**تنظیمات فایروال ویندوز**

**فایروال ویندوز**

تنظیمات فایروال: ویندوز شامل یک [فایروال](https://softyab.com/what-is-firewall/) داخلی است که انتقال داده‌ها بین رایانه شما و سایر رایانه‌ها را از طریق شبکه یا اینترنت کنترل می‌کند. فایروال به کاربران اجازه می‌دهد، برنامه‌های مورد اعتماد را که اجازه انتقال اطلاعات بین رایانه محلی و رایانه‌های از راه دور را دارند مشخص کنند و درخواست‌های دیگر برنامه‌ها و رایانه‌ها را مسدود کنند.

هنگامی که آزمایشی در حال اجرا است، داده‌ها را از طریق یک پورت با موتور آزمایش مبادله می کند. که به طور پیش فرض پورت 2377 است. بنابراین، باید فایروال را تنظیم کنید تا ترافیک از طریق پورت بتواند آزمایشات را با موفقیت اجرا کند.

علاوه بر این، اگر از مجوز کاربر شناور استفاده می‌کنید، TestLeft از پروتکل‌های TCP و UPD و پورت 1947 برای ارتباط با رایانه‌ای که مجوز شما فعال است (License Manager PC) استفاده می‌کند. این پروتکل‌ها و پورت‌ها نباید مسدود شوند.

**نکات مهم**

* فایروال را در همه رایانه‌هایی که در آن تست‌ها را اجرا می کنید تنظیم کنید.
* اگر رایانه شما به دامنه متصل است، تنظیمات فایروال ممکن است توسط سرپرست سیستم کنترل شود. در این مورد، از سرپرست سیستم خود بخواهید TestLeft را از طریق فایروال مجاز کند.
* هنگامی که آزمایشات را روی رایانه‌های راه دور انجام می‌دهید ، رایانه شما درخواست‌های زیادی را به آزمایش کننده TestLeft ،  TestComplete یا TestExecute که در آن رایانه ها اجرا می شوند ارسال می‌کند و پاسخ‌هایی از آن دریافت می‌کند. پروکسی‌ها و فایروال‌های شرکت شما ممکن است رایانه‌هایی را که آزمایشات شما در آنها اجرا می‌شود به عنوان منبع اسپم گزارش دهند.

اطمینان حاصل کنید که بخش فناوری اطلاعات خود را در مورد TestLeft مطلع هستند تا در صورت نیاز تنظیمات فایروال را تغییر دهند.

* اگر از مجوز کاربر شناور استفاده می کنید، فایروال را هم در رایانه مجوز مدیریت خود و هم در ایستگاه کاری TestLeft خود پیکربندی کنید.

**بررسی اینکه آیا فایروال در حال اجرا است یا خیر؟**

برای اینکه بدانید فایروال ویندوز در حال اجرا است یا خیر:

* با کلیک بر روی Start و سپس روی Control Panel ، Control Panel  را باز کنید.
* در کادر جستجوFirewall  را تایپ کرده و سپس اپلت Windows Firewall را انتخاب کنید. پنجره Windows Firewall  باز می‌شود.



اگر مکان شبکه‌ای که شامل رایانه‌های آزمایشی شما یا مجوز مدیریت رایانه شما (در صورت استفاده از مجوز کاربر شناور) علامت سبز رنگی در کنار آن وجود دارد، به این معنی است که Windows Firewall در حال اجرا و کنترل انتقال داده‌ها است. در این مورد، شما باید فایروال را پیکربندی کنید تا فعالیت‌های شبکه TestLeft مجاز شود.

**پیکربندی و تنظیمات فایروال**

اگر Windows Firewall برای مکان شبکه‌ای که شامل رایانه‌های آزمایشی شما است روشن است، باید قانونی ایجاد کنید که پورت TestLeft استفاده می‌کند (به طور پیش فرض 2377) باز شود.

1. در سمت چپ پنجره Windows Firewall ، روی Advanced settings کلیک کنید. پنجره Windows Firewall با تنظیمات پیشرفته باز می‌شود.
2. در شاخه سمت چپ پنجره، روی Inbound Rules کلیک کنید.
3. ایجاد یک قانون جدید:
* در پنل Actions پنجره، روی New Rule کلیک کنید New Inbound Rule Wizard ظاهر می شود.
* در صفحه نوع Wizard ،Port  را انتخاب کنید و Next را کلیک کنید.
* در صفحه Protocol and Ports جادوگر‌، Port  را انتخاب کنید. در کادر ویرایش پورت‌های محلی خاص، پورت مورد نیاز را وارد کنید (به طور پیش فرض 2377) و Next را کلیک کنید.
* در صفحه Action Wizard ،Allow the connection را انتخاب کرده و روی Next کلیک کنید.
* در صفحه نمایه Wizard ، مکان شبکه‌ای را که می‌خواهید پورت برای آن باز شود انتخاب کرده و روی Next کلیک کنید.
* در صفحه نام Wizard، در قسمت Name، نام قانون را مشخص کرده و Finish را فشار دهید.

4. در شاخه سمت چپ پنجره Windows Firewall with Advanced Security ،Outbound Rules را انتخاب کنید.

5. مرحله 3 را تکرار کنید تا همان پورت برای اتصالات خروجی باز شود.

اگر از مجوز کاربر شناور استفاده می کنید و Windows Firewall برای مکان شبکه که شامل رایانه مجوز مدیریت شما است روشن است، مطمئن شوید که تردد TCP و UDP از طریق درگاه 1947 مجاز است:

1. در قسمت چپ پنجره Windows Firewall، روی Advanced settings کلیک کنید.
2. در پنجره Windows Firewall و Advanced Security، گزینه Inbound Rules را انتخاب کرده و سپس روی New Rule  کلیک کنید.
3. در Wizard روی Port و سپس Next کلیک کنید.
4. روی TCP کلیک کنید. سپس روی Specific local ports کلیک کرده و 1947  را وارد کنید. روی Next کلیک کنید.
5. روی Allow the connection و سپس Next کلیک کنید.
6. محدوده مورد نیاز را انتخاب کرده و روی Next کلیک کنید.
7. نام قانون را وارد کرده و روی Finish کلیک کنید.

مراحل مربوط به پروتکل UPD را تکرار کنید. سپس مراحل ایجاد قوانین خروجی را تکرار کنید که به ترافیک TCP و UDP از طریق پورت 1947 اجازه می‌دهد.

پنجره Windows Firewall را ببندید.

منبع: [smartbear](https://support.smartbear.com/testleft/docs/using/configuring/os/windows-firewall.html)

لطفا جهت مشاوره در [انتخاب محصول امنیتی مناسب](https://softyab.com/product-category/security/antivirus/) خود با این شماره **09224971053** تماس بگیرید.

**مارو در شبکه های**[**اجتماعی**](https://www.instagram.com/softyab)**خودتان به اشتراک بگذارید.**