

# Организация пространств (Realm). Настройки времени действия токенов

## Введение

Realm - пространство управляет набором пользователей, учетных данных, ролей и групп. Пользователь принадлежит к пространству и входит в него. Пространства изолированы друг от друга и могут только управлять и аутентифицировать пользователей, которыми они управляют.

При установке Keycloak в первый раз создается пространство Master. Это пространство является главным. Это самый высокий уровень в иерархии Realms. Учетные записи администратора в этом пространстве имеют разрешения на просмотр и управление любым другим пространством, созданным на сервере.

**Не рекомендуется** использовать Master-пространство для управления пользователями и приложениями в организации. Использование Master-пространства необходимо закрепить за администраторами для создания и управления пространствами в системе.

Можно отключить Master-пространство и определить учетные записи администратора в каждом отдельном новом пространстве, которое вы создаете. Каждое пространство имеет свою собственную выделенную консоль администратора, в которую можно войти с помощью локальных учетных записей.

## Создание и настройка Realm в Keycloak. Общее описание

Кроме редактирования конфигурации вручную через панель администрирования Keycloak, имеется возможность изменить конфигурацию сервера с помощью jboss-cli или через загрузку конфигурационного файла.


### Примечание.

На текущий момент, загрузка и выгрузка конфигурации пространства все еще не соответствует ожиданиям. Работает некорректно.

Действие	Описание
Создание	<div>1. Доступ для фронтальной части допустимо указать через внешний балансировщик</div> <div><div>Frontend URL ⓘ</div><div></div></div>

Режим SSL

Для каждого пространства имеется возможность использования режима SSL. Браузеры и приложения, взаимодействующие с пространством, должны соблюдать требования SSL/HTTPS, определенные режимом SSL, иначе им не будет разрешено взаимодействовать с сервером. Keycloak генерирует self-signed сертификат в первый раз. self-signed сертификаты не являются безопасными и должны использоваться только для тестирования.

Demo 

General

Login

Keys

Email

Themes

Cap

User registration ?

ON

Email as username ?

OFF

Edit username ?

OFF

Forgot password ?

ON

Remember Me ?

OFF

Verify email ?

OFF

Login with email ?

ON

Require SSL ?

external requests

Save

Cancel


external requests	none	all requests
Пользователи могут взаимодействовать с Keycloak без SSL, пока они используют частные IP-адреса, такие как localhost, 127.0.0.1, 10.0.x.x, 192.168.x. x, и 172.16.x. x. При попытке получить доступ к Keycloak без SSL с не частного IP-адреса, будет выведено сообщение об ошибке.	Keycloak не требует SSL.	Keycloak требует SSL для всех IP-адресов.





Настройка почты


Keycloak отправляет электронные письма пользователям для проверки их адреса электронной почты, когда они забывают свои пароли или когда администратору необходимо получать уведомления о событии сервера. Чтобы включить Keycloak для отправки электронной почты, необходимо в Keycloak ввести настройки SMTP-сервера. Настройка учетных данных (логин и пароль для запроса на сервер) задается отдельно для каждого пространства.

Demo 


General Login Keys **Email** Themes Cache Tokens Client Registration Security Defenses

\* Host SMTP Host Test connection


Port SMTP Port (defaults to 25)

From Display Name  Display Name for Sender Email Address

\* From Sender Email Address

Reply To Display Name  Display Name for Reply To Email Address

Reply To Reply To Email Address



Envelope From  Sender Envelope Email Address

Enable SSL ☐ OFF

Enable StartTLS ☐ OFF

Enable Authentication ☒ ON

\* Username Login Username

\* Password   

Save Cancel


Host	Port	From
Хост - имя хоста SMTP-сервера, используемого для отправки электронной почты.	Порт SMTP-сервера.	адрес, используемый для SMTP-заголовка From для отправленных сообщений электронной почты.

Настройка темы

Темы позволяют изменить внешний вид любого пользовательского интерфейса в Keycloak. Темы настраиваются для каждого пространства отдельно.

Login Theme	Account Theme	Admin Console Theme	Email Theme
Ввод пароля пользователя, регистрация нового пользователя и другие подобные экраны, связанные с входом в систему.	Каждый пользователь имеет User Account Management UI.	Интерфейс администратора Keycloak.	Всякий раз, когда Keycloak должен отправить электронное письмо, он использует шаблоны, определенные в этой теме.

# Конфигурация токенов (таймаутов)

Demo 

General

Login

Keys

Email

Themes

Cache

Tokens

Client Registration

Security Defenses

Default Signature Algorithm ?

Revoke Refresh Token ?

OFF

SSO Session Idle ?

30

Minutes ▾

SSO Session Max ?

10

Hours ▾

SSO Session Idle Remember Me ?

0

Minutes ▾

SSO Session Max Remember Me ?

0

Minutes ▾

Offline Session Idle ?

30

Days ▾

Offline Session Max Limited ?

OFF

Client Session Idle ?

0

Minutes ▾

Client Session Max ?

0

Minutes ▾

Access Token Lifespan ?

5

Minutes ▾

Access Token Lifespan For Implicit Flow ?

15

Minutes ▾

Client login timeout ?

1

Minutes ▾

Login timeout ?

30

Minutes ▾

Login action timeout ?

5

Minutes ▾

User-Initiated Action Lifespan ?

5

Minutes ▾

Default Admin-Initiated Action Lifespan ?

12

Hours ▾

Override User-Initiated Action Lifespan ?

Select one...

▾

Minutes ▾

Reset

Save

Cancel

Наименование в UI KeyCloak	Описание	Рекомендуемые значения	Уникальность	Автозаполняется
Revoke Refresh Token	<div>Относится к клиентам OIDC.</div> <div><div>Revoke Refresh Token ?</div><div><div>ON</div></div></div> <div><div>Refresh Token Max Reuse ?</div><div><div>1</div></div></div> <div>Запрос токенов обновления.</div> <div>При включенном значении можно задавать число допустимых вариантов использования токенов обновления.</div>	Y	N	N

SSO Session Idle	Если пользователь неактивен дольше заданного времени ожидания, сеанс пользователя будет признан недействительным. Как проверяется время простоя? Клиент, запрашивающий проверку подлинности, увеличит время простоя. Запросы токенов обновления также увеличат время простоя. Существует небольшое окно времени, которое всегда добавляется к таймауту простоя до того, как сеанс станет фактически недействителен.	30 min	N	N
SSO Session Max	Максимальное время до истечения срока действия и аннулирования сеанса пользователя. Настройка управляет максимальным временем, в течение которого сеанс пользователя может оставаться активным, независимо от активности.	10 hours	N	N
SSO Session Idle Remember Me	Аналогична конфигурации SSO Session Idle, но специфичная для входа в систему с включенным параметром "remember me". Это необязательная конфигурация, и если не установлено значение больше 0, он использует тот же SSO Session Idle, установленный в SSO Session Idle.	0	N	Y
SSO Session Max Remember Me	Аналогична конфигурации SSO Session Max, но специфичная для входа в систему с включенным параметром "remember me". Это необязательная конфигурация, и если не установлено значение больше 0, он использует тот же SSO Session Max, установленный в SSO Session Idle.	0	N	Y
Offline Session Idle	Для offline access это время, когда сеансу разрешено оставаться в режиме ожидания до отзыва offline token.	30 days	N	Y
Offline Session Max Limited	Для автономного доступа, если этот флаг включен, Offline Session Max включен для управления максимальным временем, в течение которого offline token может оставаться активным, независимо от активности.	off	N	Y
Offline Session Max	Для offline access это максимальное время действия offline token. Параметр задает максимальное время, в течение которого offline token может оставаться валидным независимо от активности пользователей.	-	-	-
Access Token Lifespan	При создании access token это значение влияет на его срок действия.	5 min	N	Y
Access Token Lifespan For Implicit Flow	С Implicit Flow токен обновления (refresh token) не предоставляется. По этой причине существует отдельный таймаут для access tokens, созданных с Implicit Flow.	15 min	N	Y
Client login timeout	Это максимальное время, в течение которого <b>клиент</b> должен завершить Authorization Code Flow в OIDC.	1 min	N	Y

Login timeout	Общее время, необходимое для входа в систему. Если аутентификация занимает больше времени, чем это время, то пользователь должен будет начать процесс аутентификации снова.	30 min	N	Y
Login action timeout	Максимальное время, которое пользователь может потратить на любую страницу в процессе аутентификации.	5 min	N	Y
User-Initiated Action Lifespan	Максимальное время на действие, запрошенного пользователем (например, забыл пароль от электронной почты). Это значение рекомендуется использовать коротким, так как ожидается, что пользователь быстро отреагирует на самостоятельно инициированное действие.	5 min	N	Y
Default Admin-Initiated Action Lifespan	Максимальное время до истечения срока действия разрешения, отправленного пользователю администратором. Это значение рекомендуется использовать для разрешения администраторам отправлять электронные письма пользователям, которые в данный момент находятся не в системе (offline).	12 hours	N	Y
Override User-Initiated Action Lifespan	Предоставляет возможность задания независимых тайм-аутов для каждой операции (например, e-mail verification, forgot password, user actions and Identity Provider E-mail Verification). Это поле не является обязательным, и если ничего не указано, оно по умолчанию имеет значение, настроенное для <i>User-Initiated Action Lifespan</i> .	<b>e-mail verification : 20 min</b>	N	N
Default Signature Algorithm	Алгоритм подписи токена.			