URLs e palavras-chave bloqueadas e liberadas

O administrador pode especificar URLs e palavras-chave para bloquear ou liberar o acesso no aplicativo. Permitindo um controle granular sobre o conteúdo acessado pelos usuários, garantindo que sites indesejados sejam bloqueados enquanto sites aprovados permaneçam acessíveis.

Bloqueio de Sites por Categoria

Pode-se bloquear o acesso a sites com base em categorias específicas. O administrador pode selecionar diferentes categorias de sites que deseja bloquear. Quando o bloqueio por categoria está ativado, qualquer site que pertença a uma dessas categorias selecionadas será automaticamente bloqueado.

Bloquear todos os sites

Como administrador, é possível ativar o bloqueio total de acesso a todos os sites. Quando o bloqueio total está ativado, nenhum site pode ser acessado pelo dispositivo. Isso significa que qualquer tentativa de navegação será bloqueada, garantindo que os usuários não consigam visitar nenhuma página da web.

Sites favoritos

Como administrador, é possível configurar sites favoritos no Security Browser para disponibilizá-los aos usuários. Adicione os sites favoritos com Nome e URL, e ao salvar a política, as configurações serão enviadas para os dispositivos. No dispositivo ao abrir o menu Favoritos do aplicativo Security Browser, será exibida as URLs cadastradas na lista de sites favoritos da configuração gerenciada.

Página de Bloqueio

Informe a URL da página que será exibida ao é possível personalizar o bloqueio de sites redirecionando para uma página definida como padrão. Ou seja, caso o usuário tente acessar um site que possui bloqueio de URL, palavra chave ou categoria, quando o app bloquear o site, ele redirecionará para a URL de bloqueio recebida na configuração gerenciada e não irá registrar a URL como site acessado

Configurações de login do navegador

Você pode decidir se os usuários podem fazer login no Google Chrome com suas contas para usar serviços como sincronização de favoritos, senhas e configurações. Caso o login no navegador esteja desativado, o usuário ainda poderá acessar serviços como Gmail, mas não conseguirá usar funcionalidades de sincronização do navegador. Se ativado, o login será automático ao acessar outros serviços do Google, mas a sincronização precisará ser ativada separadamente.

Configurações do ciclo de vida dos dados de navegação

Permite configurar quanto tempo certos dados do navegador, como histórico, senhas e cookies, serão mantidos antes de serem automaticamente apagados. Essa funcionalidade é útil para proteger informações sensíveis, mas é importante testá-la antes para evitar perder dados importantes.

Configurar o URL da página inicial

Define qual página será exibida quando o usuário clicar no botão "Início" no Google Chrome. Isso não afeta a página que aparece quando o navegador é aberto, mas os usuários não poderão alterar o URL definido.

Permitir acesso a sensores nesses sites

Você pode permitir que sites específicos utilizem sensores do dispositivo, como luz e movimento. Caso não configure nada, a decisão será baseada nas preferências gerais ou pessoais do usuário. Padrões específicos de sites podem ser usados para conceder ou bloquear esse acesso.

Permitir cookies nestes sites

Permite que você escolha quais sites têm autorização para salvar cookies no navegador. Isso pode ser configurado para aplicar a todos os subdomínios de um site ou a domínios específicos. Caso nada seja definido, as configurações padrão do navegador ou do usuário serão aplicadas.

Permitir JavaScript nestes sites

Permite habilitar JavaScript para sites específicos, garantindo que eles possam carregar conteúdos dinâmicos, como animações ou recursos interativos. Se nada for configurado, o navegador seguirá as preferências padrão do usuário. Suporta curinga (\*) nos padrões de URL.

Permitir que JavaScript use JIT nestes sites

Você pode decidir em quais sites o JavaScript pode usar a tecnologia JIT (Just In Time), que melhora o desempenho de scripts no navegador. Isso funciona apenas no domínio principal configurado e, se nada for definido, segue as configurações padrão do navegador.

Permitir pop-ups nestes sites

Você pode criar uma lista de sites que estão autorizados a abrir pop-ups no navegador. Se essa política não for configurada, a decisão será baseada na configuração padrão do navegador ou nas preferências definidas pelo próprio usuário. É possível usar curingas (\*) para incluir subdomínios.

Permitir que páginas de aviso SSL em origens específicas sejam ignoradas

Se o acesso a páginas com erro de SSL estiver desativado por padrão, você pode criar uma lista de sites em que os usuários estão autorizados a ignorar o aviso de segurança e prosseguir. Para outros sites fora dessa lista, os usuários não poderão continuar. Caso nada seja configurado, o navegador seguirá as configurações padrão.

Permitir que os sites da lista façam solicitações para endpoints de rede mais particulares de forma não segura

Permite que você especifique uma lista de sites que podem fazer solicitações para redes privadas, mesmo que essas solicitações não sejam totalmente seguras. Se não for configurada, a política agirá como se nenhuma exceção fosse permitida, e as solicitações seguirão as configurações padrão do navegador ou do usuário.

Permitir WebUSB nesses sites

Essa política permite definir quais sites podem solicitar acesso ao dispositivo USB do usuário. Se não configurada, os sites seguirão a configuração padrão ou a escolha do usuário. Certifique-se de evitar conflitos com outras políticas relacionadas ao WebUSB. O uso de caracteres curinga (\*) não é permitido.

Bloquear acesso a sensores nesses sites

Com essa configuração, você pode listar os sites que não poderão acessar sensores de luz e movimento. Caso exista conflito entre esta lista e a de sites permitidos, a lista de bloqueio terá prioridade. Caracteres curinga (\*) são permitidos para maior flexibilidade.

Bloquear cookies nestes sites

Essa política permite criar uma lista de sites que não terão permissão para configurar cookies. Se não definida, os sites seguirão a configuração padrão ou a preferência do usuário. Evite conflitos entre esta política e outras listas de cookies. O uso de caracteres curinga (\*) não é permitido.

Bloquear o uso de JIT pelo JavaScript nestes sites

Essa configuração impede que sites específicos utilizem o compilador JIT (Just In Time) para executar JavaScript, aumentando a segurança, mas potencialmente reduzindo o desempenho. A política deve ser aplicada ao domínio principal (eTLD+1), e não a subdomínios. Caso a política não seja definida, o JIT será ativado por padrão. Caracteres curinga (\*) são permitidos.

Bloquear o JavaScript nestes sites

Permite criar uma lista de sites onde o JavaScript será bloqueado. Se não configurada, o comportamento padrão ou preferências do usuário serão aplicados. A política não impede que scripts de terceiros sejam executados em subframes. Caracteres curinga (\*) são permitidos.

Bloquear pop-ups nesses sites

Essa política permite configurar sites que não podem abrir pop-ups. Caso não seja definida, a configuração padrão ou a preferida pelo usuário será aplicada. Caracteres curinga (\*) são permitidos.

Desativar o particionamento de armazenamento de terceiros para origens específicas

Permite listar origens de nível superior onde o particionamento de armazenamento de terceiros será desativado. Se não configurada, a configuração padrão será aplicada. Não especifique caminhos nos padrões de URL, pois a política considera apenas as origens.

Bloquear o WebUSB nesses sites

Essa configuração bloqueia solicitações de acesso ao dispositivo USB para os sites especificados. Em caso de conflito com outras políticas do WebUSB, nenhuma delas terá prioridade. Não permite o uso de caracteres curinga (\*).

Configuração de cookies padrão

Permite definir padrões para configuração de cookies, determinando quais sites podem ou não configurá-los durante uma sessão. Padrões conflitantes com outras políticas devem ser evitados. Caracteres curinga (\*) não são permitidos.

Limita cookies de URLs correspondentes à sessão atual

Cria uma lista de sites que podem ou não configurar cookies para a sessão atual. Em caso de não definição, a configuração padrão será aplicada. Evite conflitos com outras políticas de cookies. Caracteres curinga (\*) não são permitidos.

Tipo de conta para autenticação HTTP Negotiate

Define o tipo de conta usado para autenticação HTTP Negotiate no Android. Deixar sem definição desativa o recurso. As informações devem ser obtidas com o fornecedor do aplicativo de autenticação.

Permitir a filtragem de desempenho de acessibilidade

Controla se o Google Chrome pode otimizar dinamicamente a árvore de acessibilidade para melhorar o desempenho. Se ativada ou não definida, a otimização será permitida. Caso desativada, o recurso será bloqueado.

Permitir consultas DNS em mais tipos de registro DNS

Esta política permite ao Google Chrome consultar tipos adicionais de registro DNS ao realizar solicitações DNS não seguras, como registros HTTPS (tipo 65 de DNS), além dos padrões A (tipo 1) e AAAA (tipo 28). Se ativada ou não configurada, esses tipos adicionais serão incluídos. Caso seja desativada, apenas os tipos A e AAAA serão consultados. Esta configuração é temporária e será removida em versões futuras do navegador.

Permitir solicitações de autenticação da Web em sites com certificados TLS corrompidos

Permite que o Google Chrome aceite solicitações de autenticação da Web em sites com certificados TLS com erros. Quando ativada, essas solicitações são permitidas; caso contrário, o comportamento padrão de bloqueio será aplicado.

Lista de permissões do servidor de autenticação

Permite configurar uma lista de servidores que têm autorização para autenticação integrada. Quando o Chrome recebe um desafio de autenticação de um servidor dessa lista, ele responde. Caso não configurada, o navegador tenta detectar se o servidor está na intranet antes de responder. Caracteres curinga (\*) são permitidos.

Controlar o uso do JIT do JavaScript

Define se o Google Chrome utilizará o compilador JIT (Just In Time) para executar JavaScript. Quando desativado, o desempenho da renderização pode ser afetado, mas a segurança do conteúdo Web será aumentada. Esta configuração pode ser ajustada para sites específicos usando políticas relacionadas.

Controla o modo de DNS sobre HTTPS

Determina o comportamento do DNS sobre HTTPS no Google Chrome. O modo pode ser:"off": desativa o DNS sobre HTTPS."automatic": utiliza DNS sobre HTTPS se disponível e volta ao DNS inseguro em caso de erro."secure": usa apenas DNS sobre HTTPS, falhando em caso de indisponibilidade.

Se não configurada, o navegador segue as configurações do sistema ou do usuário.

Controla se a sintaxe :--foo descontinuada para CSS está ativadav

efine se a sintaxe :--foo, substituída por :state(foo), permanece ativa. Se ativada, permite a compatibilidade com sites que ainda utilizam a sintaxe antiga. Caso contrário, a sintaxe será desativada..

Controla se os manipuladores de eventos unload podem ser desativados

Regula a continuidade dos manipuladores de eventos unload, usados para salvar dados ao sair de uma página. Por padrão, eles serão gradualmente desativados, mas podem ser mantidos ativos se a política for configurada como verdadeira. O uso desses eventos não é recomendado devido à baixa confiabilidade e impacto no desempenho.

Suporte a cabeçalhos de solicitação de CORS sem caractere curinga

Determina se o Google Chrome suporta cabeçalhos CORS sem caracteres curingas, como "\*", para autorizar explicitamente o uso do cabeçalho Authorization. Quando ativada ou não configurada, o navegador segue esse comportamento. Caso desativada, o caractere curinga será permitido para incluir o cabeçalho Authorization. Esta política é temporária e será removida no futuro.

Desativar a aplicação da Transparência dos certificados para uma lista de hashes subjectPublicKeyInfo

Esta política permite desativar os requisitos de Transparência dos Certificados para determinados certificados identificados por um hash subjectPublicKeyInfo. Isso possibilita que hosts comerciais continuem usando certificados que, normalmente, seriam considerados inválidos devido à falta de divulgação pública. Essa política é útil para casos específicos, mas sua não configuração significa que o Google Chrome não confiará em certificados que não atendam aos requisitos de transparência.

Desativar a aplicação da Transparência dos certificados para uma lista de URLs

Permite desativar os requisitos de Transparência dos Certificados para nomes de host especificados. Essa configuração pode dificultar a detecção de certificados incorretos, mas os hosts ainda poderão utilizar certificados normalmente não confiáveis. Se a política não for configurada, o navegador não confiará em certificados que não atendam aos requisitos de transparência.

Ativar upgrades automáticos do HTTPS

O navegador tenta atualizar conexões HTTP para HTTPS automaticamente. Quando ativado (ou sem configuração), esse comportamento será padrão. Determinados hosts podem ser excluídos usando uma política separada (HttpAllowlist).

Ativar controles de rolagens focalizáveis do teclado

Essa política permite temporariamente que controles de rolagem sem filhos focalizáveis possam ser navegados pelo teclado. Quando desativada, essa funcionalidade será removida. Essa política será descontinuada após a versão M135 do Google Chrome.

Ativar previsão de rede

Controla recursos de pré-busca de DNS, pré-conexão SSL/TCP e pré-renderização de páginas no Chrome. Se configurada, impede alterações pelo usuário. Sem definição, a previsão de rede é ativada, mas o usuário pode desativá-la.

Ativar ou desativar a User-Agent Reduction

Permite controlar a redução do cabeçalho HTTP User-Agent para facilitar testes e compatibilidade com sites. Quando ativada ou sem configuração, a funcionalidade será aplicada conforme o cronograma de implementação do Google Chrome.

Ativar o contrato de chave pós-quântica para TLS

Habilita o uso de um algoritmo de contrato de chave pós-quântico em conexões TLS, protegendo o tráfego contra futuros ataques de computadores quânticos. Quando desativada, o tráfego não estará protegido. A política é temporária e será removida após a versão 141 do Chrome.

Ativar o Gerador de QR Code

Habilita o recurso de geração de QR codes no navegador. Quando desativada, essa funcionalidade será completamente removida.

Ativa o isolamento de sites para origens específicas em dispositivos Android

Permite isolar sites específicos em processos separados no Android, aumentando a segurança para origens confidenciais. Essa configuração é recomendada apenas para dispositivos com mais de 1 GB de RAM, devido a possíveis impactos de desempenho. Se desativada, todo isolamento será desabilitado, incluindo sites protegidos por padrão.

Ativar a verificação rigorosa de tipo MIME para scripts de worker

Esta política controla se o Chrome aplica verificação rigorosa de tipo MIME para scripts de worker. Quando ativada ou não configurada, apenas scripts com tipos MIME válidos, como JavaScript, serão aceitos. Desativar esta política permite o uso de tipos MIME legados, como text/ascii, mas isso pode comprometer a segurança.

Ativar a resolução de DNS do sistema fora do serviço de rede

Permite configurar se as resoluções de DNS do sistema serão executadas dentro ou fora do processo de rede do Chrome. Ativá-la pode melhorar o desempenho, enquanto desativá-la mantém a execução no processo de rede para maior segurança. Sem configuração, o comportamento será baseado na configuração do sistema e em flags.

Ativar Encrypted ClientHello do TLS

Habilita o uso do recurso Encrypted ClientHello (ECH), que protege informações sensíveis durante conexões TLS. Quando ativada ou sem definição, o Chrome seguirá o cronograma padrão para implementação. Desativá-la impede o uso do ECH, que é um protocolo experimental e sujeito a mudanças futuras.

Ativar suporte à codificação de conteúdo zstd

Habilita o suporte para compactação de conteúdo usando "zstd" no Chrome. Se ativada ou sem definição, o navegador aceitará conteúdo compactado nesse formato. Desativar essa política desabilita o suporte ao zstd. Essa é uma configuração temporária e será removida em versões futuras.

URLs de inicialização de apps para autenticação externa

Permite especificar URLs de autenticação processados pelo Android WebView, que podem inicializar aplicativos de autenticação externos. Essa funcionalidade é útil para Single Sign-On (SSO) ou autenticação baseada em segurança avançada. Se não houver aplicativos compatíveis instalados, a autenticação continuará no WebView.

Lista de permissões de HTTP

Define uma lista de domínios que não serão atualizados para HTTPS nem exibirão mensagens de erro no modo HTTPS-First. Essa política é usada para manter compatibilidade com servidores que não suportam HTTPS. Apenas nomes de host específicos são permitidos, e curinga (\*) não é aceito.

Disponibilidade do modo de navegação anônima

Controla se o usuário pode acessar o modo de navegação anônima no Chrome. As opções são permitir (Enabled), bloquear (Disabled) ou forçar o uso exclusivo do modo anônimo (Forced). No iOS, alterações nessa configuração só entram em vigor após reiniciar o navegador.

Lista de permissões do servidor de delegação Kerberos

Define quais servidores podem delegar credenciais de usuários por meio de autenticação Kerberos no Chrome. É possível usar caracteres curinga (\*) para abranger vários servidores. Se a política não for definida, a delegação de credenciais será desativada.

Lista de nomes que contornarão a verificação de política HSTS

Permite que determinados nomes de host ignorem a política HSTS, evitando a obrigatoriedade de upgrades de HTTP para HTTPS. Aplica-se apenas a nomes de host específicos e estáticos, não abrangendo subdomínios. Essa configuração é útil para compatibilidade com sistemas legados.

Lista de origens que autorizam todas as autenticações HTTP

Permite especificar origens onde todos os esquemas de autenticação HTTP são aceitos, independentemente de outras políticas de autenticação. É possível configurar até 1.000 exceções utilizando padrões de URL, incluindo caracteres curinga, para definir as origens permitidas.

Lista de tipos a serem excluídos da sincronização

Define quais tipos de dados não serão sincronizados no Chrome, como extensões, senhas ou histórico de navegação. Isso ajuda a reduzir o tamanho do perfil sincronizado. Alguns tipos de dados estão interligados, como "autofill" e "payments", que são desativados juntos.

Configurações de proxy

Permite definir configurações específicas de proxy no Chrome, como uso de servidores específicos, scripts PAC ou detecção automática. A configuração pode ser adaptada para diferentes cenários, como ignorar proxies para determinados hosts ou aplicar proxies fixos.

Contas restritas que estão visíveis no Google Chrome

Controla quais contas do Google são exibidas no navegador com base em padrões de nome configurados. Contas não correspondentes aos padrões definidos serão ocultadas, mas ainda podem ser acessadas pelos usuários. Caracteres curinga são suportados.

Mostrar uma visualização do histórico do Chrome com grupos de páginas

Ativa ou desativa a exibição de histórico organizado em grupos de páginas no Chrome. Quando ativada, os usuários podem acessar o histórico agrupado em chrome://history/grouped. Caso desativada, a funcionalidade será removida.

Especifica o modelo de URI do resolvedor DNS sobre HTTPS desejado

Permite configurar modelos de URI para usar DNS sobre HTTPS (DoH). Isso define servidores específicos de DoH, que podem ser usados em conjunto com o modo "secure" ou "automatic" do Chrome. Configurações incorretas serão ignoradas.

Esquemas de autenticação compatíveis

Define quais esquemas de autenticação HTTP (como basic, digest, NTLM ou Negotiate) serão suportados no Chrome. Caso não definido, todos os esquemas disponíveis serão permitidos.

Token de registro da política de nuvem

Permite registrar o Chrome no gerenciamento de políticas de nuvem do Google. O administrador deve fornecer um token de inscrição obtido no Google Admin Console para configurar essa política.

Usar cliente DNS integrado

Controla se o Chrome utiliza o cliente DNS integrado ou o cliente do sistema operacional para consultas DNS. O cliente integrado é sempre usado para DNS sobre HTTPS. Desativar essa política força o uso do cliente DNS integrado apenas para consultas seguras.

Permitir a mescla de políticas de dicionário de diferentes fontes

Habilita a mesclagem de políticas baseadas em dicionário vindas de origens distintas, considerando a prioridade das origens. Conflitos são resolvidos com base no escopo ou nível mais alto de prioridade.

Permitir a mescla de políticas de lista de diferentes fontes

Semelhante à mescla de políticas de dicionário, mas para políticas baseadas em listas. Valores de origens com o mesmo escopo são mesclados, e origens de maior prioridade prevalecem em conflitos.

Permitir relatórios de dados relacionados à confiabilidade do domínio

Controla o envio de relatórios diagnósticos sobre confiabilidade do domínio. Se desativada, nenhum dado será enviado ao Google. Caso ativada ou indefinida, o envio seguirá a configuração global de relatórios de métricas do Chrome.

Permitir que o recurso da lista de compras seja ativado

Controla a disponibilidade do recurso da lista de compras. Quando ativada ou indefinida, o recurso será acessível para monitorar preços de produtos no painel lateral de favoritos.

Permitir que as políticas da nuvem de usuários substituam as políticas do Chrome Browser Cloud Management

Permite que políticas associadas ao Google Workspace tenham precedência sobre políticas do Chrome Browser Cloud Management, desde que sejam originadas de usuários seguros.

Controlar o recurso de BackForwardCache

Habilita ou desabilita o BackForwardCache, que armazena páginas em estado atual para navegação mais rápida ao retornar.

Configuração padrão do particionamento de armazenamento de terceiros

Controla o particionamento de armazenamento de terceiros, permitindo ou bloqueando por padrão para todas as origens, salvo definições específicas.

Determinar a disponibilidade de variações

Especifica se variações podem ser aplicadas ao navegador, incluindo correções críticas de segurança ou desativação completa.

Ativar atualizações de componentes no Google Chrome

Controla as atualizações de componentes do navegador. Certos componentes essenciais para segurança não são afetados.

Ativar o First-Party Sets

Ativa ou desativa o recurso de conjuntos primários, que facilita integrações entre sites relacionados.

Ativar conjuntos de sites relacionados

Permite o controle de conjuntos de sites relacionados, substituindo a política de conjuntos primários.

Ativar relato de uso e dados relacionados a falhas

Ativa o envio de relatórios anônimos de uso e falhas ao Google, permitindo que os usuários alterem essa configuração.

Ativa políticas experimentais

Permite o carregamento de políticas experimentais, com o risco de instabilidade ou falhas não previstas.

Ativa a unificação das políticas de nuvem de usuários com políticas no nível da máquina

Mescla políticas associadas ao Google Workspace com políticas no nível da máquina, desde que sejam de usuários seguros.

Portas de rede explicitamente permitidas

Define portas UDP explícitas que podem ser usadas, mesmo se normalmente bloqueadas para segurança.

Origens ou padrões de nome do host aos quais as restrições sobre origens não seguras não se aplicam

Permite especificar origens ou hosts inseguros que não sofrerão restrições de segurança, útil para servidores de desenvolvimento.

Substituir o First-Party Sets

Permite substituir a lista de conjuntos primários usada pelo navegador, ajustando configurações específicas de sites.

Substitui conjuntos de sites relacionados

Substitui a lista de conjuntos de sites relacionados, controlando como os recursos de integração de sites são aplicados.

Restringir o alcance das portas UDP locais usadas por WebRTC

Restringe o intervalo de portas UDP que podem ser usadas pelo WebRTC, garantindo maior controle de segurança.

Especifica se os sites têm permissão para fazer solicitações para endpoints de rede mais particulares de forma não segura

Controla a permissão de solicitações inseguras para endpoints de rede mais particulares, podendo desativar avisos e bloqueios.

Especifica se é necessário aplicar restrições a solicitações para endpoints de uma rede mais particular

Bloqueia solicitações inseguras para endpoints privados sempre que verificações falharem, reforçando segurança em redes privadas.

Suprimir alertas de domínios parecidos em domínios

Desativa alertas de URLs similares para domínios especificados, prevenindo avisos de possíveis tentativas de spoofing.

Permitir o uso do Chrome for Testing

Controla se os usuários podem usar o Chrome for Testing, permitindo ou bloqueando sua execução em perfis específicos.

Permitir a criação de sessões immersive-ar da WebXR

Permite ou bloqueia a criação de sessões de realidade aumentada imersiva via WebXR Device API.

Permitir que o HTTPS-Only Mode seja ativado

Controla se os usuários podem ativar o modo somente HTTPS. Pode ser ativado, desativado ou forçado em modos diferentes.

Permitir que as páginas com o cabeçalho Cache-Control: no-store sejam inseridas no cache de avanço e retorno

Define se páginas com cabeçalho Cache-Control: no-store podem ser restauradas do cache de avanço e retorno.

Permitir a continuação na página de aviso SSL

Permite ou impede os usuários de ignorarem avisos SSL.

Permitir verificações em tempo real com o proxy da Navegação segura

Controla se o Navegação segura pode usar proxies para verificar URLs.

Permitir que sites consultem formas de pagamento disponíveis

Define se sites podem verificar se usuários salvaram formas de pagamento.

Perguntar onde salvar cada arquivo antes de fazer download

Pergunta ao usuário onde salvar arquivos antes do download.

Conceder automaticamente permissão a esses sites para se conectarem a dispositivos USB com determinados IDs de fornecedores e produtos.

Cria uma lista de padrões de URL que especifica quais sites têm permissão automática para acessar dispositivos USB específicos.

Bloquear cookies de terceiros

Controla se cookies de terceiros podem ser definidos. Pode ser ativado ou bloqueado.

Definir se a configuração do Privacy Sandbox para a medição de anúncios pode ser desativada

Controla se os usuários podem desativar a configuração de medição de anúncios no Privacy Sandbox.

Definir se a configuração do Privacy Sandbox para temas de anúncios pode ser desativada

Controla se os usuários podem desativar a configuração de temas de anúncios no Privacy Sandbox.

Definir se a solicitação do Privacy Sandbox pode ser mostrada aos usuários

Controla se a solicitação do Privacy Sandbox será exibida aos usuários.

Definir se a configuração do Privacy Sandbox para anúncios sugeridos pelo site pode ser desativada

Controla se os usuários podem desativar a configuração de anúncios sugeridos pelo site no Privacy Sandbox.

Como configurar o comportamento dos TOS durante a primeira execução do CCT

Controla se os Termos de Serviço são exibidos na primeira execução do navegador em dispositivos Android.

Controlar a filtragem de conteúdo adulto SafeSites.

Define o nível de filtro para sites com conteúdo adulto.

Controlar o recurso de IntensiveWakeUpThrottling.

Controla a limitação de timers JavaScript em guias de segundo plano para economizar bateria e CPU.

Controla o uso da API Web Bluetooth

Controla o acesso de sites a dispositivos Bluetooth via API Web Bluetooth.

Controla o uso da API WebUSB

Controla o acesso de sites a dispositivos USB via API WebUSB.

Suporte ao URL dos dados para SVGUseElement.

Ativa ou desativa o suporte a URLs de dados para SVGUseElement.

Configuração padrão de geolocalização

Define o padrão para permitir ou negar o rastreamento de localização física dos usuários.

Configuração padrão do JavaScript

Define o padrão para permitir ou bloquear a execução de JavaScript.

Configuração padrão de pop-ups

Define o padrão para permitir ou bloquear pop-ups.

Configuração padrão de sensores

Define o padrão para permitir ou bloquear o uso de sensores como luz e movimento.

Permitir que o HTTPS-Only Mode seja ativado

Controla se os usuários podem ativar o modo somente HTTPS. Configuração pode ser 'permitida', 'force\_enabled' ou 'force\_balanced\_enabled'.

Definir os domínios que têm permissão para acessar o Google Workspace

Ativa login restrito ao Google Workspace, permitindo apenas contas de domínios especificados. Impede login secundário em dispositivos gerenciados para contas fora da lista permitida. Adicione "consumer\_accounts" para incluir contas @gmail.

Desativar consulta CNAME ao negociar a autenticação do Kerberos

Ignora pesquisa CNAME, usando o nome do servidor como inserido para gerar o SPN do Kerberos. Sem definição, a pesquisa CNAME determina o nome canônico do servidor.

Desativa a continuação na página de aviso de Navegação segura

Impede usuários de prosseguir em sites sinalizados como maliciosos pelo serviço "Navegação segura". Não afeta problemas relacionados a certificados SSL.

Desativar o salvamento do histórico do navegador

Quando ativada, o histórico não é salvo e a sincronização de guias é desativada. Usuários não podem alterar essa configuração.

Ativar páginas de erro alternativas

Permite o uso de páginas de erro alternativas no Chrome, como "Página não encontrada". Pode ser configurada para impedir alterações pelos usuários.

Ativa o Preenchimento automático de endereços

Controla a ativação do preenchimento automático de endereços. Quando ativada, os usuários podem gerenciar essa configuração.

Ativar o preenchimento automático para cartões de crédito

Permite que os usuários ativem ou desativem o preenchimento automático para cartões de crédito. Quando desativada, o preenchimento automático é completamente bloqueado.

Ativar Google Cast

Controla a ativação do recurso Google Cast, permitindo ou bloqueando o acesso em menus e controles compatíveis.

Ativar a substituição da verificação de acessibilidade do IPv6

Define se a verificação de acessibilidade do IPv6 será ignorada, permitindo consultas AAAA mesmo sem acessibilidade ao IPv6.

Ativa a detecção de vazamento para credenciais digitadas

Permite que o Chrome alerte usuários sobre credenciais comprometidas em vazamentos. Requer que a Navegação segura esteja ativada.

Ativar autenticação NTLMv2.

Ativa ou desativa NTLMv2, que é compatível com servidores recentes do Windows e Samba.

Ativar ou desativar a edição de favoritos

Controla se os usuários podem adicionar, remover ou modificar favoritos no navegador.

Ativar impressão

Define se os usuários podem usar a funcionalidade de impressão do Google Chrome. Pode ser desativada para impedir o uso de impressoras.

Ativar a leitura em voz alta (destilação de texto e síntese de conversão de texto em voz) para páginas da Web

Permite leitura de páginas Web qualificadas em voz alta, utilizando destilação de texto e conversão de texto em voz.

Ativar relatórios estendidos do Navegação segura

Envia dados adicionais de sistema e páginas visitadas para ajudar a detectar sites maliciosos. Pode ser configurado para obrigatoriedade.

Ativar salvamento de senhas no gerenciador de senhas

Permite que o Chrome salve senhas automaticamente. Se desativada, impede o salvamento de novas senhas, mas mantém as já existentes.

Permitir rolagem para texto especificado em fragmentos de URL

Ativa a navegação para textos específicos em URLs. Quando desativada, bloqueia esse comportamento.

Ativa o compartilhamento de credenciais do usuário com outros usuários

Permite o envio e recebimento de senhas entre membros da família. Requer sincronização de senhas ativada.

Ativar o isolamento de todos os sites

Isola cada site em um processo próprio, melhorando a segurança. Aplicável a dispositivos Android com mais de 1 GB de RAM.

Ativar comportamento padronizado de zoom do navegador

Ajusta a propriedade "zoom" do CSS para seguir novas especificações, afetando o comportamento do navegador.

Ativa o recurso de área de transferência compartilhada

Permite enviar texto entre dispositivos Chrome e Android conectados com sincronização ativada.

Ativar Traduzir

Fornece ferramentas integradas de tradução, incluindo uma barra de tradução e opção de menu de contexto. Pode ser desativado para remover o recurso.

Ativar a coleta de dados anônimos inseridos no URL

Controla se a coleta de dados anônimos inseridos no URL será sempre ativada, desativada ou deixada para o usuário configurar.

Permitir que extensões gerenciadas usem a API Enterprise Hardware Platform

Define se extensões gerenciadas podem usar a API Enterprise Hardware Platform.

Ativar o conceito de grupos atômicos de política

Ativa o conceito de grupos atômicos de política para priorizar a origem com maior relevância em grupos.

Aplicar o Modo restrito mínimo do YouTube

Define o nível mínimo do Modo restrito aplicado ao YouTube.

A política de nuvem do Google Chrome substitui a política da plataforma

Estabelece se políticas de nuvem podem substituir políticas de plataforma em caso de conflito.

Fazer com que Access-Control-Allow-Methods corresponda à especificação de simulação do CORS em conformidade

Controla se métodos de solicitação no CORS serão case-sensitive ao serem comparados.

Nível de proteção do Navegação segura

Permite controlar o nível de proteção do Navegação segura, variando entre nenhum, padrão e avançado.

Mostrar sugestões de conteúdo na página Nova guia

Ativa ou desativa sugestões de conteúdo na página Nova guia com base no histórico de navegação.

Especifica se as pesquisas do Google Chrome no produto são mostradas aos usuários

Define se pesquisas de feedback do Google Chrome podem ser exibidas aos usuários.

Suprimir caixas de diálogo de JavaScript acionadas por subframes de origem diferentes

Configura o bloqueio de caixas de diálogo JavaScript de subframes de origem diferente.

O teclado virtual redimensiona a janela de visualização de layout por padrão

Permite que o teclado virtual redimensione a janela de layout por padrão.

Permitir a pesquisa assistida pela câmera do Google Lens

Controla se os usuários podem pesquisar com a câmera usando o Google Lens.

Codificações do provedor de pesquisa padrão

Especifica as codificações de caracteres compatíveis com o provedor de pesquisa padrão.

Nome do provedor de pesquisa padrão

Define o nome do provedor de pesquisa padrão exibido ao usuário.

URL de pesquisa do provedor de pesquisa padrão

Configura o URL de pesquisa padrão usado para realizar buscas.

URL sugerido do provedor de pesquisa padrão

Define o URL sugerido do provedor de pesquisa padrão para exibir sugestões de pesquisa.

Ativar sugestões de pesquisa

Ativa ou desativa sugestões de pesquisa na barra de endereço.

Ativar o provedor de pesquisa padrão

Controla se um provedor de pesquisa padrão será definido e ativado.

Ativar Pesquisa por toque

Habilita ou desabilita a funcionalidade de Pesquisa por toque para o usuário.

Forçar o Google SafeSearch

Força a ativação do Google SafeSearch para todas as buscas realizadas.

Lista de URLs alternativos para o provedor de pesquisa padrão

Configura URLs alternativos para o provedor de pesquisa padrão.

Parâmetro que fornece recursos de pesquisa por imagem para o provedor de pesquisa padrão

Define parâmetros de busca para recursos de pesquisa por imagem no provedor padrão.

Parâmetros para URL de imagens que usa POST

Configura parâmetros usados para pesquisa de imagem utilizando o método POST.

Parâmetros para URL de pesquisa que usa POST

Define parâmetros para pesquisas padrão usando o método POST.

Parâmetros para URL de sugestões que usa POST

Especifica restrições adicionais para certificados TLS confiáveis no Chrome.

Certificados TLS que precisam ser considerados confiáveis pelo Google Chrome para autenticação do servidor com restrições

Lista de certificados TLS que não devem ser considerados confiáveis.

Certificados TLS que não são confiáveis ou aqueles que não são confiáveis, mas podem ser usados na criação de caminhos para autenticação do servidor

Configura o uso de certificados TLS adicionados manualmente em repositórios da plataforma.

Usar certificados TLS adicionados pelo usuário de repositórios de confiança da plataforma para autenticação do servidor

Permite ou desativa a preservação de espaços em branco em URLs do tipo DataURL.

Preservação de espaços em branco do DataURL para todos os tipos de mídia

Estabelece níveis de restrição para downloads de arquivos perigosos ou maliciosos.

Permitir restrições de downloads

Controla o comportamento do analisador HTML em relação ao elemento .

Controla se o novo comportamento do analisador HTML para o elemento está ativado

Faz com que URLs de blob em SharedWorker sigam a especificação para herdar controladores.

Faça com que o comportamento do URL do blob SharedWorker esteja alinhado com a especificação

Define se gerenciadores de senhas de terceiros podem ser usados no Chrome para Android.

Permitir o uso de gerenciadores de senhas de terceiros no Google Chrome no Android

Permite o uso de gerenciadores de senhas de terceiros no Android, desde que configurados como padrão no sistema. Se definido como verdadeiro, os usuários podem alternar entre o gerenciador integrado e o de terceiros. APIs de acessibilidade não são afetadas.