# راهنمای راه اندازی **سیستم احراز هویت و بالا آمدن سایت با IIS ویندوز**

---

این راهنما برای یک APP و برای بالا آوردن آزمایشی سیستم نوشته شده است. بسته به نتیجه پیاده سازی نسخه تست و مشکلاتی که به وجود می آید. این راهنما اصلاح و یا کاملتر میشود.

---

پیش نیاز:

بک اند: ایجاد محیط مجازی و نصب کتابخانه های پایتون که در فایل requirements.txt پروژه است.

سیستم IIS: **Application Request Routing (ARR)** و URL Rewrite روی سرور نصب شود.

---

ابتدا توضیح دهیم که این سیستم چگونه کار میکند تا به آن یک دید کلی داشته باشیم:

فرانت این پروژه با استفاده از خود سیستم ویندوز یعنی Internet Information Services (IIS) روی پورتی که ما بخواهیم serve میشود. FastAPI فقط برای بک اند فعال است و درخواست های API را پردازش میکند. این درخواست توسط IIS به آن ارسال میشود.

پروژه ما از IIS طبق راهنمایی این فایل روی پورت 8080 بالا می آید. *این پورت با توجه به پورت های آزاد سیستم سرور میتواند تغییر کند.*

پورت بک اند ما یعنی FastAPI(uvicorn) روی پورت 8000 بالا می آید. *این پورت با توجه به پورت های آزاد سیستم سرور میتواند تغییر کند.*

منطق کلی احراز هویت در سیستم ما به این شکل است: کاربر ابتدا به پورت **8080** سرور که برای **IIS** تنظیم شده، درخواست می‌فرستد. این درخواست می‌تواند برای مشاهده صفحات وبسایت باشد یا برای فراخوانی یک API. **سیستم احراز هویت ویندوزی (Windows Authentication) که روی IIS فعال است، درخواست کاربر را بررسی می‌کند**. اگر هویت کاربر معتبر باشد، IIS اجازه ادامهٔ دسترسی را می‌دهد و درخواست به **FastAPI** فوروارد می‌شود. در این مرحله **FastAPI هیچ اطلاعی از رمز عبور یا اطلاعات حساس کاربر ندارد** و تنها اطلاعاتی که دریافت می‌کند، نام کاربری ویندوزی و در صورت نیاز، اطلاعات تکمیلی مانند **گروه‌های Active Directory** هستند که برای مدیریت سطح دسترسی داخل برنامه استفاده می‌شوند.

لازم به ذکر است که این مکانیزم تنها زمانی به صورت خودکار کار می‌کند که **کاربر و سرور داخل یک شبکه داخلی باشند و مرورگر کاربر از احراز هویت یکپارچه ویندوز (Integrated Windows Authentication) پشتیبانی کند**. در این حالت مرورگر به طور خودکار هویت فعلی کاربر (مثلاً

(DOMAIN\usernameرا به IIS می‌فرستد. این هویت به شکل **رمزنگاری شده توسط NTLM یا Kerberos**منتقل می‌شود و خارج از شبکه داخلی یا به سایت‌های دیگر ارسال نمی‌شود. بنابراین امنیت اطلاعات کاربر حفظ می‌شود و تنها سروری که عضو همان دامنه است می‌تواند این اطلاعات را دریافت و پردازش کند.
با استفاده از این مکانیزم، کاربران نیاز به وارد کردن نام کاربری و رمز عبور به صورت دستی ندارند و احراز هویت به صورت خودکار انجام می‌شود. این روش، استاندارد **Enterprise**در سازمان‌ها برای سیستم‌های داخلی و شبکه‌های مبتنی بر Active Directory است.

در معماری ما، IISعلاوه بر احراز هویت، نقش **Reverse Proxy** را نیز ایفا می‌کند. این یعنی تمام درخواست‌هایی که مسیرشان با api/شروع می‌شود، به FastAPI که روی پورت 8000 در حال اجراست، فوروارد می‌شوند. این کار باعث می‌شود که:

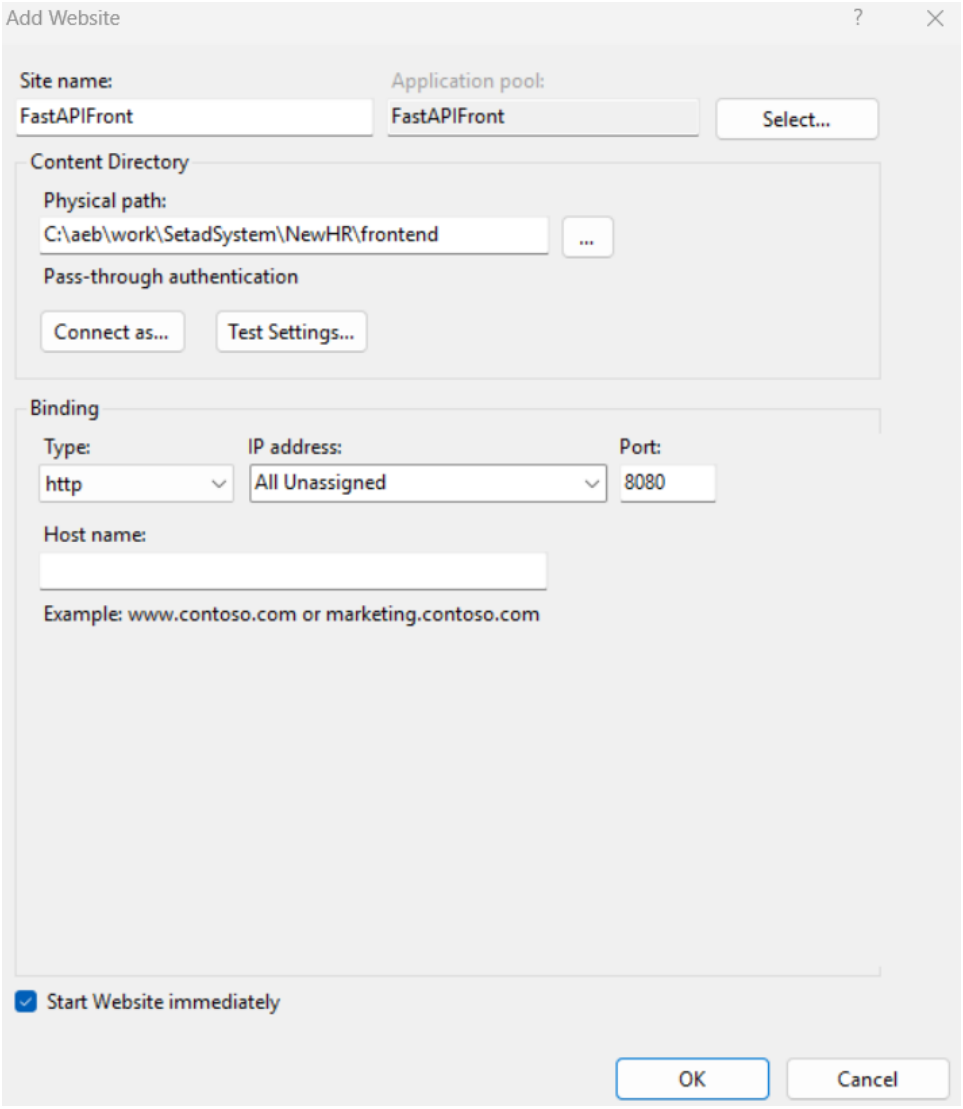
1. FastAPI بتواند **بدون نگرانی از احراز هویت** منطق خود را اجرا کند و تمرکز بر پردازش داده‌ها داشته باشد.
2. FastAPI بتواند **به‌صورت async و با عملکرد بالا** اجرا شود، چرا که uvicorn بهینه‌سازی‌های مخصوص خودش را دارد و نیازی به اجرا کردن مستقیم در IIS نیست.
3. امنیت سیستم حفظ شود، زیرا تنها IIS می‌تواند Header مربوط به کاربر را به FastAPI بفرستد و پورت FastAPIبه صورت مستقیم در دسترس کاربران خارجی نیست.

---

مراحل:

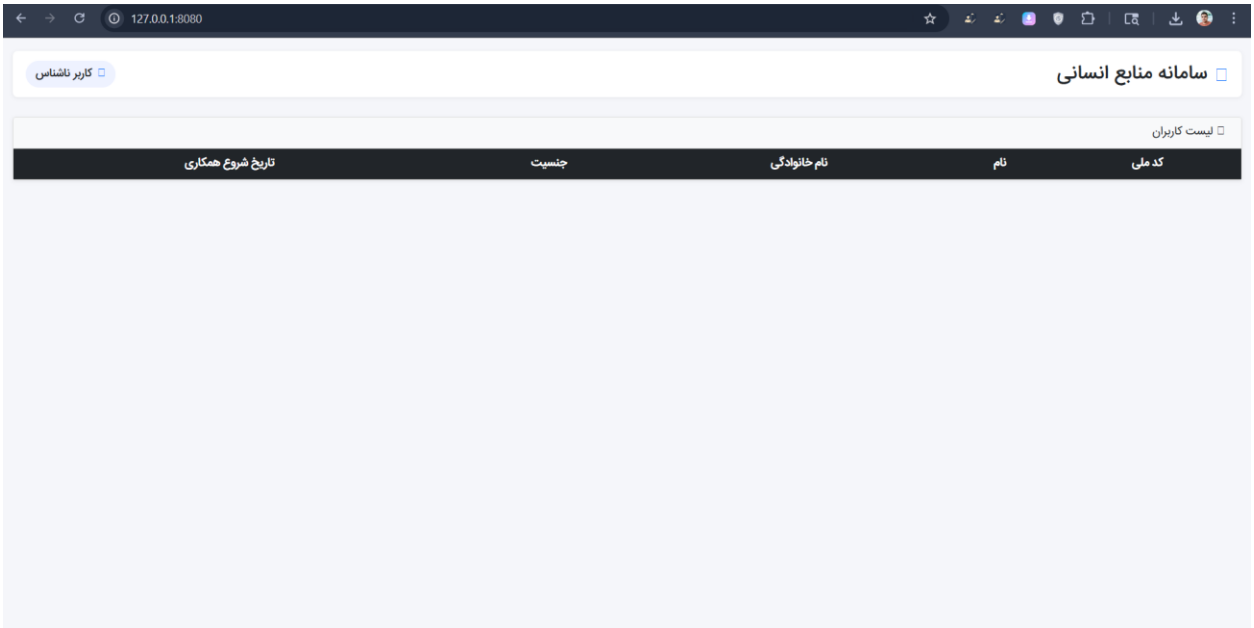
### .1راه‌اندازی Frontend باIIS :

ابتدا IIS Manager را باز کنید. می‌توانید از Start → IIS Manager یا از Run دستور inetmgr استفاده کنید.
سپس روی Sites راست‌کلیک کرده و گزینه Add Website را انتخاب کنید. در پنجره باز شده، یک نام برای سایت وارد کنید، مثلاFastAPIFront.
در بخشPhysical Path ، مسیر فولدر frontend پروژه را انتخاب کنید. این همان فولدری است که شامل فایل‌هایHTML ، CSSو JS پروژه می‌باشد.
در بخشPort ، پورتی که می‌خواهید سایت روی آن بالا بیاید را وارد کنید، مثلا 8080. اگر این پورت آزاد نیست، می‌توانید هر پورت آزاد دیگری را انتخاب کنید.




اگر روی ویندوز سرور اجرا میکنید: پس از ایجاد سایت، سایت جدید را انتخاب کرده و به بخش Authenticationبروید Windows Authentication .را فعال کنید و Anonymous Authenticationرا غیرفعال کنید. این کار باعث می‌شود که احراز هویت کاربران توسط ویندوز انجام شود و کاربران بدون وارد کردن نام کاربری و رمز عبور به سایت دسترسی پیدا کنند.

هم اکنون باید بتوانید نمای کلی سایت را از طریق مرورگر خود ببینید.

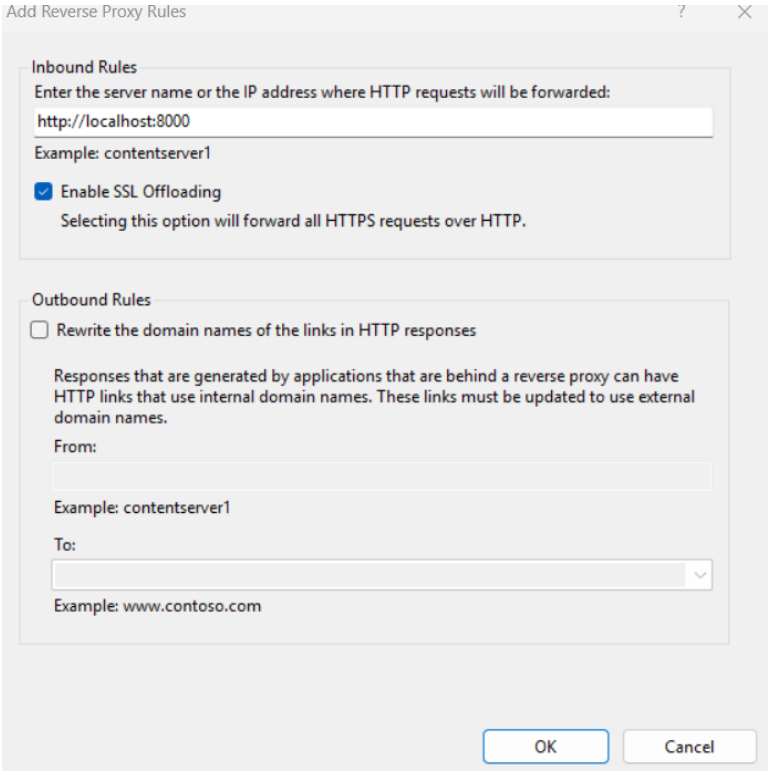



## 2. تنظیم Reverse Proxy برای مسیرهای API

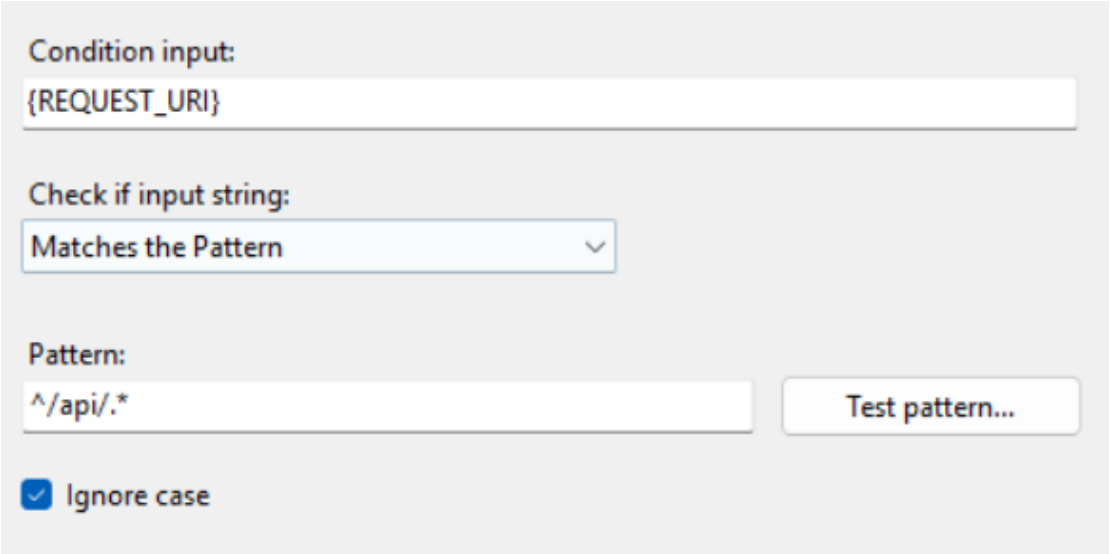
فعال‌سازی: IIS Manager رو باز کن

1. در پنل سمت چپ، روی اسم کامپیوتر کلیک کن
   (همون بالاتر از Sites — خیلی مهمه روی سایت کلیک نکنی)
2. وسط صفحه دنبال Application Request Routing Cache بگرد
3. روش دوبار کلیک کن
4. از پنل سمت راست، روی Server Proxy Settings... کلیک کن
5. تیک Enable Proxy رو بزن
6. روی Apply کلیک کن

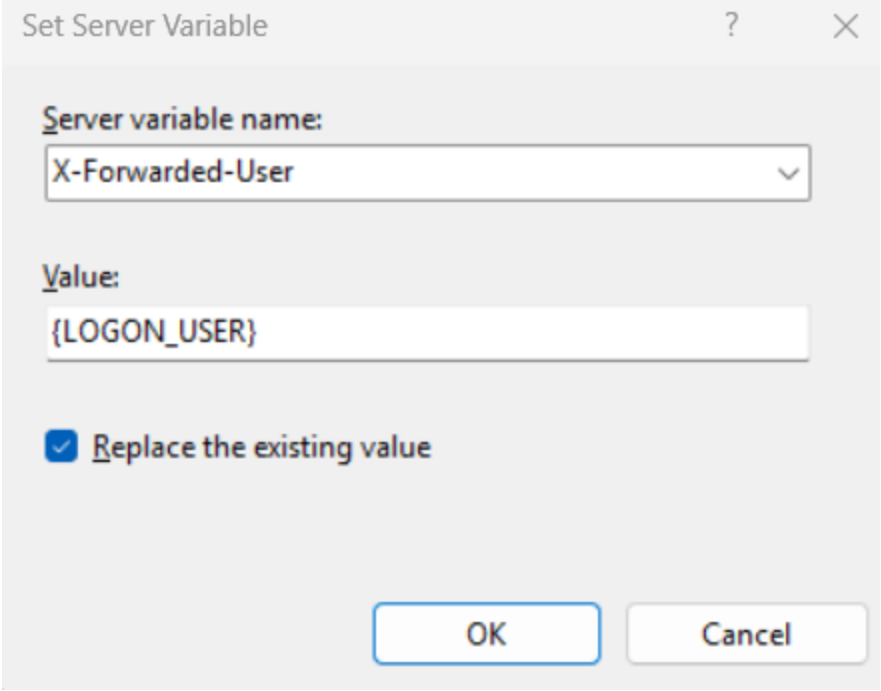
برای اینکه درخواست‌های مسیرهای /api به FastAPI فوروارد شوند، به بخش URL Rewrite در IIS بروید و Add Rule → Reverse Proxy را انتخاب کنید.
Destination را روی http://localhost:8000 تنظیم کنید.




شرط را به گونه‌ای بگذارید که فقط مسیرهایی که با /api شروع می‌شوند، فوروارد شوند.



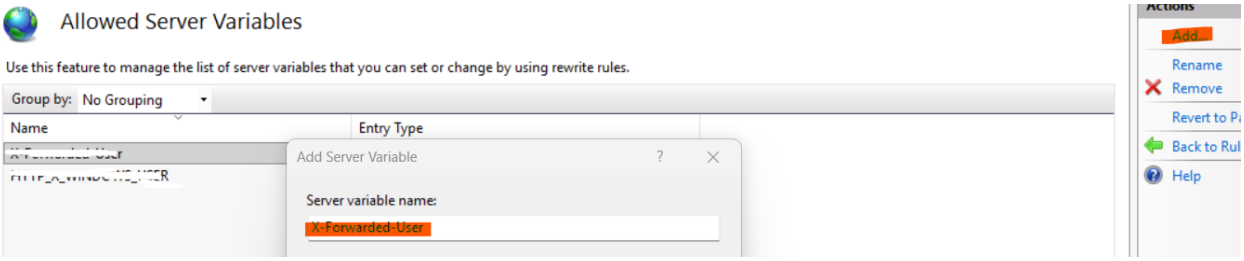

همچنین برای ارسال نام کاربری کاربر به FastAPI ، یک Header جدید ایجاد کنید با نام X-Forwarded-User و مقدار {LOGON_USER}. این Header شامل نام کاربری ویندوز کاربر است و در FastAPI برای مدیریت سطح دسترسی استفاده می‌شود.




به صفحه اصلی url rewrite سایت، بروید

در سمت راست، روی "View Server Variables" کلیک کن.

Server Variable جدید اضافه کن.



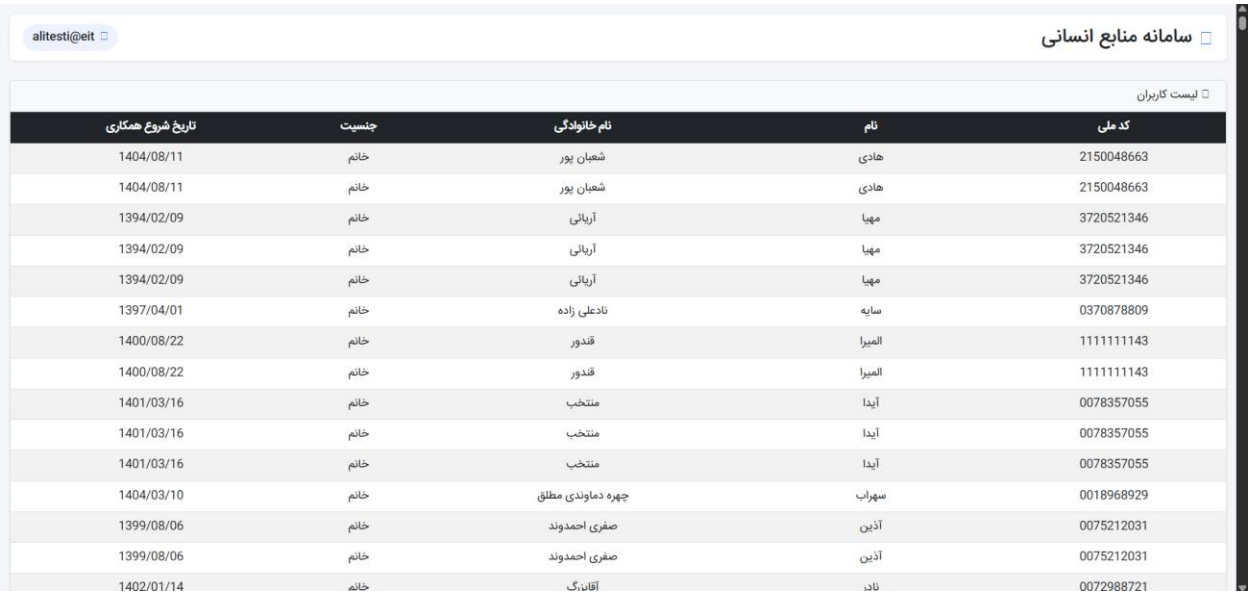

## 3. اجرای Backend (FastAPI)

ما میخواهیم بک اند را اجرا کنیم. حالا برای اجرای دائمی اون به عنوان سرویس بعدا از NSSM کمک میگیریم. برای تست اولیه کافی هستش با فعال بودن محیط مجازی و نصب بودن کتابخانه های مورد نیاز در پوشه بک اند بزنید و آن را اجرا کنید:

```
python run.py
```

## دسترسی کاربران به سایت

کاربران در شبکه داخلی فقط کافی است مرورگر خود را باز کرده و به URL سایت روی پورت IIS دسترسی داشته باشند. مرورگر به صورت خودکار احراز هویت ویندوز را انجام می‌دهد و نام کاربری کاربر به FastAPI ارسال می‌شود. هیچ فرم Login یا تنظیم اضافی روی سیستم کاربر لازم نیست.

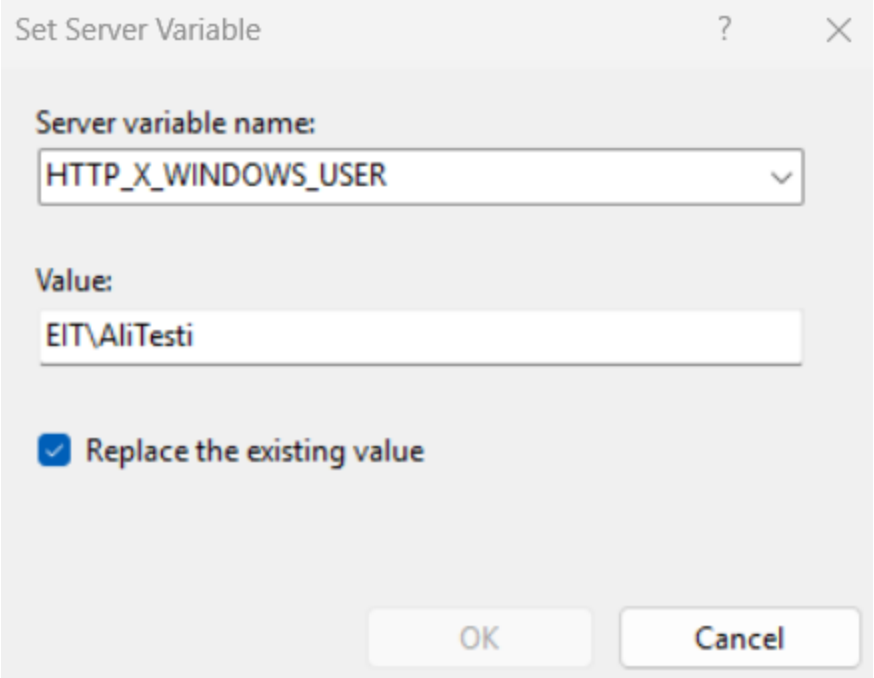



| کد ملی | نام | نام خانوادگی | جنسیت | تاریخ شروع همکاری |
|---|---|---|---|---|
| 2150048663 | هادی | شعبان پور | خانم | 1404/08/11 |
| 2150048663 | هادی | شعبان پور | خانم | 1404/08/11 |
| 3720521346 | مهیا | آریائی | خانم | 1394/02/09 |
| 3720521346 | مهیا | آریائی | خانم | 1394/02/09 |
| 3720521346 | مهیا | آریائی | خانم | 1394/02/09 |
| 0370878809 | سایه | نادعلی زاده | خانم | 1397/04/01 |
| 1111111143 | المیرا | قندور | خانم | 1400/08/22 |
| 1111111143 | المیرا | قندور | خانم | 1400/08/22 |
| 0078357055 | آیدا | منتخب | خانم | 1401/03/16 |
| 0078357055 | آیدا | منتخب | خانم | 1401/03/16 |
| 0078357055 | آیدا | منتخب | خانم | 1401/03/16 |
| 0018968929 | سهراب | چهره دماوندی مطلق | خانم | 1404/03/10 |
| 0075212031 | آذین | صفری احمدوند | خانم | 1399/08/06 |
| 0075212031 | آذین | صفری احمدوند | خانم | 1399/08/06 |
| 0072988721 | نادر | آقایی | خانم | 1402/01/14 |

## نکات مهم

کد ها روی حالت توسعه اجرا میشود. به این معنا که همیشه یک یوزر خاص رو با تمام دسترسی ها فعال میکند. برای تست، محیط حتما باید روی چیزی غیر از DEV قرار بگیرد. فایل env در پوشه بک اند را ببینید متوجه میشوید.

اگر از روی ویندوزی که windows Authentication ندارد برای تست استفاده میکنید باید به صورت فیک هدر بدهید.




باید همین اسم را به متغیر های سرور هم اضافه کنید (شبیه متغیری که برای legon اضافه کردیم)