

[Click Here](#)



Esto se aplica a navegadores Chrome y dispositivos ChromeOS gestionados. Como administrador de Chrome Enterprise, puedes bloquear o permitir URLs para que los usuarios solo puedan visitar determinados sitios web. Restringir el acceso de los usuarios a Internet puede ayudarte a aumentar la productividad y a proteger tu organización contra los virus y el contenido malicioso de algunos sitios web. Cuando bloquear o permitir URLs Con las listas de URLs permitidas y bloqueadas puedes gestionar URLs de manera básica. Si necesitas opciones de filtrado más avanzadas, usa una herramienta para filtrar contenido, un servidor proxy web o una extensión. Incluye URLs en la lista de URLs permitidas o en la de URLs bloqueadas para hacer lo siguiente: Permitir el acceso a todas las URLs, excepto a las que quieras bloquear; puedes usar la lista de URLs bloqueadas para impedir que los usuarios visiten determinados sitios web, pero permitirles que accedan a todos los demás. Bloquear el acceso a todas las URLs, excepto a las que quieras permitir; puedes usar la lista de URLs bloqueadas para impedir el acceso a todas las URLs y, a continuación, usar la lista de permitidas para permitir el acceso a una lista limitada de URLs. Definir excepciones para listas de URLs bloqueadas muy restrictivas; puedes usar la lista de URLs bloqueadas para impedir el acceso a todas las URLs y, a continuación, la lista de URLs permitidas para que los usuarios accedan a ciertos esquemas, subdominios de otros dominios, puertos o rutas específicas. Permitir que el navegador Chrome abra aplicaciones; puedes permitir controladores de protocolos externos específicos para que el navegador Chrome pueda abrir ciertas aplicaciones automáticamente. A veces, la lista de URLs bloqueadas y la de permitidas no funcionan según lo previsto. Por ejemplo, si bloqueas el acceso a un sitio web completo, pero permites la URL de una página web concreta de ese sitio web, los usuarios podrían tener acceso a otro contenido del sitio web. Cuando se utiliza el inicio de sesión único de SAML u OpenID Connect para la autenticación de usuarios, o cuando se configuran conexiones de red con portales cautivos fuera de las sesiones de usuario, puedes bloquear o permitir URLs en las pantallas de inicio de sesión y de bloqueo de los usuarios mediante las políticas DeviceAuthenticationURLBlocklist y DeviceAuthenticationURLAllowlist. Para obtener más información, consulta URLs bloqueadas en las pantallas de inicio de sesión o de bloqueo y Excepciones de URLs bloqueadas en las pantallas de inicio de sesión o de bloqueo. Excepciones de bloqueo de URLs Se recomienda no bloquear algunas URLs, como: chrome://settings chrome://os-settings chrome-untrusted:// Para bloquear URLs de Chrome, te recomendamos que uses la opción Bloquear URLs internas sensibles de Chrome en la consola de administración de Google en lugar de añadir las URLs manualmente a la lista de URLs bloqueadas. Es una forma más rápida y segura de bloquear el acceso de los usuarios a URLs internas sensibles. Si añades URLs manualmente, puede que se produzcan problemas inesperados en el dispositivo. Para ver la lista completa de URLs de Chrome bloqueadas, consulta el artículo Bloquear URLs internas sensibles de Chrome. Para bloquear funciones del sistema, como la cámara, los ajustes del SO y la configuración del navegador, te recomendamos que uses la opción Funciones inhabilitadas del sistema en la consola de administración en lugar de usar el ajuste Bloqueo de URLs o bloquear aplicaciones y extensiones por ID. De esta forma, se bloquean todos los ajustes, no solo la parte de las URLs. Si quieres bloquear una página concreta, deberías aislar los elementos específicos a los que quieres impedir que accedan los usuarios. Después, puedes comunicar al equipo de asistencia de Chrome o de ChromeOS las políticas que quieres que se implementen. A continuación, los desarrolladores podrán añadir una política para las funciones específicas que deberían bloquearse. Paso 1: Revisa las políticas Política Descripción URLBlocklist Impide que los usuarios accedan a la lista de URLs bloqueadas. Los usuarios pueden acceder a todas las URLs, excepto a las bloqueadas. Sin definir: los usuarios pueden acceder a todas las URLs de sitios web, sin excepción. URLAllowlist Usala junto con URLBlocklist para permitir que los usuarios accedan a URLs específicas como excepción a la lista de bloqueadas. La lista de URLs permitidas tiene prioridad con respecto a la lista de URLs bloqueadas. Para que esta política funcione, necesitas añadir al menos una entrada en la lista de URLs bloqueadas. Sin definir: no hay ninguna excepción a la lista de URLs bloqueadas. Paso 2: Especifica las URLs que pueden visitar los usuarios de Chrome En función de cómo quieras gestionar estas políticas, haz clic en la opción correspondiente para ver los pasos que debes seguir. Consola de administración Se pueden aplicar a usuarios que hayan iniciado sesión desde cualquier dispositivo o navegador registrado en Windows, Mac, Linux o Android. Para obtener más información, consulta Saber cuándo se aplican los ajustes. Inicia sesión con una cuenta de administrador en consola de administración de Google. Si no usas una cuenta de administrador, no podrás acceder a la consola de administración. (Opcional) Para aplicar el ajuste solo a algunos usuarios y navegadores registrados, en un lateral, selecciona una unidad organizativa (que se suele usar para los departamentos) o un grupo de configuración (avanzado). Ver cómo funciona. La configuración de los grupos prevalece sobre las unidades organizativas. Más información Vé a Contenido. Haz clic en Bloqueo de URLs e introduce las URLs según sea necesario: Puedes bloquear o permitir hasta 1000 URLs. Haz clic en Guardar. También puedes hacer clic en Anular en una unidad organizativa. Para restaurar más tarde el valor heredado, haz clic en Heredar (o en Sin definir, si se trata de un grupo). Las aplicaciones que utilizan el componente WebView del sistema Android no reconocen el ajuste URLs bloqueadas. Para requerir que estas aplicaciones tengan en cuenta la lista de URLs bloqueadas, define las URLs bloqueadas en un archivo de texto y aplica dicha lista a las aplicaciones Android una por una. En el caso de las aplicaciones que no usen el componente WebView del sistema Android, consulta la documentación de la aplicación para obtener más información sobre cómo restringir el acceso de una forma similar. Las aplicaciones que utilizan el componente WebView del sistema Android suelen reconocer el ajuste Excepciones de URLs bloqueadas. Sin embargo, es posible que otras aplicaciones no respeten la lista de URLs bloqueadas. Puedes permitir las aplicaciones que utilicen el componente WebView del sistema Android y omitir las que no. Para obtener información sobre cómo permitir aplicaciones Android, consulta el procedimiento para permitir que se instalen aplicaciones aprobadas. Windows La información de este artículo está dirigida a los usuarios de Windows que inician sesión en una cuenta gestionada con el navegador Chrome. Mediante el Editor de administración de directivas de grupo En el editor de directivas de grupo local de Microsoft Windows (carpeta Configuración del equipo o Configuración de usuario): Ve a Directivas Plantillas administrativasGoogleGoogle Chrome. Habilita Bloquear el acceso a una lista de URLs. Nota: Si no aparece esta política, descarga la plantilla de políticas más reciente. Añade las URLs que quieres bloquear. Si esta política se deja como No configurada, seguirá el comportamiento Sin definir descrito más arriba en este artículo. Habilita Permitir el acceso a una lista de URLs. Añade las URLs a las que quieres que puedan acceder los usuarios. Si esta política se deja como No configurada, seguirá el comportamiento Sin definir descrito más arriba en este artículo. Implementa la actualización en las cuentas de tus usuarios. Puedes bloquear o permitir hasta 1000 URLs. Consulta la sintaxis de URL correcta en el artículo Permitir o bloquear sitios web: formato de los filtros de URLs. Mac Se aplica a los usuarios de AppleMac que hayan iniciado sesión con cuentas gestionadas en el navegador Chrome. En el perfil de configuración de políticas de Chrome (archivo .plist). Añade o actualiza las siguientes claves. Añade las URLs que quieres bloquear a la clave URLBlocklist. Añade a la clave URLAllowlist las URLs a las que quieres que puedan acceder los usuarios. Implementa los cambios en las cuentas de tus usuarios. Puedes bloquear o permitir hasta 1000 URLs. Consulta la sintaxis de URL correcta en el artículo Permitir o bloquear sitios web: formato de los filtros de URLs. En este ejemplo se muestra cómo bloquear todas las URL, excepto mail.example.com, wikipedia.org y google.com. URLBlocklist * URLAllowlist mail.example.com wikipedia.org google.com Linux Se aplica a los usuarios de Linux que hayan iniciado sesión con cuentas gestionadas en el navegador Chrome. En el editor de archivos JSON que prefieras: Ve a la carpeta /etc/opt/chrome/policies/managed. Crea o actualiza un archivo JSON e introduce las URLs según sea necesario: En URLBlocklist, añade las URLs que quieras bloquear. En URLAllowlist, añade las URLs a las que quieres que puedan acceder los usuarios. Implementa la actualización en las cuentas de tus usuarios. Puedes bloquear o permitir hasta 1000 URLs. Consulta la sintaxis de URL correcta en el artículo Permitir o bloquear sitios web: formato de los filtros de URLs. En este ejemplo se muestra cómo bloquear todas las URL, excepto mail.example.com, wikipedia.org y google.com. Primero, crea un archivo que contenga las URLs bloqueadas. { "URLBlocklist": ["*"] } A continuación, crea un archivo con la lista de URLs permitidas. { "URLAllowlist": ["mail.example.com", "wikipedia.org", "google.com"] } Android Se aplica a los usuarios de Android que inician sesión en el navegador Chrome con una cuenta gestionada. Si te has registrado en Chrome Enterprise Core, usa la consola de administración para gestionar el navegador Chrome en dispositivos Android. Sigue los pasos que se indican en la sección Consola de administración de este artículo. De lo contrario, te recomendamos que pidas a tu proveedor de gestión de dispositivos móviles (MDM) que configure políticas de bloqueo de URLs para Chrome en Android. Consulta el artículo Configurar Chrome Enterprise Core. iOS y iPadOS La información de este artículo se aplica a los usuarios de iPhone y iPad que inician sesión en el navegador Chrome con una cuenta gestionada. Si te has registrado en Chrome Enterprise Core, usa la consola de administración para gestionar el navegador Chrome en dispositivos iPhone y iPad. Sigue los pasos que se indican en la sección Consola de administración de este artículo. De lo contrario, te recomendamos que pidas a tu proveedor de gestión de dispositivos móviles (MDM) que configure políticas de bloqueo de URLs para Chrome en iOS y iPadOS. Consulta el artículo Configurar Chrome Enterprise Core. Paso 3: Verifica que las políticas se han aplicado Después de aplicar una política de Chrome, los usuarios deben reiniciar el navegador Chrome para que los cambios surtan efecto. Puedes revisar los dispositivos de los usuarios para asegurarte de que la política se ha aplicado correctamente. En un dispositivo Chrome gestionado, ve a chrome://policy. Haz clic en Volver a cargar políticas. Comprueba que el estado de URLBlocklist y de URLAllowlist sea Correcto. En URLBlocklist y URLAllowlist, haz clic en Mostrar el valor y comprueba que los campos de valores sean los mismos que has definido en la política. A página "Contas vinculadas" em Administrador foi movida para "Central de dados" em Ferramentas . A Central de Dados do Google Ads é uma ferramenta de importação e gerenciamento de dados com uma interface simplificada e que permite trazer dados dos clientes de fora do Google e ativar essas informações no Google Ads. Saiba mais sobre a Central de Dados do Google Ads. Para oferecer uma visão abrangente e consolidada dos seus públicos-alvo e simplificar a otimização e o gerenciamento deles, implementamos as seguintes melhorias no Google Ads: Novo Relatório de público-alvoAgora, os relatórios detalhados sobre informações demográficas, segmentos e exclusões de públicos-alvo estão consolidados em um só lugar. Clique no ícone Campanhas , abra a guia "Públicos-alvo, palavras-chave e conteúdo" e clique em Públicos-alvo. Também é possível gerenciar facilmente seus públicos-alvo nessa página de relatórios. Saiba mais sobre os Relatórios de público-alvo. Novos termos Estamos usando novos termos no seu Relatório de público-alvo e no Google Ads. Por exemplo, os "tipos de públicos-alvo" (incluindo personalizados, no mercado e de afinidade) agora são conhecidos como "segmentos de público-alvo" e o "remarketing" agora é chamado de "seus dados". Saiba mais sobre as atualizações das frases e termos relacionados a públicos-alvo. Com a Segmentação por Lista de Clientes, é possível segmentar anúncios para seus clientes com base nos dados que eles compartilham com você. Basta criar um arquivo CSV com esses dados e fazer o upload dele no Google Ads ou conectar uma nova fonte de dados para incorporar essa segmentação às suas campanhas. Neste artigo, vamos mostrar como fazer o upload dos arquivos de dados para criar listas de clientes. Para usar o arquivo de dados de clientes, é preciso formatá-lo corretamente. Se você está com dificuldade no processo de upload, saiba como corrigir problemas com listas de clientes. Antes de começar Consulte o artigo Sobre a Segmentação por Lista de Clientes para entender como ela funciona. Para mais informações sobre como o Google usa os arquivos de dados enviados e como o processo de correspondência funciona, consulte o artigo Como o Google usa os dados de Segmentação por Lista de Clientes. Instruções As instruções a seguir ensinam a conectar uma nova fonte de dados para criar uma lista de clientes. Na sua conta do Google Ads, clique no ícone Ferramentas . Clique no menu suspenso Biblioteca compartilhada no menu da seção. Clique em Gerenciador de públicos-alvo. Clique no botão de adição para criar um novo segmento. Selecione Lista de clientes no menu suspenso. Observação: se você já criou um segmento e não adicionou uma fonte de dados, clique em Ferramentas > Central de dados > Produtos conectados > + Conectar produto. Em Fonte de dados, selecione Conectar uma nova fonte de dados e escolha uma opção na lista. Selecione Conexão direta e clique em Continuar. Selecione o tipo de dados e clique em Avançar. Digite o banco de dados do Redshift que você quer usar e o local, a porta, o nome de usuário e a senha dele, depois clique em "Conectar". Por padrão, o Redshift usa URLs de local do banco de dados que seguem este modelo: cluster-identifier.account-number.aws-region.redshift.amazonaws.com. Informe o esquema e a tabela (ou visualização) do Redshift que você quer usar e clique em Avançar. Selecione Conexão direta e clique em Continuar. Insira sua chave de acesso secreta do Amazon S3 e clique em Conectar. Clique em Avançar. Selecione o tipo de dados e clique em Avançar. Insira o URL do arquivo que você quer enviar (em relação ao endereço do host) e clique em Avançar. Confira os tipos de arquivo compatíveis conforme a seção Requisitos deste artigo. Selecione Conexão direta e clique em Continuar. Observação: se você já vinculou uma fonte de dados na tela "Central de dados", escolha Selecionar uma fonte. Em Selecione um tipo de dados, escolha o tipo de dados e clique em Continuar. Selecione o projeto, o conjunto de dados e a tabela do BigQuery que você quer usar. Um alerta vai aparecer. Clique em Aplicar para conceder acesso e, depois, em Avançar. Selecione o tipo de dados e clique em Avançar. Digite o caminho do arquivo para upload e clique em Avançar. Saiba como Formatar seu arquivo de dados de clientes. Se você nunca se conectou a esse recurso antes, um alerta vai aparecer. Clique em Aplicar para conceder acesso e, depois, em Avançar. Observação: você precisa ter um papel com permissão para delegar storage.bucket.setIamPolicy ao bucket relevante. Selecione Conexão direta e clique em Continuar. Selecione o tipo de dados e clique em Avançar. Digite o banco de dados do PostgreSQL que você quer usar e o local, a porta, o nome de usuário e a senha dele, depois clique em Conectar. Informe o esquema e a tabela (ou visualização) do PostgreSQL que você quer usar e clique em Avançar. Saiba como Formatar seu arquivo de dados de clientes. Insira suas credenciais do SFTP. Clique em Testar conexão para verificar se a conexão está configurada corretamente e clique em Avançar. Insira o caminho do arquivo que você quer enviar (em relação ao endereço do host) e clique em Avançar. Vale lembrar que a porta 21 é usada por padrão. Para especificar uma porta diferente, acrescente dois-pontos e o número da porta ao caminho. Por exemplo, sftp://example.com/path/file.csv:2222. Selecione Conexão direta e clique em Continuar. Selecione o tipo de dados e clique em Avançar. Digite o identificador da conta, o nome de usuário e a senha do Snowflake e clique em Conectar. Insira o banco de dados, o esquema e a tabela (ou visualização) do Snowflake que você quer usar e clique em Avançar. Saiba como Formatar seu arquivo de dados de clientes. Selecione o warehouse, o banco de dados e a tabela do MySQL que você quer usar e clique em Avançar. Para mapear campos, selecione os campos da fonte de dados nas listas suspensas que correspondem aos campos de destino e clique em Continuar. Opcional: para usar as transformações, clique em e em Transformar. Clique em Avançar. Insira um nome para a conexão. Opcional: edite os detalhes da conexão. Selecione Finalizar. Digite um nome para o segmento, confirme se ele obedece à política e clique em Salvar e continuar. Fazer upload de um arquivo de dados de clientes As instruções a seguir ensinam como enviar um arquivo de dados de clientes para criar uma nova lista de clientes. Na sua conta do Google Ads, clique no ícone Ferramentas . Clique no menu suspenso Biblioteca compartilhada no menu da seção. Clique em Gerenciador de públicos-alvo. Clique na guia Segmentos dos seus dados na parte de cima da página. Observação: se você escolher "Ativar listas de clientes com base em conversões" nas configurações da conta, as listas de clientes geradas pelo Google vão aparecer em cada meta de conversão específica. Clique no botão de adição para criar um novo segmento. Selecione Lista de clientes no menu suspenso. Escolha um nome para o novo segmento. Faça upload do novo arquivo CSV. Observação: o Google vai identificar se os seus dados foram criptografados com hash ou não. Se você concordar, marque a caixa "Esses dados foram coletados e estão sendo compartilhados com o Google em conformidade com as políticas da Segmentação por Lista de Clientes do Google". Defina a duração da associação. A duração máxima é de 540 dias. Clique em Fazer upload e criar. É possível verificar o progresso do upload do seu arquivo de dados em "Listas de público-alvo". Esse processo pode levar até 48 horas para ser concluído. Depois de enviar seus dados, uma página informando a conclusão do upload do arquivo vai aparecer, com informações sobre o número de linhas que foram enviadas e a porcentagem da taxa de correspondência. Observação importante Duração da associação A duração máxima da associação aos segmentos de público-alvo por lista de clientes é de 540 dias. As associações adicionadas ou atualizadas há mais de 540 dias não estarão mais qualificadas. Para continuar qualificada, uma lista precisa ter pelo menos 100 membros adicionados ou atualizados nos últimos 540 dias. Recomendamos atualizar seus segmentos de público-alvo regularmente. É possível fazer isso de várias maneiras, incluindo a sincronização contínua com CRMs de terceiros ou uploads manuais. Compartilhamento de dados entre contas É possível compartilhar segmentos de público-alvo em várias contas gerenciadas se: Você tiver um segmento de público-alvo por lista de clientes na sua conta de administrador; ou Uma conta de cliente compartilhar o segmento de público-alvo por lista de clientes com sua conta de administrador. Todas as contas que usam um segmento de público-alvo por lista de clientes precisam estar em conformidade com a política de Segmentação por Lista de Clientes. O Google não permite o compartilhamento ou o uso desses dados fora da sua conta gerenciada. Somente proprietários e administradores da conta com acesso de administrador podem adicionar ou remover dados de clientes dos segmentos de público-alvo por lista de clientes. Integração da Segmentação por Lista de Clientes com o Zapier Você pode integrar as fontes de dados do sistema de gestão de relacionamento com o cliente (CRM) à Segmentação por Lista de Clientes do Google usando o Zapier como parceiro de integração. O Zapier faz upload automático dos detalhes de um novo contato. Ele recolhe as informações da ferramenta de CRM, e-commerce ou automação de marketing onde você coleta as informações dos usuários para usar nas listas de clientes do Google Ads. Isso significa que você não precisa fazer o upload manual dos contatos para o Google Ads nem classificar nas listas certas ou remover de uma lista. As listas de clientes enviadas são atualizadas de forma automática e sincronizadas com seu CRM. Como usar a API Google Ads Os proprietários ou administradores da conta também podem usar a API Google Ads para fazer o upload de arquivos de dados e gerenciar os segmentos de público-alvo por lista de clientes. Os anunciantes podem fazer upload de um arquivo de dados, adicionar ou remover informações de clientes ou editar configurações usando a API. Para saber mais, abra a seção de dados da API Google Ads no site do Google Developers. Listas de clientes com base em conversões Você pode ativar as listas de clientes com base em conversões na conta do Google Ads. Para isso, acesse "Configurações da conta" e marque a caixa ao lado de "Ative as listas de clientes com base em conversões". Quando você ativa essas listas, o Google gera segmentos de público-alvo por lista de clientes para cada meta de conversão específica (por exemplo, compras). Essas listas vão ser categorizadas como listas de clientes com base em conversões criadas automaticamente no Gerenciador de públicos-alvo. A medida que novas conversões forem capturadas, essas listas vão ser atualizadas em tempo real como dados com hash fornecidos pelo usuário. Vincular parceiros de Segmentação por Lista de Clientes ao criar uma lista de clientes É possível conectar seus parceiros de Segmentação por lista de clientes ao criar uma lista de clientes. Basta seguir estas instruções. Links relacionados PesquisaLimpar pesquisaFechar pesquisaGoogle AppsMenu principalPesquisar na Central de Ajuda