

Guia do administrador para Isolamento remoto do navegador

0.0

Contact Information

Corporate Headquarters:

Palo Alto Networks

3000 Tannery Way

Santa Clara, CA 95054

www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Palo Alto Networks, Inc.

www.paloaltonetworks.com

© 2023-2025 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

January 31, 2025

Table of Contents

Isolamento remoto do navegador.....	5
Remote Browser Isolation na China.....	9
Como o Remote Browser Isolation funciona.....	11
Comportamento do navegador de isolamento.....	13
Tipos de arquivo suportados para exibir arquivos isoladamente.....	14
Configurar o Remote Browser Isolation.....	15
Integrar a um provedor de desarme e reconstrução de conteúdo de terceiros.....	41
Integrar o RBI ao Votiro.....	42
Experiência de navegação isolada.....	45
Banner de isolamento.....	46
Relatar um problema.....	47
Controle de segurança do navegador.....	48
Análise dos arquivos baixados.....	49
Experiência de navegação móvel.....	50
Monitorar o Remote Browser Isolation.....	53
Painel de integridade do SASE.....	54
Monitorar usuários do RBI.....	55
Monitorar localizações do Prisma Access com RBI.....	59
Detalhes do usuário do RBI.....	61
Monitorar o consumo de licenças do RBI.....	64
Logs do Remote Browser Isolation.....	65

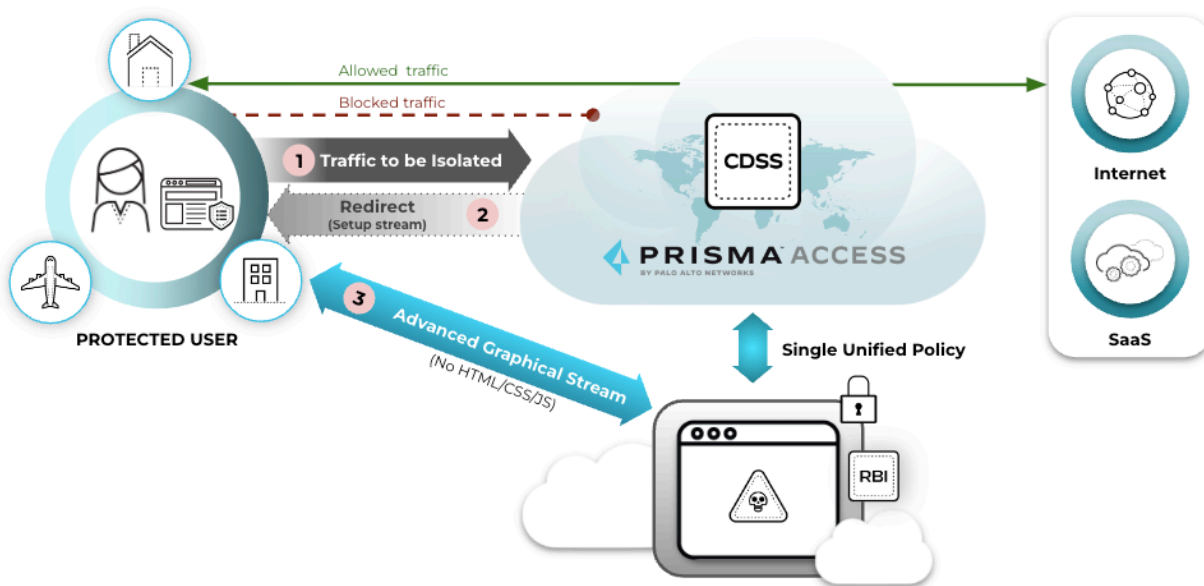
Isolamento remoto do navegador

Onde posso usar isso?	O que eu preciso?
<ul style="list-style-type: none"> Prisma Access (Managed by Panorama or Strata Cloud Manager) 	<ul style="list-style-type: none"> Prisma Access 5.0 Innovation Licença do Prisma Access com a assinatura de licença de Usuário móvel ou Redes remotas Licença de isolamento remoto do navegador

Os ataques baseados em navegadores e na Web estão em constante evolução, resultando em desafios de segurança para muitas empresas. Os navegadores da Web são um dos principais pontos de entrada de malware nas redes, representando um grande risco de segurança para as empresas. Isso reforça a importância de proteger redes e dispositivos contra ataques de dia zero. Setores altamente regulamentados, como instituições governamentais e financeiras, também exigem o isolamento do tráfego do navegador como um requisito de conformidade.

Embora a maioria das empresas deseje bloquear 100% dos ataques usando métodos de segurança de rede e segurança de endpoint, esse objetivo pode não ser realista. A maioria dos ataques começa com a exploração de um endpoint que acessa sites maliciosos ou comprometidos, ou ao abrir conteúdos maliciosos desses sites. Um invasor só precisa de uma falha para assumir um endpoint e comprometer a rede. Quando isso acontece, as consequências desse comprometimento e o impacto para sua organização podem ser desastrosos.

O Remote Browser Isolation (RBI) isola a execução de sites no navegador local do usuário, impedindo que códigos ou arquivos do site sejam processados diretamente no dispositivo. Ao contrário de outras soluções de isolamento, o RBI usa tecnologias de isolamento de última geração para oferecer experiências quase nativas para usuários que acessam sites sem comprometer a segurança.



O RBI é um serviço que isola e transfere toda a atividade de navegação dos dispositivos gerenciados e redes corporativas do usuário para uma entidade externa, como o Prisma Access. A entidade externa protege e isola o código e o conteúdo potencialmente malicioso em sua plataforma e separa quaisquer ameaças das conexões diretas com os dispositivos e redes do usuário final.

Integrado nativamente ao Prisma Access, o RBI permite que você aplique perfis de isolamento com facilidade às políticas de segurança existentes. Os perfis de isolamento podem restringir muitos controles do usuário, como ações de copiar e colar, entradas do teclado e opções como carregar, baixar e imprimir arquivos para manter dados e informações confidenciais seguros. Todo o tráfego isolado passa por análise e prevenção de ameaças através de serviços de segurança adicionais fornecidos na nuvem (CDSS), como Prevenção avançada contra ameaças, WildFire avançado, Filtragem avançada de URL, Segurança de DNS e Segurança de SaaS.

Você e seus usuários podem se beneficiar dos seguintes recursos:

- **Experiência de navegação quase nativa:** quando os usuários navegam de forma isolada, os sites são carregados em um ambiente protegido que parece ter sido acessado diretamente de um navegador da Web local, incluindo todas as tecnologias da Web compatíveis com um navegador padrão. Isso permite que você e seus usuários acessem sites da Internet de forma isolada, sem sacrificar a funcionalidade ou o desempenho do navegador da Web.

O RBI é compatível a maioria das tecnologias da Web, incluindo JavaScript, frameworks modernos, HTML5, protocolo HTTP e suporte a mídia avançada, como vídeo, áudio e GIFs animados. Os URLs mostrados no navegador remoto terão a mesma aparência dos URLs nativos originais, sem prefixos adicionados aos endereços.

- **Orientado por políticas de segurança:** você pode especificar categorias de URL cujo conteúdo do site você deseja redirecionar para o RBI usando perfis de isolamento, que você anexa a regras de política de segurança do Prisma Access que protegem seus usuários. Você também pode criar perfis de isolamento que controlam quais ações do navegador são permitidas durante a navegação isolada. O RBI é integrado ao Prisma Access para que você possa aplicar serviços adicionais de segurança da Internet ao tráfego de sessões de navegação isoladas.

Em combinação com o Prisma Access, o RBI fornece os seguintes benefícios de segurança:

- Sessões isoladas, cookies e dados do usuário
- Visualizações seguras de documentos, como PDFs
- Proteção contra phishing de credenciais (fornecida pela desativação do teclado em um perfil de isolamento)
- Serviços de segurança fornecidos na nuvem, como:
 - Prevenção de XSS
 - Filtragem avançada de URL
 - Proteção avançada contra ameaças
 - WildFire avançado
 - Segurança integrada de SaaS (fornecida pela Segurança de SaaS)
 - Segurança de DNS

Como resultado, o RBI pode ajudar a impedir que seus usuários comprometam informações corporativas ou pessoais em dispositivos gerenciados enquanto acessam a Internet. Isso

também inclui a prevenção contra perda de dados (DLP) de dados confidenciais ou críticos ao acessar aplicativos da Web ou a Internet.

- **Integração e configuração simples:** os usuários gerenciados que foram integrados ao Prisma Access usando conexões de GlobalProtect, Proxy explícito ou Redes remotas podem navegar isoladamente. Nenhuma etapa de autenticação extra é necessária para RBI.

Como o RBI está em conformidade com a estrutura de políticas de segurança existente do Prisma Access, você pode integrar e configurar facilmente o RBI para seus usuários finais. Isso reduz a sobrecarga, pois você pode configurar facilmente perfis de isolamento e anexá-los às regras de segurança existentes.

- **Monitoramento e solução de problemas:** usando a interface de gerenciamento do Strata Cloud Manager ou do Panorama Managed Prisma Access, você pode monitorar a integridade da implantação do RBI, os resultados de segurança alcançados e problemas de experiência do usuário sem precisar usar várias ferramentas de gerenciamento. Você pode monitorar a integridade da implantação do RBI (como informações de uso, integridade e licença do RBI) e solucionar problemas comuns do usuário final.

Remote Browser Isolation na China

Onde posso usar isso?	O que eu preciso?
<ul style="list-style-type: none"> Prisma Access (Managed by Strata Cloud Manager) 	<ul style="list-style-type: none"> Licença Prisma Access China 5.2.0 com a assinatura de licença de Usuário móvel ou Redes remotas Versão mínima do Prisma Access plano de dados: 11.2.3 Licença de isolamento remoto do navegador

O Remote Browser Isolation (RBI) estende seu serviço e infraestrutura associada dentro dos limites geográficos da China. As empresas na China podem se beneficiar da solução totalmente integrada de RBI e Prisma Access para manter malware, incluindo ataques de dia zero resultantes da navegação e da atividade na Web, longe dos dispositivos gerenciados dos usuários e da rede.

O RBI China é suportado no [Prisma Access na China](#) (Aplicam-se limitações e condições do Prisma Access China). Os locatários habilitados para RBI na China são separados dos locatários do resto do mundo e suportam apenas o tráfego dos métodos de conexão compatíveis do Prisma Access (Usuário móvel, Proxy explícito e Redes remotas).

Os recursos disponíveis no RBI China são os mesmos que os [recursos do RBI](#) para o resto do mundo. No entanto, observe as seguintes diferenças:

- Você pode integrar o RBI China apenas em locatários do Strata Cloud Manager Managed Prisma Access localizados na China. Os locatários podem ser novos ou existentes.
- Você não pode usar localizações do RBI China com locatários do Prisma Access hospedados no resto do mundo. Para usar localizações do RBI China, você terá que gerenciar um locatário separado. Veja [Prisma Access na China](#) para obter a lista de diferenças entre o Prisma Access e o Prisma Access China.
- O RBI China permite que o tráfego local seja direcionado localmente e que o tráfego internacional passe por linhas de locação transfronteiriças para contornar o sistema de censura da Internet da China, por meio da Conexão de serviço.
- As comunicações entre os componentes do RBI implantados na China com os componentes fora da China (como ativação de licença, Strata Cloud Manager etc.) passarão por uma ponte segura com uma raiz de confiança separada.
- Não há suporte para integrações autônomas de DEM, Visibilidade e insights e AIOps.
- Não há suporte a fallback de redes remotas em alta disponibilidade.

As seguintes considerações de licenciamento e ativação se aplicam:

- Você pode ativar os SKUs do Prisma Access China com o SKU do RBI ao selecionar o SKU do RBI.

- O RBI China usa os mesmos SKUs e preços que o resto do mundo.
- Ative o RBI China apenas em locatários do Prisma Access localizado na China.

Todos os locais de computação e borda do Prisma Access China permitem a localização de sessões do RBI.

Para usuários do RBI, as seguintes condições do Prisma Access se aplicam:

- Quando um usuário de dispositivo gerenciado visita a China, ele não pode usar o RBI na China, a menos que se conecte a um locatário do Prisma Access China. Se o sistema de censura da Internet da China permitir, ele ainda poderá acessar suas respectivas instâncias do RBI, embora a latência possa ser alta.
- Da mesma forma, se um usuário do RBI China viajar para fora da China, ele não poderá usar o RBI para o resto do mundo, a menos que se conecte a um locatário do Prisma Access hospedado fora da China.

Para começar, certifique-se de que você [configurou uma implantação do Prisma Access China](#). Em seguida, siga as instruções para [configurar o RBI](#). Os procedimentos que você usa para integrar o RBI na China são os mesmos usados para integrar o RBI em outros locais ao redor do mundo.

Como o Remote Browser Isolation funciona

Onde posso usar isso?	O que eu preciso?
<ul style="list-style-type: none"> Prisma Access (Managed by Panorama or Strata Cloud Manager) 	<ul style="list-style-type: none"> Prisma Access 5.0 Innovation Licença do Prisma Access com a assinatura de licença de Usuário móvel ou Redes remotas Licença de isolamento remoto do navegador

O Remote Browser Isolation (RBI) protege os usuários gerenciados por meio do isolamento, garantindo que os sites sejam carregados em um ambiente protegido e isolado e que nenhum código mal-intencionado seja executado no navegador em seus dispositivos gerenciados.

Você pode proteger a experiência de navegação dos usuários seguindo as seguintes etapas durante a integração do Remote Browser Isolation:

- [Crie perfis de isolamento](#) que determinem quais ações do navegador um usuário tem permissão para realizar durante uma sessão de navegação isolada. Por exemplo, você pode impedir que o usuário copie, baixe e imprima qualquer coisa de um site isolado. Dessa forma, você pode minimizar a perda potencial de dados quando os usuários tentam copiar, baixar ou imprimir dados confidenciais de sites isolados.
- Crie ou atualize um perfil de gerenciamento de acesso ao URL e anexe o perfil de isolamento a ele. No perfil de gerenciamento de acesso ao URL, você pode configurar o controle de acesso para categorias específicas de sites que passam por isolamento durante a navegação e associar um perfil de isolamento que define as ações permitidas do navegador para os sites nessas categorias.
- Configure serviços de segurança adicionais fornecidos na nuvem, como Prevenção avançada contra ameaças, WildFire avançado, Filtragem avançada de URL, Segurança de DNS e Segurança de SaaS, e aplique-os ao tráfego de sessões de navegação isoladas.

O RBI está disponível nas seguintes [localizações](#) do Prisma Access:

- Sudeste da Austrália (Sydney)
- Bélgica
- Finlândia
- Sul da Índia
- Japão
- Cingapura
- Taiwan
- Centro dos EUA (Chicago)
- Leste dos EUA

- Oeste dos EUA

Os usuários podem se conectar ao Prisma Access usando [Usuários móveis do Prisma Access](#) ou [Redes remotas do Prisma Access](#).

Comportamento do navegador de isolamento

Quando os usuários em dispositivos gerenciados se conectam ao Prisma Access usando o método de conexão Usuários móveis ou Redes remotas, eles podem navegar em um site isoladamente se o site pertencer a uma categoria de URL que você designou para isolamento.

Seus usuários gerenciados em computadores e dispositivos móveis compatíveis podem usar os seguintes navegadores da Web de 64 bits para navegação isolada. A: indica que a combinação de sistema operacional e navegador não é compatível.

Sistema operacional	Firefox	Google Chrome	Microsoft Edge	Safari
Android	—	✓	—	—
iOS	—	✓	—	✓
iPadOS	—	—	—	✓
macOS	✓	✓	✓	✓
Windows	✓	✓	✓	—

Os URLs mostrados no navegador remoto terão a mesma aparência dos URLs originais, sem prefixos adicionados aos endereços. Quando um usuário tenta executar ações do navegador que você proibiu, o RBI notifica-os com notificações pop-up.

Se o usuário acessar um link em um site não isolado, o URL do link será comparado com as políticas de segurança de isolamento para o método de conexão (GlobalProtect, Explicit Proxy ou Remote Networks). Quando há uma correspondência de política, a sessão do navegador é isolada.

Quando os usuários encontram problemas durante a navegação isolada, eles podem relatar o problema no navegador isolado.

Você pode aplicar qualquer perfil de segurança no Prisma Access para o tráfego de RBI para os sites de destino.

Para obter informações sobre a experiência de navegação em computadores e dispositivos móveis, consulte [Experiência de navegação isolada](#) e [Experiência de navegação móvel](#).

Tipos de arquivo suportados para exibir arquivos isoladamente

Os seguintes tipos de arquivo são suportados para exibição em sessões de navegação isoladas:

- Microsoft Word (.doc, .docm, .docx)
- Microsoft Excel (.xls, .xlsb, .xlsx)
- Microsoft PowerPoint (.ppt, .pptm, .pptx)
- PDFs da Adobe

Os seguintes tipos de arquivo não são suportados para exibição no RBI:

- Texto do OpenOffice (.odt)
- Planilha do OpenOffice (.ods)
- Apresentação do OpenOffice (.odp)
- Ichitaro (.jtd)
- Visio (.vsd, .vsdx)
- Formato Rich Text (.rtf)
- CSV
- Texto (.txt)

Configurar o Remote Browser Isolation

Onde posso usar isso?	O que eu preciso?
<ul style="list-style-type: none"> Prisma Access (Managed by Panorama or Strata Cloud Manager) 	<ul style="list-style-type: none"> Prisma Access 5.0 Innovation Licença do Prisma Access com a assinatura de licença de Usuário móvel ou Redes remotas Licença de isolamento remoto do navegador

Para integrar seus usuários finais ao RBI, você precisa configurar o RBI usando Strata Cloud Manager Managed Prisma Access ou Panorama Managed Prisma Access e enviar a configuração para os endpoints.

Neste procedimento, você irá:

- Definir as configurações de infraestrutura para RBI que especificam a sessão e o aspecto do navegador durante a navegação isolada
- Configurar perfis de isolamento que definem quais ações do navegador um usuário pode ou não executar
- Usar a estrutura de políticas existente no Prisma Access para definir de forma rápida e fácil os URLs ou sites (incluindo categorias) que um usuário pode acessar usando RBI

As instruções para configurar o RBI em Strata Cloud Manager e Panorama Managed Prisma Access são fornecidas.

- [Strata Cloud Manager](#)
- [Panorama](#)

Configurar o Remote Browser Isolation (Strata Cloud Manager)

Você pode proteger a experiência de navegação dos usuários finais configurando o Remote Browser Isolation (RBI) para isolar o tráfego do navegador.

Configure o RBI concluindo as seguintes etapas:

STEP 1 | Antes de começar a configurar o RBI, certifique-se de:

- Comprar uma licença válida do [Prisma Access](#) com uma assinatura de licença de Usuários móveis ou Redes remotas.
- [Ativar o Strata Cloud Manager Managed Prisma Access](#).
- Comprar e [ativar a licença de Isolamento remoto do navegador](#).
- [Configurar o Strata Cloud Manager Managed Prisma Access](#).
- Configurar pelo menos um método de conexão Prisma Access, como [GlobalProtect](#), [Proxy explícito](#) ou [Redes remotas](#); caso contrário, você não poderá habilitar RBI.
- [Ativar acriptografia](#) para que o Prisma Access possa criptografar e inspecionar o tráfego para determinar o que precisa ser isolado de acordo com as políticas configuradas.

STEP 2 | No Strata Cloud Manager, vá para a página de configuração do Remote Browser Isolation selecionando **Workflows > Prisma Access Setup > Remote Browser Isolation**.



A página de configuração do Remote Browser Isolation está disponível somente se você comprou e ativou a licença do Remote Browser Isolation.

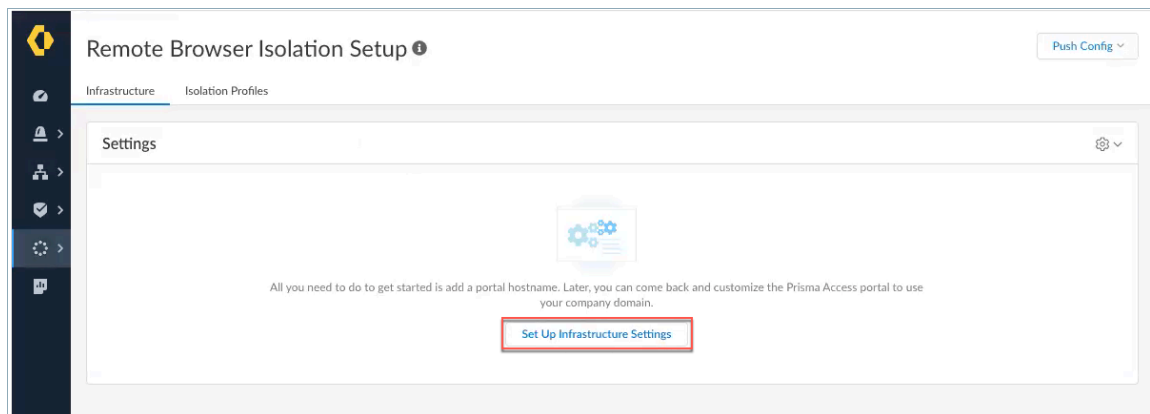
Como alternativa, você pode selecionar **Manage > Configuration > NGFW e Prisma Access > Security Services > URL Access Management**. Em seguida, selecione **Settings** (Configurações), abra as **Third Party Remote Browser Isolation Settings** (Configurações de RBI de terceiros) e clique em **Configure Remote Browser Isolation** (Configurar isolamento remoto do navegador).



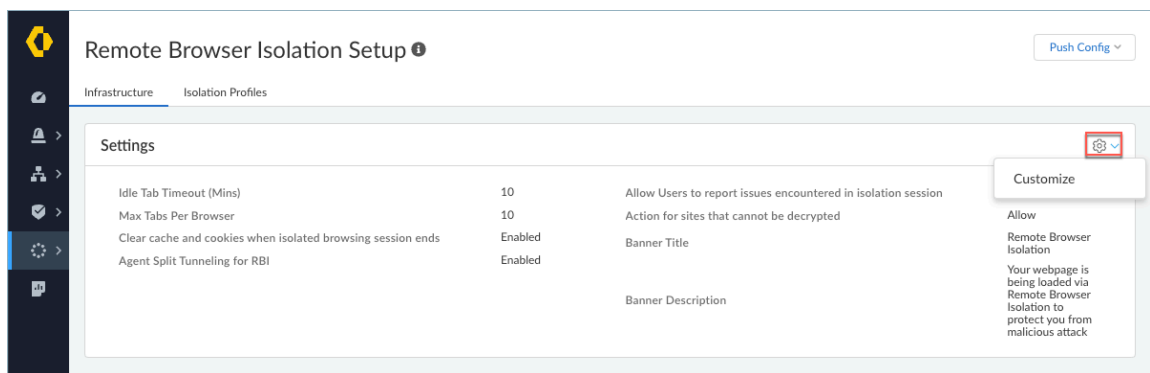
*O botão **Configure Remote Browser Isolation** (Configurar isolamento remoto do navegador) está disponível somente se você comprou e ativou a licença do Remote Browser Isolation.*

STEP 3 | Defina as configurações de infraestrutura do RBI que especificarão o comportamento e o aspecto do navegador durante sessões de navegação isoladas.

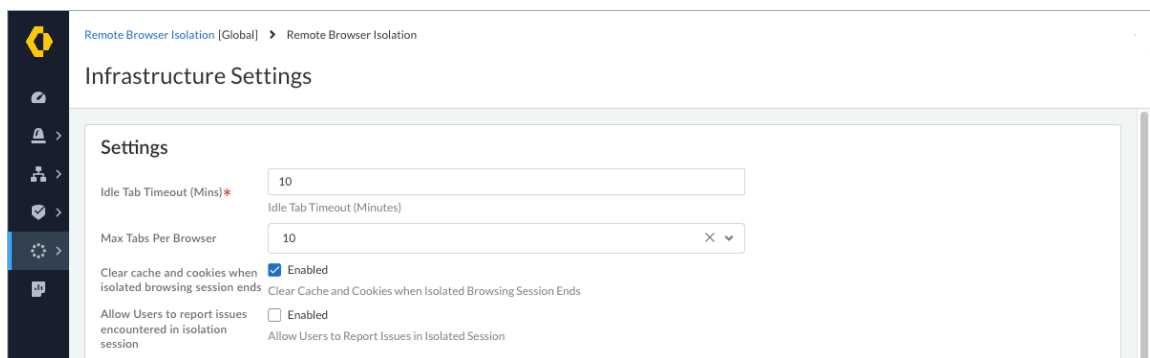
1. Se você estiver configurando o RBI pela primeira vez, selecione **Infrastructure > Set Up Infrastructure Settings** (Definir configurações de infraestrutura).



Caso contrário, edite as **Settings** (Configurações) e selecione **Customize** (Personalizar).



2. Defina o comportamento do navegador durante uma sessão de navegação isolada.



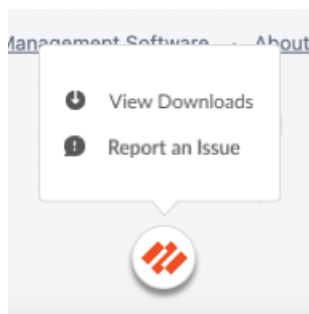
- **Idle Tab Timeout (Mins)** (Tempo limite de guia ociosa [minutos]): defina quanto tempo de inatividade do usuário leva para que uma guia do navegador expire. O valor do tempo limite padrão é de 10 minutos. O intervalo é de 5 a 20 minutos.

O cronômetro de inatividade começa na última ação do usuário, como clicar com o mouse, rolar, navegar, carregar ou baixar arquivos e interromper um vídeo ou áudio. Apenas mover o cursor não é considerado uma atividade.

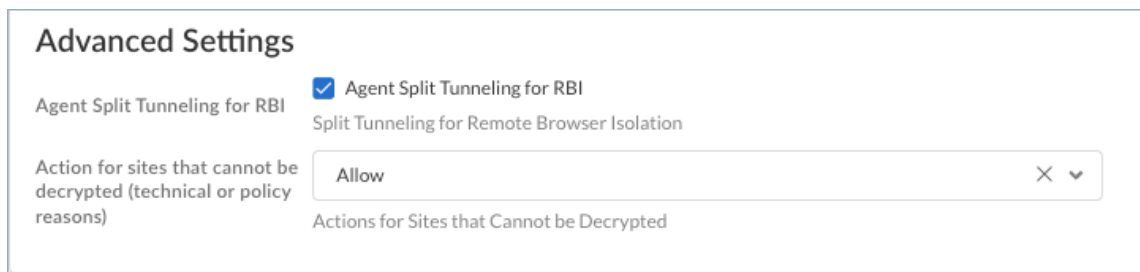
- **Max Tabs Per Browser** (Máximo de guias por navegador): selecione o número máximo de guias que o usuário pode abrir por navegador. Você pode escolher no máximo 5, 10 ou 15 guias. O padrão é 10.

Quando o número de guias exceder o máximo, os usuários serão solicitados a fechar as guias existentes se quiserem abrir mais guias para navegação.

- **Clear cache and cookies when isolated browsing session ends** (Limpar cache e cookies quando a sessão de navegação isolada terminar): ative essa configuração para limpar o cache e os cookies do navegador quando o usuário encerrar a sessão de navegação isolada (fechando o navegador). Limpar o cache e os cookies pode potencialmente ajudar a resolver alguns problemas do navegador, acelerando o carregamento de páginas ou removendo os dados de rastreamento do site.
- **Allow users to report issues encountered in isolation sessions** (Permitir que os usuários relatem problemas encontrados em sessões de isolamento): quando essa configuração está **ativada**, os usuários móveis podem relatar problemas encontrados durante a navegação isolada. Os usuários podem clicar no botão de ação flutuante e selecionar **Report an issue** (Relatar um problema).



3. Defina configurações avançadas para navegação isolada, como configurações de túnel dividido.



- **Agent Split Tunneling for RBI** (Túnel dividido do agente para RBI): para melhorar ainda mais a experiência do usuário enquanto estiver isolado, ative o [túnel dividido](#), que permite que o navegador remoto se conecte diretamente aos endpoints para um acesso mais rápido.

Essa configuração é ativada por padrão e se aplica somente às conexões de usuários móveis, como GlobalProtect e Proxy explícito. Para Redes remotas, todo o tráfego

passa pelo túnel para o Prisma Access. Para Proxy explícito, você precisa excluir o domínio do RBI no arquivo PAC, adicionando as seguintes declarações:

```
if (shExpMatch(host, "*.rbi.io")) return "DIRECT";
```



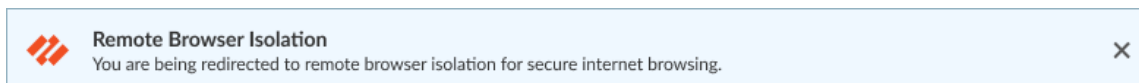
A configuração do túnel dividido de RBI não é visível na área de configuração do GlobalProtect. O RBI usa túnel dividido com base no domínio e no aplicativo, e a configuração é baseada em FQDN. Para que o túnel dividido funcione, você deve ativar o [DNS dividido](#) para permitir que os usuários móveis direcionem suas consultas de DNS de aplicativos e recursos pelo túnel ou fora do túnel, além do tráfego da rede.

- **Action for sites that cannot be decrypted (technical or policy reason)** (Ação para sites que não podem ser descriptografados [motivo técnico ou político]): o Prisma Access precisa descriptografar sites criptografados para que possa inspecionar o tráfego e determinar quais sites isolar de acordo com as políticas configuradas.

Escolha se deseja **Allow** (Permitir) ou **Block** (Bloquear) o acesso a sites que não podem ser descriptografados por motivos técnicos ou políticos.

4. Defina as configurações do tema para a sessão de navegação isolada. Quando um usuário entra em uma sessão de navegação isolada, um banner de notificação aparece por cerca de cinco segundos no navegador para que ele saiba que está entrando em isolamento. Você pode personalizar essa notificação para se alinhar com a aparência da sua organização.

Veja a seguir um exemplo de banner de notificação:



É aqui que você configura o tema de isolamento:

Isolation Theme Settings

Banner Settings

Name *

Remote Browser Isolation

Endpoint Banner Title

Description *

Your webpage is being loaded via Remote Browser Isolation to protect you from malicious at

Endpoint Banner Message

Banner Logo

Choose File

No file chosen

Floating Banner Logo

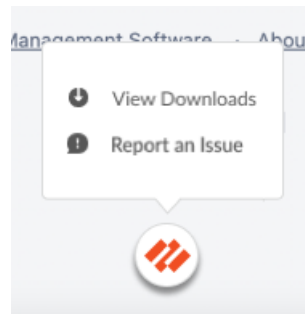
Choose File

No file chosen

- **Name** (Nome): insira o nome que aparecerá no banner de notificação quando o usuário entrar em uma sessão isolada no navegador. (Campo obrigatório)
- **Description** (Descrição): insira o texto que aparece no banner de notificação. (Campo obrigatório)
- **Banner Logo** (Logotipo do banner): use **Choose File** (Escolher arquivo) para carregar um arquivo de imagem que aparecerá como o logotipo do banner. Se você não fizer o upload de um arquivo, o logotipo da Palo Alto Networks será usado por padrão. Você

somente pode fazer upload de um arquivo. Os formatos de arquivo válidos são JPG e PNG.

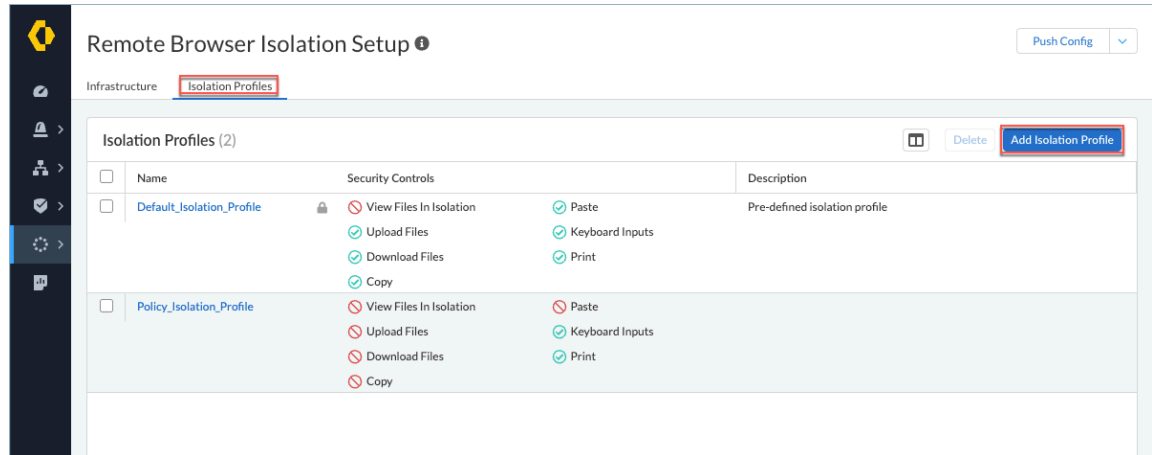
- **Floating Banner Logo** (Logotipo de banner flutuante): use **Choose File** (Escolher arquivo) para carregar um arquivo de imagem que aparecerá no botão de ação flutuante no qual os usuários podem clicar para invocar uma ação, como relatar um problema. Se você não fizer o upload de um arquivo, o logotipo da Palo Alto Networks será usado por padrão. Você somente pode fazer upload de um arquivo. Os formatos de arquivo válidos são JPG e PNG. A imagem deve ter 42x42 pixels para ser renderizada corretamente no RBI.



5. Clique em **Salvar** para salvar as configurações de infraestrutura.

STEP 4 | Configure um ou mais perfis de isolamento que definam quais ações do navegador os usuários podem realizar durante uma sessão isolada.

1. Na página Remote Browser Isolation Setup (Configuração do RBI), selecione **Isolation Profiles** (Perfis de isolamento).
2. Um perfil de isolamento padrão é fornecido para você. Você pode criar perfis de isolamento personalizados em **Add Isolation Profile** (Adicionar perfil de isolamento).



3. Insira um **Name** (Nome) e **Description** (Descrição) para o perfil de isolamento.
4. Selecione os controles de segurança que você deseja implementar para o navegador. Você pode permitir ou proibir um usuário de realizar as seguintes ações:
 - Exibir arquivos de forma isolada
 - Carregar arquivos
 - Baixar arquivos
 - Copiar conteúdo
 - Colar conteúdo
 - Usar o teclado para entrada
 - Imprimir conteúdo

Ao selecionar uma ação, ela será ativada e permitida para o usuário na navegação isolada.

The screenshot shows the 'Remote Browser Isolation Profiles' configuration page for a profile named 'Policy_Isolation_Profile'. The page has a dark sidebar on the left with various icons. The main content area is titled 'Policy_Isolation_Profile' and contains two sections: 'Settings' and 'Security Control'.

Settings

Name *	<input type="text" value="Policy_Isolation_Profile"/>
Description	<input type="text"/>

Security Control

View Files In Isolation	<input type="checkbox"/>	Allow Viewing of Files in Isolation
Upload Files	<input type="checkbox"/>	Allow Uploading of Files in Isolation
Download Files	<input type="checkbox"/>	Allow Downloading of File in Isolation
Copy	<input type="checkbox"/>	Allow Copying of Content in Isolation
Paste	<input type="checkbox"/>	Allow Pasting of Content in Isolation
Keyboard Inputs	<input checked="" type="checkbox"/>	Allow Keyboard Inputs in Isolation
Print	<input checked="" type="checkbox"/>	Allow Printing of Content in Isolation

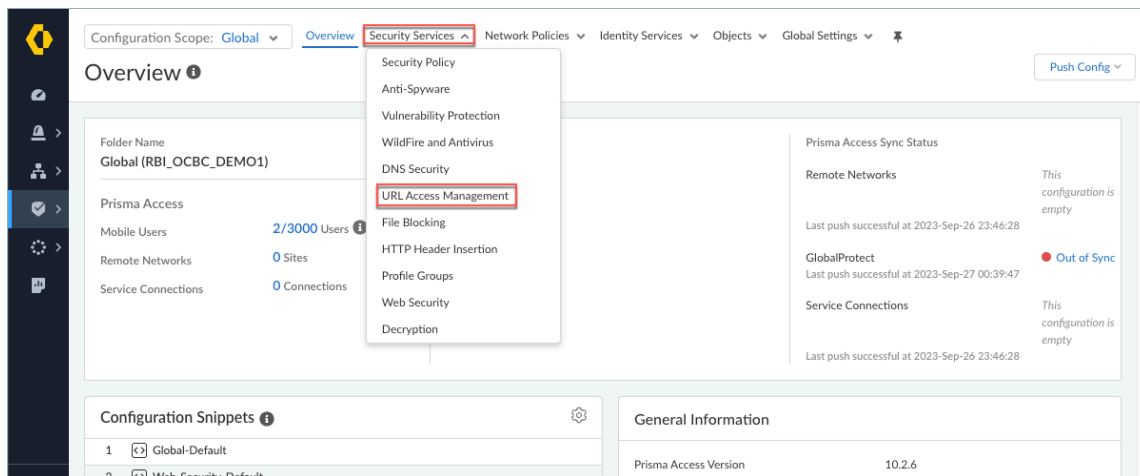
* Required Field

Cancel Save

5. Clique em **Save** (Salvar) para salvar as configurações do seu perfil de isolamento.

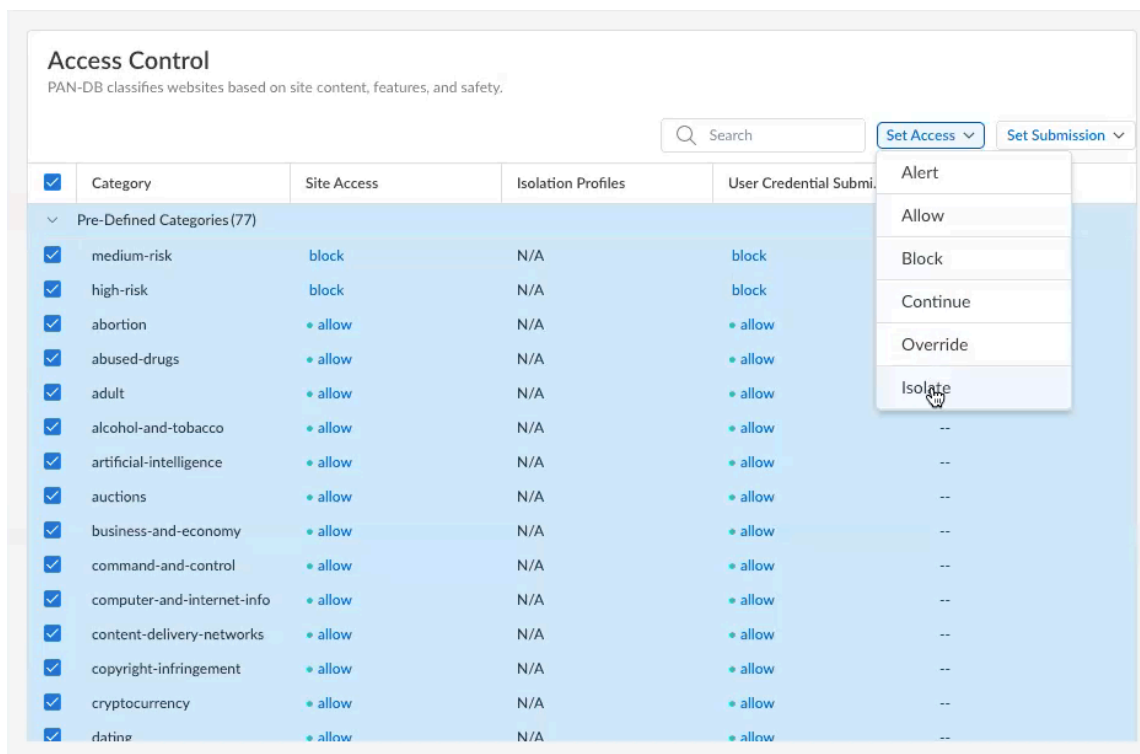
STEP 5 | Crie ou atualize um perfil de gerenciamento de acesso ao URL e anexe o perfil de isolamento a ele.

1. No Strata Cloud Manager, selecione **Manage > Configuration > NGFW e Prisma Access**
2. Selecione **Security Services > URL Access Management**.

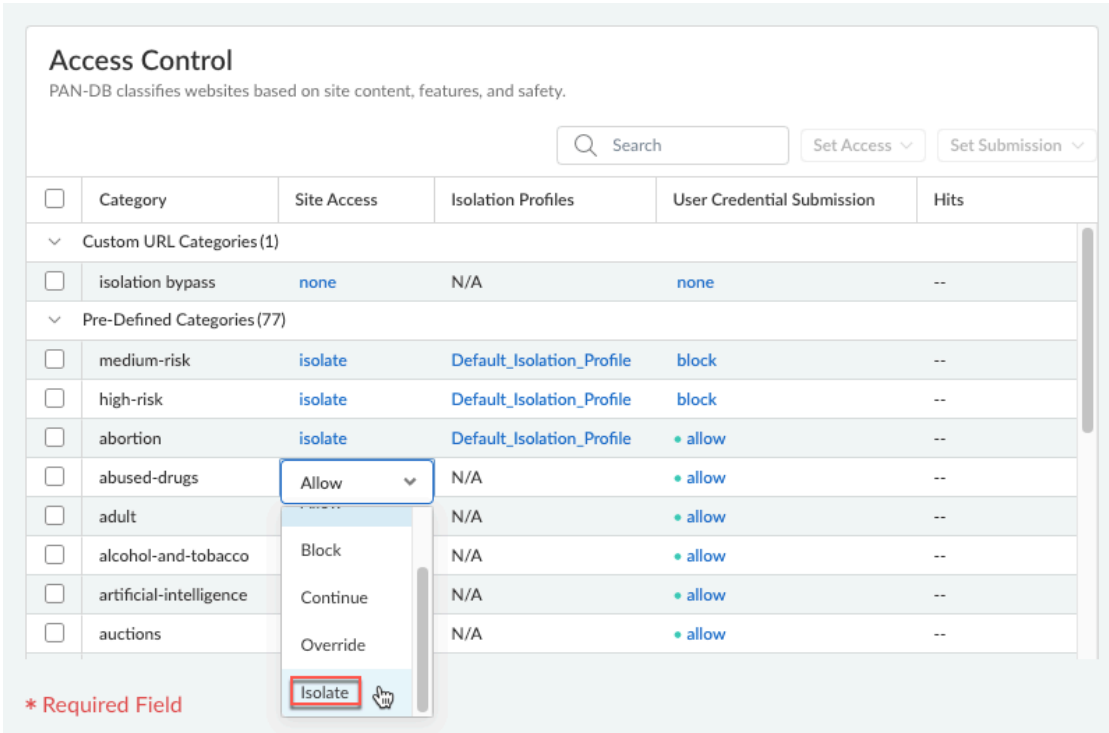


3. Edite um perfil existente de gerenciamento de acesso ao URL selecionando o nome ou clicando em **Add Profile** (Adicionar perfil) para criar um novo.
4. Se você estiver adicionando um perfil, insira um **Name** (Nome) e uma **Description** (Descrição) para ele, marque a caixa de seleção ao lado do título da coluna **Category** (Categoria) e selecione **Set Access > Isolate**.

Essa ação define automaticamente **Site Access** (Acesso ao site) como **isolate** (isolar) e associa **Default_Isolation_Profile** a todas as categorias de URL.



5. Se necessário, altere o **Access Control** (Controle de Acesso) para categorias específicas do site.
 1. Use **Search** (Pesquisar) para pesquisar uma categoria de URL ou navegue até uma categoria.
 2. Se você estiver editando um perfil de gerenciamento de URL existente, clique no menu suspenso **Site Access** (Acesso ao site) de uma categoria de URL e selecione **Isolate** (Isolar) para permitir a navegação isolada de sites nessa categoria.

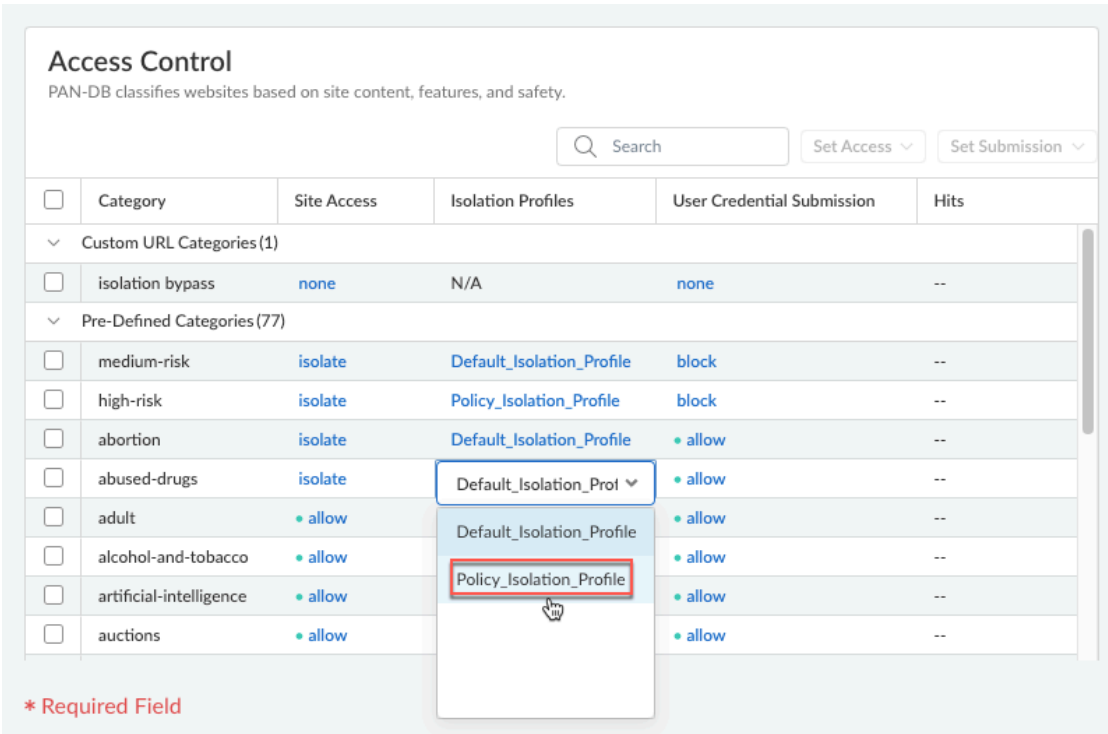


Para sites que pertencem a várias categorias de URL, a ação efetiva da categoria de URL é a ação correspondente de maior prioridade em todas essas categorias. A prioridade em ordem decrescente é a seguinte: **Block** > **Isolate** > **Override** > **Continue** > **Alert** > **Allow**. Portanto, para o RBI funcionar, você precisa definir a ação como **Isolate** (Isolar) para todas as categorias que correspondam a um site.

Por exemplo, **cnn.com** pertence às categorias **news** (notícias) e **low-risk** (baixo risco). Se a categoria **news** (notícias) estiver definida como **Block** (Bloquear) e a categoria **low-risk** (baixo risco) estiver definida como **Isolate** (Isolar), o site **cnn.com** será bloqueado porque a ação **Block** (Bloquear) substitui a ação **Isolate** (Isolar). Para que a navegação isolada funcione para **cnn.com**, você deve definir ambas as categorias para a ação **Isolate** (Isolar).

3. Depois de selecionar o acesso ao site, o **Default_Isolation_Profile** é automaticamente anexado à categoria de URL. Se você criou perfis de isolamento adicionais que controlam as ações do navegador no modo de isolamento, você pode anexar um

perfil diferente clicando no menu suspenso **Isolation Profile** (Perfil de isolamento) e selecionando um perfil disponível.



6. Clique em **Save** (Salvar) para salvar as configurações.

STEP 6 | Crie uma regra de política de segurança que use o perfil de gerenciamento de acesso ao URL que você configurou para isolamento.

1. No Strata Cloud Manager, selecione **Manage > Configuration > NGFW e Prisma Access**
2. Se ainda não tiver feito isso, crie um grupo de perfis.
 1. Selecione **Security Services > Profile Groups** e **Add Profile Group** (Adicionar grupo de perfis).
 2. Insira o **Name** (Nome) do grupo de perfis.
 3. Selecione os perfis de segurança que você deseja usar e certifique-se de selecionar o **URL Access Management Profile** (Perfil de gerenciamento de acesso ao URL) que deseja usar para isolamento.

4. Clique em **Save** (Salvar) para salvar as alterações.
3. Associe o grupo de perfis a uma regra de segurança. Se ainda não tiver feito isso, crie uma regra de segurança.
 1. Selecione **Security Services > Security Rules > Add Rule > Pre Rules**.
 2. Insira o **Name** (Nome) da regra de segurança.
 3. Selecione uma zona de origem para os **Match Criteria** (Critérios de correspondência).
 4. Selecione uma zona de destino e um endereço para os **Match Criteria** (Critérios de correspondência).
 5. Selecione um **Application** (Aplicativo).
 6. Selecione a ação **Allow** (Permitir) e selecione o **Profile Group** (Grupo de perfis) que você criou para isolamento.



Você pode usar os grupos que você criou ou preencheu no Cloud Identity Engine para o mapeamento de usuários e grupos de usuários do RBI.

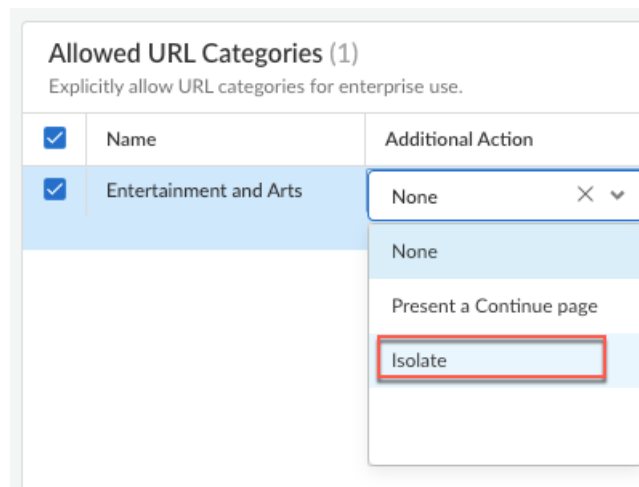
The screenshot shows the 'Security Policy' configuration page in the Strata Cloud Manager. The policy is named 'RBI_All_Policy' and has a description 'rbi ocbs testing'. It is currently 'Enabled'. The 'Match Criteria' section is divided into four panels: 'SOURCE', 'DESTINATION', 'APPLICATION / SERVICE', and 'URL CATEGORY / TENANT RESTRICTION'. In the 'SOURCE' panel, 'Zones' is set to 'Any', 'Addresses' to 'Any', 'Users' to 'Any', and 'Devices' to 'Any'. In the 'DESTINATION' panel, 'Zones' is set to 'Any', 'Addresses' to 'Any', and 'Devices' to 'Any'. In the 'APPLICATION / SERVICE' panel, 'Application' is set to 'Any' and 'Service' to 'Application Default'. In the 'URL CATEGORY / TENANT RESTRICTION' panel, 'URL Category' is set to 'Any' and 'Tenant Restriction' to 'Any'. The 'Actions' section at the bottom has a tab for 'Profile Group' selected, showing 'Allow' as the action and 'RBI_Profile_Group' as the profile group. A red box highlights the 'Allow' action and the 'RBI_Profile_Group' profile group. A red asterisk indicates a required field. The 'Cancel' and 'Save' buttons are at the bottom right.

STEP 7 | Você também pode criar uma regra de segurança da Web para controlar o acesso a sites em categorias de URL com base no perfil de isolamento configurado anteriormente.

1. No Strata Cloud Manager, selecione **Manage > Configuration > NGFW e Prisma Access**
2. Selecione **Security Services > Web Security > Add Policy**.
3. Insira o **Name** (Nome) da política personalizada de acesso à web.
4. Adicione as **Allowed URL Categories** (Categorias de URL permitidas) para navegação isolada. Por exemplo, para permitir que sites na categoria Entretenimento e

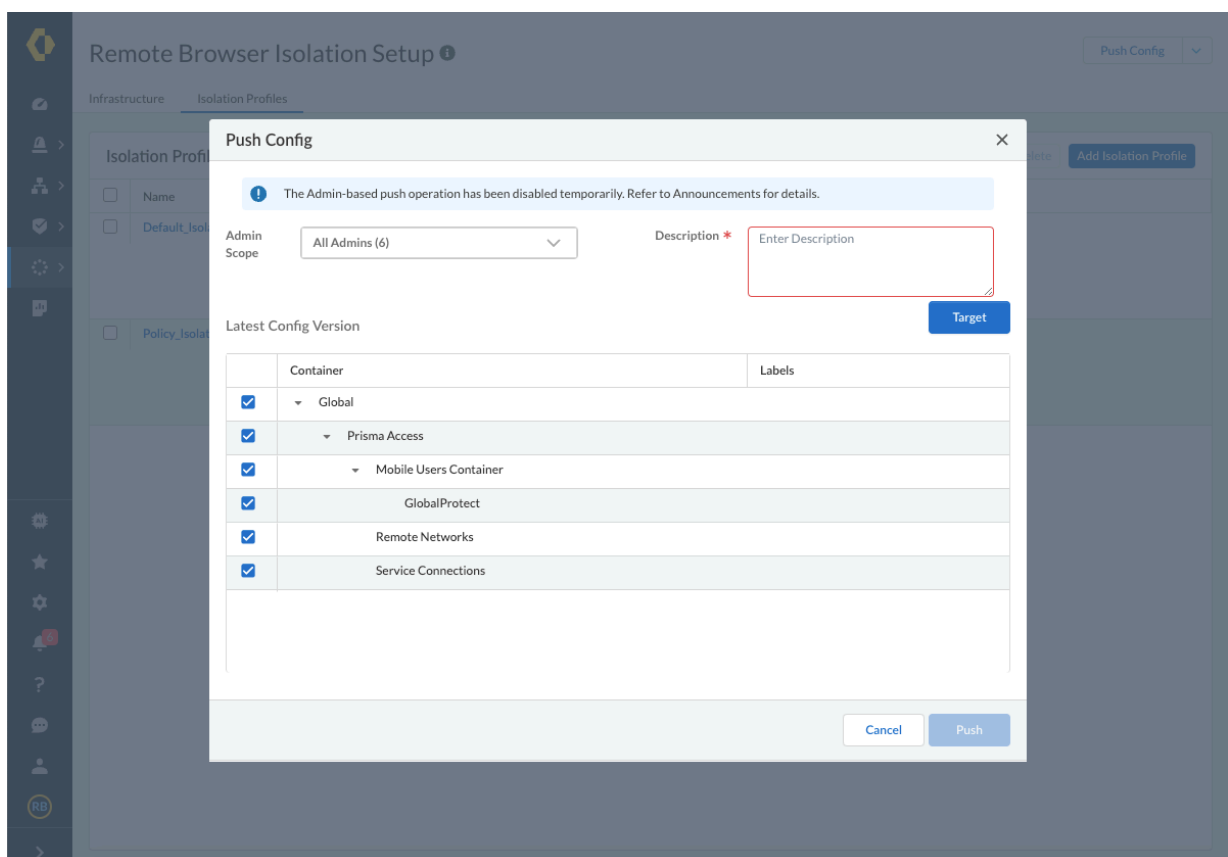
artes naveguem isoladamente, clique em + e selecione **Entertainment and Arts** (Entretenimento e artes).

5. Clique em **None** (Nenhuma) na coluna Additional Action (Ação adicional) e selecione **Isolate** (Isolar).



6. Na coluna **Isolation Profile** (Perfil de isolamento), use o perfil de isolamento padrão ou selecione um perfil de isolamento que você criou.
7. Clique em **Save** (Salvar) para salvar as alterações.

STEP 8 | Envie a configuração para seus usuários móveis ou redes remotas selecionando **Push Config** > **Push**, selecionando **Target** (Destino) da configuração e **Push** (Aplicar).



Configurar o Remote Browser Isolation (Panorama)

Você pode proteger a experiência de navegação dos usuários finais configurando o Remote Browser Isolation (RBI) para isolar o tráfego do navegador.

Configure o RBI concluindo as seguintes etapas:

STEP 1 | Antes de começar a configurar o RBI, certifique-se de:

- Comprar uma licença válida do [Prisma Access](#) com uma assinatura de licença de Usuários móveis ou Redes remotas.
- [Ativar o Panorama Managed Prisma Access](#).
- Comprar e [ativar a licença de Isolamento remoto do navegador](#).
- [Configurar o Panorama Managed Prisma Access](#).
- Configurar pelo menos um método de conexão do Prisma Access, como [GlobalProtect](#), [Proxy explícito](#) ou [Redes remotas](#); caso contrário, você não poderá habilitar RBI.
- [Ativar acriptografia](#) para que o Prisma Access possa criptografar e inspecionar o tráfego para determinar o que precisa ser isolado de acordo com as políticas configuradas.

STEP 2 | Siga as instruções para [configurar um perfil de filtragem de URL e aplicá-lo a uma regra de segurança](#).

Ao configurar o perfil de filtragem de URL, você pode selecionar **alert** (alertar) ou **allow** (permitir) em **Site Access** (Acesso ao site) para uma categoria de URL e, em seguida, [anexar um perfil de isolamento](#) à categoria de URL e associá-la a uma política de segurança.

URL Filtering Profile

NameAlert-All-PA

Description

☐ Shared

☐ Disable override

Categories

URL Filtering Settings

User Credential Detection

HTTP Header Insertion

Inline Categorization

78 items

→

×

<input type="checkbox"/>	CATEGORY	SITE ACCESS	USER CREDENTIAL SUBMISSION
▼	Custom URL Categories		
<input type="checkbox"/>	SSO_List *	alert	allow
▼	Pre-defined Categories		
<input checked="" type="checkbox"/>	abortion	<div><div>alert</div><div>block</div><div>allow</div><div>continue</div><div>override</div></div>	allow
<input type="checkbox"/>	abused-drugs		block
<input type="checkbox"/>	adult		allow
<input type="checkbox"/>	alcohol-and-tobacco		allow

* indicates a custom URL category, + indicates external dynamic list

[Check URL Category](#)

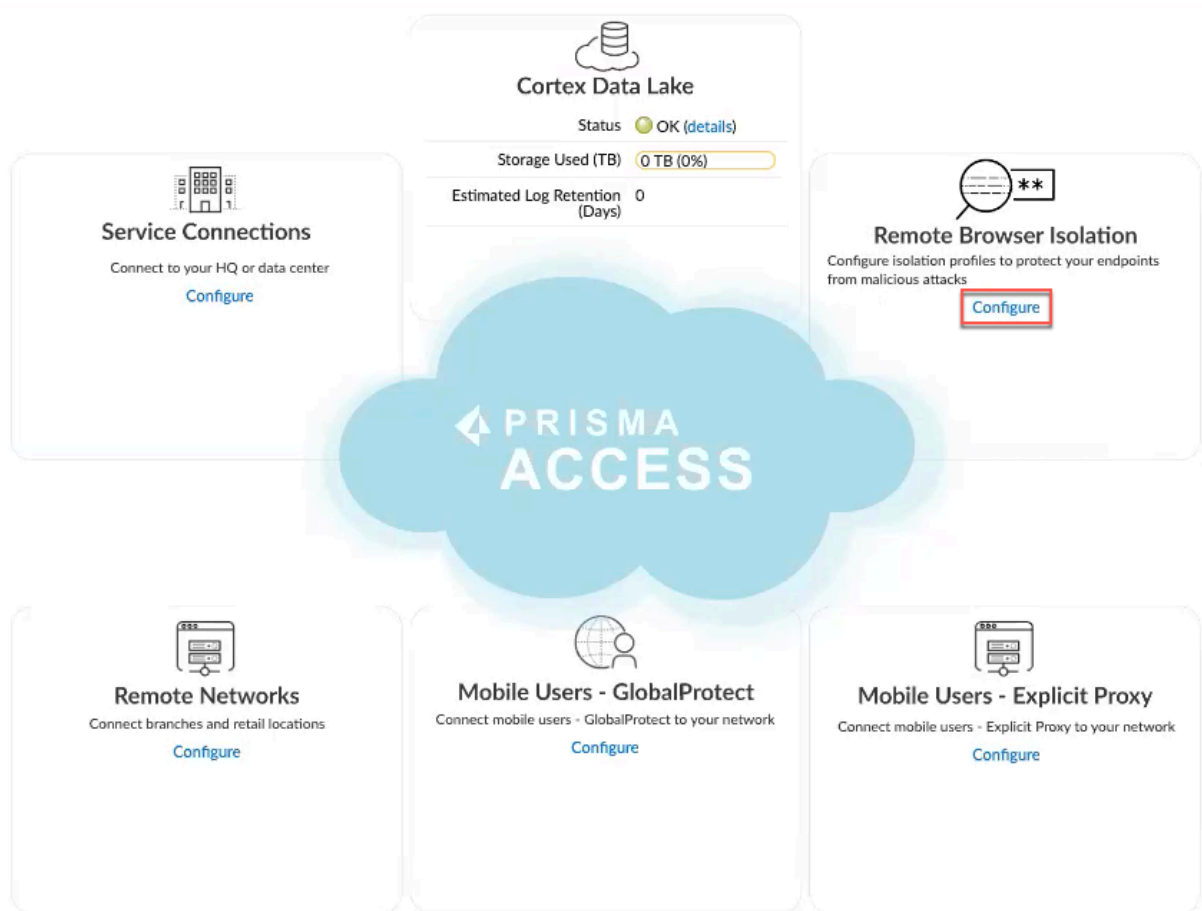
OK

Cancel

STEP 3 | Se você estiver configurando o RBI pela primeira vez no Panorama Managed Prisma Access, selecione **Panoram > Cloud Services > Status > Remote Browser Isolation > Configure**.



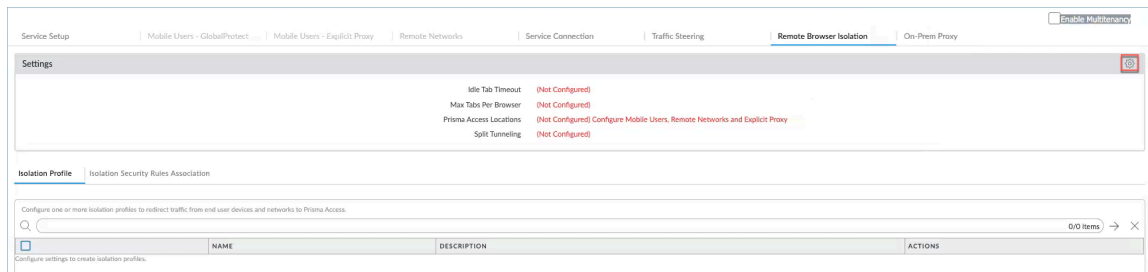
O botão **Configure** (Configurar) somente estará disponível se você tiver comprado a licença do Remote Browser Isolation.



Se você já configurou o RBI e deseja editar a configuração, selecione **Panorama > Cloud Services > Configuration > Remote Browser Isolation**.

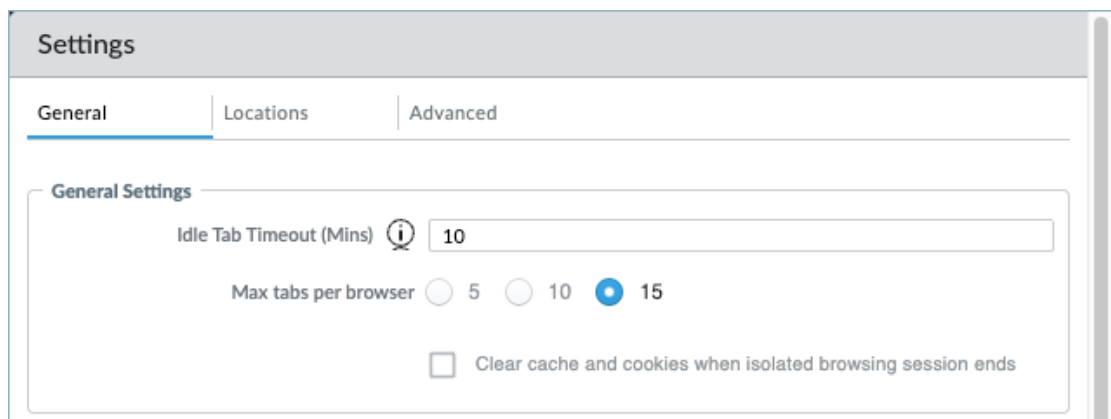
STEP 4 | Defina as configurações de infraestrutura do RBI que especificarão o comportamento e o aspecto do navegador durante sessões de navegação isoladas.

1. Edite as **Settings** (Configurações).



2. Selecione a guia **General** (Geral) para começar a definir o comportamento do navegador durante uma sessão de navegação isolada ao

1. Definir as configurações gerais do navegador:



- **Idle Tab Timeout (Mins)** (Tempo limite de guia ociosa [minutos]): defina quanto tempo de inatividade do usuário leva para que uma guia do navegador expire. O valor do tempo limite padrão é de 10 minutos. O intervalo é de 5 a 20 minutos.

O cronômetro de inatividade começa na última ação do usuário, como clicar com o mouse, rolar, navegar, carregar ou baixar arquivos e interromper um vídeo ou áudio. Apenas mover o cursor não é considerado uma atividade.

- **Max Tabs Per Browser** (Máximo de guias por navegador): selecione o número máximo de guias que o usuário pode abrir por navegador. Você pode escolher no máximo 5, 10 ou 15 guias. O padrão é 10.

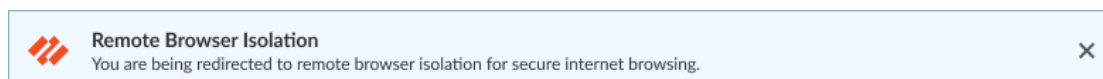
Quando o número de guias exceder o máximo, os usuários serão solicitados a fechar as guias existentes se quiserem abrir mais guias para navegação.

- **Clear cache and cookies when isolated browsing session ends** (Limpar cache e cookies quando a sessão de navegação isolada terminar): ative essa configuração para limpar o cache e os cookies do navegador quando o usuário encerrar a sessão de navegação isolada (fechando o navegador). Limpar o cache e os cookies pode potencialmente ajudar a resolver alguns problemas do navegador, acelerando o carregamento de páginas ou removendo os dados de rastreamento do site.

2. Defina as configurações do tema para a sessão de navegação isolada. Quando um usuário entra em uma sessão de navegação isolada, um banner de notificação aparece

por cerca de cinco segundos no navegador para que ele saiba que está entrando em isolamento. Você pode personalizar essa notificação para se alinhar com a aparência da sua organização.

Veja a seguir um exemplo de banner de notificação:



Aqui é onde você especifica o conteúdo do banner:

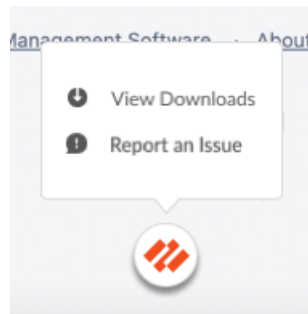
A imagem é uma captura de tela da interface de configuração de banners e mensagens. No topo, há uma seção intitulada "Banners and Messages" com o subtítulo "A notification message will be displayed in the EndPoint interface indicating user(s) they are browsing in an isolated session." Abaixo disso, há uma seção "Banner Settings". Nesta seção, o campo "Title" contém o texto "RBI Panorama QA6 - 1000813". O campo "Banner Content" contém o texto "Isolated through Prisma Access RBI - QA6 - 1000813". Abaixo do campo de conteúdo, há uma opção "Logo Type" com dois botões de rádio: "Default(Palo Alto)" e "Custom", sendo que "Custom" está selecionado. Abaixo das opções de logotipo, há uma área para upload de uma imagem com o texto "Upload a logo of your choice to appear in the Banner notification." e um botão "Browse". Abaixo disso, há uma confirmação de upload com um ícone de checkmark verde, o nome do arquivo "logo_pan_pa_455.png" e o tamanho "5.49 KB", além de ícones de zoom e exclusão. Abaixo da seção "Banner Settings", há uma seção "Floating Action Button Settings". Nesta seção, também há uma opção "Logo Type" com "Default(Palo Alto)" e "Custom" (selecionado). Abaixo, há uma área para upload de uma imagem com o texto "Upload a logo of your choice to appear in the Banner notification." e um botão "Browse". Abaixo disso, há uma confirmação de upload com um ícone de checkmark verde, o nome do arquivo "logo_pan_pa_455.png" e o tamanho "19.53 KB", além de ícones de zoom e exclusão.

- **Title (Título):** digite o nome que aparecerá no banner de notificação quando o usuário entrar em uma sessão isolada no navegador.
- **Banner Content (Conteúdo do banner):** insira o texto que aparecerá no banner de notificação.
- **Logo Type (Banner)** (Tipo de logotipo [banner]): selecione o tipo de logotipo que aparecerá no banner. O logotipo padrão é o ícone da Palo Alto Networks. Para personalizar o logotipo, clique em **Custom** (Personalizar) e **Browse** (procurar) para carregar de um arquivo de imagem de sua escolha. Você somente pode fazer upload de um arquivo. Os formatos de arquivo válidos são JPG e PNG.
- **Logo Type (Floating Action Button)** (Tipo de logotipo [botão de ação flutuante]): selecione o tipo de logotipo que aparecerá no botão de ação flutuante no navegador de isolamento. O botão de ação flutuante fornece uma lista de ações

que o usuário pode executar, como relatar um problema. O usuário pode arrastar o botão para diferentes locais no navegador.

O logotipo **Default** (Padrão) do botão de ação flutuante é o ícone da Palo Alto Networks. Para personalizar o logotipo, clique em **Custom** (Personalizar) e **Browse** (procurar) para carregar de um arquivo de imagem de sua escolha. Você somente pode fazer upload de um arquivo. Os formatos de arquivo válidos são JPG e PNG. A imagem deve ter 42x42 pixels para ser renderizada corretamente no RBI.

A imagem a seguir mostra um exemplo do botão de ação flutuante:

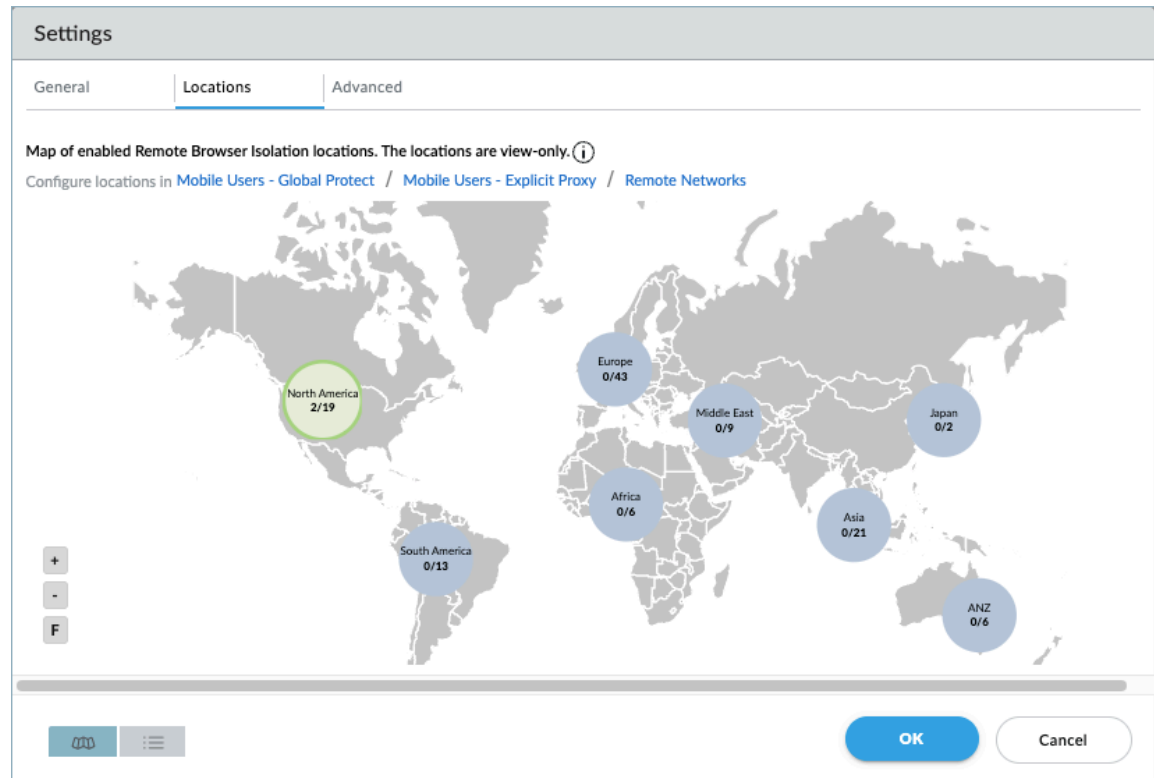


3. Habilite **Allow users to report issues encountered in isolated sessions?** (Permitir que os usuários relatem problemas encontrados em sessões isoladas?) se você quiser que os usuários finais relatem problemas encontrados durante a navegação isolada.

Os usuários podem clicar no botão de ação flutuante e selecionar **Report an issue** (Relatar um problema).

3. Revise um mapa dos locais do RBI selecionando a guia **Locations** (Locais). Os locais mostrados são os mesmos que os locais GlobalProtect, Explicit Proxy e Remote Network que você já configurou.

Se você não configurou nenhum local, poderá clicar nos links no mapa para navegar até as páginas de configuração relevantes.



4. Defina configurações avançadas para navegação isolada, como configurações de túnel dividido, selecionando a guia **Advanced** (Avançado).

Settings

General | Locations | **Advanced**

Split Tunneling Settings

For better performance enable Split Tunneling for Remote Browser Isolation on the agent.

Agent Split Tunneling For Remote Browser Isolation ☒ Enable ☐ Disable

Site Decryption Settings

Action for sites that cannot be decrypted (technical or policy reasons) ☒ Allow ☐ Block

OK Cancel

- **Agent Split Tunneling for RBI** (Túnel dividido do agente para RBI): para melhorar ainda mais a experiência do usuário enquanto estiver isolado, ative o [túnel dividido](#), que permite que o navegador remoto se conecte diretamente aos endpoints para um acesso mais rápido.

Essa configuração é ativada por padrão e se aplica somente às conexões de usuários móveis, como GlobalProtect e Proxy explícito. Para Redes remotas, todo o tráfego passa pelo túnel para o Prisma Access. Para Proxy explícito, você precisa excluir o domínio do RBI no arquivo PAC, adicionando as seguintes declarações:

```
if (shExpMatch(host, "*.rbi.io")) return "DIRECT";
```



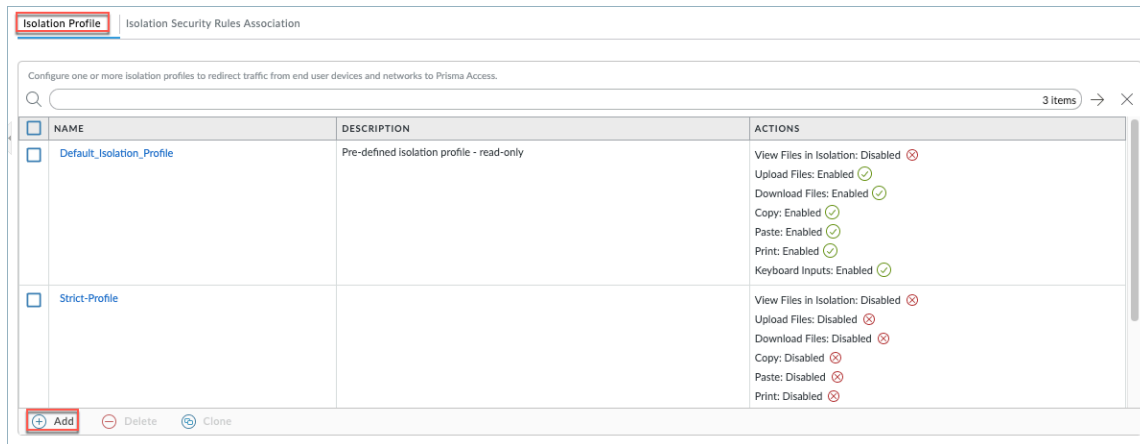
A configuração do túnel dividido de RBI não é visível na área de configuração do GlobalProtect. O RBI usa túnel dividido com base no domínio e no aplicativo, e a configuração é baseada em FQDN. Para que o túnel dividido funcione, você deve ativar o [DNS dividido](#) para permitir que os usuários móveis direcionem suas consultas de DNS de aplicativos e recursos pelo túnel ou fora do túnel, além do tráfego da rede.

- **Action for sites that cannot be decrypted (technical or policy reason)** (Ação para sites que não podem ser descriptografados [motivo técnico ou político]): o Prisma Access precisa descriptografar sites criptografados para que possa inspecionar o tráfego e determinar quais sites isolar de acordo com as políticas configuradas.

Escolha se deseja **Allow** (Permitir) ou **Block** (Bloquear) o acesso a sites que não podem ser descriptografados por motivos técnicos ou políticos.

STEP 5 | Configure um ou mais perfis de isolamento que definam quais ações do navegador os usuários podem realizar durante uma sessão isolada.

1. Na página de configuração do Remote Browser Isolation, selecione **Isolation Profile** (Perfil de isolamento).
2. Um perfil de isolamento padrão é fornecido para você. É possível **Add** (Adicionar) um perfil de isolamento personalizado.



3. Insira um **Name** (Nome) e **Description** (Descrição) para o perfil de isolamento.
4. Selecione os controles de segurança para o navegador. Você pode permitir ou proibir um usuário de realizar as seguintes ações:
 - Exibir arquivos de forma isolada
 - Carregar arquivos
 - Baixar arquivos
 - Copiar conteúdo
 - Colar conteúdo
 - Usar o teclado para entrada
 - Imprimir conteúdo

Ao selecionar um controle de segurança, a ação do navegador será permitida para o usuário em navegação isolada.

Isolation Profile

Name

Description

Profile Actions

View Files in Isolation ☐ Enable ☒ Disable

Upload Files ☐ Enable ☒ Disable

Download Files ☐ Enable ☒ Disable

Copy ☐ Enable ☒ Disable

Paste ☐ Enable ☒ Disable

Print ☐ Enable ☒ Disable

Keyboard Inputs ☐ Enable ☒ Disable

5. Clique em **OK** para salvar o perfil de isolamento.

STEP 6 | Anexe um perfil de isolamento a uma regra de segurança à qual você aplicou um perfil de Filtragem de URL contendo categorias para navegação isolada.

1. Na configuração do Remote Browser Isolation, selecione **Isolation Security Rules Association** (Associação de regras de segurança de isolamento).
2. Selecione **Add** (Adicionar) para adicionar um grupo de dispositivos e associe um perfil de isolamento e categorias de URL às regras de segurança do grupo de dispositivos.

Isolation Profile: **Isolation Security Rules Association**

Associate isolation profile and URL categories with the security rules for the selected Device Groups.

DEVICE GROUP	SECURITY RULE	URL CATEGORY	ACTIONS
<input type="checkbox"/> Mobile_User_Device_Group	Isolate_All_MU	Selected Categories (77)	<input checked="" type="checkbox"/> Modify
<input type="checkbox"/> Remote_Network_Device_Group	Isolate_All_RN	Selected Categories (77)	<input checked="" type="checkbox"/> Modify
<input type="checkbox"/> Explicit_Proxy_Device_Group	Isolate_All_EP	Selected Categories (77)	<input checked="" type="checkbox"/> Modify

Se você quiser atualizar um grupo de dispositivos existente, marque a caixa de seleção ao lado do nome do grupo de dispositivos e selecione **Modify** (Modificar) na coluna Actions (Ações).

3. Selecione um **Device Group** (Grupo de dispositivos) e uma **Security Rule** (Regra de segurança) predefinida para o grupo de dispositivos selecionado.
4. Pesquise ou navegue pelas categorias de URL que você deseja associar ao grupo de dispositivos e marque as caixas de seleção ao lado das categorias de URL.



*Para configurar rapidamente o controle de acesso para todas as categorias de URL, marque a caixa de seleção ao lado do cabeçalho da tabela **URL Categories** (Categorias de URL). Todas as categorias de URL serão selecionadas.*

5. Para anexar um perfil de isolamento à regra de segurança, clique em **Isolation Profile** (Perfil de isolamento) e selecione um perfil de isolamento disponível. Certifique-se de

que **Site Access** (Acesso ao site) para uma categoria de URL esteja definido como **alert** (alertar) ou **allow** (permitir).

Isolation Security Rules Association

Device Group

Mobile_User_Device_Group

Security Rule

Isolate_All_MU

<input checked="" type="checkbox"/>	URL CATEGORIES	SITE ACCESS	ISOLATION PROFILE
Pre-defined Categories			
<input checked="" type="checkbox"/>	unknown	alert	Not-So-Strict-Profile
<input checked="" type="checkbox"/>	copyright-infringement	alert	Not-So-Strict-Profile
<input checked="" type="checkbox"/>	low-risk	alert	Not-So-Strict-Profile
<input checked="" type="checkbox"/>	gambling	alert	Not-So-Strict-Profile
		alert	Not-So-Strict-Profile
		alert	Not-So-Strict-Profile
		alert	Not-So-Strict-Profile

Default_Isolation_Profile

Strict-Profile

Not-So-Strict-Profile

Isolation Profile

OK

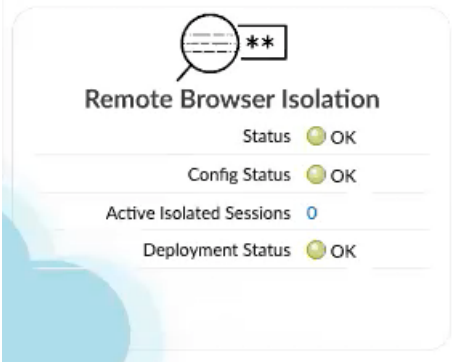
Cancel

Todas as categorias de URL selecionadas serão associadas ao perfil de isolamento selecionado.

6. Clique em **OK** para salvar as configurações.

STEP 7 | Confirme e envie as alterações de configuração para o firewall de nuvem.

STEP 8 | Depois que a configuração for enviada com sucesso, você poderá visualizar o status da configuração do RBI em **Panorama > Cloud Services > Status**.



Integrar a um provedor de desarme e reconstrução de conteúdo de terceiros

Onde posso usar isso?	O que eu preciso?
<ul style="list-style-type: none"> Prisma Access (Managed by Strata Cloud Manager) 	<ul style="list-style-type: none"> Prisma Access 5.1 Innovation Licença do Prisma Access com a assinatura de licença de Usuário móvel ou Redes remotas Licença de isolamento remoto do navegador

Quando seus usuários baixam arquivos para suas máquinas locais durante a navegação isolada, eles podem ficar expostos a ameaças de dia zero se os arquivos baixados contiverem conteúdo malicioso. Mesmo que os arquivos baixados possam ser verificados quanto a vulnerabilidades usando soluções antivírus ou de verificação de arquivos, ameaças desconhecidas ainda podem escapar da detecção. Você pode integrar o Remote Browser Isolation (RBI) a um provedor de conteúdo e desarme (CDR) terceirizado para verificar ameaças nos arquivos e deixá-los seguros para uso pelos usuários.

Quando um usuário tenta baixar um arquivo durante a navegação isolada, o arquivo será analisado pelo provedor de CDR. Se o arquivo contiver conteúdo malicioso ativo, como malware, macros ou fontes incorporadas, o provedor de CDR desarmará o arquivo removendo o conteúdo malicioso e reconstruirá o arquivo em seu formato original antes de entregá-lo ao usuário. O usuário poderá então visualizar e baixar o arquivo com segurança e ficar protegido contra malware e possíveis ameaças de dia zero.

Ao baixar um arquivo, o RBI notificará o usuário dos seguintes eventos:

- Quando RBI enviar o arquivo para o serviço de CDR para análise
- Quando o RBI estiver aguardando uma resposta do serviço de CDR
- Quando o RBI receber uma resposta bem-sucedida do serviço de CDR
- Quando o RBI encontrar algum erro durante o processo

Você pode integrar o RBI ao seguinte provedor de CDR terceirizado:

- [Votiro](#)

Integrar o RBI ao Votiro

Onde posso usar isso?	O que eu preciso?
<ul style="list-style-type: none"> Prisma Access (Managed by Strata Cloud Manager) 	<ul style="list-style-type: none"> Prisma Access 5.1 Innovation Licença do Prisma Access com a assinatura de licença de Usuário móvel ou Redes remotas Licença de isolamento remoto do navegador Votiro

O Votiro Disarmer é um provedor terceirizado de desarme e reconstrução de conteúdo (CDR) que pode ser integrado ao RBI para analisar e remover ameaças de dia zero de arquivos que os usuários do seu RBI tentam baixar.

Quando um usuário baixa um arquivo durante a navegação isolada, o RBI envia o arquivo para o Votiro para verificação, análise e remoção de quaisquer ameaças ou malware que o Votiro detecte. O arquivo seguro é então entregue ao dispositivo local do usuário para consumo. Todos os arquivos que o usuário baixar serão enviados ao Votiro para análise.

Para integrar o Votiro, você precisará configurar uma política de seleção no Votiro que determine como os arquivos são processados. Em seguida, configure a integração do Votiro no Strata Cloud Manager.



Arquivos protegidos por senha não são suportados no momento. Os arquivos aparecerão como bloqueados para o usuário do RBI.

Antes de começar:

- Certifique-se de comprar uma licença do Votiro
- Entre em contato com seu representante de conta da Palo Alto Networks para habilitar o recurso de CDR para Remote Browser Isolation

STEP 1 | Crie uma política no console do Votiro chamada **PANWRBI** para especificar como os arquivos são verificados e processados. Você deve usar este nome de política porque o RBI usa o mesmo nome de política predefinido na chamada de API para enviar arquivos para o Votiro.

STEP 2 | Configure a integração com o Votiro no Strata Cloud Manager.

1. Entre no Strata Cloud Manager e selecione **Workflows > Prisma Access Setup > Remote Browser Isolation**.
2. Se você estiver integrando o Votiro ao RBI pela primeira vez, clique em **Set Up Votiro Integration** (Configurar integração do Votiro). Caso contrário, edite as configurações de integração do Votiro.

3. Clique em **Enable** (Habilitar) o estado do administrador para habilitar a integração. Se você desabilitar a integração após configurá-la, o RBI deixará de enviar arquivos para análise do Votiro.

4. Insira o **API Endpoint** (Endpoint de API) do Votiro. Este é o site para o qual o RBI enviará arquivos para análise. Você pode obter o endpoint da API no console Votiro.
5. Insira o **JSON Token** (Token JSON) que é usado para autenticação com o Votiro. Você pode obter o token JSON na página Service Tokens (Tokens de serviço) no console do

Votiro. Copie o token JSON e cole-o no campo **JSON Token** (Token JSON) no Strata Cloud Manager.

6. Clique em **Save** (Salvar) para salvar as configurações.
7. Clique em **Push Config** (Aplicar configuração) para aplicar a configuração no Prisma Access.

A configuração foi concluída e o RBI enviará todos os arquivos que um usuário baixar para o Votiro para CDR.



Se um perfil de isolamento for configurado para bloquear downloads de arquivos, essa ação substituirá e bloqueará os downloads de arquivos antes que eles sejam enviados ao Votiro.

Experiência de navegação isolada

Onde posso usar isso?	O que eu preciso?
<ul style="list-style-type: none">• Prisma Access (Managed by Panorama or Strata Cloud Manager)	<ul style="list-style-type: none">❑ Prisma Access 5.0 Innovation❑ Licença do Prisma Access com a assinatura de licença de Usuário móvel ou Redes remotas❑ Licença de isolamento remoto do navegador

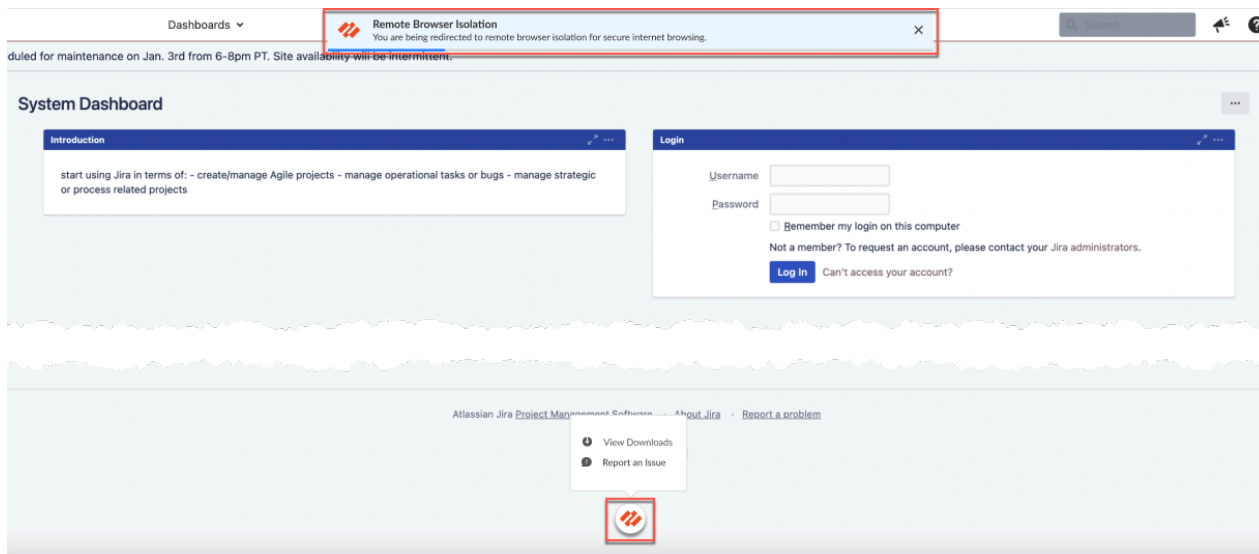
Depois de [configurar o RBI](#) e aplicar a configuração em seus endpoints, seus usuários podem entrar na navegação isolada dos sites que você designou para isolamento.

Antes de começarem a navegação isolada, seus usuários precisam garantir que estejam conectados ao Prisma Access usando um dos métodos de conexão, como o aplicativo GlobalProtect. Quando seus usuários navegam em sites em categorias designadas para isolamento, eles podem desfrutar de uma experiência de navegação quase nativa, em que o conteúdo carrega quase tão rápido quanto sites que não estão isolados.

O RBI é compatível com a maioria das tecnologias da Web suportadas por um navegador padrão, incluindo JavaScript, frameworks modernos, HTML5, protocolo HTTP e suporte a mídia avançada, como vídeo, áudio e GIFs animados. Os endereços de URL mostrados no navegador remoto terão a mesma aparência dos URLs nativos originais, sem prefixos adicionados aos endereços.

Banner de isolamento

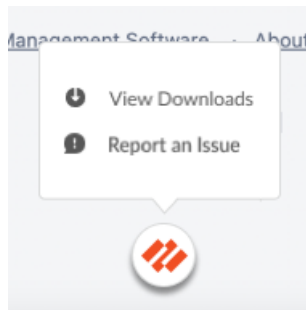
Quando seus usuários entram na navegação isolada, o RBI alerta os usuários de que estão em navegação isolada exibindo o banner de isolamento que você definiu ao [configurar o RBI](#). O banner aparece por cerca de cinco segundos e depois fecha.



Relatar um problema

Um *botão de ação flutuante* aparece no navegador de isolamento para ajudar seus usuários a realizar ações no navegador, como relatar um problema ou visualizar downloads. Seus usuários podem clicar no botão para exibir uma lista de ações. Eles também podem arrastar o botão para locais diferentes no navegador.

Veja este exemplo do botão de ação flutuante:



Se você configurou o RBI para permitir que seus usuários relatem problemas encontrados durante a navegação isolada, eles poderão clicar no botão de ação flutuante **Report an Issue** (Relatar um problema). O RBI solicitará que eles relatem um problema preenchendo e enviando um formulário:

Report an Issue

Select a Reason for report *

☐ Unable to access the site

☐ Video/ Audio Performance

☐ Site Performance

☒ Other

Tell us what happened and what's not working

Jira application is not loading

only 200 characters supported

• Required Field

Cancel

Report

Controle de segurança do navegador

Dependendo das ações do navegador que você definiu em um perfil de isolamento, seus usuários podem ou não realizar as seguintes ações no navegador:

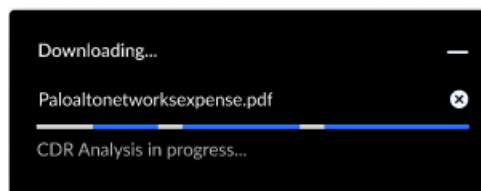
- Exibir arquivos isoladamente: exibir um arquivo do site isolado (desativado por padrão).
Quando essa ação estiver ativada, os arquivos serão convertidos em formato PDF e serão somente leitura. Se a ação de download de arquivos estiver ativada, será fornecida uma opção para baixar o arquivo original. Você pode visualizar [Tipos de arquivo suportados para exibir arquivos isoladamente](#) em uma sessão de navegação isolada.
- Carregar arquivos: carregar um arquivo (incluindo por arrastar e soltar) em um site isolado (permitido por padrão).
- Baixar arquivos: baixar um arquivo (incluindo por arrastar e soltar) de um site isolado (permitido por padrão).
- Salvar (Copiar): copie qualquer conteúdo do site isolado (permitido por padrão).
- Paste (Colar): cole qualquer conteúdo no site isolado (permitido por padrão).
- Entradas de teclado: digitar texto usando o teclado físico ou virtual (permitido por padrão).
- Print (Imprimir): imprima qualquer conteúdo de um site isolado (permitido por padrão).

Análise dos arquivos baixados

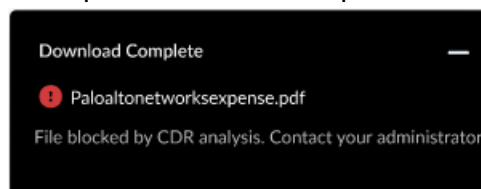
Quando você se integra o RBI a um [provedor de CDR terceirizado](#), como o [Votiro](#), seus usuários ficam protegidos contra qualquer conteúdo potencialmente malicioso que possa estar incorporado aos arquivos que baixam.

Quando um usuário navega em vários sites com isolamento e seleciona um arquivo para baixar, o RBI envia o arquivo ao provedor de CDR para verificação, análise e remoção de conteúdo malicioso. O arquivo é então reconstruído em seu formato original e entregue ao dispositivo do usuário final.

Durante o download, o RBI mostra uma notificação pop-up para informar ao usuário que o arquivo está sendo analisado. Quando o arquivo for limpo e o download for concluído, ele poderá salvá-lo no dispositivo local.



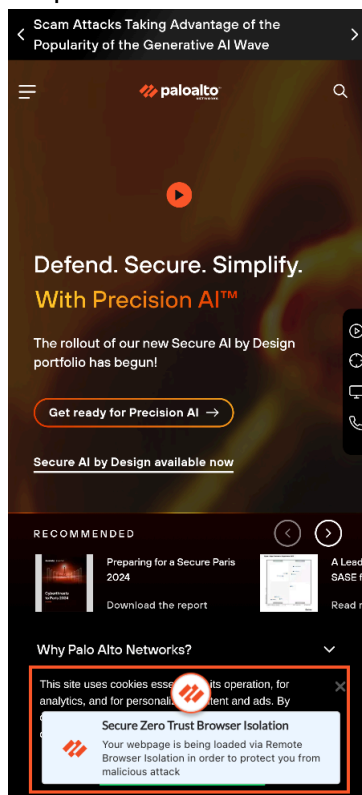
O usuário também é notificado se a política de CDR bloqueou o download do arquivo.



Experiência de navegação móvel

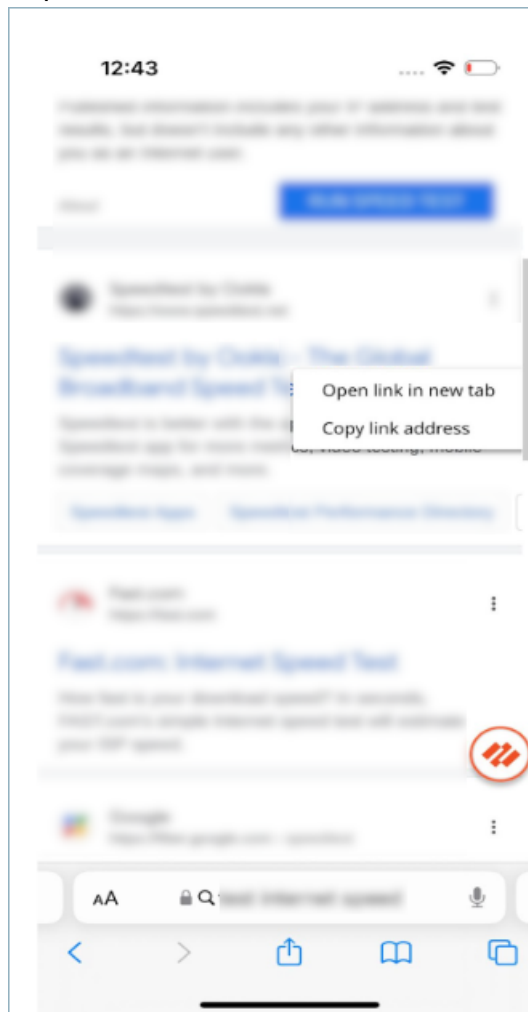
Os usuários podem usar seus dispositivos móveis para navegar em sites isoladamente. A funcionalidade do RBI em dispositivos móveis é semelhante à funcionalidade no computador, exceto pelo seguinte:

- O banner de isolamento é exibido na parte inferior da tela do dispositivo móvel.



- Ações móveis nativas, como tocar e segurar, tocar e aplicar zoom, são suportadas.

- O menu de contexto para imagens, hiperlinks ou elementos de texto pode ser acessado com um toque longo na tela do dispositivo móvel.



- O botão de ação flutuante pode ser movido tocando e arrastando-o para outro local na tela do dispositivo móvel.

A navegação remota em um dispositivo móvel tem as seguintes limitações:

- No iOS e no iPadOS, ao usar um aplicativo da Web por meio do navegador Chrome, os usuários verão uma mensagem de acesso à área de transferência sempre que interagirem com recursos que exigem acesso à área de transferência.
- Não há suporte para links diretos para acessar páginas ou recursos específicos em um aplicativo móvel usando um URL. O link somente será aberto em um navegador móvel.
- O RBI não lerá as permissões definidas pelos usuários para o aplicativo do navegador, incluindo permissões de acesso à localização, câmera, microfone e contatos.

Você pode ver a combinação de [sistemas operacionais móveis e navegadores da Web compatíveis](#) com o RBI.

Monitorar o Remote Browser Isolation

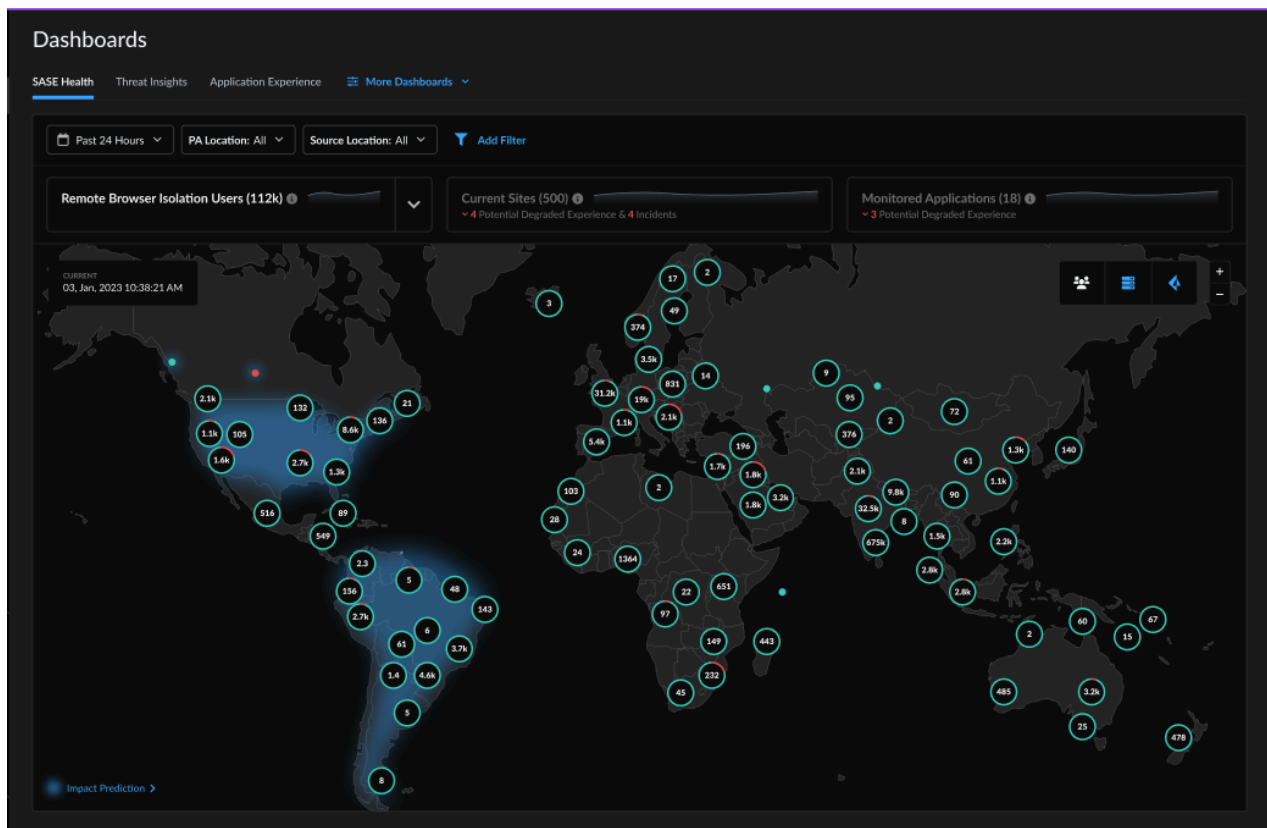
Onde posso usar isso?	O que eu preciso?
<ul style="list-style-type: none"> Prisma Access (Managed by Panorama or Strata Cloud Manager) 	<ul style="list-style-type: none"> Prisma Access 5.0 Innovation Licença do Prisma Access com a assinatura de licença de Usuário móvel ou Redes remotas Licença de isolamento remoto do navegador

Você pode usar o Strata Cloud Manager para obter visibilidade abrangente do tráfego de rede e para o Remote Browser Isolation (RBI) usando as seções [Monitor](#) (Monitorar) e [Workflows](#) (Fluxos de trabalho) do Strata Cloud Manager. Obtenha visibilidade da sua implantação do RBI exibindo métricas como o número de usuários ativos do RBI, tendências, status de conectividade, status de localização do RBI, medições de tráfego e consumo de licenças. Ao exibir dados sobre seus usuários, você pode obter uma visão geral da integridade e da conectividade da sua implantação.

Painel de integridade do SASE

Selecione **Dashboards** > **SASE Health** para monitorar a integridade geral dos seus usuários móveis que estão conectados no momento ao Prisma Access.

Selecione **Remote Browser Isolation Users** (Usuários do isolamento remoto do navegador) para mostrar a integridade geral dos usuários do RBI que estão conectados no momento ao Prisma Access. Os números nos círculos representam o número de usuários ou sites que estão conectados no momento a partir da Localização do Prisma Access onde aparecem. Um ponto representa um único usuário ou site. As áreas no mapa com um fundo azul indicam que os números mostrados nessa região são uma previsão.

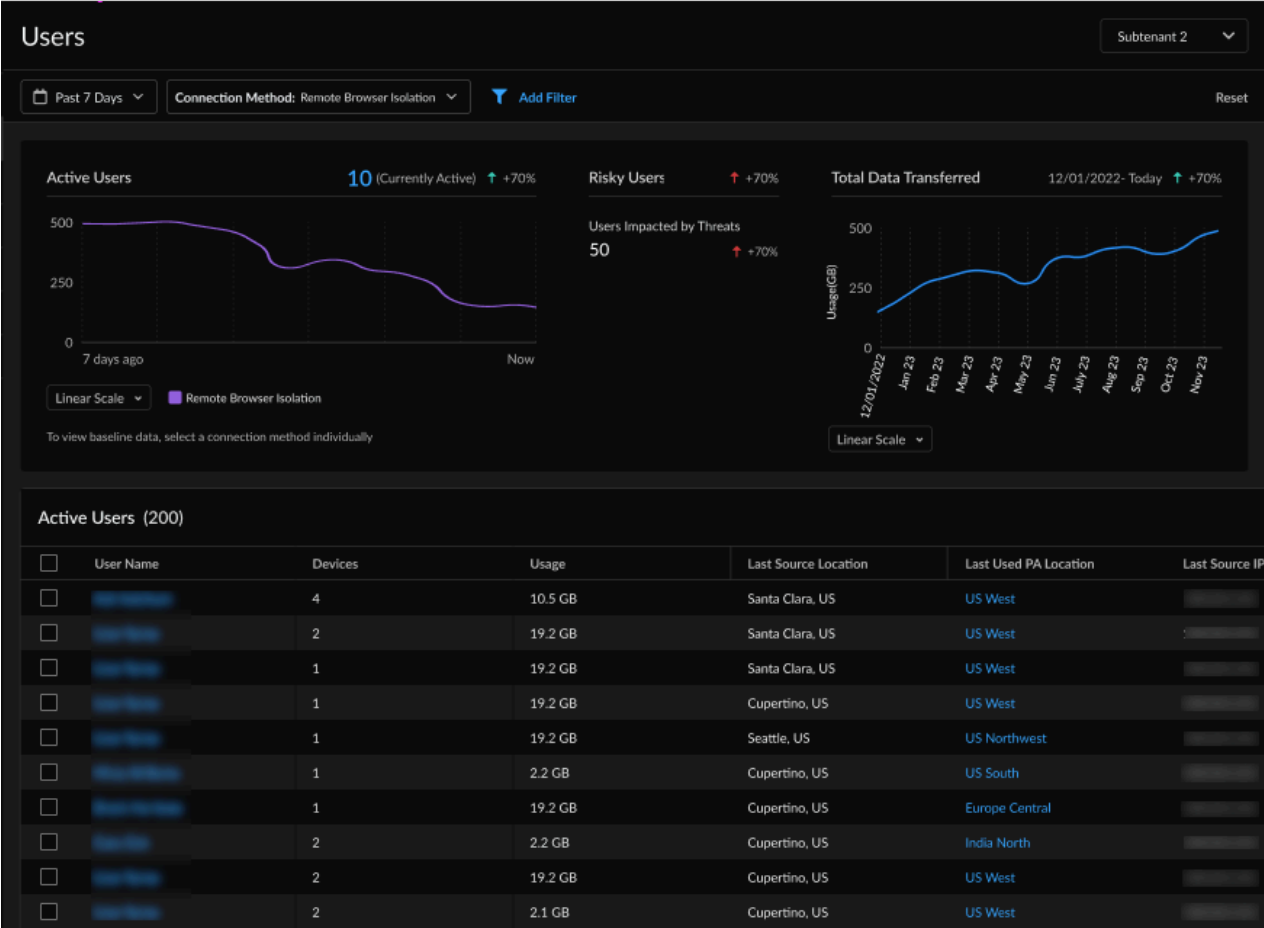


Você pode filtrar os dados mostrados nesse painel usando um ou mais dos seguintes filtros:

- Intervalo de tempo
- Localização do Prisma Access
- Localização de origem

Monitorar usuários do RBI

Selecione **Monitor > Users** para visualizar os usuários do Remote Browser Isolation (RBI) que se conectam aos serviços de segurança do Prisma Access por meio dos métodos de conexão do Prisma Access, como GlobalProtect e Explicit Proxy.



Você pode visualizar os seguintes dados de conectividade:

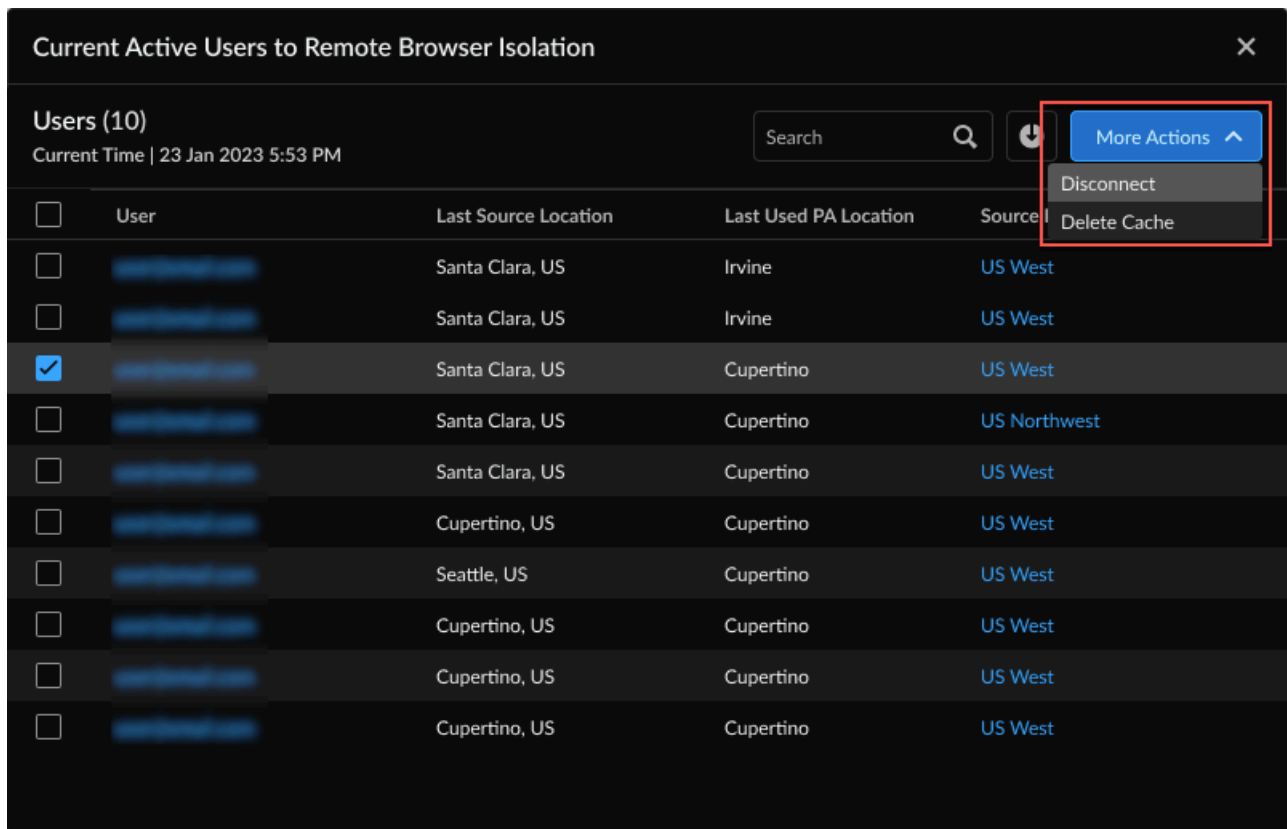
- **Connection Method** (Método de conexão): selecione **Remote Browser Isolation** para visualizar dados sobre os usuários do RBI.
- **Filters** (Filtros): você pode filtrar os usuários por:
 - Intervalo de tempo
 - Método conectado
 - Nome de usuário
 - Localização do Prisma Access
- **Active Users** (Usuários ativos): mostra o número de usuários do RBI conectados às localizações do Prisma Access no **Time Range** (Intervalo de tempo) selecionado. Passe o cursor sobre um ponto no gráfico para ver o número de usuários em um momento específico. Conhecer as tendências dos usuários em um período específico de tempo pode ajudá-lo a monitorar o uso

e investigar padrões incomuns. Por exemplo, se houver uma redução no uso, você poderá verificar se os usuários estão enfrentando problemas de desempenho do navegador.



- **Risky Users** (Usuários de risco): mostra o número de **Active Users** (Usuários ativos) impactados por ameaças. A seta para cima ou para baixo compara esse intervalo de tempo com um intervalo de tempo anterior para determinar a diferença, em porcentagem, no número de dispositivos conectados. Por exemplo, você pode monitorar a alteração na porcentagem ou nos usuários de risco para determinar se deve alertar os usuários sobre hábitos de navegação arriscados ou ajustar as configurações de isolamento para determinadas categorias de sites.
- **Currently Active** (Atualmente ativo): mostra o número de usuários do RBI que estão atualmente em sessões de navegação isoladas. Clique no número para abrir uma janela pop-up que mostra a lista de usuários ativos no momento com mais detalhes, incluindo **User** (Usuário),

Last Source Location (Última localização de origem), **Last Used PA Location** (Última localização do PA usada) e **Source IP** (IP de origem).



Current Active Users to Remote Browser Isolation

Users (10)
Current Time | 23 Jan 2023 5:53 PM

Search [] [] []

<input type="checkbox"/>	User	Last Source Location	Last Used PA Location	Source IP
<input type="checkbox"/>	[redacted]	Santa Clara, US	Irvine	US West
<input type="checkbox"/>	[redacted]	Santa Clara, US	Irvine	US West
<input checked="" type="checkbox"/>	[redacted]	Santa Clara, US	Cupertino	US West
<input type="checkbox"/>	[redacted]	Santa Clara, US	Cupertino	US Northwest
<input type="checkbox"/>	[redacted]	Santa Clara, US	Cupertino	US West
<input type="checkbox"/>	[redacted]	Cupertino, US	Cupertino	US West
<input type="checkbox"/>	[redacted]	Seattle, US	Cupertino	US West
<input type="checkbox"/>	[redacted]	Cupertino, US	Cupertino	US West
<input type="checkbox"/>	[redacted]	Cupertino, US	Cupertino	US West
<input type="checkbox"/>	[redacted]	Cupertino, US	Cupertino	US West

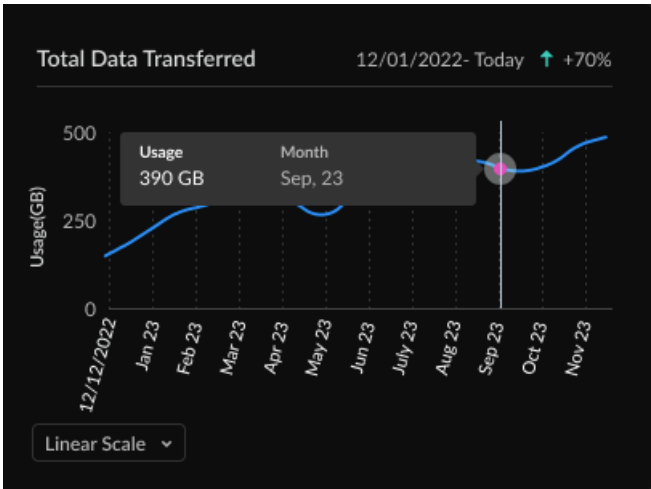
More Actions ^

- Disconnect
- Delete Cache

Nessa janela, você pode executar as seguintes ações:

- Selecione **More Actions** > **Disconnect** para desconectar um usuário do Remote Browser Isolation
- Selecione **More Actions** > **Delete Cache** para excluir o cache no navegador de isolamento remoto do usuário
- **Total Data Transferred** (Total de dados transferidos): mostra a quantidade de dados transferidos durante as sessões de navegação para todos os usuários do RBI.
 - Selecione **Count** (Contagem) na lista suspensa para mostrar o uso de dados agregados durante o período de um ano.
 - Selecione **Linear Scale** (Escala linear) no menu suspenso para mostrar a tendência da quantidade de dados transferidos durante sessões de navegação isoladas por todos os

usuários do RBI conectados durante o período de um ano. Passe o cursor sobre um ponto no gráfico para exibir o uso de dados em um mês específico.



- Tabela **Active Users** (Usuários ativos): mostra a lista de usuários que se conectaram durante o **Time Range** (Intervalo de tempo). Para cada usuário, você pode visualizar:
 - O número de dispositivos usados para navegação isolada
 - A quantidade de dados usados
 - A última localização de origem
 - A última localização do Prisma Access usada
 - O último endereço IP de origem
 - A hora do último acesso
 - O sistema operacional e a versão do sistema operacional em execução

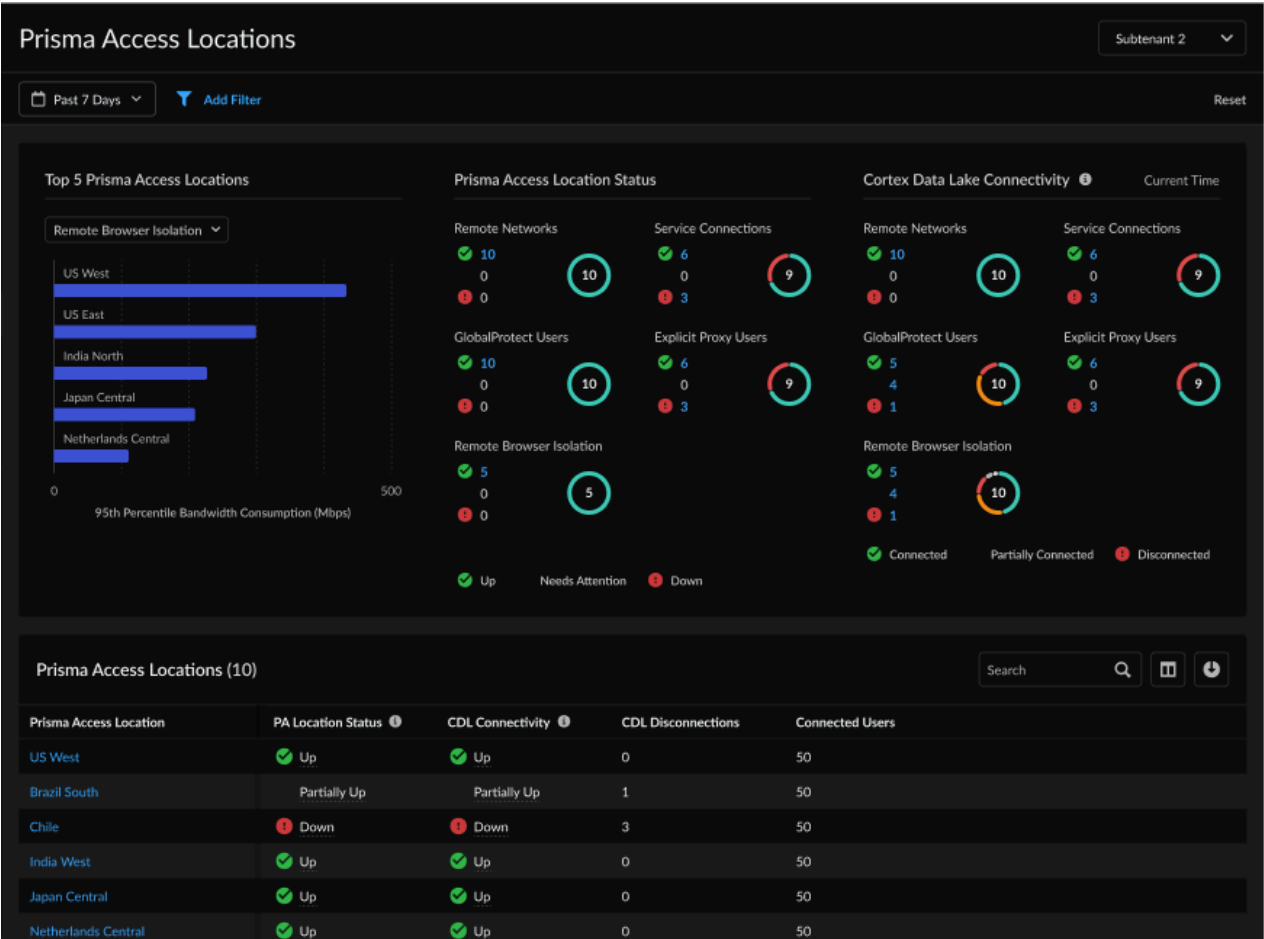
Active Users (200)								More Actions	
<input type="checkbox"/>	User Name	Devices	Usage	Last Source Location	Last Used PA Location	Last Source IP location	Last Login Time	Disconnect	Delete Cache
<input type="checkbox"/>	[Redacted]	4	10.5 GB	Santa Clara, US	US West		23 Jan 2023 10:10 AM		
<input checked="" type="checkbox"/>	[Redacted]	2	19.2 GB	Santa Clara, US	US West		23 Jan 2023 10:10 AM		
<input type="checkbox"/>	[Redacted]	1	19.2 GB	Santa Clara, US	US West		23 Jan 2023 10:10 AM		
<input type="checkbox"/>	[Redacted]	1	19.2 GB	Cupertino, US	US West		23 Jan 2023 10:10 AM		
<input type="checkbox"/>	[Redacted]	1	19.2 GB	Seattle, US	US Northwest		-		
<input type="checkbox"/>	[Redacted]	1	2.2 GB	Cupertino, US	US South		23 Jan 2023 10:10 AM		
<input type="checkbox"/>	[Redacted]	1	19.2 GB	Cupertino, US	Europe Central		23 Jan 2023 10:10 AM		
<input type="checkbox"/>	[Redacted]	2	2.2 GB	Cupertino, US	India North		23 Jan 2023 10:10 AM		
<input type="checkbox"/>	[Redacted]	2	19.2 GB	Cupertino, US	US West		23 Jan 2023 10:10 AM		
<input type="checkbox"/>	[Redacted]	2	2.1 GB	Cupertino, US	US West		23 Jan 2023 10:10 AM		
<input type="checkbox"/>	[Redacted]	2	2.2 GB	Cupertino, US	US West		23 Jan 2023 10:10 AM		
<input type="checkbox"/>	[Redacted]	2	19.2 GB	Cupertino, US	US West		23 Jan 2023 10:10 AM		
<input type="checkbox"/>	[Redacted]	3	2.1 GB	Cupertino, US	US West		23 Jan 2023 10:10 AM		
<input type="checkbox"/>	[Redacted]	6	2.2 GB	Cupertino, US	US West		23 Jan 2023 10:10 AM		

Usando **More Actions** (Mais ações), você também pode selecionar **Disconnect** (Desconectar) para desconectar um usuário do Remote Browser Isolation ou selecionar **Delete Cache** (Excluir cache) para excluir o cache do navegador de isolamento do usuário.

Para ver mais [detalhes sobre um usuário](#), selecione um **Active User** (Usuário ativo) na tabela.

Monitorar localizações do Prisma Access com RBI

Selecione **Monitor > Prisma Access Locations** para visualizar a integridade geral de todas as localizações do Prisma Access.



Você pode visualizar os seguintes dados:

- **Top 5 Prisma Access Locations** (5 principais localizações): selecione **Remote Browser Isolation** no menu suspenso para mostrar um gráfico de barras com dados sobre as cinco principais localizações do Prisma Access usadas para RBI com base na largura de banda total consumida durante o **Time Range** (Intervalo de tempo).
- **Prisma Access Location Status** (Status da localização): dependendo da sua licença, este widget mostra o número de sites de **Remote Network** (Rede remota), sites de **Service Connection** (Conexão de serviço), **GlobalProtect Users** (Usuários GlobalProtect) únicos, **Explicit Proxy Users** (Usuários de proxy explícito) e usuários únicos do **Remote Browser Isolation** conectados ao Prisma Access. O filtro de seleção **Time Range** (Intervalo de tempo) não se aplica a este widget.

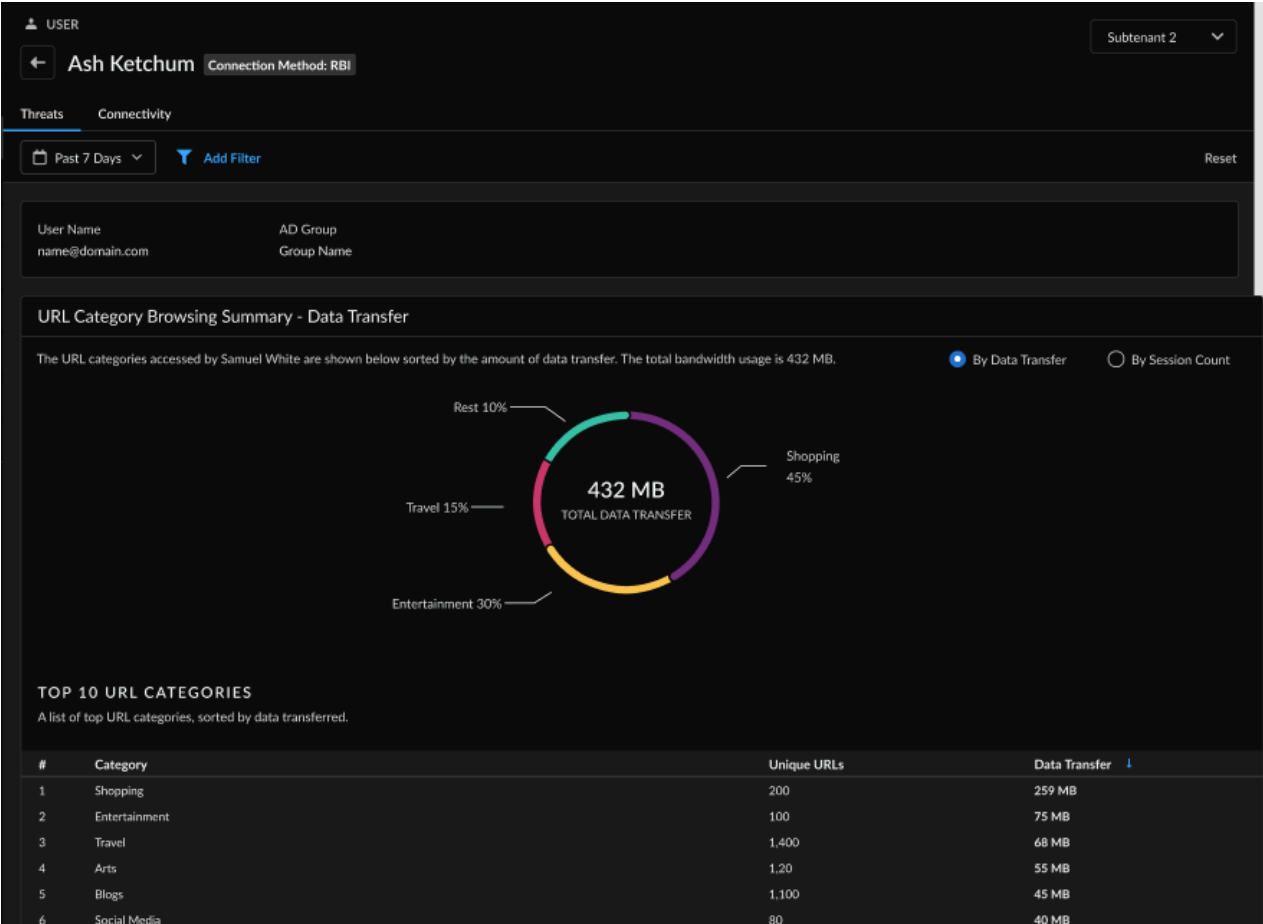
O código de cores do widget se baseia no número de usuários em cada categoria que estão no seguinte status:

- **Connected** (Conectado, verde): Todos os locais de Prisma Access estão conectados.

- **Disconnected** (Desconectado, vermelho): Todos os locais de Prisma Access estão conectados.
- **Partially Connected** (Parcialmente conectado, laranja): Uma ou mais localizações do Prisma Access estão desconectadas.
- **Strata Logging Service Connectivity**: este widget oferece visibilidade sobre o status de integridade da conectividade Strata Logging Service de todas as instâncias do Prisma Access para a região Strata Logging Service selecionada durante a ativação da licença do Prisma Access. Ajuda a determinar se os firewalls foram desconectados do Strata Logging Service e você não está mais obtendo logs de firewall. Cada locatário pode se conectar a apenas um Strata Logging Service em uma região de sua escolha. O Prisma Access verifica o banco de dados Strata Logging Service a cada 5 minutos para verificar a conectividade entre os nós (Redes Remotas, Conexões de serviço, Usuários GlobalProtect, Usuários de proxy explícito e RBI) e o banco de dados Strata Logging Service.
- **Prisma Access Location Status** (Status da localização): mostra o status das localizações do Prisma Access em tempo real. Em uma localização específica, se um usuário acessar vários hosts, ele será contado como um único usuário. No entanto, se algum usuário acessar duas localizações do Prisma Access, desconectando-se de uma e acessando outra dentro do período de tempo, ele será contado como dois usuários. Selecione uma localização para exibir detalhes, como largura de banda consumida, status, Conectividade Strata Logging Service e mapeamentos de ID de usuário e grupo.

Detalhes do usuário do RBI

Além de uma [exibição agregada dos usuários](#), você pode ver informações detalhadas sobre usuários individuais do RBI selecionando **Monitor > Users > Connection Method > Remote Browser Isolation** e selecionando um usuário na tabela **Active Users** (Usuários ativos).

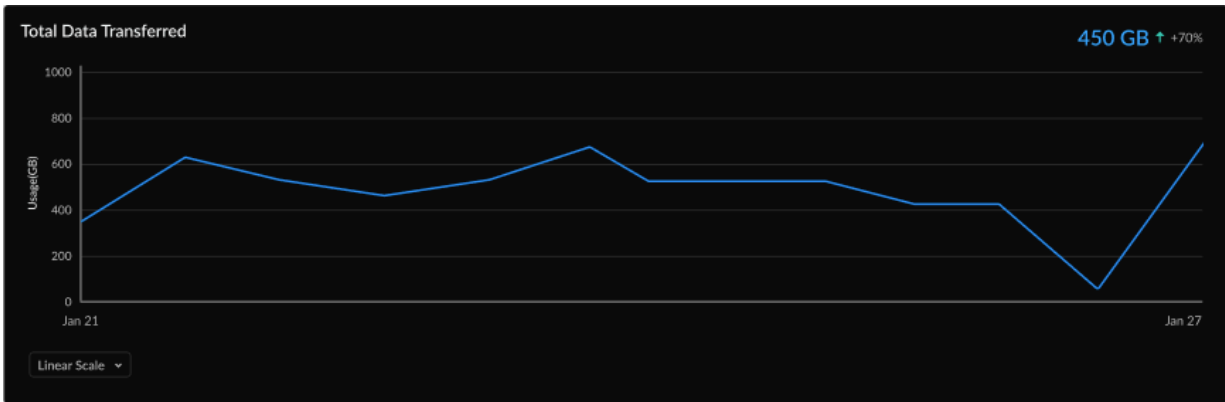


Ameaças

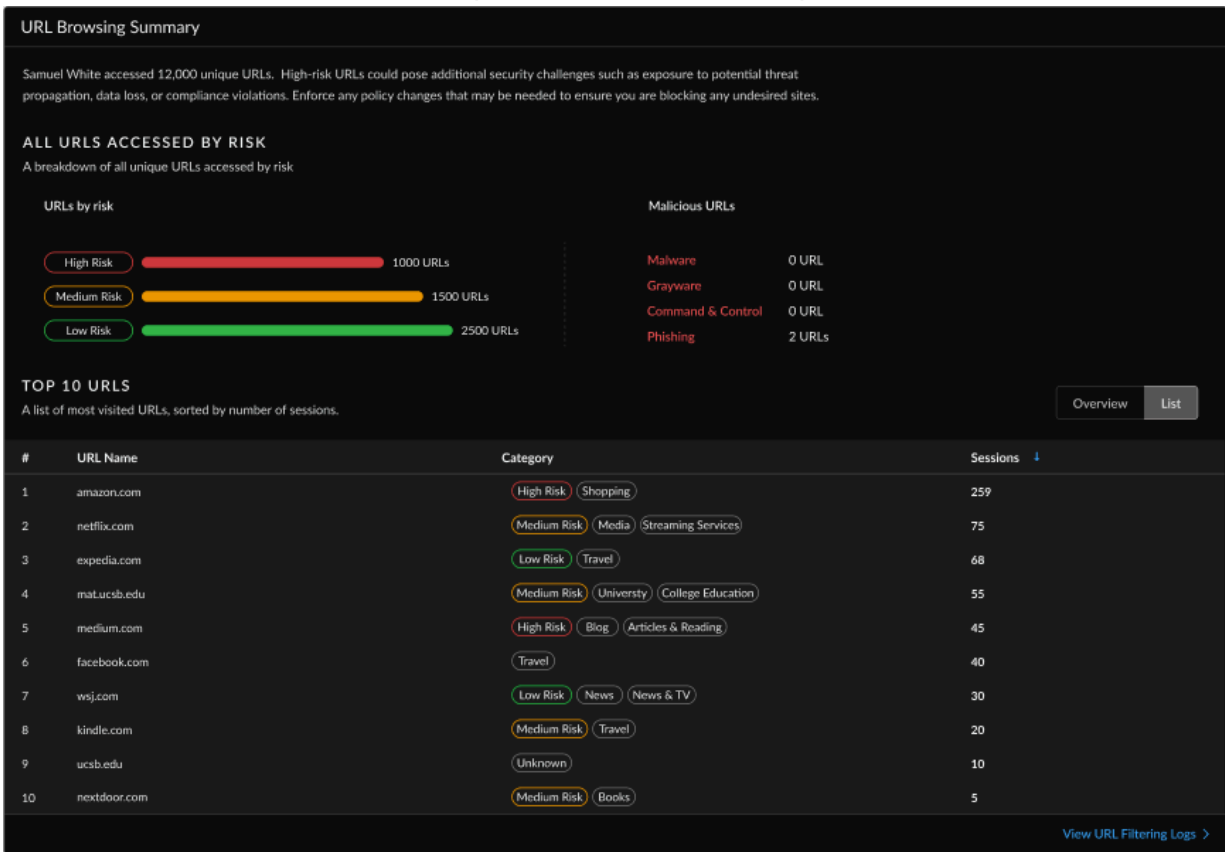
Na página de detalhes do usuário, você pode selecionar **Threats** (Ameaças) para ver um resumo da navegação por categoria de URL do usuário, incluindo:

- **URL Category Browsing Summary - Data Transfer** (Resumo de navegação da categoria de URL - Transferência de dados): mostra um resumo das categorias de URL que o usuário acessou e os dados transferidos durante essas sessões de navegação isoladas. Você pode ver este resumo **By Data Transfer** (Por transferência de dados) ou **By Session Count** (Por contagem de sessões).
- **TOP 10 URL CATEGORIES** (10 principais categorias de URL): mostra as 10 principais categorias de URL que o usuário acessou, classificadas pela quantidade de dados transferidos.

- **Total Data Transferred** (Total de dados transferidos): mostra o total de dados transferidos durante a navegação isolada para um usuário.



- **URL Browsing Summary** (Resumo da navegação de URL): mostra um resumo do histórico de navegação de URL do usuário que inclui o número de URLs visitados classificados por risco e os 10 URLs mais visitados classificados pelo número de sessões que visitaram esses URLs.



Conectividade

Na página de detalhes do usuário, selecione **Connectivity** (Conectividade) para ver uma tabela listando **User Sessions** (Sessões de usuário) para o usuário. Você pode classificar o endereço IP de origem do dispositivo do usuário, a localização do usuário, o horário de acesso, o horário de saída, a duração da sessão e a última localização do RBI usada. Você também pode selecionar **More Actions > Delete Cache** para limpar o cache no navegador isolado do usuário. Um ponto verde indica uma sessão RBI ativa.

USER

Subtenant 2

←

Ash Ketchum

Connection Method: RBI

Threats

Connectivity

Past 7 Days

Add Filter

Reset

User Sessions (10)

All Devices

Active Session

Search

More Actions

	User Source IP Address	User Location	Login Time	Logout Time	Session Duration	Last RBI Location Use	
<input type="checkbox"/>		Santa Clara, US	20 Feb 2023 8:20 PM	20 Feb 2023 8:20 PM	20h 10m 30s	US Northwest	Disconnect
<input type="checkbox"/>		Bengaluru, India	20 Feb 2023 8:20 PM	20 Feb 2023 8:20 PM	20h 10m 30s	India West	Delete Cache
<input type="checkbox"/>		Bengaluru, India	20 Feb 2023 8:20 PM	20 Feb 2023 8:20 PM	20h 10m 30s	India West	
<input type="checkbox"/>		Bengaluru, India	20 Feb 2023 8:20 PM	20 Feb 2023 8:20 PM	20h 10m 30s	India West	
<input type="checkbox"/>		Bengaluru, India	20 Feb 2023 8:20 PM	20 Feb 2023 8:20 PM	20h 10m 30s	India West	
<input type="checkbox"/>		Bengaluru, India	20 Feb 2023 8:20 PM	20 Feb 2023 8:20 PM	20h 10m 30s	India West	
<input type="checkbox"/>		Bengaluru, India	20 Feb 2023 8:20 PM	20 Feb 2023 8:20 PM	20h 10m 30s	India West	
<input type="checkbox"/>		Bengaluru, India	20 Feb 2023 8:20 PM	20 Feb 2023 8:20 PM	20h 10m 30s	India West	
<input type="checkbox"/>		Bengaluru, India	20 Feb 2023 8:20 PM	20 Feb 2023 8:20 PM	20h 10m 30s	India West	
<input type="checkbox"/>		Bengaluru, India	20 Feb 2023 8:20 PM	20 Feb 2023 8:20 PM	20h 10m 30s	India West	

10 Rows

Page 1 of 1

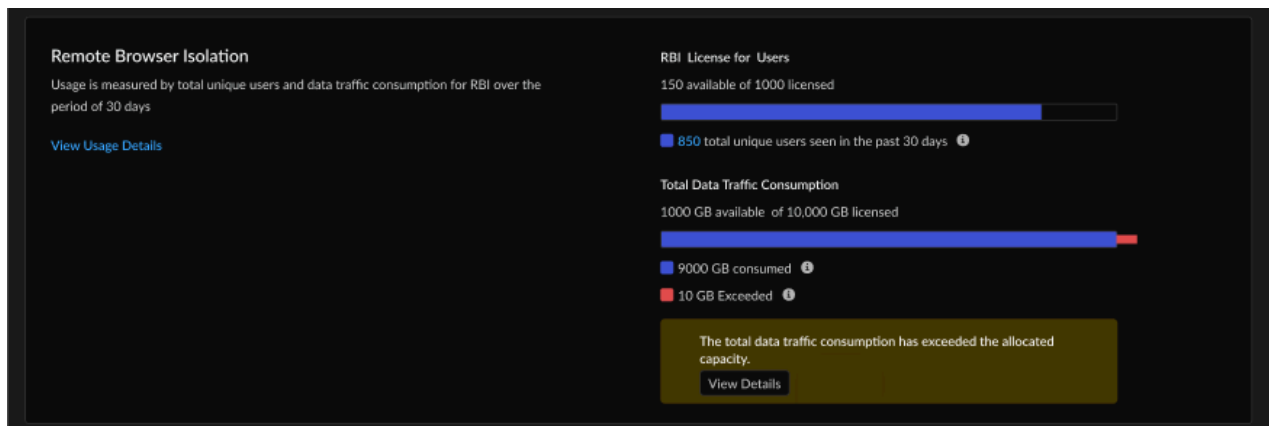
<

>

Monitorar o consumo de licenças do RBI

Você pode monitorar o consumo de licença do RBI selecionando **Monitor > Subscription Usage**. Na página Subscription Usage (Uso da assinatura), role até a seção **Remote Browser Isolation** (Isolamento remoto do navegador).

O uso do RBI é uma medida do total de usuários únicos e do tráfego consumido pelo RBI durante um período de tempo. Você pode selecionar **View Usage Details** (Ver detalhes de uso) para ir para a página [Users summary](#) (Resumo dos usuários).



Você pode monitorar dados de consumo de licenças, como:

- O número de licenças disponíveis consumidas pelos usuários do RBI.
- O número total de usuários únicos vistos nos últimos 30 dias. Um usuário único é um usuário com um nome de usuário único que acessou o Prisma Access pelo menos uma vez durante um período de tempo.
- A quantidade total de tráfego de dados consumida por todos os usuários.
- A quantidade de uso de dados que ultrapassou a capacidade alocada pela sua licença do RBI.

Logs do Remote Browser Isolation

Onde posso usar isso?	O que eu preciso?
<ul style="list-style-type: none"> Prisma Access (Managed by Panorama or Strata Cloud Manager) 	<ul style="list-style-type: none"> Prisma Access 5.0 Innovation Licença do Prisma Access com a assinatura de licença de Usuário móvel ou Redes remotas Licença de isolamento remoto do navegador

Você pode visualizar automaticamente os logs de Remote Browser Isolation (RBI) no visualizador de log do Prisma Access. O RBI captura logs e eventos de segurança, como eventos de sistema, configuração e rede, para ajudá-lo a realizar análises de ameaças, solução de problemas e auditoria do histórico de eventos do RBI.

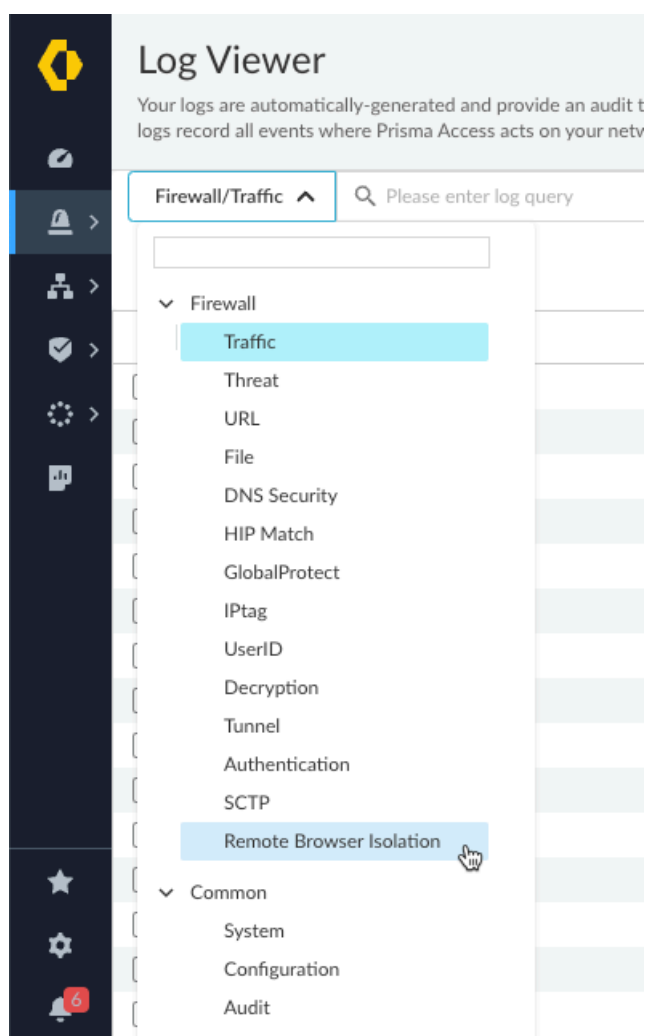
O sistema Strata Logging Service coleta e disponibiliza esses dados para o visualizador de log.

Para o RBI, um novo atributo está disponível nos logs **Firewall/Traffic** (Firewall/Tráfego) e **Firewall/Threat** (Firewall/Ameaça) para indicar que os logs se originaram no RBI. Um novo tipo de log do RBI também está disponível para registrar eventos de sessão e política.



Para saber como usar o visualizador de logs, você pode [explorar os logs](#) em detalhes.

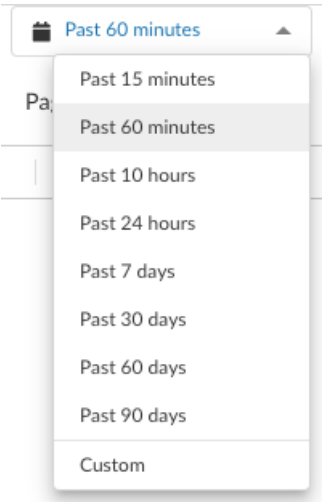
Para visualizar os logs do RBI, selecione **Incidents & Alerts > Log Viewer > Firewall > Remote Browser Isolation**.



Você pode executar as seguintes ações no visualizador de logs:

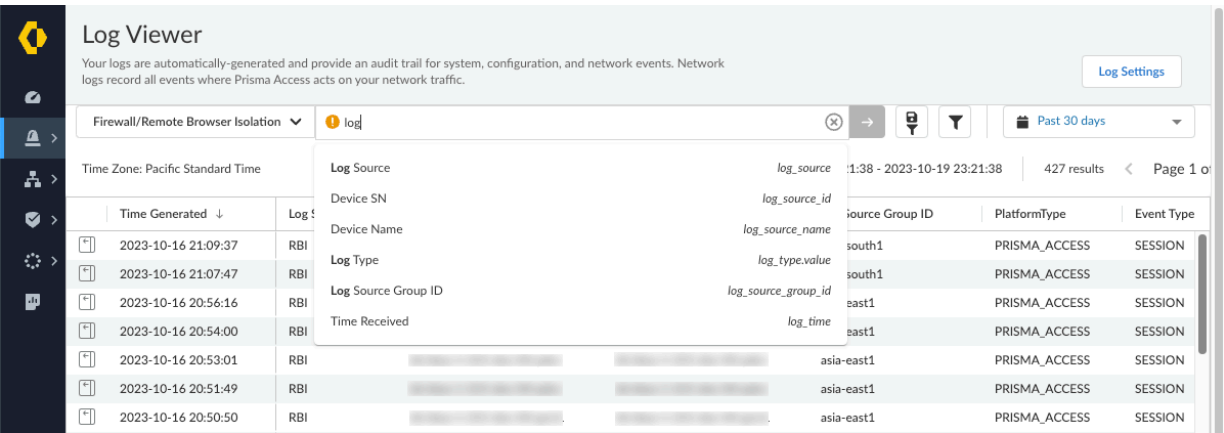
- **Definir o intervalo de tempo:** você pode usar o filtro de intervalo de tempo para especificar um intervalo de tempo para exibir entradas de log na tabela. Por exemplo, se nenhum dado aparecer na tabela, você poderá aumentar o intervalo de tempo para mostrar mais entradas.

Ou, se você quiser mostrar apenas os logs que foram gerados nas últimas 24 horas, diminua o intervalo de tempo para **Past 24 hours** (Últimas 24 horas).



- **Criar consultas de log:** para restringir o escopo dos logs mostrados na tabela, você pode criar consultas com base nos cabeçalhos das colunas ou nos campos de RBI no visualizador de log e salvar as consultas como filtros para uso posterior.

Insira uma consulta de log no campo de pesquisa. Clique no campo para exibir uma lista de campos de RBI e selecione um item na lista. Você também pode começar a digitar o nome de um campo e selecionar na lista de itens correspondentes.



Você pode criar uma consulta usando as informações no [esquema de log do RBI](#).

- **Usar operadores de consulta:** selecione um operador, como =, !=, < > ou **LIKE** (Semelhante) e um valor para o campo de consulta. Você pode expandir a consulta, adicionando operadores

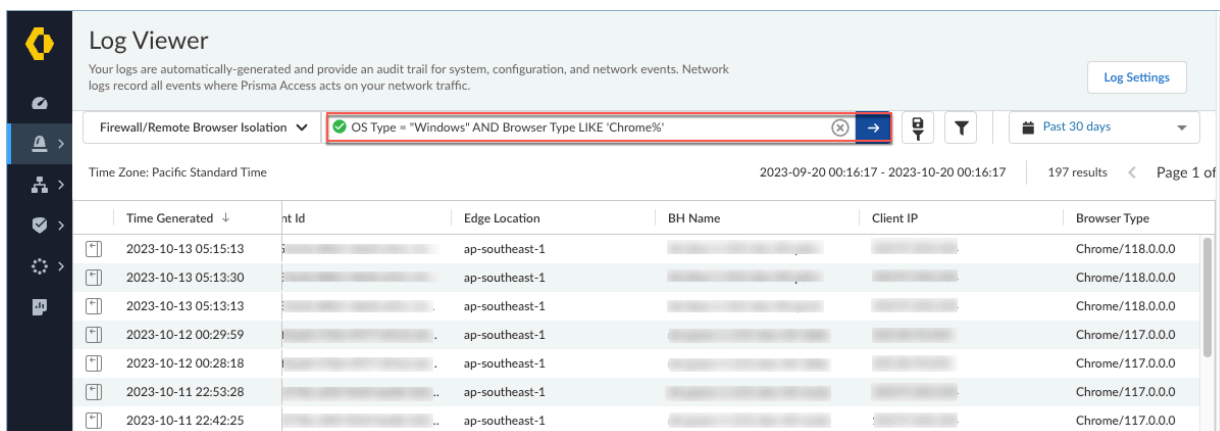
AND ou OR. Por exemplo, para consultar endpoints do macOS com uma severidade de evento de WARN (Alertar), você pode criar uma consulta como:

```
OS Type = 'MacOS' AND Event Severity = 'WARN'
```

Você pode usar o **LIKE** (Semelhante) para filtrar os valores que correspondem a um padrão inserido. Por exemplo, para ver quais versões dos navegadores Chrome os endpoints do Windows estão executando, você pode criar uma consulta como:

```
OS Type = "Windows" AND Browser Type LIKE 'Chrome%'
```

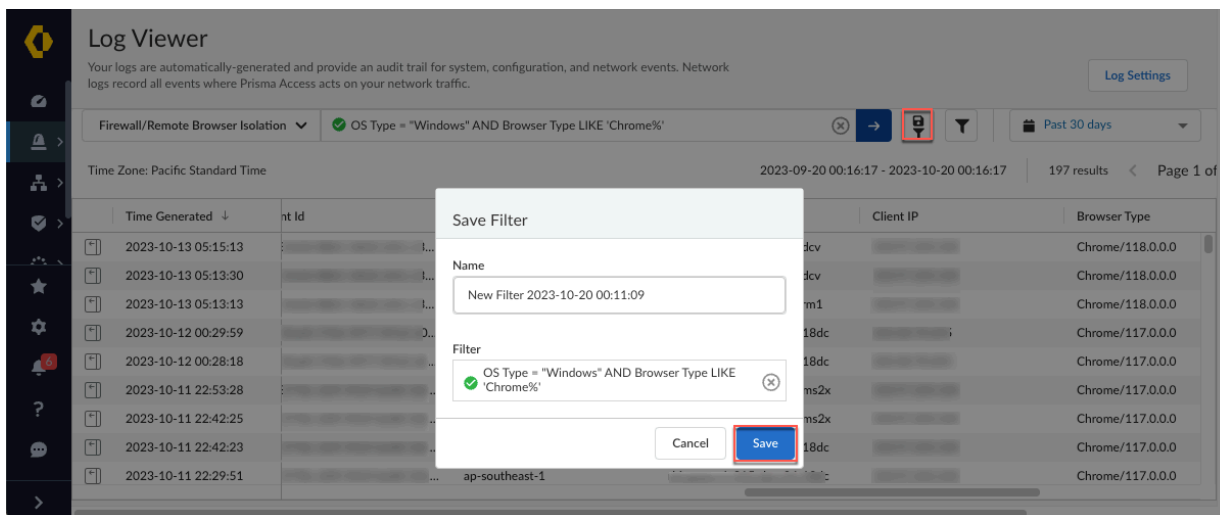
Você pode clicar na seta para a direita para iniciar a consulta.



The screenshot shows the Log Viewer interface with the search filter `OS Type = "Windows" AND Browser Type LIKE 'Chrome%'` applied. The results table shows logs for various endpoints, all with a Browser Type of Chrome/118.0.0.0 or Chrome/117.0.0.0.

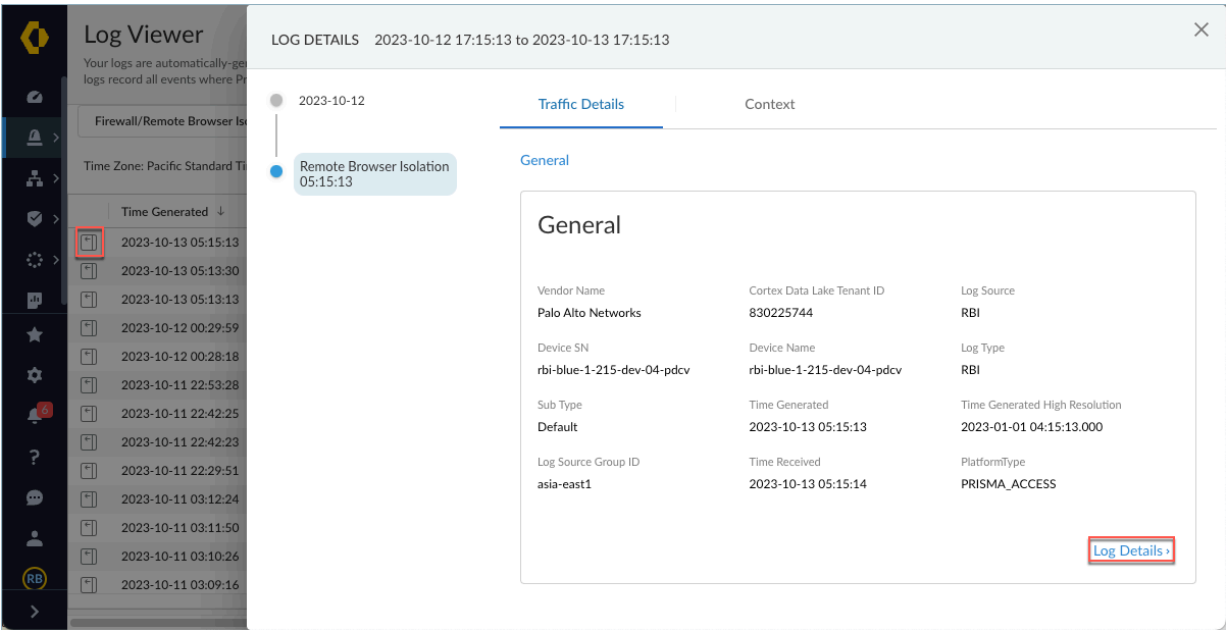
Time Generated	Event Id	Edge Location	BH Name	Client IP	Browser Type
2023-10-13 05:15:13		ap-southeast-1			Chrome/118.0.0.0
2023-10-13 05:13:30		ap-southeast-1			Chrome/118.0.0.0
2023-10-13 05:13:13		ap-southeast-1			Chrome/118.0.0.0
2023-10-12 00:29:59		ap-southeast-1			Chrome/117.0.0.0
2023-10-12 00:28:18		ap-southeast-1			Chrome/117.0.0.0
2023-10-11 22:53:28		ap-southeast-1			Chrome/117.0.0.0
2023-10-11 22:42:25		ap-southeast-1			Chrome/117.0.0.0

- **Salvar a consulta:** você pode clicar em **Save** (Salvar) para salvar a consulta como um filtro para uso futuro.



The screenshot shows the Log Viewer interface with the search filter `OS Type = "Windows" AND Browser Type LIKE 'Chrome%'` applied. A 'Save Filter' dialog box is open, allowing the user to save the current filter. The dialog box has a 'Name' field with the text 'New Filter 2023-10-20 00:11:09' and a 'Filter' field with the text `OS Type = "Windows" AND Browser Type LIKE 'Chrome%'`. The 'Save' button is highlighted.

- **Exibir detalhes do log:** para ver detalhes em um log, abra a janela LOG DETAILS (Detalhes do log) clicando no ícone ao lado de uma entrada de log na tabela.



Selecione **Log Details** (Detalhes do log) para mostrar mais detalhes no log. Selecione **Minimize** (Minimizar) para mostrar menos detalhes.

