
راهنمای کامل پیکربندی HR با IIS و Windows Authentication

مقدمه

هدف این راهنما راه اندازی سایت به گونه ای است که:

1. کاربران بدون نیاز به ورود دستی، با نام کاربری ویندوز خود شناسایی شوند. (Windows Authentication)
 2. Frontend سایت توسط IIS سرو شود.
 3. Backend FastAPI فقط مسیرهای API را پردازش کند و درخواست های .../api/ از IIS عبور کنند.
 4. محیط DEV قابل شبیه سازی باشد تا بدون سرور ویندوز واقعی بتوان فرآیند Authentication را تست کرد.
- توجه: در ویندوز Home ، Windows Authentication واقعی در IIS در دسترس نیست؛ در این حالت شبیه سازی با Fake Header انجام می شود.

آماده سازی سایت در IIS

1-1: ایجاد سایت جدید

1. IIS Manager را باز کنید.
2. روی **Sites → Add Website** کلیک کنید.
3. نام سایت را **HR-Frontend** بگذارید.
4. مسیر **Physical Path** را به فولدر Frontend سایت (HTML/JS/CSS) تنظیم کنید.
5. پورت سایت را مشخص کنید (مثلاً برای تست 8080).
6. روی **OK** کلیک کنید.

1-2: تنظیم مسیر فایل های استاتیک

- مطمئن شوید Frontend شامل index.html و فایل های JS/CSS است.
- IIS به صورت پیش فرض قادر به سرو فایل های استاتیک است، نیازی به نصب اضافی نیست مگر اینکه MIME Type خاصی نیاز باشد.

2 پیکربندی Authentication

هدف Frontend: فقط وقتی نمایش داده شود که کاربر احراز هویت شده باشد و API ها بتوانند نام کاربر را دریافت کنند.

2-1: غیرفعال کردن Anonymous Authentication

1. در IIS Manager روی سایت HR-Frontend کلیک کنید.
2. وسط صفحه روی **Authentication** دوبار کلیک کنید.
3. **Anonymous Authentication** را انتخاب کرده و **Disable** کنید.

2-2: فعال کردن Windows Authentication

- در ویندوز سرور:
 - گزینه **Windows Authentication** را Enable کنید.
 - گزینه **Anonymous Authentication** را Disable نگه دارید.
 - در ویندوز Home:
 - **Windows Authentication** در IIS موجود نیست.
 - برای تست، می‌توان از یک **Fake Header** در درخواست‌ها استفاده کرد (مثلاً: x-windows-user: DOMAIN\Username) تا Backend بتواند نام کاربر را شبیه‌سازی کند.
- توضیح Windows Authentication: به IIS اجازه می‌دهد نام کاربر ویندوز را دریافت کند و آن را در هدرهای استاندارد مانند REMOTE_USER یا LOGON_USER ارسال کند.

3 نصب و فعال‌سازی Reverse Proxy

برای اینکه IIS بتواند درخواست‌های .../api/ را به FastAPI هدایت کند:

3-1: نصب Application Request Routing (ARR)

1. اگر در IIS گزینه ARR را نمی‌بینید، باید آن را نصب کنید:

○ از **Web Platform Installer** یا **Microsoft Download Center** برای نصب ARR استفاده کنید.

○ این نصب معمولاً نیاز به دسترسی Administrator دارد.

2-3 فعال سازی Proxy در ARR:

1. در IIS Manager روی نام کامپیوتر (سرور) کلیک کنید.
 2. وسط صفحه روی **Application Request Routing Cache** کلیک کنید.
 3. در پنل سمت راست روی **Server Proxy Settings** کلیک کنید.
 4. گزینه **Enable Proxy** را فعال کنید.
 5. روی **Apply** کلیک کنید.
- توضیح Proxy: اجازه می دهد IIS درخواست ها را به Backend (FastAPI) هدایت کند بدون اینکه کاربر مستقیماً با آن ارتباط داشته باشد.

4 ایجاد Rule برای هدایت API ها به Backend

1-4 ورود به URL Rewrite

1. در IIS Manager روی سایت HR-Frontend کلیک کنید.
2. وسط صفحه روی **URL Rewrite** دوبار کلیک کنید.
3. روی **Add Rules(s)...** کلیک کنید.
4. گزینه **Reverse Proxy** را انتخاب کنید و OK کنید.

2-4 تنظیم مسیر Backend

- Backend: URL سرور → Inbound Rules وارد کنید
- http://127.0.0.1:8000
- تیک گزینه **Enable SSL Offloading** را در صورت نیاز فعال کنید.
- روی **OK** کلیک کنید.

3-4 محدود کردن فقط به مسیر /api/

1. Rule ساخته شده را باز کنید.

2. در بخش **Conditions** شرط اضافه کنید تا فقط مسیرهایی که با /api/ شروع می شوند هدایت شوند.

/*api/

3. سایر مسیرها (صفحه اصلی و صفحات Frontend) توسط IIS سرو شوند.

توضیح: این محدودیت باعث می شود Frontend تحت مدیریت IIS باشد و Backend فقط API را پردازش کند.

5 اجرای Backend FastAPI

1. به فولدر Backend بروید:

2. cd C:\Projects\HR\backend

3. محیط مجازی را فعال کنید:

4. venv\Scripts\activate

5. Backend را اجرا کنید:

6. python run.py

7. پنجره ترمینال را باز نگه دارید تا Backend فعال باشد.

توضیح Backend: فقط مسیرهای API را پاسخ می دهد و Frontend از IIS سرو می شود.

6 شبیه سازی Windows Authentication در محیط DEV

- اگر روی ویندوز Home هستید یا Windows Authentication فعال نیست، می توانید از Fake Header استفاده کنید:

○ مثال هدر:

○ x-windows-user: DOMAIN\AliTest

- Backend FastAPI این هدر را می خواند و نام کاربر شبیه سازی شده را دریافت می کند.

توضیح: این روش برای تست قابلیت احراز هویت بدون سرور واقعی مفید است.

تست نهایی

1. مرورگر را باز کنید و به IIS سایت (مثلاً پورت 8080) بروید:
 2. `http://localhost:8080/`
 - صفحه اصلی Frontend باید بالا بیاید.
 3. تست API:
 4. `http://localhost:8080/api/hr/users`
 - درخواست باید به Backend FastAPI هدایت شود و اطلاعات JSON کاربران را برگرداند.
 - در حالت DEV با Fake Header، نام کاربر شبیه‌سازی شده را دریافت می‌کند.
 5. بررسی هدرها و لاگ‌ها در FastAPI برای اطمینان از درست بودن Authentication.
-

نکات مهم

- همه مسیرهای Frontend از IIS سرو می‌شوند، Backend فقط API دارد.
 - Windows Authentication واقعی فقط روی Windows Server در دسترس است، در ویندوز Home باید Fake Header یا محیط DEV استفاده شود.
 - URL Rewrite و ARR برای هدایت به `.../api/` به Backend ضروری است.
 - Frontend و Backend در یک پورت ظاهر نمی‌شوند، IIS همه مسیرها را یکپارچه به کاربر ارائه می‌دهد.
-

نتیجه نهایی:

با این پیکربندی، کاربران سایت بدون ورود دستی شناسایی می‌شوند، Frontend سریع و امن سرو می‌شود، و Backend مسئول پردازش API هاست. این ساختار هم برای تست DEV و هم برای محیط واقعی Production آماده است.
