

KEYCLOAK

NEDİR ?

En basit haliyle Keycloak, uygulamalarda kimlik doğrulama ve yetkilendirme işlemlerini kolaylaştıran açık kaynaklı bir kimlik yönetim sistemidir. Keycloak, kullanıcı girişlerini, sosyal girişleri (Google, Facebook gibi), tek oturum açma (SSO), iki faktörlü kimlik doğrulama, kullanıcı yönetimi ve yetkilendirme gibi süreçleri yönetir. Ayrıca, uygulamalara token tabanlı kimlik doğrulama eklemeyi sağlar. Kısaca özetlemek gerekirse uygulamaya giriş yapma, kimlik doğrulama ve yetkilendirme işlemleri Keycloak ile kolayca gerçekleştirilebilir.

REALM NEDİR ?

Realm bir kimlik ve erişim yönetimi bağlamıdır. Realm, kullanıcıların, kimlik doğrulama süreçlerinin, rollerin ve istemcilerin (client) yönetildiği izole bir güvenlik alanıdır. Her realm, kendi başına bağımsız olarak çalışabilir ve diğer realmlerden izole edilir. Bu, bir uygulamanın güvenlik gereksinimlerine göre esnek ve ayrıştırılmış kimlik yönetimi sunar.

TEMEL REALM ÖZELLİKLERİ

Kullanıcı Yönetimi: Her realm, kendi kullanıcılarını yönetir. Bir realm'deki kullanıcılar, başka bir realm'deki kullanıcılar ile karışmaz. Aynı kullanıcı adı farklı realmlerde kullanılabilir, çünkü her realm birbirinden bağımsızdır.

İstemci (Client) Yönetimi: Realm, birden fazla istemciyi (örneğin, bir web uygulaması, mobil uygulama, API) destekler. İstemciler, realm içinde tanımlanır ve her biri için ayrı ayrı kimlik doğrulama, yetkilendirme kuralları belirlenir.

Kimlik Doğrulama ve Yetkilendirme: Realm, kullanıcılara nasıl kimlik doğrulama yapılacağını belirler (şifre, iki faktörlü doğrulama, sosyal giriş vb.). Ayrıca, kullanıcıların hangi kaynaklara ve rollere erişebileceği de realm düzeyinde tanımlanır.

Roller ve Yetkiler: Realm'de roller tanımlanır ve kullanıcılara bu roller atanır. Bu roller, bir kullanıcının hangi yetkilere sahip olduğunu belirler. Rollerin istemcilerle ilişkisi de realm içinde yapılandırılabilir.

Gruplar: Kullanıcılar, gruplara atanabilir ve gruplara özel izinler tanımlanabilir. Bu da yetkilendirme sürecini daha esnek hale getirir.

İzole Yapı: Bir realm, diğer realmlere tamamen izole edilmiştir. Örneğin, bir şirket içinde bir realm bir departmana atanırken, başka bir realm başka bir departmana atanabilir.

Böylece her departman kendi kullanıcıları, istemcileri ve izinleri üzerinde tam kontrol sahibi olur.

Küresel Realm (Master Realm): Keycloak'un varsayılan realm'idir. Diğer tüm realm'leri yönetmek için kullanılır. Genellikle yönetici hesaplarının oluşturulduğu ve tüm sistemin yönetildiği alandır.

CLIENTS

1- Client List

Clients

Clients are applications and services that can request authentication of a user. [Learn more](#)

Clients list

Initial access token

Client registration

Q Search for client

→

Create client

Import client

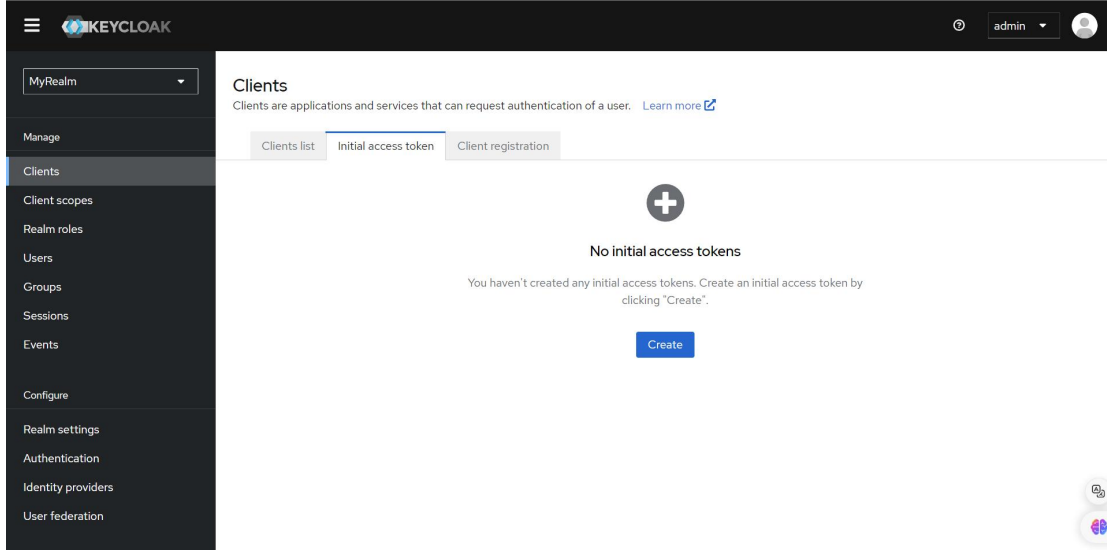
Refresh

1 - 9

Client ID	Name	Type	Description	Home URL
abc	test	OpenID Connect	test	—
account	\$_client_account}	OpenID Connect	—	http://localhost:8080
account-console	\$_client_account-console}	OpenID Connect	—	http://localhost:8080
admin-cli	\$_client_admin-cli}	OpenID Connect	—	—
broker	\$_client_broker}	OpenID Connect	—	—
myapp	test	OpenID Connect	test	http://localhost:7191
myapp2	—	OpenID Connect	—	—

İçinde bulunan Realm'lere ait clientlerin listelendiği alandır.

2- Initial Access Token



Keycloak'taki Clients sekmesinde bulunan **Initial Access Token** alanı, yönetici paneline manuel olarak girip kullanıcı arayüzü üzerinden istemci eklemek yerine, bu token'ı kullanarak programatik olarak API üzerinden istemci eklememizi sağlar.

[Clients](#) > [Create initial access token](#)

Create initial access token

An initial access token can only be used to create clients

Expiration ?

Days ▼

Count ?

–

1

+

Save

Cancel

Bu alanda istemci eklenebilecek token'a ait süre ve tek sorguda kaç istemci eklenebileceği ayarlanabilmektedir.

3- Client Registration

Clients

Clients are applications and services that can request authentication of a user. [Learn more](#)

Clients list

Initial access token

Client registration

Anonymous access policies

Authenticated access policies

Search for policy

→

Create client policy

Refresh

1 - 6

Name	Provider ID	
Trusted Hosts	trusted-hosts	⋮
Max Clients Limit	max-clients	⋮
Full Scope Disabled	scope	⋮
Allowed Client Scopes	allowed-client-templates	⋮
Consent Required	consent-required	⋮
Allowed Protocol Mapper Types	allowed-protocol-mappers	⋮

1 - 6

Initial Access Token belirli bir token ile sınırlı sayıda istemci kaydetmeye odaklanırken, Client Registration daha geniş kapsamlıdır ve API üzerinden dinamik olarak birçok istemcinin kaydolmasını sağlar. Initial Access Token, Client Registration API'sini güvence altına almak için kullanılabilir.

4- CREATE CLIENT

Clients > Create client

Create client

Clients are applications and services that can request authentication of a user.

1 General settings

2 Capability config

3 Login settings

Client authentication

Off

Authorization

Off

Authentication flow

☒ Standard flow

☒ Direct access grants

☐ Implicit flow

☐ Service accounts roles

☐ OAuth 2.0 Device Authorization Grant

☐ OIDC CIBA Grant

Back

Next

Cancel

1. Standard Flow (Authorization Code Flow):

OAuth 2.0 ve OpenID Connect (OIDC) standartlarının en yaygın kullanılan akışıdır. Kullanıcı, kimlik doğrulama işlemini tamamladığında bir yetkilendirme kodu alır ve bu kod sunucuya gönderilir. Sunucu bu kodu bir erişim token'ına dönüştürür. Genellikle web uygulamaları için kullanılır. Tarayıcı tabanlı kimlik doğrulama için tercih edilir.

2. Direct Access Grants (Resource Owner Password Credentials Flow):

Kullanıcının kimlik bilgilerini (kullanıcı adı ve şifre) doğrudan istemciye ilettiği bir akıştır. İstemci bu bilgileri Keycloak'a gönderir ve doğrudan bir erişim token'ı alır. Güvenilen istemciler (örneğin, dahili uygulamalar) veya sunucu tabanlı işlemler için kullanılır. Genelde kullanıcı deneyimini düşürmemek için tavsiye edilmez.

3. Implicit Flow:

İstemci , yetkilendirme kodu olmadan doğrudan erişim token'ını alır. Güvenli bir tarayıcı üzerinden çalışır, ancak token doğrudan istemciye döndüğü için güvenlik riskleri içerir. Genellikle tek sayfa uygulamaları (SPA) için kullanılır. Ancak özellikle modern uygulamalarda güvenlik nedeniyle önerilmez.

4. Service Accounts Roles:

İstemci için bir hizmet hesabı oluşturur ve bu hesap üzerinden kimlik doğrulama yapılır. Hizmet hesapları, bir kullanıcı adına değil, istemci adına kimlik doğrulama sağlar. Genellikle Makine-makine (M2M) etkileşimlerinde kullanılır, yani bir hizmet başka bir hizmete erişmek istediğinde kullanılır.

5. OAuth 2.0 Device Authorization Grant:

Kullanıcının bir cihaz üzerinden kimlik doğrulama yapmasına olanak tanır (örneğin, bir TV veya IoT cihazı). Kullanıcı cihaz üzerinde bir kod girer ve başka bir cihaz (örneğin, bilgisayar veya telefon) üzerinden kimlik doğrulama işlemi yapılır. Ekranı olmayan veya sınırlı giriş imkanı olan cihazlar için kullanılır.

6. OIDC CIBA Grant (Client Initiated Backchannel Authentication):

OpenID Connect'te, istemcinin arka planda başlattığı kimlik doğrulama akışıdır. Kullanıcıya bir bildirim gönderilir (örneğin SMS veya mobil uygulama üzerinden) ve kullanıcı kimliği doğrular. Kullanıcı etkileşiminden bağımsız olarak arka planda kimlik doğrulamanın yapılması gereken durumlarda sıklıkla tercih edilir. Özellikle finansal ve yüksek güvenlik gerektiren işlemlerde kullanılır.

Genel Kullanım Tavsiyeleri:

Web uygulamaları için genellikle **Standard Flow** tercih edilir.

Mobil uygulamalar veya SPA'lar için **Implicit Flow** ya da **Authorization Code Flow with PKCE** önerilir.

Makine-makine iletişimi veya arka plan işlemleri için **Service Accounts** kullanılır.

Özel cihazlar için **OAuth 2.0 Device Authorization Grant** ve yüksek güvenlikli işlemler için **OIDC CIBA Grant** tercih edilir.

Client Scopes

Client Scopes, istemcilerin erişim token'larına ve kimlik token'larına hangi bilgilerin ekleneceğini ve istemcinin hangi yetkilere sahip olacağını tanımlayan kapsamlar veya izinlerdir. Bu özellik, her istemciye özel bilgi ve yetkilendirme yapılandırması yapılmasına olanak tanır ve güvenlik ile veri gizliliği üzerinde daha ince ayar yapmayı sağlar.

Client scopes

Client scopes are a common set of protocol mappers and roles that are shared between multiple clients. [Learn more](#)

<input type="text" value="Name"/>	<input type="text" value="Search for client scope"/>	Create client scope	Change type to	Refresh	1 - 10
<input type="checkbox"/> Name	Assigned type	Protocol	Display order	Description	
<input type="checkbox"/> acr	Default	OpenID Connect	–	OpenID Connect scope for add acr (authentication context class reference) to the token	
<input type="checkbox"/> address	Optional	OpenID Connect	–	OpenID Connect built-in scope: address	
<input type="checkbox"/> basic	Default	OpenID Connect	–	OpenID Connect scope for add all basic claims to the token	
<input type="checkbox"/> email	Default	OpenID Connect	–	OpenID Connect built-in scope: email	
<input type="checkbox"/> microprofile-jwt	Optional	OpenID Connect	–	Microprofile - JWT built-in scope	
<input type="checkbox"/> offline_access	Optional	OpenID Connect	–	OpenID Connect built-in scope: offline_access	
<input type="checkbox"/> phone	Optional	OpenID Connect	–	OpenID Connect built-in scope: phone	
<input type="checkbox"/> profile	Default	OpenID Connect	–	OpenID Connect built-in scope: profile	

1- Create Client Scope

Create client scope

Name *	<input type="text"/>
Description	<input type="text"/>
Type	None
Protocol	OpenID Connect
Display on consent screen	<input checked="" type="checkbox"/> On
Consent screen text	<input type="text"/>
Include in token scope	<input type="checkbox"/> Off
Display Order	<input type="text"/>

Name ve Description: Kapsamın adı ve açıklaması.

Type: Kapsam türü.

Protocol: Kullanılacak protokol.

SAML: XML tabanlı, genellikle kurumsal ortamlarda kullanılan bir protokoldür.

OpenID Connect (OIDC): OAuth 2.0 üzerine kurulu, modern uygulamalar için kullanılan JSON tabanlı bir protokoldür.

Display on consent screen: İzin ekranında gösterilip gösterilmeyeceği.

Consent screen text: İzin ekranında görünecek metin.

Include in token scope: Token'larda bu kapsamın yer alıp almayacağı.

Display Order: İzin ekranındaki sıralama.

REALM ROLES

Realm roles

Realm roles are the roles that you define for use in the current realm. [Learn more](#)

Q Search role by name	→	Create role	Refresh	1 - 3	<	>
Role name	Composite	Description				
default-roles-myrealm	True	`\${role_default-roles}`				
offline_access	False	`\${role_offline-access}`				
uma_authorization	False	`\${role_uma_authorization}`				

Mevcut realm'de kullanılması için tanımlanan rollerin listelendiği alandır.

Create Role

[Realm roles](#) > Create role

Create role

Role name *

Description

Save

Cancel

Yeni bir rol oluşturma ekranıdır.

USERS

Users

Users are the users in the current realm. [Learn more](#)

User list									
Default search	Q Search user	→	Add user	Delete user	Refresh	1 - 7	<	>	
<input type="checkbox"/> Username	Email	Last name	First name						
<input type="checkbox"/> caybardagi	test@gmail.com	çay	bardak						
<input type="checkbox"/> fener	fener@gmail.com	fener	fener						
<input type="checkbox"/> lorem	lorem@gmail.com	lorem	lorem						
<input type="checkbox"/> movercrack	move@gmail.com	tea	move						
<input type="checkbox"/> onur	onur@gmail.com	bural	onur						
<input type="checkbox"/> test	-	-	-						
<input type="checkbox"/> testtttt	tesst@gmail.com	tea	tesst						

Mevcut realm'de bulunan kullanıcıların listelendiği alandır.

Create User

[Users](#) > [Create user](#)

Create user

Required user actions ⓘ

Select action ▼

Email verified ⓘ

☐ Off

General

Username *

Email

First name

Last name

Groups ⓘ

[Join Groups](#)

Jump to section

[General](#)

Create

Cancel

Yeni user oluşturma alanıdır. Bu alanda User Actions kısmından kullanıcı giriş yaptıktan sonra e-mail doğrulaması, şifre değiştirme isteği vs. gibi alanlar yönetilebilir.

USER DETAILS

a. Details

İlgili kullanıcıya ait bilgilerin listelendiği alandır.

onur

Details

Credentials

Role mapping

Groups

Consents

Identity provider links

Sessions

ID *

7944a00c-7da2-4375-8ae3-6860d8e05312

Created at *

8/15/2024, 8:48:15 PM

Required user actions

Select action

Email verified

☒ On

General

Jump to section

General

Username *

onur

Email

onur@gmail.com

First name

onur

Last name

bural

Save

Revert

b.Credentials

Credentials sekmesi, Keycloak'ta kullanıcıların kimlik doğrulama bilgilerini (şifre, kullanıcı adı, vs.) yönetmek için kullanılır. Bu sekme, bir kullanıcının kimlik doğrulama bilgilerini güncelleme veya ayarlama imkanı sağlar.

Users > User details

onur

Enabled

Action

Details

Credentials

Role mapping

Groups

Consents

Identity provider links

Sessions

Credential Reset

Type	User label	Created at	Data
Password	My password	8/16/2024, 10:59:24 AM	Show data

Reset password

c.Role Mapping

Kullanıcıların Keycloak'taki rollerle ilişkilendirilmesini sağlar. Roller, kullanıcıların uygulamalara veya sistemlere erişim yetkilerini belirlemek için kullanılır. Role Mapping sayesinde, kullanıcıların hangi rollerle ilişkilendirileceğini tanımlayarak, bu rollerin getirdiği izinleri ve yetkileri kullanıcılara atayabilirsiniz.

d.Groups


Groups (Gruplar), kullanıcıları bir araya getiren ve bu kullanıcılar üzerinde topluca işlemler yapmayı kolaylaştıran bir yapıdır. Gruplar, kullanıcıların yönetimini basitleştirir ve erişim kontrolünü daha düzenli hale getirir.

Users > User details

onur

Enabled Action

Details Credentials Role mapping Groups Consents Identity provider links Sessions



No groups

You haven't added this user to any groups. Join a group to get started.

Join Group


e.Consents

Consents (Kabul), Keycloak'ta kullanıcıların uygulamalar veya hizmetler için erişim izinlerini yönetmelerini sağlar. Bu, kullanıcıların hangi verilere erişim izni verdiğini onaylamalarını ve bu izinleri kontrol etmelerini sağlar. Ayrıca, gizlilik ve güvenlik açısından önemli bir rol oynar.

Users > User details

onur

Details Credentials Role mapping Groups Consents Identity provider links Sessions



No consents

The consents will only be recorded when users try to access a client that is configured to require consent. In that case, users will get a consent page which asks them to grant access to the client.

f.Identity Provider Links

Keycloak'un farklı kimlik sağlayıcılarıyla entegre olmasını sağlar ve kullanıcıların bu sağlayıcılar aracılığıyla giriş yapmasını veya kimlik doğrulamasını sağlar. Bu bağlantılar, sosyal medya girişleri, kurumsal kimlik sağlayıcıları ve tek oturum açma (SSO) gibi senaryoları destekler.(OAuth 2.0 gibi)

[Users](#) > [User details](#)

onur

Enabled

Action ▾

Details

Credentials

Role mapping

Groups

Consents

Identity provider links

Sessions

Linked identity providers

The identity providers which are already linked to this user account

No identity providers linked.

Available identity providers

All the configured identity providers in this realm are listed here. You can link the user account to any of the IdP accounts.

No available identity providers.

g.Sessions

Keycloak'ta kullanıcıların aktif oturumlarını görüntüleme, yönetme ve sonlandırma işlemlerinin yapılmasına olanak tanır. Bu özellik, güvenlik yönetimi, oturum süresi izleme ve kullanıcı desteği için kullanılır.

[Users](#) > [User details](#)

onur

Enabled

Action ▾

Details

Credentials

Role mapping

Groups

Consents

Identity provider links

Sessions

No sessions

There are currently no active sessions for this user.

GROUPS

Kullanıcıları organize etmek ve topluca yönetmek için kullanılır. Gruplar, kullanıcıların benzer niteliklere göre sınıflandırılmasını sağlar ve topluca izinler veya roller atamanızı kolaylaştırır. Bu, yönetimi basitleştirir ve erişim kontrolünü daha düzenli hale getirir.

Search group

→

☐ Exact search

1-1 ▾ < >

> test-group

⋮

1-1 ▾ < >

Groups

A group is a set of attributes and role mappings that can be applied to a user. You can create, edit, and delete groups and manage their child-parent organization. [Learn more](#)

Filter groups

→

Create group

⋮

Refresh

1-1 ▾ < >

☐ Group name

☐ test-group

⋮

1-1 ▾ < >

SESSIONS

Belirli bir Realm içindeki tüm aktif kullanıcı oturumlarını izlemeye ve yönetmeye olanak tanır. Bu özellik, oturumları görüntülemeyi, sonlandırmayı ve oturum bilgilerini takip etmeyi sağlar, böylece güvenlik ve yönetim işlemleri daha etkin bir şekilde gerçekleştirilir.

Sessions

Sessions are sessions of users in this realm and the clients that they access within the session. [Learn more](#)



No sessions

There are currently no active sessions in this realm.

EVENTS

Events, Keycloak'ta kullanıcı & admin hareketleri ve sistem etkinliklerinin takip edilmesini sağlar. Bu özellik, güvenlik denetimleri, sorun giderme ve sistem performansının analiz edilmesi için kullanılır. Olay kayıtları incelenerek, sistemde gerçekleşen çeşitli olaylar izlenebilir ve analiz edilebilir.

Events

Events are records of user and admin events in this realm. To configure the tracking of these events, go to [Event configs](#). [Learn more](#)

User events

Admin events



No user events

There are no user events in this realm.

CONFIGURE KISMI

Realm Settings

GENERAL

Bu ayarlar, Keycloak'taki bir realm'in genel yapılandırmasını ve güvenlik ayarlarını düzenlemek için kullanılır.

MyRealm

Realm settings are settings that control the options for users, applications, roles, and groups in the current realm. [Learn more](#)

Enabled

General

Login

Email

Themes

Keys

Events

Localization

Security defenses

Sessions

Tokens

Client policies

User profile

User registration

Realm ID *

MyRealm

Display name

HTML Display name

Frontend URL ⓘ

Require SSL ⓘ

External requests

ACR to LoA Mapping ⓘ

No ACR to LoA Mapping have been defined yet. Click the below button to add ACR to LoA Mapping. key and value are required for a key pair.

Add ACR to LoA Mapping

User-managed access ⓘ

Off

Unmanaged Attributes ⓘ

Disabled

Endpoints ⓘ

[OpenID Endpoint Configuration](#)

[SAML 2.0 Identity Provider Metadata](#)

Save

Revert

Realm ID: Realm'lere ait özel tanımlayıcı id alanıdır.

Display name: Bu alan, realm için bir gösterim adıdır. Keycloak yönetici konsolu veya kullanıcı oturum açma ekranı gibi yerlerde görüntülenir.

HTML Display name: Realm için HTML formatında bir gösterim adıdır

Frontend URL: Kullanıcıların bu realm ile etkileşime geçmek için kullandığı frontend uygulamasının URL'sini belirtir. Bu, istemcilerin kullanacağı temel URL'dir.

Require SSL: Bu seçenek, SSL'in zorunlu olup olmadığını belirler. Aşağıdaki seçeneklerden biri seçilebilir:

External requests: Yalnızca dış talepler için SSL gereklidir.

All requests: Tüm talepler için SSL gereklidir.

ACR to LoA Mapping:

ACR (Authentication Context Class Reference): Kimlik doğrulama sürecinin gerektirdiği güvenlik düzeyini belirten bir referans.

LoA (Level of Assurance): Kimlik doğrulamanın güvenilirlik veya doğruluk seviyesini ifade eder.

ACR to LoA Mapping: ACR değerlerinin belirli LoA seviyelerine nasıl karşılık geldiğini gösteren eşleme tablosu.

User-managed access: Kullanıcılara kendi kaynaklarına erişim izni verme olanağı tanır. Kullanıcılar, kendi kaynaklarını yönetebilir ve diğer kullanıcılara erişim izni verebilir.

Unmanaged Attributes

Bir kimlik yönetim sisteminde (örneğin, bir kullanıcı veya uygulama için) otomatik olarak yönetilmeyen, yani sistem tarafından doğrudan kontrol edilmeyen veya güncellenmeyen özellikler veya veri alanlarıdır. Bu özellikler genellikle kullanıcılar veya uygulama yöneticileri tarafından manuel olarak tanımlanır veya değiştirilir.

Endpoints

Belirli protokollere erişim için kullanılan uç noktaların yapılandırmalarını içerir

OpenID Endpoint Configuration: OpenID Connect protokolüyle ilgili uç noktaların yapılandırma detaylarını içerir.

SAML 2.0 Identity Provider Metadata: SAML 2.0 kimlik sağlayıcılarıyla entegrasyon için gerekli olan metadata bilgilerini sağlar.

LOGIN

MyRealm
Realm settings are settings that control the options for users, applications, roles, and groups in the current realm. [Learn more](#)

General

Login

Email

Themes

Keys

Events

Localization

Security defenses

Sessions

Tokens

Client policies

User profile

User registration

Login screen customization
User registration ☒ On
Forgot password ☒ On
Remember me ☒ On

Email settings
Email as username ☐ Off
Login with email ☒ On
Duplicate emails ☐ Off
Verify email ☐ Off

User info settings
Edit username ☐ Off

İlgili alanlar ile alakalı özelleştirmelerin yapıldığı alandır.

EMAIL

Keycloak'tan gönderilecek e-postaların kimden gönderileceği ve nasıl görüneceği gibi temel ayarlar yapılandırılır.

From *: Bu, e-posta göndericisinin e-posta adresidir. Bu alana gönderen kişinin e-posta adresi girilir.

Sender email address: E-postanın gönderildiği adres. Bu, yukarıdaki "From" alanıyla aynı olabilir veya farklı bir adres olabilir.

From display name: E-postanın kimden geldiğini gösterecek alan.

Display name for Sender email address: Gönderen e-posta adresinin görünür adını tanımlar. Yukarıdaki "From display name" ile aynıdır, ancak bu daha detaylı olabilir.

Reply to: Bu alan, kullanıcının yanıtlamak istediğinde e-postanın gönderileceği adresi tanımlar.

Reply to email address: Yanıtların yönlendirileceği e-posta adresidir. "Reply to" alanıyla aynı işlevi görür.

Reply to display name: "Reply to" adresi için görüntülenen ad. Yanıtların hangi kişiye veya kuruluşa gittiğini gösterir.

Envelope from: Bu, e-posta sunucularının kullandığı teknik bir gönderici adresidir.

Sender envelope email address: Bu, yukarıdaki Envelope From için kullanılan e-posta adresidir. Genellikle teknik e-postalar için kullanılır ve normal kullanıcılar tarafından görülmez.

Connection & Authentication (Bağlantı ve Kimlik Doğrulama)

Bu bölüm, e-posta göndermek için kullanılan SMTP sunucusunun yapılandırılmasını içerir.

Host *: SMTP sunucusunun adresidir.

Port: SMTP sunucusunun port numarasıdır. Varsayılan olarak 25'dir, ancak şifreleme ve güvenli bağlantı gerektiren sunucular farklı portlar kullanabilir.

Encryption: E-posta sunucusuyla iletişimi güvenli hale getirmek için şifreleme kullanılıp kullanılmayacağını belirler.

Enable SSL: E-posta trafiğini SSL ile şifrelemek için bu seçeneği etkinleştirirsiniz.

Enable StartTLS: TLS (Transport Layer Security) kullanarak güvenli bir bağlantı başlatmak için bu seçeneği etkinleştirirsiniz.

Authentication: SMTP sunucusuna bağlanmak için kimlik doğrulama gerekip gerekmediğini belirler. Genellikle sunucuya erişim sağlamak için kullanıcı adı ve parola gerekir.

THEMES

Themes alanı, kullanıcı arayüzü (UI) için görsel tasarım ve kullanıcı deneyimi yapılandırmasını sağlar. Bu alan, oturum açma ekranları, e-posta şablonları, hesap yönetim sayfaları ve yönetici konsolu gibi farklı kullanıcı etkileşim noktalarının görünümünün özelleştirilmesine olanak tanır.

KEYS

MyRealm

Realm settings are settings that control the options for users, applications, roles, and groups in the current realm. [Learn more](#)

Enabled

Action

General

Login

Email

Themes

Keys

Events

Localization

Security defenses

Sessions

Tokens

Client policies

User profile

User registration

Keys list

Add providers

Active keys

Search key

Refresh

1-4

Algorithm	Type	Kid	Use	Provider	Valid to	Public keys
RS256	RSA	_3HkYsFNsUaXSkoLWs_HoOhHxMq5bemv2ls784dalo	SIG	rsa-generated	8/15/2034, 5:06:14 PM	Public key Certificate
RSA-OAEP	RSA	WZm0l-Crt9ueYBWLsfQ_0Yjw-IBSY2LkLDTYbpYL4ns	ENC	rsa-enc-generated	8/15/2034, 5:06:14 PM	Public key Certificate
HS512	OCT	641405d3-2069-41dd-9dcf-8aeca9034a3	SIG	hmac-generated-hs512	-	
AES	OCT	10931a17-b183-4262-9b0b-248639f27aa5	ENC	aes-generated	-	

1-4

Kimlik doğrulama ve yetkilendirme işlemleri sırasında kullanılan kriptografik anahtarların yönetildiği yerdir. Bu anahtarlar, token imzalama, şifreleme ve diğer güvenlik işlevleri için kullanılır. Realm'in güvenlik anahtarlarını ve sertifikalarının yönetilmesine olanak tanır. Bu anahtarlar, özellikle JSON Web Token (JWT) gibi dijital imzalama ve şifreleme gerektiren işlemlerde kritik bir rol oynar.

EVENTS

MyRealm

Realm settings are settings that control the options for users, applications, roles, and groups in the current realm. [Learn more](#)

General

Login

Email

Themes

Keys

Events

Localization

Security defenses

Sessions

Tokens

Client policies

User profile

User registration

Event listeners

User events settings

Admin events settings

Event listeners

jboss-logging

email

Save

Revert

Sistemde gerçekleşen önemli olayların ve kullanıcı etkileşimlerinin kaydedilmesini ve izlenmesini sağlar. Bu özellik, sistemde meydana gelen kimlik doğrulama, yetkilendirme, yönetim işlemleri ve diğer önemli olaylar hakkında bilgi edinilmesi gerektiğinde bu olayların analiz edilmesini mümkün kılar.

Admin Events (Yönetim Olayları):

Yönetici tarafından yapılan tüm değişikliklerin ve işlemlerin kaydedildiği olaylardır. Örneğin, yeni bir kullanıcı eklemek, roller atamak veya yapılandırma ayarlarını değiştirmek gibi işlemler bu kategoride izlenir. Bu olaylar, yönetici değişikliklerinin izlenmesi ve gerektiğinde denetlenmesi için kullanılır. Özellikle sistem yöneticileri tarafından, güvenlik veya yapılandırma sorunlarının tespit edilmesi için incelenebilmektedir.

User Events (Kullanıcı Olayları):

Kullanıcıların sisteme giriş yapması, çıkış yapması, oturum açma hataları, parola sıfırlama gibi tüm kullanıcı etkileşimlerinin kaydedildiği olaylardır. Kullanıcı davranışlarını izlemek, güvenlik sorunlarını tespit etmek (örneğin başarısız oturum açma denemeleri) ve genel kullanıcı deneyimi hakkında bilgi edinmek için kullanılır.

Event Kategorileri:

Login: Kullanıcı girişleri ve başarısız giriş denemeleri gibi olaylar kaydedilir.

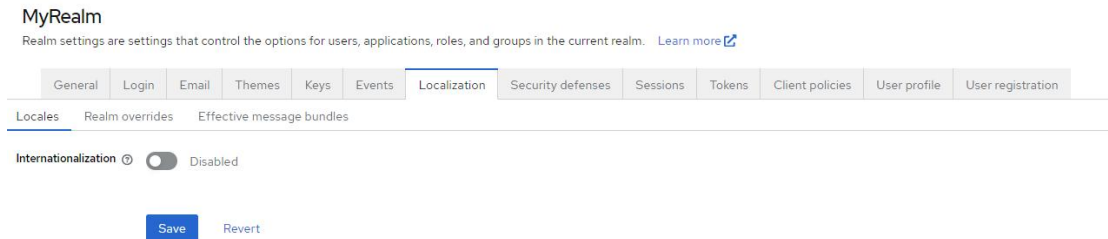
Logout: Kullanıcı çıkışları izlenir.

Register: Yeni bir kullanıcı kaydı gerçekleştiğinde bu olay kaydedilir.

Password Reset: Kullanıcılar parolalarını sıfırladığında bu olay izlenir.

Profile Update: Kullanıcıların profil bilgilerini güncellemesi durumunda bu olaylar kaydedilir.

LOCALIZATION



Kullanıcı etkileşimleri sırasında kullanılan metinlerin, hata mesajlarının, talimatların ve diğer dil bazlı içeriklerin farklı dillerde sunulmasına olanak tanır.

SECURITY DEFENSES

Sistemin güvenlik tehditlerine karşı korunmasını sağlayan çeşitli yapılandırmalar ve önlemler içerir. Bu bölüm, saldırılara karşı ek savunma mekanizmaları sunarak Keycloak'ın güvenliğini artırmaya yardımcı olur. Bu özellikler, sistemin saldırılara karşı daha dayanıklı hale getirilmesine yönelik çeşitli güvenlik önlemleri içerir.

MyRealm

Realm settings are settings that control the options for users, applications, roles, and groups in the current realm. [Learn more](#)

General

Login

Email

Themes

Keys

Events

Localization

Security defenses

Sessions

Tokens

Client policies

User profile

User registration

Headers

Brute force detection

X-Frame-Options ⓘ

SAMEORIGIN

Content-Security-Policy ⓘ

frame-src 'self'; frame-ancestors 'self'; object-src 'none';

Content-Security-Policy-Report-Only ⓘ

X-Content-Type-Options ⓘ

nosniff

X-Robots-Tag ⓘ

none

X-XSS-Protection ⓘ

1; mode=block

HTTP Strict Transport Security (HSTS) ⓘ

max-age=31536000; includeSubDomains

Referrer Policy ⓘ

no-referrer

Save

Revert

X-Frame-Options (SAMEORIGIN): Sitenizin yalnızca kendi içinde iframe olarak gösterilmesine izin verir.

Content-Security-Policy (CSP): Tarayıcının hangi kaynaklardan içerik yükleyebileceğini kısıtlayarak güvenliğini artırır.

Content-Security-Policy-Report-Only: CSP ihlallerini raporlar ancak engellemez.

X-Content-Type-Options (nosniff): Tarayıcının içerik türünü tahmin etmesini engeller.

X-Robots-Tag (none): Sayfanın arama motorları tarafından indekslenmesini ve takip edilmesini engeller.

X-XSS-Protection (1; mode=block): XSS saldırılarını algıladığında sayfanın yüklenmesini engeller.

HTTP Strict Transport Security (HSTS): Tarayıcıya yalnızca HTTPS bağlantılarını kullanma zorunluluğu getirir.

Referrer Policy: Yönlendirme bilgilerini (referrer) nasıl ileteceğinizi kontrol eder.

SESSIONS

Kullanıcı oturumlarını izler, yönetir ve gerekirse sonlandırır, ayrıca oturum süreleri ve yenileme politikaları gibi oturum yönetim ayarlarını içerir.

MyRealm
Realm settings are settings that control the options for users, applications, roles, and groups in the current realm. [Learn more](#)

General

Login

Email

Themes

Keys

Events

Localization

Security defenses

Sessions

Tokens

Client policies

User profile

User registration

SSO Session Settings

SSO Session Idle ⓘ

30

Minutes ▼

SSO Session Max ⓘ

10

Hours ▼

SSO Session Idle Remember Me ⓘ

Minutes ▼

SSO Session Max Remember Me ⓘ

Minutes ▼

Client session settings

Client Session Idle ⓘ

Minutes ▼

Client Session Max ⓘ

Minutes ▼

(**Idle (etkinlik göstermeme) terimi, bir kullanıcının veya sistemin belirli bir süre boyunca herhangi bir işlem veya etkileşimde bulunmadığı süreyi ifade eder.)

SSO Session Idle: SSO oturumunun idle (etkinlik göstermeme) süresi.

SSO Session Max: SSO oturumunun maksimum süresi.

SSO Session Idle Remember Me: "Beni Hatırla" seçeneği ile oturum açan kullanıcılar için idle süresi.

SSO Session Max Remember Me: "Beni Hatırla" seçeneği ile oturum açan kullanıcılar için maksimum süre.

Client Session Idle: İstemci oturumlarının idle süresi.

Client Session Max: İstemci oturumlarının maksimum süresi.

TOKENS

Kullanıcıların kimlik doğrulama ve yetkilendirme işlemlerinde kullanılan çeşitli token türlerinin yönetimi ve yapılandırılmasını içerir. Bu alan, tokenların nasıl oluşturulacağı, geçerlilik süreleri ve özelliklerinin nasıl yapılandırılacağı hakkında ayarları içerir.

a.General

MyRealm
Realm settings are settings that control the options for users, applications, roles, and groups in the current realm. [Learn more](#)

General Login Email Themes Keys Events Localization Security defenses Sessions **Tokens** Client policies User profile User registration

General

Default Signature Algorithm

OAuth 2.0 Device Code Lifespan Minutes

OAuth 2.0 Device Polling Interval

Short verification_uri in Device Authorization flow

Lifetime of the Request URI for Pushed Authorization Request Minutes

Default Signature Algorithm: Varsayılan token imzalama algoritması (RS256).

OAuth 2.0 Device Code Lifespan: Cihaz kodunun geçerlilik süresi (10 dakika).

OAuth 2.0 Device Polling Interval: Cihaz kodunun durumunun kontrol edilme aralığı (5 dakika).

Short verification_uri: Cihaz yetkilendirme akışında kullanılan kısa süreli doğrulama URI'si.

Lifetime of the Request URI: İstek URI'sinin geçerlilik süresi.

b.Refresh Tokens

Refresh tokens

Revoke Refresh Token ☐ Disabled [?](#)

Yenileme tokenlarının geçersiz kılınmasını devre dışı bırakır. Yani, yenileme tokenları otomatik olarak geçersiz kılınmaz.

c. Access tokens

Access tokens

Access Token Lifespan ?	<input type="text" value="5"/>	Minutes ▼
It is recommended for this value to be shorter than the SSO session idle timeout: 30 minutes		
Access Token Lifespan For Implicit Flow ?	<input type="text" value="15"/>	Minutes ▼
Client Login Timeout ?	<input type="text" value="1"/>	Minutes ▼

Access Token Lifespan: Erişim tokenlarının geçerlilik süresi (5 dakika).

Access Token Lifespan For Implicit Flow: İmplicit akışındaki erişim tokenlarının geçerlilik süresi (15 dakika).

Client Login Timeout: İstemci oturum açma işleminin zaman aşımı süresi (1 dakika).

d. Action tokens

Action tokens

User-Initiated Action Lifespan ?	<input type="text" value="5"/>	Minutes ▼
Default Admin-Initiated Action Lifespan ?	<input type="text" value="12"/>	Hours ▼

User-Initiated Action Lifespan: Kullanıcı tarafından başlatılan eylem tokenlarının geçerlilik süresi (5 dakika).

Default Admin-Initiated Action Lifespan: Yönetici tarafından başlatılan eylem tokenlarının geçerlilik süresi (12 saat).

e.Override Action Tokens

Override Action Tokens

Email Verification ?	<input type="text"/>	Minutes ▼
IdP account email verification ?	<input type="text"/>	Minutes ▼
Forgot password ?	<input type="text"/>	Minutes ▼
Execute actions ?	<input type="text"/>	Minutes ▼

Save

Revert

Email Verification: E-posta doğrulama işlemi için kullanılan eylem tokenının geçerlilik süresi.

IdP account email verification: Kimlik Sağlayıcı (IdP) hesap e-posta doğrulaması için kullanılan eylem tokenının geçerlilik süresi.

Forgot password: Şifre unuttum işlemi için kullanılan eylem tokenının geçerlilik süresi.

Execute actions: Diğer eylem işlemleri için kullanılan eylem tokenının geçerlilik süresi.

CLIENT POLICIES

MyRealm

Realm settings are settings that control the options for users, applications, roles, and groups in the current realm. [Learn more](#)

General

Login

Email

Themes

Keys

Events

Localization

Security defenses

Sessions

Tokens

Client policies

User profile

User registration

Profiles Policies

Configure via: ☒ Form view ☐ JSON editor

Q Search

Create client profile

Refresh

1-8

Name	Description
fgapi-baseline Global	Client profile, which enforce clients to conform 'Financial-grade API Security Profile 1.0 - Part 1: Baseline' specification.
fgapi-advanced Global	Client profile, which enforce clients to conform 'Financial-grade API Security Profile 1.0 - Part 2: Advanced' specification.
fgapi-ciba Global	Client profile, which enforce clients to conform 'Financial-grade API: Client Initiated Backchannel Authentication Profile' specification (Implementer's Draft ver1). To satisfy FAPI-CIBA, both this profile and fgapi-advanced global profile need to be used.
fgapi-2-security-profile Global	Client profile, which enforce clients to conform 'FAPI 2.0 Security Profile' specification.
fgapi-2-message-signing Global	Client profile, which enforce clients to conform 'FAPI 2.0 Message Signing' specification.
oauth-2-1-for-confidential-client Global	Client profile, which enforce confidential clients to conform 'OAuth 2.1' specification.
oauth-2-1-for-public-client Global	Client profile, which enforce public clients to conform 'OAuth 2.1' specification.
saml-security-profile Global	Client profile that enforces SAML clients to be secure.

İstemciler (uygulamalar veya servisler) için güvenlik kuralları ve yapılandırmaları belirler. Bu politikalar, istemcilerin kimlik doğrulama, erişim izinleri ve güvenlik ayarlarını nasıl uygulayacağını kontrol eder.

USER PROFILE

Realm settings

User profile

MyRealm

Realm settings are settings that control the options for users, applications, roles, and groups in the current realm. [Learn more](#)

General

Login

Email

Themes

Keys

Events

Localization

Security defenses

Sessions

Tokens

Client policies

User profile

User registration

Attributes Attributes Group JSON editor

All groups

Create attribute

	Attribute [Name]	Display name	Attribute group
⋮	username	`\${username}`	
⋮	email	`\${email}`	
⋮	firstName	`\${firstName}`	
⋮	lastName	`\${lastName}`	

Kullanıcıların kişisel bilgilerini ve profillerini yönetir. Bu alan, kullanıcıların hesap bilgilerinin, kimlik bilgilerinin ve profil ayarlarının yapılandırılmasını sağlar.

AUTHENTICATION

Authentication		
Authentication is the area where you can configure and manage different credential types. Learn more		
Flows	Required actions	Policies
<input type="text" value="Search for flow"/> Create flow Refresh		
Flow name	Used by	Description
browser (Built-in)	Browser flow	browser based authentication
clients (Built-in)	Client authentication flow	Base authentication for clients
direct grant (Built-in)	Direct grant flow	OpenID Connect Resource Owner Grant
docker auth (Built-in)	Docker authentication flow	Used by Docker clients to authenticate against the IDP
first broker login (Built-in)	First broker login flow	Actions taken after first broker login with identity provider account, which is not yet linked to any Keycloak account
registration (Built-in)	Registration flow	registration flow
reset credentials (Built-in)	Reset credentials flow	Reset credentials for a user if they forgot their password or something

Kimlik doğrulama süreçlerinin yönetilmesini sağlayan alanları içerir. Bu sekme, kullanıcıların sisteme giriş yaparken hangi kimlik doğrulama adımlarından geçeceklerini tanımlamanıza olanak tanır. Burada kullanıcı giriş akışları, kimlik doğrulama mekanizmaları, zorunlu adımlar ve diğer güvenlik ayarları yapılandırılabilir.

a.Flows (Akışlar)

Kimlik doğrulama işlemlerinin adımlarını tanımlayan akışlardır. Örneğin, bir kullanıcı sisteme giriş yaparken hangi adımları takip edecek (şifre girme, iki faktörlü kimlik doğrulama vb.) bu alanda belirlenir.

b.Required Actions (Zorunlu Eylemler)

Kullanıcıların oturum açtıklarında yapmaları gereken zorunlu eylemleri içerir. Örneğin, e-posta doğrulama, şifreyi değiştirme veya ek güvenlik sorusu oluşturma gibi eylemler burada belirlenir.

Authentication

Authentication is the area where you can configure and manage different credential types. [Learn more](#)

Flows

Required actions

Policies

Action	Enabled	Set as default action	Configure
Configure OTP	<div><div></div>On</div>	<div><div></div>Off</div>	
Terms and Conditions	<div><div></div>Off</div>	<div><div></div>Disabled off</div>	
Update Password	<div><div></div>On</div>	<div><div></div>Off</div>	<div></div>
Update Profile	<div><div></div>On</div>	<div><div></div>Off</div>	
Verify Email	<div><div></div>On</div>	<div><div></div>Off</div>	
Delete Account	<div><div></div>Off</div>	<div><div></div>Disabled off</div>	
Webauthn Register	<div><div></div>On</div>	<div><div></div>Off</div>	
Webauthn Register Passwordless	<div><div></div>On</div>	<div><div></div>Off</div>	
Verify Profile	<div><div></div>On</div>	<div><div></div>Off</div>	
Delete Credential	<div><div></div>On</div>	<div><div></div>Off</div>	
Update User Locale	<div><div></div>On</div>	<div><div></div>Off</div>	

c.Policies

Kimlik doğrulama işlemleriyle ilgili kurallar ve politikalar tanımlanır. Bu politikalar, belirli kimlik doğrulama adımlarının nasıl uygulanacağını veya kimlik doğrulama süreçlerinde hangi kısıtlamaların kullanılacağını belirler.

Authentication
Authentication is the area where you can configure and manage different credential types. [Learn more](#)

Flows Required actions Policies

Password policy OTP Policy Webauthn Policy Webauthn Passwordless Policy CIBA Policy

No password policies

You haven't added any password policies to this realm. Add a policy to get started.

Add policy

1.Password Policy: Şifre güvenliği ve karmaşıklığını düzenler.

2.OTP Policy: Tek kullanımlık şifrelerin ayarlarını yapar.

3.Webauthn Policy: Biyometrik veya donanım tabanlı kimlik doğrulamayı yönetir.

4.Webauthn Passwordless Policy: Şifresiz, yalnızca biyometrik/donanım tabanlı girişleri düzenler.

5.CIBA Policy: Arka kanal üzerinden istemci başlatılan kimlik doğrulama süreçlerini yönetir.

Identity providers

Kullanıcıların harici kimlik sağlayıcıları aracılığıyla kimlik doğrulama yapmasını sağlayan bir alanı yönetir. Bu sekme, uygulamanızın çeşitli harici kimlik sağlayıcılarıyla (Google, Facebook, GitHub gibi) entegrasyonunu ayarlamanıza olanak tanır.

Identity providers
Identity providers are social networks or identity brokers that allow users to authenticate to Keycloak. [Learn more](#)

To get started, select a provider from the list below.

User-defined:

Keycloak OpenID Connect

OpenID Connect v1.0

SAML v2.0

Social:

BitBucket

Facebook

GitHub

GitLab

Google

Instagram

LinkedIn

Microsoft

OpenShift v3

OpenShift v4

PayPal

StackOverflow

Twitter

User federation

Keycloak'ta dış sistemlerden (örneğin, LDAP veya Active Directory) gelen kullanıcıları yönetmek ve entegre etmek için kullanılır. Bu özellik, merkezi bir kimlik doğrulama ve kullanıcı yönetimi sağlamak amacıyla harici dizinler veya veritabanları ile entegrasyon yapmanıza olanak tanır.