Bloqueios de IP e Configurações Recomendadas

1. Visão Geral

Alguns tribunais — com destaque para o **PJe** — adotam validações sobre a origem das conexões de login. Quando identificam que uma mesma origem concentra muitos acessos ou detectam um padrão de troca de IP durante a sessão, esses sistemas podem **bloquear o IP** utilizado.

Na configuração padrão do Presto, a autenticação passa pela **infraestrutura compartilhada e disponibilizada pela Oystr** (IP `177.220.183.60`). Quando um tribunal bloqueia esse IP, o bloqueio afeta **todos os clientes que ainda usam essa configuração padrão** — ou seja, os que não possuem VPN, Proxy Autenticado ou Edge Proxy configurados.

Esse cenário tem solução, fazer o Presto se autenticar pelo **IP do próprio escritório ou colaborador**. Este artigo explica por que os bloqueios acontecem, como resolvê-los e responde às dúvidas mais frequentes.

> Clientes com VPN, Proxy Autenticado ou Edge Proxy configurados ficam isolados desse tipo de instabilidade, porque não dependem do IP compartilhado da Oystr.

---

2. Por que os bloqueios acontecem

Para entender o problema, é preciso entender o caminho que uma autenticação percorre no Presto:

1. O colaborador clica para se autenticar em um tribunal a partir da plataforma Presto — nesse momento a requisição parte do **IP da máquina do colaborador**.

2. O Presto recebe a solicitação e realiza o login usando a credencial protegida — porém, na configuração padrão, esse login sai pela **infraestrutura compartilhada da Oystr** (outro IP).
3. O Presto devolve a **sessão autenticada** ao colaborador, que volta a operar com o **IP de origem** (o da máquina dele).

Alguns tribunais realizam duas verificações que entram em conflito com esse fluxo:

- Se o IP de origem é **nacional**.
- Se o IP que **iniciou** a sessão é o **mesmo** que continua acessando o sistema.

Quando o tribunal percebe que a sessão foi iniciada por um IP e continua por outro, ou quando há muitos acessos a partir de um IP específico, ele interpreta isso como um padrão de automação e pode **bloquear o IP compartilhado da Oystr**. Como esse IP é comum a vários clientes, o bloqueio se propaga para todos que não têm uma configuração de rede própria.

> **Importante:** a igualdade de IP é exigida apenas em **alguns** tribunais. Na maioria dos casos o Presto funciona mesmo com IPs diferentes — mas nos tribunais mais rígidos (como o PJe em algumas regiões), a divergência é o que dispara o bloqueio.

---

3. A solução: fazer o Presto usar o IP do escritório

A causa raiz dos bloqueios é a divergência de IP entre quem inicia e quem continua a sessão. A solução, portanto, é **alinhar o IP**: fazer com que o Presto se autentique usando o mesmo IP do escritório ou do colaborador.

Com isso, do ponto de vista do tribunal, **não há automação nem troca de IP** — apenas um usuário do escritório acessando o sistema diretamente. Isso elimina o gatilho do bloqueio e torna o acesso do cliente **independente da infraestrutura compartilhada da Oystr**.

Existem **três alternativas** de implementar esse alinhamento. Todas atingem o mesmo objetivo; a escolha depende do porte e do perfil de infraestrutura do cliente.

---

4. Três Alternativas de Configurações Recomendadas

Opção	O que é	Indicado para
Edge Proxy	Container Docker instalado na máquina do colaborador. O Presto roteia o tráfego pelo IP daquele colaborador.	Maioria dos casos — solução mais prática e robusta, funciona em escritório e em home office.
Proxy Autenticado	Container com autenticação básica exposto na porta `8888` na infraestrutura do cliente.	Clientes que preferem um ponto de saída controlado na própria rede.
VPN Dedicada	Túnel OpenVPN (v2.5) em modelo client/server, roteando todo o tráfego HTTP/HTTPS.	Clientes maiores que precisam de IP fixo e estável.

As instruções técnicas de cada opção estão nas páginas correspondentes desta Wiki:

- **Edge Proxy** → página *Edge Proxy*
- **Proxy Autenticado** → página *Proxy autenticado*
- **VPN** → página *VPN*

> **Dica:** o cenário ideal para a maioria dos clientes é **um Edge instalado em cada máquina de colaborador** que usa o Presto. O Presto busca automaticamente qualquer Edge associado à conta do usuário que esteja com o IP correto — se ao menos um for encontrado, o acesso funciona.

---

5. A Segurança Não Muda

Este é o ponto mais importante para tranquilizar o cliente: **habilitar uma dessas configurações não altera o modelo de segurança do Presto**.

- As credenciais continuam **protegidas e inacessíveis** ao colaborador.
- O colaborador continua recebendo apenas a **sessão autenticada**, nunca a credencial em si.
- A configuração altera **somente o caminho de rede** (por qual IP o login sai), não a forma como a credencial é armazenada ou utilizada.

Em outras palavras: a proposta de valor do Presto — segurança de credenciais compartilhadas entre colaboradores — permanece integralmente preservada.

6. Perguntas Frequentes (FAQ)

Por que meu acesso ao tribunal parou de funcionar de repente? Provavelmente o tribunal bloqueou o IP compartilhado da Oystr, usado na configuração padrão do Presto. O bloqueio afeta todos os clientes sem configuração de rede própria. A solução é habilitar uma das três opções (Edge Proxy, Proxy Autenticado ou VPN) para que o acesso passe a usar o IP do seu escritório.

O problema é do Presto ou do tribunal? O bloqueio é aplicado pelo tribunal, com base na política de validação de IP dele — que varia de sistema para sistema e foge ao controle da Oystr. O que está sob o seu controle é o caminho de rede: alinhando o IP, o tribunal deixa de identificar o padrão que dispara o bloqueio.

Preciso configurar isso mesmo se hoje está tudo funcionando? É altamente recomendado. Sem uma configuração própria, seu acesso depende do IP compartilhado da Oystr e fica sujeito a bloqueios coletivos a qualquer momento. Com a configuração ativa, seu escritório fica blindado contra esse tipo de instabilidade.

Configurar isso deixa minhas credenciais menos seguras? Não. A configuração muda apenas por qual IP o login sai. As credenciais continuam protegidas e inacessíveis aos colaboradores, exatamente como antes. O modelo de segurança do Presto não é alterado.

Qual das três opções eu devo escolher? Para a maioria dos clientes, o **Edge Proxy** é o mais prático, pois acompanha o IP de cada colaborador e funciona tanto no escritório quanto em home office. Clientes maiores que precisam de IP fixo costumam preferir a **VPN dedicada**. Nossa equipe ajuda a definir a melhor opção para o seu ambiente.

Preciso instalar em todas as máquinas? Não necessariamente, o cenário ideal é um Edge por colaborador que usa o Presto. Um único Edge centralizado funciona apenas se todos os colaboradores estiverem no mesmo IP (por exemplo, dentro do escritório ou sob a mesma VPN).

Home office funciona? Sim, desde que a solução acompanhe o IP do colaborador. O Edge instalado na máquina do próprio colaborador funciona em home office.

Quanto tempo leva para configurar? Depende da opção e da infraestrutura, mas a instalação do Edge costuma ser rápida. Nossa equipe acompanha a configuração de ponta a ponta e valida o acesso antes de liberar.

Se a infraestrutura da Oystr tiver instabilidade no futuro, eu serei afetado? Clientes com configuração própria não dependem do IP compartilhado da Oystr, portanto ficam isolados desse tipo específico de instabilidade normalmente. (Vale lembrar que cada solução tem seus próprios pontos de atenção operacional — como manter o container do Edge ativo — descritos nas páginas

técnicas.)

Quem devo acionar para configurar? Entre em contato com o suporte Presto/Oystr e, de preferência, envolva a equipe de TI do seu escritório. A configuração deve ser feita junto ao responsável técnico de TI do cliente.

---

7. Suporte

Em caso de dúvidas ou dificuldades durante a configuração, entre em contato com a equipe de suporte Presto/Oystr pelo número de Whatsapp +55 41 8458-5837 para verificação erros e avaliação da melhor estratégia de implantação para o seu ambiente.

Revision #3
Created 12 August 2026 13:37:39 by Flávio Santos
Updated 14 August 2026 16:14:46 by Flávio Santos