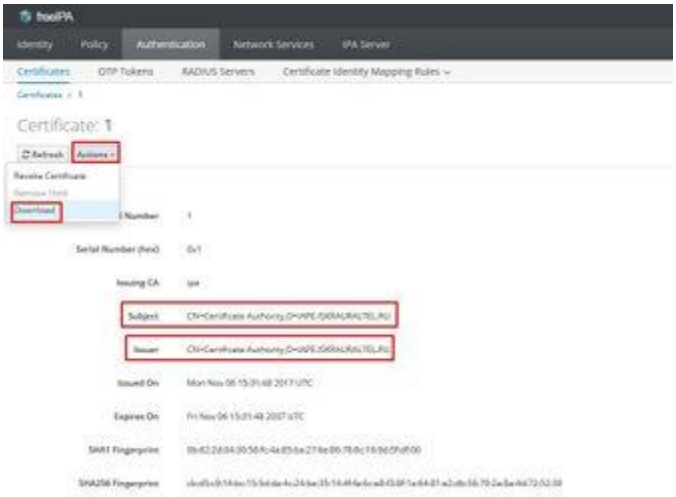


Рис. 24 – Загрузка сертификата FreeIPA

При сохранении сертификата изменяется его расширение с *.*pem* на *.crt.

### 3.3.1. Для браузера Mozilla Firefox browser

1. На вкладке **Options** под **Certificates** выберите элемент **View Certificates**.
2. Во окне **Certificate Manager** на вкладке **Authorities** выберите **Import,** и выберите нужный корневой сертификат rootCA.
3. Установите все флажки и щелкните кнопку **OK**.

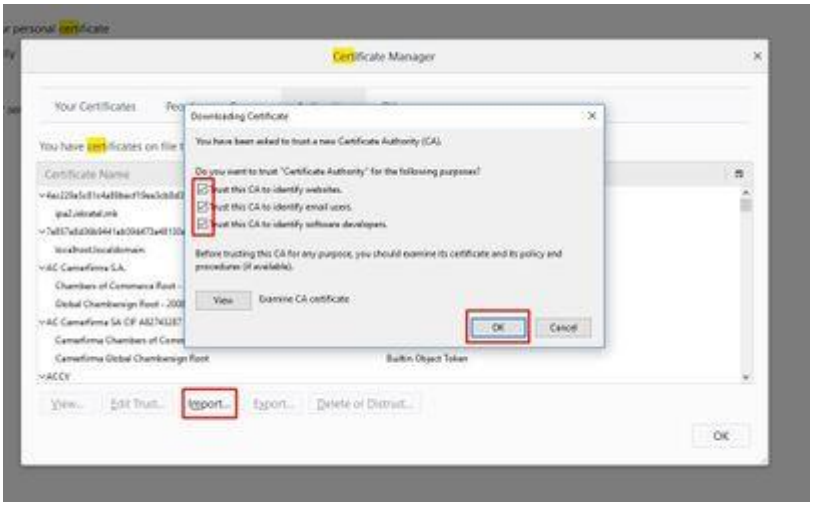


Рис. 25 – Импортирование сертификата FreeIPA в браузере Firefox

### 3.3.2. Для всех компьютеров и других браузеров

1. Перейдите в директорию загруженного сертификата и дважды щелкните файл сертификата или щелкните файл сертификата правой кнопкой и выберите **Install Certificate**.
2. Под **Store Location** выберите **Current User** и щелкните кнопку **Next**.

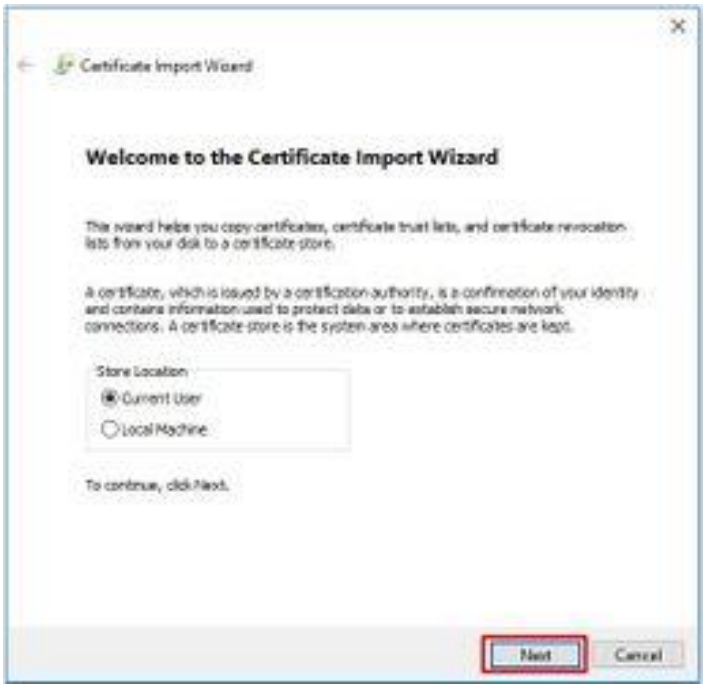


Рис. 26 – Импортирование сертификата FreeIPA в ОС Windows

3. Выберите **Place all certificates in the following store,** щелкните кнопку **Browse**, выберите **Trusted Root Certification Authorities**, щелкните кнопку **OK**, а затем кнопку **Next**.

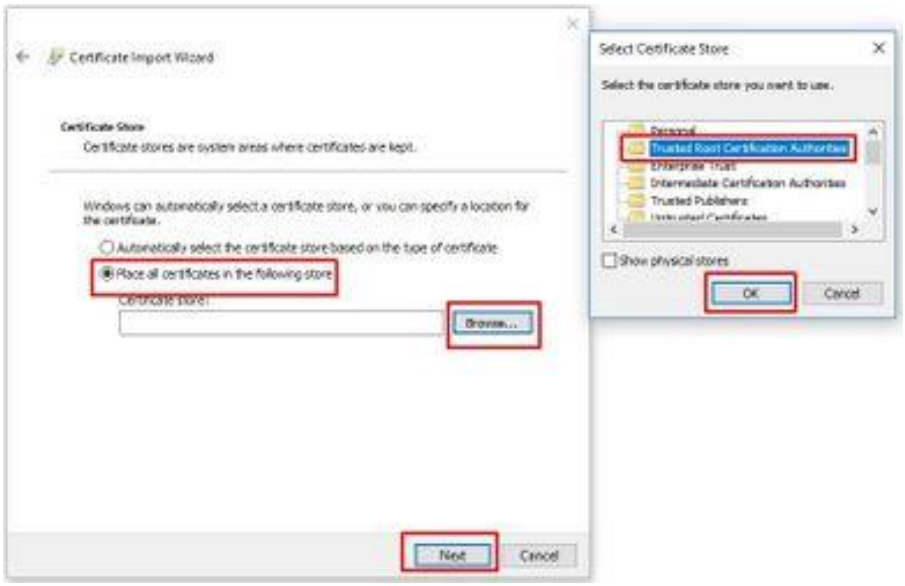


Рис. 27 – Выбор хранилища сертификатов

### 3.3.3. Импортирование клиентского сертификата в браузере

1. Загрузите сертификат из директории */ete/pki/tls/client.pfx* на машине FreeIPA.
2. В браузере на вкладке **Options** под **Certificates** выберите элемент **View Certificates**.
3. Во окне **Certificate Manager** на вкладке **Your Certificates** выберите **Import,** и выберите нужный клиентский сертификат с расширением *.pfx.
4. Введите пароль, который был использован для шифрования сертификата, и щелкните кнопку **OK**.

Импортированный сертификат появится в окне **Certificate Manager** на вкладке **Your Certificates**.

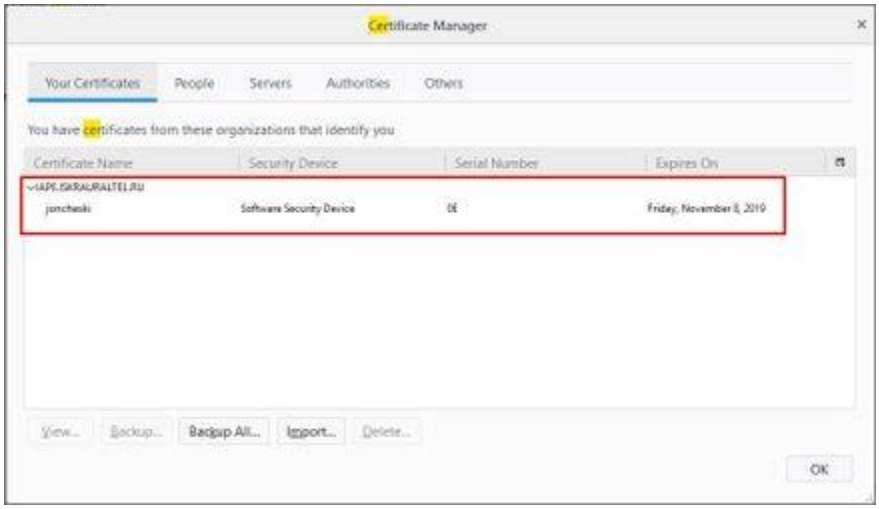


Рис. 28 – Окно Certificate Manager

## 3.4. Создание нового пользователя

Команды и процедуры, приведенные ниже, выполняются на сервере FreeIPA.

1. Перейдите на главную страницу FreeIPA и выберите элементы **Identity → Users → Active Users → Add**.
2. Заполните необходимые поля и подтвердите создание пользователя.

### 3.4.1. Генерирование сертификата для клиента

1. Войдите на сервер FreeIPA посредством SSH.
2. Выполните команду:

```
cd /etc/pki/tls
openssl req -new -sha256 -nodes -out <name_of_user>.csr -newkey rsa:2048 -
keyout <name_of_user>.key -config openssl.cnf
```

3. Перейдите по URL-адресу FreeIPA, *https://<ipa.hostname>/ipa/ui*, выберите элемент **Active users**, а затем щелкните имя нужного пользователя.
4. Чтобы создать сертификат с расширением **.pem*, в меню **Action** выберите **New Certificate**, а затем скопируйте текст из файла */etc/pki/tls/<имя_пользователя>.csr* в соответствующее поле ввода текста.

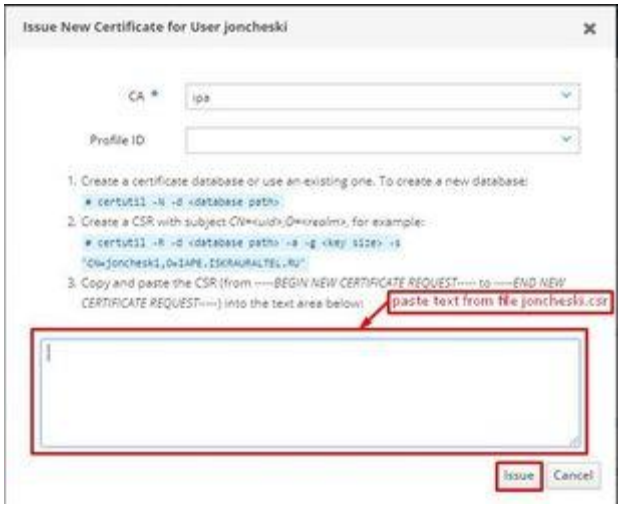


Рис. 29 – Создание сертификата с расширением *.pem

5. Загрузите сертификат с расширением **.pem* (имя файла – *<имя_пользователя>.pem*) из FreeIPA: щелкните имя нужного пользователя, под **Account Settings** выберите нужный сертификат, а затем в меню **Actions** выберите **Download**.
6. Скопируйте сертификат в директорию */etc/pki/tls* на сервере FreeIPA.
7. Экспортируйте сертификат с расширением *.pfx для клиента, выполнив команду:

```
openssl pkcs12 -export -out <name_of_user>.pfx -inkey <name_of_user>.key -in
<name_of_user>.pem
```

## 3.5. Генерирование сертификата для хоста

Команды и процедуры, приведенные ниже, выполняются на сервере FreeIPA.

1. Создайте хост в FreeIPA из Keycloak, выполнив команду:

```
cd /etc/pki/tls
openssl req -new -sha256 -nodes -out <fqdn of host>.csr -newkey rsa:2048 -
keyout <fqdn of host>.key -config openssl.cnf
```

Пример входных аргументов:

```
Organization Name (организация) [Default Company Ltd]:IAPE.ISKRAURALTEL.RU

Common Name (сетевое имя сервера) []:<fqdn of host>
```

2. Перейдите по адресу FreeIPA, *https://<ipa.hostname>/ipa/ui*, выберите элементы **Identity** > **Hosts**, а затем щелкните кнопку **Add**.

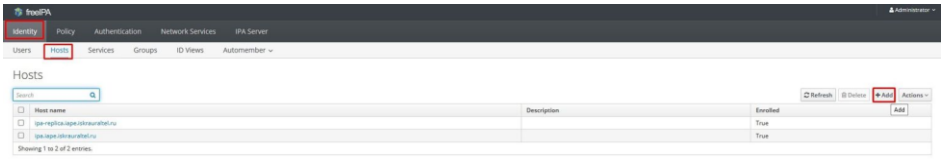


Рис. 30 – Хосты FreeIPA

3. В поле **Host name** введите сетевое имя Keycloak (оно должно совпадать с сетевым именем в DNS) и в поле **IP Address** введите внутренний IP-адрес OpenStack.

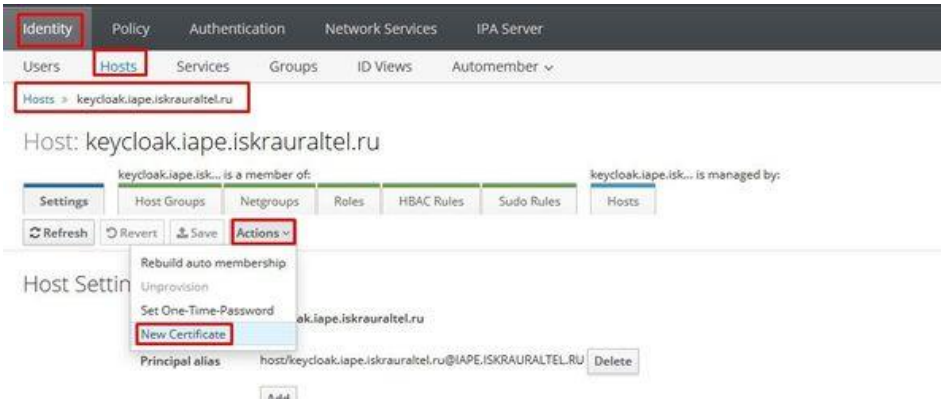


Рис. 31 – Создание сертификата для нового хоста

4. Перейдите по адресу FreeIPA, https://<ipa.hostname>/ipa/ui, выберите элемент **Hosts** и щелкните имя нужного хоста.
5. Выберите элементы **Actions → New Certificate**.
6. Во всплывающем окне в списке **CA** выберите **IPA**, а в поле ввода текста скопируйте текст из файла *host.csr*.
7. Загрузите сертификат с расширением *.pem (имя файла – <*fqdn_xocma*>*.pem*) из FreeIPA: щелкните имя хоста, под Host Certificate выберите нужный сертификат, а затем в меню **Actions** выберите **Download**.
8. Скопируйте сертификат в директорию */etc/pki/tls* на сервере FreeIPA.
9. Экспортируйте сертификат, выполнив команду:

```
openssl pkcs12 -export -clcerts -in <fqdn of host>.pem -inkey <fqdn of
host>.key -out <fqdn of host>.p12
```

### 3.5.1. Генерирование файла keystore.jks

Примечание. Команды и процедуры, приведенные ниже, выполняются на сервере FreeIPA.

- Выполните команду:

```
cd /etc/pki/tls
keytool -importkeystore -srckeystore <fqdn of host>.p12 -srcstoretype pkcs12
-destkeystore <fqdn of host>.jks -deststoretype JKS
```

### 3.5.2. Генерирование файла truststore.jks

Команды и процедуры, приведенные ниже, выполняются на сервере FreeIPA.

- Выполните команду:

```
cd /etc/pki/tls
keytool -import -file /etc/ipa/ca.crt -keystore truststore.jks
Trust this certificate? [no]: yes
```

### 3.5.3. Создание клиента в FreeIPA для архитектуры SDP

Команды и процедуры, приведенные ниже, выполняются на сервере FreeIPA.

1. Создайте пользователя в FreeIPA. Общее имя (Common name) в сертификатах должно совпадать с именем пользователя FreeIPA.
2. Создайте клиентский сертификат, выданный ЦС SDP и использующийся для связи SDP-клиента с SDP-шлюзом и другими SDP-клиентами.
3. Войдите в машину FreeIPA.
4. Выполните команду:

```
cd /etc/pki/tls

openssl req -new -sha256 -nodes -out <username of client>.csr -newkey
rsa:2048 -keyout <username of client>.key -config openssl.cnf
```

Пример входных аргументов:

| **Organization Name (организация) [Default Company Ltd]:IAPE.ISKRAURALTEL.RU**<br><br>**Common Name (имя пользователя или сетевое имя сервера) []:<username of client>** |
|---|

5. На SDP-клиенте перенесите личный ключ в директорию */root/<имя_клиента>.key*.
6. Создайте нового пользователя: выберите элементы **Identity** → **Users**, под **User Categories** выберите элемент **Active Users**, а затем щелкните кнопку **Add**.
7. Во всплывающем окне введите реквизиты доступа для нового пользователя.
8. Перейдите по адресу https://ipa.iape.iskrauraltel.ru/ipa/ui, выберите элемент **Active Users** и щелкните имя нужного пользователя.
9. В меню **Actions** выберите **New Certificate**.
10. Во всплывающем окне в списке **CA** выберите **SDP0**, а в поле ввода текста скопируйте текст из файла */etc/pki/tls/<имя_пользователя>.csr*.
11. Загрузите сертификат с расширением *.crt (имя файла – *<имя_клиента>.crt*) из FreeIPA: щелкните имя пользователя, под **Account Settings** выберите нужный сертификат, а затем в меню **Actions** выберите **Download**.
12. Скопируйте сертификат в директорию */etc/pki/tls* на сервере FreeIPA.
13. На SDP-клиенте перенесите файл в директорию */root/joncheski.crt*.

### 3.5.4. Вкладка Ingestor Management

(здесь исходно ничего не было)