مدیریت کاربران و ساخت کلاینت در Keycloak

- راهنمای تصویری مدیریت کاربران و ساخت کلاینت

راهنمای تصویری مدیریت کاربران و ساخت کلاینت

۱. ورود به پنل مدیریت

این راهنما برای انجام کارهای روزمرهٔ راهبر سامانه در پنل مدیریت ورود یکپارچه تهیه شده است. منظور از کاربر شخصی است که وارد برنامه می‌شود و منظور از کلاینت برنامه‌ای است که برای ورود کاربران به سامانهٔ ورود یکپارچه متصل می‌شود.

آدرس پنل را در مرورگر باز کنید

اگر صفحهٔ ورود نمایش داده شد، با حساب راهبری تحویل‌شده به شما وارد شوید.

از منوی سه‌خط بالای صفحه، بخش موردنظر را انتخاب کنید. عنوان Current realm باید مطابق با مقدار داده شده باشد. Realm محدوده‌ای است که کاربران و برنامه‌های شما در آن مدیریت می‌شوند.

برای این آموزش از بخش‌های Users و Clients استفاده می‌کنیم. بخش‌های تنظیمات پیشرفته برای انجام مراحل این راهنما لازم نیستند.

01-home.jpg

تصویر ۱ ـ منوی مدیریت؛ Users برای کاربران و Clients برای برنامه‌ها

۲. مشاهده و جست‌وجوی کاربران

از منوی اصلی وارد Users شوید.

نام کاربری فرد را وارد کنید و جست‌وجو را اجرا کنید.

برای باز کردن مشخصات، روی نام کاربری کلیک کنید.

image-1793112916817.pngimage-1793112949168.png

۳. ایجاد کاربر جدید

در Users روی Add User کلیک کنید.

در قسمت General اطلاعات کاربر را مطابق توضیحات زیر وارد کنید. برای دیدن همهٔ فیلدها، صفحه را به پایین حرکت دهید.

Username — نام کاربری یکتا؛ مانند کدملی. این فیلد در فرم فعلی اجباری است.

Email — ایمیل کاربر؛ در صورت استفاده از ایمیل در فرایندهای سامانه، آدرس صحیح را ثبت کنید.

First name — نام

Last name — نام خانوادگی

Email verified به معنی تأییدشدن ایمیل است.

image-1793170599673.png04-user-fields.jpg

تصویر ـ مشخصات یک کاربر نمونه و دکمهٔ Create

پس از کنترل اطلاعات، روی Create کلیک کنید. سپس برای کاربر رمز اولیه تعیین و وضعیت فعال‌بودن حساب را بررسی کنید.

۴. تنظیم و بازنشانی رمز عبور

مسیر: Users ← انتخاب کاربر ← Credentials

در زبانهٔ Credentials، گزینهٔ Set password یا برای رمز موجود Reset password را انتخاب کنید.

رمز جدید و تکرار آن را وارد کنید.

ثبت و تأیید را انجام دهید و رمز اولیه را طبق روش موردتأیید سازمان به کاربر تحویل دهید.

رمز باید با سیاست رمز عبور سامانه سازگار باشد. برای کاربری که رمز را فراموش کرده است، همین مسیر را دنبال کنید.

image-1793170777783.png

image-1793170960838.png

image-1793171005486.png

image-1793171074061.png

image-1793171109692.png

image-1793171468626.png

۵. ویرایش کاربر، وضعیت حساب و گروه‌ها

اصلاح مشخصات و فعال یا غیرفعال‌کردن

از Users کاربر را باز کنید. در Details مشخصات را اصلاح و Save را بزنید. کلید Enabled وضعیت حساب را تعیین می‌کند؛ روشن برای اجازهٔ ورود و خاموش برای جلوگیری از ورود بعدی است. نتیجه تغییر را در پنل کنترل کنید.

image-1793171709388.png

اختصاص گروه به کاربر

از بخش Users، کاربر موردنظر را باز کنید و وارد زبانهٔ Groups شوید. روی Join Group کلیک کنید، گروه موردنظر را از فهرست انتخاب کنید و دکمهٔ Join را بزنید. سپس بررسی کنید نام گروه در فهرست گروه‌های کاربر نمایش داده شود.

گروه را مطابق مسئولیت و دسترسی مصوب کاربر انتخاب کنید. کاربر با عضویت در گروه، دسترسی‌های تعریف‌شده برای آن گروه را دریافت می‌کند. اگر گروه مناسب موجود نیست، موضوع را به تیم پشتیبانی ارجاع دهید.

image-1793172306443.png

image-1793172460165.png

۶. ساخت کلاینت؛ مشخصات اولیه

برای اتصال یک برنامهٔ جدید، ابتدا نام و آدرس‌های اتصال را از مسئول فنی همان برنامه دریافت کنید. اطلاعات موردنیاز: شناسهٔ کلاینت، نام نمایشی، نوع برنامه و آدرس دقیق بازگشت از ورود. نمونه‌های این راهنما مخصوص آموزش‌اند و باید با مقادیر واقعی برنامه جایگزین شوند.

از منوی اصلی وارد Clients شوید.

روی Create client کلیک کنید.

image-1793174193556.png

تصویر ـ فهرست کلاینت‌ها و دکمهٔ Create client

فیلد — مقدار ای توضیح

Client type — برای اتصال مطرح‌شده در این راهنما، OpenID Connect.

Client ID — شناسهٔ یکتای برنامه؛ مانند customer-portal. همین مقدار باید در تنظیمات برنامه استفاده شود.

Name — نام خوانا؛ مانند «پرتال مشتری».

Description — توضیح کوتاه، در صورت نیاز.

Always display in UI — برای این نمونه در حالت پیش‌فرض باقی می‌ماند.

روی Next کلیک کنید.

06-client-general.jpg

تصویر ۶ ـ مرحلهٔ General settings با شناسه و نام نمونه

۷. تنظیم احراز هویت و مجوزدهی کلاینت

در مرحلهٔ Capability config، برای اتصال موردنظر این راهنما، هر دو گزینهٔ Client authentication و Authorization را در حالت On قرار دهید.

تنظیمات موردنیاز

Client authentication: ابتدا این گزینه را روشن کنید تا برنامه هنگام اتصال، هویت خود را به سامانه اثبات کند. پس از ساخت کلاینت، رمز آن از بخش Credentials قابل دریافت است و باید در بخش سرور برنامه نگهداری شود.

Authorization: سپس این گزینه را روشن کنید تا قابلیت مدیریت مجوزهای دسترسی برای این کلاینت فعال شود. تنظیمات جزئی مجوزها در محدودهٔ این آموزش نیست.

Standard flow را برای ورود از طریق صفحهٔ ورود فعال نگه دارید. با روشن‌شدن Authorization، گزینه Service accounts roles نیز به‌صورت خودکار فعال می‌شود؛ آن را در همین وضعیت باقی بگذارید. سایر گزینه‌ها را مطابق تصویر تغییر ندهید و برای رفتن به مرحلهٔ آدرس‌های برنامه روی Next کلیک کنید.

07-client-capabilities-enabled.jpg

تصویر ۷ ـ مرحلهٔ Capability config؛ هر دو گزینهٔ Client authentication و Authorization روشن هستند

۸. آدرس‌های برنامه و ذخیرهٔ کلاینت

در مرحلهٔ Login settings، آدرس‌های دقیق برنامه را ثبت کنید. portal.example.org یک دامنهٔ نمونه است و نباید عیناً برای برنامهٔ واقعی استفاده شود.

فیلد — کاربرد و نمونه

Root URL — آدرس پایهٔ برنامه: https://portal.example.org

Home URL — صفحهٔ اصلی برنامه: https://portal.example.org/

Valid redirect URIs — آدرس مجاز بازگشت پس از ورود؛ مسیر دقیق را از مسئول فنی دریافت کنید: https://portal.example.org/login/callback

Valid post logout redirect URIs — اگر برنامه پس از خروج کاربر را برمی‌گرداند، آدرس مورد نیاز را وارد کنید: https://portal.example.org/

Web origins — در صورت نیاز برنامه به درخواست مرورگری بین دو مبدأ، مبدأ دقیق شامل پروتکل، دامنه و درگاه: https://portal.example.org؛ بدون مسیر.

08-client-login.jpg

تصویر ۸ ـ آدرس پایه، صفحهٔ اصلی و آدرس بازگشت نمونه

برای افزودن چند آدرس، از گزینهٔ Add زیر همان فیلد استفاده کنید. آدرس بازگشت باید با تنظیمات برنامه یکسان باشد؛ تفاوت در پروتکل، دامنه، درگاه یا مسیر می‌تواند باعث خطای ورود شود. آدرس دقیق ثبت کنید و از مقدار عمومی * استفاده نکنید.

پس از کنترل اطلاعات، Save را بزنید. نمایش صفحهٔ تنظیمات کلاینت و حضور آن در فهرست بررسی کنید. برای اطمینان از اتصال، یک‌بار ورود و خروج را از خود برنامه آزمایش کنید.

09-client-save.jpg

تصویر ۹ ـ تنظیمات تکمیلی آدرس‌ها و دکمهٔ Save؛ این نمونه ذخیره نشده است

۹. ویرایش کلاینت و اطلاعات اتصال

برای ویرایش، از Clients شناسهٔ برنامه را جستجو و همان کلاینت را باز کنید. آدرس‌ها را در Settings اصلاح و با Save ثبت کنید. برای تغییر وضعیت، گزینهٔ Enabled کلاینت را بررسی کنید؛ غیرفعال‌کردن آن، اتصال برنامه را مختل می‌کند.

image-1793174278028.png

image-1793174464933.png

روش دریافت Client secret

۱. از منوی اصلی وارد Clients شوید و کلاینت برنامه‌ٔخود را با جستوجوی Client ID پیدا کنید. روی شناسه‌ٔهمان کلاینت کلیک کنید.

۲. در زبانه‌ٔSettings بررسی کنید Client authentication در حالت On باشد. اگر آن را تغییری دادید، روی Save کلیک کنید.

۳. زبانه‌ٔCredentials را در صفحه‌ٔهمان کلاینت باز کنید. این زبانه مربوط به اطلاعات اتصال برنامه است؛ با Credentials در صفحه‌ٔکاربران تفاوت دارد.

۴. در قسمت Client secret، مقدار رمز کلاینت قرار دارد که ممکن است به‌صورت مخفی نمایش داده شود. برای مشاهده از آیکون نمایش رمز کنار فیلد استفاده کنید. برای دریافت مقدار کامل، دکمه کپی کنار Client secret را بزنید؛ ستاره‌ها یا نقطه‌های نمایش‌داده‌شده را به‌عنوان رمز کپی نکنید.

۵. مقدار کپی‌شده را همراه با Client ID همان کلاینت و base url سرویس sso، از مسیری محرمانه موردتأیید سازمان به مسئول فنی برنامه تحویل دهید تا در تنظیمات بخش سرور برنامه ثبت کند. Client ID شناسه‌ٔبرنامه است و Client secret رمز محرمانه‌ٔآن؛ این دو مقدار را جابه‌جا وارد نکنید.

image-1793175385063.png

برای دریافت رمز موجود، نیازی به زدن Regenerate نیست. این گزینه رمز جدید ایجاد می‌کند و ممکن است اتصال برنامه‌هایی را که از رمز قبلی استفاده می‌کنند مختل کند.

اگر زبانه‌ٔCredentials یا فیلد Client secret را نمی‌بینید، ابتدا مطمئن شوید کلاینت درست را باز کرده‌اید و Client authentication روشن و ذخیره شده است. اگر همچنان در دسترس نبود، موضوع را با پشتیبانی مطرح کنید.

Client secret را داخل مستند عمومی، تصویر آموزشی یا کد سمت مرورگر قرار ندهید.

کلاینت‌های پیش‌فرض پنل، مانند account و realm-management، متعلق به خود سامانه‌اند. برای برنامه‌ٔمشتری یک کلاینت جدا بسازید.

۱۰. رفع اشکال‌های متداول

مشکل — بررسی ساده

کاربر پیدا نمی‌شود — در realm، املای نام کاربری و فیلتر جستوجو را بررسی کنید.

کاربر نمی‌تواند وارد شود — نام کاربری، فعال‌بودن حساب و رمز را بررسی کنید. اگر رمز موقت است، کاربر باید آن را هنگام ورود تغییر دهد.

کاربر وارد می‌شود ولی دسترسی برنامه را ندارد — نقش‌های مصوب کاربر و تنظیمات دسترسی داخل برنامه را با مسئول برنامه بررسی کنید.

خطای آدرس بازگشت نمایش داده میشود — آدرس اعلامشده از طرف برنامه را با Valid redirect URIs مقایسه کنید.

کلاینت ای برنامه شناخته نمیشود — یکسانبودن Client ID در برنامه و پنل و فعالبودن کلاینت را بررسی کنید.