

Configurações

- [Token A3 Físico](#)
- [Presto Edge](#)
- [VPN](#)
- [Proxy autenticado](#)
- [Bloqueios de IP e Configurações Recomendadas](#)

Token A3 Físico

Este guia é um passo a passo sobre como instalar o componente do Presto para que seja possível acessar sistemas via Presto com o token A3 físico.

Suporte: em caso de dúvidas, entre em contato com a nossa equipe de suporte pelo e-mail leandro@oysttr.com.br.

Pré-requisitos de funcionamento

Para que o Presto possa usar o A3 para acessar um sistema, é necessário que:

1. O token A3 esteja instalado em uma máquina ligada e com acesso à internet no momento em que o usuário do Presto deseja realizar o login.
2. A máquina deve estar rodando o componente `a3-proxy-go`, que faz a conexão entre o Presto e o A3.
3. O certificado A3 deve estar corretamente configurado no cofre do Presto.
4. O usuário tenha a permissão de acessar o site desejado com o A3.

Requisitos

Para instalação do `a3-proxy-go`, é necessária uma máquina Linux com Ubuntu 22.04 LTS ou Ubuntu 24.04 LTS, com os seguintes pacotes instalados:

- `pcscd` (instalado e rodando)
- `docker` (instalado e rodando)
- driver do seu token físico
- `a3-proxy-go` (instalado e rodando)
- token A3 (plugado na máquina e devidamente reconhecido)

Preparação

Interface USB

Certifique-se de que o token A3 está conectado à máquina e execute o seguinte comando:

```
sudo lsusb | grep -iE 'giesecke|starsign|token|smart'
```

O resultado deve ser algo semelhante a:

```
Bus 001 Device 004: ID 0529:0620 Giesecke & Devrient GmbH StarSign CUT
```

Indicando que o token A3 está conectado à máquina e que o sistema USB reconheceu o token.

pcscd

Certifique-se de que o daemon pcscd esteja rodando e execute os seguintes comandos:

```
sudo pcscd --version
sudo systemctl is-active pcscd
sudo ls -la /run/pcscd/pcscd.comm
sudo pcsc_scan -n
```

O resultado do último comando deve ser algo semelhante a:

```
Scanning present readers...
0: Giesecke & Devrient StarSign CUT (00000000) 00 00
Reader 0: Giesecke & Devrient StarSign CUT (00000000) 00 00
Card state: Card inserted,
ATR: 3B FF 96 00 00 81 31 FE 43 80 31 80 65 B0 84 41 3D F6 12 0F FE 82 90 00 55
```

Indicando que o pcscd reconhece o seu token A3. Em caso de erro, verifique se o token A3 está devidamente conectado à máquina, com o driver instalado e com o daemon pcscd rodando.

Caso seja necessário, instale os pacotes do pcscd com:

```
sudo apt update
sudo apt install -y pcscd libccid pcsc-tools
sudo systemctl enable --now pcscd
```

docker

Instale o docker no Ubuntu:

```
sudo apt install -y ca-certificates curl gnupg
sudo install -m 0755 -d /etc/apt/keyrings
curl -fsSL https://download.docker.com/linux/ubuntu/gpg \
| sudo gpg --dearmor -o /etc/apt/keyrings/docker.gpg
sudo chmod a+r /etc/apt/keyrings/docker.gpg
echo "deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.gpg] \
https://download.docker.com/linux/ubuntu jammy stable" \
| sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
sudo apt update
sudo apt install -y docker-ce docker-ce-cli containerd.io docker-buildx-plugin docker-compose-plugin
sudo usermod -aG docker "$USER" # faça logout/login para o grupo ter efeito
```

Teste o docker com:

```
sudo docker run --rm hello-world
```

Instalação do a3-proxy-go

Faça o download das 2 versões disponíveis do nosso container com:

```
sudo docker pull southamerica-east1-docker.pkg.dev/oystre-presto-test/presto-public/a3-proxy-go:<versão-1>
sudo docker pull southamerica-east1-docker.pkg.dev/oystre-presto-test/presto-public/a3-proxy-go:<versão-2>
```

Atenção: as tags de versão das imagens (nos comandos docker pull e na imagem do docker run) aparecem truncadas no documento de origem. Substitua <versão-1>, <versão-2> e v1.1.<patch> pelas tags exatas informadas pela equipe do Presto.

Após a realização de todos os passos anteriores, você está pronto para rodar o a3-proxy-go. Antes de rodar, é necessário entrar em contato com a nossa equipe e requisitar o id a ser usado. No exemplo abaixo, usamos <id> como exemplo:

```
sudo docker run -d \  
  --name a3-proxy-go \  
  --restart unless-stopped \  
  -e HOST_PCSC=1 \  
  -e FRP_NAME=<id> \  
  -e POLL_INTERVAL=5 \  
  -e PKCS11_MODULE=/usr/lib/libaetpkss.so \  
  -p 8443:8443 \  
  -v /run/pcscd/pcscd.comm:/run/pcscd/pcscd.comm \  
  southamerica-east1-docker.pkg.dev/oyster-presto-test/presto-public/a3-proxy-go:v1.1.<patch>
```

A depender da sua versão de Linux, o parâmetro HOST_PCSC deve ser alterado segundo a tabela abaixo:

Host	pcscd version	HOST_PCSC
Ubuntu 22.04	1.9.x	1
Ubuntu 24.04	2.0.3	1
Fedora 41+	2.3.x	2
macOS	(none)	unsupported

Pronto!

Depois de obter o id com a equipe do Presto e rodar o container, você está pronto para configurar o token A3 no nosso cofre.

Manutenção

1. Se a máquina estiver desligada, o container do docker parado, ou sem acesso à internet, o acesso ao A3 não funciona e, por consequência, o login via Presto também não.
2. Eventualmente será necessário retirar e recolocar o A3 na máquina. Isso não tem relação com o Presto, mas com o hardware da máquina.
3. Se o container a3-proxy-go tiver problemas, é necessário enviar os logs para a nossa equipe avaliar. Rode: `sudo docker logs --tail 5000 a3-proxy-go`
4. Caso seja necessário, reinicie o container com: `sudo docker restart a3-proxy-go`

Presto Edge

1. Visão Geral

O **Presto Edge** é um componente do ecossistema Presto que resolve um problema crítico de acesso: alguns tribunais e sistemas jurídicos validam o IP de origem da requisição de login, exigindo que ele seja o mesmo da rede do usuário ou do escritório.

Ao instalar o Presto Edge na máquina do colaborador (ou em um servidor da rede do escritório), o Presto consegue rotear o tráfego pelo IP correto, garantindo que o acesso ao tribunal ocorra com o **mesmo endereço IP do usuário**.

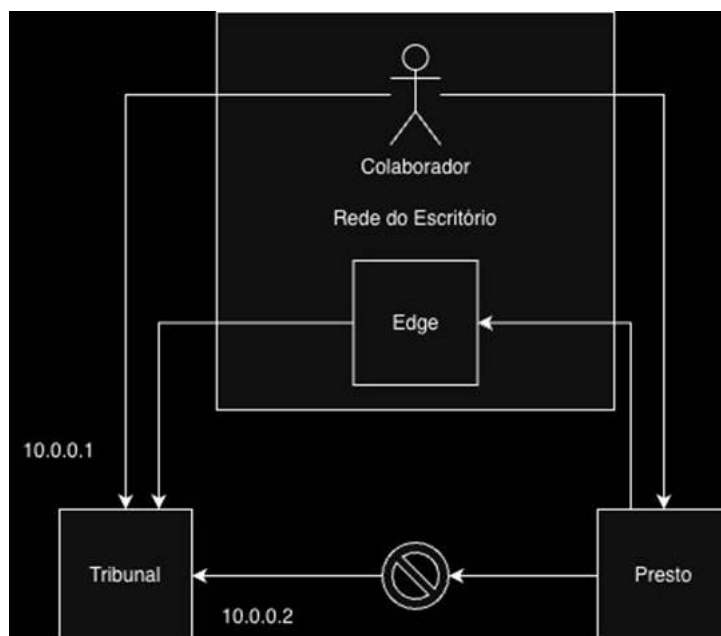


Figura 1 — Arquitetura do Presto Edge : roteamento pelo IP do colaborador

Importante: Como o Presto Edge roda na mesma máquina (ou na mesma rede) do usuário, o Presto acessa o tribunal com o mesmo IP do colaborador. Isso funciona tanto no escritório quanto em home office, pois o Presto Edge acompanha a conexão do usuário.

2. Pré-Requisitos

Antes de instalar o Presto Edge , certifique-se de que os seguintes requisitos estão atendidos:

Requisito	Detalhe
Sistema Operacional	Windows 10 ou superior, macOS, ou Linux
Virtualização habilitada na BIOS/UEFI	Obrigatório para WSL2 — deve ser verificado e habilitado antes de qualquer instalação
WSL2 com Ubuntu 24.04	Obrigatório para Windows — deve ser instalado antes do Docker Desktop
Docker Desktop	Versão mais recente — instalado como Administrador após o WSL2
Inicialização automática	Docker Desktop configurado para iniciar com o Windows
Permissão de Administrador	Necessária para instalação e configuração do Docker Desktop
Conexão com a Internet	Necessária para download da imagem do container do Presto Edge
Acesso ao Console Presto	Conta com acesso a console.presto.oysttr.com.br para obter o comando de instalação

3. Passo 0 — Verificar e Habilitar a Virtualização (Windows)

O WSL2 e o Docker Desktop dependem do recurso de **virtualização de hardware** da CPU. Antes de iniciar a instalação, é necessário confirmar que este recurso está habilitado no Windows e na BIOS/UEFI da máquina.

Este passo é necessário apenas para Windows. Usuários de macOS e Linux podem pular para a Seção 5.

3.1 Verificar se a Virtualização está Habilitada

Para checar rapidamente se a virtualização já está ativa na máquina:

1. Pressione **Ctrl + Shift + Esc** para abrir o **Gerenciador de Tarefas**.
2. Clique na aba **Desempenho** e selecione **CPU** no painel esquerdo.
3. No painel direito, verifique o campo **Virtualização**: se estiver como **Habilitada**, está tudo certo — pule para a Seção 4.

- Se estiver como **Desabilitada**, siga os passos da Seção 3.2 para habilitar.

Alternativamente, você pode verificar via PowerShell executando o comando:

```
systeminfo | findstr /I "Virtualization"
```

Se o resultado mostrar **A hypervisor has been detected**, a virtualização já está ativa.

3.2 Habilitar a Virtualização pela BIOS/UEFI

Caso a virtualização esteja desabilitada, é necessário acessar a **BIOS/UEFI** da máquina para ativá-la. O processo varia conforme o fabricante:

Fabricante	Tecla de Acesso à BIOS	Onde encontrar a opção
Dell	F2 ou F12	Advanced > CPU Configuration > Virtualization Technology
HP	F10 ou Esc	Advanced > System Options > Virtualization Technology (VTx)
Lenovo	F1, F2 ou Delete	Security > Virtualization ou Advanced > CPU Setup
ASUS	Delete ou F2	Advanced > CPU Configuration > Intel Virtualization Technology
Acer	F2 ou Delete	Main > Virtualization Technology
MSI	Delete	OC > CPU Features > Intel Virtualization Tech

Atenção: A tecla de acesso à BIOS deve ser pressionada imediatamente ao ligar o computador, antes do Windows começar a carregar. O nome exato da opção pode variar mesmo entre modelos do mesmo fabricante.

3.3 Passo a passo para acessar a BIOS/UEFI

5. **Reinicie o computador.**
6. Pressione repetidamente a **tecla de acesso à BIOS** do seu fabricante (consulte a tabela acima) assim que a tela do fabricante aparecer.
7. Dentro da BIOS, navegue até a seção de **Advanced, CPU Configuration** ou equivalente.
8. Localize a opção **Virtualization Technology, Intel VT-x, AMD-V** ou similar.
9. Altere o valor para **Enabled**.
10. **Salve as alterações** (geralmente **F10**) e reinicie o computador.

3.4 Habilitar Virtualização pelo Windows (Plataforma de Máquina Virtual)

Além da BIOS, é necessário garantir que o recurso **Plataforma de Máquina Virtual** esteja ativado no próprio Windows:

11. Pressione **Win + R**, digite **optionalfeatures** e pressione Enter.
12. Na janela **Recursos do Windows**, localize e marque as seguintes opções:
 - **Plataforma de Máquina Virtual** (Virtual Machine Platform)
 - **Subsistema do Windows para Linux** (Windows Subsystem for Linux)
13. Clique em **OK** e aguarde a instalação. Reinicie o computador quando solicitado.

Dica: Se ao tentar instalar o WSL você receber um erro como 'WSL 2 requires an update to its kernel component' ou '0x80370102', é sinal de que a virtualização ainda está desabilitada na BIOS ou que o recurso Plataforma de Máquina Virtual não foi ativado.

4. Passo 1 — Instalar o Ubuntu 24.04 via WSL (Windows)

O Presto Edge roda dentro de um container Docker que utiliza o **WSL2 (Windows Subsystem for Linux)** como base. Por isso, antes de instalar o Docker Desktop, é necessário instalar o **Ubuntu 24.04 via WSL** no Windows.

Este passo é necessário apenas para Windows. Usuários de macOS e Linux podem pular para a Seção 4.

3.1 Como instalar o Ubuntu 24.04 via WSL

14. Abra o **PowerShell como Administrador** (clique com o botão direito no menu Iniciar > Windows PowerShell (Admin)).
15. Execute o comando abaixo para instalar o WSL com Ubuntu 24.04:

```
wsl --install -d Ubuntu-24.04
```

16. Aguarde o download e a instalação. O sistema poderá solicitar uma **reinicialização**.
17. Após reiniciar, o Ubuntu abrirá automaticamente — defina um **nome de usuário** e **senha** quando solicitado.
18. Para verificar se a instalação foi bem-sucedida, execute no PowerShell:

```
wsl --list --verbose
```

O Ubuntu-24.04 deve aparecer na lista com status **Running** e versão **2**.

Para um passo a passo visual completo, assista: [Instalação do Ubuntu 24.04 via WSL no Windows \(YouTube\)](#)

5. Passo 2 — Instalar o Docker Desktop

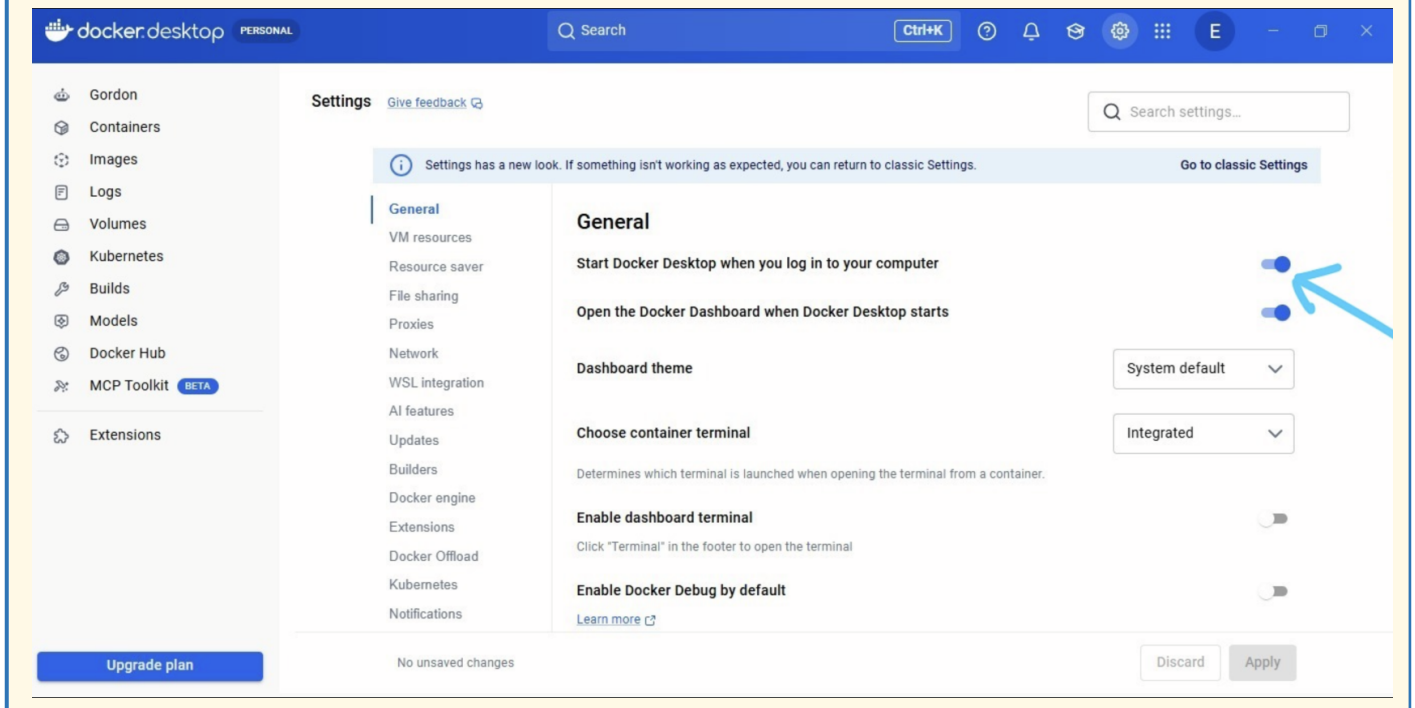
Com o WSL2 e o Ubuntu 24.04 instalados, o próximo passo é instalar o **Docker Desktop**. O Presto Edge é um container Docker e o Docker Desktop é o ambiente que o executa no Windows.

4.1 Download e Instalação

19. Acesse o site oficial: <https://docs.docker.com/desktop/setup/install/windows-install/>
20. **Execute o instalador como Administrador** (clique com o botão direito > Executar como Administrador).
21. Durante a instalação, **mantenha marcada a opção** de iniciar o Docker Desktop ao iniciar o Windows.
22. Ao final, abra o Docker Desktop > **Settings** > **General** e confirme que **Use the WSL 2 based engine** está ativado.

23. Verifique se o ícone do Docker aparece na barra de tarefas com status **Engine running**.

Atenção: O Docker Desktop deve ser instalado obrigatoriamente como Administrador. Caso contrário, o container do Presto Edge não conseguirá iniciar corretamente. É importante também que o Docker esteja configurado para iniciar junto com o Windows como na imagem abaixo:



Para um passo a passo visual completo, assista: [Instalação do Docker Desktop no Windows \(YouTube\)](#)

6. Passo 3 — Obter o Comando no Console Presto

O comando para iniciar o container do Presto Edge é **personalizado por usuário/máquina** e deve ser obtido diretamente no Console do Presto. Cada proxy possui um identificador único (**EDGE_NAME**) que vincula o container ao usuário correto.

5.1 Acessando a lista de Proxies

24. Acesse console.presto.oysttr.com.br/proxies e faça login com sua conta Presto.

25. Na tela de **Proxies**, localize o proxy correspondente à sua máquina ou usuário.

26. Se não existir um proxy cadastrado para você, clique em **Adicionar novo proxy** para criar um.

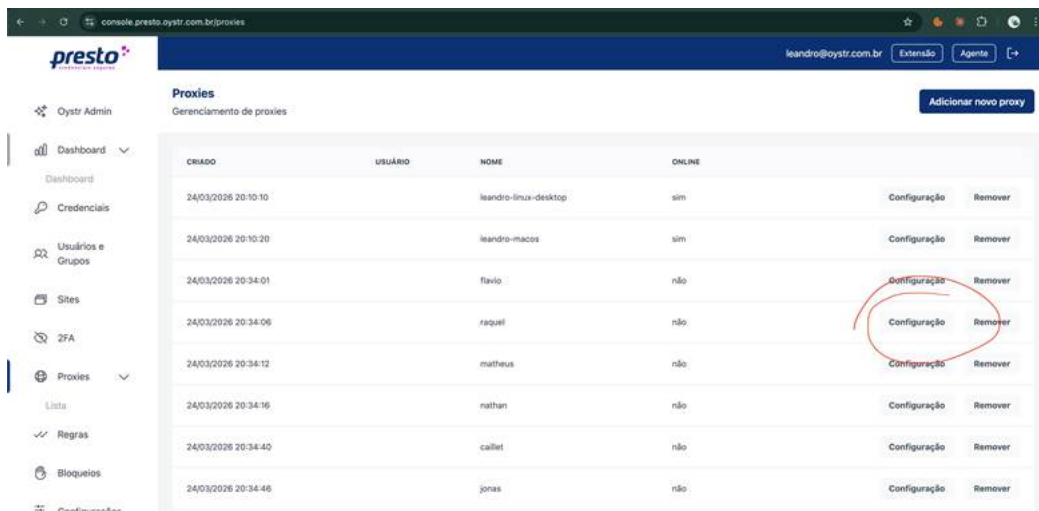


Figura 2 — Tela de listagem de Proxies no Console Presto

5.2 Copiando o Comando Docker

27. Clique no botão **Configuração** ao lado do proxy desejado.
28. No painel **Detalhes do proxy**, localize o campo **Config** — ele contém o comando Docker completo e personalizado para aquele proxy.
29. Clique em **copiar** para copiar o comando para a área de transferência.

7. Passo 4 — Executar o Comando no Terminal Ubuntu

Com o comando copiado do Console, execute-o no terminal do **Ubuntu (WSL)** para iniciar o container do Presto Edge.

6.1 Abrindo o Terminal Ubuntu

30. Pressione **Win + S** e pesquise por Ubuntu.
31. Abra o aplicativo **Ubuntu 24.04** instalado via WSL.
32. Cole o comando copiado do Console e pressione **Enter**.

6.2 Verificando se o Container Subiu

33. Abra o **Docker Desktop**.
34. Clique em **Containers** no menu lateral esquerdo.
35. Localize o container **presto-edge** — o indicador deve estar **verde**, indicando que está ativo.



Figura 4 — Painel de Containers do Docker Desktop com o presto-edge ativo

8. Gerenciamento do Presto Edge via Docker Desktop

Após a instalação, é possível monitorar e gerenciar o Presto Edge diretamente pelo Docker Desktop.

7.1 Visualizando Logs e Status

Clique no nome do container **presto-edge** para acessar a tela de detalhes. Nesta tela é possível:

- Visualizar os **logs em tempo real** do Edge
- Verificar o **status da conexão** com a infraestrutura Presto
- Identificar eventuais erros de conectividade (exibidos em amarelo nos logs)

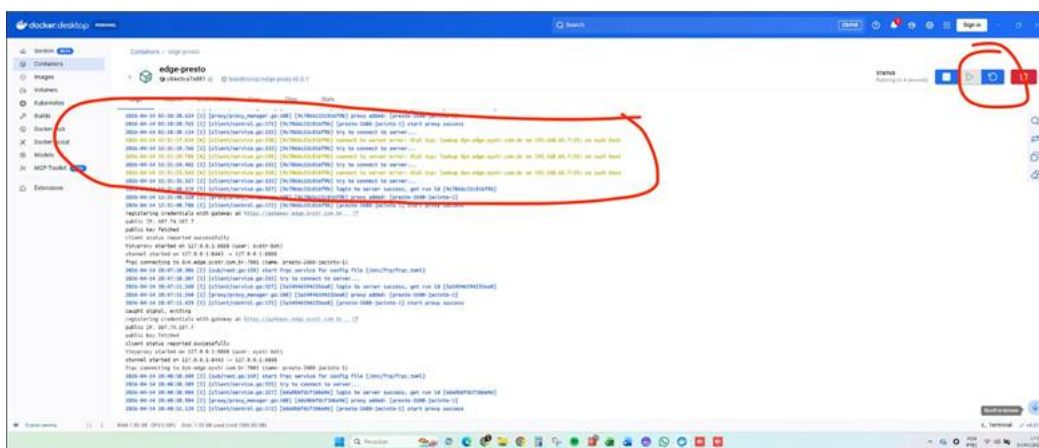


Figura 5 — Tela de logs do container *presto-edge* no Docker Desktop

Dica: Linhas de log em amarelo indicam dificuldade de conexão com a infraestrutura. Neste caso, utilize o botão de restart (destacado na imagem) para reconectar.

7.2 Reiniciando o Container

Caso o Presto Edge apresente falhas de conexão, o primeiro passo é reiniciá-lo:

36. Acesse a tela de detalhes do container **presto-edge** no Docker Desktop.
37. Clique no **botão de Restart** (ícone circular com seta) no canto superior direito da tela.
38. Aguarde alguns segundos e observe os logs — o Presto Edge deverá reconectar à infra automaticamente.
39. Após reconectar, teste a conexão usando o botão **Testar VPN** na extensão do Presto.

9. Botão Testar VPN

O botão **Testar VPN** está disponível no diálogo de login da extensão do Presto e serve para validar a configuração do proxy antes de realizar o login no tribunal.



Figura 6 — Diálogo de login da extensão Presto com o botão Testar VPN

8.1 O que é testado

Ao clicar em **Testar VPN**, o sistema valida automaticamente os seguintes pontos:

40. **Configuração:** Verifica se o Presto Edge (ou VPN) está instalado e configurado na máquina do usuário.
41. **Funcionamento:** Confirma se o Presto Edge/VPN tem acesso ativo à internet.
42. **Equivalência de IP:** Verifica se o IP do Presto Edge/VPN é o mesmo IP do usuário.

Nota: A igualdade de IP é exigida apenas em alguns tribunais. Na maioria dos casos, o Presto funciona mesmo que os IPs sejam diferentes.

8.2 Resultado do Teste

Quando os 3 testes passam, o botão fica com indicação visual de sucesso. Se o IP for diferente, o botão sinaliza a divergência — mas isso não impede o funcionamento do Presto na maioria dos tribunais.

Quando o cliente **não possui VPN ou Presto Edge configurado**, o tráfego cai na VPN/Proxy compartilhada da Oystre (IP: 177.220.183.60). Neste caso, se houver dificuldade de acesso, recomenda-se adotar uma das soluções descritas na seção 10.

10. Cenários de Implantação Recomendados

A instalação do Presto Edge pode ser feita de diferentes formas dependendo do tamanho e perfil do cliente. A tabela abaixo resume as recomendações:

Perfil do Cliente	Recomendação	Observação
Clientes menores	Presto Edge instalado em todos os computadores dos usuários do Presto	Solução mais simples e robusta para equipes pequenas
Clientes maiores	Container/VPN centralizado + Presto Edge nas máquinas dos colaboradores	Garante redundância e continuidade mesmo com oscilações
Clientes corajosos	1 ou mais Presto Edges em máquinas fixas do escritório	Funciona apenas se a máquina com o Edge estiver ligada e com o mesmo IP do usuário

7.1 Presto Edge por Colaborador vs. Presto Edge Centralizado

Uma dúvida comum é se basta instalar **1 único Presto Edge** para toda a empresa ou se é necessário **1 Presto Edge por colaborador**. Veja as considerações a seguir:

- **O Presto busca automaticamente qualquer Presto Edge** associado à conta do usuário que esteja com o mesmo IP.
- Se **ao menos 1 Presto Edge** for encontrado com o IP correto, o acesso funciona.
- Um **Presto Edge** centralizado **não funciona em home office** (sem VPN), pois o IP do colaborador será diferente do IP do Edge.
- Depender de **apenas 1 Presto Edge centralizado é arriscado** — oscilações de conexão entre o **Presto Edge** e a infraestrutura podem interromper o serviço.
- O **cenário ideal** é 1 **Presto Edge** instalado em cada máquina de colaborador que usa o Presto.

11. Opções para Resolver Problemas de IP

Quando um usuário apresenta dificuldade de acesso por divergência de IP, existem **3 opções** para resolver o problema:

- 43. **Configuração de VPN dedicada** com a Oystr — recomendado para clientes maiores que necessitam de um IP fixo e estável.
- 44. **Container Docker centralizado** — implantação de um container **Presto** Edge em servidor centralizado da empresa, conectado à infraestrutura da Oystr.
- 45. **Instalação do Presto Edge** na máquina do colaborador — solução mais prática e indicada para a maioria dos cenários.

12. Solução de Problemas (Troubleshooting)

Problema	Causa Provável	Solução
Presto Edge não aparece na lista de containers	Docker Desktop não foi iniciado	Abra o Docker Desktop e aguarde o status "Engine running"
Logs exibem linhas em amarelo	Falha de conexão com a infraestrutura Presto	Clique no botão Restart do container no Docker Desktop
Botão "Testar VPN" indica IP diferente	Usuário em home office sem Presto Edge instalado localmente	Instalar o Presto Edge na máquina do colaborador ou configurar VPN
Container para após reiniciar o PC	Parâmetro --restart always não foi usado na criação	Recrie o container com o parâmetro --restart always
Presto Edge instalado mas login no tribunal falha	Tribunal exige IP específico e o Presto Edge não está naquela rede	Verificar junto ao suporte Oystr a necessidade de VPN dedicada

13. Suporte

Em caso de dúvidas ou problemas não resolvidos pelo troubleshooting acima, entre em contato com a equipe de suporte Presto/Oystr para verificação dos logs e avaliação da melhor estratégia de implantação para o seu ambiente.

Este documento é de uso interno e deve ser compartilhado com os responsáveis técnicos de TI do cliente para realização da instalação.

VPN

Acesso aos Portais via Presto com VPN

Configurar uma VPN para usar o Presto é necessário devido à maneira como alguns portais funcionam. Esses portais realizam duas verificações principais: se o IP é nacional e se o IP que iniciou a sessão é o mesmo que continua acessando o site.

Para que o Presto funcione corretamente nesses portais, o IP dele precisa ser o mesmo do usuário final. A solução é o usuário do Presto configurar um **Servidor de VPN** e fornecer as configurações de acesso **client para o Presto**. Assim, o Presto acessa os portais usando o IP do usuário via VPN. Sendo assim, é necessário uma configuração *Client/Server*. *Obs: Não é possível uma configuração site to site.*

A configuração da VPN para uso do Presto é altamente recomendada e garante que o acesso aos sites e portais seja feito de forma transparente, como se fosse um usuário acessando manualmente.

Por enquanto, apenas o Open VPN (v2.5) são suportados.

Hosts liberados:

- cloudflare.com:443
- https://api.ipify.org

Demais configurações:

- Os IPs que vão se conectar a VPN estão fora do Brasil e precisam ser liberados
- Todo o tráfego http/https deve ser roteado pela VPN
- O cliente de VPN deve aceitar conexões externas

Informação Importante:

Em casos onde o login via Presto apresenta falhas intermitentes, é importante verificar se há inconsistência entre a rede utilizada pelo Presto e a rede em que os usuários estão conectados. Quando o Presto acessa a internet por uma rede diferente da dos usuários, a funcionalidade do proxy pode ser comprometida, resultando em falhas de autenticação para alguns usuários. A recomendação é alinhar o ambiente de rede, colocando todos os usuários na mesma VPN utilizada pelo Presto ou, alternativamente, ajustando as configurações de rede para garantir que o tráfego passe adequadamente pelo proxy. Em situações semelhantes, entre em contato com a equipe de TI local para definir o melhor ajuste.

Proxy autenticado

Alguns clientes da Oystre têm preferido configurar um proxy autenticado em vez de utilizar uma VPN. Essa abordagem permite que nossos robôs do Presto se conectem à infraestrutura do cliente de forma segura e eficiente.

Passo a Passo para Configuração do Proxy

1. Rodar o container com o proxy

O cliente deve rodar o seguinte comando em sua máquina, utilizando nosso container pré-configurado:

```
docker run --name proxy -v /opt/oyster:/opt/oyster/ -p 8888:8888 -d leandrocruz/oyster-tinyproxy:v1.0.0
```

Esse comando irá:

- Criar e rodar um container chamado `proxy`;
- Mapear a pasta local `/opt/oyster` para dentro do container;
- Expor a porta `8888` para acesso externo.

2. Criar o arquivo de configuração

Na pasta local `/opt/oyster` o cliente deve criar um arquivo chamado `tinyproxy.cfg` com o seguinte conteúdo:

```
Port 8888
Listen 0.0.0.0
Timeout 600
DisableViaHeader Yes
BasicAuth oyster-bot SENHA
```

O container roda um proxy http autenticado na porta 8888

Importante:

- **SENHA** deve ser substituída pela senha de autenticação que o cliente deverá criar e nos informar para ser usado pela nossa solução para autenticar os robôs na infraestrutura do cliente.
- A configuração define que o proxy ficará escutando na porta 8888 em todas as interfaces de rede (0.0.0.0).

3. Garantir o acesso externo

A porta **8888** precisa estar publicamente acessível na infraestrutura do cliente, para que os robôs do Presto consigam se conectar ao proxy.

4. Testar o funcionamento do proxy

Após a configuração, o cliente deve executar o seguinte comando para verificar se o proxy está funcionando corretamente:

```
curl --proxy http://oystre-bot:SENHA@IP:8888 http://ipinfo.io
```

Substitua:

- **SENHA** pela senha de autenticação fornecida;
- **IP** pelo endereço IP público ou interno da máquina onde o proxy foi configurado (ou do gateway).

Se o comando retornar um **JSON com as informações do IP da infraestrutura do cliente**, significa que o proxy está configurado corretamente.

☐ Exemplo de retorno esperado:

```
{  
  "city": "São Paulo",  
  "country": "BR",  
  "hostname": "customer.splobra1.pop.starlinkisp.net",  
  "ip": "216.234.208.75",  
  "loc": "-23.5475,-46.6361",  
  "org": "AS14593 Space Exploration Technologies Corporation",  
  "postal": "01000-000",  
  "readme": "https://ipinfo.io/missingauth",  
  "region": "São Paulo",  
  "timezone": "America/Sao_Paulo"  
}
```

⚠ Importante

Enquanto esse teste não for bem-sucedido, os **robôs do Presto não conseguirão utilizar o proxy do cliente**.

Suporte

Em caso de dúvidas ou dificuldades durante a configuração, entre em contato com nosso time de suporte técnico.

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 Oyster** (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 Oyster.

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 Oyster** (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 Oyster**. 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 Oyster**.

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 <code>8888</code> 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 Oystre, 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 Oystre. 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 Oystre 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 Oystre tiver instabilidade no futuro, eu serei afetado? Clientes com configuração própria não dependem do IP compartilhado da Oystre, 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.