

بسم الله

## قفل کننده دسترسی IP خاص

### معرفی

هدف از این ماژول این است که در سه عمل ثبت نام (Register)، ورود (Login) و بازیابی گذرواژه (reset credential)، هر گاه کاربر در مدت M دقیقه N بار تلاش ناموفق داشته باشد، آن IP برای آن دسترسی خاص به مدت K مسدود خواهد شد.

### فعالسازی ماژول

۱. ابتدا فایل db.json را در مسیر اجرای کیکلاک قرار دهید. بطور مثال :

YourDrive:\keycloak\bin\db.json

در صورت وجود مشکل در ثبت لاگ، فایل db.json را در مسیر زیر قرار دهید:

WindowsDir:\Users\UserName\db.json

توجه کنید که لازم است پایگاه داده کیکلاک بر روی PostgreSQL تنظیم شده باشد و کاربر تعریف شده در فایل db.json به پایگاه داده دسترسی کامل داشته باشد. سپس مقادیر نام کاربر، پسورد و کانکشن دیتابیس را مطابق سیستم خود تنظیم کنید.

۲. سپس دستورات درون فایل createTable.sql را در پایگاه داده خود اجرا کنید تا جداول

ip\_blocklist و custom\_logger ایجاد شوند.

۳. بعد از انجام مراحل ذکر شده، فایل

request-locker-eventListener-1.0-SNAPSHOT-jar-with-dependencies.jar

را از پوشه requestLockerProviders\EventListener\request-locker\target کپی و در

مسیر زیر قرار دهید:

keycloak-x.x.x/standalone/deployments

۴. سپس فایل

request-locker-authenticator-1.0-SNAPSHOT-jar-with-dependencies.jar را از

پوشه requestLockerProviders\Authenticator\RequestLocker\target کپی و در

مسیر زیر قرار دهید:

keycloak-x.x.x/standalone/deployments

سپس در پنل ادمین Keycloak مراحل زیر را انجام دهید:

The screenshot shows the Keycloak Admin Console interface. On the left, a 'Manage' sidebar lists 'Groups', 'Users', 'Sessions', 'Events', 'Import', and 'Export'. A blue arrow points to 'Events'. The main area shows 'Events' with tabs for 'Login Events', 'Admin Events', and 'Config'. A blue arrow points down to 'Config'. Below this, the 'Login Events Settings' section shows 'Save Events' set to 'ON' (indicated by a blue arrow and the text 'باید روشن باشد'). Below this, a grid of event types is shown, including 'UPDATE\_CONSENT\_ERROR', 'SEND\_RESET\_PASSWORD', 'GRANT\_CONSENT', 'UPDATE\_TOTP', 'REMOVE\_TOTP', 'REVOKE\_GRANT', 'LOGIN\_ERROR', 'CLIENT\_LOGIN', 'RESET\_PASSWORD\_ERROR', 'IMPERSONATE\_ERROR', 'CODE\_TO\_TOKEN\_ERROR', and 'CUSTOM\_REQUIRED\_ACTION'. The 'Events Config' section shows tabs for 'Login Events', 'Admin Events', and 'Config'. A blue arrow points to the 'Config' tab. Below this, the 'Events Config' section shows 'Event Listeners' with a list containing 'jboss-logging' and 'Request Locker Event Listener'. A blue arrow points to 'Request Locker Event Listener', which has 'email' listed below it.

## Admin Events Settings

Save Events ?

ON

Include Representation ?

ON

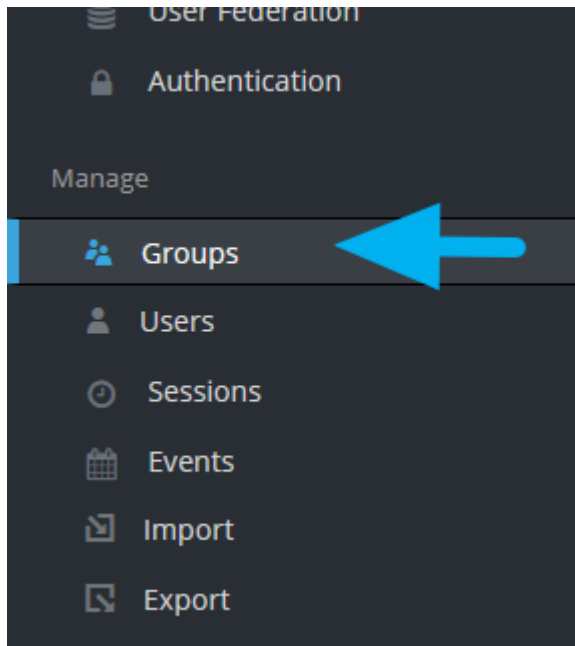
Clear admin events ?

Clear admin events

Clear changes

Save

ایجاد گروه پیشفرض:




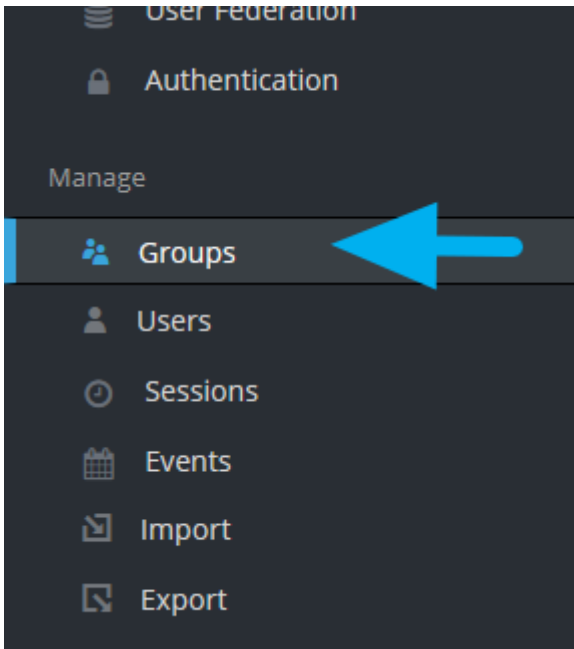
## User Groups




## Create group


Name \*







## User Groups





 Groups

 request-locker-group

## User Groups

 request-locker-group

## اضافه کردن attribute به گروه ایجاد شده:



attribute ها را طبق شکل زیر (همه حروف بزرگ هستند) وارد کنید و سپس بسته به نیاز خود آن را مقدار دهی کنید.

ERROR\_PERIOD\_DAYS طول بازه زمانی شمارش خطاهای کاربر بر حسب روز است.

ERROR\_PERIOD\_HOURS طول بازه زمانی شمارش خطاهای کاربر بر حسب ساعت است.

ERROR\_PERIOD\_MINS طول بازه زمانی شمارش خطاهای کاربر بر حسب دقیقه است.

ERROR\_PERIOD\_SECS طول بازه زمانی شمارش خطاهای کاربر بر حسب ثانیه است.

- اگر هر کدام از این چهار attribute را احتیاج نداشتید مقدار آن را صفر قرار دهید. به طور مثال اگر می خواهید خطاهای کاربر در یه بازه ۱ دقیقه ای محاسبه شود، مقدار ERROR\_PERIOD\_MINS را ۱ و سه attribute دیگر را صفر قرار دهید.

ERRORS\_LIMIT تعداد دفعات مجاز برای خطای کاربر است و پس از آن IP قفل خواهد شد.

## Request-locker-group

Settings

Attributes

Role Mappings

Members

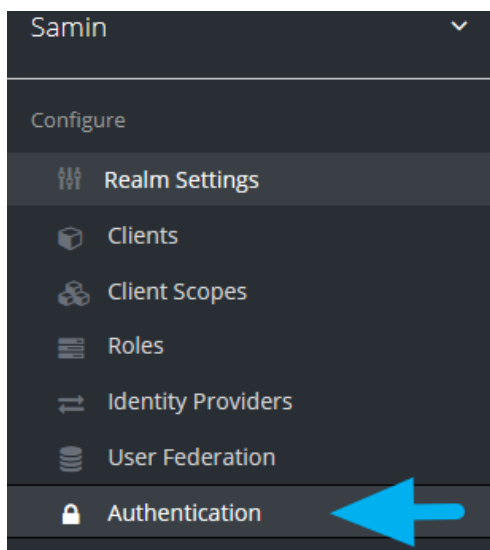
Key	Value
ERROR_PERIOD_DAYS	0
ERROR_PERIOD_HOURS	0
ERROR_PERIOD_MINS	1
ERROR_PERIOD_SECS	0
ERRORS_LIMIT	3

Save

Cancel

ایجاد روندها (Flows):

۱. روند Login



## Authentication

Flows							
Bindings Required Actions Password Policy OTP Policy WebAuthn Policy WebAuthn Passwordless Policy							
Browser							
New Copy							
Auth Type			Requirement				
Cookie			<input type="radio"/> REQUIRED	<input checked="" type="radio"/> ALTERNATIVE	<input type="radio"/> DISABLED		
Kerberos			<input type="radio"/> REQUIRED	<input type="radio"/> ALTERNATIVE	<input checked="" type="radio"/> DISABLED		
Identity Provider Redirector			<input type="radio"/> REQUIRED	<input checked="" type="radio"/> ALTERNATIVE	<input type="radio"/> DISABLED		Actions
Forms			<input type="radio"/> REQUIRED	<input checked="" type="radio"/> ALTERNATIVE	<input type="radio"/> DISABLED	<input type="radio"/> CONDITIONAL	
	Username Password Form		<input checked="" type="radio"/> REQUIRED				
	Browser - Conditional OTP		<input type="radio"/> REQUIRED	<input type="radio"/> ALTERNATIVE	<input type="radio"/> DISABLED	<input checked="" type="radio"/> CONDITIONAL	
		Condition - User Configured	<input checked="" type="radio"/> REQUIRED	<input type="radio"/> DISABLED			
		OTP Form	<input checked="" type="radio"/> REQUIRED	<input type="radio"/> ALTERNATIVE	<input type="radio"/> DISABLED		

### Copy Authentication Flow

New Name

Samin Browser

CancelOk

یک نام دلخواه وارد کنید (توصیه می شود نام هر flow با نام اصلی آن تمام شود مثلا Samin Browser)

## Authentication

Flows Bindings Required Actions Password Policy OTP Policy WebAuthn Policy WebAuthn Passwordless Policy

Samin Browser

New Copy Delete Edit Flow Add execution Add flow

Auth Type	Requirement				
Cookie	<input type="radio"/> REQUIRED <input checked="" type="radio"/> ALTERNATIVE <input type="radio"/> DISABLED				Actions
Kerberos	<input type="radio"/> REQUIRED <input type="radio"/> ALTERNATIVE <input checked="" type="radio"/> DISABLED				Actions
Identity Provider Redirector	<input type="radio"/> REQUIRED <input checked="" type="radio"/> ALTERNATIVE <input type="radio"/> DISABLED				Actions
Samin Browser Forms	<input type="radio"/> REQUIRED <input checked="" type="radio"/> ALTERNATIVE <input type="radio"/> DISABLED <input type="radio"/> CONDITIONAL				Actions
Username Password Form	<input checked="" type="radio"/> REQUIRED <input type="radio"/> ALTERNATIVE <input type="radio"/> DISABLED				Actions
Samin Browser Browser - Conditional OTP	<input type="radio"/> REQUIRED <input type="radio"/> ALTERNATIVE <input type="radio"/> DISABLED <input checked="" type="radio"/> CONDITIONAL				Actions
Condition - User Configured	<input checked="" type="radio"/> REQUIRED <input type="radio"/> ALTERNATIVE <input type="radio"/> DISABLED				Actions
OTP Form	<input checked="" type="radio"/> REQUIRED <input type="radio"/> ALTERNATIVE <input type="radio"/> DISABLED				Actions

گزینه Actions را انتخاب و Add Execution را انتخاب کنید.

## Create Authenticator Execution

Flows Bindings Required Actions Password Policy OTP Policy WebAuthn Policy WebAuthn Passwordless Policy

Provider

Browser Redirect/Refresh

- Condition - User Role
- Conditional OTP Form
- Confirm Link Existing Account
- Cookie
- Create User If Unique
- Docker Authenticator
- HTTP Basic Authentication
- Identity Provider Redirector
- Inactive User Disabler
- IP Range Authenticator
- Kerberos
- Login Locker**
- LoginLocker
- OTP
- OTP Form
- Password
- Password Form
- Register Locker
- Reset OTP

Login Locker را انتخاب و save کنید.

## Authentication

Flows Bindings Required Actions Password Policy OTP Policy WebAuthn Policy WebAuthn Passwordless Policy

Samin Browser

New Copy Delete Edit Flow Add execution Add flow

Auth Type	Requirement				
Cookie	<input type="radio"/> REQUIRED <input checked="" type="radio"/> ALTERNATIVE <input type="radio"/> DISABLED				Actions
Kerberos	<input type="radio"/> REQUIRED <input type="radio"/> ALTERNATIVE <input checked="" type="radio"/> DISABLED				Actions
Identity Provider Redirector	<input type="radio"/> REQUIRED <input checked="" type="radio"/> ALTERNATIVE <input type="radio"/> DISABLED				Actions
Samin Browser Forms	<input type="radio"/> REQUIRED <input checked="" type="radio"/> ALTERNATIVE <input type="radio"/> DISABLED <input type="radio"/> CONDITIONAL				Actions
Username Password Form	<input checked="" type="radio"/> REQUIRED <input type="radio"/> ALTERNATIVE <input type="radio"/> DISABLED				Actions
Login Locker	<input checked="" type="radio"/> REQUIRED <input type="radio"/> ALTERNATIVE <input type="radio"/> DISABLED				Actions

حال از Login Locker گزینه Action و سپس config را انتخاب کنید.

فیلدها را بسته به نیاز خود مقداردهی کنید و save کنید.

Alias: یک نام دلخواه

Lock duration in days: مدت زمان قفل بودن IP کاربر بر حسب روز

Lock duration in hours: مدت زمان قفل بودن IP کاربر بر حسب ساعت

Lock duration in minutes: مدت زمان قفل بودن IP کاربر بر حسب دقیقه

Lock duration in seconds: مدت زمان قفل بودن IP کاربر بر حسب ثانیه

با تکرار چند مرحله گذشته (از Add Execution) یک Execution دیگر دقیقا به همین شکل بسازید و با کلیدهای جهت کنار نام Execution آنرا به صورتی جابجا کنید که ترتیب نهایی flow به شکل زیر درآید:

Flows	Bindings	Required Actions	Password Policy	OTP Policy	WebAuthn Policy ?	WebAuthn Passwordless Policy ?
-------	----------	------------------	-----------------	------------	-------------------	--------------------------------

Samin Browser ?

NewCopy

Auth Type		Requirement		
<div>^v</div>	Cookie	<div><input type="radio"/> REQUIRED</div>	<div><input checked="" type="radio"/> ALTERNATIVE</div>	<div><input type="radio"/> DISABLED</div>
<div>^v</div>	Kerberos	<div><input type="radio"/> REQUIRED</div>	<div><input type="radio"/> ALTERNATIVE</div>	<div><input checked="" type="radio"/> DISABLED</div>
<div>^v</div>	Identity Provider Redirector	<div><input type="radio"/> REQUIRED</div>	<div><input checked="" type="radio"/> ALTERNATIVE</div>	<div><input type="radio"/> DISABLED</div>
<div>^v</div>	Samin Browser Forms ?	<div><input type="radio"/> REQUIRED</div>	<div><input checked="" type="radio"/> ALTERNATIVE</div>	<div><input type="radio"/> DISABLED</div>
	<div>^v</div> Login Locker (locker)	<div><input checked="" type="radio"/> REQUIRED</div>		
	<div>^v</div> Username Password Form	<div><input checked="" type="radio"/> REQUIRED</div>		
	<div>^v</div> Login Locker (locker)	<div><input checked="" type="radio"/> REQUIRED</div>		

در آخر از سربرگ Binding در قسمت Browser Flow روندی که ایجاد کردید (در اینجا Samin Browser) را انتخاب و save کنید.

## Authentication

Flows	Bindings	Required Actions	Password Policy	OTP P
-------	----------	------------------	-----------------	-------

Browser Flow ?

samin browser

Registration Flow ?

saminRegistration

Direct Grant Flow ?

direct grant

Reset Credentials ?

samin reset password

Client Authentication ?

clients

Save

Cancel



## ۲. روند Register

از روند Registration مشابه مرحله قبل یک کپی بگیرید و اینبار برای ایجاد Execution از منوی بالای flow گزینه Add Excution را انتخاب کنید و از لیست providers گزینه register locker را انتخاب و save کنید. بقیه مراحل دقیقا مشابه روند Login است. ترتیب نهایی flow باید به شکل زیر باشد:

### Authentication

The screenshot shows the 'Authentication' configuration page for the 'SaminRegistration' flow. The 'Auth Type' section is highlighted with a blue box. It contains a table with the following rows:

Auth Type	
Register Locker (locker)	
SaminRegistration Registration Form	
	Registration User Creation
	Profile Validation
	Password Validation
	Recaptcha
Register Locker (locker)	

## ۳. روند reset credential:

دقیقا مشابه روند قبلی است فقط از لیست providers باید reset password locker را انتخاب کنید. ترتیب نهایی flow باید به شکل زیر باشد:

The screenshot shows the 'Authentication' configuration page for the 'Samin Reset Password' flow. The 'Auth Type' section contains a table with the following rows:

Auth Type	
Reset Password Locker (locker)	
Choose User	
Send Reset Email	
Reset Password	
Samin Reset Password Reset - Conditional OTP	
	Condition - Us
	Reset OTP
Reset Password Locker (locker)	