



Guia de administração

WorkSpaces Navegador Amazon Secure



WorkSpaces Navegador Amazon Secure: Guia de administração

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens comerciais da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestige a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

Table of Contents

O que é o Amazon WorkSpaces Secure Browser?	1
Histórico de versões	1
Termos que você deve conhecer	2
Serviços relacionados	4
Arquitetura	4
Acesso	5
Configurar	6
Cadastrar e criar um usuário	6
Inscreva-se para um Conta da AWS	6
Criar um usuário com acesso administrativo	7
Conceder acesso programático	8
Redes	10
Configuração do VPC	10
Conexões de usuários	26
Conceitos básicos	29
Criação de um portal da web	29
Configurações de rede	30
Configurações de portal	30
Configurações de usuário	32
Configuração do provedor de identidade	34
Iniciar	45
Teste do portal da web	45
Distribuição do portal da web	46
Gerenciar seu portal da web	47
Visualizar detalhes do portal da web	47
Editar um portal da web	48
Excluir um portal da web	48
Gerenciar cotas de serviço	49
Solicitar um aumento de cota de serviço	50
Solicitar um aumento do portal	51
Solicitar um aumento máximo de sessões simultâneas	51
Exemplo de limite	52
Outras cotas de serviço	52
Autenticar novamente um token do IdP SAML	53

Configurar o registro de acesso do usuário	54
Exemplos de log	56
Gerenciar a política do navegador	57
Tutorial: Como configurar uma política de navegador personalizada	58
Editar a política básica do navegador	64
Configurar o editor de método de entrada	65
Configurar a localização na sessão	67
Códigos de idiomas compatíveis	68
Configurações de navegador do usuário	70
Gerenciar controles de acesso de IP	70
Criar um grupo de controle de acesso de IP	71
Associar uma configuração de acesso de IP	72
Editar um grupo de controle de acesso de IP	72
Excluir um grupo de controle de acesso de IP	73
Gerenciar a extensão de login único	73
Identificar domínios para a extensão de login único	74
Adicionar a extensão de login único a um novo portal da web	75
Adicionar a extensão de login único a um portal da web existente	75
Editar ou remover a extensão de login único	76
Configurar a filtragem de URL	76
Configurar a filtragem de URL usando o console	77
Configurar a filtragem de URL usando o editor JSON ou o upload de arquivo	77
Deep links	78
Configurar deep links	78
Utilizar a filtragem de URL para deep links	79
Painel de gerenciamento de sessões	79
Acesso ao painel	79
Filtros do painel	80
Encerrar sessões	80
Histórico da sessão	81
Proteger de dados em trânsito	81
Configurações de proteção de dados	82
Redação de dados em linha	82
Configuração de redação padrão	84
Redação básica em linha	85
Redação embutida personalizada	88

Crie configurações de proteção de dados	89
Associar configurações de proteção de dados	89
Editar configurações de proteção de dados	90
Excluir configurações de proteção de dados	91
Controles da barra de ferramentas	91
Segurança	93
Proteção de dados	94
Criptografia de dados	95
Privacidade do tráfego entre redes	104
Registro em log do acesso do usuário	105
Gerenciamento de Identidade e Acesso	105
Público	105
Autenticar com identidades	106
Gerenciar o acesso usando políticas	110
Como o Amazon WorkSpaces Secure Browser funciona com o IAM	113
Exemplos de políticas baseadas em identidade	120
AWS políticas gerenciadas	123
Solução de problemas	133
Uso de perfis vinculados ao serviço	135
Resposta a incidentes	139
Validação de conformidade	139
Resiliência	141
Segurança da infraestrutura	141
Análise de configuração e vulnerabilidade	142
Interface VPC endpoint ()AWS PrivateLink	143
Considerações sobre o Amazon WorkSpaces Secure Browser	143
Criação de uma interface VPC endpoint para o Amazon Secure Browser WorkSpaces	144
Criação de uma política de endpoint para sua interface VPC endpoint	144
Solução de problemas	145
Práticas recomendadas de segurança	145
Monitoramento	147
Monitoramento com CloudWatch	148
CloudTrail troncos	149
Informações em CloudTrail	150
Entradas do arquivo de log	151
Registro em log do acesso do usuário	153

Orientação ao usuário	154
Compatibilidade de navegadores e dispositivos	154
Acesso ao portal da web	155
Orientação da sessão	155
Iniciar uma sessão	155
Usar a barra de ferramentas	156
Usar o navegador	159
Encerrar uma sessão	159
Solução de problemas do usuário	160
Extensão de autenticação única	161
Compatibilidade de extensão de login único	162
Instalar a extensão de login único	162
Solução de problemas da extensão de login único	163
Histórico de documentos	164
.....	clxix

O que é o Amazon WorkSpaces Secure Browser?

Note

O Amazon WorkSpaces Secure Browser era conhecido anteriormente como Amazon WorkSpaces Web.

O Amazon WorkSpaces Secure Browser é um serviço de navegador hospedado, totalmente gerenciado e nativo da nuvem, usado para acessar com segurança sites privados e aplicativos web (software-as-a-service SaaS), interagir com recursos on-line e navegar na Internet a partir de um contêiner descartável. O Amazon WorkSpaces Secure Browser funciona com os navegadores da Web existentes do usuário, sem sobrecarregar a TI com o gerenciamento de dispositivos, infraestrutura, software cliente especializado ou conexões de rede privada virtual (VPN). O conteúdo da Web é transmitido para o navegador da Web do usuário, enquanto o navegador real e o conteúdo da Web são isolados em AWS. Ao usar as mesmas tecnologias subjacentes que impulsionam os serviços de computação do usuário AWS final, como Amazon WorkSpaces e Amazon AppStream 2.0, o Amazon WorkSpaces Secure Browser pode ser mais econômico do que os desktops virtuais tradicionais e reduzir a complexidade em comparação com o fornecimento de software de gerenciamento aos dispositivos da empresa. O Amazon WorkSpaces Secure Browser reduz o risco de exfiltração de dados ao transmitir conteúdo da web. Nenhum HTML, modelo de objeto de documento (DOM) ou dados confidenciais da empresa são transmitidos para a máquina local. Ao isolar o dispositivo, a rede corporativa e a Internet um do outro, a superfície de ataque do navegador é praticamente eliminada.

Você pode aplicar a política do navegador corporativo (incluindo permissão/bloqueio de URL) em todas as sessões e incluir controles em nível de sessão para área de transferência, transferência de arquivos e impressora. Você também pode restringir o acesso a redes ou dispositivos confiáveis usando controles de acesso IP. O Amazon WorkSpaces Secure Browser é fácil de configurar e operar. Cada sessão é iniciada com uma versão nova e totalmente corrigida do navegador Chrome, com políticas e configurações da empresa aplicadas.

Histórico de lançamento do Amazon WorkSpaces Secure Browser

Em 20 de maio de 2024, o Amazon WorkSpaces Web foi renomeado para Amazon WorkSpaces Secure Browser. Para os clientes existentes, não houve mudança na forma como eles gerenciam usuários ou recursos com o serviço. A lista a seguir descreve as atualizações aplicáveis que também ocorreram como resultado dessa renomeação.

O namespace da API workspaces-web permanece inalterado em termos de compatibilidade com versões anteriores. Como resultado, os seguintes recursos ainda são os mesmos:

- Comandos da CLI.
- CloudWatch Métricas da Amazon. Para obter mais informações, consulte [the section called “Monitoramento com CloudWatch”](#).
- Service endpoints. Para obter mais informações, consulte os [endpoints e cotas do Amazon WorkSpaces Secure Browser](#).
- AWS CloudFormation recursos. Para obter mais informações, consulte a [referência do tipo de recurso do Amazon WorkSpaces Secure Browser](#).
- Perfil vinculado ao serviço contendo workspaces-web. Para obter mais informações, consulte [the section called “Uso de perfis vinculados ao serviço”](#).
- Console URLs contendo espaços de trabalho-web.
- Documentação URLs contendo workspaces-web. Para obter mais informações, consulte a [documentação do Amazon WorkSpaces Secure Browser](#).
- Função ReadOnly gerenciada existente. Para obter mais informações, consulte [the section called “AWS políticas gerenciadas”](#).
- Nome da concessão do KMS.
- Prefixo de stream do Kinesis UAL (User-Activity Logging).

Além disso, o portal existente URLs permanece o mesmo. URLs <UUID>para portais criados antes de 20 de maio de 2024, usei o formato .workspaces-web.com. WorkSpaces Os portais do Secure Browser continuam usando esse formato e o domínio workspaces-web.com.

Termos a serem conhecidos ao usar o Amazon WorkSpaces Secure Browser

Para ajudá-lo a começar a usar o WorkSpaces Secure Browser, você deve se familiarizar com os conceitos a seguir.

Identity provider (IdP) (Provedor de identidade (IdP))

Um provedor de identidade verifica as credenciais de seus usuários. Em seguida, ele emite asserções de autenticação para fornecer acesso a um provedor de serviços. Você pode configurar seu IdP existente para funcionar com o WorkSpaces Secure Browser.

O processo de configuração do provedor de identidades (IdP) varia de acordo com o IdP.

Você deve carregar o arquivo de metadados do provedor de serviços no seu IdP. Caso contrário, os usuários não poderão fazer login. Você também deve conceder acesso para que seus usuários usem o Navegador WorkSpaces Seguro em seu IdP.

Documento de metadados do provedor de identidades (IdP)

WorkSpaces O Secure Browser exige metadados específicos do seu provedor de identidade (IdP) para estabelecer confiança. Você pode adicionar esses metadados ao WorkSpaces Secure Browser fazendo o upload de um arquivo de troca de metadados baixado do seu IdP.

Provedor de serviço (SP)

Um provedor de serviços aceita declarações de autenticação e fornece um serviço ao usuário. WorkSpaces O Secure Browser atua como um provedor de serviços para usuários que foram autenticados por seu IdP.

Documento de metadados do provedor do serviço (SP)

Você precisará adicionar os detalhes dos metadados do provedor de serviços à interface de configuração do provedor de identidades (IdP). Os detalhes desse processo de configuração variam entre os provedores.

SAML 2.0

Um padrão para a troca de dados de autenticação e autorização entre um IdP e um provedor de serviços.

Nuvem privada virtual (VPC)

Você pode usar uma VPC nova ou existente, sub-redes correspondentes e grupos de segurança para vincular seu conteúdo ao Secure Browser. WorkSpaces

As sub-redes devem ter uma conexão estável com a internet, e a VPC e as sub-redes também devem ter uma conexão estável com qualquer site interno e de software como serviço (SaaS) para que os usuários acessem esses recursos.

As VPCs sub-redes e os grupos de segurança listados são retirados da mesma região do console do WorkSpaces Secure Browser.

Armazenamento de confiança

Se um usuário acessando um site por meio do Navegador WorkSpaces Seguro receber um erro de privacidade, como NET: :ERR_CERT_INVALID, esse site pode estar usando um certificado

assinado por uma autoridade de certificação privada (PCA). Talvez seja necessário adicionar ou alterar o PCAs em sua loja confiável. Além disso, se o dispositivo de um usuário exigir que você instale um certificado específico para carregar um site, você precisará adicionar esse certificado ao seu armazenamento confiável para permitir que o usuário acesse esse site no Navegador WorkSpaces Seguro.

Os sites acessíveis ao público geralmente não exigem nenhuma alteração em um armazenamento confiável.

Portal da web

Um portal da web fornece aos usuários acesso a sites internos e de SaaS por meio de navegadores. É possível criar um portal da web em qualquer região com suporte por conta. Para solicitar um aumento de limite para mais de um portal, entre em contato com o suporte.

Endpoint do portal da web

O endpoint do portal da web é o ponto de acesso pelo qual os usuários iniciarão seu portal da web após fazerem login com o provedor de identidades configurado para o portal.

O endpoint está disponível publicamente na internet e pode ser incorporado à sua rede.

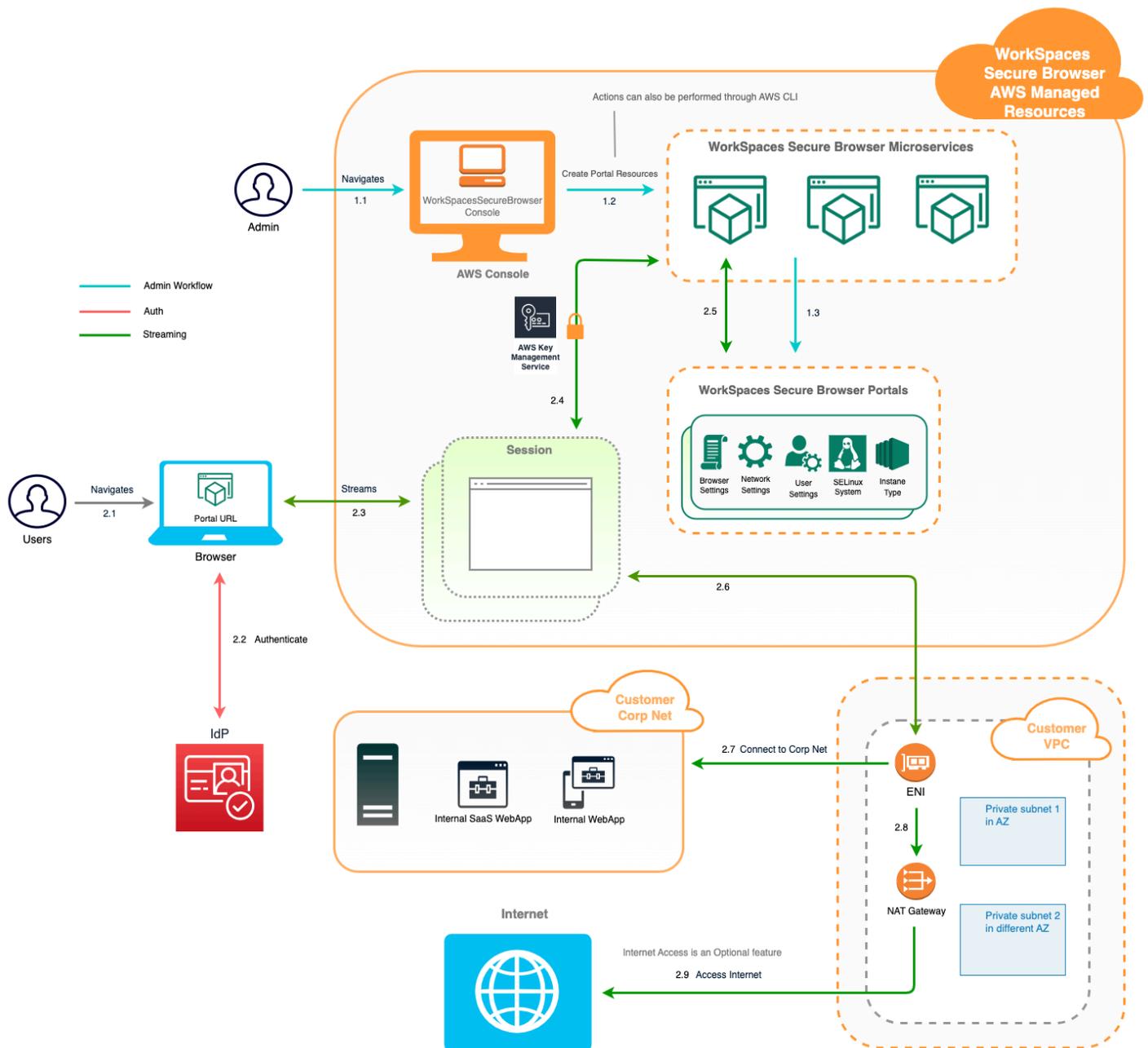
AWS serviços relacionados ao Amazon WorkSpaces Secure Browser

Existem vários AWS serviços relacionados ao WorkSpaces Secure Browser.

WorkSpaces O Secure Browser é um recurso da Amazon WorkSpaces no portfólio de computação para usuários AWS finais. Comparado com o WorkSpaces e AppStream 2.0, o WorkSpaces Secure Browser foi desenvolvido especificamente para facilitar cargas de trabalho seguras baseadas na web. WorkSpaces O Secure Browser é gerenciado automaticamente, com capacidade, escalabilidade e imagens provisionadas e atualizadas sob demanda pela AWS. Por exemplo, você pode optar por oferecer um Workspace Desktop persistente para seus desenvolvedores de software que precisam acessar os recursos do desktop e o WorkSpaces Secure Browser para os usuários do contact center que precisam acessar apenas alguns sites internos e SaaS (incluindo aqueles hospedados fora da sua rede) em computadores desktop.

Arquitetura do Amazon WorkSpaces Secure Browser

O diagrama a seguir mostra a arquitetura do WorkSpaces Secure Browser.



Acessando o Amazon WorkSpaces Secure Browser

Você pode acessar o WorkSpaces Secure Browser de várias maneiras.

Os administradores acessam o WorkSpaces Secure Browser por meio do console do WorkSpaces Secure Browser, SDK, CLI ou API. Seus usuários o acessam por meio do endpoint do WorkSpaces Secure Browser.

Configurando o Amazon WorkSpaces Secure Browser

Antes de configurar o WorkSpaces Secure Browser para acessar seus sites internos e aplicativos SaaS, você deve preencher os seguintes pré-requisitos.

Tópicos

- [Cadastrar e criar um usuário](#)
- [Conceder acesso programático](#)
- [Rede para o Amazon WorkSpaces Secure Browser](#)

Cadastrar e criar um usuário

Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

1. Abra a <https://portal.aws.amazon.com/billing/inscrição>.
2. Siga as instruções online.

Parte do procedimento de inscrição envolve receber uma ligação ou mensagem de texto e inserir um código de verificação no teclado do telefone.

Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWS é criado. O usuário-raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar [tarefas que exigem acesso de usuário-raiz](#).

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, você pode visualizar a atividade atual da sua conta e gerenciar sua conta acessando <https://aws.amazon.com/e> escolhendo Minha conta.

Criar um usuário com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS AWS IAM Identity Center, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login [AWS Management Console](#) como proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, insira a senha.

Para obter ajuda ao fazer login usando o usuário-raiz, consulte [Fazer login como usuário-raiz](#) no Guia do usuário do Início de Sessão da AWS .

2. Habilite a autenticação multifator (MFA) para o usuário-raiz.

Para obter instruções, consulte [Habilitar um dispositivo de MFA virtual para seu usuário Conta da AWS raiz \(console\) no Guia](#) do usuário do IAM.

Criar um usuário com acesso administrativo

1. Habilita o Centro de Identidade do IAM.

Para obter instruções, consulte [Habilitar o AWS IAM Identity Center](#) no Guia do usuário do AWS IAM Identity Center .

2. No Centro de Identidade do IAM, conceda o acesso administrativo a um usuário.

Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte [Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM](#) no Guia AWS IAM Identity Center do usuário.

Iniciar sessão como o usuário com acesso administrativo

- Para fazer login com o seu usuário do Centro de Identidade do IAM, use o URL de login enviado ao seu endereço de e-mail quando o usuário do Centro de Identidade do IAM foi criado.

Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte [Como fazer login no portal de AWS acesso](#) no Guia Início de Sessão da AWS do usuário.

Atribuir acesso a usuários adicionais

1. No Centro de Identidade do IAM, crie um conjunto de permissões que siga as práticas recomendadas de aplicação de permissões com privilégio mínimo.

Para obter instruções, consulte [Criar um conjunto de permissões](#) no Guia do usuário do AWS IAM Identity Center .

2. Atribua usuários a um grupo e, em seguida, atribua o acesso de autenticação única ao grupo.

Para obter instruções, consulte [Adicionar grupos](#) no Guia do usuário do AWS IAM Identity Center .

Conceder acesso programático

Os usuários precisam de acesso programático se quiserem interagir com pessoas AWS fora do AWS Management Console. A forma de conceder acesso programático depende do tipo de usuário que está acessando AWS.

Para conceder acesso programático aos usuários, selecione uma das seguintes opções:

Qual usuário precisa de acesso programático?	Para	Por
Identidade da força de trabalho (Usuários gerenciados no Centro de Identidade do IAM)	Use credenciais temporárias para assinar solicitações programáticas para o AWS CLI AWS SDKs, ou. AWS APIs	Siga as instruções da interface que deseja utilizar. <ul style="list-style-type: none"> • Para o AWS CLI, consulte Configurando o AWS CLI para uso AWS IAM Identity Center no Guia do AWS Command Line Interface usuário. • Para AWS SDKs, ferramentas e AWS APIs, consulte a autenticação do IAM Identity Center no Guia de referênci

Qual usuário precisa de acesso programático?	Para	Por
		<p>a de ferramentas AWS SDKs e ferramentas.</p>
IAM	<p>Use credenciais temporárias para assinar solicitações programáticas para o AWS CLI AWS SDKs, ou. AWS APIs</p>	<p>Siga as instruções em Como usar credenciais temporárias com AWS recursos no Guia do usuário do IAM.</p>
IAM	<p>(Não recomendado) Use credenciais de longo prazo para assinar solicitações programáticas para o AWS CLI, AWS SDKs, ou. AWS APIs</p>	<p>Siga as instruções da interface que deseja utilizar.</p> <ul style="list-style-type: none"> • Para isso AWS CLI, consulte Autenticação usando credenciais de usuário do IAM no Guia do AWS Command Line Interface usuário. • Para ferramentas AWS SDKs e ferramentas, consulte Autenticar usando credenciais de longo prazo no Guia de referência de ferramentas AWS SDKs e ferramentas. • Para isso AWS APIs, consulte Gerenciamento de chaves de acesso para usuários do IAM no Guia do usuário do IAM.

Rede para o Amazon WorkSpaces Secure Browser

Os tópicos a seguir explicam como configurar instâncias de streaming do WorkSpaces Secure Browser para que os usuários possam se conectar a elas. Também explica como habilitar suas instâncias de streaming do WorkSpaces Secure Browser para acessar recursos de VPC, bem como a Internet.

Tópicos

- [Configurando uma VPC para o Amazon WorkSpaces Secure Browser](#)
- [Habilitando conexões de usuários para o Amazon WorkSpaces Secure Browser](#)

Configurando uma VPC para o Amazon WorkSpaces Secure Browser

Para instalar e configurar uma VPC para o WorkSpaces Secure Browser, conclua as etapas a seguir.

Tópicos

- [Requisitos de VPC para o Amazon Secure WorkSpaces Browser](#)
- [Criação de uma nova VPC para o Amazon WorkSpaces Secure Browser](#)
- [Habilitando a navegação na Internet para o Amazon WorkSpaces Secure Browser](#)
- [Melhores práticas de VPC para o Secure Browser WorkSpaces](#)
- [Zonas de disponibilidade suportadas para o Amazon WorkSpaces Secure Browser](#)

Requisitos de VPC para o Amazon Secure WorkSpaces Browser

Durante a criação do portal do WorkSpaces Secure Browser, você selecionará uma VPC em sua conta. Você também deverá escolher pelo menos duas sub-redes em duas zonas de disponibilidade diferentes. Essas VPCs e as sub-redes devem atender aos seguintes requisitos:

- A VPC deve ter locação padrão. VPCs com locação dedicada não são suportadas.
- Para considerar a disponibilidade, exigimos pelo menos duas sub-redes criadas em duas zonas de disponibilidade diferentes. Suas sub-redes devem ter endereços IP suficientes para suportar o tráfego esperado do Navegador WorkSpaces Seguro. Configure cada uma das sub-redes com uma máscara de sub-rede que permita endereços IP de cliente suficientes para contabilizar o número máximo de sessões simultâneas. Para obter mais informações, consulte [Criação de uma nova VPC para o Amazon WorkSpaces Secure Browser](#).

- Todas as sub-redes devem ter uma conexão estável com qualquer conteúdo interno, localizado no local Nuvem AWS ou no local, que os usuários acessarão com o WorkSpaces Secure Browser.

Recomendamos que você escolha três sub-redes em diferentes zonas de disponibilidade para considerar a disponibilidade e a escalabilidade. Para obter mais informações, consulte [Criação de uma nova VPC para o Amazon WorkSpaces Secure Browser](#).

WorkSpaces O Secure Browser não atribui nenhum endereço IP público às instâncias de streaming para permitir o acesso à Internet. Essa ação tornaria suas instâncias de streaming acessíveis pela internet. Portanto, as instâncias de streaming conectadas à sub-rede pública não terão acesso à internet. Se você quiser que seu portal do WorkSpaces Secure Browser tenha acesso tanto ao conteúdo público da Internet quanto ao conteúdo privado da VPC, conclua as etapas em [Habilitar a navegação irrestrita na Internet para o Amazon WorkSpaces Secure Browser \(recomendado\)](#)

Criação de uma nova VPC para o Amazon WorkSpaces Secure Browser

Essa seção descreve como usar o assistente da VPC para criar uma VPC com uma sub-rede pública e uma sub-rede privada. Como parte desse processo, o assistente cria um gateway de Internet e um gateway NAT. Ele também cria uma tabela de rotas personalizada associada à sub-rede pública. Depois, ele atualiza a tabela de rotas principal associada à sub-rede privada. O gateway NAT é criado automaticamente na sub-rede pública da VPC.

Depois de usar o assistente para criar a configuração da VPC, você adicionará uma segunda sub-rede privada. Para obter mais informações sobre essa configuração, consulte [Exemplo: VPC com servidores em sub-redes privadas e NAT](#).

Tópicos

- [Alocar um endereço IP elástico](#)
- [Criar uma nova VPC](#)
- [Adicionar uma segunda sub-rede privada](#)
- [Verificar e nomear as tabelas de rotas da sub-rede](#)

Alocar um endereço IP elástico

Antes de criar sua VPC, você deve alocar um endereço IP elástico na sua região de navegador WorkSpaces seguro. Depois da alocação, associe o endereço IP elástico ao gateway NAT. Com um endereço IP elástico, você pode mascarar uma falha da instância de streaming fazendo rapidamente

um novo mapeamento do endereço para outra instância de streaming na VPC. Para obter mais informações, consulte [Endereços IP elásticos](#).

Note

Cobranças podem ser aplicadas aos endereços IP elásticos que você usa. Para obter mais informações, consulte a [Página de preços de Endereços IP elásticos](#).

Se você ainda não tiver um endereço IP elástico, conclua as etapas a seguir. Se desejar usar um endereço IP elástico existente, primeiro é necessário verificar se, no momento, ele não está associado a outra instância ou interface de rede.

Para alocar um endereço IP elástico

1. Abra o EC2 console da Amazon em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, em Rede e Segurança, escolha Elastic IPs.
3. Escolha Allocate New Address (Alocar novo endereço) e Allocate (Alocar).
4. Observe o endereço IP elástico mostrado no console.
5. No canto superior direito do IPs painel elástico, clique no ícone × para fechar o painel.

Criar uma nova VPC

Conclua as etapas a seguir para criar uma VPC com uma sub-rede pública e uma sub-rede privada.

Como criar uma nova VPC

1. Abra o console do Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, escolha VPC Dashboard (Painel da VPC).
3. Selecione Launch VPC Wizard (Iniciar o assistente de VPC).
4. Em Step 1: Select a VPC Configuration (Etapa 1: selecionar uma configuração de VPC), escolha VPC with Public and Private Subnets (VPC com sub-redes públicas e privadas) e Select (Selecionar).
5. Em Step 2: VPC with Public and Private Subnets (VPC com sub-redes públicas e privadas), configure a VPC da seguinte forma:
 - Para o bloco IPv4 CIDR, especifique um bloco IPv4 CIDR para a VPC.

- Para o bloco IPv6 CIDR, mantenha o valor padrão, Sem bloco IPv6 CIDR.
- Em Nome da VPC, insira um nome exclusivo para a VPC.
- Configure a sub-rede pública da seguinte forma:
 - Para o IPv4 CIDR da sub-rede pública, especifique o bloco CIDR para a sub-rede.
 - Em Availability Zone (Zona de disponibilidade), mantenha o valor padrão, No Preference (Sem preferência).
 - Em Nome da sub-rede pública, insira um nome para a sub-rede. Por exemplo, **.WorkSpaces Secure Browser Public Subnet**
- Configure a primeira sub-rede privada da seguinte forma:
 - Para o IPv4 CIDR da sub-rede privada, especifique o bloco CIDR para a sub-rede. Anote o valor especificado.
 - Em Availability Zone (Zona de disponibilidade), selecione uma zona específica e anote a zona selecionada.
 - Em Nome da sub-rede privada, insira um nome para a sub-rede. Por exemplo, **.WorkSpaces Secure Browser Private Subnet1**
- Mantenha os valores padrão nos campos restantes, quando aplicável.
- Em ID da alocação do IP elástico, insira o valor que corresponde ao endereço IP elástico que você criou. Esse endereço é então atribuído ao gateway NAT. Se você não tiver um endereço IP elástico, crie um usando o console da Amazon VPC em. <https://console.aws.amazon.com/vpc/>
- Em Endpoints de serviço, se um endpoint do Amazon S3 for necessário para seu ambiente, especifique um.

Para especificar um endpoint do Amazon S3, faça o seguinte:

1. Escolha Add Endpoint (Adicionar endpoint).
 2. Em Serviço, selecione com.amazonaws. **Region**Entrada.s3, onde **Region** é a entrada em Região da AWS que você está criando sua VPC.
 3. Em Subnet (Sub-rede), escolha Private subnet (Sub-rede privada).
 4. Em Policy (Política), mantenha o valor padrão, Full Access (Acesso total).
- Em Enable DNS hostnames (Habilitar nomes de host DNS), mantenha o valor padrão, Yes (Sim).
 - Em Hardware tenancy (Locação de hardware), mantenha o valor padrão, Default (Padrão).

- A configuração da VPC leva vários minutos. Após a criação da VPC, escolha OK.

Adicionar uma segunda sub-rede privada

Na etapa anterior, você criou uma VPC com uma sub-rede pública e uma sub-rede privada. Conclua as etapas a seguir para adicionar uma segunda sub-rede privada à VPC. Recomendamos que você adicione uma segunda sub-rede privada em uma zona de disponibilidade diferente da primeira sub-rede privada.

Para adicionar uma segunda sub-rede privada

1. No painel de navegação, escolha Sub-redes.
2. Selecione a primeira sub-rede privada que você criou na etapa anterior. Na guia Description (Descrição), abaixo da lista de sub-redes, anote a zona de disponibilidade dessa sub-rede.
3. No canto superior esquerdo do painel de sub-redes, escolha Create Subnet (Criar sub-rede).
4. Em Etiqueta de nome, insira um nome para a sub-rede privada. Por exemplo, **WorkSpaces Secure Browser Private Subnet2**
5. Em VPC, selecione a VPC que você criou na etapa anterior.
6. Em Zona de disponibilidade, selecione uma zona de disponibilidade diferente da que você está usando para sua primeira sub-rede privada. Selecionar uma zona de disponibilidade diferente aumenta a tolerância a falhas e ajuda a evitar erros de capacidade insuficiente.
7. Para o bloco IPv4 CIDR, especifique um intervalo exclusivo de blocos CIDR para a nova sub-rede. Por exemplo, se sua primeira sub-rede privada tiver um intervalo de blocos IPv4 CIDR de **10.0.1.0/24**, você poderá especificar um intervalo de blocos CIDR de **10.0.2.0/24** para a segunda sub-rede privada.
8. Escolha Criar.
9. Depois que a sub-rede for criada, selecione Close (Fechar).

Verificar e nomear as tabelas de rotas da sub-rede

Depois de criar e configurar a VPC, conclua as etapas a seguir para especificar um nome para as tabelas de rotas. Você precisará confirmar se as seguintes informações estão corretas em sua tabela de rotas:

- A tabela de rotas associada à sub-rede em que reside o gateway NAT deve incluir uma rota que aponta o tráfego da internet para um gateway da Internet. Isso garante que seu gateway NAT possa acessar a Internet.
- As tabelas de rota associadas às sub-redes privadas devem ser configuradas para apontar o tráfego da internet para o gateway NAT. Isso permite que as instâncias de streaming nas sub-redes privadas se comuniquem com a Internet.

Para verificar e nomear as tabelas de rotas da sub-rede

1. No painel de navegação, escolha Sub-redes e selecione a sub-rede pública que você criou. Por exemplo, WorkSpaces Secure Browser 2.0 Public Subnet.
2. Na Tabela de rotas, escolha o ID da tabela de rotas. Por exemplo, rtb-12345678.
3. Selecione a tabela de rotas. Em Nome, escolha o ícone de edição (lápis) e insira um nome para a tabela. Por exemplo, insira o nome **workspacesweb-public-routetable**. Depois, selecione a marca de seleção para salvar o nome.
4. Com a tabela de rotas públicas ainda selecionada, na guia Rotas, verifique se há duas rotas: uma para o tráfego local e outra que envie todo o outro tráfego para o gateway da Internet da VPC. A tabela a seguir descreve essas duas rotas:

Destino	Alvo	Descrição
Bloco IPv4 CIDR de sub-rede pública (por exemplo, 10.0.0/20)	Local	Todo o tráfego dos recursos destinados aos IPv4 endereços dentro do bloco IPv4 CIDR da sub-rede pública. Esse tráfego é roteado localmente dentro da VPC.
Tráfego destinado a todos os outros IPv4 endereços (por exemplo, 0.0.0.0/0)	Saída (igw-ID)	O tráfego destinado a todos os outros IPv4 endereços é roteado para o gateway da Internet (identificado pelo iGW-ID) que foi criado pelo assistente de VPC.

5. No painel de navegação, escolha Sub-redes. Depois, selecione a primeira sub-rede privada que você criou (por exemplo, **WorkSpaces Secure Browser Private Subnet1**).
6. Na guia Tabela de rotas, escolha o ID da tabela de rotas.
7. Selecione a tabela de rotas. Em Nome, escolha o ícone de edição (lápis) e insira um nome para a tabela. Por exemplo, insira o nome **workspacesweb-private-routetable**. Depois, selecione a marca de verificação para salvar o nome.
8. Na guia Routes (Rotas), verifique se a tabela de rotas inclui as seguintes rotas:

Destino	Alvo	Descrição
Bloco IPv4 CIDR de sub-rede pública (por exemplo, 10.0.0/20)	Local	Todo o tráfego dos recursos destinados aos IPv4 endereços dentro do bloco IPv4 CIDR da sub-rede pública é roteado localmente dentro da VPC.
Tráfego destinado a todos os outros IPv4 endereços (por exemplo, 0.0.0.0/0)	Saída (nat-ID)	O tráfego destinado a todos os outros IPv4 endereços é roteado para o gateway NAT (identificado pelo NAT-ID).
Tráfego destinado a buckets do S3 (aplicável se você especificou um endpoint do S3) [pl-ID (com.amazonaws.region.s3)]	Armazenamento (vpce-ID)	O tráfego destinado aos buckets do S3 é roteado para o endpoint do S3 (identificado por vpce-ID).

9. No painel de navegação, escolha Sub-redes. Depois, selecione a segunda sub-rede privada que você criou (por exemplo, **WorkSpaces Secure Browser Private Subnet2**).
10. Na guia Tabela de rotas, verifique se a tabela de rotas selecionada é a privada (por exemplo, **workspacesweb-private-routetable**). Se a tabela de rotas for diferente, escolha Editar e selecione sua tabela de rotas.

Habilitando a navegação na Internet para o Amazon WorkSpaces Secure Browser

Você pode optar por ativar a navegação irrestrita na Internet (a opção recomendada) ou a navegação restrita na Internet.

Tópicos

- [Habilitar a navegação irrestrita na Internet para o Amazon WorkSpaces Secure Browser \(recomendado\)](#)
- [Habilitando a navegação restrita na Internet para o Amazon WorkSpaces Secure Browser](#)
- [Portas de conectividade com a Internet para o Amazon WorkSpaces Secure Browser](#)

Habilitar a navegação irrestrita na Internet para o Amazon WorkSpaces Secure Browser (recomendado)

Siga estas etapas para configurar uma VPC com um gateway NAT para navegação irrestrita na internet. Isso concede ao WorkSpaces Secure Browser acesso a sites na Internet pública e sites privados hospedados em ou com uma conexão com sua VPC.

Para configurar uma VPC com um gateway NAT para navegação irrestrita na internet

Se você quiser que seu portal do WorkSpaces Secure Browser tenha acesso tanto ao conteúdo público da Internet quanto ao conteúdo privado da VPC, siga estas etapas:

Note

Se você já configurou uma VPC, conclua as etapas a seguir para adicionar um gateway NAT à VPC. Se você precisar criar uma nova VPC, consulte [Criação de uma nova VPC para o Amazon WorkSpaces Secure Browser](#).

1. Para criar o gateway NAT, conclua as etapas em [Create a NAT gateway](#). Certifique-se de que esse gateway NAT tenha conectividade pública e esteja em uma sub-rede pública na VPC.
2. Você deve especificar ao menos duas sub-redes privadas de zonas de disponibilidade diferentes. Atribuir suas sub-redes a diferentes zonas de disponibilidade ajuda a garantir melhor disponibilidade e tolerância a falhas. Para obter informações sobre como criar uma segunda sub-rede privada, consulte [the section called “ID da segunda sub-rede privada”](#).

Note

Para garantir que todas as instâncias de streaming tenham acesso à Internet, não conecte uma sub-rede pública ao portal do WorkSpaces Secure Browser.

3. Atualize a tabela de rotas associada às sub-redes privadas para apontar o tráfego vinculado à internet para o gateway NAT. Isso permite que as instâncias de streaming nas sub-redes privadas se comuniquem com a Internet. Para obter informações sobre como associar uma tabela de rotas a uma sub-rede privada, conclua as etapas em [Configurar tabelas de rotas](#).

Habilitando a navegação restrita na Internet para o Amazon WorkSpaces Secure Browser

A configuração de rede recomendada de um portal do WorkSpaces Secure Browser é usar sub-redes privadas com o gateway NAT, para que o portal possa navegar pela Internet pública e pelo conteúdo privado. Para obter mais informações, consulte [the section called “Navegação irrestrita na Internet”](#). No entanto, talvez seja necessário controlar a comunicação de saída de um portal do Navegador WorkSpaces Seguro para a Internet usando um proxy da web. Por exemplo, se você usar um proxy da Web como gateway para a Internet, poderá implementar controles preventivos de segurança, como lista de permissões de domínio e filtragem de conteúdo. Isso também pode reduzir o uso da largura de banda e melhorar o desempenho da rede armazenando em cache recursos acessados com frequência, como páginas da Web ou atualizações de software localmente. Para alguns casos de uso, você pode ter conteúdo privado que só pode ser acessado por meio de um proxy da Web.

Talvez você já esteja familiarizado com a configuração de proxy em dispositivos gerenciados ou na imagem de seus ambientes virtuais. Mas isso representará desafios se você não estiver no controle do dispositivo (por exemplo, quando os usuários estão em dispositivos que não são de propriedade ou gerenciados pela empresa) ou se você precisar gerenciar a imagem em seu ambiente virtual. Com o Navegador WorkSpaces Seguro, você pode definir configurações de proxy usando as políticas do Chrome incorporadas ao navegador da web. Você pode fazer isso configurando um proxy de saída HTTP para o WorkSpaces Secure Browser.

Essa solução é baseada em uma configuração recomendada de proxy VPC de saída. A solução de proxy é baseada no proxy HTTP de código aberto [Squid](#). Em seguida, ele usa as configurações do navegador WorkSpaces Secure Browser para configurar o portal do WorkSpaces Secure Browser para se conectar ao endpoint do proxy. Para obter mais informações, consulte [Como configurar um proxy VPC de saída com lista de permissões de domínio e filtragem de conteúdo](#).

Essa solução oferece a você os seguintes benefícios:

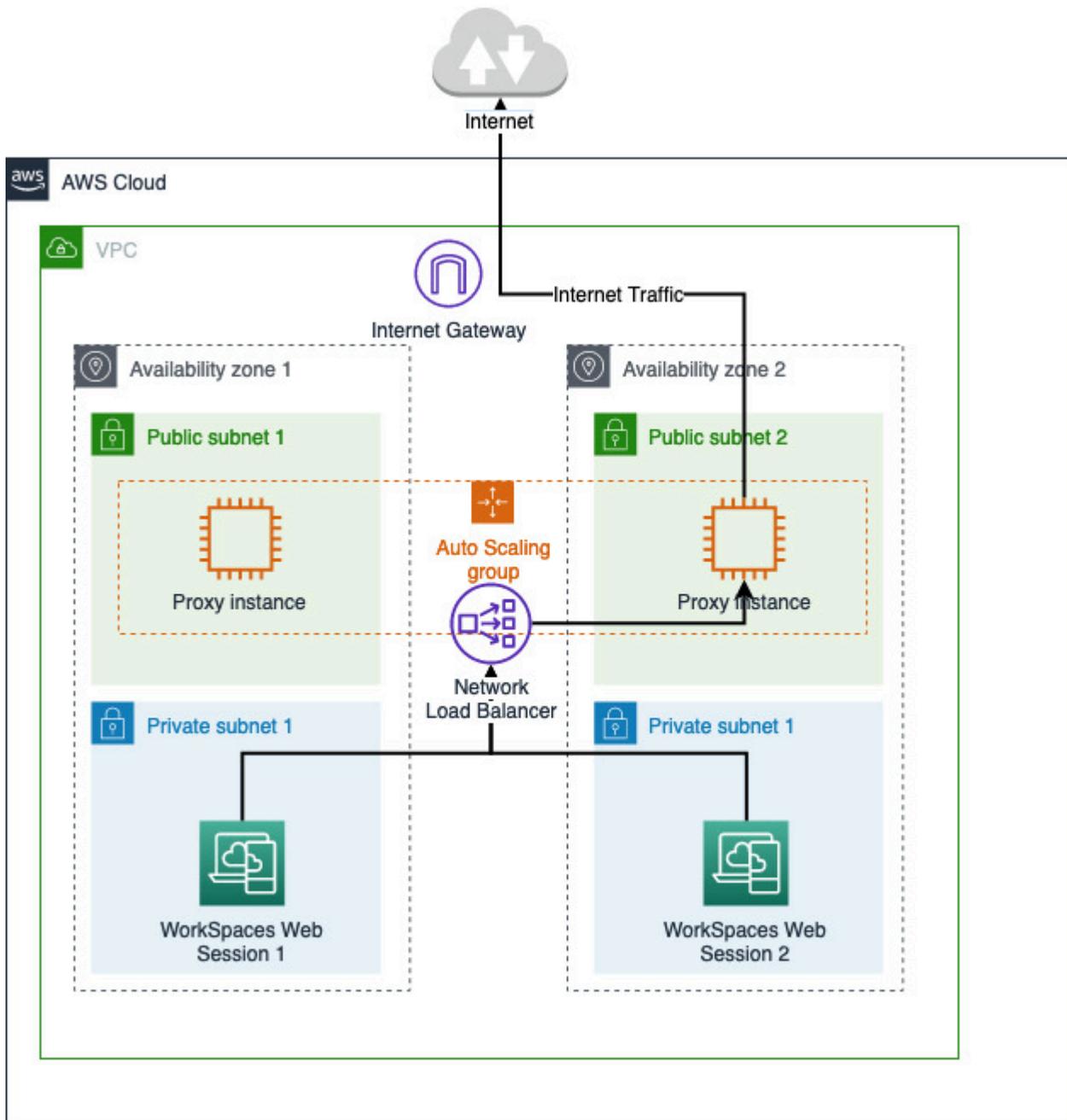
- Um proxy de saída que inclui um grupo de instâncias EC2 Amazon com escalabilidade automática, hospedadas por um balanceador de carga de rede. As instâncias de proxy residem em uma sub-rede pública e cada uma delas é conectada com um IP elástico, para permitir o acesso à Internet.
- Um portal do WorkSpaces Secure Browser implantado em sub-redes privadas. Você não precisa configurar o gateway NAT para habilitar o acesso à Internet. Em vez disso, você configura a política do seu navegador para que todo o tráfego da Internet passe pelo proxy de saída. Se você quiser usar seu próprio proxy, a configuração do portal do WorkSpaces Secure Browser será semelhante.

Tópicos

- [Arquitetura de navegação restrita na Internet para o Amazon WorkSpaces Secure Browser](#)
- [Pré-requisitos de navegação restrita na Internet para o Amazon Secure Browser WorkSpaces](#)
- [Proxy de saída HTTP para o Amazon WorkSpaces Secure Browser](#)
- [Solução de problemas de navegação restrita na Internet para o Amazon WorkSpaces Secure Browser](#)

Arquitetura de navegação restrita na Internet para o Amazon WorkSpaces Secure Browser

Veja a seguir um exemplo de uma configuração de proxy típica na sua VPC. A EC2 instância proxy da Amazon está em sub-redes públicas e associada ao Elastic IP, então eles têm acesso à Internet. Um balanceador de carga de rede hospeda um grupo de instâncias de proxy com ajuste de escala automático. Isso garante que as instâncias de proxy possam ser escaladas automaticamente e que o balanceador de carga de rede seja o único endpoint de proxy, que pode ser consumido pelas sessões do WorkSpaces Secure Browser.



Pré-requisitos de navegação restrita na Internet para o Amazon Secure Browser WorkSpaces

Antes começar, certifique-se de que os seguintes pré-requisitos sejam atendidos:

- Você precisa de uma VPC já implantada, com sub-redes públicas e privadas espalhadas por várias zonas de disponibilidade (). AZs [Para obter mais informações sobre como configurar seu ambiente VPC, consulte Padrão. VPCs](#)

- Você precisa de um único endpoint de proxy que seja acessível a partir de sub-redes privadas, onde estão as sessões do WorkSpaces Secure Browser (por exemplo, o nome DNS do balanceador de carga de rede). Se você quiser usar um proxy existente, certifique-se de que ele também tenha um único endpoint acessível a partir de suas sub-redes privadas.

Proxy de saída HTTP para o Amazon WorkSpaces Secure Browser

Para configurar um proxy de saída HTTP para o WorkSpaces Secure Browser, siga estas etapas.

1. Para implantar um exemplo de proxy de saída em sua VPC, siga as etapas em [Como configurar um proxy VPC de saída com lista de permissões de domínio e filtragem de conteúdo](#).
 - a. Siga as etapas em “Instalação (configuração única)” para implantar o CloudFormation modelo em sua conta. Certifique-se de escolher a VPC e as sub-redes corretas como parâmetros do modelo. CloudFormation
 - b. Após a implantação, encontre o parâmetro CloudFormation de saída `OutboundProxyDomainOutboundProxyPorte`. Esse é o nome e a porta DNS do seu proxy.
 - c. Se você já tem seu próprio proxy, pule esta etapa e use o nome e a porta DNS do seu proxy.
2. No console do Navegador WorkSpaces Seguro, selecione seu portal e, em seguida, escolha Editar.
 - a. Nos detalhes da conexão de rede, escolha a VPC e as sub-redes privadas que têm acesso ao proxy.
 - b. Nas configurações de política, adicione a ProxySettings política a seguir usando um editor JSON. O campo `ProxyServer` deve ser o nome e a porta DNS do seu proxy. Para obter mais detalhes sobre a ProxySettings política, consulte [ProxySettings](#).

```
{
  "chromePolicies":
  {
    ...
    "ProxySettings": {
      "value": {
        "ProxyMode": "fixed_servers",
        "ProxyServer": "OutboundProxyLoadBalancer-0a01409a46943c47.elb.us-
west-2.amazonaws.com:3128",
        "ProxyBypassList": "https://www.example1.com,https://
www.example2.com,https://internalsite/"
      }
    },
  },
}
```

```
}  
}
```

3. Na sua sessão do Navegador WorkSpaces Seguro, você verá que o proxy é aplicado à configuração do Chrome. O Chrome está usando as configurações de proxy do seu administrador.
4. Acesse `chrome://policy` e a guia Política do Chrome para confirmar que a política foi aplicada.
5. Verifique se sua sessão do WorkSpaces Secure Browser pode navegar com êxito pelo conteúdo da Internet sem o gateway NAT. Nos CloudWatch Registros, verifique se os registros de acesso ao proxy do Squid estão registrados.

Solução de problemas de navegação restrita na Internet para o Amazon WorkSpaces Secure Browser

Depois que a política do Chrome for aplicada, se sua sessão do Navegador WorkSpaces Seguro ainda não conseguir acessar a Internet, siga estas etapas para tentar resolver o problema:

- Verifique se o endpoint do proxy está acessível a partir das sub-redes privadas em que seu portal do WorkSpaces Secure Browser está localizado. Para fazer isso, crie uma EC2 instância na sub-rede privada e teste a conexão da EC2 instância privada com seu endpoint de proxy.
- Verifique se o proxy tem acesso à Internet.
- Verifique se a política do Chrome está correta.
 - Confirme a formatação a seguir para o campo `ProxyServer` da política: `<Proxy DNS name>:<Proxy port>`. Não deve haver `http://` ou `https://` no prefixo.
 - Na sessão do Navegador WorkSpaces seguro, use o Chrome para navegar até `chrome://policy` e certifique-se de que a `ProxySettings` política seja aplicada com sucesso.

Portas de conectividade com a Internet para o Amazon WorkSpaces Secure Browser

Cada instância de streaming do WorkSpaces Secure Browser tem uma interface de rede do cliente que fornece conectividade aos recursos em sua VPC, bem como à Internet, se sub-redes privadas com gateway NAT estiverem configuradas.

Para conectividade com a Internet, as portas a seguir devem ser abertas para todos os destinos. Se você estiver usando um grupo de segurança personalizado ou modificado, será necessário adicionar as regras exigidas manualmente. Para obter mais informações, consulte [Regras de grupos de segurança](#).

Note

Isso se aplica ao tráfego de saída.

- TCP 80 (HTTP)
- TCP 443 (HTTPS)
- UDP 8433

Melhores práticas de VPC para o Secure Browser WorkSpaces

As recomendações a seguir podem ajudá-lo a configurar sua VPC de forma mais eficaz e segura.

Configuração geral da VPC

- Verifique se a configuração da VPC pode satisfazer suas necessidades de escalabilidade.
- Certifique-se de que as cotas do serviço WorkSpaces Secure Browser (também chamadas de limites) sejam suficientes para atender à demanda prevista. Para solicitar um aumento de cota, você pode usar o console Service Quotas em <https://console.aws.amazon.com/servicequotas/>. Para obter informações sobre as cotas padrão do WorkSpaces Secure Browser, consulte [the section called “Gerenciar cotas de serviço”](#).
- Se você planeja conceder acesso à internet para suas sessões de streaming, é recomendável configurar uma VPC com um gateway NAT em uma sub-rede pública.

Interfaces de rede elástica

- Cada sessão do WorkSpaces Secure Browser requer sua própria interface de elastic network durante a duração do streaming. WorkSpaces O Secure Browser cria tantas [interfaces de rede elásticas](#) (ENIs) quanto a capacidade máxima desejada de sua frota. Por padrão, o limite ENIs por região é 5000. Para obter mais informações, consulte [Interfaces de rede](#).

Ao planejar a capacidade para implantações muito grandes, por exemplo, milhares de sessões de streaming simultâneas, considere o número ENIs que pode ser necessário para seu uso máximo. Recomendamos manter o limite de ENI igual ou superior ao limite máximo de uso simultâneo configurado para seu portal da web.

Sub-redes

- Ao desenvolver seu plano para aumentar a escala de usuários, lembre-se de que cada sessão do WorkSpaces Secure Browser exige um endereço IP de cliente exclusivo das sub-redes configuradas. Portanto, o tamanho do espaço de endereço IP do cliente configurado em suas sub-redes define o número de usuários que podem fazer streaming de maneira simultânea.
- Recomendamos que cada sub-rede seja configurada com uma máscara de sub-rede que permita endereços IP de cliente suficientes para contabilizar o número máximo de usuários simultâneos esperados. Além disso, considere adicionar mais endereços IP para comportar o crescimento previsto. Para obter mais informações, consulte [Dimensionamento de VPC e sub-rede](#) para IPv4.
- Recomendamos que você configure uma sub-rede em cada zona de disponibilidade exclusiva que o WorkSpaces Secure Browser suporta na região desejada para considerar a disponibilidade e a escalabilidade. Para obter mais informações, consulte [the section called “Criar uma nova VPC”](#).
- Verifique se os recursos de rede necessários para suas aplicações web podem ser acessados pelas sub-redes.

Grupos de segurança

- Use grupos de segurança para fornecer controle de acesso adicional à sua VPC.

Os grupos de segurança que pertencem à sua VPC permitem que você controle o tráfego de rede entre as instâncias de streaming do WorkSpaces Secure Browser e os recursos de rede exigidos pelos aplicativos web. Verifique se os grupos de segurança fornecem acesso aos recursos de rede que as aplicações web exigem.

Zonas de disponibilidade suportadas para o Amazon WorkSpaces Secure Browser

Ao criar uma nuvem privada virtual (VPC) para uso com o WorkSpaces Secure Browser, as sub-redes da VPC devem residir em diferentes zonas de disponibilidade na região em que você está iniciando o Secure Browser. WorkSpaces As zonas de disponibilidade são locais distintos projetados para serem isolados de falhas em outras zonas de disponibilidade. Ao iniciar as instâncias em zonas de disponibilidade separadas, você pode proteger seus aplicativos de falhas de um único local. Cada sub-rede deve residir inteiramente dentro de uma zona de disponibilidade e não pode abranger zonas. Recomendamos configurar uma sub-rede para cada AZ compatível na região desejada para obter máxima resiliência

Uma zona de disponibilidade é representada por um código de região seguido por um identificador de letra, por exemplo, us-east-1a. Para garantir a distribuição de recursos entre as zonas de disponibilidade de uma região, mapeamos as zonas de disponibilidade de forma independente para

os nomes de cada conta da AWS . Por exemplo, a zona de disponibilidade da us-east-1a para sua conta da AWS pode não ter o mesmo local que a us-east-1a de outra conta da AWS .

Para coordenar as zonas de disponibilidade entre contas, use o ID da AZ que é um identificador exclusivo e consistente para uma zona de disponibilidade. Por exemplo, use1-az2 é uma ID AZ para a us-east-1 região e tem a mesma localização em todas as AWS contas.

A visualização do AZ IDs permite determinar a localização dos recursos em uma conta em relação aos recursos em outra conta. Por exemplo, se você compartilhar uma sub-rede na zona de disponibilidade com o ID de AZ use1-az2 com outra conta, essa sub-rede estará disponível para essa conta na zona de disponibilidade cujo ID de AZ também é use1-az2. O ID da AZ de cada VPC e sub-rede é exibido no console da Amazon VPC.

WorkSpaces O Navegador Seguro está disponível em um subconjunto das zonas de disponibilidade para cada região compatível. A tabela a seguir lista as AZ IDs que você pode usar para cada região. Para ver o mapeamento de AZ IDs para zonas de disponibilidade em sua conta, consulte [AZ IDs para seus recursos](#) no Guia do AWS RAM usuário.

Nome da região	Código da região	AZ suportado IDs
Leste dos EUA (N. da Virgínia)	us-east-1	use1-az1, use1-az2, use1-az4, use1-az5, use1-az6
Oeste dos EUA (Oregon)	us-west-2	usw2-az1, usw2-az2, usw2-az3
Ásia-Pacífico (Mumbai)	ap-south-1	aps1-az1, aps1-az3
Ásia-Pacífico (Singapura)	ap-southeast-1	apse1-az1 , apse1-az2 , apse1-az3
Ásia-Pacífico (Sydney)	ap-southeast-2	apse2-az1 , apse2-az2 , apse2-az3
Ásia-Pacífico (Tóquio)	ap-northeast-1	apne1-az1 , apne1-az2 , apne1-az4
Canadá (Central)	ca-central-1	cac1-az1, cac1-az2, cac1-az4

Nome da região	Código da região	AZ suportado IDs
Europa (Frankfurt)	eu-central-1	euc1-az2, euc1-az2, euc1-az3
Europa (Irlanda)	eu-west-1	euw1-az1, euw1-az2, euw1-az3
Europa (Londres)	eu-west-2	euw2-az1, euw2-az2

Para obter mais informações sobre Zonas de disponibilidade e AZ IDs, consulte [Regiões, Zonas de disponibilidade e Zonas Locais](#) no Guia EC2 do usuário da Amazon.

Habilitando conexões de usuários para o Amazon WorkSpaces Secure Browser

WorkSpaces O Secure Browser está configurado para rotear conexões de streaming pela Internet pública. A conectividade com a Internet é necessária para autenticar os usuários e fornecer os ativos da Web que o WorkSpaces Secure Browser exige para funcionar. Para permitir esse tráfego, você deve inserir os domínios listados em [Domínios permitidos para o Amazon WorkSpaces Secure Browser](#).

Os tópicos a seguir fornecem informações sobre como habilitar conexões de usuário com o WorkSpaces Secure Browser.

Tópicos

- [Requisitos de endereço IP e porta para o Amazon WorkSpaces Secure Browser](#)
- [Domínios permitidos para o Amazon WorkSpaces Secure Browser](#)

Requisitos de endereço IP e porta para o Amazon WorkSpaces Secure Browser

Para acessar as instâncias do WorkSpaces Secure Browser, os dispositivos do usuário precisam de acesso de saída nas seguintes portas:

- Porta 443 (TCP)
 - A porta 443 é usada para comunicação HTTPS entre dispositivos de usuário e instâncias de streaming ao usar os endpoints de internet. Normalmente, quando os usuários finais navegam

na web durante sessões de streaming, o navegador da web seleciona aleatoriamente uma porta de origem no intervalo para streaming de tráfego. Você deve garantir que o tráfego de retorno para essa porta seja permitido.

- Essa porta deve estar aberta para os domínios exigidos listados em [Domínios permitidos para o Amazon WorkSpaces Secure Browser](#).
- AWS publica seus intervalos de endereços IP atuais, incluindo os intervalos para os quais o Session Gateway e CloudFront os domínios podem resolver, no formato JSON. Para obter informações sobre como baixar o arquivo.json e visualizar os intervalos atuais, consulte [Intervalos de endereços IP da AWS](#). Ou, se estiver usando AWS Tools for Windows PowerShell, você pode acessar as mesmas informações usando o Get-AWSPublicIpAddressRange PowerShell comando. Para obter mais informações, consulte [Consultar intervalos de endereços IP públicos para a AWS](#).
- (Opcional) Porta 53 (UDP)
 - A porta 53 é usada para comunicação entre dispositivos de usuário e os servidores DNS.
 - Essa porta é opcional se você não estiver usando servidores DNS para resolução de nomes de domínio.
 - A porta deve estar aberta para os endereços IP dos seus servidores DNS, de forma que os nomes de domínio público possam ser resolvidos.

Domínios permitidos para o Amazon WorkSpaces Secure Browser

Para que os usuários possam acessar portais da Web pelo navegador local, você deve adicionar os domínios a seguir à lista de permissões na rede da qual o usuário está tentando acessar o serviço.

Na tabela a seguir, *{region}* substitua pelo código da região do portal web operacional. Por exemplo, s3. *{region}*.amazonaws.com deve ser s3.eu-west-1.amazonaws.com para um portal da web na região da Europa (Irlanda). Para obter uma lista de códigos de região, consulte os [endpoints e cotas do Amazon WorkSpaces Secure Browser](#).

Categoria	Domínio ou endereço IP
WorkSpaces Recursos de streaming do Secure Browser	s3. <i>{region}</i> .amazonaws.com
	s3.amazonaws.com
	appstream2. <i>{region}</i> .aws.amazon.com

Categoria	Domínio ou endereço IP
	*.amazonappstream.com *.shortbread.aws.dev
WorkSpaces Recursos estáticos do Secure Browser	*.workspaces-web.com di5ry4hb4263e.cloudfront.net
WorkSpaces Autenticação de navegador seguro	*.auth. <i>{region}</i> .amazoncognito.com identidade cognitiva. <i>{region}</i> .amazonaws.com cognito-idp. <i>{region}</i> .amazonaws.com *.cloudfront.net
WorkSpaces Métricas e relatórios do Secure Browser	*.execute-api. <i>{region}</i> .amazonaws.com unagi-na.amazon.com

Dependendo do provedor de identidade configurado, talvez seja preciso incluir domínios adicionais à lista de permissões. Revise a documentação do seu IdP para identificar quais domínios você precisa permitir na lista para que o WorkSpaces Secure Browser use esse provedor. Se você estiver usando o Centro de Identidade do IAM, consulte [IAM Identity Center prerequisites](#) para obter mais informações.

Introdução ao Amazon WorkSpaces Secure Browser

Siga estas etapas para criar um portal web do WorkSpaces Secure Browser e fornecer aos usuários acesso a sites internos e SaaS a partir de seus navegadores existentes. É possível criar um portal da web em qualquer região com suporte por conta.

Note

Para solicitar um aumento de limite para mais de um portal, entre em contato com o suporte com seu Conta da AWS ID, número de portais a serem solicitados e. Região da AWS

Esse processo normalmente leva cinco minutos com o assistente de criação do portal da web e até 15 minutos adicionais para que o portal se torne Ativo.

Não há custos associados à criação de um portal da web. WorkSpaces O Secure Browser oferece pay-as-you-go preços, incluindo um preço baixo mensal para usuários que usam ativamente o serviço. Não há custos antecipados, licenças nem compromissos de longo prazo.

Important

Antes de começar, você deve atender aos pré-requisitos necessários para um portal da web. Para ter mais informações sobre os pré-requisitos do portal da web, consulte [Configurando o Amazon WorkSpaces Secure Browser](#).

Tópicos

- [Criação de um portal web para o Amazon WorkSpaces Secure Browser](#)
- [Testando seu portal web no Amazon WorkSpaces Secure Browser](#)
- [Distribuindo seu portal web no Amazon WorkSpaces Secure Browser](#)

Criação de um portal web para o Amazon WorkSpaces Secure Browser

Siga estas etapas para criar um portal da web.

Tópicos

- [Definindo as configurações de rede para o Amazon WorkSpaces Secure Browser](#)
- [Definindo as configurações do portal para o Amazon WorkSpaces Secure Browser](#)
- [Definindo as configurações do usuário para o Amazon WorkSpaces Secure Browser](#)
- [Configurando seu provedor de identidade para o Amazon WorkSpaces Secure Browser](#)
- [Lançamento de um portal web com o Amazon WorkSpaces Secure Browser](#)

Definindo as configurações de rede para o Amazon WorkSpaces Secure Browser

Para definir as configurações de rede para o WorkSpaces Secure Browser, siga estas etapas.

1. Abra o console do WorkSpaces Secure Browser em <https://console.aws.amazon.com/workspaces-web/casa>.
2. Escolha Navegador WorkSpaces seguro, depois Portais da Web e escolha Criar portal da Web.
3. Na página Etapa 1: especificar conexão de rede, conclua as etapas a seguir para conectar a VPC ao portal da web e configurar a VPC e sub-redes.
 1. Para obter detalhes da rede, escolha uma VPC com uma conexão com o conteúdo que você deseja que seus usuários acessem com o WorkSpaces Secure Browser.
 2. Escolha até três sub-redes privadas que atendam aos requisitos a seguir. Para obter mais informações, consulte [Rede para o Amazon WorkSpaces Secure Browser](#).
 - Escolha um mínimo de duas sub-redes privadas para criar um portal.
 - Para garantir a alta disponibilidade do portal da web, recomendamos que você forneça o número máximo de sub-redes privadas em zonas de disponibilidade exclusivas para a VPC.
 3. Escolha um grupo de segurança.

Definindo as configurações do portal para o Amazon WorkSpaces Secure Browser

Na página Etapa 2: definir configurações do portal da web, conclua as etapas a seguir para personalizar a experiência de navegação dos usuários quando eles iniciam uma sessão.

1. Em Detalhes do portal da web, em Nome de exibição, insira um nome identificável para o seu portal da web.
2. Em Tipo de instância, selecione o tipo de instância no portal da web no menu suspenso. Em seguida, insira seu limite máximo de usuários simultâneos para o portal da web. Para obter mais informações, consulte [the section called “Gerenciar cotas de serviço”](#).

 Note

A seleção de um novo tipo de instância alterará o custo de cada usuário ativo mensal. Para obter mais informações, consulte os [preços do Amazon WorkSpaces Secure Browser](#).

3. Em Log de acesso do usuário, em ID de fluxo do Kinesis, selecione o fluxo de dados do Amazon Kinesis para o qual você deseja enviar seus dados. Para obter mais informações, consulte [the section called “Configurar o registro de acesso do usuário”](#).
4. Em Configurações de política, conclua o seguinte:
 - Para Opções de política, selecione Editor visual ou Carregamento do arquivo JSON. Você pode usar qualquer um dos métodos para fornecer os detalhes da configuração da política para o portal da web. Para obter mais informações, consulte [the section called “Gerenciar a política do navegador”](#).
 - WorkSpaces O Secure Browser inclui suporte para as políticas corporativas do Chrome. É possível adicionar e gerenciar políticas com um editor visual ou um carregamento manual de arquivos de políticas. É possível alternar entre qualquer uma das opções a qualquer momento.
 - Ao carregar um arquivo de política, você pode ver as políticas disponíveis no arquivo no console. No entanto, não é possível editar todas as políticas no editor visual. O console lista políticas no arquivo JSON que você não pode editar com o editor visual em Políticas JSON adicionais. Para fazer alterações nessas políticas, você deve editá-las manualmente.
 - (Opcional) Em URL de inicialização – opcional, insira um domínio para usar como página inicial quando os usuários iniciarem o navegador. A VPC deve ter uma conexão estável com esse URL.
 - Selecione ou desmarque a opção de Navegação privada e Exclusão do histórico para ativar ou desativar esses recursos durante a sessão de um usuário.

Note

URLs visitado enquanto navega de forma privada, ou antes de um usuário excluir o histórico do navegador, não pode ser registrado no registro de acesso do usuário. Para obter mais informações, consulte [the section called “Configurar o registro de acesso do usuário”](#).

- Em Filtragem de URL, você pode configurar quais URLs usuários podem visitar durante uma sessão. Para obter mais informações, consulte [the section called “Configurar a filtragem de URL”](#).
- (Opcional) Em Marcadores do navegador – opcional, insira o Nome de exibição, o Domínio e a Pasta de favoritos que você deseja que os usuários vejam no navegador. Depois, escolha Adicionar marcador.

Note

Domínio é um campo obrigatório para os favoritos do navegador. No Chrome, os usuários podem encontrar marcadores gerenciados na pasta Gerenciador de favoritos na barra de ferramentas de favoritos.

- (Opcional) Adicione Tags ao seu portal. Você pode usar tags para pesquisar ou filtrar seus AWS recursos. As tags consistem em uma chave e um valor opcional e estão associadas ao recurso do portal.
5. Em Controle de acesso de IP (opcional), escolha se deseja restringir o acesso a redes confiáveis. Para obter mais informações, consulte [the section called “Gerenciar controles de acesso de IP”](#).
 6. Escolha Próximo para continuar.

Definindo as configurações do usuário para o Amazon WorkSpaces Secure Browser

Na página Etapa 3: selecionar configurações do usuário, conclua as etapas a seguir para escolher quais recursos os usuários podem acessar na barra de navegação superior durante a sessão e escolha Próximo:

1. Em Permissões, escolha se deseja ativar a extensão para login único. Para obter mais informações, consulte [the section called “Gerenciar a extensão de login único”](#).
2. Em Permitir que os usuários imprimam em um dispositivo local a partir do portal da web, escolha Permitir ou Não permitir.
3. Em Permitir que os usuários façam um deep link para o portal da web, escolha Permitir ou Não permitir. Para obter mais informações sobre deep links, consulte [the section called “Deep links”](#).
4. Em Controles da barra de ferramentas, escolha as configurações desejadas em Recursos.
5. Em Configurações, gerencie a exibição da apresentação da barra de ferramentas no início da sessão, incluindo o estado da barra de ferramentas (encaixada ou desconectada), o tema (modo escuro ou claro), a visibilidade do ícone e a resolução máxima de exibição da sessão. Deixe essas configurações desdefinidas para conceder aos usuários finais controle total sobre essas opções. Para obter mais informações, consulte [the section called “Controles da barra de ferramentas”](#).
6. Para Tempos limite de sessão, especifique o seguinte:
 - Para Disconnect timeout in minutes (Tempo limite de desconexão em minutos), escolha a quantidade de tempo que uma sessão de streaming permanece ativa após os usuários se desconectarem. Se os usuários tentarem se reconectar à sessão de streaming após uma desconexão ou interrupção na rede dentro desse intervalo de tempo, eles serão conectados à sessão anterior. Caso contrário, eles serão conectados a uma nova sessão com uma nova instância de streaming.

Se um usuário encerrar a sessão, o tempo limite de desconexão não se aplicará. Em vez disso, o usuário é solicitado a salvar os documentos abertos e, depois, é desconectado imediatamente da instância de streaming. A instância que o usuário estava usando é encerrada.

- Para Idle disconnect timeout in minutes (Tempo limite de desconexão de inatividade em minutos), escolha a quantidade de tempo em que os usuários podem ficar ociosos (inativos) antes de serem desconectados de sua sessão de streaming e o início do intervalo de tempo de Disconnect timeout in minutes (Tempo limite de desconexão em minutos). Os usuários são notificados antes de serem desconectados devido à inatividade. Se eles tentarem reconectar-se à sessão de streaming antes do intervalo de tempo especificado em Disconnect timeout in minutes (Tempo limite de desconexão em minutos) terminar, eles são conectados à sessão anterior. Caso contrário, eles serão conectados a uma nova sessão com uma nova instância de streaming. Definir esse valor como 0 o desabilita. Quando esse valor estiver desabilitado, os usuários não serão desconectados devido à inatividade.

Note

Os usuários são considerados como ociosas quando param de fornecer entradas do mouse ou do teclado durante a sessão de streaming. Uploads e downloads de arquivos, entradas de áudio, saídas de áudio e alteração de pixels não são considerados atividade do usuário. Se os usuários permanecerem ociosos depois que o intervalo de tempo em Idle disconnect timeout in minutes (Limite de desconexão ociosa em minutos) terminar, eles serão desconectados.

Configurando seu provedor de identidade para o Amazon WorkSpaces Secure Browser

Use as etapas a seguir para configurar seu provedor de identidades (IdP).

Tópicos

- [Escolha do tipo de provedor de identidade para o Amazon WorkSpaces Secure Browser](#)
- [Alteração do tipo de provedor de identidade para o Amazon WorkSpaces Secure Browser](#)

Escolha do tipo de provedor de identidade para o Amazon WorkSpaces Secure Browser

WorkSpaces O Secure Browser oferece dois tipos de autenticação: Padrão AWS IAM Identity Center. Na página Configurar o provedor de identidade, escolha qual tipo de autenticação deve ser utilizada com o portal.

- Para o tipo Padrão (opção padrão), faça a federação de seu provedor de identidade SAML 2.0 de terceiros (como Okta ou Ping) diretamente com seu portal. Para obter mais informações, consulte [the section called “Tipo de autenticação padrão”](#). O tipo padrão é compatível com fluxos de autenticação iniciados pelo SP ou pelo IdP.
- Para o IAM Identity Center (opção avançada), faça a federação do IAM Identity Center com seu portal. Para usar esse tipo de autenticação, o IAM Identity Center e o portal do WorkSpaces Secure Browser devem residir no mesmo Região da AWS. Para obter mais informações, consulte [the section called “Tipo de autenticação do Centro de Identidade do IAM”](#).

Tópicos

- [Configurando o tipo de autenticação padrão para o Amazon WorkSpaces Secure Browser](#)
- [Configurando o tipo de autenticação do IAM Identity Center para o Amazon WorkSpaces Secure Browser](#)

Configurando o tipo de autenticação padrão para o Amazon WorkSpaces Secure Browser

O tipo de autenticação padrão é o tipo de autenticação inicial fornecido. Ele dá suporte a fluxos de login iniciados pelo provedor de serviços (iniciados pelo SP) e pelo provedor de identidades (iniciados pelo IdP) com IdP compatível com SAML 2.0. Para configurar o tipo de autenticação padrão, siga as etapas abaixo para federar o IdP SAML 2.0 de terceiros (como Okta ou Ping) diretamente com seu portal.

Tópicos

- [Configurando seu provedor de identidade no Amazon WorkSpaces Secure Browser](#)
- [Configurar seu IdP em seu próprio IdP](#)
- [Concluindo a configuração do IdP no Amazon Secure WorkSpaces Browser](#)
- [Orientação para uso específico IdPs com o Amazon WorkSpaces Secure Browser](#)

Configurando seu provedor de identidade no Amazon WorkSpaces Secure Browser

Conclua as etapas a seguir para configurar seu provedor de identidades:

1. Na página Configurar o provedor de identidade do assistente de criação, escolha Padrão.
2. Escolha Continuar com o IdP padrão.
3. Faça o download do arquivo de metadados do SP e mantenha a guia aberta para os valores de metadados individuais.
 - Se o arquivo de metadados do SP estiver disponível, escolha Baixar arquivo de metadados para baixar o documento de metadados do provedor de serviços (SP) e carregar o arquivo de metadados do provedor de serviços no IdP na próxima etapa. Sem isso, os usuários não conseguirão fazer login.
 - Se seu provedor não fizer upload dos arquivos de metadados do SP, insira manualmente os valores dos metadados.
4. Em Escolher tipo de login SAML, escolha entre declarações de SAML iniciadas pelo SP e iniciadas pelo IdP ou somente declarações de SAML iniciadas pelo SP.

- As declarações de SAML iniciadas pelo SP e pelo IdP permitem que seu portal ofereça suporte aos dois tipos de fluxos de login. Os portais que oferecem suporte a fluxos iniciados pelo IdP permitem que você apresente declarações de SAML ao endpoint da federação de identidade de serviço sem exigir que os usuários iniciem uma sessão visitando a URL do portal.
- Escolha essa opção para permitir que o portal aceite declarações de SAML não solicitadas iniciadas pelo IdP.
- Essa opção exige que um estado de retransmissão padrão seja configurado em seu provedor de identidade SAML 2.0. O parâmetro de estado de retransmissão do seu portal está no console em login de SAML iniciado por IdP, ou você pode copiá-lo do arquivo de metadados SP em `<md:IdPInitRelayState>`.
- Observação
 - O formato a seguir representa o estado de retransmissão:
`redirect_uri=https%3A%2F%2Fportal-id.workspaces-web.com%2Fsso&response_type=code&client_id=1example23456789&identity_provider=Example-Identity-Provider.`
 - Se você copiar e colar o valor do arquivo de metadados do SP, certifique-se de alterar `&` para `&`. `&` é um caractere de escape de XML.
- Escolha somente declarações de SAML iniciadas pelo SP para que o portal ofereça suporte somente aos fluxos de login iniciados pelo SP. Essa opção rejeitará declarações de SAML não solicitadas de fluxos de login iniciados pelo IdP.

 Note

Alguns terceiros IdPs permitem que você crie um aplicativo SAML personalizado que pode oferecer experiências de autenticação iniciadas pelo IdP aproveitando fluxos iniciados pelo SP. Consulte um exemplo em [Add an Okta bookmark application](#).

5. Escolha se você deseja habilitar Assinar solicitações de SAML para esse provedor. A autenticação iniciada pelo SP permite que o IdP valide se a solicitação de autenticação está vindo do portal, o que impede a aceitação de outras solicitações de terceiros.
 - a. Baixe o certificado de assinatura e faça o upload para o seu IdP. O mesmo certificado de assinatura pode ser usado para um único logout.
 - b. Habilitar a solicitação assinada em seu IdP. O nome pode ser diferente, dependendo do IdP.

Note

RSA- SHA256 é o único algoritmo de solicitação e assinatura de solicitação padrão suportado.

- Escolha se você deseja habilitar Exigir declarações de SAML criptografadas. Isso permite que você criptografe a declaração de SAML que vem do seu IdP. Isso pode impedir que os dados sejam interceptados em declarações SAML entre o IdP e o Secure Browser. WorkSpaces

Note

O certificado de criptografia não está disponível nessa etapa. Ele será criado após o portal ser iniciado. Depois de iniciar o portal, baixe o certificado de criptografia e faça o upload para o IdP. Em seguida, habilite a criptografia de declaração em seu IdP (o nome pode ser diferente, dependendo do IdP).

- Escolha se você deseja ativar o Logout único. O logout único permite que seus usuários finais saiam da sessão do IdP WorkSpaces e do Secure Browser com uma única ação.
 - Baixe o certificado de assinatura do WorkSpaces Secure Browser e carregue-o em seu IdP. Esse é o mesmo certificado de assinatura usado para Solicitar assinatura na etapa anterior.
 - Usar o Logout único exige que você configure um URL de logout único no seu provedor de identidade SAML 2.0. Você pode encontrar o URL de logout único do seu portal no console em Detalhes do provedor de serviços (SP) - Mostrar valores de metadados individuais ou do arquivo de metadados SP em `<md:SingleLogoutService>`.
 - Habilitar logout único em seu IdP. O nome pode ser diferente, dependendo do IdP.

Configurar seu IdP em seu próprio IdP

Para configurar seu IdP em seu próprio IdP, siga estas etapas.

- Abra uma nova guia no navegador.
- Adicione os metadados do portal ao SAML IdP.

Faça o upload do documento de metadados do SP que você baixou na etapa anterior no IdP ou copie e cole os valores dos metadados nos campos corretos do IdP. Alguns provedores não permitem o upload de arquivos.

Os detalhes desse processo podem variar entre os provedores. Encontre a documentação do seu provedor em [the section called “Orientação para fins específicos IdPs”](#) para obter ajuda sobre como adicionar os detalhes do portal à sua configuração de IdP.

3. Confirme o NameID para sua declaração de SAML.

Certifique-se de que seu SAML IdP preencha o NameID na declaração de SAML com o campo de e-mail do usuário. O NameID e e-mail do usuário são usados para identificar exclusivamente o usuário federado de SAML com o portal. Use o formato de ID de Nome do SAML persistente.

4. Opcional: configure o estado de retransmissão para a autenticação iniciada pelo IdP.

Se você escolheu Aceitar declarações de SAML iniciadas pelo SP e iniciadas pelo IdP na etapa anterior, siga as etapas na etapa 2 de [the section called “Configuração do IdP no WorkSpaces Secure Browser”](#) para definir o estado de retransmissão padrão para seu aplicativo de IdP.

5. Opcional: configure Solicitar assinatura. Se você escolheu Assinar solicitações de SAML para esse provedor na etapa anterior, siga as etapas na etapa 3 de [the section called “Configuração do IdP no WorkSpaces Secure Browser”](#) para fazer upload do certificado de assinatura no seu IdP e habilitar a assinatura da solicitação. Alguns IdPs, como o Okta, podem exigir que seu NameID pertença ao tipo “persistente” para usar a assinatura de solicitação. Certifique-se de confirmar seu NameID para sua declaração de SAML seguindo as etapas acima.

6. Opcional: configure a criptografia de declaração. Se você escolher Exigir declarações de SAML criptografadas desse provedor, aguarde até que a criação do portal seja concluída e siga a etapa 4 em “Fazer upload de metadados” abaixo para carregar o certificado de criptografia em seu IdP e habilitar a criptografia de declaração.

7. Opcional: configure o logout único. Se você escolheu Logout único, siga as etapas na etapa 5 de [the section called “Configuração do IdP no WorkSpaces Secure Browser”](#) para carregar o certificado de assinatura em seu IdP, preencher o URL de logout único e habilite o Logout único.

8. Conceda acesso aos seus usuários em seu IdP para usar o Navegador WorkSpaces Seguro.

9. Baixe um arquivo de troca de metadados do seu IdP. Você fará o upload desses metadados para o WorkSpaces Secure Browser na próxima etapa.

Concluindo a configuração do IdP no Amazon Secure WorkSpaces Browser

Para concluir a configuração do IdP no WorkSpaces Secure Browser, siga estas etapas.

1. Retorne ao console do WorkSpaces Secure Browser. Na página Configurar provedor de identidade do assistente de criação, em Metadados do IdP, faça upload de um arquivo de

- metadados ou insira um URL de metadados do IdP. O portal usa esses metadados do IdP para estabelecer confiança.
2. Para carregar um arquivo de metadados, em Documento de metadados do IdP, selecione Escolher arquivo. Carregue o arquivo de metadados no formato XML do IdP que você baixou na etapa anterior.
 3. Para usar um URL de metadados, acesse o IdP que você configurou na etapa anterior e obtenha o URL de metadados. Volte para o console do WorkSpaces Secure Browser e, em URL de metadados do IdP, insira o URL dos metadados que você obteve do seu IdP.
 4. Quando concluir, escolha Next.
 5. Para portais nos quais você habilitou a opção Exigir declarações SAML criptografadas deste provedor, você precisa baixar o certificado de criptografia da seção de detalhes do IdP do portal e carregá-lo no seu IdP. Em seguida, você pode ativar a opção lá.

 Note

WorkSpaces O Secure Browser exige que o assunto ou o nameID sejam mapeados e definidos na declaração SAML nas configurações do seu IdP. O IdP pode criar esses mapeamentos automaticamente. Se esses mapeamentos não estiverem configurados corretamente, os usuários não poderão fazer login no portal da web e iniciar uma sessão. WorkSpaces O Secure Browser exige que as seguintes afirmações estejam presentes na resposta do SAML. Você pode encontrar *<Your SP Entity ID>* e *<Your SP ACS URL>* a partir do documento de metadados ou detalhes do provedor de serviços do seu portal, seja pelo console ou pela CLI.

- Uma reivindicação AudienceRestriction com um valor de Audience que define o ID da entidade SP como o destino da resposta. Exemplo: .

```
<saml:AudienceRestriction>
  <saml:Audience><Your SP Entity ID></saml:Audience>
</saml:AudienceRestriction>
```

- Uma reivindicação Response com um valor de InResponseTo do ID da solicitação SAML original. Exemplo: .

```
<samlp:Response ... InResponseTo="<originalSAMLrequestId">
```

- Uma reivindicação SubjectConfirmationData com um valor de Recipient do URL ACS SP e um valor de InResponseTo que corresponde ao ID da solicitação SAML original. Exemplo: .

```
<saml:SubjectConfirmation>
  <saml:SubjectConfirmationData ...
    Recipient="<Your SP ACS URL>"
    InResponseTo="<originalSAMLrequestId>"
  />
</saml:SubjectConfirmation>
```

WorkSpaces O Secure Browser valida seus parâmetros de solicitação e declarações de SAML. Para declarações de SAML iniciadas pelo IdP, os detalhes da solicitação devem ser formatados como um parâmetro RelayState no corpo de uma solicitação HTTP POST. O corpo da solicitação também deve conter sua declaração de SAML como um parâmetro SAMLResponse. Ambos devem estar presentes se você tiver seguido a etapa anterior.

Veja a seguir um exemplo de corpo de POST para um provedor de SAML iniciado pelo IdP.

```
SAMLResponse=<Base64-encoded SAML assertion>&RelayState=<RelayState>
```

Orientação para uso específico IdPs com o Amazon WorkSpaces Secure Browser

Para garantir que você configure corretamente a federação SAML para seu portal, consulte os links abaixo para obter a documentação dos mais usados IdPs.

IdP	Configuração do aplicativo SAML	Gerenciamento de usuários	Autenticação iniciada pelo IDP	Solicitar assinatura	Criptografia da declaração	Logout único
Okta	Criar integração de aplicativos SAML	Gerenciamento de usuários	Referência do campo SAML do Assistent e de integração	Referência do campo SAML do Assistent e de integração	Referência do campo SAML do Assistent e de integração	Referência do campo SAML do Assistent e de integração

IdP	Configuração do aplicativo SAML	Gerenciamento de usuários	Autenticação iniciada pelo IDP	Solicitar assinatura	Criptografia da declaração	Logout único
			de aplicativo	de aplicativo	de aplicativo	de aplicativo
Entra	Criar seu próprio aplicativo	Início rápido: criar e atribuir uma conta de usuário	Habilitar o login único para um aplicativo corporativo	Verificação da assinatura da solicitação SAML	Configurar a criptografia de token SAML do Microsoft Entra	Protocolo SAML de logout único
Ping	Adicionar um aplicativo SAML	Usuários	Habilitar o SSO iniciado pelo IdP	Configurando o login da solicitação de autenticação PingOne para Enterprise	O PingOne for Enterprise e oferece suporte à criptografia?	Logout único do SAML 2.0
One Login	Conector personalizado SAML (avançado) (4266907)	Adicionar usuários OneLogin manualmente	Conector personalizado SAML (avançado) (4266907)	Conector personalizado SAML (avançado) (4266907)	Conector personalizado SAML (avançado) (4266907)	Conector personalizado SAML (avançado) (4266907)
Centro de Identidade do IAM	Configurar sua própria aplicação SAML 2.0	Configurar sua própria aplicação SAML 2.0	Configurar sua própria aplicação SAML 2.0	N/D	N/D	N/D

Configurando o tipo de autenticação do IAM Identity Center para o Amazon WorkSpaces Secure Browser

Para o Centro de Identidade do IAM (avançado), faça a federação do Centro de Identidade do IAM com seu portal. Selecione essa opção somente se o seguinte se aplicar a você:

- Seu IAM Identity Center está configurado no mesmo portal da web Conta da AWS e Região da AWS no mesmo.
- Se você estiver usando AWS Organizations, você está usando uma conta de gerenciamento.

Antes de criar um portal da web com o tipo de autenticação do Centro de Identidade do IAM, você deve configurá-lo como um provedor independente. Para obter mais informações, consulte [Get started with common tasks in IAM Identity Center](#). Ou você pode conectar seu IdP SAML 2.0 ao Centro de Identidade do IAM. Para obter mais informações, consulte [Conectar-se a um provedor de identidade externo](#). Caso contrário, você não terá nenhum usuário ou grupo para atribuir ao portal da web.

Se você já usa o Centro de Identidade do IAM, pode escolhê-lo como um tipo de provedor e seguir as etapas abaixo para adicionar, visualizar ou remover usuários ou grupos do portal da web.

Note

Para usar esse tipo de autenticação, seu IAM Identity Center precisa estar no mesmo Conta da AWS portal do WorkSpaces Secure Browser. Região da AWS Se o seu IAM Identity Center estiver em um local separado Conta da AWS ou Região da AWS, siga as instruções para o tipo de autenticação padrão. Para obter mais informações, consulte [the section called “Tipo de autenticação padrão”](#).

Se você estiver usando AWS Organizations, só poderá criar portais do WorkSpaces Secure Browser integrados ao IAM Identity Center usando uma conta de gerenciamento.

Tópicos

- [Criar um portal da web com o Centro de Identidade do IAM](#)
- [Gerenciar o portal da web com o Centro de Identidade do IAM](#)
- [Adicionar mais usuários e grupos a um portal da web](#)
- [Visualizar e remover usuários e grupos do portal da web](#)

Criar um portal da web com o Centro de Identidade do IAM

Para criar um portal da web com o Centro de Identidade do IAM, siga estas etapas.

Para criar um portal da web com o Centro de Identidade do IAM

1. Durante a criação do portal na Etapa 4: Configurar provedor de identidade, escolha AWS IAM Identity Center.
2. Escolha Continuar com o IAM Identity Center.
3. Na página Atribuir usuários e grupos, escolha a guia Usuários e/ou Grupos.
4. Marque a caixa próxima aos usuários ou grupos que deseja adicionar ao portal.
5. Depois de criar seu portal, os usuários que você associou podem entrar no WorkSpaces Secure Browser com seu nome de usuário e senha do IAM Identity Center.

Gerenciar o portal da web com o Centro de Identidade do IAM

Para gerenciar um portal da web com o Centro de Identidade do IAM, siga estas etapas.

Para gerenciar o portal da web com o Centro de Identidade do IAM

1. Depois que o portal for criado, ele será listado no console do Centro de Identidade do IAM como uma aplicação configurada.
2. Para acessar a configuração dessa aplicação, escolha Aplicações na barra lateral e procure uma aplicação configurada com um nome que corresponda ao nome de exibição do seu portal da web.

Note

Se você não inseriu um nome de exibição, o GUID do portal será exibido em vez disso. O GUID é o ID prefixado ao URL do endpoint do seu portal da web.

Adicionar mais usuários e grupos a um portal da web

Para adicionar mais usuários e grupos a um portal da web existente, siga estas etapas.

Para adicionar mais usuários e grupos a um portal da web existente

1. Abra o console do WorkSpaces Secure Browser em <https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/>.
2. Escolha Navegador WorkSpaces seguro, portais da Web, escolha seu portal da Web e escolha Editar.
3. Escolha Configurações do provedor de identidade e Atribuir usuários e grupos adicionais. Agora você pode adicionar usuários e grupos ao seu portal da web.

 Note

Não é possível adicionar usuários ou grupos pelo console do Centro de Identidade do IAM. Você deve fazer isso na página de edição do portal do WorkSpaces Secure Browser.

Visualizar e remover usuários e grupos do portal da web

Para visualizar ou remover usuários e grupos do seu portal da web, use as ações disponíveis na tabela Usuários atribuídos. Para obter mais informações, consulte [Manage access to applications](#)

 Note

Você não pode visualizar ou remover usuários e grupos da página de edição do portal do Navegador WorkSpaces Seguro. Você deve fazer isso na página de edição do console do Centro de Identidade do IAM.

Alteração do tipo de provedor de identidade para o Amazon WorkSpaces Secure Browser

É possível alterar o tipo de autenticação do portal a qualquer momento. Para isso, siga estas etapas.

- Para mudar de Centro de Identidade do IAM para Padrão, siga as etapas em [the section called “Tipo de autenticação padrão”](#).
- Para mudar de Padrão para Centro de Identidade do IAM, siga as etapas em [the section called “Tipo de autenticação do Centro de Identidade do IAM”](#).

As alterações no tipo de provedor de identidade podem levar até 15 minutos para serem implantadas e não se encerrarão automaticamente as sessões em andamento.

Você pode visualizar as alterações do tipo de provedor de identidade em seu portal AWS CloudTrail inspecionando UpdatePortal eventos. O tipo fica visível nas cargas úteis de solicitação e resposta do evento.

Lançamento de um portal web com o Amazon WorkSpaces Secure Browser

Quando terminar de configurar seu portal da web, você poderá seguir estas etapas para iniciá-lo.

1. Na página Etapa 5: analisar e executar, revise as configurações que você selecionou para o seu portal da web. Você pode selecionar Editar para alterar as configurações de determinada seção. Também é possível alterar essas configurações posteriormente na guia Portais da Web do console.
2. Quando terminar, escolha Iniciar o portal da Web.
3. Para visualizar o status do seu portal da web, selecione Portais da Web, escolha seu portal e Visualizar detalhes.

Um portal da web tem um dos seguintes status:

- Incompleto: faltam configurações necessárias do provedor de identidades no portal da web.
 - Pendente: o portal da web está aplicando alterações em suas configurações.
 - Ativo: o portal da web está pronto e disponível para uso.
4. Aguarde até 15 minutos para que o portal se torne Ativo.

Testando seu portal web no Amazon WorkSpaces Secure Browser

Depois de criar um portal da web, você pode entrar no endpoint do WorkSpaces Secure Browser para navegar nos sites conectados como um usuário final faria.

Se você já concluiu essas etapas em [the section called “Configuração do provedor de identidade”](#), ignore esta seção e vá para [Distribuindo seu portal web no Amazon WorkSpaces Secure Browser](#).

1. Abra o console do WorkSpaces Secure Browser em https://console.aws.amazon.com/workspaces-web/casa?região=us-east-1#.
2. Escolha Navegador WorkSpaces seguro, portais da Web, escolha seu portal da Web e, em seguida, escolha Exibir detalhes

3. Em Endpoint do portal da Web, vá até o URL especificada para seu portal. O endpoint do portal da web é o ponto de acesso pelo qual os usuários iniciarão seu portal da web após fazerem login com o provedor de identidades configurado para o portal. Ele está disponível publicamente na internet e pode ser incorporado à sua rede.
4. Na página de login do WorkSpaces Secure Browser, escolha Entrar, SAML e insira suas credenciais do SAML.
5. Quando você vê a página Sua sessão está sendo preparada, sua sessão do Navegador WorkSpaces Seguro está sendo iniciada. Não feche nem saia dessa página.
6. O navegador da web é iniciado, exibindo o URL de inicialização e qualquer outro comportamento adicional definido por meio das configurações de política do navegador.
7. Agora você pode navegar até sites conectados escolhendo links ou URLs entrando na barra de endereço.

Distribuindo seu portal web no Amazon WorkSpaces Secure Browser

Quando estiver pronto para que seus usuários comecem a usar o Navegador WorkSpaces Seguro, você escolhe entre as seguintes opções para distribuir o portal:

- Adicione o portal ao gateway do aplicativo SAML para que os usuários iniciem uma sessão diretamente do IdP. Você pode fazer isso por meio do fluxo de login iniciado pelo IdP com seu IdP compatível com SAML 2.0. Para obter mais informações, consulte Declarações de SAML iniciadas pelo SP e iniciadas pelo IdP em [the section called “Tipo de autenticação padrão”](#). Como alternativa, você pode criar um aplicativo SAML personalizado que possa fornecer experiências de autenticação iniciadas pelo IdP usando fluxos iniciados pelo SP. Para ver mais informações, consulte [Create a Bookmark App integration](#).
- Adicione o URL do portal a um site de sua propriedade e use um redirecionamento de navegador para direcionar os usuários ao portal da web.
- Envie por e-mail o URL do portal para seus usuários ou envie para um dispositivo que você gerencia como página inicial ou marcador do navegador.

Gerenciando seu portal web no Amazon WorkSpaces Secure Browser

Depois de configurar o portal da web, você pode executar as ações a seguir para gerenciá-lo.

Tópicos

- [Visualizando detalhes do portal web no Amazon WorkSpaces Secure Browser](#)
- [Editando um portal da web no Amazon WorkSpaces Secure Browser](#)
- [Excluindo um portal da web no Amazon WorkSpaces Secure Browser](#)
- [Gerenciando cotas de serviço para seu portal no Amazon WorkSpaces Secure Browser](#)
- [Controle do intervalo para reautenticar um token SAML IdP no Amazon Secure Browser WorkSpaces](#)
- [Configurando o login de acesso do usuário no Amazon WorkSpaces Secure Browser](#)
- [Gerenciando a política do navegador no Amazon WorkSpaces Secure Browser](#)
- [Configurando o editor de método de entrada para o Amazon WorkSpaces Secure Browser](#)
- [Configurando a localização em sessão para o Amazon Secure Browser WorkSpaces](#)
- [Gerenciando controles de acesso IP no Amazon WorkSpaces Secure Browser](#)
- [Gerenciando a extensão de login único no Amazon WorkSpaces Secure Browser](#)
- [Configurando a filtragem de URL no Amazon WorkSpaces Secure Browser](#)
- [Links diretos no Amazon WorkSpaces Secure Browser](#)
- [Usando o painel de gerenciamento de sessões no Amazon WorkSpaces Secure Browser](#)
- [Protegendo dados em trânsito com endpoints FIPS e Amazon WorkSpaces Secure Browser](#)
- [Gerenciando configurações de proteção de dados no Amazon WorkSpaces Secure Browser](#)
- [Gerenciamento de controles da barra de ferramentas no Amazon WorkSpaces Secure Browser](#)

Visualizando detalhes do portal web no Amazon WorkSpaces Secure Browser

Para visualizar detalhes do portal da web, siga estas etapas.

1. Abra o console do WorkSpaces Secure Browser em <https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/>.
2. Escolha Navegador WorkSpaces seguro, portais da Web, escolha seu portal da Web e, em seguida, escolha Exibir detalhes.

Editando um portal da web no Amazon WorkSpaces Secure Browser

Para editar um portal da web, siga estas etapas.

1. Abra o console do WorkSpaces Secure Browser em <https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/>.
2. Escolha Navegador WorkSpaces seguro, portais da Web, escolha seu portal da Web e, em seguida, escolha Editar.

Note

Alterações nas configurações de rede ou nas configurações de tempo limite encerram imediatamente qualquer sessão ativa do portal. Os usuários são desconectados e precisam se reconectar para iniciar uma nova sessão. As alterações nas Permissões da área de transferência, nas Permissões de transferência de arquivos ou em Imprimir no dispositivo local são aplicadas a partir da primeira nova sessão. As sessões que estão ativas não são desconectadas. Os usuários conectados às sessões ativas não são afetados pelas alterações até que se desconectem e se conectem a uma nova sessão.

Excluindo um portal da web no Amazon WorkSpaces Secure Browser

Para excluir um portal da web, siga estas etapas.

1. Abra o console do WorkSpaces Secure Browser em <https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/>.
2. Escolha Navegador WorkSpaces seguro, Portais da Web, escolha seu portal da Web e, em seguida, escolha Excluir.

Gerenciando cotas de serviço para seu portal no Amazon WorkSpaces Secure Browser

Quando você cria seu Conta da AWS, definimos automaticamente as cotas de serviço padrão (também chamadas de limites) para o uso de recursos com Serviços da AWS. Os administradores devem estar cientes de duas cotas que talvez precisem ser aumentadas para dar suporte ao caso de uso. Essas duas cotas são o número de portais da web que você pode criar em cada região e o número máximo de sessões simultâneas que você pode manter com cada tipo de instância disponível em cada região. Você pode solicitar um aumento para elas na página Service Quotas no AWS Console.

A tabela a seguir lista os limites de cotas de serviço padrão.

Cotas padrão em uma conta Região da AWS por	Valor
Portais da web	3
Máximo de sessões simultâneas - standard. regular	25
Máximo de sessões simultâneas - standard. large	10
Máximo de sessões simultâneas - standard. xlarge	5

Para ver as cotas de serviço alocadas à sua conta para cada região a qualquer momento, consulte a [página Service Quotas](#).

Important

As cotas de serviço afetam uma Região da AWS de cada vez. Você deve solicitar aumentos de cota de serviço em cada um dos Região da AWS casos em que precisar de mais recursos. Para obter mais informações, [endpoints e cotas do Amazon WorkSpaces Secure Browser](#).

Tópicos

- [Solicitando um aumento da cota de serviço no Amazon WorkSpaces Secure Browser](#)
- [Solicitando um aumento do portal no Amazon WorkSpaces Secure Browser](#)
- [Solicitando um aumento máximo de sessões simultâneas no Amazon WorkSpaces Secure Browser](#)
- [Exemplo de limite para o Amazon WorkSpaces Secure Browser](#)
- [Outras cotas de serviço no Amazon WorkSpaces Secure Browser](#)

Solicitando um aumento da cota de serviço no Amazon WorkSpaces Secure Browser

Para solicitar um aumento da cota de serviço, siga estas etapas.

1. Abra o [painel do AWS Support](#).
2. Escolha Aumento do limite de serviço.

Important

WorkSpaces As cotas do serviço Secure Browser afetam uma região por vez. Você deve solicitar aumentos de cota de serviço em cada região da AWS em que precisa de mais recursos. Para obter mais informações, consulte os [Endpoints de serviço da AWS](#).

3. Em Descrição do caso de uso, insira as seguintes informações:
 - Se você estiver solicitando um aumento no número de portais da web, especifique esse tipo de recurso e inclua o ID da sua conta da AWS, a região em que você gostaria de aumentar e o novo valor de limite.
 - Se você estiver solicitando um aumento para o máximo de sessões simultâneas, especifique esse tipo de recurso e inclua o ID da sua conta da AWS, a região em que você gostaria de aumentar, o ARN do portal da web e o novo valor de limite.
4. (Opcional) Para solicitar vários aumentos de cota de serviço ao mesmo tempo, conclua uma solicitação de aumento de cota na seção Solicitações e escolha Adicionar outra solicitação.

Solicitando um aumento do portal no Amazon WorkSpaces Secure Browser

Um portal é o recurso fundamental do serviço. Cada portal é uma associação entre seu provedor de identidades SAML 2.0 e sua conexão de rede com a internet e qualquer conteúdo privado da web. Cada portal pode ter uma política de navegador do portal e configurações de usuário separadas, portanto, os administradores geralmente criam vários portais na mesma região para tratar de diferentes casos de uso. Por exemplo, você pode fornecer ao Grupo A acesso a um site específico com políticas restritivas (por exemplo, área de transferência e transferência de arquivos desabilitadas) e ao Grupo B acesso à Internet geral sem filtragem de URL. Você pode criar um portal em qualquer Região da AWS compatível. Para ver a disponibilidade atual do serviço, consulte [Serviços da AWS por região](#).

Para solicitar um aumento de cota de serviço

1. Abra a [página Service Quotas](#) na região desejada.
2. Escolha Número de portais da web.
3. Escolha Solicitar um aumento no nível da conta.
4. Para Aumentar valor da cota, insira o valor total que você deseja que a cota tenha.

Solicitando um aumento máximo de sessões simultâneas no Amazon WorkSpaces Secure Browser

A cota máxima de sessões simultâneas é a maior quantidade de usuários que podem ser conectados ao mesmo tempo a determinado portal. Se o limite de cota de serviço para o máximo de sessões simultâneas não for definido adequadamente, os usuários poderão encontrar uma sessão indisponível ao fazer login. Além de aumentar essa cota de serviço, os clientes também devem garantir que a VPC e as sub-redes tenham espaço de IP suficiente para dar suporte ao máximo de sessões simultâneas.

Para solicitar um aumento máximo de sessões simultâneas

1. Abra a [página Service Quotas](#) na região desejada.
2. Escolha Número máximo de sessões simultâneas por portal para o tipo de instância que você deseja aumentar.
3. Escolha Solicitar um aumento no nível da conta.
4. Para Aumentar valor da cota, insira o valor total que você deseja que a cota tenha.

Note

Para aumentos grandes ou urgentes, acesse sua [página de histórico de Service Quotas](#), selecione o link na coluna de status de sua solicitação, siga o link do seu caso de suporte e adicione uma resposta com detalhes sobre seu caso de uso e/ou a urgência. Essas informações ajudam a equipe de atendimento a priorizar as solicitações e garantir que a capacidade suficiente seja alocada para sua conta.

Exemplo de limite para o Amazon WorkSpaces Secure Browser

Por exemplo, suponha que um administrador esteja configurando dois portais da web na região Leste dos EUA (Norte da Virgínia) para um total de 125 usuários. Antes de criar o portal da web, o administrador identifica que o primeiro portal da web (Portal A) dará suporte a 100 usuários. Ao testar o fluxo de trabalho desses usuários, o administrador determina que eles precisarão do tipo de instância XL para oferecer suporte ao streaming de áudio e vídeo durante a sessão. O segundo portal da web (Portal B) precisa estar disponível para até 25 usuários para dar suporte ao acesso a uma única página da web estática hospedada na VPC do cliente. Ao testar esse caso de uso, o administrador determina que o tipo de instância padrão pode oferecer suporte a esse caso de uso.

Para o portal A, o administrador deve enviar uma solicitação de aumento da cota de serviço para aumentar o limite de instâncias XL da região padrão (ou seja, 5) para 100. Depois de preenchido, o administrador pode alocar a capacidade editando o portal da web. Para o portal B, o administrador pode avançar sem solicitar um aumento de cota (ou seja, já que a região tem uma cota padrão de 25 para o tipo de instância padrão).

Outras cotas de serviço no Amazon WorkSpaces Secure Browser

Você pode visualizar e solicitar aumentos de outras cotas listadas na [página Service Quotas](#). Na prática, a maioria dos clientes achará desnecessário solicitar aumentos desses limites. Essas cotas são amplamente agrupadas em dois tipos: Número e Taxa.

Para cotas de Número, ao enviar um aumento de cota de serviço para Número de portais da web, você receberá automaticamente um aumento no número de sub-recursos necessários para criar um portal exclusivo. Isso será refletido na [página Service Quotas](#). Por exemplo, se você solicitar um aumento nos portais de 3 para 5, receberá automaticamente um aumento na cota de serviço de 3

para 5 nas configurações do navegador e do usuário. Você tem a opção de reutilizar ou criar novos sub-recursos conforme desejado.

Em raras ocasiões, os clientes podem encontrar um caso de uso para aumentar o número ou a taxa de outras cotas de recursos. Por exemplo, os administradores podem querer aumentar o número de configurações do navegador para testar configurações adicionais do portal. Essas solicitações de cota de serviço serão analisadas e atendidas case-by-case com base nisso.

Para cotas de Taxa, os limites de taxa expostos em Service Quotas não precisam ser ajustados, independentemente do limite do portal da conta.

Controle do intervalo para reautenticar um token SAML IdP no Amazon Secure Browser WorkSpaces

Quando um usuário visita um portal do WorkSpaces Secure Browser, ele pode entrar para iniciar uma sessão de streaming. Todas as sessões começam na página inicial, a menos que eles tenham feito login há menos de cinco minutos. O portal verifica os tokens do provedor de identidades (IdP) para determinar se as credenciais do usuário devem ser solicitadas ao iniciar uma sessão. Um usuário sem um token de IdP válido deve inserir um nome de usuário, uma senha e, opcionalmente, a autenticação multifator (MFA) para iniciar uma sessão de streaming. Se um usuário já tiver gerado um token do IdP SAML fazendo login em seu IdP ou em uma aplicação protegida pelo mesmo IdP, as credenciais de login não serão solicitadas a ele.

Se um usuário tiver um token SAML IdP válido, ele poderá WorkSpaces acessar o Secure Browser. É possível controlar o intervalo necessário para autenticar novamente um token do IdP SAML.

Para controlar o intervalo para autenticar novamente um token do IdP SAML

1. Defina a duração do tempo limite do IdP com seu provedor de IdP SAML. Recomendamos configurar a duração do tempo limite do IdP com o menor tempo necessário para que o usuário conclua suas tarefas.
 - Para obter mais informações sobre o Okta, consulte [Impor uma vida útil de sessão limitada para todas as políticas](#).
 - Para obter mais informações sobre o Azure AD, consulte [Configurar controles da sessão de autenticação](#).
 - Para obter mais informações sobre Ping, consulte [Sessões](#).

- Para obter mais informações sobre AWS IAM Identity Center, consulte [Definir a duração da sessão](#).
2. Defina os valores de inatividade e tempo limite de inatividade do portal do WorkSpaces Secure Browser. Esses valores controlam a quantidade de tempo entre a última interação do usuário e o término de uma sessão do Navegador WorkSpaces Seguro devido à inatividade. Quando uma sessão termina, o usuário perde o estado da sessão (incluindo guias abertas, conteúdo da web não salvo e histórico) e retorna a um novo estado no início da próxima sessão. Para obter mais informações, consulte a etapa 5 em [the section called “Criação de um portal da web”](#).

Note

Se a sessão de um usuário expirar, mas o usuário ainda tiver um token SAML IdP válido, ele não precisará inserir o nome de usuário e a senha para iniciar uma WorkSpaces nova sessão do Navegador Seguro. Para controlar como os tokens são autenticados novamente, siga os guias na etapa anterior.

Configurando o login de acesso do usuário no Amazon WorkSpaces Secure Browser

É possível configurar o log de acesso do usuário para registrar os seguintes eventos do usuário:

- Início da sessão - Marca o início de uma sessão do Navegador WorkSpaces Seguro.
- Fim da sessão - marca o fim de uma sessão do Navegador WorkSpaces Seguro.
- Navegação por URL: registra o URL que um usuário carrega.

Note

Os registros de navegação por URL são registrados a partir do histórico do navegador. URLs não registrados no histórico do navegador (visitados no modo de navegação anônima ou excluídos do histórico do navegador) não são registrados nos registros. Cabe aos clientes determinar se devem desativar o modo de navegação anônima ou a exclusão do histórico com a política do navegador.

Além disso, as seguintes informações estão incluídas para cada evento:

- Hora do evento
- Nome de usuário
- ARN do portal da web

Os clientes são responsáveis por compreender os possíveis problemas legais que surgem com o uso do WorkSpaces Secure Browser e garantir que o uso do WorkSpaces Secure Browser esteja em conformidade com todas as leis e regulamentos aplicáveis. Isso inclui leis que regulam a capacidade do empregador de monitorar o uso do Navegador WorkSpaces Seguro por um funcionário, incluindo atividades realizadas dentro do aplicativo.

A ativação dos registros de acesso do usuário no portal do WorkSpaces Secure Browser pode resultar em cobranças do Amazon Kinesis Data Streams. Para obter detalhes de preço, consulte [Preços do Amazon Kinesis Data Streams](#).

Para ativar o registro de acesso do usuário no console do WorkSpaces Secure Browser, em Registro de acesso do usuário, selecione o Kinesis Stream ID que você deseja usar para receber dados. Os dados gravados serão entregues diretamente para esse fluxo.

Para obter mais informações sobre como criar um Amazon Kinesis Data Stream, consulte [What Is Amazon Kinesis Data Streams?](#).

Note

Para receber registros do WorkSpaces Secure Browser, você deve ter um Amazon Kinesis Data Stream que comece com "amazon-workspaces-web-*". Seu stream de dados do Amazon Kinesis deve ter a criptografia do lado do servidor desativada ou deve ser usada para criptografia do lado do servidor. Chaves gerenciadas pela AWS

Para obter mais informações sobre a configuração da criptografia do lado do servidor no Amazon Kinesis, consulte [How Do I Get Started with Server-Side Encryption?](#).

Tópicos

- [Exemplos de registros de acesso de usuários para o Amazon WorkSpaces Secure Browser](#)

Exemplos de registros de acesso de usuários para o Amazon WorkSpaces Secure Browser

Abaixo está um exemplo de cada evento disponível, incluindo Validação StartSessionVisitPage,, EndSessione.

Os campos a seguir estão sempre incluídos em cada evento:

- timestamp é incluído como tempo epoch em milissegundos.
- eventType é incluído como uma string.
- details é incluído como outro objeto json.
- portalArn e userName são incluídos em todos os eventos, exceto em Validation.

```
{
  "timestamp": "1665430373875",
  "eventType": "Validation",
  "details": {
    "permission": "Kinesis:PutRecord",
    "userArn": "userArn",
    "operation": "AssociateUserAccessLoggingSettings",
    "userAccessLoggingSettingsArn": "userAccessLoggingSettingsArn"
  }
}

{
  "timestamp": "1665179071723",
  "eventType": "StartSession",
  "details": {},
  "portalArn": "portalArn",
  "userName": "userName"
}

{
  "timestamp": "1665179084578",
  "eventType": "VisitPage",
  "details": {
    "title": "Amazon",
    "url": "https://www.amazon.com/"
  },
  "portalArn": "portalArn",
```

```
"userName": "userName"
}

{
  "timestamp": "1665179155953",
  "eventType": "EndSession",
  "details": {},
  "portalArn": "portalArn",
  "userName": "userName"
}
```

Gerenciando a política do navegador no Amazon WorkSpaces Secure Browser

Com o Navegador WorkSpaces Seguro, você pode definir uma política de navegador personalizada usando as políticas do Chrome disponíveis para a versão estável mais recente. Há mais de 300 políticas que você pode aplicar a um portal da web. Para obter mais informações, consulte [the section called “Tutorial: Como configurar uma política de navegador personalizada”](#) e [Lista de políticas do Chrome Enterprise](#).

Ao usar a visualização do console para criar um portal da web, você pode aplicar as seguintes políticas:

- StartURL
- Favoritos e pastas de favoritos
- Ativar e desativar a navegação privada
- Exclusão do histórico
- Filtro de URL com AllowURL e BlockURL

Para obter mais informações sobre como usar políticas de visualização do console, consulte [Conceitos básicos](#).

WorkSpaces O Secure Browser aplica uma configuração básica da política do navegador a todos os portais junto com todas as políticas que você especificar. Você pode editar algumas dessas políticas com seu arquivo JSON personalizado. Para obter mais informações, consulte [the section called “Editar a política básica do navegador”](#).

Tópicos

- [Tutorial: Definindo uma política de navegador personalizada no Amazon WorkSpaces Secure Browser](#)
- [Editando a política básica do navegador no Amazon WorkSpaces Secure Browser](#)

Tutorial: Definindo uma política de navegador personalizada no Amazon WorkSpaces Secure Browser

É possível definir qualquer política compatível do Chrome para Linux carregando um arquivo JSON. Para saber mais sobre as políticas do Chrome, consulte a [Lista de políticas do Chrome Enterprise](#) e selecione a plataforma Linux. Depois, pesquise e revise as políticas da versão estável mais recente.

No tutorial a seguir, você cria um portal da web com os seguintes controles de política:

- Configurar favoritos
- Configurar páginas de inicialização padrão
- Impedir que o usuário instale outras extensões
- Impedir que o usuário exclua o histórico
- Impedir que o usuário acesse o modo de navegação anônima
- Pré-instale a extensão do [plug-in Okta](#) para todas as sessões.

Tópicos

- [Etapa 1: criar um portal da web](#)
- [Etapa 2: reunir políticas](#)
- [Etapa 3: criar um arquivo de política JSON personalizado](#)
- [Etapa 4: adicionar políticas ao modelo](#)
- [Etapa 5: carregue o arquivo JSON de política em seu portal da web](#)

Etapa 1: criar um portal da web

Para fazer o upload do arquivo JSON da política do Chrome, você deve criar um portal do Navegador WorkSpaces Seguro. Para obter mais informações, consulte [the section called “Criação de um portal da web”](#).

Etapa 2: reunir políticas

Pesquise e localize as políticas que você deseja na Política do Chrome. Depois, use as políticas para criar um arquivo JSON na próxima etapa.

1. Acesse a [Lista de políticas do Chrome Enterprise](#).
2. Escolha a plataforma Linux e selecione a versão mais recente do Chrome.
3. Pesquise as políticas que você deseja definir. Neste exemplo, pesquise extensões para encontrar políticas para gerenciá-las. Cada política inclui uma descrição, nome de preferência do Linux e valor de amostra.
4. Nos resultados da pesquisa, há três políticas que atendem aos requisitos empresariais se usadas em conjunto:
 - ExtensionSettings: instala uma extensão na inicialização do navegador.
 - ExtensionInstallBlocklist: impede que extensões específicas sejam instaladas.
 - ExtensionInstallAllowlist— Permite que determinadas extensões sejam instaladas.
5. Políticas adicionais atendem aos requisitos restantes:
 - ManagedBookmarks— Adiciona marcadores às páginas da web.
 - RestoreOnStartupURLs— Configura quais páginas da web são abertas sempre que uma nova janela do navegador é aberta.
 - AllowDeletingBrowserHistory— Configura se os usuários podem excluir seu histórico de navegação.
 - IncognitoModeAvailability— Configura se os usuários podem acessar o modo de navegação anônima.

Etapa 3: criar um arquivo de política JSON personalizado

Crie um arquivo JSON usando um editor de texto, um modelo e as políticas encontradas na etapa anterior.

1. Abra um editor de texto.
2. Copie e cole o seguinte modelo em seu editor de texto:

```
{
  "chromePolicies":
  {
```

```
"ManagedBookmarks":
{
  "value":
  [
    {
      "name": "Bookmark 1",
      "url": "bookmark-url-1"
    },
    {
      "name": "Bookmark 2",
      "url": "bookmark-url-2"
    }
  ]
},
"RestoreOnStartup":
{
  "value": 4
},
"RestoreOnStartupURLs":
{
  "value":
  [
    "startup-url"
  ]
},
"ExtensionInstallBlocklist": {
  "value": [
    "insert-extensions-value-to-block",
  ]
},
"ExtensionInstallAllowlist": {
  "value": [
    "insert-extensions-value-to-allow",
  ]
},
"ExtensionSettings":
{
  "value":
  {
    "insert-extension-value-to-force-install":
    {
      "installation_mode": "force_installed",
      "update_url": "https://clients2.google.com/service/update2/crx",
      "toolbar_pin": "force_pinned"
    }
  }
}
```

```
    },
  },
  "AllowDeletingBrowserHistory":
  {
    "value": should-allow-history-deletion
  },
  "IncognitoModeAvailability":
  {
    "value": incognito-mode-availability
  }
}
```

Etapa 4: adicionar políticas ao modelo

Adicione suas políticas personalizadas ao modelo para cada requisito empresarial.

1. Configurar marcador URLs.

- a. Abaixo da chave `value`, adicione pares de chaves `name` e `url` para cada marcador que você deseja adicionar.
- b. Defina `bookmark-url-1` como `https://www.amazon.com`.
- c. Defina `bookmark-url-2` como `https://docs.aws.amazon.com/workspaces-web/latest/adminguide/`.

```
"ManagedBookmarks":
  {
    "value":
    [
      {
        "name": "Amazon",
        "url": "https://www.amazon.com"
      },
      {
        "name": "Bookmark 2",
        "url": "https://docs.aws.amazon.com/workspaces-web/latest/  
adminguide/"
      }
    ]
  }
}
```

```
    },  
  ],  
},
```

2. Configure a inicialização URLs. Essa política permite que os administradores definam os sites exibidos quando um usuário abre uma nova janela do navegador.
 - a. Defina `RestoreOnStartup` como 4 . Isso define a `RestoreOnStartup` ação para abrir uma lista de URLs . Você também pode usar outras ações na sua startup URLs. Para obter mais informações, consulte [Lista de políticas do Chrome Enterprise](#).
 - b. Defina como `RestoreOnStartupURLs` `https://www.aboutamazon.com /news`.

```
"RestoreOnStartup":  
  {  
    "value": 4  
  },  
"RestoreOnStartupURLs":  
  {  
    "value":  
    [  
      "https://www.aboutamazon.com/news"  
    ]  
  },
```

3. Para evitar que o usuário exclua o histórico do navegador, defina `AllowDeletingBrowserHistory` como `false`.

```
"AllowDeletingBrowserHistory":  
  {  
    "value": false  
  },
```

4. Para desativar o acesso ao modo de navegação anônima para os usuários, defina `IncognitoModeAvailability` como 1.

```
"IncognitoModeAvailability":
```

```
{
  "value": 1
}
```

5. Defina e aplique o [plug-in Okta](#) com as seguintes políticas:

- **ExtensionSettings**: instala uma extensão na inicialização do navegador. O valor da extensão está disponível na página de ajuda do plug-in Okta.
- **ExtensionInstallBlocklist**: impede que extensões específicas sejam instaladas. Use um valor `*` para evitar todas as extensões por padrão. Os administradores podem controlar quais extensões permitir em **ExtensionInstallAllowlist**.
- **ExtensionInstallAllowlist** permite que você instale determinadas extensões. Já que **ExtensionInstallBlocklist** está definido como `*`, adicione o valor do plug-in Okta aqui para permiti-lo.

Veja a seguir um exemplo de política para ativar o plug-in Okta:

```
"ExtensionInstallBlocklist": {
  "value": [
    "*"
  ]
},
"ExtensionInstallAllowlist": {
  "value": [
    "glnpjglilkicbckjpbgcfkogebgllemb",
  ]
},
"ExtensionSettings": {
  "value": {
    "glnpjglilkicbckjpbgcfkogebgllemb": {
      "installation_mode": "force_installed",
      "update_url": "https://clients2.google.com/service/update2/crx",
      "toolbar_pin": "force_pinned"
    }
  }
}
```

Etapa 5: carregue o arquivo JSON de política em seu portal da web

1. Abra o console do WorkSpaces Secure Browser em https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#.
2. Escolha Navegador WorkSpaces seguro e, em seguida, escolha Portais da Web.
3. Selecione seu portal da web e escolha Editar.
4. Escolha Configurações da política e Carregamento do arquivo JSON.
5. Selecione Escolher arquivo. Navegue até o arquivo JSON, selecione-o e carregue-o.
6. Escolha Salvar.

Editando a política básica do navegador no Amazon WorkSpaces Secure Browser

Para fornecer o serviço, o WorkSpaces Secure Browser aplica uma política básica de navegador a todos os portais. Essa política base é aplicada além das que você especifica na visualização do console ou no carregamento do JSON. Veja a seguir a lista de políticas aplicadas pelo serviço no formato JSON:

```
{
  "chromePolicies":
  {
    "DefaultDownloadDirectory": {
      "value": "/home/as2-streaming-user/MyFiles/TemporaryFiles"
    },
    "DownloadDirectory": {
      "value": "/home/as2-streaming-user/MyFiles/TemporaryFiles"
    },
    "DownloadRestrictions": {
      "value": 1
    },
    "URLBlocklist": {
      "value": [
        "file://",
        "http://169.254.169.254",
        "http://[fd00:ec2::254]",
      ]
    },
    "URLAllowlist": {
```

```
    "value": [
      "file:///home/as2-streaming-user/MyFiles/TemporaryFiles",
      "file:///opt/appstream/tmp/TemporaryFiles",
    ]
  }
}
```

Os clientes não podem fazer alterações nas seguintes políticas:

- `DefaultDownloadDirectory`: essa política não pode ser editada. O serviço substitui todas as alterações nessa política.
- `DownloadDirectory`: essa política não pode ser editada. O serviço substitui todas as alterações nessa política.

Os clientes podem atualizar as seguintes políticas em seu portal da web:

- `DownloadRestrictions`: o padrão é definido como 1 para evitar downloads identificados como mal-intencionados pela Navegação segura do Chrome. Para obter mais informações, consulte [Bloquear o download de arquivos nocivos pelos usuários](#). É possível definir o valor de 0 para 4.
- As políticas `URLAllowlist` e `URLBlocklist` podem ser estendidas usando o recurso de filtragem de URL da visualização do console ou o carregamento de JSON. No entanto, a linha de base não URLs pode ser substituída. Essas políticas não são visíveis de um arquivo JSON baixado do seu portal da web. No entanto, se você acessar “chrome://policy” durante uma sessão, o navegador remoto exibirá as políticas aplicadas.

Configurando o editor de método de entrada para o Amazon WorkSpaces Secure Browser

Um editor de método de entrada (IME) é um utilitário que fornece opções ao usuário final para inserir texto em idiomas que usam um layout de teclado diferente do teclado QWERTY. IMEs ajudam os usuários a inserir texto em idiomas com conjuntos de idiomas maiores e mais complexos, como japonês, chinês e coreano. WorkSpaces As sessões do Secure Browser incluem suporte a IME por padrão. Os usuários podem selecionar idiomas alternativos na barra de ferramentas do IME na sessão ou usando atalhos de teclado.

Atualmente, os seguintes idiomas são suportados pelo IME do WorkSpaces Secure Browser:

- Inglês
- Chinês simplificado (pinyin)
- Chinês tradicional (bopomofo)
- Japonês
- Coreano

Para selecionar um idioma na barra de ferramentas do IME, faça o seguinte:

1. Selecione o menu suspenso do seletor de idiomas localizado no lado direito da barra preta do painel superior. Por padrão, o seletor mostrará en, para inglês.
2. No menu suspenso, escolha o idioma desejado.
3. No submenu exibido após a escolha de um idioma, selecione detalhes adicionais do idioma.

Para selecionar um idioma usando atalhos de teclado, faça o seguinte:

- Tudo IMEs
 - Para avançar o IME (ou mover para o layout direito do teclado), pressione Shift+Control+Left Alt.
- Japonês
 - Para escolher hiragana, pressione F6.
 - Para escolher katakana, pressione F7.
 - Para escolher latim, pressione F10.
 - Para escolher latim estendido, pressione F9.
 - Para escolher Entrada direta, pressione ALT +, ALT+@, Zenkaku Hankaku.
- Coreano
 - Para escolher hangul, pressione Shift+Space.
 - Para escolher hanja, pressione F9.

Para remover a barra de ferramentas e o menu do IME, ou para desativar o teclado virtual das sessões do Navegador WorkSpaces Seguro, entre em contato com. Suporte

Configurando a localização em sessão para o Amazon Secure Browser WorkSpaces

Quando um usuário inicia uma sessão, o WorkSpaces Secure Browser detecta as configurações de idioma e fuso horário do navegador local do usuário e as aplica à sessão. Isso afeta o idioma de exibição durante a sessão e ajuda a garantir que a hora exibida corresponda à hora atual na localização do usuário.

O idioma da sessão é determinado na seguinte ordem de prioridade:

1. A `ForcedLanguages` política nas configurações do navegador do portal da web. Para obter mais informações, consulte [ForcedLanguages](#).
2. A configuração do idioma do navegador local do usuário final.
3. O valor padrão, inglês (en-US).

O fuso horário é determinado pelas configurações de fuso horário local especificadas no navegador do usuário final. Se a configuração do fuso horário não for válida, o UTC será usado.

Os seguintes componentes no WorkSpaces Secure Browser oferecem suporte à localização:

- WorkSpaces Página de login do Secure Browser
- WorkSpaces Mensagens de status do portal do Secure Browser (incluindo mensagens de carregamento e erros)
- Navegador Chrome
- Menu de Contexto do sistema e janela Salvar como

Tópicos

- [Códigos de idioma compatíveis com o Amazon WorkSpaces Secure Browser](#)
- [Selecionar idiomas nas configurações de navegador do usuário](#)

Códigos de idioma compatíveis com o Amazon WorkSpaces Secure Browser

A lista a seguir mostra os códigos de idioma atualmente suportados pelo WorkSpaces Secure Browser. Se o navegador local do usuário estiver configurado para usar um código de idioma que não é compatível, o padrão da sessão será inglês (en-US).

- Alemão
 - de: alemão
 - de-AT: alemão (Áustria)
 - de-DE: alemão (Alemanha)
 - de-CH: alemão (Suíça)
 - De-LI: alemão (Liechtenstein)
- Inglês
 - en: inglês
 - en-AU: inglês (Austrália)
 - en-CA: inglês (Canadá)
 - en-IN: inglês (Índia)
 - en-NZ: inglês (Nova Zelândia)
 - en-ZA: inglês (África Meridional)
 - en-GB – Inglês (Reino Unido)
 - en-US – Inglês (Estados Unidos)
- Espanhol
 - es: espanhol
 - es-AR: espanhol (Argentina)
 - es-CL: espanhol (Chile)
 - es-CO: espanhol (Colômbia)
 - es-CR: espanhol (Costa Rica)
 - es-HN: espanhol (Honduras)
 - es-419: espanhol (América Latina)
 - es-MX: espanhol (México)
 - es-PE: espanhol (Peru)

- es-ES: espanhol (Espanha)
- es-US: espanhol (Estados Unidos)
- es-UY: espanhol (Uruguai)
- es-VE: espanhol (Venezuela)
- Francês
 - fr: francês
 - fr-CA: francês (Canadá)
 - fr-FR: francês (França)
 - fr-CH: francês (Suíça)
- Indonésio
 - id: indonésio
 - id-ID: indonésio (Indonésia)
- Italiano
 - it: italiano
 - it-IT: italiano (Itália)
 - it-CH: italiano (Suíça)
- Japonês
 - ja: japonês
 - Ja-JP: japonês (Japão)
- Coreano
 - ko: coreano
 - ko-KR: coreano (Coreia)
- Português
 - pt: português
 - pt-BR: português (Brasil)
 - pt-PT: português (Portugal)
- Chinês
 - zh: chinês
 - zh-CN: chinês (China)
 - zh-HK: chinês (Hong Kong)

- zh-TW: chinês (Taiwan)

Selecionar idiomas nas configurações de navegador do usuário

Para definir as configurações do navegador local do usuário, siga as etapas apropriadas.

- No Chrome, escolha Configurações, Idiomas e ordene os idiomas com base na preferência.
- No Firefox, escolha Configurações, Geral, Idioma e selecione o idioma no menu suspenso.
- No Edge, escolha Configurações, escolha Idiomas e ordene os idiomas com base na preferência.

Gerenciando controles de acesso IP no Amazon WorkSpaces Secure Browser

WorkSpaces O Navegador Seguro permite que você controle de quais endereços IP seu portal da web pode ser acessado. Ao usar as configurações de acesso de IP, é possível definir e gerenciar grupos de endereços IP confiáveis e só permitir que os usuários acessem seu portal quando estiverem conectados a uma rede confiável.

Por padrão, o WorkSpaces Secure Browser permite que os usuários acessem seu portal da web de qualquer lugar. Um grupo de controle de acesso de IP atua como um firewall virtual que filtra o endereço IP que um usuário pode usar para se conectar ao portal da web. Quando associadas ao seu portal da web, as configurações de acesso de IP detectarão o IP do usuário antes da autenticação para determinar se ele está qualificado a se conectar. Uma vez conectado, o WorkSpaces Secure Browser monitora continuamente o endereço IP do usuário para garantir que ele permaneça conectado a partir de uma rede confiável. Se o IP de um usuário mudar, o WorkSpaces Secure Browser detectará e encerrará a sessão.

Para especificar os intervalos de endereços CIDR, adicione regras ao seu grupo de controle de acesso de IP e, depois, associe o grupo ao seu portal da web. É possível associar cada configuração de acesso de IP a um ou mais portais da web. Para especificar os endereços IP públicos e intervalos de endereços IP para suas redes confiáveis, adicione regras para seus grupos de controle de acesso IP. Se os usuários acessam o portal da web por meio de um gateway NAT ou uma VPN, você deverá criar regras que permitam o tráfego de endereços IP públicos para o gateway NAT ou a VPN.

Note

Os clientes são responsáveis por compreender os possíveis problemas legais que surgem com o uso do WorkSpaces Secure Browser e devem garantir que o uso do WorkSpaces Secure Browser esteja em conformidade com todas as leis e regulamentos aplicáveis. Isso inclui leis que regulam a capacidade do empregador de monitorar o uso do Navegador WorkSpaces Seguro por um funcionário, incluindo atividades realizadas dentro do aplicativo.

Tópicos

- [Criação de um grupo de controle de acesso IP no Amazon WorkSpaces Secure Browser](#)
- [Associando uma configuração de acesso IP a um portal da web no Amazon WorkSpaces Secure Browser](#)
- [Editando um grupo de controle de acesso IP no Amazon WorkSpaces Secure Browser](#)
- [Excluindo um grupo de controle de acesso IP no Amazon WorkSpaces Secure Browser](#)

Criação de um grupo de controle de acesso IP no Amazon WorkSpaces Secure Browser

Para criar um grupo de controle de acesso de IP, siga estas etapas.

1. Abra o console do WorkSpaces Secure Browser em <https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/>.
2. No painel de navegação, selecione Controles de acesso a IP.
3. Selecione Criar grupo de controle de acesso IP.
4. Na caixa de diálogo Criar grupo de controle de acesso IP, insira um nome (obrigatório) e uma descrição (opcional) para o grupo.
5. Insira o endereço IP ou o intervalo de IP CIDR que será associado à Origem e uma Descrição (opcional).
6. Em Tags, escolha se deseja marcar um par de chave-valor para cada grupo de controle de acesso de IP.
7. Quando terminar de adicionar regras e tags, escolha Salvar.

Associando uma configuração de acesso IP a um portal da web no Amazon WorkSpaces Secure Browser

Para associar um grupo de controle de acesso de IP a um portal da web existente, siga estas etapas.

1. Abra o console do WorkSpaces Secure Browser em https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#.
2. No painel de navegação, selecione Portais da Web.
3. Selecione o portal da web e escolha Editar.
4. Em Grupo de controle de acesso de IP, selecione os grupos de controle de acesso de IP para o portal da web.
5. Escolha Salvar.

Para associar um grupo de controle de acesso de IP ao criar um portal da web, siga estas etapas.

1. Conclua as etapas de 1 a 4 em [the section called “Configurações de portal”](#) para acessar Controle de acesso de IP (opcional).
2. Escolha Criar controles de acesso de IP.
3. Na caixa de diálogo Criar grupo de IP, insira um nome (obrigatório) e uma descrição (opcional) para o grupo.
4. Insira o endereço IP ou o intervalo de IP CIDR que será associado à Origem e uma Descrição (opcional).
5. Em Tags, escolha se deseja marcar um par de chave-valor para cada grupo de controle de acesso de IP.
6. Quando terminar de adicionar regras e tags, escolha Criar controle de acesso de IP.
7. O grupo de controle de acesso IP será associado a esse portal da web quando iniciado.

Editando um grupo de controle de acesso IP no Amazon WorkSpaces Secure Browser

Você pode excluir uma regra de uma configuração de acesso de IP a qualquer momento. Se você remover uma regra que foi usada para permitir uma conexão com um portal da web, todos os usuários com uma sessão atual serão desconectados do portal da web.

Para editar um grupo de controle de acesso de IP, siga estas etapas.

1. Abra o console do WorkSpaces Secure Browser em https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#.
2. No painel de navegação, selecione Controles de acesso a IP.
3. Selecione o grupo e escolha Edit (Editar).
4. Edite a Origem e a Descrição (opcional) das regras existentes ou adicione outras regras.
5. Em Tags, escolha se deseja marcar um par de chave-valor para cada grupo de controle de acesso de IP.
6. Quando terminar de adicionar regras e tags, escolha Salvar.
7. Se você atualizou uma configuração de acesso de IP existente, aguarde até 15 minutos para que a regra nova ou editada entre em vigor.

Excluindo um grupo de controle de acesso IP no Amazon WorkSpaces Secure Browser

Você pode excluir uma regra de um grupo de controle de acesso IP a qualquer momento. Se você remover uma regra que foi usada para permitir uma conexão com um portal da web, todos os usuários com uma sessão atual serão desconectados do portal da web.

Para excluir um grupo de controle de acesso de IP, siga estas etapas.

1. Abra o console do WorkSpaces Secure Browser em https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#.
2. No painel de navegação, selecione Grupo de controle de acesso de IP.
3. Selecione o grupo e escolha Excluir.

Gerenciando a extensão de login único no Amazon WorkSpaces Secure Browser

É possível habilitar uma extensão para que os usuários finais tenham uma melhor experiência de login no portal. Por exemplo, se você usar o Okta como provedor de identidades (IdP) SAML 2.0 do seu portal e também usá-lo como o IdP dos sites que você deseja que os usuários acessem durante uma sessão, será possível passar o cookie de login do Okta para a sessão com a extensão.

Posteriormente, quando os usuários acessarem um site que requer o cookie de domínio Okta, eles não precisarão fazer login durante a sessão.

A extensão é compatível com os navegadores Chrome e Firefox. A extensão permite a sincronização de cookies para os domínios permitidos pelo login dos usuários na sessão. A extensão não exige que o usuário faça login e funciona nos bastidores para permitir a sincronização de cookies sem exigir que o usuário execute nenhuma ação após a instalação. Nenhum dado é armazenado pela extensão.

Por padrão, as extensões não estão habilitadas no Chrome nas janelas anônimas ou nas janelas de navegação privada do Firefox. Os usuários podem habilitá-las manualmente. Para obter mais informações sobre o Chrome, consulte [Extensões no modo de navegação anônima](#). Para obter mais informações sobre o Firefox, consulte [Extensões na navegação privativa](#).

Os usuários são solicitados a instalar a extensão quando fazem login em um portal. Para obter detalhes sobre a experiência do usuário com a extensão, consulte [the section called “Extensão de autenticação única”](#).

Tópicos

- [Identificação de domínios para a extensão de login único no Amazon Secure Browser WorkSpaces](#)
- [Adicionar a extensão de login único a um novo portal da web no Amazon WorkSpaces Secure Browser](#)
- [Adicionar a extensão de login único a um portal web existente no Amazon WorkSpaces Secure Browser](#)
- [Editando ou removendo a extensão de login único no Amazon WorkSpaces Secure Browser](#)

Identificação de domínios para a extensão de login único no Amazon Secure Browser WorkSpaces

Primeiro, determine quais domínios você precisa para o IdP SAML e sites. É possível adicionar até 10 domínios.

Você é responsável por testar e identificar o domínio apropriado para que os cookies sejam sincronizados. Pode ser necessário fazer alterações no nível de autenticação do IdP ou do site para garantir que a autenticação única funcione conforme o esperado.

Para ver quais domínios usar com o IdP mais comuns, consulte a tabela a seguir:

IdP e domínios

IdP	Domínio
Okta	okta.com
ID Entra	microsoftonline.com
Centro de Identidade da AWS	awsapps.com
One Login	onelogin.com
Duo	duosecurity.com

Adicionar a extensão de login único a um novo portal da web no Amazon WorkSpaces Secure Browser

Para permitir a extensão ao criar um portal da web, siga estas etapas.

1. Siga as etapas em [the section called “Criação de um portal da web”](#) até chegar a [the section called “Configurações de usuário”](#).
2. Para a etapa 1 de [the section called “Configurações de usuário”](#), em Permissões do usuário, escolha Permitido para habilitar a extensão para seu portal da web.
3. Insira o domínio para sincronização de cookies e escolha Adicionar novo domínio.
4. Conclua as etapas em [the section called “Configurações de usuário”](#) e as seções restantes em [the section called “Criação de um portal da web”](#) para criar seu portal da web.

Adicionar a extensão de login único a um portal web existente no Amazon WorkSpaces Secure Browser

Para adicionar a extensão a um portal da web existente, siga estas etapas.

1. Abra o console do WorkSpaces Secure Browser em <https://console.aws.amazon.com/workspaces-web/casa>.
2. Selecione o portal da web a ser editado.
3. Escolha Configurações do usuário, Permissões do usuário e Permitido para habilitar a extensão para seu portal da web.

4. Insira o domínio para sincronização de cookies e escolha Adicionar novo domínio.
5. Salve as alterações do portal. Os portais solicitarão que os usuários instalem a extensão em até 15 minutos.

Editando ou removendo a extensão de login único no Amazon WorkSpaces Secure Browser

Para editar domínios ou remover a extensão, siga estas etapas.

1. Abra o console do WorkSpaces Secure Browser em <https://console.aws.amazon.com/workspaces-web/casa>.
2. Selecione o portal da web a ser editado.
3. Escolha Configurações do usuário, Permissões do usuário e Não permitido para remover a extensão do seu portal da web.
4. Remova ou edite domínios individuais.
5. Depois de removidas, as sessões não sincronizarão mais os cookies, mesmo que o usuário tenha a extensão WorkSpaces Secure Browser instalada em seu navegador.

Configurando a filtragem de URL no Amazon WorkSpaces Secure Browser

Você pode usar a Política do Chrome para filtrar quais URLs usuários podem acessar a partir do navegador remoto. A Política do Chrome fornece dois mecanismos para filtrar URLs: URLAllowlist URLBlocklist e. Você pode usar a interface do console do WorkSpaces Secure Browser para configurar a filtragem de URL como uma configuração do portal ou adicioná-la como parte de sua instrução JSON personalizada (no editor embutido ou como um upload de arquivo JSON).

Tópicos

- [Configurando a filtragem de URL usando o console no Amazon WorkSpaces Secure Browser](#)
- [Configurando a filtragem de URL usando o editor JSON ou o upload de arquivos para o Amazon WorkSpaces Secure Browser](#)

Configurando a filtragem de URL usando o console no Amazon WorkSpaces Secure Browser

Para configurar a filtragem de URL usando o console, siga estas etapas.

1. Abra o console do WorkSpaces Secure Browser em [https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.](https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/)
2. Escolha Navegador WorkSpaces seguro, portais da Web, escolha seu portal da Web e, em seguida, escolha Exibir detalhes.
3. Para filtragem de URL, é possível escolher entre as opções a seguir:
 - Permitir acesso a todos URLs: Por padrão, um portal da web permite acesso a todos URLs. Você pode adicionar sites específicos à lista BlockURL para impedir que os usuários visitem esses sites durante uma sessão. Por exemplo, adicionar `www.anycorp.com` à lista BlockURL impedirá que o usuário navegue até `www.anycorp.com` durante a sessão.
 - Bloquear o acesso a todos URLs: por padrão, o portal da web bloqueia o acesso a todos os URLs. Você pode adicionar sites específicos à lista de URLs permitidos para organizar uma lista de sites que os usuários podem visitar e bloquear o tráfego para outros. Considere adicionar cada URL como um marcador para permitir o acesso com um clique para os usuários durante a sessão.
 - Configuração avançada: escolha essa opção para criar listas allowURL e blockURL em paralelo. A lista de permissões de URL tem prioridade sobre a lista de bloqueio de URL. Essa opção habilita a filtragem de URL por caminho. Por exemplo, você pode adicionar `www.anycorp.com` à lista de bloqueio e, em seguida, adicionar `www.anycorp.com/hr` à lista de permissões. Isso permite que os usuários visitem `www.anycorp.com/hr`, but they won't be able to access other URL paths, such as `www.anycorp.com/finance`.

Para obter mais orientações sobre como usar bloquear e permitir URLs, consulte [Permitir ou bloquear o acesso a sites](#). Adicione URLs a essas listas seguindo o formato de filtro de lista de bloqueio do Chrome para obter os melhores resultados. Para obter mais informações, consulte [Formato do filtro da lista de bloqueio de URLs](#).

Configurando a filtragem de URL usando o editor JSON ou o upload de arquivos para o Amazon WorkSpaces Secure Browser

Para configurar a filtragem de URL usando o editor JSON ou o upload de arquivo, siga estas etapas.

1. No módulo de Configurações de política, escolha Editor JSON e ignore o módulo de interface do usuário do console para a visualização de Editor ou Upload de arquivo.
 - O Editor permite que os clientes criem declarações de políticas personalizadas em linha no console. O Editor destaca os erros na instrução JSON durante a criação de uma política.
 - O Upload de arquivos permite que os clientes adicionem um arquivo JSON criado fora do console (como exportado de um navegador Chrome existente).
2. Consulte os detalhes da Política do Chrome para URLAllowlist URLBlocklist formatar adequadamente uma lista de permissão/negação de URL para seu portal da web. Para ter mais informações, consulte [URLAllowlist](#) e [URLBlocklist](#).

Links diretos no Amazon WorkSpaces Secure Browser

Quando um usuário faz login no WorkSpaces Secure Browser, ele inicia a sessão em uma página inicial definida pelo administrador. Você também pode permitir que os portais recebam deep links que conectam usuários a um site específico durante uma sessão. Quando um deep link é selecionado, o portal exibe o URL especificado no deep link. O link é exibido ao lado das páginas iniciais configuradas para o início da sessão ou por si só, se uma sessão já estiver em andamento. Esse recurso permite que os administradores criem experiências de usuário mais dinâmicas com o WorkSpaces Secure Browser.

Links diretos abrem páginas em uma sessão do WorkSpaces Secure Browser. Se uma sessão já estiver em execução, ela abrirá o deep link em uma nova guia. Se uma sessão ainda não estiver em execução, ela abrirá o URL do deep link em uma nova guia e a página inicial padrão do portal em uma guia separada. Se um deep link contiver mais de um URL, ele exibirá o primeiro da lista em foco, com cada URL subsequente (incluindo a página inicial padrão) aberto em guias separadas.

Tópicos

- [Configurando links diretos no Amazon WorkSpaces Secure Browser](#)
- [Usando a filtragem de URL para links diretos no Amazon WorkSpaces Secure Browser](#)

Configurando links diretos no Amazon WorkSpaces Secure Browser

Para dar a permissão a deep links, escolha Permitido ao criar as configurações do usuário. O site para o qual você deseja criar um deep link deve estar codificado em URL. Por exemplo, para vincular

um usuário a “https://www.example.com/? query=true”, atualize o link para %2F%3Fquery%3Dtrue. https%3A%2F%2Fwww.example.com

Um link direto pode conter até 10 URLs, delineado por vírgula. Por exemplo:

```
<uuid>https://.workspaces-web.com/? DeepLinks= %2F%3Fquery%3Dtrue, %2F%3Fquery%3Dtrue2, %2F%3Fquery%3Dtrue3, %2F%3Fquery%3Dtrue4https%3A%2F%2Fwww.example.com. https%3A%2F%2Fwww.example.com https%3A%2F%2Fwww.example.com https%3A%2F%2Fwww.example.com
```

Para obter mais informações sobre a permissão de deep links, consulte [the section called “Configurações de usuário”](#).

Usando a filtragem de URL para links diretos no Amazon WorkSpaces Secure Browser

Qualquer usuário com quem você compartilhar esse link do portal pode manipular o valor do deep link para visitar um site, se esse domínio estiver acessível a partir do portal e não estiver na lista de bloqueio de URL. Para criar uma lista restritiva de permissões ou lista de bloqueio para impedir que os usuários visitem domínios inadequados com seu portal, utilize a filtragem de URL.

A lista de permissões e de bloqueio de um portal podem ser editadas com a filtragem de URL nas configurações do navegador do seu portal. <uuid>Para fazer isso, anexe a URL a uma URL de portal listada como permitida no seguinte formato, em que UUID é a ID do portal: https://.workspaces-web.com/? DeepLinks= %2F%3Fquery%3Dtrue https%3A%2F%2Fwww.example.com

Para obter mais informações, consulte [the section called “Configurar a filtragem de URL”](#) e [Permitir ou bloquear o acesso a sites](#).

Usando o painel de gerenciamento de sessões no Amazon WorkSpaces Secure Browser

Use o painel de gerenciamento de sessões no console do WorkSpaces Secure Browser para monitorar e gerenciar sessões ativas e completas.

Acesso ao painel

Para acessar o painel, siga estas etapas.

Para acessar o painel

1. Abra o console do WorkSpaces Secure Browser em <https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/>.
2. Escolha Navegador WorkSpaces seguro, portais da Web e escolha seu portal da web.
3. Escolha a guia Sessão ou escolha Visualizar sessões para abrir o painel em um painel dividido abaixo.

Filtros do painel

No painel de sessões, você pode filtrar as sessões pelas seguintes propriedades ou valores:

- Status
 - Ativo: indica que uma sessão está sendo executada no momento. Para encerrar a sessão, consulte abaixo.
 - Encerrado: indica que uma sessão não está mais ativa.
- ID da sessão
- Nome de usuário
- Hora de início da sessão

Encerrar sessões

Para encerrar uma sessão, siga estas etapas.

Para encerrar uma sessão

1. No painel de sessões, selecione a sessão que deseja interromper.
2. Escolha Encerrar.
3. Usuários desconectados perdem todo o estado da sessão. Todas as guias abertas, o histórico do navegador e os arquivos baixados para o navegador seguro são reciclados.

Histórico da sessão

O painel contém sessões dos últimos 35 dias. Você pode usar a CLI para listar sessões, com ou sem filtro. O histórico da sessão é entregue como JSON, que os administradores podem processar, gerenciar e armazenar em um repositório separado.

Veja a seguir exemplos de comandos da CLI para gerenciar sessões na região US-West-2 (Oregon).

Para listar todas as sessões de um portal da web, execute o seguinte comando:

```
aws workspaces-web list-sessions --portal-arn arn:aws:workspaces-web:us-west-2:<accountId>:portal/<portalId>
```

Para listar todas as sessões de um usuário específico de um portal da web, execute o seguinte comando:

```
aws workspaces-web list-sessions --portal-arn arn:aws:workspaces-web:us-west-2:<accountId>:portal/<portalId> --username <username>
```

Protegendo dados em trânsito com endpoints FIPS e Amazon WorkSpaces Secure Browser

Por padrão, quando você se comunica com o serviço WorkSpaces Secure Browser como administrador usando o console, a AWS CLI (AWS Command Line Interface) ou um AWS SDK, ou durante a sessão de um usuário, todos os dados em trânsito são criptografados usando o TLS 1.2.

Se você precisar de módulos criptográficos validados pelo FIPS 140-3 ao acessar a AWS por meio de uma interface de linha de comandos ou de uma API, use um endpoint do FIPS. Quando você usa um endpoint do FIPS, todos os dados em trânsito são criptografados usando padrões criptográficos que estão em conformidade com o Federal Information Processing Standard (FIPS) 140-3. Para obter informações sobre endpoints FIPS, incluindo uma lista de endpoints do WorkSpaces Secure Browser, consulte <https://aws.amazon.com/compliance/fips>

Depois que um portal é criado com endpoints do FIPS, todas as sessões de usuário e alterações administrativas são feitas automaticamente usando endpoints 140-3 do FIPS. Você pode usar a variável do ambiente `AWS_USE_FIPS_ENDPOINT=true` para localizar endpoints do FIPS e enviar solicitações com o SDK. Veja um exemplo a seguir.

```
$ export AWS_USE_FIPS_ENDPOINT=true
```

```
$ aws workspaces-web list-portal
```

Você também pode usar a opção `--endpoint-url` de enviar solicitações diretamente para endpoints do FIPS. O exemplo a seguir é um exemplo de portais de lista de chamadas na região US-West-2 (Oregon):

```
$ aws workspaces-web list-portal --endpoint-url https://workspaces-web-fips.us-west-2.amazonaws.com
```

Gerenciando configurações de proteção de dados no Amazon WorkSpaces Secure Browser

As configurações de proteção de dados são usadas para ajudar a impedir que os dados sejam compartilhados durante uma sessão. As configurações podem ser criadas e aplicadas a vários portais.

Tópicos

- [Redação de dados em linha no Amazon WorkSpaces Secure Browser](#)
- [Configuração de redação padrão no Amazon WorkSpaces Secure Browser](#)
- [Baseie a redação em linha no Amazon Secure WorkSpaces Browser](#)
- [Redação embutida personalizada no Amazon WorkSpaces Secure Browser](#)
- [Crie configurações de proteção de dados no Amazon WorkSpaces Secure Browser](#)
- [Associe as configurações de proteção de dados no Amazon WorkSpaces Secure Browser](#)
- [Edite as configurações de proteção de dados no Amazon WorkSpaces Secure Browser](#)
- [Exclua as configurações de proteção de dados no Amazon WorkSpaces Secure Browser](#)

Redação de dados em linha no Amazon WorkSpaces Secure Browser

Ao adicionar a redação de dados em linha a um portal, você pode prever e redigir automaticamente determinados dados de uma sequência de texto exibida em páginas da web. Você pode criar políticas de redação escolhendo entre padrões incorporados (como números de previdência social ou números de cartão de crédito) ou criar seus próprios tipos de dados personalizados usando

expressões regulares e palavras-chave. As políticas incluem níveis configuráveis de fiscalização e controles sobre URLs onde a redação deve ser aplicada.

Os componentes a seguir determinam quando os dados são editados:

- Configurações de proteção de dados - Configurações de proteção de dados é o nome do recurso que inclui seus tipos de dados e critérios de imposição. Para utilizar esse recurso, primeiro crie suas configurações e, em seguida, associe-as a um portal. Quando os usuários iniciam uma sessão, suas configurações são aplicadas durante a sessão.
- Extensão do navegador na sessão - Quando você associa as configurações de redação ao seu portal, o navegador da sessão será iniciado com uma extensão de navegador imposta pelo sistema que impõe suas configurações. As configurações de proteção de dados impõem a redação por meio de correspondência de padrões (expressões regulares) e pesquisa por palavra-chave de acordo com seu nível de confiança e configuração de imposição de URL. O conteúdo é previsto a partir de sequências de texto e editado antes de ser exibido na tela. A extensão também define políticas de navegador relacionadas que controlam a capacidade dos usuários de contornar a redação (como navegação privada desativada, acesso às ferramentas do desenvolvedor e inspeção de rede).

As seguintes alterações na política do navegador Chrome são aplicadas pela extensão do navegador em sessão. Para obter mais informações, consulte [Lista de políticas do Chrome Enterprise](#).

- Aplique a política do navegador para impedir que os usuários visualizem a sessão sem redação:
 - [IncognitoModeAvailability](#) = 1
 - [DeveloperToolsAvailability](#) = 2
 - [BrowserAddPersonEnabled](#) = falso
 - [BrowserGuestModeEnabled](#) = falso
- A extensão também impede que os usuários baixem arquivos HTML URLs que estejam aplicando as configurações de proteção de dados cancelando o evento de download.

Em geral, você deve usar a redação com sites privados e estruturados (como suas ferramentas de gerenciamento de clientes, sistemas de emissão de bilhetes ou wikis), e não para navegação pública não estruturada (como Facebook ou Google). Você pode escolher entre os tipos de dados incorporados (veja abaixo a lista completa) ou definir tipos de dados personalizados usando seus próprios valores de expressão regular e palavras-chave. Os administradores são responsáveis por testar e validar se cada tipo de dados, nível de confiança e aplicação de URL estão funcionando

conforme o esperado. AWS não podemos garantir a compatibilidade com sites ou aplicativos personalizados fornecidos por terceiros.

WorkSpaces Atualmente, o Secure Browser não oferece suporte à redação de tipos de dados compatíveis ou personalizados em formatos não textuais, incluindo texto nos seguintes formatos:

- Imagens, como JPEG, PNG ou GIF
- Páginas da Web que permitem que os usuários usem processamento ou edição dinâmica de texto, como Google Docs ou Sheets
- Fluxos de áudio ou vídeo acessados no navegador, como YouTube vídeos
- PDFs visualizado pelo navegador Chrome

Não use redação para conteúdo em um formato não suportado. Os administradores são responsáveis por validar a compatibilidade do site e do conteúdo antes de conceder aos usuários acesso ao conteúdo que eles pretendem editar.

Configuração de redação padrão no Amazon WorkSpaces Secure Browser

A configuração de redação padrão aplicará automaticamente um nível de confiança e uma imposição de URL para todos os tipos de dados incorporados nas configurações de proteção de dados. Você tem a opção de substituir a configuração padrão ao adicionar um tipo de dados incorporado.

Os níveis de confiança permitem que você ajuste a lógica de redação para tipos de dados incorporados usando uma combinação de formato, palavras-chave e texto não formatado. Escolha o nível de rigor de como a redação é aplicada, incluindo Alto, Médio ou Baixo. O valor padrão será aplicado a todos os tipos de dados, a menos que uma substituição seja aplicada no nível do tipo de dados. Em geral, comece com uma configuração padrão do Medium e refine validando se a redação é aplicada conforme o esperado em seus sites.

Nível de confiança	Descrição	Exemplo
Alto	Requer uma correspondência de padrão de texto formatado para que o conteúdo seja editado.	O SSN de 123-45-6798 seria redigido, enquanto 123456789 não.
Médio	A redação considera texto formatado e não formatado	O SSN de 123-45-6798 seria editado. 123456789 seria

Nível de confiança	Descrição	Exemplo
	e adiciona a palavra-chave associada à lógica.	editado se detectado próximo a uma palavra-chave (como “número do seguro social”).
Baixo	Redação aplicada tanto para padrão formatado quanto para padrão não formatado sem palavra-chave.	Os SSN em qualquer formato - 123-45-6798 e 123456789 - são editados sem a necessidade de palavra-chave.

Você deve definir a configuração de redação padrão para todos os tipos de dados. Você pode escolher entre as seguintes opções:

- Tudo URLs
- Específico URLs
- Configuração avançada

O valor padrão será aplicado a todos os tipos de dados, a menos que uma substituição seja aplicada no nível do tipo de dados. A fiscalização de URL usa uma lógica semelhante à política do Chrome para gerenciar listas de permissões e bloqueios. Para obter orientação sobre como bloquear e permitir URLs, consulte [Permitir ou bloquear o acesso a sites](#). Para obter os melhores resultados, adicione essas listas seguindo URLs o formato de filtro de lista de bloqueio do Chrome. Para obter mais informações, consulte [Formato do filtro da lista de bloqueio de URLs](#).

Baseie a redação em linha no Amazon Secure WorkSpaces Browser

A redação de dados em linha tem suporte para padrões integrados (como números de previdência social e números de cartão de crédito), que você pode encontrar listados em Base de redação embutida. Escolha o (s) tipo (s) de dados no menu suspenso e especifique o valor de substituição para cada tipo de dados. Todos os tipos de dados seguem o padrão de imposição de configuração padrão acima, mas você pode optar por substituir o nível de confiança e ajustar o padrão de imposição de domínio para cada tipo de dados.

Para inserir um valor alternativo da configuração padrão, escolha Substituição do nível de confiança. Por exemplo, com a configuração padrão definida como Média, você pode notar durante o teste que um dos seus tipos de dados não está sendo editado de forma confiável. Você pode definir a

substituição como Baixa para aumentar a chance de redação, sem ajustar a lógica usada para seus outros tipos de dados.

Para ajustar a forma como a redação é aplicada URLs sem alterar a configuração padrão, aplique substituições de imposição de URL. Por exemplo, você pode definir o uso de substituições de URL para impor a redação de endereços de e-mail em seu sistema de gerenciamento de relacionamento com o cliente, sem interromper o acesso do usuário aos endereços de e-mail no site do diretório da empresa ou no e-mail baseado na web.

Veja a seguir uma lista de tipos de dados e seus padrões incorporados correspondentes IDs:

builtInPatternIdentificação	Tipo de dados
awsAccessKey:	Chave de acesso da AWS
awsSecretKey:	Chave secreta da AWS
Números do cartão:	Números de cartão de crédito
criptografia:	Endereços de criptomoeda
CusipNum:	Número CUSIP
data:	Data
Anum:	Números DEA dos EUA
cão:	Data de nascimento
Carteira de motorista:	Carteiras de motorista dos EUA
Endereço de e-mail:	Endereço de e-mail
uma:	Número de identificação do empregador dos EUA
Data de expiração:	Data de expiração do cartão de crédito
healthInsuranceNum:	Número de reclamação do seguro de saúde do Medicare

builtInPatternIdentificação	Tipo de dados
Código HIPAA:	Código HIPAA ICD-10
indivTaxId:	ID fiscal individual dos EUA
Endereço IP:	Endereço IP
está em:	Números de identificação de valores mobiliários internacionais
jato:	JSON Web Token
Coordenada de localização:	Coordenadas de localização
Endereço MAC:	MAC Address
medicareBeneficiaryId:	Número do beneficiário do Medicare
npi:	Número de identificação do provedor nacional
ndc:	Códigos Nacionais de Medicamentos (NDC)
Número do passaporte:	Número do passaporte dos EUA
Número de telefone:	Número de telefone
Número de roteamento:	Número de roteamento ABA
ssn:	Número do Seguro Social dos EUA
Código Swift:	Código SWIFT
hora:	Tempo
vinho:	Número de identificação do veículo nos EUA

Redação embutida personalizada no Amazon WorkSpaces Secure Browser

Os clientes podem definir seus próprios padrões usando expressões regulares, como aplicativos internos personalizados IDs. Para criar seu padrão de redação em linha personalizado, siga estas etapas:

1. Acesse sua configuração de proteção de dados.
2. Escolha Redação embutida personalizada e adicione.
3. Insira um nome para o tipo de dados personalizado.
4. Insira o valor da expressão regular.
 - Os valores da expressão regular devem corresponder à sintaxe literal da expressão JavaScript regular. Para obter mais informações, consulte [Expressões regulares](#). Um exemplo de expressão regular é `/ex[am]+ple/i`.
 - Certifique-se de testar seus padrões personalizados nos sites que você planeja oferecer suporte. Se os padrões personalizados forem escritos com erros, eles podem introduzir problemas de desempenho não intencionais.
5. Especifique o valor de substituição.
6. Escolha Mais opções para obter mais personalizações opcionais, incluindo as seguintes:
 - Adicione palavras-chave para ajustar a lógica de redação. As palavras-chave podem aumentar a precisão da fiscalização. Adicione palavras-chave na sintaxe literal da expressão regular do Javascript. Para obter mais informações, consulte [Expressões regulares](#).

Por exemplo, se você estiver criando um padrão de redação personalizado para o cliente IDs usado em um sistema interno, poderá adicionar `/client name/i` ao campo de palavra-chave para informar a lógica de digitalização e detecção.

- Aplique substituições de imposição de URL para ajustar a forma como a redação é aplicada URLs, sem alterar a configuração padrão.

Por exemplo, você pode definir o uso de substituições de URL para impor a redação de endereços de e-mail em seu sistema de gerenciamento de relacionamento com o cliente, sem interromper o acesso do usuário aos endereços de e-mail no site do diretório da empresa ou no e-mail baseado na web.

- Insira uma descrição (opcional) para o tipo de dados.

Crie configurações de proteção de dados no Amazon WorkSpaces Secure Browser

Você pode criar configurações de proteção de dados no WorkSpaces Secure Browser.

Para criar configurações de proteção de dados

1. Abra o console do WorkSpaces Secure Browser em https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#.
2. No painel de navegação à esquerda, escolha Configurações de proteção de dados.
3. Escolha Criar configurações de proteção de dados.
4. Insira um nome de exibição (obrigatório) e uma descrição (opcional) para a configuração.
5. Selecione as configurações padrão para redação em linha. Você pode definir o seguinte:
 - O nível de rigor de todos os tipos de dados
 - Os domínios nos quais a redação deve ser aplicada
6. Escolha seus tipos básicos de dados de redação em linha dentre os tipos compatíveis ou crie um tipo de dados personalizado. Você pode definir substituições para cada tipo de dados, incluindo o nível de rigor e as exceções de domínio.
7. Adicione quaisquer tags (opcional) para gerar relatórios.
8. Quando concluir, selecione Save.

Associe as configurações de proteção de dados no Amazon WorkSpaces Secure Browser

Você pode associar as configurações de proteção de dados no WorkSpaces Secure Browser.

Para associar uma configuração de proteção de dados a um portal existente

1. Abra o console do WorkSpaces Secure Browser em https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#.
2. No painel de navegação à esquerda, escolha Portais da Web.
3. Selecione o portal da web e escolha Editar.
4. Em Configurações de proteção de dados, selecione a configuração do seu portal.
5. Escolha Salvar.

Para associar uma configuração de proteção de dados ao criar um novo portal, siga estas etapas.

Para associar uma configuração de proteção de dados ao criar um novo portal

1. Siga as instruções em [the section called “Criação de um portal da web”](#) para criar um portal, até chegar à configuração de proteção de dados.
2. Escolha sua configuração de proteção de dados no menu suspenso.
3. Conclua as etapas [the section called “Criação de um portal da web”](#) para concluir a criação do seu portal.

Para criar uma configuração de proteção de dados ao criar um novo portal, siga estas etapas.

Para criar uma configuração de proteção de dados ao criar um novo portal

1. Siga as instruções em [the section called “Criação de um portal da web”](#) para criar um portal, até chegar à configuração de proteção de dados.
2. Escolha as configurações de proteção de dados no menu suspenso.
3. Insira um nome de exibição (obrigatório) e uma descrição (opcional) para a configuração.
4. Selecione as configurações padrão para redação em linha. Você pode definir o seguinte:
 - O nível de rigor de todos os tipos de dados
 - Os domínios nos quais a redação deve ser aplicada
5. Escolha seus tipos básicos de dados de redação em linha dentre os tipos compatíveis ou crie um tipo de dados personalizado. Você pode definir substituições para cada tipo de dados, incluindo o nível de rigor e as exceções de domínio.
6. Adicione quaisquer tags (opcional) para gerar relatórios.
7. Quando concluir, selecione Save.
8. Selecione o botão de atualização nas configurações de proteção de dados e, em seguida, escolha sua configuração de proteção de dados no menu suspenso.
9. Continue seguindo as instruções de criação do portal para concluir a criação do seu portal.

Edite as configurações de proteção de dados no Amazon WorkSpaces Secure Browser

Você pode editar as configurações de proteção de dados no WorkSpaces Secure Browser.

Para editar as configurações de proteção de dados

1. Abra o console do WorkSpaces Secure Browser em <https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/>.
2. Escolha as configurações de proteção de dados e a configuração de proteção de dados que você deseja editar na exibição em lista.
3. Você pode atualizar o nome, a descrição, as configurações padrão, os tipos de dados (compatíveis ou personalizados) e aplicar substituições de nível de confiança ou domínio.
4. Escolha Salvar.

Exclua as configurações de proteção de dados no Amazon WorkSpaces Secure Browser

Você pode excluir as configurações de proteção de dados no WorkSpaces Secure Browser.

Para excluir as configurações de proteção de dados

1. Se você tiver um portal associado a uma configuração de proteção de dados, primeiro remova a associação antes de excluir a configuração de proteção de dados.
2. Abra o console do WorkSpaces Secure Browser em <https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/>.
3. Escolha as configurações de proteção de dados e a configuração de proteção de dados que você deseja excluir da exibição em lista.
4. Escolha Excluir.

Gerenciamento de controles da barra de ferramentas no Amazon WorkSpaces Secure Browser

Com os controles da barra de ferramentas, você pode configurar a apresentação da barra de ferramentas para as sessões do usuário final, incluindo as seguintes opções:

- Atributos
 - Área de transferência: quando ativada, permite copiar/colar com controles granulares (somente copiar, somente colar ou ambos). Quando desativado, oculta o ícone e impede o uso da barra de ferramentas.

- **Transferência de arquivos:** quando ativada, permite operações de arquivo com controles granulares (somente upload, somente download ou ambos). Quando desativado, oculta o ícone e impede transferências.
- **Microfone:** quando ativado, permite o uso do microfone. Quando desativado, oculta o ícone.
- **Webcam:** quando ativada, permite o uso da câmera. Quando desativado, oculta o ícone.
- **Monitor duplo:** quando ativado, permite o uso de dois monitores. Quando desativado, oculta o ícone.
- **Tela cheia:** quando ativada, ativa o modo de tela cheia. Quando desativado, oculta o ícone.
- **Windows:** Quando ativado, permite mover-se entre janelas. Quando desativado, oculta o ícone.
- **Configurações**
 - **Tema da barra de ferramentas:** controla a exibição do modo claro ou escuro. A configuração remove o controle do tema do usuário final.
 - **Estado da barra de ferramentas:** define o estado encaixado ou desconectado da barra de ferramentas. A configuração remove o controle do usuário final sobre o estado da barra de ferramentas.
 - **Resolução máxima:** define a maior resolução de exibição permitida. Os usuários só podem selecionar resoluções até esse limite definido.

Segurança no Amazon WorkSpaces Secure Browser

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de uma arquitetura de data center e rede criada para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O [modelo de responsabilidade compartilhada](#) descreve isso como a segurança da nuvem e a segurança na nuvem:

- **Segurança da nuvem** — AWS é responsável por proteger a infraestrutura que executa AWS os serviços na AWS nuvem. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte dos Programas de Conformidade Programas de [AWS](#) de . Para saber mais sobre os programas de conformidade que se aplicam ao Amazon WorkSpaces Secure Browser, consulte [AWS Services in Scope by Compliance Program](#) .
- **Segurança na nuvem** — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade dos dados, os requisitos da empresa e quaisquer leis e regulamentos aplicáveis aos seus dados.

Essa documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar o Amazon WorkSpaces Secure Browser. Ele mostra como configurar o Amazon WorkSpaces Secure Browser para atender aos seus objetivos de segurança e conformidade. Você também aprende a usar outros AWS serviços que ajudam a monitorar e proteger seus recursos do Amazon WorkSpaces Secure Browser.

Conteúdo

- [Proteção de dados no Amazon WorkSpaces Secure Browser](#)
- [Identity and Access Management para o Amazon WorkSpaces Secure Browser](#)
- [Resposta a incidentes no Amazon WorkSpaces Secure Browser](#)
- [Validação de conformidade para o Amazon WorkSpaces Secure Browser](#)
- [Resiliência no Amazon WorkSpaces Secure Browser](#)
- [Segurança da infraestrutura no Amazon WorkSpaces Secure Browser](#)
- [Análise de configuração e vulnerabilidade no Amazon WorkSpaces Secure Browser](#)
- [Acesse APIs usando uma interface VPC endpoint \(\)AWS PrivateLink](#)

- [Melhores práticas de segurança para o Amazon WorkSpaces Secure Browser](#)

Proteção de dados no Amazon WorkSpaces Secure Browser

O [modelo de responsabilidade AWS compartilhada](#) se aplica à proteção de dados no Amazon WorkSpaces Secure Browser. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre o conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre a privacidade de dados, consulte as [Data Privacy FAQ](#). Para obter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog [AWS Shared Responsibility Model and RGPD](#) no Blog de segurança da AWS .

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail. Para obter informações sobre o uso de CloudTrail trilhas para capturar AWS atividades, consulte Como [trabalhar com CloudTrail trilhas](#) no Guia AWS CloudTrail do usuário.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-3 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para obter mais informações sobre os endpoints FIPS disponíveis, consulte [Federal Information Processing Standard \(FIPS\) 140-3](#).

É altamente recomendável que nunca sejam colocadas informações confidenciais ou sigilosas, como endereços de e-mail de clientes, em tags ou campos de formato livre, como um campo Nome. Isso

inclui quando você trabalha com o WorkSpaces Secure Browser ou outro Serviços da AWS usando o console AWS CLI, a API ou AWS SDKs. Quaisquer dados inseridos em tags ou em campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, é fortemente recomendável que não sejam incluídas informações de credenciais no URL para validar a solicitação nesse servidor.

Tópicos

- [Criptografia de dados no Amazon WorkSpaces Secure Browser](#)
- [Privacidade do tráfego entre redes no Amazon WorkSpaces Secure Browser](#)
- [Login de acesso do usuário no Amazon WorkSpaces Secure Browser](#)

Criptografia de dados no Amazon WorkSpaces Secure Browser

O Amazon WorkSpaces Secure Browser coleta dados de personalização do portal, como configurações do navegador, configurações do usuário, configurações de rede, informações do provedor de identidade, dados do armazenamento confiável e dados do certificado do armazenamento confiável. WorkSpaces O Secure Browser também coleta dados de políticas do navegador, preferências do usuário (para configurações do navegador) e registros de sessão. Os dados coletados são armazenados no Amazon DynamoDB e no Amazon S3. WorkSpaces O Secure Browser usa AWS Key Management Service para criptografia.

Para proteger seu conteúdo, siga estas diretrizes:

- Implemente o acesso com privilégios mínimos e crie funções específicas para serem usadas nas ações do Navegador WorkSpaces Seguro. Use modelos do IAM para criar um perfil de acesso total ou somente leitura. Para obter mais informações, consulte [AWS políticas gerenciadas para o WorkSpaces Secure Browser](#).
- Proteja os dados de ponta a ponta fornecendo uma chave gerenciada pelo cliente, para que o WorkSpaces Secure Browser possa criptografar seus dados em repouso com as chaves que você fornece.
- Tenha cuidado ao compartilhar domínios do portal e credenciais do usuário:
 - Os administradores devem fazer login no WorkSpaces console da Amazon e os usuários devem fazer login no portal do WorkSpaces Secure Browser.
 - Qualquer pessoa na internet pode acessar o portal da web, mas não pode iniciar uma sessão a menos que tenha credenciais de usuário válidas no portal.

- Os usuários podem encerrar suas sessões explicitamente escolhendo Encerrar sessão. Isso descarta a instância que hospeda a sessão do navegador e resulta no isolamento do navegador.

WorkSpaces O Secure Browser protege conteúdo e metadados por padrão, criptografando todos os dados confidenciais com AWS KMS. Ele coleta a política do navegador e as preferências do usuário para aplicar políticas e configurações durante as sessões do WorkSpaces Secure Browser. Se ocorrer um erro ao aplicar as configurações existentes, o usuário não poderá acessar novas sessões nem acessar os sites internos e as aplicações de SaaS da empresa.

Criptografia em repouso para o Amazon WorkSpaces Secure Browser

A criptografia em repouso é configurada por padrão e todos os dados do cliente (por exemplo, declarações de política do navegador, nomes de usuário, registros ou endereços IP) usados no Navegador WorkSpaces Seguro são criptografados usando AWS KMS. Por padrão, o WorkSpaces Secure Browser ativa a criptografia com uma chave AWS própria. Você também pode usar uma chave gerenciada pelo cliente (CMK), especificando sua CMK na criação de recursos. Este é o único valor aceito no momento via CLI.

Se você optar por passar uma CMK, a chave fornecida deverá ser uma AWS KMS chave de criptografia simétrica e você, como administrador, deverá ter as seguintes permissões:

```
kms:DescribeKey  
  
kms:GenerateDataKey  
  
kms:GenerateDataKeyWithoutPlaintext  
  
kms:Decrypt  
  
kms:ReEncryptTo  
kms:ReEncryptFrom
```

Se você usar uma CMK, precisará permitir que o responsável pelo serviço externo do WorkSpaces Secure Browser acesse a chave.

Para obter mais informações, consulte [Exemplo de política de chaves CMK com escopo definido com aws](#): SourceAccount

Sempre que possível, o WorkSpaces Secure Browser usará as credenciais do Forward Access Sessions (FAS) para acessar sua chave. Para obter mais informações sobre o FAS, consulte [Sessões de acesso direto](#).

Há casos em que o WorkSpaces Secure Browser pode precisar acessar sua chave de forma assíncrona. Ao listar o principal serviço externo do WorkSpaces Secure Browser em sua política de chaves, o WorkSpaces Secure Browser poderá realizar o conjunto permitido de operações criptográficas com sua chave.

Depois que um recurso é criado com a chave, ela não pode ser removida nem alterada. Se você usou uma CMK, você, como administrador que acessa o recurso, deve ter as seguintes permissões:

```
kms:GenerateDataKey
kms:GenerateDataKeyWithoutPlaintext
kms:Decrypt

kms:ReEncryptTo
kms:ReEncryptFrom
```

Se você ver um erro de Acesso negado ao usar o console, é provável que o usuário que está acessando o console não tenha as permissões necessárias para usar a CMK na chave atual.

Principais exemplos de políticas e escopo para o WorkSpaces Secure Browser

CMKs exigem a seguinte política fundamental:

```
{
  "Version": "2012-10-17",
  "Statement": [
    ...,
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource": "*"
    }
  ]
}
```

```
]
}
```

As seguintes permissões são exigidas pelo WorkSpaces Secure Browser:

- `kms:DescribeKey`— Valida se a AWS KMS chave fornecida está configurada corretamente.
- `kms:GenerateDataKeyWithoutPlaintext` `kms:GenerateDataKey` — Solicitação da AWS KMS chave para criar chaves de dados usadas para criptografar objetos.
- `kms:Decrypt`— Solicita a AWS KMS chave para descriptografar as chaves de dados criptografadas. Essas chaves de dados são usadas para criptografar seus dados.
- `kms:ReEncryptTo` `kms:ReEncryptFrom` — Solicitação da AWS KMS chave para permitir a recriptografia de ou para uma chave KMS.

Definindo o escopo das permissões do WorkSpaces Secure Browser em sua chave AWS KMS

Quando o diretor em uma declaração de política chave é um [diretor de AWS serviço](#), é altamente recomendável que você use [as chaves de condição SourceAccount globais `aws:SourceArn` ou `aws:`](#), além do contexto de criptografia.

O contexto de criptografia utilizado para um recurso sempre conterá uma entrada no formato `aws:workspaces-web:RESOURCE_TYPE:id` e o ID do recurso correspondente.

O ARN de origem e os valores da conta de origem são incluídos no contexto de autorização somente quando uma solicitação AWS KMS vem de outro AWS serviço. Essa combinação de condições implementa permissões de privilégio mínimo e evita um possível [cenário de auxiliar confuso](#). Para obter mais informações, consulte [Permissões para serviços da AWS nas políticas de chave](#).

```
"Condition": {
  "StringEquals": {
    "aws:SourceAccount": "AccountId",
    "kms:EncryptionContext:aws:workspaces-web:resourceType:id": "resourceId"
  },
  "ArnEquals": {
    "aws:SourceArn": [
      "arn:aws:workspaces-web:Region:AccountId:resourceType/resourceId"
    ]
  },
}
```

Note

Antes da criação do recurso, a política de chave deve usar apenas a Condição `aws:SourceAccount`, pois o ARN completo do recurso ainda não terá sido criado. Após a criação do recurso, a política de chave pode ser atualizada para incluir as Condições `aws:SourceArn` e `kms:EncryptionContext`.

Exemplo da política de chaves CMK com escopo definido com `aws:SourceAccount`

```
{
  "Version": "2012-10-17",
  "Statement": [
    ...,
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "<AccountId>"
        }
      }
    }
  ]
}
```

Exemplo da política de chave CMK com escopo definido e caractere curinga de recursos

aws:SourceArn

```
{
  "Version": "2012-10-17",
  "Statement": [
    ...,
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource": "*",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:workspaces-web:<Region>:<AccountId>:*/*"
        }
      }
    }
  ]
}
```

Exemplo da política de chaves CMK com escopo definido com **aws:SourceArn**

```
{
  "Version": "2012-10-17",
  "Statement": [
    ...,
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
    }
  ]
}
```

```

    "Action": [
      "kms:DescribeKey",
      "kms:GenerateDataKey",
      "kms:GenerateDataKeyWithoutPlaintext",
      "kms:Decrypt",
      "kms:ReEncryptTo",
      "kms:ReEncryptFrom"
    ],
    "Resource": "*",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": [
          "arn:aws:workspaces-web:<Region>:<AccountId>:portal/*",
          "arn:aws:workspaces-web:<Region>:<AccountId>:browserSettings/*",
          "arn:aws:workspaces-web:<Region>:<AccountId>:userSettings/*",
          "arn:aws:workspaces-web:<Region>:<AccountId>:ipAccessSettings/*"
        ]
      }
    }
  }
]
}

```

Note

Depois de criar o recurso, você pode atualizar o caractere curinga em `SourceArn` para ele. Se você usa o WorkSpaces Secure Browser para criar um novo recurso que exija acesso à CMK, certifique-se de atualizar sua política de chaves adequadamente.

Exemplo da política de chave CMK com **aws:SourceArn** e **EncryptionContext** específico do recurso

```

{
  "Version": "2012-10-17",
  "Statement": [
    ...,
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt portal",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      }
    },
  ],
}

```

```

    "Action": [
      "kms:DescribeKey",
      "kms:GenerateDataKey",
      "kms:GenerateDataKeyWithoutPlaintext",
      "kms:Decrypt",
      "kms:ReEncryptTo",
      "kms:ReEncryptFrom"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "<AccountId>",
        "kms:EncryptionContext:aws:workspaces-web:portal:id": "<portalId>"
      }
    }
  },
  {
    "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt userSettings",
    "Effect": "Allow",
    "Principal": {
      "Service": "workspaces-web.amazonaws.com"
    },
    "Action": [
      "kms:DescribeKey",
      "kms:GenerateDataKey",
      "kms:GenerateDataKeyWithoutPlaintext",
      "kms:Decrypt",
      "kms:ReEncryptTo",
      "kms:ReEncryptFrom"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "<AccountId>",
        "kms:EncryptionContext:aws:workspaces-web:userSettings:id":
"<userSettingsId>"
      }
    }
  },
  {
    "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt browserSettings",
    "Effect": "Allow",
    "Principal": {
      "Service": "workspaces-web.amazonaws.com"
    }
  }
}

```

```

    },
    "Action": [
      "kms:DescribeKey",
      "kms:GenerateDataKey",
      "kms:GenerateDataKeyWithoutPlaintext",
      "kms:Decrypt",
      "kms:ReEncryptTo",
      "kms:ReEncryptFrom"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "<AccountId>",
        "kms:EncryptionContext:aws:workspaces-web:browserSettings:id":
"<browserSettingsId>"
      }
    }
  },
  {
    "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt ipAccessSettings",
    "Effect": "Allow",
    "Principal": {
      "Service": "workspaces-web.amazonaws.com"
    },
    "Action": [
      "kms:DescribeKey",
      "kms:GenerateDataKey",
      "kms:GenerateDataKeyWithoutPlaintext",
      "kms:Decrypt",
      "kms:ReEncryptTo",
      "kms:ReEncryptFrom"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "<AccountId>",
        "kms:EncryptionContext:aws:workspaces-web:ipAccessSettings:id":
"<ipAccessSettingsId>"
      }
    }
  },
]
}

```

Note

Certifique-se de criar declarações separadas ao incluir um `EncryptionContext` específico do recurso na mesma política de chave. Para obter mais informações, consulte a seção [Usando vários pares de contexto de criptografia em kms:EncryptionContext: chave de contexto](#).

Criptografia em trânsito para o Amazon WorkSpaces Secure Browser

WorkSpaces O Secure Browser criptografa dados em trânsito por HTTPS e TLS 1.2. Você pode enviar uma solicitação WorkSpaces usando o console ou chamadas diretas de API. Os dados da solicitação transferidos são criptografados enviando tudo por meio de uma conexão HTTPS ou TLS. Os dados da solicitação podem ser transferidos do AWS console ou do AWS SDK para o WorkSpaces Secure Browser. AWS Command Line Interface

A criptografia em trânsito é configurada por padrão, e as conexões seguras (HTTPS, TLS) são configuradas por padrão.

Gerenciamento de chaves para o Amazon WorkSpaces Secure Browser

Você pode fornecer sua própria AWS KMS chave gerenciada pelo cliente para criptografar as informações do cliente. Se você não fornecer uma, o WorkSpaces Secure Browser usará uma AWS chave própria. É possível definir sua chave usando o SDK da AWS .

Privacidade do tráfego entre redes no Amazon WorkSpaces Secure Browser

Para proteger as conexões entre o WorkSpaces Secure Browser e os aplicativos locais, você usa o WorkSpaces Secure Browser para iniciar sessões do navegador dentro da sua própria VPC. A conexão com aplicativos locais é configurada em sua própria VPC e não é controlada pelo Secure Browser. WorkSpaces

Para proteger as conexões entre contas, o WorkSpaces Secure Browser usa uma função vinculada ao serviço para se conectar com segurança às contas dos clientes e executar operações em nome do cliente. Para obter mais informações, consulte [Usando funções vinculadas a serviços para o Amazon Secure WorkSpaces Browser](#).

Login de acesso do usuário no Amazon WorkSpaces Secure Browser

Os administradores podem registrar os eventos da sessão do WorkSpaces Secure Browser, incluindo visitas de início, término e URL. Esses logs são criptografados e entregues com segurança aos clientes por meio de um Amazon Kinesis Data Stream. As informações de navegação do registro de acesso do usuário não são AWS armazenadas nem estão disponíveis nas sessões sem o registro configurado. As visitas ao URL no modo de navegação anônima ou excluídas URLs do histórico do navegador não são registradas no registro de acesso do usuário.

Identity and Access Management para o Amazon WorkSpaces Secure Browser

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) para usar os recursos do WorkSpaces Secure Browser. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

- [Público](#)
- [Autenticar com identidades](#)
- [Gerenciar o acesso usando políticas](#)
- [Como o Amazon WorkSpaces Secure Browser funciona com o IAM](#)
- [Exemplos de políticas baseadas em identidade para o Amazon Secure WorkSpaces Browser](#)
- [AWS políticas gerenciadas para o WorkSpaces Secure Browser](#)
- [Solução de problemas de identidade e acesso ao Amazon WorkSpaces Secure Browser](#)
- [Usando funções vinculadas a serviços para o Amazon Secure WorkSpaces Browser](#)

Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz no WorkSpaces Secure Browser.

Usuário do serviço — Se você usa o serviço WorkSpaces Secure Browser para fazer seu trabalho, seu administrador fornecerá as credenciais e as permissões de que você precisa. À medida que você usa mais recursos do Navegador WorkSpaces Seguro para fazer seu trabalho, talvez precise de permissões adicionais. Compreenda como o acesso é gerenciado pode ajudar a solicitar as permissões corretas ao administrador. Se você não conseguir acessar um recurso no WorkSpaces Secure Browser, consulte [Solução de problemas de identidade e acesso ao Amazon WorkSpaces Secure Browser](#).

Administrador de serviços — Se você é responsável pelos recursos do Navegador WorkSpaces Seguro em sua empresa, provavelmente tem acesso total ao Navegador WorkSpaces Seguro. É seu trabalho determinar quais recursos e recursos do Navegador WorkSpaces Seguro seus usuários do serviço devem acessar. Envie as solicitações ao administrador do IAM para alterar as permissões dos usuários de serviço. Revise as informações nesta página para compreender os conceitos básicos do IAM. Para saber mais sobre como sua empresa pode usar o IAM com o WorkSpaces Secure Browser, consulte [Como o Amazon WorkSpaces Secure Browser funciona com o IAM](#).

Administrador do IAM — Se você for administrador do IAM, talvez queira saber detalhes sobre como criar políticas para gerenciar o acesso ao WorkSpaces Secure Browser. Para ver exemplos de políticas baseadas em identidade do WorkSpaces Secure Browser que você pode usar no IAM, consulte [Exemplos de políticas baseadas em identidade para o Amazon Secure WorkSpaces Browser](#)

Autenticar com identidades

A autenticação é a forma como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado AWS) como o Usuário raiz da conta da AWS, como usuário do IAM ou assumindo uma função do IAM.

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Usuários (IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login AWS, consulte [Como fazer login Conta da AWS no](#) Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para designar solicitações por conta própria, consulte [Versão 4 do AWS Signature para solicitações de API](#) no Guia do usuário do IAM.

Independente do método de autenticação usado, também pode ser necessário fornecer informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte [Autenticação multifator](#) no Guia do usuário do AWS IAM Identity Center e [Usar a autenticação multifator da AWS no IAM](#) no Guia do usuário do IAM.

Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário-raiz para tarefas diárias. Proteja as credenciais do usuário-raiz e use-as para executar as tarefas que somente ele puder executar. Para obter a lista completa das tarefas que exigem login como usuário-raiz, consulte [Tarefas que exigem credenciais de usuário-raiz](#) no Guia do Usuário do IAM.

Identidade federada

Como prática recomendada, exija que usuários humanos, incluindo usuários que precisam de acesso de administrador, usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório de usuários corporativo, de um provedor de identidade da web AWS Directory Service, do diretório do Identity Center ou de qualquer usuário que acesse usando credenciais fornecidas Serviços da AWS por meio de uma fonte de identidade. Quando as identidades federadas são acessadas Contas da AWS, elas assumem funções, e as funções fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, é recomendável usar o AWS IAM Identity Center. Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todos os seus Contas

da AWS aplicativos. Para obter mais informações sobre o Centro de Identidade do IAM, consulte [O que é o Centro de Identidade do IAM?](#) no Guia do Usuário do AWS IAM Identity Center .

Usuários e grupos do IAM

Um [usuário do IAM](#) é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, é recomendável contar com credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, é recomendável alternar as chaves de acesso. Para obter mais informações, consulte [Alternar as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo](#) no Guia do Usuário do IAM.

Um [grupo do IAM](#) é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdminse conceder a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte [Casos de uso para usuários do IAM](#) no Guia do usuário do IAM.

Perfis do IAM

Uma [função do IAM](#) é uma identidade dentro da sua Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Para assumir temporariamente uma função do IAM no AWS Management Console, você pode [alternar de um usuário para uma função do IAM \(console\)](#). Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando uma URL personalizada. Para obter mais informações sobre métodos para usar perfis, consulte [Métodos para assumir um perfil](#) no Guia do usuário do IAM.

Perfis do IAM com credenciais temporárias são úteis nas seguintes situações:

- **Acesso de usuário federado:** para atribuir permissões a identidades federadas, é possível criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas por ele. Para ter mais informações sobre perfis para federação, consulte [Criar um perfil para um provedor de identidade de terceiros \(federação\)](#) no Guia do usuário do IAM. Se usar o Centro de Identidade do IAM,

configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o Centro de Identidade do IAM correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte [Conjuntos de Permissões](#) no Guia do Usuário do AWS IAM Identity Center .

- Permissões temporárias para usuários do IAM: um usuário ou um perfil do IAM pode presumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas: é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para conhecer a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte [Acesso a recursos entre contas no IAM](#) no Guia do usuário do IAM.
- Acesso entre serviços — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos na Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões da entidade principal da chamada, usando um perfil de serviço ou um perfil vinculado ao serviço.
- Sessões de acesso direto (FAS) — Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte [Sessões de acesso direto](#).
- Perfil de serviço: um perfil de serviço é um [perfil do IAM](#) que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte [Criar um perfil para delegar permissões a um AWS service \(Serviço da AWS\)](#) no Guia do Usuário do IAM.
- Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um AWS service (Serviço da AWS) O serviço pode presumir o perfil de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para perfis vinculados ao serviço.

- Aplicativos em execução na Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma EC2 instância e fazendo solicitações AWS CLI de AWS API. Isso é preferível a armazenar chaves de acesso na EC2 instância. Para atribuir uma AWS função a uma EC2 instância e disponibilizá-la para todos os aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém a função e permite que programas em execução na EC2 instância recebam credenciais temporárias. Para obter mais informações, consulte [Usar uma função do IAM para conceder permissões a aplicativos executados em EC2 instâncias da Amazon](#) no Guia do usuário do IAM.

Gerenciar o acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte [Visão geral das políticas JSON](#) no Guia do usuário do IAM.

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e perfis não têm permissões. Para conceder permissão aos usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem assumir os perfis.

As políticas do IAM definem permissões para uma ação independentemente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de função da AWS Management Console AWS CLI, da ou da AWS API.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que

condições. Para saber como criar uma política baseada em identidade, consulte [Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente](#) no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte [Escolher entre políticas gerenciadas e políticas em linha](#) no Guia do usuário do IAM.

Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o atributo ao qual a política está anexada, a política define quais ações uma entidade principal especificado pode executar nesse atributo e em que condições. Você deve [especificar uma entidade principal](#) em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

O Amazon S3 e o AWS WAF Amazon VPC são exemplos de serviços que oferecem suporte. ACLs Para saber mais ACLs, consulte a [visão geral da lista de controle de acesso \(ACL\)](#) no Guia do desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- **Limites de permissões:** um limite de permissões é um recurso avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte [Limites de permissões para identidades do IAM](#) no Guia do usuário do IAM.
- **Políticas de controle de serviço (SCPs)** — SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em AWS Organizations. AWS Organizations é um serviço para agrupar e gerenciar centralmente várias Contas da AWS que sua empresa possui. Se você habilitar todos os recursos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as suas contas. O SCP limita as permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre Organizations e SCPs, consulte [Políticas de controle de serviços](#) no Guia AWS Organizations do Usuário.
- **Políticas de controle de recursos (RCPs)** — RCPs são políticas JSON que você pode usar para definir o máximo de permissões disponíveis para recursos em suas contas sem atualizar as políticas do IAM anexadas a cada recurso que você possui. O RCP limita as permissões para recursos nas contas dos membros e pode afetar as permissões efetivas para identidades, incluindo a Usuário raiz da conta da AWS, independentemente de pertencerem à sua organização. Para obter mais informações sobre Organizations e RCPs, incluindo uma lista Serviços da AWS desse suporte RCPs, consulte [Políticas de controle de recursos \(RCPs\)](#) no Guia AWS Organizations do usuário.
- **Políticas de sessão:** são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em recursos. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte [Políticas de sessão](#) no Guia do usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte [Lógica de avaliação de políticas](#) no Guia do usuário do IAM.

Como o Amazon WorkSpaces Secure Browser funciona com o IAM

Antes de usar o IAM para gerenciar o acesso ao WorkSpaces Secure Browser, saiba quais recursos do IAM estão disponíveis para uso com o WorkSpaces Secure Browser.

Recursos do IAM que você pode usar com o Amazon WorkSpaces Secure Browser

Atributo do IAM	WorkSpaces Suporte ao Secure Browser
Políticas baseadas em identidade	Sim
Políticas baseadas em recurso	Não
Ações de políticas	Sim
Recursos de políticas	Sim
Chaves de condição de políticas	Sim
ACLs	Não
ABAC (tags em políticas)	Parcial
Credenciais temporárias	Sim
Permissões de entidade principal	Sim
Perfis de serviço	Não
Funções vinculadas ao serviço	Sim

Para ter uma visão de alto nível de como o WorkSpaces Secure Browser e outros AWS serviços funcionam com a maioria dos recursos do IAM, consulte [AWS os serviços que funcionam com o IAM](#) no Guia do usuário do IAM.

Tópicos

- [Políticas baseadas em identidade para WorkSpaces o Secure Browser](#)
- [Políticas baseadas em recursos no Secure WorkSpaces Browser](#)
- [Ações de política para o WorkSpaces Secure Browser](#)
- [Recursos de política para o WorkSpaces Secure Browser](#)
- [Chaves de condição de política para o WorkSpaces Secure Browser](#)
- [Listas de controle de acesso \(ACLs\) no WorkSpaces Secure Browser](#)
- [Controle de acesso baseado em atributos \(ABAC\) com Secure Browser WorkSpaces](#)
- [Usando credenciais temporárias com o WorkSpaces Secure Browser](#)
- [Permissões principais entre serviços para o WorkSpaces Secure Browser](#)
- [Funções de serviço para o WorkSpaces Secure Browser](#)
- [Funções vinculadas ao serviço para WorkSpaces o Secure Browser](#)

Políticas baseadas em identidade para WorkSpaces o Secure Browser

Compatível com políticas baseadas em identidade: sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário do IAM, grupo de usuários ou perfil. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte [Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente](#) no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações e recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou perfil ao qual ela está anexada. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte [Referência de elemento de política JSON do IAM](#) no Guia do usuário do IAM.

Exemplos de políticas baseadas em identidade para WorkSpaces o Secure Browser

Para ver exemplos de políticas baseadas em identidade do WorkSpaces Secure Browser, consulte [Exemplos de políticas baseadas em identidade para o Amazon Secure WorkSpaces Browser](#)

Políticas baseadas em recursos no Secure WorkSpaces Browser

Compatibilidade com políticas baseadas em recursos: não

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o atributo ao qual a política está anexada, a política define quais ações uma entidade principal especificado pode executar nesse atributo e em que condições. Você deve [especificar uma entidade principal](#) em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Para permitir o acesso entre contas, você pode especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em recursos. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando o principal e o recurso são diferentes Contas da AWS, um administrador do IAM na conta confiável também deve conceder permissão à entidade principal (usuário ou função) para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a uma entidade principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Consulte mais informações em [Acesso a recursos entre contas no IAM](#) no Guia do usuário do IAM.

Ações de política para o WorkSpaces Secure Browser

Compatível com ações de políticas: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Action` de uma política JSON descreve as ações que podem ser usadas para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da operação de AWS API associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista de ações do WorkSpaces Secure Browser, consulte [Ações definidas pelo Amazon WorkSpaces Secure Browser](#) na Referência de Autorização de Serviço.

As ações de política no WorkSpaces Secure Browser usam o seguinte prefixo antes da ação:

```
workspaces-web
```

Para especificar várias ações em uma única declaração, separe-as com vírgulas.

```
"Action": [  
  "workspaces-web:action1",  
  "workspaces-web:action2"  
]
```

Para ver exemplos de políticas baseadas em identidade do WorkSpaces Secure Browser, consulte [Exemplos de políticas baseadas em identidade para o Amazon Secure WorkSpaces Browser](#)

Recursos de política para o WorkSpaces Secure Browser

Compatível com recursos de políticas: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática recomendada, especifique um recurso usando seu [nome do recurso da Amazon \(ARN\)](#). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem compatibilidade com permissões em nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

```
"Resource": "*"
```

Para ver uma lista dos tipos de recursos do Navegador WorkSpaces Seguro e seus ARNs, consulte [Recursos definidos pelo Amazon WorkSpaces Secure Browser](#) na Referência de Autorização de

Serviço. Para saber com quais ações você pode especificar o ARN de cada recurso, consulte [Ações definidas pelo Amazon WorkSpaces Secure Browser](#).

Para ver exemplos de políticas baseadas em identidade do WorkSpaces Secure Browser, consulte [Exemplos de políticas baseadas em identidade para o Amazon Secure WorkSpaces Browser](#)

Chaves de condição de política para o WorkSpaces Secure Browser

Compatível com chaves de condição de política específicas de serviço: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Condition` (ou bloco `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usem [agentes de condição](#), como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos de `Condition` em uma declaração ou várias chaves em um único elemento de `Condition`, a AWS os avaliará usando uma operação lógica AND. Se você especificar vários valores para uma única chave de condição, AWS avalia a condição usando uma OR operação lógica. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um recurso somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte [Elementos da política do IAM: variáveis e tags](#) no Guia do usuário do IAM.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição AWS globais, consulte as [chaves de contexto de condição AWS global](#) no Guia do usuário do IAM.

Para ver uma lista das chaves de condição do WorkSpaces Secure Browser, consulte [Chaves de condição do Amazon WorkSpaces Secure Browser](#) na Referência de Autorização de Serviço. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte [Ações definidas pelo Amazon WorkSpaces Secure Browser](#).

Para ver exemplos de políticas baseadas em identidade do WorkSpaces Secure Browser, consulte [Exemplos de políticas baseadas em identidade para o Amazon Secure WorkSpaces Browser](#)

Listas de controle de acesso (ACLs) no WorkSpaces Secure Browser

Suportes ACLs: Não

As listas de controle de acesso (ACLs) controlam quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

Controle de acesso baseado em atributos (ABAC) com Secure Browser WorkSpaces

Compatível com ABAC (tags em políticas): parcial

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define as permissões com base em atributos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a entidades do IAM (usuários ou funções) e a vários AWS recursos. Marcar de entidades e atributos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso que ela estiver tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações em que o gerenciamento de políticas se torna um problema.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no [elemento de condição](#) de uma política usando as `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou chaves de condição `aws:TagKeys`.

Se um serviço for compatível com as três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço for compatível com as três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para obter mais informações sobre o ABAC, consulte [Definir permissões com autorização do ABAC](#) no Guia do usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte [Usar controle de acesso baseado em atributos \(ABAC\)](#) no Guia do usuário do IAM.

Usando credenciais temporárias com o WorkSpaces Secure Browser

Compatível com credenciais temporárias: sim

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS "[Trabalhe com o IAM](#)" no Guia do usuário do IAM.

Você está usando credenciais temporárias se fizer login AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS usando o link de login único (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar funções, consulte [Alternar para um perfil do IAM \(console\)](#) no Guia do usuário do IAM.

Você pode criar manualmente credenciais temporárias usando a AWS API AWS CLI ou. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para obter mais informações, consulte [Credenciais de segurança temporárias no IAM](#).

Permissões principais entre serviços para o WorkSpaces Secure Browser

Compatibilidade com o recurso de encaminhamento de sessões de acesso (FAS): sim

Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte [Sessões de acesso direto](#).

Funções de serviço para o WorkSpaces Secure Browser

Compatível com perfis de serviço: não

O perfil de serviço é um [perfil do IAM](#) que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte [Criar um perfil para delegar permissões a um AWS service \(Serviço da AWS\)](#) no Guia do Usuário do IAM.

Warning

Alterar as permissões de uma função de serviço pode interromper a funcionalidade do Navegador WorkSpaces Seguro. Edite as funções de serviço somente quando o WorkSpaces Secure Browser fornecer orientação para fazer isso.

Funções vinculadas ao serviço para WorkSpaces o Secure Browser

Compatibilidade com perfis vinculados a serviços: sim

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um AWS service (Serviço da AWS). O serviço pode presumir o perfil de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para funções vinculadas ao serviço.

Para obter detalhes sobre como criar ou gerenciar perfis vinculados a serviços, consulte [Serviços da AWS que funcionam com o IAM](#). Encontre um serviço na tabela que inclua um Yes na coluna Perfil vinculado ao serviço. Escolha o link Sim para visualizar a documentação do perfil vinculado a serviço desse serviço.

Exemplos de políticas baseadas em identidade para o Amazon Secure WorkSpaces Browser

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos do Navegador WorkSpaces Seguro. Eles também não podem realizar tarefas usando a AWS API AWS Management Console, AWS Command Line Interface (AWS CLI) ou. Para conceder permissão aos usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem assumir os perfis.

Para aprender a criar uma política baseada em identidade do IAM ao usar esses documentos de política em JSON de exemplo, consulte [Criar políticas do IAM \(console\)](#) no Guia do usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos pelo WorkSpaces Secure Browser, incluindo o formato de cada um dos tipos de recursos, consulte [Ações, recursos e chaves de condição para o Amazon WorkSpaces Secure Browser](#) na Referência de autorização de serviço.

ARNs

Tópicos

- [Melhores práticas de política baseada em identidade para o Amazon WorkSpaces Secure Browser](#)
- [Usando o console do Amazon WorkSpaces Secure Browser](#)
- [Permitindo que os usuários visualizem suas próprias permissões para o Amazon WorkSpaces Secure Browser](#)

Melhores práticas de política baseada em identidade para o Amazon WorkSpaces Secure Browser

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos do Navegador WorkSpaces Seguro em sua conta. Essas ações podem incorrer em custos para sua Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para obter mais informações, consulte [Políticas gerenciadas pela AWS](#) ou [Políticas gerenciadas pela AWS para funções de trabalho](#) no Guia do usuário do IAM.
- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte [Políticas e permissões no IAM](#) no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como AWS CloudFormation. Para obter mais informações, consulte [Elementos da política JSON do IAM: condição](#) no Guia do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de cem verificações de política e recomendações práticas para ajudar a criar políticas seguras e funcionais. Para obter mais informações, consulte [Validação de políticas do IAM Access Analyzer](#) no Guia do Usuário do IAM.
- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter

mais informações, consulte [Configuração de acesso à API protegido por MFA](#) no Guia do Usuário do IAM.

Para obter mais informações sobre as práticas recomendadas do IAM, consulte [Práticas recomendadas de segurança no IAM](#) no Guia do usuário do IAM.

Usando o console do Amazon WorkSpaces Secure Browser

Para acessar o console do Amazon WorkSpaces Secure Browser, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os recursos do Navegador WorkSpaces Seguro em seu Conta da AWS. Caso crie uma política baseada em identidade mais restritiva que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis) com essa política.

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para a API AWS CLI ou para a AWS API. Em vez disso, permita o acesso somente a ações que correspondam à operação de API que estiverem tentando executar.

Para garantir que usuários e funções ainda possam usar o console do Navegador WorkSpaces Seguro, anexe também o Navegador WorkSpaces Seguro ConsoleAccess ou a política ReadOnly AWS gerenciada às entidades. Para obter informações, consulte [Adicionar permissões a um usuário](#) no Guia do usuário do IAM.

Permitindo que os usuários visualizem suas próprias permissões para o Amazon WorkSpaces Secure Browser

Este exemplo mostra como criar uma política que permita que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando a API AWS CLI ou AWS .

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",

```

```
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
    ],
    "Resource": ["arn:aws:iam::*:user/${aws:username}"]
},
{
    "Sid": "NavigateInConsole",
    "Effect": "Allow",
    "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
    ],
    "Resource": "*"
}
]
```

AWS políticas gerenciadas para o WorkSpaces Secure Browser

Para adicionar permissões a usuários, grupos e funções, é mais fácil usar políticas AWS gerenciadas do que escrever políticas você mesmo. É necessário tempo e experiência para [criar políticas gerenciadas pelo cliente do IAM](#) que fornecem à sua equipe apenas as permissões de que precisam. Para começar rapidamente, você pode usar nossas políticas AWS gerenciadas. Essas políticas abrangem casos de uso comuns e estão disponíveis em sua AWS conta. Para obter mais informações sobre políticas AWS gerenciadas, consulte [políticas AWS gerenciadas](#) no Guia do usuário do IAM.

AWS os serviços mantêm e atualizam as políticas AWS gerenciadas. Você não pode alterar as permissões nas políticas AWS gerenciadas. Ocasionalmente, os serviços podem adicionar permissões adicionais a uma política AWS gerenciada para oferecer suporte a novos recursos. Esse tipo de atualização afeta todas as identidades (usuários, grupos e funções) em que a política está

anexada. É mais provável que os serviços atualizem uma política gerenciada pela AWS quando um novo recurso for iniciado ou novas operações se tornarem disponíveis. Os serviços não removem as permissões de uma política AWS gerenciada, portanto, as atualizações de políticas não violarão suas permissões existentes.

Além disso, AWS oferece suporte a políticas gerenciadas para funções de trabalho que abrangem vários serviços. Por exemplo, a política `ReadOnlyAccess` AWS gerenciada fornece acesso somente de leitura a todos os AWS serviços e recursos. Quando um serviço lança um novo recurso, AWS adiciona permissões somente de leitura para novas operações e recursos. Para obter uma lista e descrições das políticas de perfis de trabalho, consulte [Políticas gerenciadas pela AWS para perfis de trabalho](#) no Guia do usuário do IAM.

Tópicos

- [AWS política gerenciada: `AmazonWorkSpacesWebServiceRolePolicy`](#)
- [AWS política gerenciada: `AmazonWorkSpacesSecureBrowserReadOnly`](#)
- [AWS política gerenciada: `AmazonWorkSpacesWebReadOnly`](#)
- [WorkSpaces Atualizações do Secure Browser para políticas AWS gerenciadas](#)

AWS política gerenciada: `AmazonWorkSpacesWebServiceRolePolicy`

Não é possível anexar a política `AmazonWorkSpacesWebServiceRolePolicy` às suas entidades do IAM. Essa política é anexada a uma função vinculada ao serviço que permite que o WorkSpaces Secure Browser execute ações em seu nome. Para obter mais informações, consulte [the section called “Uso de perfis vinculados ao serviço”](#).

Essa política concede permissões administrativas que permitem acesso aos AWS serviços e recursos usados ou gerenciados pelo WorkSpaces Secure Browser.

Detalhes de permissões

Esta política inclui as seguintes permissões:

- **workspaces-web**— Permite acesso a AWS serviços e recursos usados ou gerenciados pelo WorkSpaces Secure Browser.
- **ec2**— permite que os diretores descrevam VPCs, sub-redes e zonas de disponibilidade; criem, marquem, descrevam e excluam interfaces de rede; associem ou desassociem um endereço; e descrevam tabelas de rotas, grupos de segurança e endpoints de VPC.
- **CloudWatch**: permite que as entidades principais coloquem dados de métricas.
- **Kinesis**: permite que as entidades principais descrevam um resumo dos fluxos de dados do Kinesis e coloquem registros nos fluxos de dados do Kinesis para registro em log de acesso do usuário. Para obter mais informações, consulte [the section called “Configurar o registro de acesso do usuário”](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    }
  ],
}
```

```

    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface"
      ],
      "Resource": "arn:aws:ec2:*:*:network-interface/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/WorkSpacesWebManaged": "true"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:*:*:network-interface/*",
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction": "CreateNetworkInterface"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "WorkSpacesWebManaged"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2>DeleteNetworkInterface"
      ],
      "Resource": "arn:aws:ec2:*:*:network-interface/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/WorkSpacesWebManaged": "true"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [

```

```

        "cloudwatch:PutMetricData"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "cloudwatch:namespace": [
                "AWS/WorkSpacesWeb",
                "AWS/Usage"
            ]
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "kinesis:PutRecord",
        "kinesis:PutRecords",
        "kinesis:DescribeStreamSummary"
    ],
    "Resource": "arn:aws:kinesis:*:*:stream/amazon-workspaces-web-*"
}
]
}

```

AWS política gerenciada: AmazonWorkSpacesSecureBrowserReadOnly

É possível anexar a política AmazonWorkSpacesSecureBrowserReadOnly às identidades do IAM.

Essa política concede permissões somente para leitura que permitem acesso ao WorkSpaces Secure Browser e suas dependências por meio do AWS Management Console, SDK e CLI. Essa política não inclui as permissões necessárias para interagir com portais usando o IAM_Identity_Center como tipo de autenticação. Para obter essas permissões, combine essa política com AWSSSOReadOnly.

Detalhes das permissões

Esta política inclui as seguintes permissões.

- **workspaces-web**— Fornece acesso somente de leitura ao WorkSpaces Secure Browser e suas dependências por meio do console AWS de gerenciamento, SDK e CLI.
- **ec2**— Permite que os diretores descrevam VPCs, sub-redes e grupos de segurança. Isso é usado no console AWS de gerenciamento do WorkSpaces Secure Browser para mostrar suas VPCs sub-redes e grupos de segurança que estão disponíveis para uso com o serviço.
- **Kinesis**: permite que as entidades principais listem fluxos de dados do Kinesis. Isso é usado no console AWS de gerenciamento do WorkSpaces Secure Browser para mostrar os streams de dados do Kinesis que estão disponíveis para uso com o serviço.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces-web:GetBrowserSettings",
        "workspaces-web:GetIdentityProvider",
        "workspaces-web:GetNetworkSettings",
        "workspaces-web:GetPortal",
        "workspaces-web:GetPortalServiceProviderMetadata",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetTrustStoreCertificate",
        "workspaces-web:GetUserSettings",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:ListBrowserSettings",
        "workspaces-web:ListIdentityProviders",
        "workspaces-web:ListNetworkSettings",
        "workspaces-web:ListPortals",
        "workspaces-web:ListTagsForResource",
        "workspaces-web:ListTrustStoreCertificates",
        "workspaces-web:ListTrustStores",
        "workspaces-web:ListUserSettings",
        "workspaces-web:ListUserAccessLoggingSettings"
      ],
      "Resource": "arn:aws:workspaces-web:*:*:*"
    },
    {
      "Effect": "Allow",
      "Action": [
```

```
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "kinesis:ListStreams"
    ],
    "Resource": "*"
}
]
```

AWS política gerenciada: AmazonWorkSpacesWebReadOnly

É possível anexar a política `AmazonWorkSpacesWebReadOnly` às identidades do IAM.

Essa política concede permissões somente para leitura que permitem acesso ao WorkSpaces Secure Browser e suas dependências por meio do AWS Management Console, SDK e CLI. Essa política não inclui as permissões necessárias para interagir com portais usando o `IAM_Identity_Center` como tipo de autenticação. Para obter essas permissões, combine essa política com `AWSSSOReadOnly`.

Note

Se você estiver usando essa política no momento, mude para a nova política de `AmazonWorkSpacesSecureBrowserReadOnly`.

Detalhes das permissões

Esta política inclui as seguintes permissões.

- `workspaces-web`— Fornece acesso somente de leitura ao WorkSpaces Secure Browser e suas dependências por meio do console AWS de gerenciamento, SDK e CLI.
- `ec2`— Permite que os diretores descrevam VPCs, sub-redes e grupos de segurança. Isso é usado no console AWS de gerenciamento do WorkSpaces Secure Browser para mostrar suas VPCs sub-redes e grupos de segurança que estão disponíveis para uso com o serviço.

- **Kinesis:** permite que as entidades principais listem fluxos de dados do Kinesis. Isso é usado no console AWS de gerenciamento do WorkSpaces Secure Browser para mostrar os streams de dados do Kinesis que estão disponíveis para uso com o serviço.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces-web:GetBrowserSettings",
        "workspaces-web:GetIdentityProvider",
        "workspaces-web:GetNetworkSettings",
        "workspaces-web:GetPortal",
        "workspaces-web:GetPortalServiceProviderMetadata",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetTrustStoreCertificate",
        "workspaces-web:GetUserSettings",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:ListBrowserSettings",
        "workspaces-web:ListIdentityProviders",
        "workspaces-web:ListNetworkSettings",
        "workspaces-web:ListPortals",
        "workspaces-web:ListTagsForResource",
        "workspaces-web:ListTrustStoreCertificates",
        "workspaces-web:ListTrustStores",
        "workspaces-web:ListUserSettings",
        "workspaces-web:ListUserAccessLoggingSettings"
      ],
      "Resource": "arn:aws:workspaces-web:*:*:*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "kinesis:ListStreams"
      ],
      "Resource": "*"
    }
  ]
}
```

}

WorkSpaces Atualizações do Secure Browser para políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas do WorkSpaces Secure Browser desde que esse serviço começou a rastrear essas alterações. Para obter alertas automáticos sobre alterações feitas nesta página, inscreva-se no feed RSS na página [Histórico de documentos](#).

Alteração	Descrição	Data
AmazonWorkSpacesSecureBrowserReadOnly – Nova política	WorkSpaces O Secure Browser adicionou uma nova política para fornecer acesso somente de leitura ao WorkSpaces Secure Browser e suas dependências por meio do AWS Management Console, SDK e CLI.	24 de junho de 2024
AmazonWorkSpacesWebServiceRolePolicy : política atualizada	WorkSpaces O Secure Browser atualizou a política CreateNetworkInterface para restringir a marcação com awsRequestTag/WorkSpacesWebManaged: true and act on subnet and security group resources, as well as restrict DeleteNetworkInterface to ENIs tagged with aws:ResourceTag/WorkSpacesWebManaged:: true.	15 de dezembro de 2022
AmazonWorkSpacesWebReadOnly : política atualizada	WorkSpaces O Secure Browser atualizou a política para incluir permissões de	2 de novembro de 2022

Alteração	Descrição	Data
	<p>leitura para o registro de acesso do usuário e para listar streams de dados do Kinesis. Para obter mais informações, consulte the section called “Configurar o registro de acesso do usuário”.</p>	
<p>AmazonWorkSpacesWebServiceRolePolicy: política atualizada</p>	<p>WorkSpaces O Secure Browser atualizou a política para descrever um resumo dos fluxos de dados do Kinesis e colocar registros nos fluxos de dados do Kinesis para registro de acesso do usuário. Para obter mais informações, consulte the section called “Configurar o registro de acesso do usuário”.</p>	<p>17 de outubro de 2022</p>
<p>AmazonWorkSpacesWebServiceRolePolicy: política atualizada</p>	<p>WorkSpaces O Secure Browser atualizou a política para criar tags durante a criação do ENI.</p>	<p>6 de setembro de 2022</p>
<p>AmazonWorkSpacesWebServiceRolePolicy: política atualizada</p>	<p>WorkSpaces O Secure Browser atualizou a política para adicionar o namespace AWS/Usage às permissões da API. PutMetricData</p>	<p>6 de abril de 2022</p>

Alteração	Descrição	Data
AmazonWorkSpacesWebReadOnly – Nova política	WorkSpaces O Secure Browser adicionou uma nova política para fornecer acesso somente de leitura ao WorkSpaces Secure Browser e suas dependências por meio do AWS Management Console, SDK e CLI.	30 de novembro de 2021
AmazonWorkSpacesWebServiceRolePolicy – Nova política	WorkSpaces O Secure Browser adicionou uma nova política para permitir o acesso aos serviços e recursos da AWS usados ou gerenciados pelo WorkSpaces Secure Browser.	30 de novembro de 2021
WorkSpaces O Secure Browser começou a rastrear as alterações	WorkSpaces O Secure Browser começou a rastrear as alterações em suas políticas AWS gerenciadas.	30 de novembro de 2021

Solução de problemas de identidade e acesso ao Amazon WorkSpaces Secure Browser

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com o WorkSpaces Secure Browser e o IAM.

Tópicos

- [Não estou autorizado a realizar uma ação no WorkSpaces Secure Browser](#)
- [Não estou autorizado a realizar iam: PassRole](#)
- [Quero permitir que pessoas fora da minha AWS conta acessem os recursos do meu Navegador WorkSpaces Seguro](#)

Não estou autorizado a realizar uma ação no WorkSpaces Secure Browser

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, suas políticas deverão ser atualizadas para permitir que você realize a ação.

O erro do exemplo a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para visualizar detalhes sobre um atributo `my-example-widget` fictício, mas não tem as permissões `workspaces-web:GetWidget` fictícias.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
workspaces-web:GetWidget on resource: my-example-widget
```

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao recurso `my-example-widget` usando a ação `workspaces-web:GetWidget`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Não estou autorizado a realizar iam: PassRole

Se você receber um erro informando que não está autorizado a realizar a `iam:PassRole` ação, suas políticas devem ser atualizadas para permitir que você passe uma função para o Navegador WorkSpaces Seguro.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O exemplo de erro a seguir ocorre quando um usuário do IAM chamado `marymajor` tenta usar o console para realizar uma ação no WorkSpaces Secure Browser. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero permitir que pessoas fora da minha AWS conta acessem os recursos do meu Navegador WorkSpaces Seguro

É possível criar um perfil que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. É possível especificar quem é confiável para assumir o perfil. Para serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se o WorkSpaces Secure Browser oferece suporte a esses recursos, consulte [Como o Amazon WorkSpaces Secure Browser funciona com o IAM](#).
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Como [fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui](#) no Guia do usuário do IAM.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como [fornecer acesso Contas da AWS a terceiros](#) no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte [Conceder acesso a usuários autenticados externamente \(federação de identidades\)](#) no Guia do usuário do IAM.
- Para conhecer a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte [Acesso a recursos entre contas no IAM](#) no Guia do usuário do IAM.

Usando funções vinculadas a serviços para o Amazon Secure WorkSpaces Browser

O Amazon WorkSpaces Secure Browser usa AWS Identity and Access Management funções [vinculadas ao serviço](#) (IAM). Uma função vinculada ao serviço é um tipo exclusivo de função do IAM vinculada diretamente ao WorkSpaces Secure Browser. As funções vinculadas ao serviço são predefinidas pelo WorkSpaces Secure Browser e incluem todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome.

Uma função vinculada ao serviço facilita a configuração do Navegador WorkSpaces Seguro porque você não precisa adicionar manualmente as permissões necessárias. WorkSpaces O Navegador

Seguro define as permissões de suas funções vinculadas ao serviço e, a menos que seja definido de outra forma, somente o Navegador WorkSpaces Seguro pode assumir suas funções. As permissões definidas incluem as políticas de confiança e de permissões. A política de permissões não pode ser anexada a nenhuma outra entidade do IAM.

Você só pode excluir um perfil vinculado a serviço depois de excluir os recursos relacionados. Isso protege seus recursos do Navegador WorkSpaces Seguro porque você não pode remover inadvertidamente a permissão para acessar os recursos.

Para obter informações sobre outros serviços compatíveis com perfis vinculados a serviços, consulte [Serviços da AWS compatíveis com o IAM](#) e procure os serviços que contenham Sim na coluna Service-Linked Role. Escolha um Sim com um link para visualizar a documentação do perfil vinculado para esse serviço.

Tópicos

- [Permissões de função vinculadas ao serviço para WorkSpaces o Secure Browser](#)
- [Criação de uma função vinculada ao serviço para WorkSpaces o Secure Browser](#)
- [Editando uma função vinculada ao serviço para WorkSpaces o Secure Browser](#)
- [Excluindo uma função vinculada ao serviço para o Secure Browser WorkSpaces](#)
- [Regiões suportadas para funções vinculadas ao serviço WorkSpaces Secure Browser](#)

Permissões de função vinculadas ao serviço para WorkSpaces o Secure Browser

WorkSpaces O Secure Browser usa a função vinculada ao serviço chamada `AWSServiceRoleForAmazonWorkSpacesWeb` — O WorkSpaces Secure Browser usa essa função vinculada ao serviço para acessar EC2 recursos da Amazon de contas de clientes para instâncias e métricas de streaming. CloudWatch

O perfil vinculado ao serviço `AWSServiceRoleForAmazonWorkSpacesWeb` confia nos seguintes serviços para aceitar o perfil:

- `workspaces-web.amazonaws.com`

A política de permissões de função denominada `AmazonWorkSpacesWebServiceRolePolicy` permite que o WorkSpaces Secure Browser conclua as seguintes ações nos recursos especificados. Para obter mais informações, consulte [the section called “AmazonWorkSpacesWebServiceRolePolicy”](#).

- Ação: `ec2:DescribeVpcs` em all AWS resources
- Ação: `ec2:DescribeSubnets` em all AWS resources
- Ação: `ec2:DescribeAvailabilityZones` em all AWS resources
- Ação: `ec2:CreateNetworkInterface` com `aws:RequestTag/WorkSpacesWebManaged: true` em recursos de sub-rede e grupo de segurança
- Ação: `ec2:DescribeNetworkInterfaces` em all AWS resources
- Ação: `ec2>DeleteNetworkInterface` em interfaces de rede com `aws:ResourceTag/WorkSpacesWebManaged: true`
- Ação: `ec2:DescribeSubnets` em all AWS resources
- Ação: `ec2:AssociateAddress` em all AWS resources
- Ação: `ec2:DisassociateAddress` em all AWS resources
- Ação: `ec2:DescribeRouteTables` em all AWS resources
- Ação: `ec2:DescribeSecurityGroups` em all AWS resources
- Ação: `ec2:DescribeVpcEndpoints` em all AWS resources
- Ação: `ec2:CreateTags` na operação `ec2:CreateNetworkInterface` com `aws:TagKeys: ["WorkSpacesWebManaged"]`
- Ação: `cloudwatch:PutMetricData` em all AWS resources
- Ação: `kinesis:PutRecord` em fluxos de dados do Kinesis com nomes que começam com `amazon-workspaces-web-`
- Ação: `kinesis:PutRecords` em fluxos de dados do Kinesis com nomes que começam com `amazon-workspaces-web-`
- Ação: `kinesis:DescribeStreamSummary` em fluxos de dados do Kinesis com nomes que começam com `amazon-workspaces-web-`

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua um perfil vinculado a serviço. Para mais informações, consulte [Permissões de perfil vinculado ao serviço](#) no Guia do usuário do IAM.

Criação de uma função vinculada ao serviço para WorkSpaces o Secure Browser

Não é necessário criar manualmente um perfil vinculado ao serviço. Quando você cria seu primeiro portal na AWS Management Console, na ou na AWS API AWS CLI, o WorkSpaces Secure Browser cria a função vinculada ao serviço para você.

⚠ Important

Esse perfil vinculado ao serviço pode aparecer em sua conta se você concluiu uma ação em outro serviço que usa os atributos compatíveis com esse perfil.

Se excluir esse perfil vinculado ao serviço e precisar criá-lo novamente, você poderá usar esse mesmo processo para recriar o perfil em sua conta. Quando você cria seu primeiro portal, o WorkSpaces Secure Browser cria a função vinculada ao serviço para você novamente.

Você também pode usar o console do IAM para criar uma função vinculada ao serviço com o caso de uso do WorkSpaces Secure Browser. Na AWS CLI ou na AWS API, crie uma função vinculada ao serviço com o nome do `workspaces-web.amazonaws.com` serviço. Para obter mais informações, consulte [Criar uma função vinculada ao serviço](#) no Guia do usuário do IAM. Se você excluir essa função vinculada ao serviço, será possível usar esse mesmo processo para criar a função novamente.

Editando uma função vinculada ao serviço para WorkSpaces o Secure Browser

WorkSpaces O Secure Browser não permite que você edite a função `AWSServiceRoleForAmazonWorkSpacesWeb` vinculada ao serviço. Depois que você criar um perfil vinculado ao serviço, não poderá alterar o nome do perfil, pois várias entidades podem fazer referência ao perfil. No entanto, você poderá editar a descrição do perfil usando o IAM. Para obter mais informações, consulte [Editar uma função vinculada a serviço](#) no Guia do usuário do IAM.

Excluindo uma função vinculada ao serviço para o Secure Browser WorkSpaces

Se você não precisar mais usar um atributo ou serviço que requer uma função vinculada a serviço, é recomendável excluí-la. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, você deve limpar os recursos de seu perfil vinculado ao serviço antes de excluí-lo manualmente.

ℹ Note

Se o serviço Navegador WorkSpaces Seguro estiver usando a função quando você tentar excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Para excluir os recursos do Navegador WorkSpaces Seguro usados pelo AWSService RoleForAmazonWorkSpacesWeb

- Escolha uma das seguintes opções:
 - Se você usa o console, exclua todos os seus portais no console.
 - Se você usa a CLI ou a API, desassocie todos os seus recursos (incluindo configurações do navegador, configurações de rede, configurações do usuário, armazenamentos confiáveis e configurações de registro de acesso do usuário) dos seus portais, exclua esses recursos e exclua os portais.

Como excluir manualmente o perfil vinculado ao serviço usando o IAM

Use o console do IAM AWS CLI, o ou a AWS API para excluir a função AWSService RoleForAmazonWorkSpacesWeb vinculada ao serviço. Para obter mais informações, consulte [Excluir um perfil vinculado ao serviço](#) no Guia do usuário do IAM.

Regiões suportadas para funções vinculadas ao serviço WorkSpaces Secure Browser

WorkSpaces O Secure Browser oferece suporte ao uso de funções vinculadas ao serviço em todas as regiões em que o serviço está disponível. Para obter mais informações, consulte [Regiões e endpoints da AWS](#).

Resposta a incidentes no Amazon WorkSpaces Secure Browser

Você pode detectar incidentes monitorando a CloudWatch métrica da SessionFailure Amazon. Para receber alertas de incidentes, use um CloudWatch alarme para a SessionFailure métrica. Para obter mais informações, consulte [Monitorando o Amazon WorkSpaces Secure Browser com a Amazon CloudWatch](#).

Validação de conformidade para o Amazon WorkSpaces Secure Browser

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte [Serviços da AWS Escopo por Programa de Conformidade](#) [Serviços da AWS](#) e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de [AWS conformidade Programas AWS](#) de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte [Baixar relatórios em AWS Artifact](#).

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- [Governança e conformidade de segurança](#): esses guias de implementação de solução abordam considerações sobre a arquitetura e fornecem etapas para implantar recursos de segurança e conformidade.
- [Referência de serviços qualificados para HIPAA](#): lista os serviços qualificados para HIPAA. Nem todos Serviços da AWS são elegíveis para a HIPAA.
- AWS Recursos de <https://aws.amazon.com/compliance/resources/> de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- [AWS Guias de conformidade do cliente](#) — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- [Avaliação de recursos com regras](#) no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- [AWS Security Hub](#) — Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os recursos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a [Referência de controles do Security Hub](#).
- [Amazon GuardDuty](#) — Isso AWS service (Serviço da AWS) detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de conformidade, como o PCI DSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.
- [AWS Audit Manager](#) — Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

Resiliência no Amazon WorkSpaces Secure Browser

A infraestrutura AWS global é construída em torno Regiões da AWS de zonas de disponibilidade. Regiões da AWS fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Para obter mais informações sobre zonas de disponibilidade Regiões da AWS e zonas de disponibilidade, consulte [Infraestrutura AWS global](#).

No momento, o WorkSpaces Secure Browser não oferece suporte aos itens a seguir:

- Fazendo backup de conteúdo em AZs nossas regiões
- Backups criptografados
- Criptografando conteúdo em trânsito entre AZs ou regiões
- Backups padrão ou automáticos

Para configurar a alta disponibilidade da internet, é possível ajustar a configuração da VPC. Para alta disponibilidade da API, você pode solicitar a quantidade certa de TPS.

Segurança da infraestrutura no Amazon WorkSpaces Secure Browser

Como um serviço gerenciado, o Amazon WorkSpaces Secure Browser é protegido pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte [AWS Cloud Security](#). Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte [Proteção](#) de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar o Amazon WorkSpaces Secure Browser pela rede. Os clientes devem oferecer compatibilidade com:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.

- Conjuntos de criptografia com perfect forward secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou é possível usar o [AWS Security Token Service](#) (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

WorkSpaces O Secure Browser isola o tráfego do serviço aplicando a autenticação e autorização AWS SigV4 padrão a todos os serviços. O endpoint de recursos do cliente (ou endpoint do portal da web) é protegido pelo seu provedor de identidades. Você pode isolar ainda mais o tráfego usando a autorização multifator e outros mecanismos de segurança em seu provedor de identidades (IdP).

Todo o acesso à internet pode ser controlado definindo configurações de rede, como VPC, sub-rede ou grupo de segurança. Atualmente, não há suporte para endpoints de multilocação e VPC (PrivateLink).

Análise de configuração e vulnerabilidade no Amazon WorkSpaces Secure Browser

WorkSpaces O Secure Browser atualiza e corrige aplicativos e plataformas conforme necessário em seu nome, incluindo Chrome e Linux. Você não precisa corrigir nem recriar. No entanto, é sua responsabilidade configurar o Navegador WorkSpaces Seguro de acordo com as especificações e diretrizes e monitorar o uso do Navegador WorkSpaces Seguro por seus usuários. Todas as configurações relacionadas ao serviço e a análise de vulnerabilidades são de responsabilidade do WorkSpaces Secure Browser.

Você pode solicitar um aumento de limite para os recursos do WorkSpaces Secure Browser, como o número de portais da web e o número de usuários. WorkSpaces O Secure Browser garante a disponibilidade do serviço e do SLA.

Acesse APIs usando uma interface VPC endpoint ()AWS PrivateLink

Você pode ligar diretamente para o endpoint da API do Amazon WorkSpaces Secure Browser de dentro de uma nuvem privada (VPC), em vez de se conectar pela Internet. Você pode fazer isso sem o uso de um gateway de internet, dispositivo NAT, conexão VPN ou AWS Direct Connect conexão.

Você estabelece essa conexão privada criando uma interface VPC endpoint que é alimentada por [AWS PrivateLink](#). Para cada sub-rede que você especifica em sua VPC, criamos uma interface de rede de endpoint na sub-rede. Uma interface de rede de endpoint é uma interface de rede gerenciada pelo solicitante que serve como ponto de entrada para o tráfego da API do Amazon WorkSpaces Secure Browser.

Para obter mais informações, consulte [Acessar AWS serviços por meio de AWS PrivateLink](#).

Tópicos

- [Considerações sobre o Amazon WorkSpaces Secure Browser](#)
- [Criação de uma interface VPC endpoint para o Amazon Secure Browser WorkSpaces](#)
- [Criação de uma política de endpoint para sua interface VPC endpoint](#)
- [Solução de problemas](#)

Considerações sobre o Amazon WorkSpaces Secure Browser

[Antes de configurar uma interface VPC endpoint para o Amazon WorkSpaces Secure Browser APIs, certifique-se de revisar os “Pré-requisitos” nos serviços de acesso por meio de. AWSAWS PrivateLink](#) O Amazon WorkSpaces Secure Browser oferece suporte para fazer chamadas para todas as suas ações de API por meio da interface VPC endpoint.

Por padrão, o acesso total ao Amazon WorkSpaces Secure Browser é permitido por meio do endpoint. Para obter mais informações, consulte [Controlar o acesso a serviços com endpoints da VPC](#) no Guia do Usuário do Amazon VPC.

Criação de uma interface VPC endpoint para o Amazon Secure Browser WorkSpaces

Você pode criar uma interface VPC endpoint para o serviço Amazon WorkSpaces Secure Browser usando o console Amazon VPC ou o `awscli`. Para obter mais informações, consulte [Criar um endpoint de interface](#) no Guia do usuário da Amazon VPC.

Crie uma interface VPC endpoint para o Amazon WorkSpaces Secure Browser usando o seguinte nome de serviço:

- `com.amazonaws.region.espacos de trabalho na web`

Para regiões compatíveis com FIPS, crie uma interface VPC endpoint para o WorkSpaces Amazon Secure Browser usando o seguinte nome de serviço:

- `com.amazonaws.region.workspaces-web-fips`

Criação de uma política de endpoint para sua interface VPC endpoint

Uma política de endpoint é um recurso do IAM que você pode anexar a uma interface VPC endpoint. A política de endpoint padrão oferece acesso total ao Amazon WorkSpaces Secure Browser APIs por meio da interface VPC endpoint. Para controlar o acesso concedido ao Amazon WorkSpaces Secure Browser a partir de sua VPC, anexe uma política de endpoint personalizada à interface VPC endpoint.

Uma política de endpoint especifica as seguintes informações:

- As entidades principais que podem realizar ações (Contas da AWS, usuários do IAM e perfis do IAM).
- As ações que podem ser realizadas.
- Os recursos aos quais as ações podem ser aplicadas.

Para obter mais informações, consulte [Controlar o acesso a serviços com endpoints da VPC](#) no Guia do Usuário do Amazon VPC.

Exemplo: política de VPC endpoint para ações do Amazon WorkSpaces Secure Browser

Veja a seguir um exemplo de uma política de endpoint personalizado. Quando você anexa essa política à sua interface VPC endpoint, ela concede acesso às ações listadas do Amazon WorkSpaces Secure Browser para todos os diretores em todos os recursos.

```
{
  "Statement": [
    {
      "Action": "workspaces-web:*",
      "Effect": "Allow",
      "Resource": "*",
      "Principal": "*"
    }
  ]
}
```

Solução de problemas

Se suas chamadas para o Amazon WorkSpaces Secure Browser APIs estiverem suspensas, é provável que haja uma configuração incorreta no grupo de segurança do VPC Endpoint Service ou na configuração da função do IAM. Para resolver isso, tente o seguinte:

- Ao criar sua interface VPC endpoint, ela pode ter sido automaticamente anexada ao seu grupo Conta da AWS de segurança padrão. Tente usar um grupo de segurança diferente e certifique-se de que as permissões de entrada e saída permitam que você transfira seus dados adequadamente.
- Verifique se você está usando uma função do IAM que permite chamar o Amazon WorkSpaces Secure Browser APIs.

Para obter mais informações, consulte [O que é AWS PrivateLink?](#) no Guia do usuário da Amazon VPC.

Melhores práticas de segurança para o Amazon WorkSpaces Secure Browser

O Amazon WorkSpaces Secure Browser fornece vários recursos de segurança que você pode usar ao desenvolver e implementar suas próprias políticas de segurança. As práticas recomendadas a seguir são diretrizes gerais e não representam uma solução completa de segurança. Como essas

práticas recomendadas podem não ser adequadas ou suficientes para o seu ambiente, trate-as como considerações úteis em vez de prescrições.

As melhores práticas para o Amazon WorkSpaces Secure Browser incluem o seguinte:

- Para detectar possíveis eventos de segurança associados ao uso do WorkSpaces Secure Browser, use AWS CloudTrail CloudWatch a Amazon para detectar e rastrear o histórico de acesso e os registros de processos. Para ter mais informações, consulte [Monitorando o Amazon WorkSpaces Secure Browser com a Amazon CloudWatch](#) e [Registrando chamadas da API do WorkSpaces Secure Browser usando AWS CloudTrail](#).
- Para implementar controles de detetive e identificar anomalias, use CloudTrail registros e métricas. CloudWatch Para ter mais informações, consulte [Monitorando o Amazon WorkSpaces Secure Browser com a Amazon CloudWatch](#) e [Registrando chamadas da API do WorkSpaces Secure Browser usando AWS CloudTrail](#).
- É possível configurar o registro em log de acesso do usuário para registrar os eventos do usuário. Para obter mais informações, consulte [the section called “Configurar o registro de acesso do usuário”](#).

Para evitar possíveis eventos de segurança associados ao uso do WorkSpaces Secure Browser, siga estas melhores práticas:

- Implemente o acesso com privilégios mínimos e crie funções específicas para serem usadas nas ações do Navegador WorkSpaces Seguro. Use modelos do IAM para criar um perfil de acesso total ou somente leitura. Para obter mais informações, consulte [AWS políticas gerenciadas para o WorkSpaces Secure Browser](#).
- Tenha cuidado ao compartilhar domínios do portal e credenciais do usuário. Qualquer pessoa na internet pode acessar o portal da web, mas não pode iniciar uma sessão a menos que tenha uma credencial de usuário válida para o portal. Tenha cuidado sobre como, quando e com quem você compartilha as credenciais do portal da web.

Monitorando o Amazon WorkSpaces Secure Browser

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho do Amazon WorkSpaces Secure Browser e de suas outras AWS soluções. AWS fornece as seguintes ferramentas de monitoramento para monitorar seus portais do WorkSpaces Secure Browser e seus recursos, relatar quando algo está errado e realizar ações automáticas quando apropriado:

- A Amazon CloudWatch monitora seus AWS recursos e os aplicativos em que você executa AWS em tempo real. É possível coletar e rastrear métricas, criar painéis personalizados e definir alarmes que o notificam ou que realizam ações quando uma métrica especificada atinge um limite especificado. Por exemplo, você pode CloudWatch rastrear o uso da CPU ou outras métricas para suas EC2 instâncias da Amazon e iniciar automaticamente novas instâncias quando necessário. Para obter mais informações, consulte o [Guia CloudWatch do usuário da Amazon](#).
- O Amazon CloudWatch Logs permite monitorar, armazenar e acessar seus arquivos de log a partir de EC2 instâncias da Amazon e de outras fontes. CloudTrail CloudWatch Os registros podem monitorar as informações nos arquivos de log e notificá-lo quando determinados limites forem atingidos. É possível também arquivar seus dados de log em armazenamento resiliente. Para obter mais informações, consulte o [Guia do usuário do Amazon CloudWatch Logs](#).
- AWS CloudTrail captura chamadas de API e eventos relacionados feitos por ou em nome de sua AWS conta e entrega os arquivos de log para um bucket do Amazon S3 que você especificar. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem a partir do qual as chamadas foram feitas e quando elas ocorreram. Para obter mais informações, consulte o [Guia do usuário do AWS CloudTrail](#).

Tópicos

- [Monitorando o Amazon WorkSpaces Secure Browser com a Amazon CloudWatch](#)
- [Registrando chamadas da API do WorkSpaces Secure Browser usando AWS CloudTrail](#)
- [Login de acesso do usuário no Amazon WorkSpaces Secure Browser](#)

Monitorando o Amazon WorkSpaces Secure Browser com a Amazon CloudWatch

Você pode monitorar o Amazon WorkSpaces Secure Browser usando CloudWatch, que coleta dados brutos e os processa em métricas legíveis, quase em tempo real. Essas estatísticas são mantidas por 15 meses, de maneira que você possa acessar informações históricas e ter uma perspectiva melhor de como o aplicativo web ou o serviço está se saindo. Você também pode definir alarmes que observam determinados limites e enviam notificações ou realizam ações quando esses limites são atingidos. Para obter mais informações, consulte o [Guia CloudWatch do usuário da Amazon](#).

O namespace `AWS/WorkSpacesWeb` inclui as métricas a seguir.

CloudWatch métricas para o Amazon WorkSpaces Secure Browser

Métrica	Descrição	Dimensões	Statistics	Unidades
<code>SessionAttempt</code>	O número de tentativas de sessões do Amazon WorkSpaces Secure Browser.	<code>PortalId</code>	Média, Soma, Máximo, Mínimo	Contagem
<code>SessionSuccess</code>	O número de sessões bem-sucedidas do Amazon WorkSpaces Secure Browser começa.	<code>PortalId</code>	Média, Soma, Máximo, Mínimo	Contagem
<code>SessionFailure</code>	O número de sessões com falha do Amazon WorkSpaces Secure Browser começa.	<code>PortalId</code>	Média, Soma, Máximo, Mínimo	Contagem

Métrica	Descrição	Dimensões	Statistics	Unidades
GlobalCpuPercent	O uso da CPU da instância de sessão do Amazon WorkSpaces Secure Browser.	PortalId	Média, Soma, Máximo, Mínimo	Percentual
GlobalMemoryPercent	O uso da memória (RAM) da instância de sessão do Amazon WorkSpaces Secure Browser.	PortalId	Média, Soma, Máximo, Mínimo	Percentual

Note

Você pode visualizar a estatística métrica “SampleCount” GlobalMemoryPercent para GlobalCpuPercent ou determinar o número de sessões simultâneas ativas no seu portal. Os pontos de dados são emitidos por cada sessão uma vez por minuto.

Registrando chamadas da API do WorkSpaces Secure Browser usando AWS CloudTrail

WorkSpaces O Secure Browser é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço no Amazon WorkSpaces Secure Browser. CloudTrail captura todas as chamadas de API para o Amazon WorkSpaces Secure Browser como eventos. Isso inclui chamadas do console do Amazon WorkSpaces Secure Browser e chamadas de código para operações da API do Amazon WorkSpaces Secure Browser. Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para o Amazon WorkSpaces Secure Browser. Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, você pode identificar a solicitação que foi feita ao

Amazon WorkSpaces Secure Browser, o endereço IP a partir do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita, bem como detalhes adicionais.

Para saber mais sobre isso CloudTrail, consulte o [Guia AWS CloudTrail do usuário](#).

Tópicos

- [WorkSpaces Informações do Navegador Seguro em CloudTrail](#)
- [Entendendo as entradas do arquivo de log do WorkSpaces Secure Bro](#)

WorkSpaces Informações do Navegador Seguro em CloudTrail

CloudTrail é ativado em sua AWS conta quando você cria a conta. Quando a atividade ocorre no Amazon WorkSpaces Secure Browser, essa atividade é registrada em um CloudTrail evento junto com outros eventos AWS de serviço no histórico de eventos. No Histórico de eventos, você pode visualizar, pesquisar e baixar eventos recentes em sua AWS conta. Para obter mais informações, consulte [Visualização de eventos com histórico de CloudTrail eventos](#).

Para um registro contínuo de eventos em sua AWS conta, incluindo eventos para o Amazon WorkSpaces Secure Browser, você pode criar uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando uma trilha é criada no console, a mesma é aplicada a todas as regiões da AWS. A trilha registra eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para obter mais informações, consulte:

- [Visão geral da criação de uma trilha](#)
- [CloudTrail serviços e integrações suportados](#)
- [Configurando notificações do Amazon SNS para CloudTrail](#)
- [Recebendo arquivos de CloudTrail log de várias regiões](#) e [Recebendo arquivos de CloudTrail log de várias contas](#)

Todas as ações do Amazon WorkSpaces Secure Browser são registradas CloudTrail e documentadas na Amazon WorkSpaces API Reference. Por exemplo, chamadas para o `CreatePortalDeleteUserSettings` e `ListBrowserSettings` as ações geram entradas nos arquivos de CloudTrail log.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário-raiz ou usuário do IAM.
- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado.
- Se a solicitação foi feita por outro AWS serviço.

Para obter mais informações, consulte [Elemento userIdentity do CloudTrail](#).

Entendendo as entradas do arquivo de log do WorkSpaces Secure Bro

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contém uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros da solicitação e outros detalhes. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica.

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a `ListBrowserSettings` ação.

```
{
  "Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
      "type": "IAMUser",
      "principalId": "111122223333",
      "arn": "arn:aws:iam::111122223333:user/myUserName",
      "accountId": "111122223333",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "userName": "myUserName"
    },
    "eventTime": "2021-11-17T23:44:51Z",
    "eventSource": "workspaces-web.amazonaws.com",
    "eventName": "ListBrowserSettings",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "127.0.0.1",
    "userAgent": "[]"
  ]
}
```

```
    "requestParameters": null,
    "responseElements": null,
    "requestID": "159d5c4f-c8c8-41f1-9aee-b5b1b632e8b2",
    "eventID": "d8237248-0090-4c1e-b8f0-a6e8b18d63cb",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
  },
  {
    "eventVersion": "1.08",
    "userIdentity": {
      "type": "IAMUser",
      "principalId": "111122223333",
      "arn": "arn:aws:iam::111122223333:user/myUserName",
      "accountId": "111122223333",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "userName": "myUserName"
    },
    "eventTime": "2021-11-17T23:55:51Z",
    "eventSource": "workspaces-web.amazonaws.com",
    "eventName": "CreateUserSettings",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "5127.0.0.1",
    "userAgent": "[]",
    "requestParameters": {
      "clientToken": "some-token",
      "copyAllowed": "Enabled",
      "downloadAllowed": "Enabled",
      "pasteAllowed": "Enabled",
      "printAllowed": "Enabled",
      "uploadAllowed": "Enabled"
    },
    "responseElements": "arn:aws:workspaces-web:us-
west-2:111122223333:userSettings/04a35a2d-f7f9-4b22-af08-8ec72da9c2e2",
    "requestID": "6a4aa162-7c1b-4cf9-a7ac-e0c8c4622117",
    "eventID": "56f1fbee-6a1d-4fc6-bf35-a3a71f016fcb",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
  }
}]
```

```
}
```

Login de acesso do usuário no Amazon WorkSpaces Secure Browser

O Amazon WorkSpaces Secure Browser permite que os clientes registrem eventos da sessão, incluindo início, parada e visitas de URL. Esses logs são entregues a um Amazon Kinesis Data Stream que você especifica para o seu portal da web. Para obter mais informações, consulte [the section called “Configurar o registro de acesso do usuário”](#).

Orientação para usuários do Amazon WorkSpaces Secure Browser

Os administradores usam o WorkSpaces Secure Browser para criar portais da Web que se conectam aos sites da empresa, como sites internos, aplicativos da Web software-as-a-service (SAAS) ou à Internet. Os usuários finais usam os navegadores da web existentes para acessar esses portais da web a fim de iniciar uma sessão e acessar o conteúdo.

O conteúdo a seguir ajuda a orientar os usuários finais que desejam saber mais sobre como acessar o WorkSpaces Secure Browser, iniciar e configurar uma sessão e usar a barra de ferramentas e o navegador da web.

Tópicos

- [Compatibilidade de navegadores e dispositivos com o Amazon WorkSpaces Secure Browser](#)
- [Acesso ao portal da web para o Amazon WorkSpaces Secure Browser](#)
- [Orientação de sessão para o Amazon WorkSpaces Secure Browser](#)
- [Solução de problemas de usuários no Amazon WorkSpaces Secure Browser](#)
- [Extensão de login único para o Amazon WorkSpaces Secure Browser](#)

Compatibilidade de navegadores e dispositivos com o Amazon WorkSpaces Secure Browser

O Amazon WorkSpaces Secure Browser é desenvolvido pelo cliente de navegador Amazon DCV, que é executado dentro de um navegador da web, portanto, nenhuma instalação é necessária. O cliente do navegador da web é compatível com navegadores comuns, como Chrome e Firefox, e com os principais sistemas operacionais de desktop, como Windows, macOS e Linux.

Para up-to-date obter mais detalhes sobre o suporte ao cliente do navegador da Web, consulte [Cliente do navegador da Web](#).

Note

Atualmente, o suporte para webcam está disponível apenas em navegadores baseados em Chromium, como Google Chrome e Microsoft Edge. Atualmente, o Apple Safari e o Mozilla FireFox não suportam webcam.

Acesso ao portal da web para o Amazon WorkSpaces Secure Browser

Seu administrador pode fornecer acesso ao portal da web com as seguintes opções:

- Você pode selecionar um link de um e-mail ou site e entrar com suas credenciais de identidade SAML.
- É possível entrar no seu provedor de identidade SAML (como Okta, Ping ou Azure) e iniciar uma sessão com um clique na página inicial da aplicação do provedor de SAML (como o Painel do Usuário Final do Okta ou o portal Myapps do Azure).

Orientação de sessão para o Amazon WorkSpaces Secure Browser

Depois de entrar no portal da web, você pode iniciar uma sessão e realizar várias ações durante sua sessão.

Tópicos

- [Iniciando uma sessão no Amazon WorkSpaces Secure Browser](#)
- [Usando a barra de ferramentas no Amazon WorkSpaces Secure Browser](#)
- [Usando o navegador no Amazon WorkSpaces Secure Browser](#)
- [Encerramento de uma sessão no Amazon WorkSpaces Secure Browser](#)

Iniciando uma sessão no Amazon WorkSpaces Secure Browser

Depois de entrar para iniciar uma sessão, você verá a mensagem de Inicialização da sessão e a barra de progresso. Isso indica que o Amazon WorkSpaces Secure Browser está criando uma

sessão para você. Nos bastidores, o Amazon WorkSpaces Secure Browser está criando a instância, iniciando o navegador gerenciado e aplicando as configurações do administrador e as políticas do navegador.

Se essa é a primeira vez que você faz login no portal da web, você verá ícones azuis + na barra de ferramentas. Esse ícone indica que um tutorial está disponível, que orientará os recursos disponíveis na barra de ferramentas. Você pode usar esses ícones para aprender a:

- Conceder permissões do navegador para o microfone, a webcam e a área de transferência selecionando o ícone de cadeado ao lado do navegador local e configurando o botão para Ativado ao lado da área de transferência, do microfone e da câmera.

Note

Quando você habilita as permissões da webcam no início da primeira sessão, a webcam é ativada brevemente e uma luz no computador pisca. Isso concede acesso do navegador local à sua webcam.

- Ative o Amazon WorkSpaces Secure Browser para abrir janelas de monitor adicionais, selecionando o ícone de cadeado no seu navegador e a configuração Sempre permitir pop-ups.

Se quiser reiniciar um tutorial, você pode escolher Perfil na barra de ferramentas, Ajuda e Iniciar tutorial.

Usando a barra de ferramentas no Amazon WorkSpaces Secure Browser

Para aprender a usar a barra de ferramentas, siga estas etapas:

Para mover a barra de ferramentas, selecione a barra mais clara na parte superior da barra de ferramentas, arraste-a até o local desejado e solte-a.

Para contrair a barra de ferramentas, passe o mouse sobre ela e selecione o botão de seta para cima ou clique duas vezes na barra mais clara na seção superior. A visualização reduzida fornece mais espaço na tela e acesso com um clique aos ícones mais usados.

Para aumentar o tamanho da tela, selecione a janela do navegador e aumente o zoom. Para aumentar o tamanho de exibição dos ícones e do texto da barra de ferramentas, selecione a barra de ferramentas e aumente o zoom.

Para ampliar ou reduzir o zoom em um dispositivo Windows, siga estas etapas:

1. Selecione a barra de ferramentas ou o conteúdo da web.
2. Pressione Ctrl + para ampliar ou pressione Ctrl + - para diminuir o zoom.

Para ampliar ou reduzir o zoom em um dispositivo Mac, siga estas etapas:

1. Selecione a barra de ferramentas ou o conteúdo da web.
2. Pressione Cmd + + para ampliar ou pressione Cmd + - para diminuir o zoom.

Para encaixar a barra de ferramentas na parte superior da tela, escolha Preferências, Geral e Encaixado no modo Barra de ferramentas.

A tabela a seguir inclui uma descrição de todos os ícones disponíveis na barra de ferramentas:

Icon	Title	Description
	Windows	Move between windows or launch additional browser windows.
	Launch additional monitor window	Launch an additional monitor window with a separate browser window. Then drag to your secondary monitor.
	Full screen	Launch a full screen experience view.
 	Microphone	Activate mic input for the session. Use the down arrow to select from a list of available microphones.
 	Webcam	Activate webcam for the session. Use the down arrow to select from a list of available webcams.
	Preferences	Access the General and Keyboard menus. From the General menu, toggle between light and dark mode, activate the keyboard input selector (for changing the keyboard language), and switch between streaming mode or display resolution. From the Keyboard menu, change the option and command key settings (on Mac devices), or activate Functions (see below).
	Profile	End your session, view performance metrics, access Feedback and Help , and learn about Amazon WorkSpaces Web. End Session ends the Amazon WorkSpaces Web session. Performance metrics displays the frame rate, network latency, and bandwidth usage graph. This information is useful for administrators when investigating issues with the service. Feedback provides you with an email address to share feedback to the Amazon WorkSpaces Web team. Help provides you with access to Frequently Asked Questions, such as how to use the clipboard, microphone, and webcam during the session, or how to troubleshoot launching an additional monitor window. From help, you can also launch the tutorial or user guide. About provides more information about Amazon WorkSpaces Web.
	Notifications	Get one-click access to session notifications.
	Clipboard	Access clipboard shortcut descriptions, links to set the command key preference, and troubleshoot clipboard permissions from the local web browser. You can use the content preview text box to test clipboard functionality. This icon only displays if clipboard permission is granted by your administrator.
	Files	From the files menu, you can upload content to the remote browser. Once uploaded, you can rename, download, or delete, as well as create folders in the temporary file menu. All files and data in Files are deleted at the end of the session. This icon only displays if Files permission is granted by your administrator.

Note

Os ícones da Área de transferência e Arquivos ficam ocultos por padrão, a menos que o administrador conceda essas permissões. Somente administradores podem habilitar ou desabilitar a área de transferência e os arquivos em um portal da web. Se esses ícones estiverem ocultos e você precisar acessá-los, entre em contato com o administrador.

Usando o navegador no Amazon WorkSpaces Secure Browser

Quando você inicia sua sessão, o navegador exibe o URL de inicialização, que é um URL escolhido pelo administrador. Se o administrador não tiver escolhido um URL de inicialização, você verá a experiência padrão da nova guia do Google Chrome.

No navegador, é possível abrir guias, abrir janelas adicionais do navegador (no ícone da barra de ferramentas do Windows ou no menu de três pontos do navegador), inserir um URL ou pesquisar na barra de URL ou acessar sites a partir dos favoritos gerenciados. Para acessar os favoritos do portal da web, abra a pasta Marcadores gerenciados na barra de favoritos (abaixo da barra de URL) ou abra o gerenciador de favoritos no menu de três pontos no lado direito da barra de URL.

Para redimensionar ou mover a janela do navegador, arraste para baixo a barra de guias do Chrome. Essa ação libera mais espaço na tela para várias janelas do navegador durante a sessão.

Note

Os recursos do navegador, como o modo de navegação anônima, podem não estar disponíveis durante a sessão se o administrador os tiver desativado.

Encerramento de uma sessão no Amazon WorkSpaces Secure Browser

Para encerrar uma sessão, escolha Perfil e Encerrar sessão. Após o término de uma sessão, o Amazon WorkSpaces Secure Browser exclui todos os dados da sessão. Nenhum dado do navegador, como sites abertos ou histórico, ou arquivos ou dados do Explorador de Arquivos, fica disponível após o término da sessão.

Se você fechar uma guia durante uma sessão ativa, a sessão será encerrada após um período definido pelo administrador. Se você fechar a guia e revisitar o portal da web antes que esse tempo

limite entre em vigor, poderá ingressar na sessão atual e ver todos os dados da sessão anterior, como sites e arquivos abertos.

Solução de problemas de usuários no Amazon WorkSpaces Secure Browser

Se você encontrar algum dos problemas a seguir ao usar o WorkSpaces Secure Browser, tente as seguintes resoluções.

Meu portal do Amazon WorkSpaces Secure Browser não permite que eu faça login. Recebi uma mensagem de erro que diz “Seu portal da web ainda não está configurado. Entre em contato com o administrador para obter ajuda.”

Seu administrador precisa concluir a criação do portal com um provedor de identidade SAML 2.0 para permitir que você faça login. Entre em contato com o administrador para obter ajuda.

Meu portal não inicia uma sessão. Recebi uma mensagem de erro que diz “Falha ao reservar a sessão. Ocorreu um erro interno. Tente novamente.”

Ocorreu um problema com a inicialização da sessão do portal da web. Tente inicializar a sessão novamente. Se isso continuar, entre em contato com seu administrador para obter ajuda.

Não consigo usar a área de transferência, o microfone ou a webcam.

Para permitir permissões do navegador, selecione o ícone de cadeado ao lado do URL e alterne o botão azul ao lado de Área de transferência, Microfone, Câmera e Pop-ups e redirecionamentos para ativar esses recursos.

Note

Se o navegador não permitir entrada de vídeo ou áudio, essas opções não aparecerão na barra de ferramentas.

O áudio e vídeo (AV) em tempo real do Amazon WorkSpaces Secure Browser redireciona o vídeo da webcam local e a entrada de áudio do microfone para a sessão de streaming do navegador. Dessa forma, você pode usar seus dispositivos locais para videoconferência e audioconferência em sua sessão de streaming com navegadores da web baseados em Chromium, como o Google Chrome ou o Microsoft Edge. Atualmente, a webcam não é compatível com navegadores que não sejam Chromium.

Para obter informações sobre como configurar o Google Chrome, consulte [Usar a câmera e o microfone](#).

Meu portal da web não abre uma janela de monitor adicional.

Se você tentar iniciar dois monitores e ver um ícone de Pop-ups bloqueados no final da barra de endereço no navegador superior, selecione o ícone e o botão de opções ao lado de Sempre permitir pop-ups e redirecionamentos. Com os pop-ups permitidos, selecione o ícone de Monitor duplo na barra de ferramentas para abrir uma nova janela, reposicionar a janela no monitor e arrastar uma guia do navegador até a janela.

Quando tento baixar arquivos do painel Arquivos, nada acontece.

Se você tentar baixar arquivos do painel Arquivos e ver um ícone de Pop-ups bloqueados no final da barra de endereço no navegador superior, selecione o ícone e o botão de opção ao lado de Sempre permitir pop-ups e redirecionamentos. Com os pop-ups permitidos, tente baixar os arquivos novamente.

Como posso saber qual microfone e/ou webcam está sendo usado e como posso alterá-lo?

Clique no ícone de seta para baixo ao lado do microfone ou da câmera. O menu exibe os dispositivos disponíveis, com uma marca de seleção indicando seu dispositivo atual. Selecione um dispositivo diferente para alterar o dispositivo que você deseja usar na sua sessão.

Extensão de login único para o Amazon WorkSpaces Secure Browser

O Amazon WorkSpaces Secure Browser oferece uma extensão para login único com os navegadores Chrome e Firefox em computadores desktop. Se o administrador tiver habilitado a extensão, o portal da web solicitará que você instale a extensão ao fazer login.

O Amazon WorkSpaces Secure Browser criou a extensão para permitir o login único em sites durante sua sessão. Por exemplo, se você entrar no seu portal da web com um provedor de identidade SAML 2.0 (como Okta ou Ping) e acessar um site durante a sessão que usa o mesmo provedor de identidade, a extensão pode facilitar o acesso ao site removendo solicitações adicionais de login.

Não é necessário instalar a extensão para acessar seu portal da web, mas ela pode melhorar sua experiência ao reduzir o número de vezes que você precisa digitar o nome de usuário e senha.

Quando você faz login, a extensão localiza os cookies que seu administrador listou para sua sessão. Todos os dados que a extensão localiza são criptografados em repouso e durante o trânsito. Nenhum desses dados é armazenado no navegador local. Quando você encerra sua sessão, todos os dados da sessão (como guias abertas, arquivos baixados e cookies entregues ou criados durante a sessão) são excluídos.

Tópicos

- [Compatibilidade da extensão de login único para o Amazon WorkSpaces Secure Browser](#)
- [Instalação da extensão de login único para o Amazon WorkSpaces Secure Browser](#)
- [Solução de problemas da extensão de login único para o Amazon WorkSpaces Secure Browser](#)

Compatibilidade da extensão de login único para o Amazon WorkSpaces Secure Browser

A extensão de login único funciona com os seguintes dispositivos e navegadores:

- Dispositivos
 - Notebooks
 - Computadores desktop
- Navegadores
 - Google Chrome
 - Mozilla Firefox

Instalação da extensão de login único para o Amazon WorkSpaces Secure Browser

Para instalar a extensão de login único, siga estas etapas.

Ao fazer login no portal, siga as instruções para instalar a extensão para seu navegador Chrome ou Firefox. Você só precisa fazer isso uma vez para cada navegador da web.

Se você trocar de dispositivo, alternar para um navegador diferente no mesmo dispositivo ou excluir a extensão do navegador local, verá uma solicitação para instalar a extensão ao iniciar a próxima sessão.

Para garantir que a extensão funcione conforme o esperado, use a extensão em uma janela de navegação normal, em vez de uma de navegação anônima (Chrome) ou navegação privada (Firefox).

Solução de problemas da extensão de login único para o Amazon WorkSpaces Secure Browser

Ao usar a extensão de login único, você pode encontrar o problema a seguir.

Se você tiver a extensão instalada, mas ainda for solicitado que você faça login durante a sessão, siga estas etapas:

1. Certifique-se de ter a extensão Amazon WorkSpaces Secure Browser instalada em seu navegador. Se você excluiu os dados do navegador, talvez tenha removido a extensão acidentalmente.
2. Verifique se você não está navegando de forma anônima (Chrome) ou privada (Firefox). Esses modos podem causar problemas com extensões.
3. Se o problema persistir, entre em contato com o administrador do portal para obter ajuda adicional.

Histórico de documentos do Guia de administração do Amazon WorkSpaces Secure Browser

A tabela a seguir descreve os lançamentos da documentação do Amazon WorkSpaces Secure Browser.

Alteração	Descrição	Data
Controles da barra de ferramentas	Com os controles da barra de ferramentas, você pode configurar a apresentação da barra de ferramentas para as sessões do usuário final.	21 de fevereiro de 2025
Acesse APIs usando uma interface VPC endpoint (AWS PrivateLink)	Ligue diretamente para o endpoint da API do Amazon WorkSpaces Secure Browser de dentro de uma nuvem privada (VPC), em vez de se conectar pela Internet.	10 de janeiro de 2025
Configurações de proteção de dados	Adicione configurações de proteção de dados para ajudar a impedir que os dados sejam compartilhados durante uma sessão.	20 de novembro de 2024
Endpoints do FIPS	Proteger dados em trânsito com endpoints do FIPS.	7 de outubro de 2024
Painel de gerenciamento de sessões	Use o painel de gerenciamento de sessões para monitorar e gerenciar sessões ativas e completas.	19 de setembro de 2024
Permitir deep links	Permita que os portais recebam deep links que	25 de junho de 2024

	conectam usuários a um site específico durante uma sessão.	
Atualização da política gerenciada	Política AmazonWorkSpacesSecureBrowserReadOnly gerenciada adicionada	24 de junho de 2024
Use a barra de ferramentas para ampliar	Você pode aumentar o tamanho da tela, dos ícones e do texto com a barra de ferramentas.	1º. de maio de 2024
Novas configurações do portal web	Agora você pode especificar o tipo de instância e o limite máximo de usuários simultâneos para seu portal da web.	22 de abril de 2024
CloudWatch métricas	Adicionado GlobalCpuPercent e GlobalMemoryPercent métricas.	26 de fevereiro de 2024
Configurar filtragem de URL	Você pode usar a Política do Chrome para filtrar quais URLs usuários podem acessar a partir do navegador remoto.	21 de fevereiro de 2024
Tipos de autenticação IdP	Você pode escolher o tipo de autenticação padrão ou a do IAM Identity Center.	5 de fevereiro de 2024
Habilitar extensão de autenticação única	É possível habilitar uma extensão para que os usuários finais tenham uma melhor experiência de login no portal.	28 de agosto de 2023

Orientação do usuário para o Amazon WorkSpaces Secure Browser	Conteúdo adicionado para ajudar a orientar os usuários finais que desejam saber mais sobre como acessar o Amazon WorkSpaces Secure Browser, iniciar e configurar uma sessão e usar a barra de ferramentas e o navegador da web.	17 de julho de 2023
Controles de acesso de IP	WorkSpaces O Navegador Seguro permite que você controle de quais endereços IP seu portal da web pode ser acessado.	31 de maio de 2023
Atualização da política gerenciada	Política AmazonWorkSpacesWebReadOnly gerenciada atualizada	15 de maio de 2023
Configurar a atualização do provedor de identidades	WorkSpaces O Secure Browser oferece dois tipos de autenticação: Padrão e AWS IAM Identity Center	15 de março de 2023
Atualização da política do navegador	Seção de política do navegador atualizada e reestruturada	31 de janeiro de 2023
Atualização da política gerenciada	Política AmazonWorkSpacesWebServiceRolePolicy gerenciada atualizada	15 de dezembro de 2022

Lista de permissões e lista de bloqueio	Especifique a Lista de permissões e a Lista de bloqueios para especificar uma lista de domínios que seus usuários podem ou não acessar.	14 de novembro de 2022
Atualização da política gerenciada	Política AmazonWorkSpacesWebReadOnly gerenciada atualizada	2 de novembro de 2022
Atualização da política gerenciada	Política AmazonWorkSpacesWebServiceRolePolicy gerenciada atualizada	24 de outubro de 2022
Registro em log do acesso do usuário	Configurar o registro em log de acesso do usuário para registrar eventos do usuário	17 de outubro de 2022
Atualizações de rede	Várias atualizações na seção “Redes e acesso”	22 de setembro de 2022
Atualização da política gerenciada	Política AmazonWorkSpacesWebServiceRolePolicy gerenciada atualizada	6 de setembro de 2022
Configurar sessões do usuário	Configurar o Input Method Editor (IME) e a localização na sessão	28 de julho de 2022
Atualizações de rede	Várias atualizações na seção “Redes e acesso”	7 de julho de 2022

Valores de tempo limite	Especifique o Tempo limite de desconexão em minutos e o Tempo limite de desconexão de inatividade em minutos	16 de maio de 2022
Política gerenciada atualizada	Atualizou a política AmazonWorkSpacesWebServiceRolePolicy gerenciada para adicionar o namespace AWS/Usage às permissões da API PutMetricData	6 de abril de 2022
Perfil vinculado ao serviço	Nova função AWSServiceRoleForAmazonWorkSpacesWeb vinculada ao serviço	30 de novembro de 2021
Política gerenciada	Nova política AmazonWorkSpacesWebReadOnly gerenciada	30 de novembro de 2021
Política gerenciada	Nova política AmazonWorkSpacesWebServiceRolePolicy gerenciada	30 de novembro de 2021
Lançamento inicial	Versão inicial do Guia de Administração do Navegador WorkSpaces Seguro	30 de novembro de 2021

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.