Ayuda de Websense Manager

Websense® Web Security
Websense Web Filter

v7

Publicado el 2009
Impreso en los Estados Unidos e Irlanda.

Marcas comerciales

Contenido

1 Primeros pasos

El software de Websense permite que los administradores de red de todos los sectores de la industria, desde los negocios y la educación hasta el gobierno, entre otros, controlen o supervisen el tráfico de red a Internet.

- Minimice el tiempo de inactividad de los empleados que acceden a información en Internet que puede ser considerada cuestionable, inapropiada o no relacionada con el trabajo.
- Evite el uso inadecuado de los recursos de la red y la amenaza de acciones legales debido a accesos inapropiados.
- Incorpore un sólido nivel de seguridad en la red, que brinda protección frente a posibles ataques de spyware, malware, hacking y otras intrusiones.

En este documento, puede obtener información sobre los siguientes temas:

La configuración básica de Websense.	**La implementación del filtrado de Internet.**
• *Uso de Websense Manager*, página 17	• *Protocolos y categorías de filtrado*, página 38
• *Suscripción*, página 28	• *Cómo agregar un cliente*, página 68
• *Base de datos principal de Websense*, página 31	• *Cómo trabajar con políticas*, página 75
• *Cómo verificar la configuración de Network Agent*, página 354	• *Cómo asignar una política a clientes*, página 79

También puede aprender a llevar a cabo las siguientes tareas:

Evaluar la configuración.	**Mejorar las políticas de filtrado.**
• *Hoy: Estado, Seguridad y Utilidad desde medianoche*, página 21	• *Cómo crear una categoría personalizada*, página 178
• *Historial: últimos 30 días*, página 24	• *Cómo redefinir el filtrado para sitios específicos*, página 182
• *Informes de presentación*, página 98	• *Cómo restringir usuarios a una lista definida de sitios de Internet*, página 168
• *Informes de investigación*, página 117	• *Cómo filtrar según palabras clave*, página 180

Evaluar la configuración.	Mejorar las políticas de filtrado.
• *Cómo utilizar la Caja de herramientas para comprobar el patrón de filtrado*, página 198	• *Cómo administrar tráfico en función del tipo de archivo*, página 193 • *Cómo utilizar Bandwidth Optimizer para administrar el ancho de banda*, página 191

Visión general

El software de Websense trabaja junto con dispositivos de integración (servidores proxy, firewalls, routers y dispositivos caching) y proporciona las herramientas de configuración y el motor necesarios para desarrollar, supervisar y aplicar políticas de acceso a Internet.

Una serie de componentes de Websense (descritos en *Componentes del producto Websense*, página 272) brindan funcionalidades de filtrado de Internet, identificación de usuarios, alertas, informes y solución de problemas.

Puede obtener una visión general de las nuevas funciones de esta versión de software de Websense en las Notas de la versión, disponible en el Portal de soporte de Websense

Después de la instalación, el software de Websense aplica la política **predeterminada** para supervisar el uso de Internet sin bloquear las solicitudes. Esta política rige el acceso a Internet de todos los clientes de la red hasta que defina sus propias políticas y las asigne a los clientes. Incluso luego de crear configuraciones de filtrado personalizadas, se aplica la política predeterminada siempre que un cliente no esté regido por otra política. Consulte *Política predeterminada*, página 74, para obtener más información.

Los procesos de creación de filtros, incorporación de clientes, definición de políticas y aplicación de políticas a clientes se describen en:

- *Filtros para el uso de Internet*, página 37
- *Clientes*, página 59
- *Políticas de filtrado de Internet*, página 73

Websense Manager, una única herramienta basada en navegador, brinda una interfaz gráfica central para las funciones de informes, administración de políticas y configuración general del software de Websense. Consulte *Uso de Websense Manager*, página 17, para obtener más información.

Puede definir niveles de acceso a Websense Manager para permitir que ciertos administradores gestionen únicamente grupos específicos de clientes o para permitir que personas ejecuten informes sobre su uso de Internet. Consulte *Administración delegada*, página 237, para obtener más información.

Uso de Websense Manager

Temas relacionados:

- *Cómo iniciar sesión en Websense Manager*, página 18
- *Cómo navegar en Websense Manager*, página 19
- *Hoy: Estado, Seguridad y Utilidad desde medianoche*, página 21
- *Historial: últimos 30 días*, página 24

Websense Manager es la interfaz de configuración central que se usa para personalizar el comportamiento del filtrado, supervisar el uso de Internet, generar informes de uso de Internet y administrar la configuración y los valores del software de Websense. Esta herramienta basada en navegador se ejecuta en dos navegadores compatibles.

- Microsoft Internet Explorer7
- Mozilla Firefox 2

Si bien se puede iniciar Websense Manager con otros navegadores, para obtener todas las funcionalidades y la visualización correcta de la aplicación, es conveniente usar los navegadores compatibles.

Para iniciar Websense Manager, lleve a cabo una de las siguientes acciones:

- En equipos Windows:
  - Vaya a **Inicio > Todos los programas > Websense** y, luego, seleccione **Websense Manager**
  - Haga doble clic en el icono de escritorio de Websense Manager.
- Abra un navegador compatible en cualquier equipo de la red y escriba lo siguiente:

  ```
  https://<dirección IP>:9443/mng
  ```

  Reemplace la *<dirección IP>* por la dirección IP del equipo de Websense Manager.

Si no puede conectarse a Websense Manager en el puerto predeterminado, consulte el archivo **tomcat.log** del equipo de Websense Manager (ubicado, en forma predeterminada, en el directorio **C:\Archivos de programa\Websense\tomcat\logs** o **/opt/Websense/tomcat/logs/**) para comprobar el puerto.

Si no puede usar el puerto correcto y sigue sin poder conectarse a Websense Manager desde un equipo remoto, asegúrese de que el firewall permita las comunicaciones con el puerto.

Se usa una conexión SSL para obtener una comunicación con Websense Manager segura basada en navegador. Esta conexión usa un certificado de seguridad emitido por Websense, Inc. Dado que los navegadores compatibles no reconocen a Websense, Inc. como entidad emisora de certificados conocida, se mostrará un error de certificado la primera vez que inicie Websense Manager desde un nuevo navegador. Para no ver este error, puede instalar o aceptar en forma permanente el certificado en el navegador. Consulte los artículos de la Knowledge Base de Websense para obtener más información.

Una vez que se haya aceptado el certificado de seguridad, se muestra la página de inicio de sesión de Websense Manager en la ventana del navegador (consulte *Cómo iniciar sesión en Websense Manager*).

Cómo iniciar sesión en Websense Manager

Temas relacionados:

- *Uso de Websense Manager*
- *Cómo navegar en Websense Manager*, página 19
- *Hoy: Estado, Seguridad y Utilidad desde medianoche*, página 21
- *Historial: últimos 30 días*, página 24

Después de la instalación, el primer usuario queinicia sesión en Websense Manager obtiene acceso administrativo completo. El nombre de usuario es **WebsenseAdministrator**, y no se puede cambiar. La contraseña del WebsenseAdministrator se configura durante la instalación.

Para iniciar sesión, inicie primero Websense Manager (consulte *Uso de Websense Manager*). En la página de inicio de sesión:

1. Seleccione el **Policy Server** que desea administrar.

   Si el entorno cuenta sólo con un Policy Server, éste se selecciona de manera predeterminada.
2. Seleccione un **tipo de cuenta**:
   - Para iniciar sesión con una cuenta de usuario de Websense, como WebsenseAdministrator, haga clic en **Cuenta de Websense** (predeterminada).
   - Para iniciar sesión con las credenciales de red, haga clic en **Cuenta de red**
3. Escriba un **nombre de usuario** y una **contraseña**, y haga clic en**Iniciar sesión**

Ya inició sesión en Websense Manager.

- Si es la primera vez que inicia sesión en Websense Manager, podrá iniciar un tutorial de primeros pasos. Si es la primera vez que usa software de Websense o esta versión del software de Websense, se recomienda que realice el tutorial.
- Si está usando una administración delegada y creó roles administrativos, es posible que se le solicite que seleccione un rol para administrar. Consulte *Administración delegada*, página 237, para obtener más información.

Una sesión de Websense Manager termina 30 min después de la última acción realizada en la interfaz de usuario (acciones como hacer clic para cambiar de página, ingresar información, realizar cambios en la memoria caché o guardar cambios). Se muestra un mensaje de advertencia 5 min antes de que termine la sesión.

- Si hay cambios no guardados en caché en la página o cambios guardados en caché pendientes, se pierden cuando finaliza la sesión. Recuerde hacer clic en **Aceptar** para almacenar en caché y en **Guardar todos** para guardar e implementar los cambios.

- Si Websense Manager está abierto en varias fichas de la misma ventana del navegador, todas las instancias comparten la misma sesión. Si se excede el tiempo de espera de la sesión en una ficha, se excede en todas las fichas.
- Si Websense Manager está abierto en varias ventanas del navegador en el mismo equipo, las instancias comparten la misma sesión **si**:
  - Está usando Microsoft Internet Explorer y usa el método abreviado de teclado Ctrl-N para abrir una nueva instancia de Websense Manager.
  - Si está usando Mozilla Firefox.

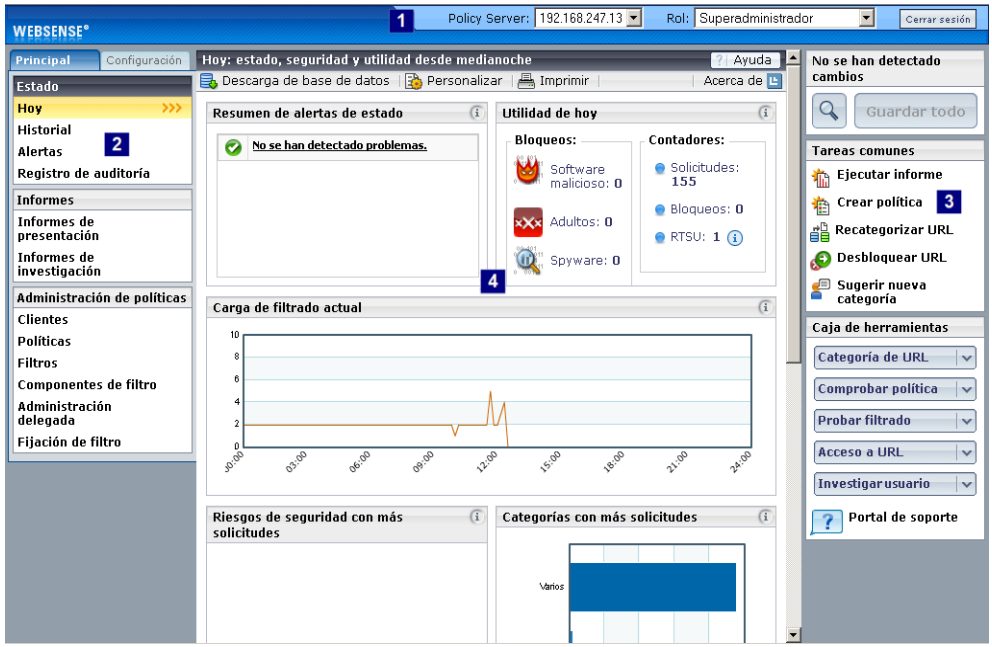
  Si se excede el tiempo de espera de la sesión en una ventana, se excede en todas las ventanas.
- Si inicia varias ventanas de Internet Explorer en forma independiente y las usa para iniciar sesión como diferentes administradores de Websense Manager, las ventanas **no** comparten la sesión. Si se excede el tiempo de espera en una ventana, no se excede en las otras.

Si cierra el navegador sin cerrar la sesión de Websense Manager o si el equipo remoto desde el cual está accediendo a Websense Manager se cierra en forma inesperada, es posible que se bloquee la sesión. El software de Websense detecta el problema en aproximadamente 2 min y finaliza la sesión interrumpida, luego de lo cual podrá volver a iniciar sesión.

Cómo navegar en Websense Manager

La interfaz de Websense Manager se puede dividir en 4 áreas principales:

1. anuncio de Websense
2. Panel de navegación izquierdo
3. Panel derecho de accesos directos
4. Panel de contenido



El **anuncio de Websense** muestra:

- El **Policy Server** en el que inició sesión (consulte *Cómo trabajar con Policy Server*, página 278).
- El **Rol** administrativo actual (consulte *Introducción a los roles administrativos*, página 238).
- Un botón de **cierre de sesión** para cuando desee finalizar la sesión administrativa.

El contenido mostrado en Websense Manager varía según los privilegios conferidos al usuario que inició sesión. A un usuario que sólo tiene privilegios relacionados con informes, por ejemplo, no se le muestra los valores de configuración del servidor o las herramientas de administración de políticas. Consulte *Administración delegada*, página 237, para obtener más información.

Esta sección describe las opciones disponibles para el WebsenseAdministrator y para otros usuarios con privilegios de superadministrador.

El **panel de navegación izquierdo** tiene dos fichas: **Principal** y **Configuración**. En la ficha **Principal**, puede acceder a funciones y características de administración de políticas, informes y estado. En la ficha **Configuración**, puede administrar la cuenta de Websense y realizar tareas globales de administración del sistema.

El **panel derecho de accesos directos** tiene vínculos a herramientas útiles y tareas administrativas comunes. También puede revisar y guardar los cambios hechos en Websense Manager.

- En la zona superior del panel de navegación se indica si hay cambios que deben guardarse en caché. Cuando trabaja en Websense Manager, la barra Cambios indica si hay **Cambios pendientes**

  En la mayoría de los casos, cuando realiza una tarea en Websense Manager y hace clic en **Aceptar**, los cambios se almacenan en caché. (En algunos casos, debe hacer clic en Aceptar en una página subordinada y en una página principal para guardar los cambios en caché).

  Después de guardar los cambios en caché, haga clic en **Guardar todos** para guardar e implementar los cambios. Para visualizar los cambios guardados en caché antes de guardarlos (consulte *Cómo revisar, guardar y descartar cambios*, página 21), haga clic en el botón **Ver cambios pendientes**. Es el botón más pequeño ubicado a la izquierda de Guardar todos.
- **Tareas comunes** proporciona accesos directos a tareas administrativas frecuentes. Haga clic en un elemento de la lista para pasar a la página en la que se realiza la tarea.
- La **Caja de herramientas** contiene herramientas de búsqueda rápida que se pueden usar para comprobar la configuración de filtros. Consulte *Cómo utilizar la Caja de herramientas para comprobar el patrón de filtrado*, página 198, para obtener más información.

Cómo revisar, guardar y descartar cambios

Cuando realiza una tarea en Websense Manager y hace clic en **Aceptar**, los cambios se almacenan en caché. Para revisar los cambios guardados en caché, use la página **Ver cambios pendientes**

> **Importante**
> No haga doble o triple clic en el botón Aceptar. Los clics múltiples y rápidos en el mismo botón pueden ocasionar problemas de visualización en Mozilla Firefox que sólo se pueden solucionar saliendo del navegador y volviendo a abrirlo.

Por lo general, los cambios de un área única de funcionalidades se agrupan en una sola entrada en la lista de caché. Por ejemplo, si agrega 6 clientes y elimina 2, la lista de caché sólo muestra que se realizaron cambios en Clientes. Los cambios en una única página de configuración, en cambio, pueden dar como resultado varias entradas en la lista de caché. Esto ocurre cuando se usa una única página de configuración para configurar varias funciones de software de Websense.

- Para guardar todos los cambios guardados en caché , haga clic en **Guardar todos los cambios**.
- Para abandonar todos los cambios guardados en caché, haga clic en **Cancelar todos los cambios**.

Después de elegir Guardar todos o Cancelar todos, se actualiza la barra Cambios del panel derecho de accesos directos y vuelve a la última página seleccionada. Las funciones Guardar todos o Cancelar todos no se pueden deshacer.

Use el registro de auditoría para revisar los cambios realizados en Websense Manager. Consulte *Visualización y exportación del registro de auditoría*, página 284, para obtener más información.

Hoy: Estado, Seguridad y Utilidad desde medianoche

Temas relacionados:

- *Cómo navegar en Websense Manager*, página 19
- *Historial: últimos 30 días*, página 24
- *Cómo personalizar la página Hoy*, página 24
- *Alertas*, página 287

La página **Estado > Hoy: estado, seguridad y utilidad desde medianoche** aparece por primera vez cuando inicia sesión en Websense Manager. Muestra el estado actual del software de filtrado y brinda gráficos para demostrar la actividad de filtrado de

Internet por hasta 24 h, desde las 12:01 a.m. según la hora del equipo de la base de datos de registro.

En la parte superior de la página, dos secciones de resumen brindan una visión general rápida del estado actual:

- El **Resumen de alertas de estado** muestra el estado del software de Websense. Si aparece un error o una advertencia en el resumen, haga clic en el mensaje de alerta para abrir la página Alertas, donde encontrará información más detallada (consulte *Cómo revisar el estado actual del sistema*, página 294).

  La información del Resumen de alertas de estado se actualiza cada 30 s.
- En **Utilidad de hoy**, puede ver ejemplos sobre la forma en que el filtrado de Websense ha protegido hoy su red, así como la cantidad total de solicitudes de Internet gestionadas y otras cifras totales de actividades importantes.

Bajo la información de resumen, hasta 4 gráficos proporcionan información sobre las actividades de filtrado. Estos gráficos están a disposición de los superadministradores y de los administradores delegados a quienes se les conceden permisos para visualizar informes en la página Hoy. Consulte *Cómo modificar roles*, página 256.

La información en estos gráficos se actualiza cada 2 min. Es posible que deba desplazarse hacia abajo para ver todos los gráficos.

Nombre del gráfico	Descripción
Carga de filtrado actual	Vea la cantidad de tráfico de Internet filtrado procesado en la base de datos de registro que se muestra en intervalos de 10 min.
Riesgos de seguridad con más solicitudes	Conozca las categorías de riesgos de seguridad más solicitadas hoy y determine si las políticas de filtrado están proporcionando la protección adecuada a su red.
Categorías con más solicitudes	Vea las categorías que tienen más accesos hoy. Obtenga información general de alto nivel sobre los posibles problemas de ancho de banda, seguridad o productividad.
Aplicación de políticas por clase de riesgo	Vea cuántas solicitudes se han permitido y bloqueado hoy para cada clase de riesgo (consulte *Clases de riesgo*, página 41). Evalúe si las políticas actuales son eficaces o es necesario realizar cambios.
Principales protocolos por ancho de banda	Conozca los protocolos que están utilizando hoy el mayor ancho de banda de la red. Utilice esta información para valorar sus necesidades de ancho de banda y posibles cambios en las políticas.
Equipos que solicitan sitios con riesgos de seguridad	Conozca los equipos que han accedido hoy a sitios con riesgos de seguridad. Puede revisar estos equipos para asegurarse de que no estén infectados con virus o spyware.

Nombre del gráfico	Descripción
Principales usuarios bloqueados	Conozca qué usuarios han solicitado más sitios bloqueados hoy, para saber en qué grado se están cumpliendo las normas de uso de Internet de la organización.
Principales sitios sin categorizar	Conozca los sitios no categorizados en la base de datos principal de Websense a los que más se ha accedido hoy. Vaya a **Tareas comunes > Recategorizar URL** para asignar un sitio a una categoría para su filtrado.

Haga clic en cualquier gráfico de barras para abrir un informe de investigación con información más detallada.

Aparecen tres botones sobre la página:

- **Descarga de base de datos**, disponible únicamente para los superadministradores, abre una página en la que se puede ver el estado de las descargas de la base de datos principal o iniciar una descarga (consulte *Revisión del estado de descarga de la base de datos principal*, página 283).
- **Personalizar**, disponible únicamente para los superadministradores, abre una página en la que se puede cambiar qué gráficos aparecen en la página (consulte *Cómo personalizar la página Hoy*, página 24).
- **Imprimir**, disponible para todos los administradores, abre una ventana secundaria que contiene una versión que se puede imprimir de los gráficos de la página Hoy. Use las opciones del navegador para imprimir esta página, que no contiene las opciones de navegación de la ventana principal de Websense Manager.

Bajo los gráficos de actividad de Internet y filtrado, el **Resumen de Filtering Service** muestra el estado de cada Filtering Service asociado con el Policy Server actual. Haga clic en la dirección IP de Filtering Service si desea más información sobre esa instancia de Filtering Service.

Por razones de seguridad, las sesiones de Websense Manager finalizan después de 30 min de inactividad. Sin embargo, puede continuar supervisando datos de alertas y filtrado. Para hacerlo, seleccione **Supervisar ininterrumpidamente el estado de Hoy, Historial y Alertas** en la parte inferior de la página Hoy. La información de estas tres páginas se seguirá actualizando normalmente hasta que cierre el navegador o se desplace hasta otra página de Websense Manager.

Importante

Si habilita la opción de supervisión y se queda en las páginas Hoy, Historial y Alertas durante más de 30 min, cuando intente ir a otra página de Websense Manager, volverá a la página de inicio de sesión.

Cuando active esta opción, asegúrese de guardar los cambios guardados en caché antes de que finalice el periodo de tiempo de espera de 30 min.

Cómo personalizar la página Hoy

Temas relacionados:

- *Hoy: Estado, Seguridad y Utilidad desde medianoche*, página 21
- *Cómo personalizar la página Historial*, página 27

Use la página **Hoy > personalizar** para seleccionar hasta 4 gráficos para la página Estado > Hoy. Sólo los superadministradores con permisos de políticas sin restricciones (lo que incluye el WebsenseAdministrator) pueden personalizar la página Hoy.

Los gráficos seleccionados se muestran en la página Hoy a los superadministradores y a los administradores delegados con permisos para visualizarlos. Consulte *Cómo modificar roles*, página 256.

Algunos gráficos muestran información confidencial, como nombres de usuario o direcciones IP. Asegúrese de que los gráficos seleccionados sean adecuados para todos los administradores que puedan visualizarlos.

Para seleccionar los gráficos, seleccione o desactive la casilla de verificación ubicada junto al nombre del gráfico. Cuando haya terminado de seleccionar, haga clic en **Aceptar** para regresar a la página Hoy y ver los gráficos. Para regresar a la página Hoy sin hacer cambios, haga clic en **Cancelar**.

Si desea ver una descripción breve de la información mostrada en cada gráfico, consulte *Hoy: Estado, Seguridad y Utilidad desde medianoche*, página 21

Historial: últimos 30 días

Temas relacionados:

- *Hoy: Estado, Seguridad y Utilidad desde medianoche*, página 21
- *Cómo navegar en Websense Manager*, página 19
- *Cómo personalizar la página Historial*, página 27

La página **Estado > Historial: últimos 30 días** brinda una visión general del comportamiento de filtrado de hasta los últimos 30 días. Los gráficos de esta página se actualizan todos los días a las 12:01 a.m. para agregar datos del día anterior, según la hora del equipo de la base de datos de registro.

El período exacto cubierto por los gráficos y las tablas de resumen depende del tiempo durante el cual el software de Websense ha realizado actividades de filtrado. Durante el primer mes posterior a la instalación del software de Websense, la página muestra

datos de la cantidad de días posteriores a la instalación. Luego, los informes cubren los 30 días anteriores al día actual.

Las **Estimaciones de la utilidad** en la parte superior de la página proporcionan un cálculo estimado del ahorro en tiempo y ancho de banda que permite el software de Websense, además de un resumen de las solicitudes bloqueadas en categorías importantes para muchas organizaciones.

Desplace el ratón sobre **Tiempo** o **Ancho de banda** (en Ahorro) para obtener una explicación de cómo se realizó el cálculo estimado (consulte *Tiempo y ancho de banda ahorrados*, página 26). Puede hacer clic en **Personalizar** para cambiar la forma en que se calculan los valores.

El área **Solicitudes bloqueadas** brinda más información sobre la protección que el software de Websense proporciona a la red, ya que enumera varias categorías importantes para muchas organizaciones y muestra la cantidad total de solicitudes bloqueadas en cada categoría durante el período.

Según los permisos de informes del rol, es posible que los administradores delegados no vean los gráficos descritos a continuación. Consulte *Cómo modificar roles*, página 256.

La página también incluye hasta 4 gráficos con información importante de filtrado. Es posible que deba desplazarse hacia abajo para ver todos los gráficos. La información en estos gráficos se actualiza una vez por día. Haga clic en un gráfico para lanzar un informe de investigación con información más detallada.

Nombre del gráfico	Descripción
Actividad de Internet por solicitudes	Analice la cantidad de solicitudes de Internet filtradas procesadas en la base de datos de registro todos los días.
Riesgos de seguridad con más solicitudes	Conozca a qué categorías de riesgos de seguridad se ha accedido recientemente y determine si las políticas de filtrado están proporcionando la protección correcta para su red.
Categorías con más solicitudes	Vea qué categorías tienen más accesos. Obtenga información general de alto nivel sobre los posibles problemas de ancho de banda, seguridad o productividad.
Principales sitios sin categorizar	Obtenga más información sobre los sitios, no categorizados en la base de datos principal de Websense, a los que más se ha accedido. Vaya a **Tareas comunes > Recategorizar URL** para asignar un sitio a una categoría para su filtrado.
Principales protocolos por ancho de banda	Conozca los protocolos que han estado utilizando recientemente el mayor ancho de banda de la red. Utilice esta información para valorar sus necesidades de ancho de banda y los posibles cambios de política.
Aplicación de políticas por clase de riesgo	Vea cuántas solicitudes se han permitido y bloqueado recientemente para cada clase de riesgo (consulte *Clases de riesgo*, página 41). Evalúe si las políticas actuales son eficaces o es necesario realizar cambios.

Nombre del gráfico	Descripción
Principales usuarios bloqueados	Vea las solicitudes de Internet de los usuarios que más se han bloqueado. Conozca el grado en que se están cumpliendo las normas de uso de Internet de la organización.
Resumen de la aplicación de políticas	Obtenga información general de solicitudes permitidas recientemente, bloqueadas para sitios en la clase de riesgo de seguridad y bloqueadas para otros sitios. Piense qué aspectos del filtrado necesitan una evaluación más detallada.

Aparecen dos botones sobre la página:

- **Personalizar**, disponible únicamente para los superadministradores, abre una página en la que se puede cambiar qué gráficos aparecen en la página y la forma en que se calculan los ahorros estimados (consulte *Cómo personalizar la página Historial*, página 27).
- **Imprimir**, disponible para todos los administradores, abre una ventana secundaria que contiene una versión que se puede imprimir de los gráficos de la página Historial. Use las opciones del navegador para imprimir esta página, que no contiene las opciones de navegación de la ventana principal de Websense Manager.

Tiempo y ancho de banda ahorrados

El filtrado de Websense, además de ofrecer seguridad mejorada, ayuda a minimizar el tiempo y el ancho de banda que se pierden en actividades no productivas de Internet.

El área Guardado de las Estimaciones de la utilidad proporciona un cálculo estimado del ahorro en tiempo y ancho de banda. Estos valores se calculan de la siguiente forma:

- Tiempo ahorrado: se multiplica el **tiempo típico de visita** por los **sitios bloqueados**. Al principio, el software de Websense usa un valor predeterminado para representar la cantidad promedio de segundos que un usuario emplea para ver un sitio Web solicitado. El valor sitios bloqueados representa la cantidad total de solicitudes bloqueadas durante el período cubierto en la página Historial.
- Ancho de banda ahorrado: se multiplica el **ancho de banda típico de visita** por la cantidad de **sitios bloqueados**. Al principio, el software de Websense usa un valor predeterminado para representar la cantidad promedio de bytes que usa un sitio Web promedio. El valor sitios bloqueados representa la cantidad total de solicitudes bloqueadas durante el período cubierto en la página Historial.

Consulte *Cómo personalizar la página Historial*, página 27, para obtener información sobre cómo cambiar los valores usados en los cálculos de forma tal que reflejen el uso en su organización.

Cómo personalizar la página Historial

Temas relacionados:

- *Historial: últimos 30 días*, página 24
- *Cómo personalizar la página Hoy*, página 24

Use la página **Historial > Personalizar** para determinar qué gráficos aparecen en la página Estado > Historial y cómo se calculan los ahorros en tiempo y ancho de banda.

Seleccione la casilla de verificación ubicada junto al nombre de cada gráfico, hasta 4, que desea agregar en la página Historial. Si desea ver una descripción breve de cada gráfico, consulte *Historial: últimos 30 días*, página 24. Sólo los superadministradores con permisos de políticas sin restricciones (lo que incluye el WebsenseAdministrator) pueden personalizar la página Historial.

Algunos gráficos muestran información confidencial, como nombres de usuario. Asegúrese de que los gráficos seleccionados sean adecuados para todos los administradores que puedan visualizarlos.

Tanto los superadministradores como los administradores delegados pueden personalizar la forma en que se calculan los ahorros en tiempo y ancho de banda. Para obtener acceso a estos campos, los administradores delegados deben hacer clic en el vínculo **Personalizar** de la ventana emergente que describe los cálculos del ahorro en tiempo y ancho de banda.

Escriba nuevas mediciones promedio de tiempo y ancho de banda para usar como base de los cálculos:

Opción	Descripción
Promedio de segundos ahorrados por página bloqueada	Escriba la cantidad promedio de segundos que se calcula en la organización que un usuario emplea para ver páginas individuales. El software de Websense multiplica este valor por la cantidad de páginas bloqueadas para determinar los ahorros en tiempo que se muestran en la página Historial.
Promedio de ancho de banda [KB] ahorrado por página bloqueada	Escriba el tamaño promedio, en kilobytes (KB), de las páginas visualizadas. El software de Websense multiplica este valor por la cantidad de páginas bloqueadas para determinar los ahorros en ancho de banda que se muestran en la página Historial.

Cuando haya finalizado de realizar cambios, haga clic en **Aceptar** para volver a la página Historial y ver los nuevos gráficos o las estimaciones de ancho de banda o tiempo. Para regresar a la página Historial sin hacer cambios, haga clic en **Cancelar**.

Suscripción

Las suscripciones de Websense se emiten para cada cliente. Un cliente es un usuario o equipo de la red.

Cuando usted adquiere una suscripción, se envía la clave de suscripción por correo electrónico. Cada clave es válida para una instalación de Websense Policy Server. Si instala varios Policy Servers, necesita una clave para cada uno.

Para poder comenzar a utilizar el servicio de filtrado, debe ingresar una clave de suscripción válida (consulte *Cómo configurar la información de la cuenta*, página 30). De esta forma puede descargar la base de datos principal (consulte *Base de datos principal de Websense*, página 31), que permite al software de Websense filtrar clientes.

Después de la primera descarga correcta de la base de datos, Websense Manager muestra la cantidad de clientes que incluye su suscripción.

El software de Websense mantiene una tabla de suscripción de clientes filtrados cada día. La tabla de suscripción se vacía cada noche. La primera vez que un cliente realiza una solicitud de Internet luego de haberse vaciado la tabla, se ingresa la dirección IP en la tabla.

Cuando la cantidad de clientes que figuran en la tabla alcanza el nivel de suscripción, todo cliente que no haya figurado anteriormente y que solicite acceso a Internet supera el máximo de la suscripción. Si esto ocurre, el cliente que excede el nivel de suscripción recibe un bloqueo completo de Internet o bien obtiene acceso a Internet sin filtrado, según la configuración establecida. Del mismo modo, cuando caduca una suscripción, todos los clientes son bloqueados por completo o no filtrados, según esta configuración.

Para configurar el comportamiento de filtrado que se debe seguir cuando se supera la suscripción, consulte *Cómo configurar la información de la cuenta*, página 30.

Para configurar el software de Websense para que envíe advertencias por correo electrónico cuando la suscripción se aproxima o supera el límite, consulte *Configuración de alertas del sistema*, página 290.

La cantidad de categorías filtradas depende de la suscripción a Websense. El software de Websense filtra todos los sitios de todas las categorías activadas en la compra.

Cómo administrar la cuenta mediante el portal MyWebsense

Websense, Inc. cuenta con un portal para clientes en www.mywebsense.com que puede usar para acceder a actualizaciones de productos, parches, noticias de productos, evaluaciones y recursos de soporte técnico para el software de Websense.

Cuando crea una cuenta, se le solicita que ingrese todas las claves de suscripción de Websense. Esto ayuda a garantizar el acceso a la información, alertas y parches del producto de Websense y la versión.

Una vez que tenga una cuenta de MyWebsense, si no puede iniciar sesión en Websense Manager porque perdió la contraseña de WebsenseAdministrator, sólo deberá hacer clic en **¿Ha olvidado la contraseña?** en la página de inicio de sesión de Websense Manager. Se le solicitará que inicie sesión en MyWebsense y se le darán instrucciones para generar y activar la nueva contraseña.

Importante

Cuando solicita una nueva contraseña, la clave de suscripción seleccionada en el portal MyWebsense debe coincidir con la clave de la página Cuenta de Websense Manager.

Varios miembros de la organización pueden crear inicios de sesión de MyWebsense asociados con la misma clave de suscripción.

Para acceder al portal MyWebsense desde Websense Manager, vaya a **Ayuda > MyWebsense**.

Activación de Websense Web Protection Services™

Las suscripciones a Websense Web Security incluyen acceso a Websense Web Protection Services: SiteWatcher™, BrandWatcher™ y ThreatWatcher™. Una vez activados estos servicios, estos protegen los sitios Web, las marcas y los servidores Web de la organización.

Servicio	Descripción
SiteWatcher	Genera alertas cuando se infectan los sitios Web de la organización con código malicioso, lo que permite actuar en forma inmediata para proteger a clientes, posibles clientes y partners que visitan el sitio.
BrandWatcher	• Genera alertas cuando los sitios Web o las marcas de la organización han sido objeto de ataques de tipo phishing o keylogging malicioso. • Brinda información sobre la seguridad de Internet, los ataques y otros temas de seguridad para que pueda tomar las medidas necesarias, notificar a los clientes y minimizar los efectos sobre la imagen pública de la organización.
ThreatWatcher	• Proporciona una visión del servidor Web de la organización desde el punto de vista de un hacker, busca vulnerabilidades conocidas y posibles amenazas. • Genera informes sobre los niveles de riesgo y proporciona recomendaciones mediante un portal basado en navegador. • Ayuda a prevenir ataques maliciosos al servidor Web.

Inicie sesión en el portal MyWebsense para activar Websense Protection Services. Una vez que ThreatWatcher está activado, inicie sesión en MyWebsense para acceder a informes sobre amenazas para servidores Web registrados.

Cómo configurar la información de la cuenta

Temas relacionados:

- *Suscripción*, página 28
- *Configuración de descargas de la base de datos*, página 33
- *Cómo trabajar con protocolos*, página 185

Use la página **Configuración > Cuenta** para ingresar y visualizar información de suscripción, y cambiar la contraseña de WebsenseAdministrator usada para acceder a Websense Manager. WebsenseAdministrator es la cuenta administrativa principal predeterminada que se usa para Administrar software de Websense.

Aquí también puede activar el software de Websense para que envíe datos de uso de protocolos a Websense, Inc. en forma anónima. Esta información puede usarse para actualizar la base de datos principal de Websense, una recopilación de más de 36 millones de sitios de Internet y más de 100 definiciones de protocolos (consulte *Base de datos principal de Websense*, página 31, para obtener más información).

1. Después de instalar software de Websense o cuando recibe una nueva clave de suscripción, use el campo**Clave de suscripción** para escribir la clave.

   Una vez que ingresa una nueva clave de suscripción y hace clic en Aceptar, comienza a descargarse en forma automática la base de datos principal.
2. Después de la descarga de la base de datos principal, aparece la siguiente información:

La clave caduca	Fecha de finalización de la suscripción actual. Después de esta fecha, debe renovar la suscripción para seguir descargando la base de datos principal y filtrando la red.
Usuarios de red suscritos	Cantidad de usuarios de red que se pueden filtrar.
Usuarios remotos suscritos	Cantidad de usuarios que se pueden filtrar fuera de la red (requiere la función Remote Filtering opcional).

3. Seleccione **Bloquear usuarios cuando la suscripción caduca o se supera** para:
   - Bloquee el acceso a Internet de todos los usuarios cuando caduque la suscripción.
   - Bloquee el acceso a Internet de los usuarios cuando se exceda la cantidad de usuarios suscriptos.

   Si no se selecciona esta opción, los usuarios tienen acceso a Internet sin filtrado en estas situaciones.
4. Para cambiar la contraseña de WebsenseAdministrator, primero introduzca la contraseña actual y, luego, ingrese una nueva contraseña y confírmela.
   - La contraseña debe tener entre 4 y 25 caracteres. Distingue mayúsculas de minúsculas y puede incluir letras, números, caracteres especiales y espacios.

- Se recomienda crear una contraseña segura para la cuenta de WebsenseAdministrator. La contraseña debe tener 8 caracteres como mínimo e incluir al menos una letra mayúscula, letra minúscula, número y carácter especial.

5. Seleccione **Enviar datos de categorías y protocolos a Websense, Inc.** para que el software de Websense recopile datos de uso sobre protocolos y categorías definidas por Websense, y las envíe en forma anónima a Websense, Inc.

   Estos datos de uso ayudan a Websense, Inc. a mejorar en forma continua las funcionalidades de filtrado del software de Websense.

Base de datos principal de Websense

Temas relacionados:

- *Actualizaciones de base de datos en tiempo real*, página 32
- *Real-Time Security Updates™*, página 32
- *Protocolos y categorías de filtrado*, página 38
- *Cómo trabajar con Filtering Service*, página 282
- *Revisión del estado de descarga de la base de datos principal*, página 283
- *Reanudación de descargas de la base de datos principal Master Database*, página 283

La base de datos principal de Websense contiene las definiciones de categorías y protocolos que representan las bases para el filtrado del contenido de Internet (consulte *Protocolos y categorías de filtrado*, página 38).

- **Las categorías** se usan para agrupar sitios Web (identificados por URL y dirección IP) con contenido similar.
- Las definiciones de **protocolos** agrupan protocolos de comunicaciones de Internet con funciones similares, como la transferencia de archivos o el envío de mensajes instantáneos.

Durante la instalación del software de Websense, se instala una versión limitada de la base de datos de filtrado, pero se recomienda descargar la base de datos principal completa lo antes posible para obtener funcionalidades de filtrado de Internet integrales. Para descargar la base de datos principal por primera vez, escriba la clave de suscripción en la página **Configuración > Cuenta** (consulte *Cómo configurar la información de la cuenta*, página 30).

Si el software de Websense debe pasar por un proxy para realizar la descarga, también debe usar la página **Configuración > Descarga de base de datos** para configurar los valores de proxy (consulte *Configuración de descargas de la base de datos*, página 33).

La descarga de la base de datos completa puede tardar tanto unos pocos minutos como más de 60 min, en función de factores como la velocidad de la conexión a Internet, el ancho de banda, la memoria disponible y el espacio disponible en disco.

Después de la descarga inicial, el software de Websense descarga los cambios de la base de datos según una programación establecida por usted (consulte *Configuración de descargas de la base de datos*, página 33). Dado que la base de datos principal se actualiza con frecuencia, en forma predeterminada, las descargas de la base de datos se programan para que se realicen diariamente.

Si la base de datos principal tiene más de 14 días, el software de Websense no filtra las solicitudes de Internet.

Para iniciar una descarga de la base de datos en otro momento o para ver el estado de la descarga, la fecha de la última descarga o el número de versión de la base de datos actual, vaya a **Estado > Hoy** y haga clic en **Descarga de base de datos**.

Actualizaciones de base de datos en tiempo real

Además de las descargas programadas, el software de Websense realiza actualizaciones de emergencia según sea necesario. Por ejemplo, se puede usar una actualización en tiempo real para recategorizar un sitio que se categorizó en forma incorrecta temporalmente. Estas actualizaciones garantizan que los sitios y protocolos se filtren adecuadamente.

El software de Websense comprueba si hay actualizaciones de la base de datos todas las horas.

Las actualizaciones más recientes se enumeran en la página **Estado > Alertas** (consulte *Cómo revisar el estado actual del sistema*, página 294).

Real-Time Security Updates™

Además de recibir lasactualizaciones estándar de la base de datos en tiempo real, los usuarios de Websense Web Security pueden habilitar la función Real-Time Security Updates para recibir actualizaciones relacionadas con la seguridad de la base de datos principal no bien Websense, Inc las publica.

Las actualizaciones de seguridad en tiempo real proporcionan un nivel adicional de protección contra las amenazas a la seguridad basadas en Internet. La instalación de estas actualizaciones no bien se publican reduce la vulnerabilidad de nuevos ataques de phishing (suplantación de identidad), aplicaciones maliciosas y código malicioso que infecten sitios Web o aplicaciones importantes.

Filtering Service comprueba si hay actualizaciones de seguridad cada 5 min, pero, dado que las actualizaciones se envían sólo cuando hay amenazas de seguridad, los cambios reales son esporádicos y, por lo general, no interrumpen la actividad normal de la red.

Use la página **Configuración > Descarga de base de datos** para habilitar Real-Time Security Updates (consulte *Configuración de descargas de la base de datos*, página 33).

Configuración de descargas de la base de datos

Temas relacionados:

- *Cómo configurar la información de la cuenta*, página 30
- *Base de datos principal de Websense*, página 31
- *Revisión del estado de descarga de la base de datos principal*, página 283

Use la página **Configuración > Descarga de base de datos** para programar las descargas automáticas de la base de datos principal. Proporcione también información importante sobre cualquier servidor proxy o firewall a través del que el software de Websense deba pasar para descargar la base de datos.

1. Seleccione los **Días de descarga** de las descargas automáticas.

   Debe descargar la base de datos principal una vez cada 14 días como mínimo para que el software de Websense continúe filtrando sin interrupciones. Si quita la selección de todos los días de descarga, el software de Websense intenta en forma automática realizar la descarga cuando la base de datos tiene 7 días.

   Nota
   Los días de descarga se desactivan cuando se habilita la función Real-Time Security Updates (consulte Paso 3). Las descargas se realizan automáticamente todos los días para garantizar que la base de datos estándar más actualizada esté disponible para las actualizaciones de seguridad.

2. Seleccione la hora de inicio (**De**) y de finalización (**A**) para el **Margen de tiempo para la descarga**. Si no seleccionan los horarios, la descarga de la base de datos se realizará entre las 21 y las 06.

   El software de Websense selecciona una hora en forma aleatoria durante este período para establecer la conexión con el servidor de la base de datos principal. Para configurar alertas en caso de fallas en la descarga, consulte *Configuración de alertas del sistema*, página 290.

   Nota
   Tras descargar la base de datos principal o las actualizaciones, el uso de la CPU puede llegar al 90% mientras se carga la base de datos en la memoria local.

3. (*Websense Web Security*) Seleccione **Activar actualizaciones de seguridad en tiempo real** para que el software de Websense compruebe si hay actualizaciones de seguridad de la base de datos principal cada 5 min. Cuando se detecta una actualización de seguridad, se la descarga inmediatamente.

Las actualizaciones de seguridad en tiempo real protegen la red contra vulnerabilidades de ataques, como phishing (suplantación de identidad), aplicaciones maliciosas y código malicioso que infecten sitios Web o aplicaciones importantes.

4. Seleccione **Usar servidor proxy o firewall** si el software de Websense debe acceder a Internet por medio de un servidor proxy o firewall de proxy (que no sea el producto de integración con el que establece la comunicación el software de Websense) para descargar la base de datos principal. Luego, configure lo siguiente.

Nombre o IP de servidor	Ingrese el nombre o la dirección IP del equipo del servidor proxy o firewall.
Puerto	Escriba el número de puerto a través del cual debe pasar la descarga de la base de datos (el valor predeterminado es 8080).

5. Si el servidor proxy o el firewall configurado en el paso 4 requiere autenticación para acceder a Internet, seleccione **Usar autenticación** y, luego, escriba el **nombre de usuario** y la **contraseña** que debe usar el software de Websense para ello.

> **Nota**
> Si selecciona Usar autenticación, el firewall o servidor proxy deben estar configurados para aceptar texto no cifrado o autenticación básica para que se habilite la descarga de la base de datos principal.

De forma predeterminada, se cifran el nombre de usuario y la contraseña de forma tal que coincidan con el conjunto de caracteres de la configuración regional del equipo de Policy Server. El cifrado se puede configurar en forma manual mediante la página **Configuración > Servicios de directorio** (consulte *Configuración de directorio avanzada*, página 65).

Pruebas de la configuración de red

A fin de que se realice el filtrado de solicitudes de Internet, el software de Websense debe controlar el tráfico de Internet desde los equipos de su red y hacia ellos. Utilice el detector de tráfico de la red para asegurarse de que la comunicación con Internet sea visible para el software de filtrado. Consulte *Cómo verificar la configuración de Network Agent*, página 354, para obtener instrucciones.

Si el detector de tráfico no puede ver todos los segmentos de la red, consulte *Configuración de redes*, página 345, para obtener instrucciones sobre la configuración.

Soporte técnico de Websense

Websense, Inc. mantiene su compromiso de satisfacción con el cliente. Visite el sitio Web de Soporte técnico de Websense en cualquier momento para obtener información sobre el release más reciente, leer artículos de Knowledge Base o documentación de productos, o bien para crear una solicitud de soporte.

www.websense.com/SupportPortal/

El tiempo de respuesta de las solicitudes en línea en horario comercial es de aproximadamente 4 h. Las respuestas a solicitudes fuera del horario comercial se realizan al siguiente día hábil.

También se brinda asistencia telefónica. Para obtener atención rápida y eficaz a las solicitudes telefónicas, tenga la siguiente información a mano:

- Clave de suscripción de Websense.
- Acceso a Websense Manager.
- Acceso a los equipos que ejecutan Filtering Service y Log Server, y al servidor de base de datos (Microsoft SQL Server o MSDE).
- Permiso para acceder a la base de datos de registro de Websense.
- Conocimiento de la arquitectura de red o acceso a un especialista.
- Especificaciones de los equipos que ejecutan Filtering Service y Websense Manager.
- Una lista de las otras aplicaciones que se ejecutan en el equipo de Filtering Service.

Es posible que se necesite información adicional para los problemas graves.

Se brinda asistencia telefónica estándar durante el horario comercial de lunes a viernes en los siguientes números:

- San Diego, California, EE.UU: **+1 858.458.2940**
- Londres, Inglaterra: **+44 (0) 1932 796244**

Consulte los sitios Web de soporte enumerados anteriormente para obtener información sobre el horario de funcionamiento y otras opciones de soporte.

Los clientes de Japón deben contactarse con el distribuidor del servicio más rápido.

2 Filtros para el uso de Internet

Temas relacionados:

- *Protocolos y categorías de filtrado*, página 38
- *Cómo trabajar con filtros*, página 48
- *Cómo configurar los valores de filtrado de Websense*, página 56
- *Políticas de filtrado de Internet*, página 73
- *Refinar políticas de filtrado*, página 167

Las políticas rigen el acceso de los usuarios a Internet. Una política es un programa que informa al software de Websense cómo y cuándo filtrar el acceso a sitios Web y aplicaciones de Internet. En su aspecto más simple, las políticas consisten de:

- **Filtros de categorías**, utilizados para aplicar acciones (permitir, bloquear) a categorías de sitios Web.
- **Filtros de protocolos**, utilizados para aplicar acciones a aplicaciones de Internet y protocolos no HTTP.
- Un cronograma que determina cuándo se aplica cada filtro.

El filtrado basado en políticas permite la asignación de distintos niveles de acceso Internet a clientes (usuarios, grupos y equipos de la red). Primero, cree filtros para definir restricciones precisas de acceso a Internet y luego use los filtros para crear una política.

Durante una primera instalación, el software de Websense crea una política **predeterminada** y la utiliza para comenzar con el monitoreo de solicitudes de Internet apenas se ingresa una clave de suscripción (consulte *Política predeterminada*, página 74). En principio, la política predeterminada permite todas las solicitudes.

Nota

Cuando se realiza una actualización desde una versión anterior del software de Websense, se mantiene la configuración de las políticas existentes. Después de la actualización, revise las políticas para asegurarse de que aún sean adecuadas.

Para aplicar diferentes restricciones de filtrado a diferentes clientes, defina los filtros de categorías. Puede definir:

- Un filtro de categorías que bloquee el acceso a todos los sitios Web, excepto los sitios de las categorías Economía y Negocios, Educación, y Noticias y medios.
- Un segundo filtro de categorías que permita el acceso a todos los sitios Web, excepto aquellos que impliquen un riesgo de seguridad y aquellos que contengan material para adultos.
- Un tercer filtro de categorías que monitoree el acceso a sitios Web sin bloquearlos (consulte *Cómo crear un filtro de categorías*, página 49).

Para añadir a estos filtros de categorías, es posible definir:

- Un filtro de protocolos que bloquee el acceso al chat y la mensajería instantánea, el intercambio de archivos P2P, la elusión con proxy y los grupos de protocolos de transmisiones multimedia.
- Un segundo filtro de protocolos que permita el acceso a todos los protocolos no HTTP, excepto aquellos asociados con la elusión con proxy.
- Un tercer filtro de protocolos que permita el acceso a todos los protocolos no HTTP (consulte *Cómo crear un filtro de protocolos*, página 52).

Una vez que se haya definido un conjunto de filtros que se ajusten a las reglamentaciones de su organización respecto del acceso a Internet, podrá agregar esos filtros a las políticas y aplicarlos a los clientes (consulte *Políticas de filtrado de Internet*, página 73).

Protocolos y categorías de filtrado

La Base de datos principal de Websense agrupa sitios Web similares (identificados por medio de direcciones IP y URL) en **categorías**. Cada categoría cuenta con un nombre descriptivo, como material para adultos, juegos de apuestas o intercambio de archivos P2P. También es posible crear categorías propias personalizadas para agrupar sitios de interés de la organización (consulte *Cómo crear una categoría personalizada*, página 178). Las categorías de la base de datos principal y las categorías definidas por el usuario forman, de manera conjunta, la base del filtrado de Internet.

Websense, Inc. no emite juicios de valor sobre las categorías o los sitios de la base de datos principal. Las categorías están designadas para crear agrupamientos útiles de los sitios de interés de los clientes suscritos. No tienen por objeto caracterizar ningún sitio o grupo de sitios ni las personas o intereses que los publican, y no deben ser interpretados de esa forma. Asimismo, las etiquetas de las categorías de Websense son abreviaturas prácticas y no tienen por objeto transmitir ninguna opinión o actitud, de aprobación o de otro tipo, respecto del tema o los sitios clasificados; ni deben ser interpretadas de tal modo.

La lista actualizada de categorías de la base de datos principal está disponible en:

www.websense.com/global/en/ProductsServices/MasterDatabase/URLCategories.php

Para sugerir la adición de un sitio a la base de datos principal, haga clic en **Sugerir nueva categoría**, en el panel derecho de accesos directos de Websense Manager; o bien, visite:

www.websense.com/SupportPortal/SiteLookup.aspx

Después de iniciar sesión en el portal MyWebsense, ingresará a la herramienta Site Lookup and Category Suggestion (Búsqueda de sitios y Sugerencia de categoría).

Cuando se crea un **filtro de categorías** en Websense Manager, se seleccionan las categorías permitidas y las bloqueadas.

Además de incluir las categorías de URL, la base de datos de Websense incluye grupos de protocolos utilizados para administrar el tráfico de Internet no HTTP. Cada grupo de protocolos define tipos similares de protocolos de Internet (como FTP o IRC) y aplicaciones (como AOL Instant Messenger o BitTorrent). Las definiciones se verifican y actualizan todos los días.

Al igual que con las categorías, es posible definir protocolos personalizados para su uso en el filtrado de Internet.

La lista actualizada de protocolos de la base de datos principal está disponible en:

www.websense.com/global/en/ProductsServices/MasterDatabase/ProtocolCategories.php

When you create a **protocol filter**, you choose which protocols to block and which to permit.Cuando se crea un **filtro de protocolos**, se seleccionan los protocolos permitidos y los bloqueados.

> **Nota**
> Network Agent se debe instalar para activar el filtrado basado en protocolos.

Algunos protocolos definidos por Websense permiten bloquear el tráfico saliente de Internet destinado a un servidor externo, como un servidor de mensajería instantánea específico. Solo los protocolos definidos por Websense con números de puertos asignados dinámicamente pueden bloquearse como tráfico saliente.

Nuevas categorías y protocolos

Cuando se agregan categorías y protocolos nuevos a la base de datos principal, a cada uno se le asigna una acción de filtrado predeterminada, como **Permitir** o **Bloquear** (consulte *Acciones de filtrado*, página 44).

- La acción predeterminada se aplica a todos los filtros de protocolos y las categorías activos (consulte *Cómo trabajar con filtros*, página 48). Modifique los filtros activos para cambiar la forma en que se filtran la categoría o el protocolo.
- La acción predeterminada se basa en la información sobre si los sitios o los protocolos en cuestión se consideran adecuados para el negocio o no.

Puede configurar el software de Websense para que genere un sistema de alertas y le avise cada vez que se agregan categorías o protocolos nuevos a la base de datos principal. Consulte *Alertas*, página 287, para obtener más información.

Categorías especiales

La base de datos principal contiene categorías especiales para que lo ayuden a administrar tipos específicos de uso de Internet. Las siguientes categorías están disponibles en todas las ediciones del software de Websense.

- La categoría **Eventos especiales** se usa para clasificar sitios considerados temas de actualidad para ayudarlo a administrar los surgimientos relacionados con eventos del tráfico de Internet. Por ejemplo, es posible que el sitio oficial del campeonato del mundo aparezca, por lo general, en la categoría Deportes, pero que se mueva a la categoría Eventos especiales durante la final del campeonato del mundo.

  Las actualizaciones a la categoría Eventos especiales se agregan a la base de datos principal durante descargas programadas. Los sitios se agregan a esta categoría por un período breve, después del cual se mueven a otra categoría o se eliminan de la base de datos principal.
- La categoría **Productividad** se centra en la prevención de la pérdida de tiempo.
  - Publicidad
  - Descarga de programas (freeware y software)
  - Mensaje instantáneo
  - Corretaje de acciones en línea
  - Pagar por navegar
- La categoría **Ancho de banda** se centra en el ahorro de ancho de banda.
  - Radio y televisión vía Internet
  - Telefonía vía Internet
  - Compartir archivos P2P
  - Almacenamiento personal en la red, respaldo de seguridad
  - Transmisiones multimedia

Websense Web Security incluye categorías de seguridad adicionales:

- **Filtrado de seguridad de Websense** (también conocido como **Seguridad**) abarca los sitios de Internet que contienen códigos maliciosos que pueden eludir programas de software de detección de virus. Los sitios de esta categoría están bloqueados de forma predeterminada.
  - Redes de zombies
  - Keyloggers
  - Sitios Web maliciosos
  - Phishing y otros fraudes
  - Software potencialmente no deseado

- Programas espía

- **Protección extendida** se centra en sitios Web potencialmente maliciosos. Los sitios de las subcategorías Exposición elevada y Vulnerabilidad de seguridad emergente están bloqueados de forma predeterminada.
  - **Exposición elevada** contiene sitios que ocultan su verdadera naturaleza o identidad o que incluyen elementos que sugieren una intención maliciosa latente.
  - **Vulnerabilidad de seguridad emergente** contiene sitios con host conocido y código de vulnerabilidad de seguridad potencial.
  - **Contenido potencialmente peligroso** incluye sitios que pueden contener poco o ningún contenido útil.

El grupo Protección extendida filtra los sitios Web potencialmente maliciosos según la *reputación*. La reputación del sitio se basa en signos tempranos de actividad maliciosa potencial. Un atacante puede tomar como destino una URL que contenga un error ortográfico común o que sea similar a una URL legítima. Tal sitio se puede usar para distribuir malware a usuarios antes de que se puedan actualizar filtros tradicionales para reflejar estos sitios como maliciosos.

Cuando la investigación de seguridad de Websense detecta una amenaza potencial, se agrega a la categoría Protección extendida hasta que Websense esté 100% seguro de la categorización final del sitio.

Clases de riesgo

Temas relacionados:

- *Asignación de categorías a las clases de riesgo*, página 308
- *Informes de presentación*, página 98
- *Informes de investigación*, página 117

La base de datos principal de Websense agrupa las categorías en **clases de riesgo**. Las clases de riesgo sugieren tipos o niveles posibles de vulnerabilidad que presentan sitios del grupo de categorías.

Las clases de riesgo se usan, principalmente, en los informes. Las páginas Hoy e Historial incluyen gráficos en los que la actividad de Internet se muestra por clase de riesgo, y se pueden crear presentaciones o informes de investigación según la clase de riesgo.

Las clases de riesgo también pueden ser útiles para crear filtros de categorías. En principio, por ejemplo, el filtro de categorías de Seguridad básica bloquea todas las categorías predeterminadas de la clase Riesgo de seguridad. Es posible usar las agrupaciones de clase de riesgo como una guía cuando crea sus propios filtros de categorías para que sea más fácil decidir si se debe permitir, bloquear o restringir una categoría de alguna forma.

El software de Websense incluye 5 clases de riesgo, enumeradas a continuación. De forma predeterminada, el software de Websense agrupa las siguientes categorías en cada clase de riesgo.

- Una categoría puede aparecer en varias clases de riesgo o no se puede asignar a ninguna clase de riesgo.
- Es posible que las agrupaciones cambien periódicamente en la base de datos principal.

Responsabilidad legal

Material para adultos (incluidos contenido para adultos, lencería y trajes de baño, desnudez y sexo)

Ancho de banda > Compartir archivos P2P

Juegos de apuestas

Ilegal o cuestionable

Tecnología de la información > Hackers y elusión con proxy

Militancia/Extremistas

Racismo/Odio

Mal gusto

Violencia

Armas

Pérdida de ancho de banda de red

Ancho de banda (incluidos Radio y televisión via Internet, Telefonía vía Internet, Compartir archivos P2P, Almacenamiento personal en la red y Respaldo de seguridad, y Transmisiones multimedia)

Entretenimiento > Servicios de descarga de audio y MP3

Productividad > Publicidad y freeware *y* Descarga de programas

Uso relacionado con el trabajo

Comercio y economía (incluido Servicios y datos financieros)

Educación > Materiales educativos *y* Materiales de referencia

Gobierno (incluido Militar)

Tecnología de la información (incluidos Seguridad de computadoras, Portales y motores de búsqueda y Sitios de traducción de URL).

Viajes

Vehículos

Riesgo de seguridad

Ancho de banda > Compartir archivos P2P

Protección extendida (incluidos Exposición elevada, Vulnerabilidad de seguridad emergente y Contenido potencialmente peligroso) [*Websense Web Security*]

Tecnología de la información > Hackers *y* elusión con proxy

Riesgo de seguridad

Productividad > Descarga de programas (freeware y software)

Seguridad (incluidos Redes de zombies, Keyloggers, Sitios Web maliciosos, Phishing y otros fraudes, Software potencialmente no deseado y Programas espía)

Pérdida de productividad

Aborto (incluidos Pro elección) *y* Pro vida)

Material para adultos > Educación sexual

Grupos de apoyo

Ancho de banda > Radio y televisión vía Internet, Compartir archivos P2P y Transmisiones multimedia

Drogas (incluidos Abuso de drogas, Marihuana, Medicamentos recetados y Suplementos y Compuestos no regulados)

Educación (incluidos Instituciones culturales *e* Instituciones educativas)

Entretenimiento (incluidos Servicios de descarga de audio y MP3)

Juegos de apuestas

Juegos

Gobierno > Organizaciones políticas

Salud

Tecnología de la información > Host Web

Comunicación de Internet (incluidos Correo electrónico general, Correo electrónico organizativo, Mensajería de texto y multimedia y Chat Web)

Búsqueda de empleo

Noticias y medios (incluidos Diarios alternativos)

Productividad (incluidos Descarga de programas (freeware y software), Mensajería instantánea, Paneles de mensajes y foros, Corretaje de acciones en línea y Pagar por navegar)

Religión (incluidos Religiones no tradicionales y ciencias ocultas y folclore *y* Religiones tradicionales)

Compras (incluidos Subastas por Internet *y* Bienes raíces)

Organizaciones sociales (incluidos Organizaciones de trabajo y profesionales, Organizaciones filantrópicas y de servicio, y Organizaciones de afiliación y sociales)

Sociedad y estilos de vida (incluidos Alcohol y tabaco, Interés homosexual o bisexual, Pasatiempos, Personales y citas, Restaurantes y alimentación, y Redes sociales y Sitios personales)

Eventos especiales

Deportes (incluidos Caza deportiva y Clubes de tiro)

Viajes

Vehículos

Los superadministradores pueden cambiar las categorías asignadas a cada clase de riesgo en la página **Configuración > Clase de riesgo** (consulte *Asignación de categorías a las clases de riesgo*, página 308).

Grupos de protocolos de seguridad

Además de las categorías Seguridad y Protección extendida, Websense Web Security incluye dos protocolos que tienen el objetivo de ayudar a proteger y detectar códigos o contenido maliciosos y spyware o contenido transmitido por Internet.

- El grupo de protocolos **Tráfico malicioso** incluye el protocolo **Redes de zombies**, que tiene el objetivo de bloquear el tráfico de comando y control generado por un intento de bot de conectarse con una red de zombies con objetivos maliciosos.
- El grupo de protocolos **Tráfico malicioso - Sólo supervisar** se usa para identificar tráfico que puede estar relacionado con software malicioso.
  - Los **Gusanos procedentes de correo electrónico** realizan un seguimiento del tráfico SMTP saliente que puede estar generado por un ataque de gusanos basado en correo electrónico.
  - **Otro tráfico malicioso** realiza un seguimiento del tráfico entrante y saliente sospechoso de tener una conexión con aplicaciones maliciosas.

El grupo de protocolos Tráfico malicioso está bloqueado de forma predeterminada y se puede configurar dentro de los filtros de protocolos (consulte *Cómo modificar un filtro de protocolos*, página 52). Los protocolos Tráfico malicioso - Sólo supervisar se pueden registrar para generar informes, pero no se puede aplicar otra acción de filtrado.

Instant Messaging Attachment Manager

Instant Messaging (IM) Attachment Manager es una característica opcional. Si se suscribe a esta característica, puede restringir el intercambio de archivos con clientes de MI, como AOL/ICQ, Microsoft (MSN) y Yahoo. Esto hace posible permitir tráfico de MI y, al mismo tiempo, bloquear la transferencia de adjuntos entre clientes de MI.

Archivos adjuntos de mensajería instantánea es un grupo de protocolos que incluye definiciones para varios clientes de MI. Cuando se activa IM Attachment Manager, estos protocolos aparecen en la lista de protocolos de todos los filtros de protocolos y en la página Administrar protocolos.

El filtrado de adjuntos de MI se puede aplicar tanto al tráfico interno como al externo. Para activar el filtrado de tráfico interno, defina la parte de la red que desea supervisar en la página **Configuración > Network Agent > Configuración global** (consulte *Cómo establecer la configuración global*, página 348).

Acciones de filtrado

Los filtros de categorías y protocolo asignan una **acción** a cada categoría o protocolo. Esta es la acción que el software de filtrado de Websense realiza en respuesta a la solicitud de Internet de un cliente. Las acciones que se aplican tanto a las categorías como a los protocolos son:

- **Bloquear** la solicitud. Los usuarios reciben una página o un mensaje de bloqueo y no pueden ver el sitio ni usar la aplicación de Internet.
- **Permitir** la solicitud. Los usuarios pueden ver y usar la aplicación de Internet.
- Evaluar el uso de **ancho de banda actual** antes de bloquear o permitir la solicitud. Cuando esta acción está activada y el uso de ancho de banda alcanza un umbral específico, se bloquean las solicitudes de Internet de un protocolo o una categoría específicos. Consulte *Cómo utilizar Bandwidth Optimizer para administrar el ancho de banda*, página 191.

Se pueden aplicar acciones adicionales sólo a categorías.

> **Nota**
>
> Las opciones Confirmar y Cuota no se deben usar cuando varios Policy Server administran clientes individuales (usuarios, grupos y equipos).
>
> La información de cronometraje relacionada con estas características no se comparte entre los Policy Server, y a los clientes afectados se les permite tener más o menos acceso a Internet que el que planeado

- **Confirmar**: los usuarios reciben una página de bloqueo que les pide que confirmen si se está teniendo acceso al sitio con fines comerciales. Si el usuario hace clic en **Continuar**, podrá ver el sitio.

  Al hacer clic en Continuar se inicia un temporizador. Durante el período de tiempo configurado (60 segundos en forma predeterminada), el usuario puede visitar otros sitios en las categorías Confirmar sin recibir ninguna otra página de bloqueo. Una vez que finaliza el período, al visitar cualquier otro sitio Confirmar se muestra una página de bloqueo.

  El tiempo predeterminado se puede cambiar en la página **Configuración > Filtrado**.
- **Cuota**: los usuarios reciben una página de bloqueo que les pregunta si desean usar tiempo de cuota para ver el sitio. Si un usuario hace clic en **Utilizar tiempo de cuota**, podrá ver el sitio.

  Al hacer clic en Utilizar tiempo de cuota se inician dos temporizadores: un temporizador de sesión de cuota y un temporizador de asignación de cuota total.

  - Si el usuario solicita sitios de cuota adicionales durante un período de **sesión** predeterminado (10 minutos), puede visitar esos sitios sin recibir otra página de bloqueo.
  - El tiempo de cuota **total** se asigna diariamente. Una vez agotado, cada cliente debe esperar hasta el día siguiente para acceder a sitios de categorías por cuota. La asignación de cuota diaria predeterminada (60 minutos) se configura en la página **Configuración > Filtrado**. También se pueden asignar cuotas diarias a los clientes individualmente. Consulte *Cómo usar tiempo de cuota para limitar el acceso a Internet*, página 46, para obtener más información.

- **Bloquear palabra clave**: cuando define palabras clave y activa el bloqueo de palabras clave, los usuarios que solicitan un sitio cuya URL contiene una palabra clave bloqueada no pueden tener acceso al sitio. Consulte *Cómo filtrar según palabras clave*, página 180.
- **Bloquear tipos de archivo**: cuando se activa el bloqueo de tipos de archivo, los usuarios que intentan descargar un archivo cuyo tipo esté bloqueado reciben una página de bloqueo y no pueden descargar el archivo. Consulte *Cómo administrar tráfico en función del tipo de archivo*, página 193.

Cómo usar tiempo de cuota para limitar el acceso a Internet

Cuando un usuario hace clic en Utilizar tiempo de cuota, puede ver sitios de cualquier categoría de cuota hasta que finaliza la sesión de cuota. El tiempo de sesión de cuota predeterminado (configurado mediante la página **Configuración > Filtrado**) es 10 minutos.

> **Nota**
>
> La opción Cuota no se debe usar cuando varios Policy Server administren clientes individuales.
>
> La información de cronometraje relacionada con esta característica no se comparte entre los Policy Server, y a los clientes afectados se les permite tener más o menos acceso a Internet que el que planeado

Una vez que finaliza la sesión de cuota, una solicitud de un sitio de cuota da como resultado otro mensaje de bloqueo de cuota. Los usuarios que no agiten su asignación de tiempo de cuota diario pueden iniciar una nueva sesión de cuota.

Una vez que se configura el tiempo de cuota, el software de Websense usa una lista de prioridad para determinar cómo responder cuando un usuario solicita un sitio de una categoría de cuota. El software busca tiempo de cuota configurado para:

1. El usuario
2. La red o el equipo cliente
3. Grupos a los que pertenece el usuario

   Si un usuario es miembro de varios grupos, el software de Websense permite tiempo de cuota según la configuración de **Usar bloqueo más restrictivo** de la página **Configuración > Filtrado** (consulte *Cómo configurar los valores de filtrado de Websense*, página 56).
4. Tiempo de cuota predeterminado

Es posible que los applets de Internet, como applets de Java o Flash, no respondan como se esperaba a las restricciones de tiempo de cuota. Aunque se tenga acceso desde un sitio con cuota restringida, un applet que se ejecuta dentro del navegador puede seguir ejecutándose más allá del tiempo de sesión de cuota configurado.

Esto es porque los applets se descargan completamente a un equipo cliente y se ejecutan como aplicaciones, sin volverse a comunicar con el servidor host original.

Sin embargo, si el usuario hace clic en el botón Actualizar del navegador, el software de Websense detecta la comunicación con el servidor host y, a continuación, bloquea la solicitud según las restricciones de cuota aplicables.

Acceso con contraseña

Acceso con contraseña permite que los usuarios con contraseñas válidas tengan acceso a sitios bloqueados por el software de Websense. Se puede permitir el acceso con contraseña a clientes individuales (usuarios, grupos, equipos o redes).

Cuando se activa la opción de acceso con contraseña, los mensajes de bloqueo de Websense incluyen un campo de contraseña. Los clientes que escriben una contraseña válida pueden tener acceso a los sitios bloqueados por una cantidad limitada de tiempo.

> **Nota**
> La opción Acceso con contraseña no se debe usar cuando varios Policy Server administren clientes individuales.
>
> La información de cronometraje relacionada con esta característica no se comparte entre los Policy Server, y a los clientes afectados se les permite tener más o menos acceso a Internet que el que planeado

La opción de acceso con contraseña se activa mediante la página **Configuración > Filtrado** (consulte *Cómo configurar los valores de filtrado de Websense*, página 56).

Puede otorgar privilegios de acceso con contraseña a ciertos clientes mediante la página **Administración de políticas > Clientes** (consulte *Cómo agregar un cliente*, página 68, o *Cómo cambiar la configuración de clientes*, página 70).

Filtrado de búsqueda

Filtrado de búsqueda es una característica de algunos motores de búsqueda que ayuda a limitar la cantidad de resultados de búsqueda inadecuados que se muestran a los usuarios.

Por lo general, los resultados de motores de búsqueda de Internet pueden incluir imágenes en miniatura asociadas con sitios que coinciden con los criterios de búsqueda. Si esas imágenes en miniatura están relacionadas con sitios bloqueados, el software de Websense evita que los usuarios tengan acceso al sitio completo, pero no evita que el motor de búsqueda muestre la imagen.

Cuando activa el Filtrado de búsqueda, el software de Websense activa una característica de motor de búsqueda que evita que se muestren las imágenes en miniatura relacionadas con sitios bloqueados en los resultados de búsqueda. Tanto los clientes de filtrado remotos como los locales resultan afectados cuando se activa el Filtrado de búsqueda.

Websense, Inc. mantiene una base de datos de motores de búsqueda con capacidades de Filtrado de búsqueda. Cuando se agrega o se elimina un motor de búsqueda de la base de datos, se genera una alerta (consulte *Alertas*, página 287).

El Filtrado de búsqueda se activa mediante la página **Configuración > Filtrado**. Consulte *Cómo configurar los valores de filtrado de Websense*, página 56, para obtener más información.

Cómo trabajar con filtros

Temas relacionados:

- *Protocolos y categorías de filtrado*, página 38
- *Políticas de filtrado de Internet*, página 73
- *Cómo crear un filtro de categorías*, página 49
- *Cómo crear un filtro de protocolos*, página 52
- *Cómo crear un filtro de acceso limitado*, página 170

Use la página **Administración de políticas > Filtros** de Websense Manager para ver, crear y modificar filtros de protocolos y categoría, y para trabajar con otras herramientas de filtrado.

La página Filtros se divide en 3 secciones principales:

- **Filtros de categoría** determina qué categorías bloquear y permitir.
- **Filtros de protocolo** determina qué protocolos no HTTP bloquear y permitir.

  Network Agent se debe instalar para activar el filtrado basado en protocolos.
- **Filtros de acceso limitado** define una lista restrictiva de sitios Web permitidos (consulte *Cómo restringir usuarios a una lista definida de sitios de Internet*, página 168).

Los filtros de categorías, protocolo y acceso limitado forman los bloques constituyentes de **políticas**. Cada política se compone de al menos un filtro de categorías o acceso limitado y un filtro de protocolos aplicado a los clientes seleccionados en una programación específica.

- Para revisar o modificar un filtro de categorías, protocolos o acceso limitado, haga clic en el nombre del filtro. Para obtener más información, consulte:
  - *Cómo modificar un filtro de categorías*, página 50
  - *Cómo modificar un filtro de protocolos*, página 52
  - *Cómo modificar un filtro de acceso limitado*, página 170
- Para crear un nuevo filtro de categorías, protocolos o acceso limitado, haga clic en **Agregar**. Para obtener más información, consulte:
  - *Cómo crear un filtro de categorías*, página 49

- *Cómo crear un filtro de protocolos*, página 52
- *Cómo crear un filtro de acceso limitado*, página 170

Para duplicar un filtro existente, marque la casilla de verificación ubicada junto al nombre del filtro y, a continuación, haga clic en **Copiar**. A la copia se le da el nombre del filtro original con un número anexado exclusivo y, a continuación, se agrega a la lista de filtros. Modifique la copia como lo haría con cualquier otro filtro.

Si creó roles de administración delegados (consulte *Administración delegada*, página 237), los superadministradores pueden copiar filtros que hayan creado para otros roles para que los usen los administradores delegados.

Para copiar filtros a otro rol, primero marque la casilla de verificación ubicada junto al nombre del filtro y, a continuación, haga clic en **Copiar a rol**. Consulte *Cómo copiar filtros y políticas a roles*, página 173, para obtener más información.

Cómo crear un filtro de categorías

Temas relacionados:

- *Cómo trabajar con filtros*, página 48
- *Cómo modificar un filtro de categorías*, página 50

Use la página **Administración de políticas > Filtros > Agregar filtro de categorías** para crear un nuevo filtro de categorías. Puede trabajar desde una plantilla predefinida o hacer una copia de un filtro de categorías existente para usar como base del nuevo filtro.

1. Especifique un **Nombre de filtro** único. El nombre debe tener entre 1 y 50 caracteres y no puede incluir ninguno de los siguientes:

   ```
   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

   Los nombres de filtro pueden incluir espacios, guiones y apóstrofes.
2. Escriba una breve **Descripción** del filtro. Esta descripción aparece junto al nombre de filtro en la sección Filtros de categorías de la página Filtros, y debe explicar el fin del filtro.

   Las restricciones de caracteres que se aplican a nombres de filtro también se aplican a las descripciones, con 2 excepciones: las descripciones pueden incluir puntos (.) y comas (,).
3. Seleccione una entrada de la lista desplegable para determinar si usar una plantilla o hacer una copia de un filtro existente. Para obtener más información sobre plantillas, consulte *Plantillas de filtros de protocolos y categorías*, página 55.
4. Para ver y modificar el nuevo filtro, haga clic en **Aceptar**. El filtro se agrega a la lista **Filtros de categorías** de la página Filtros.

Para personalizar el filtro, haga clic en el nombre del filtro y continúe con *Cómo modificar un filtro de categorías*.

Cómo modificar un filtro de categorías

Temas relacionados:

- *Protocolos y categorías de filtrado*, página 38
- *Acciones de filtrado*, página 44
- *Cómo usar tiempo de cuota para limitar el acceso a Internet*, página 46
- *Acceso con contraseña*, página 47
- *Cómo trabajar con filtros*, página 48
- *Cómo trabajar con categorías*, página 175

Use la página **Administración de políticas > Filtros > Modificar filtro de categorías** para realizar cambios en los filtros de categorías existentes.

Importante

Cuando modifica un filtro de categorías, los cambios afectan a todas las políticas que apliquen el filtro.

No se ven afectadas las políticas que aplican un filtro de categorías con el mismo nombre en otro rol de administración delegado.

El nombre y la descripción del filtro aparecen en la parte superior de la página.

- Haga clic en **Cambiar nombre** para cambiar el nombre del filtro.
- Para cambiar la descripción del filtro, sólo debe escribir en el campo **Descripción**.

El número ubicado junto a **Políticas que utilizan este filtro** muestra la cantidad de políticas que usan actualmente el filtro seleccionado. Si el filtro de categorías está activado, haga clic en **Ver políticas** para obtener una lista de las políticas que aplican el filtro.

La parte inferior de la página muestra una lista de categorías y las acciones que se aplican actualmente a cada una.

1. Seleccione una entrada de la lista **Categorías** para ver información sobre las categorías o para cambiar la acción de filtrado relacionada con la categoría seleccionada.
2. Antes de realizar cambios en la acción aplicada a la categoría, use la sección **Detalles de la categoría** para revisar los atributos especiales relacionados con la categoría.
   - Para revisar las URL recategorizadas o no filtradas asignadas a la categoría, si las hubiera, haga clic en **Consulte las URL personalizadas de esta categoría**. Consulte *Cómo redefinir el filtrado para sitios específicos*, página 182.

- Para revisar las palabras clave asignadas a la categoría, haga clic en **Consulte las palabras clave de esta categoría**. Consulte *Cómo filtrar según palabras clave*, página 180.
- Para revisar las expresiones regulares que se usan para definir URL o palabras clave para la categoría, haga clic en **Consulte las expresiones regulares de esta categoría**.

3. Use los botones ubicados en la parte de la lista de categorías para cambiar la acción aplicada a la categoría seleccionada. Para obtener más información sobre las acciones disponibles, consulte *Acciones de filtrado*, página 44.

   Los administradores delegados no pueden cambiar la acción relacionada con las categorías que han sido bloqueadas por un superadministrador. Consulte *Cómo definir restricciones de filtrado para todos los roles*, página 266, para obtener más información.
4. Use las casillas de verificación ubicadas a la derecha de la lista Categorías para aplicar acciones de filtrado avanzadas a la categoría seleccionada:
   - Para cambiar el modo en que las palabras clave se usen para filtrar la categoría seleccionada, seleccione o desactive **Bloquear palabras clave**. *Cómo filtrar según palabras clave*, página 180
   - Para determinar si los usuarios pueden acceder a ciertos tipos de archivo desde sitios de la categoría seleccionada, seleccione o desactive **Bloquear tipos de archivo**. Consulte *Cómo administrar tráfico en función del tipo de archivo*, página 193.

     Si seleccionó bloquear tipos de archivo, seleccione uno o más tipos de archivo para bloquear.
   - Para especificar que el acceso a sitios de la categoría sea limitado según ciertos umbrales de ancho de banda, seleccione o desactive **Bloquear con Bandwidth Optimizer**. Consulte *Cómo utilizar Bandwidth Optimizer para administrar el ancho de banda*, página 191.

     Si seleccionó realizar bloqueos según ancho de banda, especifique los límites de umbral que desea usar.
5. Repita los pasos de 1 a 3 para hacer cambios en las acciones de filtrado aplicadas a otras categorías.
6. Después de modificar el filtro, haga clic en **Aceptar** para guardar los cambios en caché y volver a la página Filtros. Los cambios no se implementan hasta que haga clic en **Guardar todo**.

Para activar un nuevo filtro de categorías, agréguelo a una política y asigne la política a los clientes. Consulte *Políticas de filtrado de Internet*, página 73.

Cómo crear un filtro de protocolos

Temas relacionados:

- *Protocolos y categorías de filtrado*, página 38
- *Acciones de filtrado*, página 44
- *Cómo modificar un filtro de protocolos*, página 52
- *Cómo trabajar con protocolos*, página 185

Use la página **Administración de políticas > Filtros > Agregar filtro de protocolos** para definir un nuevo filtro de protocolos. Puede trabajar desde una plantilla predefinida o hacer una copia de un filtro de protocolos existente para usar como base del nuevo filtro.

1. Especifique un **Nombre de filtro** único. El nombre debe tener entre 1 y 50 caracteres y no puede incluir ninguno de los siguientes:

   ```
   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

   Los nombres de filtro pueden incluir espacios, guiones y apóstrofes.
2. Escriba una breve **Descripción** del filtro. Esta descripción aparece junto al nombre de filtro en la sección Filtros de protocolos de la página Filtros, y debe explicar el fin del filtro.

   Las restricciones de caracteres que se aplican a nombres de filtro también se aplican a las descripciones, con 2 excepciones: las descripciones pueden incluir puntos (.) y comas (,).
3. Seleccione una entrada de la lista desplegable para determinar si usar una plantilla (consulte *Plantillas de filtros de protocolos y categorías*, página 55) o hacer una copia de un filtro existente como base para el nuevo filtro.
4. Para ver y modificar el nuevo filtro, haga clic en **Aceptar**. El filtro se agrega a la lista **Filtros de protocolos** de la página Filtros.

Para finalizar con la personalización del nuevo filtro, continúe con *Cómo modificar un filtro de protocolos*.

Cómo modificar un filtro de protocolos

Temas relacionados:

- *Protocolos y categorías de filtrado*, página 38
- *Cómo crear un filtro de protocolos*, página 52
- *Acciones de filtrado*, página 44
- *Cómo trabajar con protocolos*, página 185
- *Cómo utilizar Bandwidth Optimizer para administrar el ancho de banda*, página 191

Use la página **Administración de políticas > Filtros > Modificar filtro de protocolos** para cambiar los filtros de protocolos existentes.

> **Importante**
>
> Los cambios que realice en este punto afectarán a todas las políticas que apliquen este filtro.
>
> No se verán afectadas las políticas que aplican un filtro de protocolos con el mismo nombre en otro rol administrativo delegado.

El nombre y la descripción del filtro aparecen en la parte superior de la página.

- Haga clic en **Cambiar nombre** para cambiar el nombre del filtro.
- Para cambiar la descripción del filtro, sólo debe escribir en el campo **Descripción**.

El número ubicado junto a **Políticas que utilizan este filtro** muestra la cantidad de políticas que usan actualmente el filtro seleccionado. Si el filtro de protocolos está activado, haga clic en **Ver políticas** para obtener una lista de las políticas que aplican este filtro.

La parte inferior de la página muestra una lista de los protocolos y las acciones que se aplican actualmente a cada uno.

Para cambiar la forma en que se filtran y registran los protocolos, haga lo siguiente:

1. Seleccione un protocolo de la lista **Protocolos**. Las acciones de filtrado avanzado para el protocolo seleccionado se muestran en la parte derecha de la lista.
2. Use los botones **Permitir** y **Bloquear** en la parte inferior de la lista de protocolos para cambiar la acción que se aplica al protocolo seleccionado.

   > **Nota**
   >
   > El software de Websense puede bloquear solicitudes de protocolos basados en TCP, pero no en UDP.
   >
   > Algunas aplicaciones utilizan mensajes basados tanto en TCP como en UDP. Si la solicitud de red inicial de una aplicación se realiza mediante TCP y los datos posteriores se envían mediante UDP, el software de Websense bloquea la solicitud TCP inicial y, por lo tanto, bloquea el tráfico UDP posterior.
   >
   > Las solicitudes de UDP se registran como bloqueadas, incluso cuando se las permite.

   Para aplicar la misma acción a otros protocolos del grupo de protocolos seleccionado, haga clic en **Aplicar al grupo**.
3. Si desea obtener información sobre el uso del protocolo seleccionado disponible para alertas e informes, seleccione la casilla de verificación **Registrar datos de protocolo**.

4. Para aplicar un límite de ancho de banda al uso de este protocolo, haga clic en **Bloquear con Bandwidth Optimizer** y, luego, establezca los umbrales de ancho de banda deseados. Consulte *Cómo utilizar Bandwidth Optimizer para administrar el ancho de banda*, página 191, para obtener más información.
5. Después de modificar el filtro, haga clic en **Aceptar** para guardar los cambios en caché y volver a la página Filtros. Los cambios no se implementan hasta que haga clic en **Guardar todo**.

Para activar un nuevo filtro de protocolos, agréguelo a una política y aplique la política a los clientes (consulte *Políticas de filtrado de Internet*, página 73).

> **Nota**
> Puede crear políticas que empiecen a aplicar el filtro de protocolos a una hora específica. Si los usuarios inician una sesión de protocolo antes de que se active el filtro, pueden seguir accediendo al protocolo, incluso si el filtro lo bloquea, mientras continúe la sesión. Una vez que un usuario termina la sesión, se bloquean las solicitudes adicionales del protocolo.

Filtros de protocolos y categorías definidos por Websense

El software de Websense incluye varios filtros de protocolos y categorías de muestra. Puede usar estos filtros tal cual o modificarlos para que se adapten a sus necesidades de filtrado. Si no necesita los filtros predefinidos, muchos de ellos pueden eliminarse.

Los filtros de categorías predefinidos son:

- Básico
- Seguridad básica
- Bloquear todo
- Predeterminado
- Sólo supervisar
- Permitir todo

Los filtros de categorías Bloquear todo y Permitir todo no se enumeran en la página Filtros, pero se pueden agregar en las políticas. Estos filtros desempeñan una función especial en el filtrado y no se pueden eliminar ni modificar. Cuando se filtra una solicitud de Internet, el software de Websense comprueba si se aplican los filtros Bloquear todo o Permitir todo antes de realizar otras comprobaciones de filtrado (consulte *Filtrado de un sitio*, página 81).

Los filtros de protocolos predefinidos son:

- Seguridad básica
- Predeterminado
- Sólo supervisar
- Permitir todo

Como su equivalente en el filtro de categorías, el filtro de protocolos Permitir todo no se enumera en la página Filtros y no se puede eliminar ni modificar. Además, tiene prioridad cuando se realiza el filtrado.

El filtro de protocolos y categorías Predeterminado se puede modificar pero no eliminar. En caso de actualización, si hay brechas en la política Predeterminada, se usa el filtro Predeterminado para filtrar solicitudes a las que no se aplica ninguna política.

Plantillas de filtros de protocolos y categorías

Cuando crea un nuevo filtro de protocolos o categorías, puede hacer una copia de un filtro existente en la página Filtros, seleccionar un filtro existente como modelo en la página Agregar filtro o usar una **plantilla** de filtro.

El software de Websense incluye 5 plantillas de filtros de categorías:

- **Sólo supervisar** y **Permitir todo**: permiten todas las categorías.
- **Bloquear todo**: bloquea todas las categorías.
- **Básico**: bloquea las categorías bloqueadas más frecuentemente y permite el resto.
- **Predeterminado**: aplica las acciones Bloquear, Permitir, Continuar y Cuota a las categorías.
- **Seguridad básica**: bloquea sólo las categorías predeterminadas de la clase Riesgo de seguridad (consulte *Clases de riesgo*, página 41).

El software de Websense también incluye 3 plantillas de filtros de protocolos:

- **Sólo supervisar** y **Permitir todo**: permiten todos los protocolos.
- **Seguridad básica**: bloquea los protocolos de intercambio de archivos P2P y elusión con proxy, además de los protocolos de archivos adjuntos de mensajería instantánea (de estar suscripto) y de tráfico malicioso (Websense Web Security).
- **Predeterminado**: bloquea los protocolos de mensajería instantánea y chat, además de los protocolos de intercambio de archivos P2P, de elusión con proxy, de archivos adjuntos de mensajería instantánea (de estar suscripto) y de tráfico malicioso (Websense Web Security).

Si bien puede modificar o eliminar la mayoría de los filtros de protocolos y categorías definidos por Websense, no puede modificar ni eliminar las plantillas. De la misma forma, si bien puede crear todos los filtros personalizados que necesite, no puede crear nuevas plantillas.

Dado que las plantillasno se pueden modificar, brindan un método constante de referencia a las acciones de filtrado originales de los filtros definidos por Websense. Por ejemplo, las plantillas del filtro de protocolos y categorías Típico aplica las mismas acciones que el filtro de protocolos y categorías Predeterminado original. Esto significa que puede restaurar la configuración de filtrado de Websense original creando filtros que usen las plantillas predeterminadas.

Para obtener instrucciones sobre el uso de plantillas para crear filtros nuevos, consulte *Cómo crear un filtro de categorías*, página 49, o *Cómo crear un filtro de protocolos*, página 52.

Cómo configurar los valores de filtrado de Websense

Temas relacionados:

- *Protocolos y categorías de filtrado*, página 38
- *Clientes*, página 59
- *Páginas de bloqueo*, página 85
- *Acciones de filtrado*, página 44
- *Acceso con contraseña*, página 47
- *Orden de filtrado*, página 80
- *Cómo utilizar Bandwidth Optimizer para administrar el ancho de banda*, página 191
- *Cómo filtrar según palabras clave*, página 180

Use la página **Configuración > Filtrado** para establecer la configuración básica de una amplia gama de funciones de filtrado.

En **Bandwidth Optimizer**, introduzca la información necesaria para filtrar el uso de Internet sobre la base del ancho de banda disponible. Para obtener más información sobre el filtrado de ancho de banda, consulte *Cómo utilizar Bandwidth Optimizer para administrar el ancho de banda*, página 191.

1. Para especificar una **velocidad de conexión a Internet**, lleve a cabo una de las siguientes acciones:
   - Seleccione una velocidad estándar de la lista desplegable.
   - Escriba la velocidad de red en kilobits por segundo en el campo de texto.
2. Use el campo **Ancho de banda predeterminado de la red** para introducir el umbral predeterminado (porcentaje del tráfico de red total) que debe usarse cuando el filtrado del ancho de banda de la red está activado.
3. Use el campo **Ancho de banda predeterminado por protocolo** para introducir el umbral predeterminado que debe usarse cuando el filtrado del ancho de banda de protocolos está activado.

Use la sección **Filtrado general** para determinar la forma en que se filtran los usuarios cuando se aplican varias políticas de grupo, especificar opciones de búsqueda de palabras clave y establecer el comportamiento de la sesión de cuota, continuar y el acceso con contraseña.

1. Para determinar la forma en que se filtran los usuarios cuando se aplican varias políticas de grupo, seleccione o desactive **Utilizar la política de grupo más restrictiva** (consulte *Orden de filtrado*, página 80).
   - Cuando se selecciona esta opción, se aplica la política que utiliza la configuración de filtrado más restrictiva. Es decir, si una política de grupo aplicable bloquea el acceso a una categoría y otra lo permite, se bloquea la solicitud del usuario de un sitio de esa categoría.

- Cuando la opción no está seleccionada, se usa la configuración más permisiva.

2. Seleccione una de las siguientes **opciones de búsqueda de palabras clave** (consulte *Cómo filtrar según palabras clave*, página 180).

Sólo CGI	Bloquea los sitios cuando las palabras clave aparecen en cadenas de consultas CGI (después del signo ? en una dirección Web). Ejemplo: **search.yahoo.com/search?p=test** El software de Websense no busca palabras clave antes del signo ? si se selecciona esta opción.
Sólo URL	Bloquea los sitios cuando aparecen las palabras clave en la URL. Si la dirección solicitada contiene una cadena de consulta CGI, el software de Websense busca palabras clave hasta el signo ?.
URL y CGI	Bloquea los sitios cuando aparecen las palabras clave en cualquier lugar de la dirección. Si existe una cadena de consulta CGI, el software de Websense busca palabras clave antes y después del signo ?.
Desactivar bloqueo por palabra clave	Debe usarse con cuidado. La función **Desactivar bloqueo por palabra clave** desactiva todo bloqueo de palabras clave, incluso si se ha seleccionado **Bloquear palabra clave** en un filtro de categorías.

3. En el campo **Tiempo de espera de acceso con contraseña**, escriba la cantidad máxima de segundos (hasta 3600, el valor predeterminado es 60) que un usuario puede acceder a sitios de todas las categorías después de seleccionar el acceso con contraseña (consulte *Acceso con contraseña*, página 47).
4. En el campo **Tiempo de espera de Continuar**, escriba la cantidad máxima de segundos (hasta 3600, el valor predeterminado es 60) que un usuario que hace clic en Continuar puede acceder a sitios de todas las categorías regidas por la acción Continuar (consulte *Acciones de filtrado*, página 44).
5. En el campo **Duración de sesión de cuota**, escriba el intervalo (hasta60 min, el valor predeterminado es 10) durante el cual un usuario puede visitar sitios de categorías limitadas por cuota (consulte *Cómo usar tiempo de cuota para limitar el acceso a Internet*, página 46).

   La sesión comienza cuando el usuario hace clic en el botón Utilizar tiempo de cuota.
6. Escriba el **Tiempo de cuota predeterminado por día** (hasta 240 min, el valor predeterminado es de 60) para todos los usuarios.

   Para cambiar el tiempo de cuota de los usuarios individuales, vaya a la página **Políticas > Clientes**.

   A medida que modifica los valores de la duración de sesión de cuota y del tiempo de cuota predeterminado por día, se calcula y muestra el valor **Sesiones de cuota predeterminadas por día**.

Use la sección **Mensajes de bloqueo** para escribir la dirección URL o la ruta de acceso a la página de bloqueo HTML alternativa que creó para los mensajes de

bloqueo de marco principal del navegador (consulte *Cómo crear mensajes de bloqueo alternativos*, página 92).

- Pueden usarse páginas separadas para los diferentes protocolos: **FTP**, **HTTP** (lo que incluye **HTTPS**) y **Gopher**.
- No complete estos campos si desea usar el mensaje de bloqueo predeterminado suministrado con el software de Websense software o una versión personalizada de ese mensaje (consulte *Cómo personalizar el mensaje de bloqueo*, página 88).

En **Filtrado de búsqueda**, seleccione **Activar filtrado de búsqueda** para que el software de Websense active una configuración que ofrecen ciertos motores de búsqueda que bloquea la visualización en los resultados de la búsqueda de imágenes en miniatura y otro contenido explícito asociado con sitios bloqueados (consulte *Filtrado de búsqueda*, página 47).

Al final de la sección, se enumeran los motores de búsqueda que admiten esta función.

Cuando haya finalizado de configurar el filtrado, haga clic en **Aceptar** para guardar los cambios en caché. Los cambios no se implementan hasta que haga clic en **Guardar todo**.

3 Clientes

Puede personalizar el modo en que el software de Websense filtra las solicitudes de usuarios o equipos específicos al agregarlos como **clientes** vía Websense Manager. Los clientes pueden ser:

- **Equipos**: equipos individuales de la red, definidos por dirección IP.
- **Redes**: grupos de equipos, definidos conjuntamente como un rango de direcciones IP.
- **Usuarios**: Cuentas de dominio, usuario, grupo en un servicio de directorio admitido.

En principio, el software de Websense filtra todos los clientes de de la misma manera con la política **predeterminada** (consulte *Política predeterminada*, página 74). Una vez que agrega un cliente a la página Clientes de Websense Manager, puede asignar una política de filtrado específica a ese cliente.

Cuando se pueden aplicar varias políticas, como cuando se asigna una política al usuario y otra al equipo, el software de Websense determina qué política implementar de la siguiente manera:

1. Aplicar la política asignada al **usuario** que realiza la solicitud. Si esa política no tiene filtros programados en el momento de la solicitud, use la siguiente política aplicable.
2. Si no hay una política específica del usuario o la política no tiene filtros activos en el momento de la solicitud , busque una política asignada en el **equipo** (primero) o la **red** (después) desde la cual se realizó la solicitud.
3. En caso de que no haya ninguna política específica de la computadora o red, o en caso de que la política no tenga filtros activos en el momento de la solicitud, busque una política asignada a cualquier **grupo** al que pertenezca el usuario. Si el usuario pertenece a varios grupos, el software de Websense considera todas las políticas de grupo que se apliquen (consulte *Orden de filtrado*, página 80).
4. Si no hay ninguna política de grupo, busque una política asignada al **dominio** del usuario (UO).
5. Si no se encuentra ninguna política aplicable o si la política no implementa un filtro de categoría en el momento de la solicitud, implemente la política **predeterminada** para el rol para el que se asignó el cliente.

Para obtener más información sobre cómo el software de Websense aplica políticas de filtrado a los clientes, consulte *Filtrado de un sitio*, página 81.

Cómo trabajar con clientes

Temas relacionados:

- *Clientes*, página 59
- *Cómo trabajar con equipos y redes*, página 61
- *Cómo trabajar con usuarios y grupos*, página 62
- *Cómo agregar un cliente*, página 68
- *Cómo cambiar la configuración de clientes*, página 70

Use la página **Administración de políticas > Clientes** para ver información sobre los clientes existentes, agregar, editar o eliminar clientes, o para mover clientes a un rol de administración delegado.

Si es un administrador delegado, debe agregar clientes a la lista de clientes administrada para verlos en la página Clientes. Consulte *Cómo agregar un cliente*, página 68, para obtener instrucciones.

Los clientes se dividen en 3 grupos:

- **Directorio**, que incluye usuarios, grupos y dominios del servicio de directorio (consulte *Cómo trabajar con usuarios y grupos*, página 62).
- **Redes**, los rangos de direcciones IP dentro de la red filtrada que se pueden regir por una sola política (consulte *Cómo trabajar con equipos y redes*, página 61).
- **Equipos**, equipos individuales en la red filtrada, identificados por dirección IP (consulte *Cómo trabajar con equipos y redes*, página 61).

Haga clic en el signo más (+) ubicado junto al tipo de cliente para ver una lista de clientes existentes del tipo seleccionado. Cada lista de clientes incluye:

- el nombre del cliente, la dirección IP o el rango de direcciones IP.
- La **política** asignada actualmente al cliente. La política **predeterminada** se usa hasta que se asigna otra política (consulte *Políticas de filtrado de Internet*, página 73).
- Si el cliente puede usar una opción **acceso con contraseña** para ver sitios Web bloqueados o no (consulte *Acceso con contraseña*, página 47).
- Si el cliente tiene una cantidad de **tiempo de cuota** asignado o no (consulte *Cómo usar tiempo de cuota para limitar el acceso a Internet*, página 46).

Para buscar un cliente específico, busque el nodo correspondiente en el árbol.

Para editar la configuración de autenticación, la política de cliente, el acceso con contraseña y el tiempo de cuota, seleccione uno o más clientes de la lista y, a continuación, haga clic en **Modificar**. Consulte *Cómo cambiar la configuración de clientes*, página 70, para obtener más información.

Para agregar un cliente o aplicar una política a un cliente administrado que no aparezca actualmente en la página Clientes, haga clic en **Agregar** y, a continuación, vaya a *Cómo agregar un cliente*, página 68, para obtener más información.

Si creó roles de administración delegados (consulte *Administración delegada*, página 237), los superadministradores pueden mover sus clientes a otros roles. Primero marque la casilla de verificación ubicada junto a la entrada de cliente y, a continuación, haga clic **Mover a rol**. Cuando un cliente se mueve a un rol de administración delegado, la política y los filtros que se aplican al cliente se copian en el rol. Consulte *Cómo mover clientes a roles*, página 70, para obtener más información.

Si configuró el software de Websense para comunicarse con un servicio de directorio basado en LDAP, aparece el botón **Administrar grupos LDAP personalizados** en la barra de tareas ubicada en la superior de la página. Haga clic en este botón para agregar o editar grupos según un atributo LDAP (consulte *Cómo trabajar con grupos LDAP personalizados*, página 66).

Para quitar un cliente de Websense Manager, seleccione el cliente y haga clic en **Eliminar**.

Cómo trabajar con equipos y redes

Temas relacionados:

- *Cómo trabajar con clientes*, página 60
- *Cómo trabajar con usuarios y grupos*, página 62
- *Cómo agregar un cliente*, página 68
- *Cómo asignar una política a clientes*, página 79

En Websense Manager, un **equipo** es la dirección IP (por ejemplo, 10.201.3.1) relacionada con un equipo filtrado. Un **equipo** es el rango de direcciones IP (por ejemplo, 10.201.3.2 - 10.201.3.44) relacionado con un grupo de equipos filtrados.

Puede asignar políticas a clientes de red y equipos tal como lo haría con usuarios, grupos o clientes de dominio.

- Asigne una política a un **equipo** que, por ejemplo, no requiera que los usuarios inicien sesión, o con la que los usuarios puedan acceder con cuentas de invitados.
- Asigne una política a una **red** para aplicar la misma política de filtrado a varios equipos al mismo tiempo.

Cuando asigna una política a un equipo o una red, esa política se implementa independientemente de quién haya iniciado sesión en el equipo filtrado, **a menos** que haya asignado una política al usuario que inició sesión. Esta política de equipo o red tiene prioridad sobre cualquier otra política de **grupo** que se pueda aplicar al usuario.

Cómo trabajar con usuarios y grupos

Temas relacionados:

- *Cómo trabajar con clientes*, página 60
- *Servicios de directorio*, página 62
- *Cómo trabajar con grupos LDAP personalizados*, página 66
- *Cómo trabajar con equipos y redes*, página 61
- *Cómo agregar un cliente*, página 68
- *Cómo asignar una política a clientes*, página 79

Para aplicar políticas a grupos y usuarios individuales de la red, configure el software de Websense para tener acceso al servicio de directorio para obtener información de objetos de directorio (usuario, grupo, dominio y unidad organizativa).

El software de Websense se puede comunicar con el directorio de Windows NT / Active Directory (modo mixto) y con Windows Active Directory, Novell eDirectory y Sun Java System Directory mediante el protocolo de acceso ligero a directorio (Lightweight Directory Access Protocol o LDAP).

Nota

Cuando usa un servicio de directorio basado en LDAP, no se admiten los nombres de usuario duplicados. Asegúrese de que el mismo nombre de usuario no aparezca en varios dominios.

Además, si está usando Windows Active Directory o Sun Java System Directory, no se admiten los nombres de usuario con contraseñas en blanco. Asegúrese de que todos los usuarios tengan contraseñas asignadas.

Websense User Service transmite información del servicio de directorio a Policy Server y Filtering Service para usar cuando se aplican políticas de filtrado.

Websense, Inc. recomienda instalar User Service en un equipo con Windows (aunque puede residir en un equipo con Linux). Generalmente, este es el equipo donde se instala Policy Server.

Para configurar el software de Websense para que se comunique con el servicio de directorio, consulte *Servicios de directorio*.

Servicios de directorio

Un servicio de directorio es una herramienta que almacena información sobre los usuarios y los recursos de una red. Antes de agregar clientes de usuarios (usuarios,

grupos, dominios o unidades organizativas) en Websense Manager, debe configurar el software de Websense para que recupere información del servicio de directorio.

Use la página **Configuración > Servicios de directorio** para identificar el servicio de directorio que se usa en la red. Puede configurar valores para un solo tipo de servicio de directorio por Policy Server.

Primero seleccione un servicio de directorio de la lista Directorios. La selección que haga determina qué configuración aparece en la página.

Consulte la sección adecuada para obtener instrucciones sobre la configuración:

- *Directorio de Windows NT / Active Directory (modo mixto)*, página 63
- *Windows Active Directory (modo nativo)*, página 63
- *Novell eDirectory y Sun Java System Directory*, página 65

Directorio de Windows NT / Active Directory (modo mixto)

Si el servicio de directorio es Directorio de Windows NT o Active Directory en modo mixto, no se necesita ninguna otra configuración.

En algunos pocos casos, si usa otro servicio de directorio, es posible que necesite proporcionar información adicional en esta pantalla. Esto sucede sólo cuando:

- DC Agent se usa para la identificación transparente (consulte *DC Agent*, página 213)

  y
- User Service se ejecuta en un equipo con Linux

Si esto coincide con su configuración, proporcione las credenciales administrativas incluidas en la lista del Directorio de Windows NT / Active Directory (modo mixto). Si su instalación no usa esta configuración, se desactivan los campos de las credenciales administrativas.

Windows Active Directory (modo nativo)

Windows Active Directory almacena información de los usuarios en uno o más *catálogos globales*. El catálogo global permite que las personas y las aplicaciones busquen objetos (usuarios, grupos, etc.) en un dominio de Active Directory.

Para que el software de Websense se comunique con Active Directory en modo nativo, debe proporcionar información sobre los servidores de catálogo global de su red.

1. Haga clic en **Agregar** ubicado junto a la lista de servidores de catálogo global. Aparece la página Agregar servidor de catálogo global.
2. Use el campo **IP del servidor o nombre** para identificar el servidor de catálogo global:
   - Si tiene varios servidores de catálogo global configurados para la conmutación por error, especifique el nombre de dominio de DNS.

- Si los servidores de catálogo global no se configuran para la conmutación por error, especifique la dirección IP o el nombre de host (si la resolución de nombres está activada en la red) del servidor que desea agregar.

3. Especifique el **Puerto** que el software de Websense debe usar para comunicarse con el catálogo global (de forma predeterminada: **3268**).
4. Opcionalmente, especifique el **Contexto root** que el software de Websense debe usar para buscar información de usuarios. Si proporciona un valor, debe ser un contexto válido en su dominio.
   - Si ha especificado un puerto de comunicaciones de 3268 o 3269, no es necesario proporcionar un contexto root.
   - Si el puerto especificado es 389 o 636, debe proporcionar un contexto root.
   - Si deja en blanco el campo Contexto root, el software de Websense comienza a buscar en el nivel superior del servicio de directorio.

   Nota
   Evite usar el mismo nombre de usuario en varios dominios. Si el software de Websense busca nombres de cuenta duplicados para un usuario, el usuario no se puede identificar de forma transparente.

5. Especifique qué cuenta administrativa del software de Websense se debe usar para recuperar el nombre de usuario y la información de ruta desde el servicio de directorio. Esta cuenta debe poder consultar y leer del servicio de directorio, pero no es necesario que pueda realizar cambios en el servicio de directorio o un administrador de dominio.

   Seleccione **Nombre distinguido por componentes** o **Nombre distinguido completo** para especificar cómo prefiere ingresar la información de cuenta.

   - Si seleccionó Nombre distinguido por componentes, especifique el **Nombre visible**, la **Contraseña** de la cuenta, la **Carpeta de cuentas** y el **nombre de dominio de DNS** para la cuenta administrativa. Utilice la forma de nombre común (cn) del nombre de usuario de administración, y no la forma ID de usuario (uid).

     Nota
     El campo **Carpeta de cuentas** no admite valores con la etiqueta de unidad organizativa (ou) (por ejemplo, *ou=Finanzas*). Si el nombre de cuenta de administración contiene una etiqueta ou, especifique el nombre distinguido completo para la cuenta de administración.

   - Si seleccionó Nombre distinguido completo, especifique el nombre distinguido como una única cadena en el campo **Nombre distinguido de usuario** (por ejemplo, *cn=Admin, cn=Usuarios, ou=SistemasInfo, dc=organización, dc=red*) y, a continuación, proporcione la **Contraseña** para esa cuenta.

6. Haga clic en **Aceptar**.

7. Repita el proceso anterior para cada servidor de catálogo global.
8. Haga clic en **Configuración** y, a continuación, vaya a *Configuración de directorio avanzada*, página 65.

Novell eDirectory y Sun Java System Directory

Para recuperar información del servicio de directorio, el software de Websense necesita el nombre distinguido, contexto root y contraseña de una cuenta de usuario con privilegios administrativos.

1. Especifique la dirección IP del equipo del servidor de directorio en el campo **IP del servidor**.
2. Especifique el número de **Puerto** que usará el software de Websense para comunicarse con el directorio. El valor predeterminado es 389.
3. Si el directorio necesita privilegios de administrador para el acceso de sólo lectura, especifique el **Nombre distinguido de administrador** y la **Contraseña**.
4. Opcionalmente, especifique el **Contexto root** que el software de Websense debe usar cuando busca información de usuarios. Por ejemplo, *o=dominio.com*.

   Si reduce el contexto, aumenta la velocidad y la eficacia para recuperar información de usuarios.

   Nota
   Evite usar el mismo nombre de usuario en varios dominios. Si el software de Websense busca nombres de cuenta duplicados para un usuario, el usuario no se puede identificar de forma transparente.

5. Haga clic en **Configuración** y, a continuación, vaya a *Configuración de directorio avanzada*, página 65.

Configuración de directorio avanzada

Temas relacionados:

- *Windows Active Directory (modo nativo)*, página 63
- *Novell eDirectory y Sun Java System Directory*, página 65

Esta configuración se puede usar para definir:

- Cómo el software de Websense busca en el servicio de directorio para encontrar información de usuario, grupo y dominio
- Si el software de Websense usa una conexión cifrada para comunicarse con el servicio de directorio
- Qué juego de caracteres usa el software de Websense para codificar información LDAP

Configure estos valores como sea necesario para cualquier servicio de directorio basado en LDAP.

1. Si usa tipos de clases de objetos personalizados (nombres de atributo) en el servicio de directorio, marque **Usar filtros personalizados**. Se muestran las cadenas de filtro predeterminadas en los campos Filtro.
2. Edite las cadenas de filtro existentes con los tipos de clases de objetos específicos de su directorio. Por ejemplo, si su directorio utiliza un tipo de clase de objeto como **depto** en lugar de **ou** (unidad organizativa), inserte un nuevo valor en el campo Filtro de búsqueda de dominio.

   Los atributos son siempre cadenas utilizadas en la búsqueda de contenidos del servicio de directorio. Los filtros personalizados ofrecen la funcionalidad descrita aquí.

   - El **Filtro de búsqueda del usuario** determina cómo User Service busca usuarios.
   - El **Filtro de búsqueda de grupo** determina cómo User Service busca grupos.
   - El **Filtro de búsqueda de dominio** determina cómo User Service busca dominios y unidades organizativas.
   - El **Filtro de búsqueda de grupos de usuarios** determina cómo User Service relaciona usuarios con grupos.
3. Para proteger las comunicaciones entre el software de Websense y el servidor de directorio, marque **Usar SSL**.
4. Para determinar qué juego de caracteres usa el software de Websense para codificar información de LDAP, seleccione **UTF-8** o **MBCS**.

   MBCS, o un juego de caracteres de varios bytes, se usa generalmente para codificar idiomas orientales como chino, japonés y coreano.
5. Haga clic en **Aceptar** para guardar los cambios. Los cambios no se implementan hasta que haga clic en **Guardar todo**.

Cómo trabajar con grupos LDAP personalizados

Temas relacionados:

- *Cómo trabajar con usuarios y grupos*, página 62
- *Servicios de directorio*, página 62
- *Cómo agregar o editar un grupo LDAP personalizado*, página 67

Use la página **Administrar grupos LDAP personalizados** para administrar grupos personalizados sobre la base de atributos definidos en el servicio de directorio. Esta

opción está disponible sólo si ha configurado el software de Websense para que se comunique con un servicio de directorio basado en LDAP.

> **Importante**
>
> Cuando agrega grupos LDAP personalizados a Websense Manager, Policy Server activo almacena las definiciones de grupo y no se influye sobre otras instancias de Policy Server. Para agregar grupos LDAP personalizados a varios Policy Server, use Websense Manager para iniciar sesión en cada Policy Server e ingrese la información.
>
> Si agrega grupos LDAP personalizados y, a continuación, cambia servicios de directorio o la ubicación del servidor de directorio, los grupos existentes se vuelven no válidos. Debe agregar los grupos de nuevo y, a continuación, definir a cada uno como cliente.

- Para agregar un grupo, haga clic en **Agregar** (consulte *Cómo agregar o editar un grupo LDAP personalizado*, página 67).
- Para cambiar una entrada de la lista, haga clic en su nombre de grupo (consulte *Cómo agregar o editar un grupo LDAP personalizado*).
- Para quitar una entrada, primero selecciónela y, a continuación, haga clic en **Eliminar**.

Cuando haya finalizado con los cambios en los grupos LDAP personalizados, haga clic en **Aceptar** para guardar los cambios en caché y volver a la página anterior. Los cambios no se implementan hasta que haga clic en **Guardar todo**.

Cómo agregar o editar un grupo LDAP personalizado

Use la página **Agregar grupo LDAP personalizado** para definir un grupo de Websense Manager según cualquier atributo definido en el servicio de directorio. Use la página **Modificar grupo LDAP personalizado** para realizar cambios en una definición existente.

> **Importante**
>
> Si agrega grupos LDAP personalizados y, a continuación, cambia servicios de directorio o la ubicación del servidor de directorio, los grupos existentes se vuelven no válidos. Debe agregar los grupos de nuevo y, a continuación, definir a cada uno como cliente.

1. Especifique o cambie el **Nombre de grupo**. Use un nombre descriptivo que indique claramente el objetivo del grupo LDAP.

   Los nombres de grupo no distinguen entre mayúsculas y minúsculas y deben ser únicos.

2. Especifique o cambie la descripción que define este grupo en su servicio de directorio. Por ejemplo:

   ```
   (WorkStatus=parttime)
   ```

   En este ejemplo, **WorkStatus** es un atributo del usuario que indica su condición de empleo y **parttime** es un valor que indica que el usuario es un empleado de tiempo parcial.
3. Haga clic en **Aceptar** para volver a la página Administrar grupos LDAP personalizados. Aparece la entrada nueva o revisada en la lista.
4. Agregue o modifique otra entrada o haga clic en **Aceptar** para guardar los cambios en caché y volver a la página anterior. Los cambios no se implementan hasta que haga clic en **Guardar todo**.

Cómo agregar un cliente

Temas relacionados:

- *Cómo trabajar con clientes*, página 60
- *Cómo trabajar con equipos y redes*, página 61
- *Cómo trabajar con usuarios y grupos*, página 62
- *Cómo buscar el servicio de directorio*, página 69
- *Cómo cambiar la configuración de clientes*, página 70

Use la página **Administración de políticas > Clientes > Agregar clientes** para agregar clientes de red, usuarios, grupos, equipos a Websense Manager para poder asignarles una política.

Si inició sesión como administrador delegado, sólo puede agregar clientes que aparezcan en la lista de clientes administrados. Cuando agrega clientes administrados a la página Clientes, debe asignarles una política.

1. Identifique uno o más clientes:
   - Para agregar un cliente de dominio, un usuario o un grupo, busque en el árbol **de directorio** entradas del servicio de directorio. Si usa un servicio de directorio basado en LDAP, también puede hacer clic en **Buscar** para activar una herramienta de búsqueda de directorio (consulte *Cómo buscar el servicio de directorio*, página 69).
   - Para agregar un cliente de red o un equipo, especifique una **dirección IP** o un **rango de direcciones IP**. No se pueden superponer dos definiciones de red, pero un cliente de red puede incluir una dirección IP identificada por separado como un cliente de equipo. En caso de que se superpongan, la política asignada al equipo tiene prioridad sobre la política asignada a la red.
2. Haga clic en el botón de flecha (>) para agregar cada cliente a la lista **Clientes seleccionados**.

Para quitar una entrada de la lista Clientes seleccionados, seleccione el cliente y, a continuación, haga clic en **Eliminar**.

3. Seleccione una **Política** para asignar a todos los clientes de la lista Clientes seleccionados.
4. Cuando haya finalizado, haga clic en **Aceptar** para guardar los cambios en caché. Los cambios no se implementan hasta que haga clic en **Guardar todo**.

Los clientes se agregan a la lista adecuada en la página **Administración de políticas > Clientes**. Para cambiar la política asignada a uno o más clientes o para establecer la configuración de clientes adicionales, seleccione las entradas de clientes y, a continuación, haga clic en **Modificar**. Consulte *Cómo cambiar la configuración de clientes*, página 70, para obtener más información.

Cómo buscar el servicio de directorio

Si configuró el software de Websense para que se comunique con un servicio de directorio basado en LDAP, puede usar una función de búsqueda para identificar a los usuarios que se agregarán como clientes en Websense Manager. La búsqueda también está disponible para agregar administradores y clientes administrados a roles de administración.

Para buscar un servicio de directorio para recuperar información de usuario, grupo y unidad organizativa:

1. Haga clic en **Buscar**.
2. Especifique todo o parte del **Nombre** de usuario, grupo o unidad organizativa.
3. Use la lista **Tipo** para indicar el tipo de entrada de directorio (usuario, grupo, UO o todo) que desea buscar.

   En un gran servicio de directorio, si selecciona **Todo** es posible que la búsqueda demore mucho tiempo.
4. Explore el árbol **Contexto de búsqueda** para especificar en qué parte del directorio desea buscar. Un contexto más preciso ayuda a aumentar la velocidad de la búsqueda.
5. Haga clic en **Ir**.

   Se muestra una lista de resultados de búsqueda.
6. Seleccione una o más entradas en los resultados de búsqueda y, a continuación, haga clic en la flecha derecha (>) para agregar cada selección como cliente o administrador.
7. Haga clic en **Nueva búsqueda** para ingresar otro conjunto de criterios de búsqueda.
8. Haga clic en **Examinar** para volver a buscar en el directorio.
9. Cuando haya finalizado con los cambios, haga clic en **Aceptar** para guardarlos en caché. Los cambios no se implementan hasta que haga clic en **Guardar todo**.

Cómo cambiar la configuración de clientes

Use la página **Administración de políticas > Clientes > Modificar cliente** para cambiar la configuración de autenticación y políticas de uno o más clientes. Si selecciona varios clientes antes de hacer clic en Modificar, los cambios en la configuración que realiza en la página Modificar clientes se aplican en todos los clientes seleccionados.

1. Seleccione una **política** para aplicarla a todos los clientes seleccionados. La política predeterminada rige a los clientes hasta que se asigne otra política.
2. Para permitir que los usuarios modifiquen una página de bloqueo de Websense al escribir una contraseña, haga clic en **Activar** debajo de Acceso con contraseña y, a continuación, escriba y confirme la contraseña.

   Para quitar los privilegios de acceso con contraseña de un cliente, haga clic en **Desactivar**.
3. Pasa asignar una cantidad personalizada de **Tiempo de cuota** a los clientes seleccionados, haga clic en **Personalizado** y, a continuación, ingrese la cantidad de minutos de tiempo de cuota que desea asignar.

   Para volver a configurar los valores de cuota predeterminados, haga clic en **Predeterminado**.
4. Haga clic en **Aceptar** para guardar los cambios en caché y volver a la página Clientes. Los cambios no se implementan hasta que haga clic en **Guardar todo**.

La nueva configuración del cliente aparece como parte de la lista de clientes en la página **Administración de políticas > Clientes**.

Cómo mover clientes a roles

Los superadministradores pueden usar la página **Mover clientes a rol** para mover uno o más clientes a un rol de administración delegado. Una vez que un cliente se ha movido, ese cliente aparece en la lista Clientes administrados y en la página Clientes en el rol de destino.

- La política aplicada al cliente en el rol de superadministradores y los filtros que implementa se copian en el rol administrativo delegado.
- Los administradores delegados pueden cambiar las políticas aplicadas a sus clientes administrados.
- Las restricciones de fijación de filtro no afectan a los clientes administrados por los superadministradores, pero afectan a los clientes administrados en los roles de administración delegados.
- Si un grupo, dominio o unidad organizativa se agrega a un rol como cliente administrado, los administradores delegados de ese rol pueden asignar políticas a usuarios individuales en el grupo, dominio o unidad organizativa.

- Si una red (rango de direcciones IP) se agrega a un rol como un cliente administrado, los administradores delegados de ese rol pueden asignar políticas a equipos individuales de esa red.
- No se puede mover el mismo cliente a varios roles.

Para mover los clientes seleccionados a un rol de administración delegado:

1. Use la lista desplegable **Seleccionar rol** para seleccionar un rol de destino.
2. Haga clic en **Aceptar**.

   Un cuadro de diálogo emergente indica que se están moviendo los clientes seleccionados. Este proceso de movimiento puede llevar un tiempo.
3. Los cambios no se implementan hasta que haga clic en **Guardar todo**.

Si los administradores delegados del rol seleccionado iniciaron sesión con acceso a políticas durante el proceso de movimiento, tendrán que cerrar sesión en Websense Manager y volver a iniciar sesión para ver a los clientes nuevos en la lista Clientes administrados.

4 Políticas de filtrado de Internet

Temas relacionados:

- *Filtros para el uso de Internet*, página 37
- *Clientes*, página 59
- *Política predeterminada*, página 74
- *Cómo trabajar con políticas*, página 75
- *Orden de filtrado*, página 80

Las políticas rigen el acceso de los usuarios a Internet. Una política está formada por:

- Filtros de categorías utilizados para aplicar acciones (permitir, bloquear) a categorías de sitios Web (consulte *Protocolos y categorías de filtrado*, página 38)
- Filtros de acceso limitado utilizados para permitir el acceso sólo a una lista restringida de sitios Web (consulte *Cómo restringir usuarios a una lista definida de sitios de Internet*, página 168)
- Filtros de protocolos utilizados para aplicar acciones a los protocolos de Internet (consulte *Protocolos y categorías de filtrado*, página 38)
- Una programación que determina cuándo se aplica cada filtro de categorías, acceso limitado y protocolos

Una nueva instalación del software de Websense incluye 3 políticas predefinidas:

- La opción **Predeterminado** filtra el acceso a Internet para todos los clientes no regidos por otra política. El software de Websense comienza a aplicar esta política al ingresar una clave de suscripción (consulte *Política predeterminada*, página 74).
- **Sin restricciones** ofrece acceso ilimitado a Internet. Esta política no se aplica a ningún cliente de forma predeterminada.
- **Ejemplo: usuario estándar** muestra cómo se pueden aplicar varios filtros de categorías y protocolos en una política para proporcionar diferentes grados de restricción de filtrado en diferentes momentos. Esta política se utiliza en el tutorial de primeros pasos para nuevos usuarios para demostrar el proceso de edición de una política y aplicarla a clientes.

Utilice cualquiera de estas políticas tal cual son, edítelas para adaptarlas a su organización o cree sus propias políticas.

Política predeterminada

Temas relacionados:

- *Políticas de filtrado de Internet*, página 73
- *Cómo trabajar con políticas*, página 75
- *Orden de filtrado*, página 80

Cuando instale el software de Websense, la política **predeterminada** comienza a supervisar el uso de Internet al ingresar la clave de subscripción. Al principio, la política predeterminada permite todas las solicitudes.

Nota

Cuando actualice desde una versión de software anterior de Websense, se conservará la configuración de la política existente. Después de actualizar, analice las políticas para asegurarse de que aún sean adecuadas.

A medida que crea y aplica sus propias políticas de filtrado, la política predeterminda continúa actuando como una red de seguridad, de manera de filtrar el acceso a Internet para cualquier cliente no regido por otra política.

En una nueva instalación, la política predeterminada debe ofrecer cobertura de filtrado de Internet (aplicar una combinación de filtros de acceso limitado y categorías y, si corresponde, filtros de protocolos) las 24 horas del día, los 7 días de la semana.

Importante

Es posible que los que actualicen desde una versión anterior del software de Websense tengan una política predeterminada que no cubra todos los períodos. No es necesario que cambie la política predeterminada. Sin embargo, si edita la política más adelante, el software de Websense no le permitirá guardar los cambios hasta que todos los períodos estén cubiertos.

Edite la política predeterminada según sea necesario para que se adapte a las necesidades de su organización. La política predeterminada no se puede eliminar.

Cómo trabajar con políticas

Temas relacionados:

- *Políticas de filtrado de Internet*, página 73
- *Cómo crear una política*
- *Cómo editar una política*
- *Filtros para el uso de Internet*
- *Refinar políticas de filtrado*

Utilice la página **Administración de políticas > Políticas** para analizar la información de la política existente. Esta página también sirve como punto de inicio para agregar, editar y eliminar políticas, copiarlas a roles de administración delegados (superadministradores solamente) e imprimir información detallada sobre la configuración de la política.

La página Políticas incluye una lista de las políticas existentes. La lista incluye un nombre y descripción de cada política así como el número de usuario, red y equipos cliente a los que se ha asignado la política.

- Para agregar una política, haga clic en **Agregar** y consulte *Cómo crear una política*, página 76, para obtener más información.
- Para editar una política , haga clic en el nombre de la política en la lista y consulte *Cómo editar una política*, página 77, para obtener más información.
- Para ver qué clientes se filtran por la política, haga clic en el número en la columna Usuarios, Redes o Equipos. La información del cliente aparece en un cuadro de diálogo emergente.

Para imprimir una lista de todas las políticas y sus componentes, incluidos los filtros, categorías y protocolos personalizados, palabras clave y URL personalizadas y expresiones regulares, haga clic en **Imprimir políticas en archivo**. Esta función crea una hoja de cálculo detallado de la información de la política en formato de Microsoft Excel. Está diseñada para ofrecer una manera cómoda a especialistas, gerentes de recursos humanos y otros con autoridad de supervisión de modo de analizar la información de la política de filtrado.

Si creó roles de administración delegados (consulte *Administración delegada*, página 237), los superadministradores pueden copiar las políticas que hayan creado a otros roles para ser utilizadas por administradores delegados. Los filtros aplicados por la política también se copian.

Nota

Como los administradores delegados están regidos por Fijación de filtro, Permitir todos los filtros y las políticas que los aplican, no se pueden copiar a roles.

Para copiar políticas a otro rol, primero marque la casilla de verificación junto al nombre de la política y haga clic en **Copiar a rol**. Consulte *Cómo copiar filtros y políticas a roles*, página 173, para obtener más información.

Cómo crear una política

Temas relacionados:

- *Políticas de filtrado de Internet*, página 73
- *Cómo trabajar con políticas*, página 75
- *Cómo editar una política*, página 77
- *Cómo trabajar con filtros*, página 48
- *Cómo restringir usuarios a una lista definida de sitios de Internet*, página 168

Utilice la página **Política Administración > Políticas > Agregarpolítica** para crear una nueva política personalizada.

1. Ingrese un **nombre de política** único. El nombre de política debe contener entre 1 y 50 caracteres y no puede incluir ninguno de los siguientes caracteres:

   ```
   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

   Los nombres de política pueden incluir espacios, guiones y apóstrofos.
2. Ingrese una **descripción** para la política. La descripción debe ser clara y detallada para facilitar la administración de políticas a lo largo del tiempo.

   Las restricciones de caracteres que se aplican a los nombres de política también se aplican a las descripciones, con 2 excepciones: Las descripciones pueden incluir puntos (.) y comas (,).
3. Para utilizar una política existente como base para la nueva política, marque la casilla de verificación**Basar en política existente** y seleccione una política de la lista desplegable.

   Para comenzar con una política vacía, deje la casilla de verificación sin marcar.
4. Haga clic en **Aceptar** para almacenar los cambios en caché y vaya a la página Editar política.

   Utilice la página Editar política para terminar de definir la nueva política. Consulte *Cómo editar una política*, página 77.

Cómo editar una política

Temas relacionados:

- *Políticas de filtrado de Internet*, página 73
- *Cómo trabajar con políticas*, página 75
- *Cómo crear una política*, página 76
- *Cómo trabajar con filtros*, página 48
- *Cómo restringir usuarios a una lista definida de sitios de Internet*, página 168

Utilice la página **Administración de políticas > Políticas > Modificar política** para realizar cambios en una política existente o terminar de definir una nueva política.

Utilice la parte superior de la página para editar el nombre y la descripción de la política.

- Haga clic en **Cambiar nombre** para cambiar el nombre de la política.
- Simplemente escriba en el campo **Descripción** para cambiar la descripción del filtro.

En la descripción de la política, el campo **Clientes** muestra cómo muchos clientes de cada tipo (usuario, equipo y red) se filtran actualmente por esta política. Para ver qué clientes están regidos por la política, haga clic en el enlace correspondiente al tipo de cliente adecuado.

Para asignar esta política a clientes adicionales, haga clic en **Aplicar a clientes** en la barra de herramientas en la parte superior de la página y consulte *Cómo asignar una política a clientes*, página 79.

Utilice el área **Definición de política** para definir los filtros que aplica esta política en diferentes momentos:

1. Para agregar un bloque horario a la programación, haga clic en **Agregar**.
2. Utilice las columnas **Iniciar** y **Fin** en la tabla Programación para definir el período que cubre este bloque horario.

   Para definir el filtrado de un período que abarque la medianoche (por ejemplo, de 5 p.m. a 8 a.m.), agregue dos bloques horarios a la programación: uno que cubra el período desde la hora de inicio hasta la medianoche y otro que cubra el período desde la medianoche hasta la hora de finalización.

   La política **Ejemplo: usuario estándar**, incluida con el software de Websense, demuestra cómo definir un período de filtrado que abarque la medianoche.
3. Utilice la columna **Días** para definir los días de la semana incluidos en este bloque horario. Para seleccionar días de la lista, haga clic en la flecha hacia abajo en la parte derecha de la columna. Cuando termine de seleccionar los días, haga clic en la flecha hacia arriba.
4. Utilice la columna **Filtro de categorías /acceso limitado** para seleccionar un filtro y aplicarlo durante este bloque horario.

Para agregar un nuevo filtro y aplicar esta política, seleccione **Agregar filtro de categorías** o **Agregar filtro de acceso limitado**. Consulte *Cómo crear un filtro de categorías*, página 49, o *Cómo crear un filtro de acceso limitado*, página 170, para obtener instrucciones.

5. Utilice la columna **Filtro de protocolos** para seleccionar un filtro de protocolos y aplicarlo durante este bloque horario.

   Para agregar un nuevo filtro y aplicarlo a esta política, seleccione **Agregar filtro deprotocolos**. Consulte *Cómo crear un filtro de protocolos*, página 52, para obtener instrucciones.

6. Repita los pasos del 1 al 5 para agregar bloques horarios adicionales a la programación.

Cuando existe algún bloque horario seleccionado en la programa, la parte inferior de la página Editar políticas muestra los filtros aplicados durante ese bloque horario. Cada lista de filtros incluye:

- El tipo de filtro (filtro de categorías, filtro de acceso limitado o filtro de protocolos)
- El nombre y la descripción del filtro
- Los contenidos del filtro (categorías o protocolos con acciones aplicadas o una lista de sitios permitidos)
- La cantidad de políticas que aplican el filtro seleccionado
- Botones que se pueden usar para editar el filtro

Al editar un filtro en esta página, los cambios afectan cada política que aplica el filtro. Antes de editar un filtro aplicado por varias políticas, haga clic en el enlace **Cantidad de políticas que utilizan este filtro** para ver exactamente las políticas que resultarán afectadas.

Los botones que aparecen en la parte inferior de la lista de filtros dependen del tipo de filtro:

Tipo de filtro	Botones
filtro de categorías	• Utilice el botón **Permitir**, **Bloquear**, **Confirmar** o **Cuota** para cambiar la acción aplicada a las categorías seleccionadas (consulte *Acciones de filtrado*, página 44). • Para cambiar la acción aplicada a una categoría principal y todas sus subcategorías, primero modifique la acción aplicada a la categoría principal y, a continuación, haga clic en **Aplicar a subcategorías**. • Para habilitar el bloqueo de palabra clave, el bloqueo de tipo de archivo o el bloqueo en función del ancho de banda, haga clic en **Opciones avanzadas**.
filtro de acceso limitado	• Utilice el botón **Agregar sitios** y **Agregar expresiones** para agregar URL permitidas, direcciones IP o expresiones regulares al filtro (consulte *Cómo restringir usuarios a una lista definida de sitios de Internet*, página 168). • Para quitar un sitio de la lista, marque la casilla de verificación junto a la URL, dirección IP o expresión y haga clic en **Eliminar**.
filtro de protocolos	• Utilice el botón **Permitir** o **Bloquear** para cambiar la acción aplicada a los protocolos seleccionados (consulte *Acciones de filtrado*, página 44). • Para cambiar la acción aplicada a todos los protocolos en un grupo de protocolos, cambie la acción aplicada a cualquier protocolo en el grupo y haga clic en **Aplicar a grupo**. • Para registrar datos para el protocolo seleccionado o habilitar el bloqueo en función del ancho de banda, haga clic en **Opciones avanzadas**.

Cuando termine de editar una política, haga clic en **Aceptar** para almacenar los cambios en caché . Los cambios no se implementan hasta que haga clic en **Guardar todo**.

Cómo asignar una política a clientes

Temas relacionados:

- *Políticas de filtrado de Internet*, página 73
- *Cómo crear una política*, página 76
- *Cómo editar una política*, página 77
- *Clientes*, página 59
- *Cómo agregar un cliente*, página 68

Utilice la página **Políticas > Editar política > Aplicar política a clientes** para asignar la política seleccionada a clientes.

La lista Clientes muestra todos los clientes de usuarios, equipos y redes así como la política actualmente asignada a cada cliente.

Marque la casilla de verificación junto a cada cliente para que se filtren por la política seleccionada y haga clic en **Aceptar** para volver a la página Editar política. Haga clic en **Aceptar** nuevamente para almacenar los cambios en caché.

Haga clic en **Guardar todos** para indicar al software de Websense que comience a utilizar la nueva política para filtrar solicitudes de los clientes seleccionados.

Orden de filtrado

El software de Websense utiliza múltiplesfiltros, aplicados en un orden específico, para determinar si debe permitir, bloquear o limitar los datos solicitados de Internet.

Por cada solicitud que recibe, el software de Websense:

1. Verifica el cumplimiento de la suscripción, de modo de asegurarse de que la suscripción sea actual y que no se haya superado la cantidad de clientes suscriptos.
2. Determina la política que se aplica al buscar en este orden.
   a. Política asignada al **usuario**.
   b. Política asignada a la **dirección IP** (equipo o red) del equipo utilizado.
   c. Políticas asignadas a **grupos** a los que pertenezca el usuario.
   d. Política asignada al **dominio**del usuario.
   e. La política **predeterminada**.

   Se utiliza la primera política aplicable que se encuentra.
3. Filtra la solicitud según las restricciones de la política.

En ciertos casos, un usuario pertenece amás de un grupo o dominio y no se aplica ninguna política de usuario, equipo o red. En estos casos, el software de Websense verifica las políticas asignadas a cada uno de los grupos del usuario.

- Si todos los grupos tienen la misma política, el software de Websense filtra la solicitud según dicha política.
- Si uno de los grupos tiene una política diferente, el software de Websense filtra la solicitud según la selección **Usar bloqueo más restrictivo** en la página **Configuración > Filtrado**.

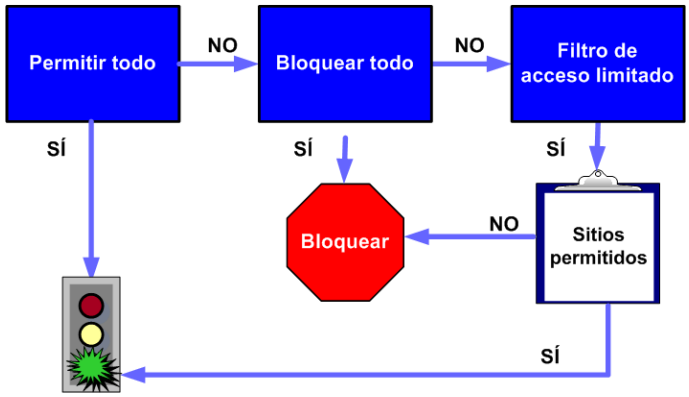
  Si la opción **Usar bloqueo más restrictivo** está marcada y alguna de las políticas aplicables bloquea el acceso a la categoría solicitada, el software de Websense bloquea el sitio.

  Si la opción no está marcada y alguna de las políticas aplicables permite el acceso a la categoría solicitada, el software de Websense permite el sitio.

Si alguna de las políticas aplicables aplica un filtro de acceso limitado, la opción **Usar bloqueo más restrictivo** puede tener diferentes efectos con respecto a lo esperado. Consulte *Filtros de acceso limitado y prioridad de filtrado*, página 168.

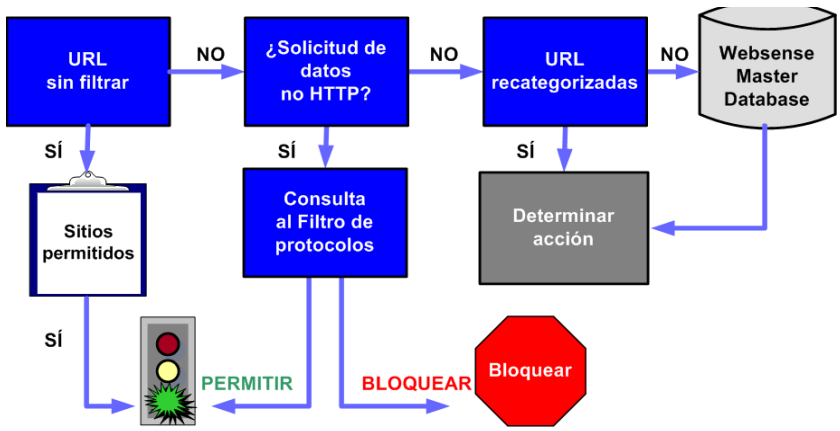
Filtrado de un sitio

El software de Websense evalúalas restricciones de la política de la siguiente forma para determinar si el sitio solicitado debe estar permitido o bloqueado.

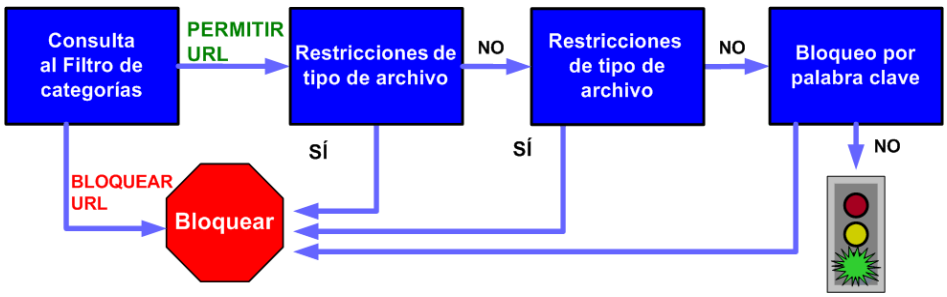


1. Determina el**filtro de categorías** o **filtro de acceso limitado** que la política aplica para el día y la hora actuales.
   - Si el filtro de categorías activo es **Permitir todos**, permite el sitio.
   - Si el filtro de categorías activo es **Bloquear todos**, bloquea el sitio.
   - Si el filtro es un **filtro de acceso limitado**, verifica si el filtro contiene la URL o la dirección IP. Si aparece, permite el sitio. Si no figura, bloquea el sitio.
   - En caso de que se aplique cualquier otro filtro de categorías, continúa con el paso 2.

> **Nota**
> El software de Websense filtra las URL a las que se accede desde la caché de un motor de búsqueda en Internet como cualquier otra URL. Las URL almacenadas de esta forma se filtran según las políticas activas para sus categorías de URL. Los registros de URL almacenadas en caché muestran todas las URL en caché, incluido cualquier parámetro de motor de búsqueda.

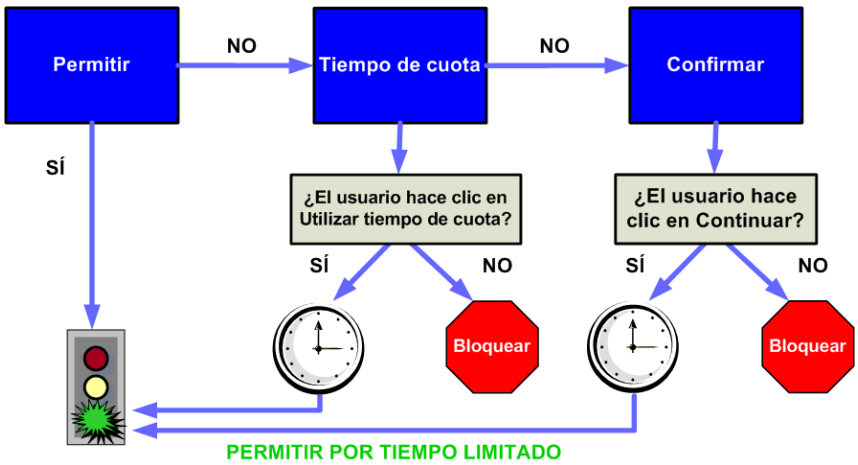


2. Intenta vincular el sitio con alguna entrada de la lista **URL sin filtrar**.
   - Si la URL figura en la lista, permite el sitio.
   - Si la URL no aparece en la lista, continúa con el paso 3.
3. Verifica el **filtro de protocolos** activo y determina sin algún protocolo no HTTP está asociado con la solicitud.
   - Si es así, aplica la configuración de filtrado de protocolos a los datos que se pueden transmitir.
   - De lo contrario, continúa con el paso 4.
4. Intenta vincular el sitio con una entrada de la lista **URL recategorizadas**.
   - Si hay una coincidencia, identifica la categoría del sitio y sigue con el paso 6.
   - Si no hay coincidencia, continúa con el paso 5.
5. Intenta vincular el sitio con una entrada de la **base de datos principal**.
   - Si la URL aparece en la base de datos principal, identifica la categoría del sitio y continúa con el paso 6.
   - Si no se encuentra una coincidencia, el sitio se categoriza como Varios/Sin categorizar y continúa con el paso 6.



6. Controla el filtro de categorías activo e identifica la acción aplicada a la categoría que contiene el sitio solicitado.
   - Si la acción es **Bloquear**, bloquea el sitio.
   - En caso de que se aplique cualquier otra acción, continúa con el paso 7.
7. Controla la configuración de **Bandwidth Optimizer** en el filtro de categorías activo (consulte *Cómo utilizar Bandwidth Optimizer para administrar el ancho de banda*, página 191).
   - Si el uso de ancho de banda supera algún límite configurado, bloquea el sitio.
   - Si el uso del ancho de banda no supera los límites especificados o no se aplica la acción en función del ancho de banda, continúa con el paso 8.
8. Controla las restricciones de **tipo de archivo** aplicadas a la categoría activa (consulte *Cómo administrar tráfico en función del tipo de archivo*, página 193).
   - Si el sitio contiene archivos cuyas extensiones están bloqueadas, bloquea el acceso a esos archivos. Si el sitio mismo está formado por un tipo de archivo bloqueado, bloquea el acceso al sitio.
   - Si el sitio no contiene archivos cuyas extensiones estén bloqueadas, va al paso 9.

9. Controla las **palabras clave** bloqueadas en la ruta de URL y CGI, si el bloqueo de palabra clave está habilitado (consulte *Cómo filtrar según palabras clave*, página 180).
   - Si encuentra una palabra clave bloqueada, bloquea el sitio.
   - Si no encuentra una palabra clave bloqueada, continúa con el paso 10.



10. Administra el sitio según la acción de filtrado aplicada a la categoría.
    - **Permitir**: Permite el sitio.
    - **Límite por cuota**: Muestra el mensaje de bloqueo con una opción para ver el sitio con tiempo de cuota o vuelve a la página anterior.
    - **Confirmar**: Muestra el mensaje de bloqueo con la opción de ver el sitio para fines relacionados con el trabajo.

El software de Websense continúa hasta que el sitio solicitado es bloqueado o permitido expresamente. En este punto, el software de Websense no intenta ningún filtrado adicional. Por ejemplo, si un sitio solicitado corresponde a una categoría bloqueada y contiene una palabra clave bloqueada, el software de Websense bloquea el sitio a nivel de categoría sin verificar el filtro de palabras clave. El servidor de registros registra la solicitud como bloqueada debido a una categoría bloqueada, no por una palabra clave.

Nota

Los usuarios con privilegios de acceso con contraseña pueden acceder a sitos de Internet independientemente del motivo por el que se bloqueó el sitio.

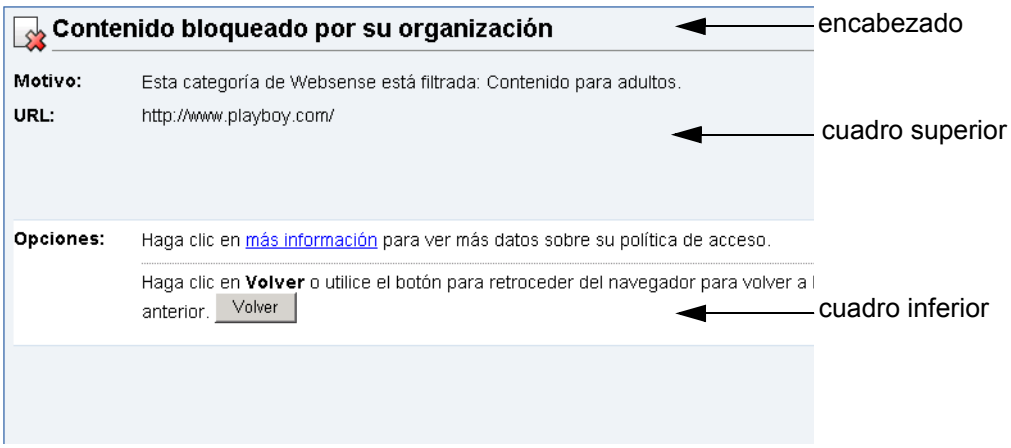
5 Páginas de bloqueo

Temas relacionados:

- *Mensajes de bloqueo de protocolos*, página 86
- *Cómo trabajar con páginas de bloqueo*, página 87
- *Cómo crear mensajes de bloqueo alternativos*, página 92
- *Cómo utilizar una página de bloqueo alternativa en otro equipo*, página 92

Cuando el software de Websense bloquea un sitio Web, muestra una página de bloqueo en el navegador del cliente. Si un sitio se bloquea porque corresponde a una categoría en la clase Riesgo de seguridad (consulte *Clases de riesgo*, página 41), se muestra una versión especial de la página de bloqueo.

De forma predeterminada, una página de bloqueo está formada por 3 secciones principales.



- El **encabezado** explica que el sitio está bloqueado.
- El **cuadro superior** contiene un mensaje de bloqueo que muestra la URL solicitada y la razón por la que se la bloqueó.
- El **cuadro inferior** presenta todas las opciones disponibles para el usuario, como la opción de volver a la página anterior o hacer clic en los botones Continuar o Utilizar tiempo de cuota para ver el sitio.

Las páginas de bloqueo se crean a partir de archivos HTML. Los archivos predeterminados de las páginas de bloqueo se incluyen con el software de Websense. Puede utilizar estos archivos predeterminados o crear sus propias versiones personalizadas.

- Personalice los archivos predeterminados para cambiar el mensaje de bloqueo (consulte *Cómo trabajar con páginas de bloqueo*, página 87).
- Configure el software de Websense para utilizar mensajes de bloqueo (predeterminados o personalizados) hospedados en un servidor Web remoto (consulte *Cómo utilizar una página de bloqueo alternativa en otro equipo*, página 92).

Mensajes de bloqueo de protocolos

Temas relacionados:

- *Cómo trabajar con páginas de bloqueo*, página 87
- *Cómo crear mensajes de bloqueo alternativos*, página 92
- *Cómo utilizar una página de bloqueo alternativa en otro equipo*, página 92

Cuando un usuario o aplicación solicita un protocolo no HTTP bloqueado, el software de Websense generalmente muestra un mensaje de bloqueo de protocolos.

Sin embargo, cuando un usuario solicita un sitio FTP, HTTPS o Gopher desde un navegador, y la solicitud pasa por un proxy, se muestra una página de bloqueo basada en HTML en el navegador, en cambio.

Si una aplicación solicita el protocolo bloqueado, el usuario puede recibir también un mensaje de error de la aplicación que indica que no se puede ejecutar. Los mensajes de error de aplicaciones no son generados por el software de Websense.

Es posible que se requiera alguna configuración del sistema para que se muestren mensajes de bloqueo de protocolos en equipos Windows:

- Para que se muestre un mensaje de bloqueo de protocolo en equipos cliente con Windows NT, XP o 200x, el servicio de mensajero de Windows debe estar habilitado. Este servicio está deshabilitado de forma predeterminada. Se puede utilizar el cuadro de diálogo Servicios de Windows para averiguar si el servicio se está ejecutando en un equipo específico (consulte *El cuadro de diálogo de Windows Services*, página 402).
- Para que se muestren mensajes de bloqueo de protocolos en un equipo Windows 98, debe iniciar **winpopup.exe**, ubicado en el directorio Windows. Ejecute esta aplicación con un símbolo del sistema o bien cópiela en la carpeta Inicio a fin de configurarla para que se inicie automáticamente.

Los mensajes de bloqueo de protocolos no se muestran en equipos Linux. Las páginas de bloqueo HTML se muestran independientemente del sistema operativo.

Si el filtrado de protocolos está habilitado, el software de Websense filtra solicitudes de protocolos independientemente de si los mensajes de bloqueo de protocolos están configurados para que se muestren en equipos cliente.

Cómo trabajar con páginas de bloqueo

Temas relacionados:

- *Mensajes de bloqueo de protocolos*, página 86
- *Cómo personalizar el mensaje de bloqueo*, página 88
- *Cómo crear mensajes de bloqueo alternativos*, página 92
- *Cómo utilizar una página de bloqueo alternativa en otro equipo*, página 92

Los archivos utilizados para crear páginas de bloqueo de Websense se almacenan en el directorio **Websense\BlockPages\es\Default**:

- **master.html** crea el cuadro de información de la página de bloqueo y utiliza uno de los siguientes archivos para que se muestren las opciones adecuadas en el cuadro inferior.

Nombre de archivo	Contenido
blockFrame.html	Texto y botón (opción Volver) para sitios en categorías bloqueadas.
continueFrame.html	Texto y botones para sitios en categorías en las que se aplica la acción **Confirmar**.
quotaFrame.html	Texto y botones para sitios en categorías en las que se aplica la acción **Cuota**.
moreInfo.html	Contenido de la página que se muestra cuando un usuario hace clic en el enlace **Más información** en la página de bloqueo.

- **block.html** contiene el texto del cuadro superior del mensaje de bloqueo que explica que el acceso está restringido, muestra el sitio solicitado y describe por qué el sitio está restringido.

Cómo personalizar el mensaje de bloqueo

Temas relacionados:

- *Cómo cambiar el tamaño del cuadro de mensaje*, página 89
- *Cómo cambiar el logotipo que aparece en la página de bloqueo*, página 89
- *Cómo utilizar variables de contenido de la página de bloqueo*, página 90
- *Cómo volver a las páginas de bloqueo predeterminadas*, página 91

Puede realizar una copia de los archivos predeterminados de páginas de bloqueo y utilizarla para personalizar el cuadro superior de la página de bloqueo que reciben los usuarios.

- Agregue información sobre las políticas de uso de Internet de su organización.
- Proporcione un método de contacto de Recursos humanos o administrador de Websense sobre las políticas de uso de Internet.

1. Navegue hasta el directorio de páginas de bloqueo de Websense.

   `<ruta de instalación>\BlockPages\es\Default`

2. Copie los archivos de páginas de bloqueo en el directorio de páginas de bloqueo personalizadas:

   `<ruta de instalación>\BlockPages\es\Custom`

   Nota

   No modifique los archivos originales de mensajes de bloqueo en el directorio **BlockPages\es\Default**. Cópielos al directorio **BlockPages\es\Custom** y luego modifique las copias.

3. Abra el archivo en un editor de texto como Notepad o vi.

   Advertencia

   Utilice un editor de texto simple para modificar los archivos de mensajes de bloqueo. Algunos editores HTML modifican el código HTML, lo cual podría corromper los archivos y ocasionar problemas en la visualización de los mensajes de bloqueo.

4. Modifique el texto. Los archivos contienen comentarios que le brindan orientación para realizar cambios.

   Nomodifique los elementos delimitados por los símbolos $* y *$ ni la estructura del código HTML. Esto permite al software de Websense mostrar información específica en el mensaje de bloqueo.

5. Guarde el archivo.

6. Reinicie Filtering Service (consulte *Cómo detener e iniciar los servicios Websense*, página 286, para obtener instrucciones).

Cómo cambiar el tamaño del cuadro de mensaje

De acuerdo con la información que desee ofrecer en el mensaje de bloqueo, es posible que el ancho predeterminado del mensaje de bloqueo y la altura del cuadro superior no sean adecuados. Para cambiar estos parámetros de tamaño en el archivo **master.html**:

1. Copie **master.html** desde el directorio **Websense\BlockPages\es\Default** a **Websense\BlockPages\es\Custom**.
2. Abra el archivo en un editor de texto como Notepad o vi (no editor de HTML).
3. Para cambiar el ancho del cuadro de mensaje, edite la siguiente línea:

   ```
   <div style="border: 1px solid #285EA6;width: 600px...">
   ```

   Cambie el valor del parámetro **ancho** según sea necesario.
4. Para que el cuadro superior del mensaje se desplace a fin de mostrar información adicional, edite la siguiente línea:

   ```
   <iframe src="$*WS_BLOCKMESSAGE_PAGE*$*WS_SESSIONID*$" ...
   scrolling="no" style="width:100%; height: 6em;">
   ```

   Cambie el valor del parámetro de **desplazamiento** a **automático** para que aparezca una barra de desplazamiento cuando el texto del mensaje supere el encabezado del cuadro.

   También puede cambiar el valor del parámetro **altura** para cambiar la altura del cuadro.
5. Guarde y cierre el archivo.
6. Reinicie Filtering Service para implementar el cambio (consulte *Cómo detener e iniciar los servicios Websense*, página 286).

Cómo cambiar el logotipo que aparece en la página de bloqueo

El archivo **master.html** también incluye el código HTML utilizado para mostrar un logotipo de Websense en la página de bloqueo. En cambio, para mostrar el logotipo de su organización:

1. Copie los archivos de la página de bloqueo desde el directorio **Websense\BlockPages\es\Default** a **Websense\BlockPages\es\Custom**, si aún no se han copiado.
2. Copie un archivo de imagen que contenga el logotipo de su organización en la misma ubicación.
3. Abra **master.html** en un editor de texto como Notepad o vi (no un editor de HTML) y edite la siguiente línea para reemplazar el logotipo de Websense con el logotipo de su organización:

   ```
   <img title="Websense" src="/en/Custom/wslogo_block_page.png"
   ...>
   ```

   - Reemplace **wslogo_block_page.png** con el nombre del archivo de imagen que contiene el logotipo de su organización.

- Reemplace los valores del parámetro **título** para reflejar el nombre de su organización.

4. Guarde y cierre el archivo.
5. Reinicie Filtering Service para implementar el cambio (consulte *Cómo detener e iniciar los servicios Websense*, página 286).

Cómo utilizar variables de contenido de la página de bloqueo

Las variables de contenido controlan la información que se muestra en las páginas de bloqueo HTML. Las siguientes variables están incluidas con el código de mensaje de bloqueo predeterminado.

Nombre de variable	Contenido que muestra
WS_DATE	Fecha actual
WS_USERNAME	Nombre del usuario actual (no incluye nombre de dominio)
WS_USERDOMAIN	Nombre de dominio para el usuario actual
WS_IPADDR	Dirección IP del equipo de origen de la solicitud
WS_WORKSTATION	Nombre del equipo bloqueado (si no hay ningún nombre disponible, se muestra la dirección IP)

Para utilizar una variable, inserte el nombre de variable entre los símbolos $* *$ en la etiqueta HTML que corresponda:

```
<p id="UserName">$*WS_USERNAME*$</p>
```

Aquí, *WS_USERNAME* es la variable.

El código de mensaje de bloqueo incluye las variables adicionales que se describen a continuación: Es posible que algunas de estas variables le resulten útiles al crear sus propios mensajes de bloqueo personalizados. Al ver estas variables en los archivos de mensaje de bloqueo definidos por Websense, **no** las modifique. Como Filtering Service utiliza estas variables al procesar solicitudes bloqueadas, deben permanecer en su lugar.

Nombre de variable	Objetivo
WS_URL	Muestra la URL solicitada.
WS_BLOCKREASON	Muestra por qué se bloqueó el sitio (es decir, qué acción de filtrado se aplicó).
WS_ISSECURITY	Indica si el sitio solicitado pertenece a alguna de las categorías predeterminadas en la clase Riesgo de seguridad. Si es VERDADERO, se muestra la página de bloqueo de seguridad.
WS_PWOVERRIDECGIDATA	Completa un campo de entrada en el código HTML de la página de bloqueo con información sobre el uso del botón **Acceso con contraseña**.

Nombre de variable	Objetivo
WS_QUOTA_CGIDATA	Completa un campo de entrada en el código HTML de la página de bloqueo con información sobre el uso del botón **Utilizar tiempo de cuota**.
WS_PASSWORDOVERRID_BEGIN, WS_PASSWORDOVERRID_END	Se relaciona con la activación de la funcionalidad de acceso con contraseña.
WS_MOREINFO	Muestra información detallada (al hacer clic en el enlace **Más información**) sobre por qué se bloqueó el sitio solicitado.
WS_POLICYINFO	Indica qué política rige al cliente que realiza la solicitud.
WS_MOREINFOCGIDATA	Envía datos a Filtering Service sobre el uso del enlace **Más información**.
WS_QUOTATIME	Muestra la cantidad de tiempo de cuota restante para el cliente de la solicitud.
WS_QUOTAINTERVALTIME	Muestra la longitud de la sesión de cuota configurada para el cliente de la solicitud.
WS_QUOTABUTTONSTATE	Indica si el botón **Utilizar tiempo de cuota** está habilitado o deshabilitado para una solicitud en particular.
WS_SESSIONID	Actúa como identificador interno asociado con una solicitud.
WS_TOPFRAMESIZE	Indica el tamaño (como porcentaje) de la parte superior de una página de bloqueo enviado por un servidor de bloqueo personalizado, si se configuró alguno.
WS_BLOCKMESSAGE_PAGE	Indica la fuente que se utiliza para el cuadro superior de la página de bloqueo.
WS_CATEGORY	Muestra la categoría de la URL bloqueada.
WS_CATEGORYID	El identificador único para la categoría de URL solicitada.

Cómo volver a las páginas de bloqueo predeterminadas

Si los usuarios presentan errores tras haber implementado mensajes de bloqueo personalizados, puede restaurar los mensajes de bloqueo originales de la siguiente manera:

1. Elimine todos los archivos del directorio **Websense\BlockPages\es\Custom**. De forma predeterminada, el software de Websense volverá a utilizar los archivos en el directorio predeterminado.
2. Reinicie Filtering Service (consulte *Cómo detener e iniciar los servicios Websense*, página 286).

Cómo crear mensajes de bloqueo alternativos

Temas relacionados:

- *Cómo trabajar con páginas de bloqueo*, página 87
- *Cómo personalizar el mensaje de bloqueo*, página 88

Puede crear sus propios archivos HTML para proporcionar el texto que aparece en el cuadro superior de la página de bloqueo. Utilice los archivos HTML existentes, cree archivos alternativos desde cero o realice copias de **block.html** para utilizarlas como una plantilla.

- Cree diferentes mensajes de bloqueo para cada uno de los 3 protocolos: HTTP, FTP y Gopher.
- Hospede archivos en el equipo de Websense o en el servidor Web interno (consulte *Cómo utilizar una página de bloqueo alternativa en otro equipo*, página 92).

Después de crear archivos de mensajes de bloqueo alternativos, debe configurar el software de Websense para que muestre los nuevos mensajes (consulte *Cómo configurar los valores de filtrado de Websense*, página 56). Durante este proceso, puede especificar los mensajes que desea utilizar para cada protocolo configurable.

Cómo utilizar una página de bloqueo alternativa en otro equipo

Temas relacionados:

- *Cómo trabajar con páginas de bloqueo*, página 87
- *Cómo personalizar el mensaje de bloqueo*, página 88
- *Cómo crear mensajes de bloqueo alternativos*, página 92

En lugar de utilizar las páginas de bloqueo de Websense y personalizar sólo los mensajes en el cuadro superior, puede crear sus propias páginas de bloqueo HTML y hospedarlas en un servidor Web interno.

Nota

Es posible almacenar páginas de bloqueo en un servidor Web externo. Sin embargo, si ese servidor hospeda un sitio especificado en la base de datos principal y ese sitio se encuentra en una categoría bloqueada, la página de bloqueo misma se bloquea.

Algunas organizaciones utilizan páginas de bloqueo alternativas remotas para ocultar la identidad del equipo servidor de Websense.

La página de bloqueo alternativa remota puede ser cualquier archivo HTML; no es necesario que siga el formato de las páginas de bloqueo de Websense. Sin embargo, con éste método para crear páginas de bloqueo, evita el uso de las funciones Continuar, Utilizar tiempo de cuota y Acceso con contraseña disponible con las páginas de bloqueo definidas por Websense (predeterminadas o personalizadas).

Cuando los archivos se encuentren en su lugar, edite el archivo **eimserver.ini** para indicar la nueva página de bloqueo.

1. Detenga los servicios Websense Filtering Service y Policy Server en ese orden (consulte *Cómo detener e iniciar los servicios Websense*, página 286).
2. En el equipo Filtering Service, navegue hasta el directorio **bin** de Websense (de forma predeterminada, \Archivos de programa\Websense\bin o /opt/websense/bin).
3. Cree una copia de respaldo del archivo **eimserver.ini** y almacénela en otro directorio.
4. Abra el archivo **eimserver.ini** en un editor de texto y ubique la sección **[WebsenseServer]** (en la parte superior del archivo).
5. Ingrese el nombre de host o la dirección IP del servidor que hospeda la página de bloqueo en el siguiente formato:

   ```
   UserDefinedBlockPage=http://<nombre de host o la dirección IP>
   ```

   La parte del protocolo de la URL (http://) es obligatoria.
6. Guarde el archivo y cierre el editor de texto.
7. Reinicie los servicios Websense Policy Server y Filtering Service, en ese orden.

Cuando los servicios se hayan iniciado, los usuarios recibirán la página de bloqueo hospedada en el equipo alternativo.

6 Uso de los informes para evaluar las políticas de filtrado

Temas relacionados:

- *Descripción general de los informes*, página 96
- *Informes de presentación*, página 98
- *Informes de investigación*, página 117
- *Acceder a ver actividad propia*, página 144

Websense Manager puede proporcionar varias herramientas de generación de informes para usar en la evaluación de la eficacia de sus políticas de filtrado. (Websense Manager y los componentes de generación de informes de Websense deben instalarse en servidores Windows.)

- La página **Hoy** aparece primero al abrir Websense Manager. Muestra el estado operativo del software Websense, y puede mostrar gráficos de las actividades de filtrado en la red desde medianoche. (Consulte *Hoy: Estado, Seguridad y Utilidad desde medianoche*, página 21.)
- La página **Historial** muestra gráficos de las actividades de filtrado en la red correspondientes a un máximo de 30 días, según la cantidad de información que haya en la base de datos de registro. Estos gráficos no incluyen las actividades del día actual. (Consulte *Historial: últimos 30 días*, página 24.)
- Los **informes de presentación** y los **informes de investigación** ofrecen muchas opciones para la generación, personalización y programación de informes. Para obtener más información, consulte *Descripción general de los informes*, página 96.

Si su empresa ha instalado Websense Manager en un servidor Linux, o si elige el programa de generación de informes Websense Explorer para Linux en vez de los componentes de generación de informes que se ejecutan con Windows, las opciones de informes no aparecerán en Websense Manager. En las páginas Hoy e Historial no se mostrará ningún gráfico de filtrado de Internet. Para obtener información sobre cómo instalar este programa y ejecutar informes, consulte la *Guía del administrador de Explorer para Linux*.

Descripción general de los informes

Temas relacionados:

- *Uso de los informes para evaluar las políticas de filtrado*, página 95
- *Informes de presentación*, página 98
- *Informes de investigación*, página 117
- *Acceder a ver actividad propia*, página 144

Además de los gráficos que aparecen en las páginas Hoy e Historial, el software Websense ofrece 2 opciones de informes: informes de presentación e informes de investigación.

> **Nota**
> En las empresas que utilizan la administración delegada, quizá algunos administradores no puedan acceder a todas las funciones de informes. Consulte *Administración delegada*, página 237.

Los **informes de presentación** ofrecen una lista de definiciones de informes. Algunos son informes en tablas; otros combinan un gráfico de barras y una tabla. Para generar un informe de presentación:

1. Seleccione un informe de la lista.
2. Haga clic en **Ejecutar**.
3. Seleccione el rango de fechas.
4. Haga clic en **Ejecutar ahora**.

Además de generar gráficos predefinidos, puede copiarlos y aplicar un filtro de informe personalizado que identifique clientes, categorías, protocolos o acciones específicos a incluir. Marque las definiciones de informes que use frecuentemente como Favoritos para que sean más fáciles de encontrar.

Puede programar cualquier informe de presentación para que se ejecute en un momento específico o en un ciclo de repetición. Para obtener más información, consulte *Informes de presentación*, página 98.

Los **informes de investigación** le permiten navegar interactivamente por los datos de registro. La página principal se muestra como un gráfico de barras de la actividad resumido, por clase de riesgos. Haga clic en los diferentes elementos de la página para actualizar el gráfico u obtener una vista diferente de los datos.

- Haga clic en el nombre de la clase de riesgo y luego seleccione un nivel de detalles más específico relacionado con esa clase de riesgo. Por ejemplo, para la clase de riesgo Responsabilidad legal, puede elegir mostrar la actividad por usuario.

- Haga clic en un nombre de usuario en el gráfico resultante para ver más detalles sobre ese usuario.
- Elija una opción diferente de la lista **Uso de Internet por** para cambiar el resumen del gráfico de barras.
- Complete los campos sobre el gráfico de barras para mostrar dos niveles de información a la vez. Por ejemplo, a partir de un gráfico de resumen de categorías, podría elegir **10**, **Usuario** y **5** para mostrar la actividad de los 5 usuarios principales en las 10 categorías principales.
- Haga clic en una barra o un número para abrir un informe detallado de ese elemento (clase de riesgo, categoría, usuario u otro).
- Haga clic en **Informes favoritos** para guardar un formato de informe particularmente útil para uso futuro, o para generar un Favorito guardado anteriormente.

Las posibilidades son casi infinitas. Para obtener más detalles sobre las numerosas formas en que puede ver los datos de uso de Internet, consulte *Informes de investigación*, página 117.

¿Qué es el tiempo de navegación en Internet?

Temas relacionados:

- *Trabajos en la base de datos*, página 325
- *Configuración de las opciones de tiempo de navegación por Internet*, página 330

Puede generar informes tanto de presentación como de investigación basados en el tiempo de navegación en Internet (IBT), es decir, la cantidad de tiempo que pasa una persona accediendo a sitios Web. Ningún programa de software puede decir la cantidad exacta de tiempo que pasa una persona viendo un sitio específico una vez que lo ha abierto. Alguien podría abrir un sitio, verlo durante unos segundos y luego responder una llamada de negocios antes de ir a otro sitio. Otra persona podría pasar varios minutos leyendo cada sitio detalladamente antes de pasar a otro.

El software Websense incluye un trabajo de Base de datos de registro para calcular el tiempo de navegación en Internet (IBT) usando una fórmula basada en ciertos valores configurables. Este trabajo se ejecuta una vez al día, de modo que la información de tiempo de navegación puede demorar un poco los datos de registro en sí.

Para el cálculo del tiempo de navegación, se considera que la sesión de Internet comienza cuando un usuario abre un navegador y continúa mientras dicho usuario siga solicitando sitios Web adicionales, al menos cada 3 minutos. (Este umbral de tiempo de lectura predeterminado es configurable.)

La sesión de Internet finaliza cuando pasan más de 3 minutos antes de que el usuario solicite otro sitio. El software Websense calcula el tiempo total de la sesión

comenzando en el momento de la primera solicitud y finalizando 3 minutos después de la última solicitud.

Si pasados más de 3 minutos el usuario hace solicitudes adicionales, comienza una nueva sesión. Comúnmente, el tiempo de navegación de un usuario consta de múltiples sesiones cada día.

Para obtener información sobre el trabajo de tiempo de navegación en Internet y las opciones de configuración asociadas, consulte *Trabajos en la base de datos*, página 325 y *Configuración de las opciones de tiempo de navegación por Internet*, página 330.

Informes de presentación

Temas relacionados:

- *Copiar un informe de presentación*, página 101
- *Copiar un informe de presentación*, página 101
- *Trabajar con Favoritos*, página 108
- *Generar informes de presentación*, página 109
- *Programar informes de presentación*, página 110
- *Ver la lista de trabajos programados*, página 115

La página **Informes > Informes de presentación** ofrece una lista de gráficos e informes en tablas predefinidos, cada uno con información específica de la base de datos de registro (consulte *Introducción a la base de datos de registro*, página 324). Seleccione un informe de este Catálogo de informes para ver una breve descripción.

Puede copiar un informe predefinido y personalizar el filtro de informe, especificando qué clientes, categorías, protocolos y acciones incluir. Los informes que se utilizan con frecuencia pueden marcarse como Favoritos para encontrarlos más rápidamente.

Ejecute cualquier informe ahora, o programe ciertos informes para que se ejecuten más tare o en forma periódica. Elija el formato de salida y distribuya los informes programados a un grupo de receptores selectos.

Si genera un informe directamente desde la página Informes de presentación en formato HTML, el mismo no se guarda al pasar a una página diferente. Si genera y visualiza inmediatamente un informe en formato PDF o XLS, el mismo no se guarda al cerrar el programa de visualización (Adobe Reader o Microsoft Excel).

Alternativamente, puede elegir guardar el archivo PDF o XLS en vez de mostrarlo inmediatamente, o puede usar la opción Guardar en el programa de visualización. En estos casos, asegúrese de eliminar o mover los informes periódicamente para evitar problemas de espacio en el disco.

Los informes programados se guardan automáticamente en el siguiente directorio:

```
<install_path>\ReportingOutput
```

La ruta de instalación predeterminada es C:\Program Files\Websense.

Al ejecutar un informe de presentación programado , el archivo del informe se envía a los destinatarios como un archivo adjunto de correo electrónico llamado **presentationreport_0**. El número aumenta según la cantidad de informes que se adjunten. Note que el nombre del adjunto no coincide con el nombre del archivo almacenado en el directorio ReportingOutput. Para encontrar un informe específico en este directorio, busque en los archivos creados en la fecha en que se ejecutó el trabajo programado.

Los informes se eliminan automáticamente del directorio ReportingOutput después de 15 días. Si desea conservar los informes durante más tiempo, inclúyalos en su rutina de respaldo o prográmelos y guarde los archivos enviados por correo electrónico en una ubicación que permita el almacenamiento a largo plazo.

Según la cantidad de informes que genere diariamente, los archivos de informes pueden ocupar importantes cantidades de espacio en disco. Asegúrese de que haya suficiente espacio en disco disponible en la máquina Websense Manager. Si el directorio ReportingOutput crece demasiado como para que los archivos puedan eliminarse automáticamente, puede eliminarlos manualmente.

El software Websense genera el informe en el formato que usted elija: PDF (Adobe Reader), XLS (Microsoft Excel) o HTML. Si elige el formato HTML, el informe se muestra en el panel de contenido de Websense Manager. Estos informes no pueden imprimirse ni guardarse como un archivo. Para imprimir o guardar un informe como archivo, elija el formato de salida PDF o XLS.

Si elige el formato PDF o XLS , tiene la opción de guardar el archivo del informe en el disco o mostrarlo en una ventana aparte.

Importante

Para mostrar informes de presentación en formato PDF, Adobe Reader v7.0 o superior debe estar instalado en la máquina desde la cual se accede a Websense Manager.

Para mostrar informes de presentación en formato XLS, Microsoft Excel 2003 o superior debe estar instalado en la máquina desde la cual se accede a Websense Manager.

En la página Informes de presentación, navegue por el Catálogo de informes y seleccione un informe de su interés. Luego use los controles en la página para ejecutar

el informe, crear una copia para la cual pueda personalizar el filtro de informe, y mucho más.

Botón	Acción
Mostrar sólo Favoritos	Seleccione esta opción para limitar el Catálogo de informes para que muestre sólo los informes marcados como Favoritos. Deseleccione esta opción para restablecer la lista completa de informes.
Modificar filtro de informe	Esta opción, disponible sólo cuando se selecciona una copia de un informe predefinido, le permite seleccionar categorías, protocolos, usuarios y acciones específicos a incluir en el informe. Consulte *Copiar un informe de presentación*, página 101.
Copiar	Hace una copia del informe seleccionado y lo agrega al Catálogo de informes como un informe personalizado. Consulte *Copiar un informe de presentación*, página 101. Seleccione el informe personalizado y luego establezca los parámetros específicos para el mismo haciendo clic en **Modificar filtro de informes**.
Favorito	Marca el informe seleccionado como Favorito, o quita la designación de Favorito. Consulte *Trabajar con Favoritos*, página 108. El Catálogo de informes muestra un símbolo de estrella al lado del nombre de cada informe marcado como Favorito. Utilice la casilla **Mostrar sólo favoritos** para controlar qué informes aparecen en el Catálogo de informes.
Eliminar	Elimina la copia del informe seleccionado del Catálogo de informes. No es posible eliminar los informes predefinidos instalados con el software. Si el informe eliminado aparece en algún trabajo programado, continuará generándose con ese trabajo.
Ejecutar	Genera el informe seleccionado una vez que se establece el rango de fechas y el formato de salida. Consulte *Generar informes de presentación*, página 109. Para controlar otros aspectos de un informe personalizado (copia de un informe predefinido), consulte *Copiar un informe de presentación*, página 101. Para programar que el informe se ejecute en un momento diferente o en un programa de repetición, haga clic en Programador.

Los botones en la parte superior de la página proporcionan opciones adicionales para la presentación de los informes.

Botón	Acción
Cola de trabajos	Muestra una página con una lista de los trabajos programados que se han creado, junto con el estado de cada trabajo. Consulte *Ver la lista de trabajos programados*, página 115.
Programador	Le permite definir la ejecución de un trabajo que incluye uno o más informes en un momento específico o en un programa de repetición. Consulte *Programar informes de presentación*, página 110.

Copiar un informe de presentación

Temas relacionados:

- *Copiar un informe de presentación*, página 101
- *Informes de presentación*, página 98

Inicialmente, la página **Informes de presentación** muestra un Catálogo de informes con un listado de todos los informes predefinidos instalados con el software. Puede generar cualquiera de estos informes para un período de tiempo específico seleccionando el informe y luego haciendo clic en Ejecutar.

Estos informes predefinidos también funcionan como plantillas que se pueden copiar para crear un filtro de informe personalizado. Cree un filtro de informe para controlar, por ejemplo, qué usuarios, categorías, protocolos y acciones deben incluirse al generar un informe a partir de la copia.

Después de copiar un informe y editar el filtro de informe, puede copiar el informe nuevo para crear variaciones basadas en esa copia.

1. Seleccione cualquier informe en el Catálogo de informes.
2. Haga clic en **Copiar**.

   En el Catálogo de informes aparecerá un duplicado del nombre del informe, con un código anexado para indicar que es una copia.
3. Seleccione la copia en el Catálogo de informes y luego haga clic en **Editar filtro de informe** para modificar los elementos del informe. Consulte *Copiar un informe de presentación*, página 101.

Definir el filtro de informe

Temas relacionados:

- *Copiar un informe de presentación*, página 101
- *Generar informes de presentación*, página 109

Los filtros de informes le permiten controlar qué información se incluirá en un informe. Por ejemplo, podría elegir limitar un informe a ciertos clientes, categorías, clases de riesgos, o protocolos, o incluso a ciertas acciones de filtrado (permitir, bloquear, etc.). Mediante el filtro de informe también puede dar un nombre y descripción nuevos a la entrada en el Catálogo de informes, especificar que aparezca un logotipo personalizado, y establecer otras opciones generales.

Nota

El uso de un logotipo personalizado requiere cierta preparación antes de definir el filtro de informe. Debe crear el gráfico deseado en un formato de gráficos admitido y colocar el archivo en la ubicación apropiada. Consulte *Personalizar el logotipo del informe*, página 107.

Las opciones específicas disponibles en el filtro dependen del informe seleccionado. Por ejemplo, si seleccionó un informe de información de grupo, como por ejemplo, Principales grupos bloqueados por solicitudes, puede controlar qué grupos aparecerán en el informe, pero no puede elegir usuarios individuales.

El filtro para los informes predefinidos no se puede cambiar, pero es posible editarlo para obtener una copia de un informe predefinido:

1. Seleccione un informe en el Catálogo de informes.

   Si el botón Editar filtro de informe está inhabilitado, continúe con el paso 2.

   Si el botón Editar filtro de informe está habilitado, continúe con el paso 3.
2. Haga clic en **Copiar** para crear una copia que pueda personalizar.

   En el Catálogo de informes aparecerá un duplicado del nombre del informe, con un código anexado para indicar que es una copia.
3. Haga clic en el botón **Editar filtro de informe**.

   Se abrirá la página Filtro de informe, con fichas separadas para manejar los diferentes elementos del informe. Seleccione los elementos que desee en cada ficha; luego haga clic en **Siguiente** para pasar a la ficha siguiente. Para obtener instrucciones detalladas, consulte:

   - *Seleccionar clientes para un informe*, página 103
   - *Seleccionar categorías para un informe*, página 104
   - *Seleccionar protocolos para un informe*, página 105
   - *Seleccionar acciones para un informe*, página 105

- *Establecer las opciones de informe*, página 106

4. En la ficha **Confirmar**, elija si desea ejecutar o programar el informe, además de guardar el filtro de informe. Consulte *Confirmar la definición del filtro de informe*, página 108.

Seleccionar clientes para un informe

Temas relacionados:

- *Seleccionar categorías para un informe*, página 104
- *Seleccionar protocolos para un informe*, página 105
- *Seleccionar acciones para un informe*, página 105
- *Establecer las opciones de informe*, página 106
- *Confirmar la definición del filtro de informe*, página 108

La ficha **Clientes** de la página Informes de presentación > Filtro de informe, le permite controlar qué clientes se incluirán en el informe. Puede seleccionar un tipo de cliente por cada informe. Por ejemplo, no puede seleccionar algunos usuarios y algunos grupos para el mismo informe.

Cuando la definición del informe especifica un tipo de cliente específico, puede elegir clientes de ese tipo o clientes que representen un grupo mayor. Por ejemplo, si está definiendo un filtro para un informe basado en Principales grupos bloqueados por solicitudes, puede seleccionar grupos, dominios o unidades organizativas para el informe, pero no puede seleccionar usuarios individuales.

No se requiere ninguna selección en esta ficha si desea ejecutar un informe sobre todos los clientes pertinentes.

1. Seleccione un tipo de cliente de la lista desplegable.
2. Establezca un número máximo de resultados de búsqueda desde la lista **Limitar la búsqueda**.

   Dependiendo del tráfico en su empresa, puede haber grandes cantidades de usuarios, grupos o dominios en la base de datos de registro. Esta opción administra la longitud de la lista de resultados, así como el tiempo que se requiere para mostrar los resultados de búsqueda.
3. Especifique uno o más caracteres para la búsqueda y luego haga clic en **Buscar**.

   Utilice el asterisco (*) como comodín para representar los caracteres faltantes. Por ejemplo, J*n podría devolver resultados como Jackson, Jan, Jason, Jon, John, etc.

   Defina cuidadosamente su cadena de búsqueda para asegurarse de que todos los resultados deseados se incluyan dentro del número seleccionado para limitar la búsqueda.
4. Resalte una o más entradas en la lista de resultados y haga clic en el botón de flecha derecha (>) para moverlas a la lista **Selección**.

5. Repita los pasos 2 a 4 según sea necesario para realizar búsquedas adicionales y agregar más clientes a la lista Selección.
6. Una vez que haya terminado de hacer sus selecciones, haga clic en **Siguiente** para abrir la ficha Categorías. Consulte *Seleccionar categorías para un informe*, página 104.

Seleccionar categorías para un informe

Temas relacionados:

- *Seleccionar clientes para un informe*, página 103
- *Seleccionar protocolos para un informe*, página 105
- *Seleccionar acciones para un informe*, página 105
- *Establecer las opciones de informe*, página 106
- *Confirmar la definición del filtro de informe*, página 108

La ficha **Categorías** de la página Informes de presentación > Filtro de informe, le permite controlar la información incluida en el informe basándose en categorías o en clases de riesgo. Consulte *Clases de riesgo*, página 41.

No se requiere ninguna selección en esta ficha si desea ejecutar un informe sobre todas las categorías o clases de riesgo pertinentes.

1. Seleccione una clasificación: **Categoría** o **Clase de riesgo**.

   Expanda una categoría principal para mostrar sus subcategorías. Expanda una clase de riesgo para ver una lista de las categorías actualmente asignadas a esa clase de riesgo.

   Si el informe asociado es para una clase de riesgo específico, sólo la clase de riesgo pertinente y las categorías que representa estarán disponibles para selección.

   Nota

   Si selecciona un subconjunto de categorías para la clase de riesgo nombrada en el informe, considere el modificar el título del informe para reflejar sus selecciones.

2. Marque la casilla de cada categoría o clase de riesgo a informar.

   Utilice los botones **Seleccionar todo** y **Borrar todo** ubicados debajo de la lista para minimizar el número de selecciones individuales requeridas.
3. Haga clic en el botón de flecha derecha (>) para mover sus selecciones a la lista **Selección**.

   Si después de marcar una clase de riesgo hace clic en la flecha derecha, todas las categorías asociadas se ubicarán en la lista Selección.

4. Una vez que todas las selecciones estén completas, haga clic en **Siguiente** para abrir la ficha Protocolos. Consulte *Seleccionar protocolos para un informe*, página 105.

Seleccionar protocolos para un informe

Temas relacionados:

- *Seleccionar clientes para un informe*, página 103
- *Seleccionar categorías para un informe*, página 104
- *Seleccionar acciones para un informe*, página 105
- *Establecer las opciones de informe*, página 106
- *Confirmar la definición del filtro de informe*, página 108

La ficha **Protocolos** de la página Informes de presentación > Filtro de informe, le permite controlar qué protocolos se incluirán en el informe.

No se requiere ninguna selección en esta ficha si desea ejecutar un informe sobre todos los protocolos pertinentes.

1. Expanda o contraiga los grupos de protocolos con el icono ubicado al lado del nombre del grupo.
2. Marque la casilla de cada protocolo a informar.

   Utilice los botones **Seleccionar todo** y **Borrar todo** ubicados debajo de la lista para minimizar el número de selecciones individuales requeridas.
3. Haga clic en el botón de flecha derecha (>) para mover sus selecciones a la lista **Selección**.
4. Una vez que todas las selecciones estén completas, haga clic en **Siguiente** para abrir la ficha Acciones. Consulte *Seleccionar acciones para un informe*, página 105.

Seleccionar acciones para un informe

Temas relacionados:

- *Seleccionar clientes para un informe*, página 103
- *Seleccionar categorías para un informe*, página 104
- *Seleccionar protocolos para un informe*, página 105
- *Establecer las opciones de informe*, página 106
- *Confirmar la definición del filtro de informe*, página 108

La ficha **Acciones** de la página Informes de presentación > Filtro de informe, le permite controlar qué acciones de filtrado precisas (dentro de lo que permita el filtro de acceso limitado) se incluirán en el informe. Si el informe especifica un tipo de

acción particular, como Bloqueado, usted estará limitado a seleccionar acciones de ese tipo para el informe.

No se requiere ninguna selección en esta ficha si desea ejecutar un informe sobre todas las acciones pertinentes.

1. Expanda o contraiga los grupos de acciones con el icono ubicado al lado del nombre del grupo.
2. Marque la casilla de cada acción a informar.

   Utilice los botones **Seleccionar todo** y **Borrar todo** ubicados debajo de la lista para minimizar el número de selecciones individuales requeridas.
3. Haga clic en el botón de flecha derecha (>) para mover sus selecciones a la lista **Selección**.
4. Una vez que todas las selecciones estén completas, haga clic en **Siguiente** para abrir la ficha Opciones. Consulte *Establecer las opciones de informe*, página 106.

Establecer las opciones de informe

Temas relacionados:

- *Personalizar el logotipo del informe*, página 107
- *Seleccionar clientes para un informe*, página 103
- *Seleccionar categorías para un informe*, página 104
- *Seleccionar protocolos para un informe*, página 105
- *Seleccionar acciones para un informe*, página 105
- *Establecer las opciones de informe*, página 106
- *Confirmar la definición del filtro de informe*, página 108

Utilice la ficha **Opciones** de la página Informes de presentación > Filtro de informe para configurar varios aspectos del informe.

1. Modifique el **Nombre del catálogo de informes** para que aparezca en el Catálogo de informes. El nombre puede tener hasta 85 caracteres.

   Este nombre no aparece en el informe en sí; sólo se utiliza para identificar la combinación única de formato y filtro de informe en el Catálogo de informes.
2. Modifique el **Título del informe** que aparece en este último. El título puede tener hasta 85 caracteres.
3. Modifique la **Descripción** para que aparezca en el Catálogo de informes. La descripción puede tener hasta 336 caracteres.

   Debe ayudarle a identificar esta combinación única de formato y filtro de informe en el Catálogo de informes.
4. Seleccione un logotipo para que aparezca en el informe.

   En la lista aparecen todos los archivos de imágenes admitidos. Consulte *Personalizar el logotipo del informe*, página 107.

5. Marque la casilla **Guardar como Favorito** para que el informe se muestre en la lista como Favorito.

   El Catálogo de informes muestra un símbolo de estrella al lado de los informes favoritos. Puede seleccionar **Mostrar sólo Favoritos** en la página Catálogo de informes para reducir el número de informes en la lista, lo cual le permite desplazarse más rápidamente a un informe específico.

6. Marque la casilla **Mostrar sólo los principales** y luego ingrese un número del 1 al 20 para limitar el número de elementos a incluir en el informe.

   Esta opción aparece sólo si el informe seleccionado tiene el formato Principales N, diseñado para mostrar un número limitado de elementos. El elemento que se limita depende del informe. Por ejemplo, para un informe Principales categorías visitadas, esta entrada determina cuántas categorías se incluirán en el informe.

7. Una vez que todas las entradas y selecciones estén completas, haga clic en **Siguiente** para abrir la ficha Confirmar. Consulte *Confirmar la definición del filtro de informe*, página 108.

Personalizar el logotipo del informe

Los informes de presentación predefinidos muestran el logotipo de Websense en la esquina superior izquierda. Al copiar un informe predefinido y definir su filtro de informe, puede elegir un logotipo diferente.

1. Cree un archivo de imágenes en uno de los siguientes formatos:

   - .bmp
   - .gif
   - .jfif
   - .jpe
   - .jpg
   - .jpeg
   - .png
   - .ttf

2. Utilice un máximo de 25 caracteres para el nombre del archivo de imágenes, incluida la extensión.
3. Coloque el archivo de imágenes en el siguiente directorio:

   ```
   <install_path>\Manager\ReportingTemplates\images
   ```

   La ruta de instalación predeterminada es C:\Program Files\Websense.

Todos los archivos de imágenes admitidos en este directorio aparecerán automáticamente en la lista desplegable de la ficha Opciones, en la página Filtro de informe. La imagen se amplía o se reduce a escala para que entre en el espacio asignado al logotipo. (Consulte *Establecer las opciones de informe*, página 106.)

Nota

No elimine imágenes que estén activas en filtros de informes de este directorio. Si falta el logotipo especificado, no se podrá generar el informe.

Confirmar la definición del filtro de informe

Temas relacionados:

- *Seleccionar clientes para un informe*, página 103
- *Seleccionar categorías para un informe*, página 104
- *Seleccionar protocolos para un informe*, página 105
- *Seleccionar acciones para un informe*, página 105
- *Establecer las opciones de informe*, página 106

La ficha **Confirmar** de la página Informes de presentación > Filtro de informe muestra el nombre y la descripción que aparecerán en el Catálogo de informes, y le permite elegir cómo proceder.

1. Revise el **Nombre** y la **Descripción**.

   Si se requiere algún cambio, haga clic en **Atrás** para volver a la ficha Opciones, donde puede hacer esos cambios. (Consulte *Establecer las opciones de informe*, página 106.)
2. Indique cómo desea continuar:

Opción	Descripción
Guardar	Guarda el filtro de informe y regresa al Catálogo de informes. Consulte *Informes de presentación*, página 98.
Guardar y ejecutar	Guarda el filtro de informe y abre la página Ejecutar informe. Consulte *Generar informes de presentación*, página 109.
Guardar y programar	Guarda el filtro de informe y abre la página Programar informe. Consulte *Programar informes de presentación*, página 110.

3. Haga clic en **Finalizar** para implementar la selección realizada en el paso 2.

Trabajar con Favoritos

Temas relacionados:

- *Informes de presentación*, página 98
- *Generar informes de presentación*, página 109
- *Programar informes de presentación*, página 110

Puede marcar cualquier informe de presentación, ya sea predefinido o personalizado, como Favorito. Utilice esta opción para identificar los informes que genera más frecuentemente y que desea poder ubicar rápidamente en el Catálogo de informes.

1. En la página **Informes de presentación**, resalte un informe que desee generar frecuentemente o que desee poder localizar rápidamente.
2. Haga clic en **Favorito**.

   Aparecerá un símbolo de estrella al lado de los nombres de informes favoritos de la lista, lo que le permitirá identificarlos rápidamente cuando se muestren todos.
3. Marque la casilla **Mostrar sólo Favoritos** encima del Catálogo de informes para limitar la lista a aquellos marcados como Favoritos. Deseleccione esta casilla para restablecer la lista completa de informes.

Si sus necesidades cambian y un informe Favorito ya no se utiliza con tanta frecuencia, puede quitarle la designación de Favorito.

1. Resalte un informe que muestre el símbolo de estrella de Favorito.
2. Haga clic en **Favorito**.

   El símbolo de estrella se elimina de ese nombre de informe en el Catálogo de informes. Ahora el informe se omite de la lista si usted elige **Mostrar sólo Favoritos**.

Generar informes de presentación

Temas relacionados:

- *Informes de presentación*, página 98
- *Programar informes de presentación*, página 110

El generar un solo informe inmediatamente implica unos pocos pasos, los cuales se muestran abajo.

Nota

Antes de generar un informe de presentación en formato PDF, asegúrese de que Adobe Reader v7.0 o superior esté instalado en la máquina desde la cual accede a Websense Manager.

Antes de generar un informe de presentación en formato XLS, asegúrese de que Microsoft Excel 2003 o superior esté instalado en la máquina desde la cual accede a Websense Manager.

Si no está instalado el software adecuado, tiene la opción de guardar el archivo.

Para crear trabajos con uno o más informes a ejecutar una vez o en un ciclo de repetición con la función de programación de informes de presentación. Consulte *Programar informes de presentación*, página 110.

1. En la página **Informes de presentación**, resalte un informe en el árbol Catálogo de informes y luego haga clic en **Ejecutar**.
2. Seleccione la **Fecha de inicio** y la **Fecha de finalización** para los datos del informe.
3. Seleccione un **Formato de salida** para el informe.

Formato	Descripción
PDF	Portable Document Format. Los archivos PDF se visualizan en Adobe Reader.
HTML	HyperText Markup Language. Los archivos HTML pueden visualizarse directamente en su navegador Internet Explorer o Firefox.
XLS	Hoja de cálculo de Excel . Los archivos XLS se visualizan en Microsoft Excel.

4. Si seleccionó un informe **Principales N**, elija el número de elementos a incluir en el informe.
5. Haga clic en **Ejecutar**.

   Los informes HTML aparecen en el panel de contenido. Si seleccionó una salida en PDF o XLS, tiene la opción de abrir el informe en una ventana aparte o de guardar el informe en el disco.
6. Para imprimir un informe, use la opción imprimir que forma parte del programa que muestra el informe.

   Para obtener los mejores resultados, genere una salida en PDF o XLS para imprimir. Luego, use las opciones de impresión en Adobe Reader o en Microsoft Excel, respectivamente.

Puede guardar un informe que se genera en formato PDF o XLS usando la función Guardar de Adobe Reader o de Microsoft Excel.

Programar informes de presentación

Temas relacionados:

- *Informes de presentación*, página 98
- *Generar informes de presentación*, página 109
- *Ver la lista de trabajos programados*, página 115
- *Copiar un informe de presentación*, página 101

Puede ejecutar informes de presentación según se requieran, o puede utilizar la página **Informes de presentación > Programador** para crear trabajos que definan un programa para ejecutar uno o más informes.

Los informes generados por trabajos programados se distribuyen a uno o más destinatarios por correo electrónico. Al crear trabajos programados, considere si su servidor de correo electrónico podrá manejar el tamaño y la cantidad de archivos de informes adjuntos.

Para acceder al Programador:

- Haga clic en el botón **Programador** en la parte superior de la página Informes de presentación (arriba del Catálogo de informes).
- Al agregar o editar un filtro de informe para un informe, elija **Guardar y programar** en la ficha Confirmar, y luego haga clic en **Finalizar**. (Consulte *Copiar un informe de presentación*, página 101.)
- Haga clic en el enlace del nombre del trabajo en la página Cola de trabajos para editar un trabajo.
- Haga clic en **Agregar** en la página Cola de trabajos para crear un trabajo nuevo.

La página Programador contiene varias fichas para seleccionar los informes a ejecutar, y el programa para ejecutarlos. Para obtener instrucciones detalladas, consulte:

- *Establecer el programa*, página 111
- *Seleccionar informes a programar*, página 113
- *Seleccionar opciones de salida*, página 114
- *Establecer el rango de fechas*, página 113
- *Seleccionar opciones de salida*, página 114

Después de crear trabajos, puede ver una lista que muestra el estado de los mismos y otra información útil. Consulte *Ver la lista de trabajos programados*, página 115.

Establecer el programa

Temas relacionados:

- *Programar informes de presentación*, página 110
- *Seleccionar informes a programar*, página 113
- *Seleccionar opciones de salida*, página 114
- *Establecer el rango de fechas*, página 113

Defina que un trabajo de informes ocurra una vez o en un ciclo de repetición en la ficha **Programar** de la página Informes de presentación > Programador.

Nota

Se aconseja programar los trabajos de informes en diferentes días o a diferentes horas, para evitar la sobrecarga de la base de datos de registro y la disminución del rendimiento a causa de los registros e informes interactivos.

1. Especifique un **Nombre de trabajo** que identifique exclusivamente este trabajo programado.
2. Seleccione un **Patrón de periodicidad** y **Opciones de periodicidad** para el trabajo. Las opciones específicas disponibles dependen del patrón seleccionado.

Patrón	Opciones
Una vez	Especifique la fecha exacta en la que desea ejecutar el trabajo, o haga clic en el icono para seleccionarla de un calendario.
Diaria	Ninguna opción de periodicidad adicional disponible.
Semanal	Marque la casilla del día en que se debe ejecutar el trabajo cada semana.
Mensual	Especifique las fechas durante el mes para la ejecución del trabajo. Las fechas deben ser un número entre el 1 y el 31, y deben estar separadas por comas (1,10,20). Para ejecutar el trabajo en fechas consecutivas cada mes, especifique una fecha de inicio y una de finalización, separadas por un guión (3-5).

3. Debajo de **Hora de programación**, establezca la hora para de inicio para ejecutar el trabajo.

   El trabajo comienza según la hora de la máquina donde se ejecuta Websense Manager.

> **Nota**
> Para comenzar a generar los informes programados hoy, seleccione una hora lo suficientemente tarde como para poder completar la definición del trabajo antes de la hora de inicio.

4. Debajo de **Período de programación**, seleccione una fecha para iniciar el trabajo, y otra para finalizarlo.

Opción	Descripción
No finalizar	El trabajo continúa ejecutándose indefinidamente según el programa establecido. Para discontinuar el trabajo en algún momento en el futuro, edítelo o elimínelo. Consulte *Ver la lista de trabajos programados*, página 115.
Finalizar tras	Seleccione el número de veces que se debe ejecutar el trabajo. Al completar ese número, el trabajo dejará de ejecutarse, pero continuará en la Cola de trabajos hasta que usted lo elimine. Consulte *Ver la lista de trabajos programados*, página 115.
Finalizar el	Establezca la fecha en que el trabajo debe dejar de ejecutarse. En y luego de esta fecha, el trabajo ya no se ejecutará.

5. Haga clic en **Siguiente** para abrir la ficha Informes. Consulte *Seleccionar informes a programar*, página 113.

Seleccionar informes a programar

Temas relacionados:

- *Programar informes de presentación*, página 110
- *Establecer el programa*, página 111
- *Seleccionar opciones de salida*, página 114
- *Establecer el rango de fechas*, página 113

Utilice la ficha **Seleccionar informe** de la página Informes de presentación > Programador para elegir los informes para el trabajo.

1. Resalte un informe para este trabajo en el árbol Catálogo de informes.
2. Haga clic en el botón de flecha derecha (>) para mover ese informe a la lista **Selección**.
3. Repita los pasos 1 y 2 hasta que todos los informes de este trabajo aparezcan en la lista **Selección**.
4. Haga clic en **Siguiente** para abrir la ficha Rango de fechas. Consulte *Establecer el rango de fechas*, página 113.

Establecer el rango de fechas

Temas relacionados:

- *Programar informes de presentación*, página 110
- *Establecer el programa*, página 111
- *Seleccionar informes a programar*, página 113
- *Seleccionar opciones de salida*, página 114

Utilice la ficha **Rango de fechas** de la página Informes de presentación > Programador para establecer el rango de fechas para el trabajo. Las opciones disponibles dependen del **Rango de fechas** que usted seleccione.

Rango de fechas	Descripción
Todas las fechas	Los informes incluyen todas las fechas disponibles en la base de datos de registro. No se requiere ninguna entrada adicional. Cuando esta opción se utiliza para trabajos que se repiten, puede haber información duplicada en los informes en ejecuciones separadas.
Fechas específicas	Elija las fechas exactas de inicio (**De**) y de finalización (**A**) para los informes de este trabajo. Esta opción es ideal para los trabajos que se ejecutan sólo una vez. La elección de esta opción para un programa de repetición resulta en informes duplicados.
Fechas relativas	Utilice las listas desplegables para el número de períodos a informar (Este, Último, Últimos 2, etc.) y para el tipo de período (Días, Semanas o Meses). Por ejemplo, el trabajo podría cubrir las Últimas 2 semanas o Este mes. Semana representa una semana calendario, de domingo a sábado. Mes representa un mes calendario. Por ejemplo, “Esta semana” genera un informe desde el domingo hasta hoy; “Este mes” genera un informe desde el primero del mes hasta hoy; “Última semana” genera un informe que cubre desde el domingo hasta el sábado anteriores, etc. Esta opción es ideal para los trabajos que se ejecutan en un programa de repetición. Le permite manejar cuántos datos aparecerán en cada informe y minimizar la duplicación de los datos en los informes de ejecuciones separadas.

Después de establecer el rango de fechas para el trabajo, haga clic en **Siguiente** para mostrar la ficha Salida. Consulte *Seleccionar opciones de salida*, página 114.

Seleccionar opciones de salida

Temas relacionados:

- *Programar informes de presentación*, página 110
- *Establecer el programa*, página 111
- *Seleccionar informes a programar*, página 113
- *Establecer el rango de fechas*, página 113

Después de seleccionar los informes para un trabajo, utilice la ficha **Salida** para seleccionar el formato de salida y las opciones de distribución.

1. Seleccione el formato de archivo para el informe terminado.

Formato	Descripción
PDF	Portable Document Format. Los destinatarios deben tener Adobe Reader v7.0 o superior para visualizar los informes PDF.
XLS	Hoja de cálculo de Excel. Los destinatarios deben tener Microsoft Excel 2003 o superior para visualizar los informes XLS.

2. Especifique direcciones de correo electrónico para distribuir el informe.

   Especifique cada dirección en una línea aparte.
3. Marque la casilla **Personalizar asunto y cuerpo del correo electrónico**, si lo desea. Luego ingrese el texto personalizado para el **Asunto** y el **Cuerpo** del correo electrónico de distribución de este trabajo.
4. Haga clic en **Guardar trabajo** para guardar e implementar la definición del trabajo, y mostrar la página Cola de trabajos.
5. Revise este trabajo y cualquier otro trabajo programado. Consulte *Ver la lista de trabajos programados*, página 115.

Ver la lista de trabajos programados

Temas relacionados:

- *Informes de presentación*, página 98
- *Programar informes de presentación*, página 110
- *Seleccionar opciones de salida*, página 114
- *Programar informes de investigación*, página 138

La página **Informes de presentación > Cola de trabajos** enumera los trabajos programados creados para los informes de presentación. La lista muestra el estado de cada trabajo, así como la información básica sobre el trabajo, como por ejemplo, con qué frecuencia se ejecuta. Desde esta página, puede agregar y eliminar trabajos programados, suspender temporalmente un trabajo, etc.

(Para revisar los trabajos programados de informes de investigación, consulte *Administrar trabajos programados de informes de investigación*, página 141.)

La lista proporciona la siguiente información de cada trabajo.

Columna	Descripción
Nombre de trabajo	El nombre asignado cuando se creó el trabajo.
Estado	Uno de los siguientes: • ACTIVADO indica un trabajo que se ejecuta según el patrón de periodicidad establecido. • DESACTIVADO indica un trabajo que está inactivo y no se ejecuta.
Periodicidad	El patrón de periodicidad (Una vez, Diaria, Semanal, Mensual) establecido para este trabajo.
Historial	Haga clic en el enlace **Detalles** para abrir la página Historial de trabajos para el trabajo seleccionado. Consulte *Ver el historial de trabajos*, página 117.
Siguiente programado	Fecha y hora para la próxima ejecución.
Propietario	El nombre de usuario del administrador que programó el trabajo.

Utilice las opciones en la página para administrar los trabajos. Algunos de los botones requieren que primero usted marque la casilla al lado del nombre de cada trabajo a incluir.

Opción	Descripción
Enlace del nombre del trabajo	Abre la página Programador, donde usted puede editar la definición del trabajo. Consulte *Programar informes de presentación*, página 110.
Agregar trabajo	Abre la página Programador, donde usted puede definir un trabajo nuevo. Consulte *Programar informes de presentación*, página 110.
Eliminar	Elimina de la Cola de trabajos todos los trabajos que se han marcado en la lista. Una vez que un trabajo se ha eliminado, no se puede restaurar. Para dejar de ejecutar temporalmente un trabajo específico, use el botón **Desactivar**.
Ejecutar ahora	Comienza a ejecutar inmediatamente los trabajos que se han marcado en la lista. Esto se hace adicionalmente a las ejecuciones programadas regularmente.
Activar	Reactiva los trabajos desactivados que se han marcado en la lista. El trabajo comienza a ejecutarse de acuerdo con el programa establecido.
Desactivar	Discontinúa la ejecución de los trabajos activados que están marcados en la lista. Úsela para suspender temporalmente un trabajo que probablemente desee restablecer en el futuro.

Ver el historial de trabajos

Temas relacionados:

- *Programar informes de presentación*, página 110
- *Ver la lista de trabajos programados*, página 115

Utilice la página **Informes de presentación > Cola de trabajos > Historial de Trabajos** para ver información sobre intentos recientes de ejecutar el trabajo seleccionado. La página enumera cada informe por separado, proporcionando la siguiente información.

Columna	Descripción
Nombre del informe	El título impreso en el informe.
Fecha de inicio	Fecha y hora en que el informe comenzó a ejecutarse.
Fecha de finalización	Fecha y hora en que el informe se completó.
Estado	Indicador de si el informe se ejecutó correctamente o falló.
Mensaje	Información relevante sobre el trabajo, como por ejemplo, si el informe se envió exitosamente por correo electrónico.

Informes de investigación

Temas relacionados:

- *Informes resumidos*, página 119
- *Informes resumidos de múltiples niveles*, página 124
- *Informes detallados flexibles*, página 125
- *Informes de Detalle de actividad del usuario*, página 129
- *Informes estándar*, página 134
- *Informes de investigación Favoritos*, página 135
- *Programar informes de investigación*, página 138
- *Informes de casos atípicos*, página 141
- *Generar archivo*, página 142
- *Opciones predeterminadas para la conexión de la base de datos y los informes*, página 338

Utilice la página **Informes > Informes de investigación** para analizar la actividad de filtrado de Internet de una forma interactiva.

Inicialmente, la página principal Informes de investigación muestra un informe resumido de las actividades por clase de riesgo. Trabaje en la vista del informe resumido haciendo clic en los enlaces y elementos disponibles para explorar las áreas de interés y obtener un conocimiento general del uso de Internet que hace su empresa. Consulte *Informes resumidos*, página 119.

Los informes resumidos de múltiples niveles (consulte *Informes resumidos de múltiples niveles*, página 124) y los informes detallados flexibles (consulte *Informes detallados flexibles*, página 125) le permiten analizar la información desde diferentes perspectivas.

Mediante los enlaces ubicados en la parte superior de la página se puede acceder a otras vistas de informes y funciones de informes de investigación. En la tabla a continuación se indica una lista de enlaces y las funciones a las que se accede mediante ellos. (No todos los enlaces están disponibles en todas las páginas.)

Opción	Acción
Usuario por día/mes	Muestra un cuadro de diálogo que le permite definir un informe de la actividad de un usuario específico, cubriendo un día o un mes. Para obtener más información, consulte *Informes de Detalle de actividad del usuario*, página 129.
Informes estándar	Muestra una lista de informes predefinidos para que usted pueda ver rápidamente una combinación de datos específica. Consulte *Informes estándar*, página 134.
Informes favoritos	Le permite guardar el informe actual como Favorito, y muestra una lista de los Favoritos existentes que usted puede generar o programar. Consulte *Informes de investigación Favoritos*, página 135.
Cola de trabajos	Muestra la lista de trabajos de informes de investigación programados. Consulte *Programar informes de investigación*, página 138.
Casos atípicos	Muestra los informes que registran un uso de Internet significativamente diferente del promedio. Consulte *Informes de casos atípicos*, página 141.
Opciones	Muestra la página para seleccionar una base de datos de registro diferente para la generación de informes. La página Opciones también le permite personalizar ciertas funciones de informe, como el período de tiempo que se muestra inicialmente en los informes resumidos y las columnas predeterminadas para los informes detallados. Consulte *Opciones predeterminadas para la conexión de la base de datos y los informes*, página 338.

Opción	Acción
	Haga clic en este botón, a la derecha de los campos Buscar, para exportar el informe actual a un archivo de hoja de cálculo compatible con Microsoft Excel. Se le preguntará si desea abrir o guardar el archivo. Para abrirlo, debe tener instalado Microsoft Excel 2003 o superior. Consulte *Generar archivo*, página 142.
	Haga clic en este botón, a la derecha de los campos Buscar, para exportar el informe actual a un archivo PDF compatible con Adobe Reader. Se le preguntará si desea abrir o guardar el archivo. Para abrirlo, deberá tener instalado Adobe Reader versión 7.0 o superior. Consulte *Generar archivo*, página 142.

Tenga en cuenta que la generación de informes se limita a la información que se ha registrado en la base de datos de registro. Si usted desactiva el registro de nombres de usuario, las direcciones IP o ciertas categorías (consulte *Configuración de Filtering Service para el registro*, página 310), esa información no podrá incluirse. De modo similar, si usted desactiva el registro para ciertos protocolos (consulte *Cómo modificar un filtro de protocolos*, página 52), las solicitudes de esos protocolos no estarán disponibles. Si desea que los informes muestren tanto el nombre de dominio (www.domain.com) como la ruta a una página específica del dominio (/products/productA), debe registrar las URL completas (consulte *Configuración de registro de URL completa*, página 329).

Los informes de investigación de Websense están limitados por el procesador y la memoria disponible en la máquina que ejecuta Websense Manager, así como por algunos otros recursos de la red. Algunos informes grandes pueden requerir mucho tiempo para generarse. El mensaje de progreso incluye una opción para guardar el informe como Favorito, de modo que usted pueda programarlo para que se ejecute a una hora diferente. Consulte *Programar informes de investigación*, página 138.

Informes resumidos

Temas relacionados:

- *Informes resumidos de múltiples niveles*, página 124
- *Informes detallados flexibles*, página 125
- *Informes de Detalle de actividad del usuario*, página 129
- *Informes estándar*, página 134
- *Informes de investigación Favoritos*, página 135
- *Programar informes de investigación*, página 138
- *Informes de casos atípicos*, página 141
- *Generar archivo*, página 142

Inicialmente, la página de informes de investigación brinda un informe resumido del uso realizado por todos los usuarios, por clase de riesgo, mostrando la actividad del día actual a partir de la base de datos de registro. La medición para este gráfico de barras inicial son los Accesos (el número de veces que se solicitó el sitio). Para configurar el período de tiempo para este informe resumido inicial, consulte *Opciones predeterminadas para la conexión de la base de datos y los informes*, página 338.

Cambie rápidamente la información que se provee o reduzca los detalles del informe haciendo clic en los diversos enlaces y opciones disponibles en la página.

1. Seleccione una de las siguientes opciones de la lista **Medida**.

Opción	Descripción
Accesos	El número de veces que se solicitó el URL. Dependiendo de cómo esté configurado Log Server, estos pueden ser accesos verdaderos, que registran en forma separada cada elemento de un sitio solicitado, o pueden ser visitas, que combinan los diferentes elementos del sitio en un solo registro. Consulte *Configuración de los archivos de caché de registro*, página 317.
Ancho de banda [KB]	La cantidad de datos, en kilobytes, contenidos en la solicitud inicial del usuario y en la respuesta del sitio Web. Este es el total combinado de los valores Enviado y Recibido. Tenga en cuenta que algunos productos de integración no envían esta información al software Websense. Dos ejemplos son Check Point FireWall-1 y Cisco PIX Firewall. Si su integración no envía esta información, y Websense Network Agent está instalado, active la opción **Registrar solicitudes HTTP (registro ampliado)** para que el NIC apropiado habilite la generación de informes sobre datos de ancho de banda. Consulte *Cómo establecer la configuración de NIC*, página 351.
Enviados [KB]	El número de kilobytes enviados como solicitud de Internet. Esto representa la cantidad de datos transmitidos, que pueden ser una simple solicitud de una URL, o un envío más importante si el usuario se está registrando para un sitio Web, por ejemplo.

Opción	Descripción
Recibidos [KB]	El número de kilobytes recibidos en respuesta a la solicitud. Esto incluye todos los textos, gráficos y secuencias de comandos (scripts) que conforman el sitio. En los sitios que están bloqueados, el número de kilobytes varía según el software que crea el registro. Cuando los registros los realiza Websense Network Agent, el número de bytes recibidos correspondientes a un sitio bloqueado representan el tamaño de la página de bloqueo de Websense. Si el registro se crea mediante Websense Security Gateway como resultado de la exploración en tiempo real, los kilobytes recibidos representan el tamaño de la página explorada. Para obtener más información sobre la exploración en tiempo real, consulte *Análisis de contenido con las opciones en tiempo real*, página 145. Si los registros los crea otro producto de integración, los kilobytes recibidos para un sitio bloqueado pueden ser cero (0), pueden representar el tamaño de la página de bloqueo, o pueden ser un valor obtenido del sitio solicitado.
Tiempo de navegación	Una estimación de la cantidad de tiempo que se pasa viendo el sitio. Consulte *¿Qué es el tiempo de navegación en Internet?*, página 97.

2. Cambie el modo de agrupación principal del informe seleccionando una opción de la lista **Uso de Internet por**, arriba del informe.

   Las opciones varían según los contenidos de la base de datos de registro y ciertas consideraciones de la red. Por ejemplo, si sólo hay un grupo o dominio en la base de datos de registro, Grupos y Dominios no aparecen en esta lista. De modo similar, si hay demasiados usuarios (más de 5.000) o grupos (más de 3.000), esas opciones no aparecen. (Algunos de estos límites pueden configurarse. Consulte *Opciones de visualización y formato de salida*, página 339.)

3. Haga clic en un nombre en la columna izquierda (o en la flecha al lado del nombre) para que se muestre una lista de opciones, por ejemplo, por usuario, por dominio o por acción.

   Las opciones que aparecen aquí son similares a las que se enumeran en Uso de Internet por, personalizadas para conformar un subconjunto del contenido que se muestra actualmente.

   > **Nota**
   > A veces una opción, como Usuario o Grupo, aparece con letras rojas. En este caso, la selección de dicha opción puede producir un informe muy grande que podría demorar bastante en generarse. Considere el reducir más los detalles antes de seleccionar esa opción.

4. Seleccione unas de estas opciones para generar un informe resumido nuevo que muestre la información seleccionada para la entrada asociada.

Por ejemplo, en un informe resumido de Clase de riesgo, al hacer clic en “por Usuario” debajo de la clase de riesgo Responsabilidad legal, se genera un informe de la actividad de cada usuario en dicha clase.

5. Haga clic en otra entrada en la columna izquierda y luego seleccione una opción para ver más detalles sobre ese elemento en particular.
6. Utilice las flechas al lado de un encabezado de columna para cambiar el orden de los elementos del informe.
7. Controle el informe resumido con las siguientes opciones sobre el gráfico. Luego profundice en los detalles relacionados haciendo clic en los elementos del informe nuevo.

Opción	Acción
Ruta del informe (Usuario > Día)	Al lado de la lista **Uso de Internet por** hay una ruta que muestra las selecciones que crearon el informe actual. Haga clic en cualquier enlace de la ruta para regresar a esa vista de los datos.
Ver	Seleccione un período para el informe: Un día, Una semana, Un mes, o Todos. El informe se actualiza para mostrar los datos para el período seleccionado. Utilice los botones de flecha adyacentes para desplazarse por los datos disponibles, de a un período (día, semana, mes) por vez. Al cambiar esta selección, los campos **Ver desde** se actualizan para reflejar el período de tiempo que se está visualizando. Si elige una fecha específica en los campos Ver desde o mediante el cuadro de diálogo de Favoritos, el campo **Ver** mostrará Personalizado en vez de un período de tiempo.
Ver desde... hasta...	Las fechas en estos campos se actualizan automáticamente para reflejar el período de tiempo que se está visualizando cuando usted hace cambios en el campo **Ver**. Alternativamente, especifique fechas exactas de inicio y finalización para los informes, o haga clic en el icono de calendario para seleccionar las fechas deseadas. Haga clic en el botón de flecha derecha adyacente para actualizar el informe después de seleccionar las fechas.
Gráfico circular / Gráfico de barras	Cuando el gráfico de barras esté activo, haga clic en **Gráfico circular** para mostrar el informe resumido actual como un gráfico circular. Haga clic en la etiqueta de la partición para mostrar las mismas opciones que están disponibles al hacer clic en una entrada de la columna izquierda del gráfico de barras. Cuando el gráfico circular esté activo, haga clic en **Gráfico de barras** para mostrar el informe resumido actual como un gráfico de barras.
Pantalla completa	Seleccione esta opción para mostrar el informe de investigación actual en una ventana aparte, sin los paneles de navegación izquierdo y derecho.

Opción	Acción
Anónimo / Nombres	Haga clic en **Anónimo** para que los informes muestren un número de identificación de usuario asignado internamente cada vez que aparezca un determinado nombre de usuario. Cuando los nombres estén ocultos, haga clic en **Nombres** para mostrar los nombres de usuario en estas ubicaciones. En ciertas circunstancias, los nombres de usuario no se pueden mostrar. Para obtener más información, consulte *Configuración de Filtering Service para el registro*, página 310. Si hace clic en Anónimo y luego pasa a una vista diferente de los datos, como una vista detallada o de casos atípicos, los nombres de usuario seguirán ocultos en el informe nuevo. Sin embargo, para regresar a la vista resumida con los nombres ocultos, debe usar los enlaces de la parte superior del informe, no las rutas de navegación en el anuncio. Si los administradores individuales no deben tener acceso nunca a los nombres de usuario en los informes, asígneles un rol donde los permisos de informe impidan ver los nombres de usuario en los informes de investigación y el acceso a los informes de presentación.
Buscar	Seleccione un elemento del informe en la lista y luego especifique un valor completo o parcial para la búsqueda en el cuadro de texto adyacente. Haga clic en el botón de flecha adyacente para iniciar la búsqueda y mostrar los resultados. Si se especifica una dirección IP parcial, como por ejemplo, 10.5., se buscará en todas las subredes, desde la 10.5.0.0 hasta la 10.5.255.255 en este ejemplo.

8. Agregue un subconjunto de información para todas o algunas entradas de la columna izquierda creando un informe resumido de múltiples niveles. Consulte *Informes resumidos de múltiples niveles*, página 124.
9. Cree un informe en tablas para un elemento específico de la columna izquierda haciendo clic en el número adyacente o en la barra de medición. Este informe detallado puede modificarse para satisfacer sus necesidades específicas. Consulte *Informes detallados flexibles*, página 125.

Informes resumidos de múltiples niveles

Temas relacionados:

- *Informes de investigación*, página 117
- *Informes resumidos*, página 119
- *Informes detallados flexibles*, página 125
- *Informes de Detalle de actividad del usuario*, página 129
- *Informes estándar*, página 134
- *Informes de investigación Favoritos*, página 135
- *Programar informes de investigación*, página 138
- *Informes de casos atípicos*, página 141
- *Generar archivo*, página 142

Los informes resumidos de múltiples niveles muestran un segundo nivel de información para complementar la información principal que se muestra. Por ejemplo, si la vista principal muestra las clases de riesgo, puede definir un segundo nivel para saber qué categorías se han solicitado más dentro de cada clase de riesgo. Como otro ejemplo, si el informe principal muestra solicitudes para cada categoría, puede hacer que se muestren las 5 principales categorías y los 10 usuarios que hicieron más solicitudes a cada una.

Utilice las opciones inmediatamente arriba del informe resumido para crear un informe resumido de múltiples niveles.

1. En la lista **Seleccionar principales**, elija un número para designar cuántas entradas principales (columna izquierda) se informarán. El informe resultante incluye las entradas principales con los valores más grandes. (Si la entrada principal es Día, se muestran las fechas más antiguas.)

   Alternativamente, marque la casilla al lado de las entradas individuales deseadas en la columna izquierda para incluir sólo esas entradas en el informe. El campo **Seleccionar principales** muestra **Personalizado**.
2. En la lista **por**, elija la información secundaria a incluir en el informe.
3. En el campo **Mostrar**, elija el número de resultados secundarios a incluir en el informe por cada entrada principal.
4. Haga clic en **Mostrar resultados** para generar el informe resumido de múltiples niveles.

   El informe resumido se actualiza para mostrar sólo el número de entradas principales seleccionado. Debajo de la barra correspondiente a cada entrada principal, aparece una lista de entradas secundarias.
5. Utilice las flechas al lado de un encabezado de columna para cambiar el orden de los elementos del informe.

Para obtener un informe resumido de un solo nivel, seleccione una opción diferente en **Uso de Internet por**. Alternativamente, haga clic en una de las entradas principales o secundarias y seleccione una opción para generar un informe de investigación nuevo de esa información.

Informes detallados flexibles

Temas relacionados:

- *Informes de investigación*, página 117
- *Informes resumidos*, página 119
- *Informes resumidos de múltiples niveles*, página 124
- *Informes de investigación Favoritos*, página 135
- *Programar informes de investigación*, página 138
- *Informes de casos atípicos*, página 141
- *Generar archivo*, página 142
- *Opciones predeterminadas para la conexión de la base de datos y los informes*, página 338
- *Columnas de los informes detallados flexibles*, página 127

Los informes detallados le ofrecen una vista en tablas de la información de la base de datos de registro. Acceda a la vista del informe detallado desde la página principal después de ver un informe resumido sobre el cual desea más detalles.

Puede solicitar una vista detallada desde cualquier fila. Sin embargo, al solicitar un informe detallado basado en los accesos, es mejor comenzar desde una fila que muestre menos de 100.000 accesos. Si hay más de 100.000 accesos para una fila específica, el valor se mostrará en rojo para alertarle que un informe detallado podría demorar bastante en generarse.

La vista de informe detallada se considera *flexible* porque le permite diseñar su propio informe. Puede agregar o eliminar columnas de información, y cambiar el orden de las columnas que se muestran. La información se ordena de acuerdo con el orden de las columnas. Incluso puede revertir el orden dentro de cualquier columna de ascendente a descendente, o viceversa.

Los informes de investigación de Websense están limitados por el procesador y la memoria disponible en la máquina que ejecuta Websense Manager, así como por algunos otros recursos de la red. Las solicitudes de algunos informes grandes pueden

demorar bastante. Cuando solicite un informe grande, se le ofrecerán opciones para generar el informe sin tiempos de espera.

> **Importante**
> En cualquier lista desplegable o de valores, algunas opciones pueden aparecer en rojo. Este color rojo indica que la selección de esta opción puede generar un informe muy grande. Generalmente es útil reducir más los detalles antes de seleccionar dicha opción.

1. Genere un informe resumido o de múltiples niveles en la página principal de informes de investigación. (Consulte *Informes resumidos*, página 119 o *Informes resumidos de múltiples niveles*, página 124.)
2. Reduzca los resultados para centrarse en la información de interés inmediato.

   Al generar un informe sobre accesos, lo mejor es reducir los resultados a una entrada que muestre menos de 100.000 accesos antes de abrir la vista de informe detallada.
3. Haga clic en el número o en la barra de la fila que desea explorar en más detalle. Para incluir múltiples filas en un informe, marque la casilla de cada fila antes de hacer clic en el número o en la barra de una fila.

   Aparecerá un mensaje emergente de progreso mientras se carga el informe detallado.

   > **Nota**
   > Si el informe requiere mucho tiempo para generarse, considere el guardarlo como un informe Favorito haciendo clic en el enlace que aparece en el mensaje Cargando, y programarlo para que se ejecute más adelante. Consulte *Informes de investigación Favoritos*, página 135.

4. Revise la información en el informe inicial.

   La columna predeterminada varía, dependiendo de si el informe es sobre accesos, ancho de banda o tiempo de navegación, y de las selecciones realizadas en la página Opciones. (Consulte *Opciones predeterminadas para la conexión de la base de datos y los informes*, página 338.)
5. Haga clic en **Modificar informe** en la parte superior de la página.

   La lista **Informe actual** en el cuadro de diálogo Modificar informe muestra qué columnas aparecen en el informe detallado actual.
6. Seleccione un nombre de columna en la lista de **Columnas disponibles** o en la de **Informe actual**, y haga clic en los botones de flecha derecha (>) o izquierda (<) para mover esa columna a la otra lista.

   Elija un máximo de 7 columnas para el informe. La columna que muestra la medida (accesos, ancho de banda, tiempo de navegación) correspondiente al informe resumido inicial siempre aparece como la columna de más a la derecha. No aparece como una opción al modificar el informe.

Consulte *Columnas de los informes detallados flexibles*, página 127 para ver una lista de las columnas disponibles y una descripción de cada una.

7. Seleccione un nombre de columna en la lista **Informe actual** y utilice los botones de flecha arriba y abajo para cambiar el orden de las columnas.

   La columna en la parte superior de la lista Informe actual se convertirá en la columna de la izquierda en el informe.

8. Haga clic en el enlace **Resumen** o **Detalle** arriba del informe para alternar entre las dos formas de visualización.

Opción	Descripción
Resumen	Para mostrar un informe resumido, debe quitar la columna Hora. Los informes resumidos agrupan en una sola entrada todos los registros que comparten un elemento en común. El elemento específico varía de acuerdo con la información que se incluye en el informe. Generalmente, la columna de más a la derecha antes de la medida muestra el elemento resumido.
Detalle	La opción Detalle muestra cada registro como una fila separada. Se puede mostrar la columna Hora.

9. Haga clic en **Enviar** para generar el informe que definió.
10. Utilice las siguientes opciones para modificar el informe que se muestra.
    - Utilice las opciones de **Ver** arriba del informe para cambiar el período de tiempo a cubrir en el informe.
    - Haga clic en la flecha arriba o abajo en un encabezado de columna para revertir el orden de esa columna, y los datos asociados.
    - Utilice los enlaces **Siguiente** y **Anterior** arriba y abajo del informe para mostrar las demás páginas del informe (si hay más). En forma predeterminada, cada página contiene 100 filas, las cuales pueden ajustarse para adecuarse a sus necesidades. Consulte *Opciones de visualización y formato de salida*, página 339.
    - Haga clic en la URL para abrir el sitio Web solicitado en una ventana nueva.
11. Haga clic en **Informe Favorito** si desea guardar el informe para poder generarlo de nuevo rápidamente o en forma periódica (consulte *Guardar un informe como Favorito*, página 136).

Columnas de los informes detallados flexibles

Temas relacionados:

- *Informes detallados flexibles*, página 125
- *Informes de investigación Favoritos*, página 135
- *Programar informes de investigación*, página 138

La tabla de abajo describe las columnas disponibles para los informes detallados (consulte *Informes detallados flexibles*, página 125).

No todas las columnas están disponibles siempre. Por ejemplo, si se muestra la columna Usuario, Grupo no estará disponible; si se muestra Categoría, Clase de riesgo no estará disponible.

Nombre de la columna	Descripción
Usuario	Nombre del usuario que realizó la solicitud. La información de usuario debe estar disponible en la base de datos de registro para que pueda incluirse en los informes. La información de grupo no está disponible en los informes basados en usuarios.
Día	Fecha en que se realizó la solicitud.
Host de URL	Nombre de dominio (también llamado host) del sitio solicitado.
Dominio	Dominio del servicio de directorio del cliente basado en directorios (usuario o grupo, dominio, o unidad organizativa) que realizó la solicitud.
Grupo	Nombre del grupo al cual pertenece el solicitante. En los informes basados en grupos no se proporcionan nombres de usuarios individuales. Si el usuario que solicitó el sitio pertenece a más de un grupo en el servicio de directorio, el informe enumerará múltiples grupos en esta columna.
Clase de riesgo	Clase de riesgo asociado con la categoría a la cual pertenece el sitio solicitado. Si la categoría está en múltiples clases de riesgo, se enumerarán todas las clases de riesgo pertinentes. Consulte *Asignación de categorías a las clases de riesgo*, página 308.
Objeto de directorio	Ruta de directorio del usuario que realizó la solicitud, excluyendo el nombre de usuario. Generalmente, esto resulta en múltiples filas para el mismo tráfico, dado que cada usuario pertenece a múltiples rutas. Si usted utiliza un servicio de directorio no LDAP, esta columna no estará disponible.
Actuación	Acción que realizó el software Websense como resultado de la solicitud; por ejemplo, permitió o bloqueó la categoría.
Servidor de origen	Dirección IP de la máquina que envía solicitudes a Filtering Service. Esta es la máquina que ejecuta ya sea el producto de integración o Websense Network Agent.
Protocolo	Protocolo de la solicitud.
Grupo de protocolos	Grupo de la base de datos principal donde se ubica el protocolo solicitado.
IP de origen	Dirección IP de la máquina desde donde se realizó la solicitud.
IP de destino	Dirección IP del sitio solicitado.
URL completa	Nombre de dominio y ruta del sitio solicitado (ejemplo: http://www.mydomain.com/products/itemone/). Si usted no registra URL completas, esta columna estará en blanco. Consulte *Configuración de registro de URL completa*, página 329.

Nombre de la columna	Descripción
Mes	Mes calendario en que se realizó la solicitud.
Puerto	Puerto TCP/IP a través del cual el usuario se comunicó con el sitio.
Ancho de banda	La cantidad de datos, en kilobytes, contenidos en la solicitud inicial del usuario y en la respuesta del sitio Web. Este es el total combinado de los valores Enviado y Recibido. Tenga en cuenta que algunos productos de integración no envían esta información al software Websense. Dos ejemplos son Check Point FireWall-1 y Cisco PIX Firewall. Si su integración no envía esta información, y Websense Network Agent está instalado, active la opción **Registrar solicitudes HTTP (registro ampliado)** para que el NIC apropiado habilite la generación de informes sobre datos de ancho de banda. Consulte *Cómo establecer la configuración de NIC*, página 351.
Bytes enviados	Número de bytes enviados como solicitud de Internet. Esto representa la cantidad de datos transmitidos, que pueden ser una simple solicitud de una URL, o un envío más importante si el usuario se está registrando para un sitio Web, por ejemplo.
Bytes recibidos	Número de bytes recibidos de Internet en respuesta a la solicitud. Esto incluye todos los textos, gráficos y secuencias de comandos (scripts) que conforman el sitio. En los sitios que están bloqueados, el número de bytes varía según el software que crea el registro. Cuando los registros los realiza Websense Network Agent, el número de bytes recibidos correspondientes a un sitio bloqueado representan el tamaño de la página de bloqueo. Si el registro se crea mediante Websense Security Gateway como resultado de la exploración en tiempo real, los bytes recibidos representan el tamaño de la página explorada. Para obtener más información sobre la exploración en tiempo real, consulte *Análisis de contenido con las opciones en tiempo real*, página 145. Si los registros los crea otro producto de integración, los bytes recibidos para un sitio bloqueado pueden ser cero (0), pueden representar el tamaño de la página de bloqueo, o pueden ser un valor obtenido del sitio solicitado.
Hora	Hora del día a la que se solicitó el sitio; se muestra en el formato HH:MM:SS, usando un reloj de 24 horas.
Categoría	Categoría bajo la cual se filtró la solicitud. Puede ser una categoría de la base de datos principal de Websense o una categoría personalizada.

Informes de Detalle de actividad del usuario

Temas relacionados:

- *Informes de investigación*, página 117

Haga clic en el enlace **Usuario por día/mes** para generar un informe de Detalle de actividad del usuario sobre un usuario. Este informe brinda una interpretación gráfica de la actividad de Internet del usuario, ya sea en un solo día o en un mes completo.

Primero, genere un informe sobre un usuario específico durante un día específico. A partir de ese informe, puede generar un informe sobre la actividad del mismo usuario durante un mes completo. Para obtener instrucciones detalladas, consulte:

- *Detalle de actividad del usuario por día*, página 130
- *Detalle de actividad del usuario por mes*, página 131

Detalle de actividad del usuario por día

Temas relacionados:

- *Informes de investigación*, página 117
- *Informes de Detalle de actividad del usuario*, página 129
- *Detalle de actividad del usuario por mes*, página 131

El informe de Detalle de actividad del usuario por día ofrece una vista detallada de la actividad de un usuario específico durante un día.

1. Seleccione **Usuario por día/mes** en la parte superior de la página principal. Se muestra el cuadro de diálogo Detalle de usuario por día.
2. Ingrese un nombre de usuario, o una parte del nombre, en el campo **Buscar un usuario** y haga clic en **Buscar**.

   La búsqueda muestra una lista desplazable de hasta 100 nombres de usuario coincidentes de la base de datos de registro.
3. Haga una selección de la lista **Seleccionar usuario**.
4. En el campo **Seleccionar día**, acepte la fecha de la última actividad que aparece en forma predeterminada o elija una fecha diferente.

   Puede escribir la fecha nueva o hacer clic en el icono de calendario para seleccionar una fecha. El cuadro de selección del calendario indica el rango de fechas cubiertas por la base de datos de registro activa.
5. Haga clic en **Ir a Usuario por día** para ver un informe detallado de la actividad de ese usuario en la fecha solicitada.

   El informe inicial muestra una línea temporal de la actividad del usuario en incrementos de 5 minutos. Cada solicitud aparece como un icono, que corresponde a una categoría de la base de datos principal de Websense. Un solo icono representa todas las categorías personalizadas. (El color de los iconos se corresponde con los grupos de riesgo que se muestran en los informes de Actividad del usuario por mes. Consulte *Detalle de actividad del usuario por mes*, página 131.)

   Lleve el puntero del ratón sobre un icono para ver la hora exacta, la categoría y la acción de la solicitud asociada.

los controles que se enumeran abajo para modificar la forma en que se muestra el informe o para ver una leyenda.

Opción	Descripción
Día anterior / Día siguiente	Muestra la actividad de Internet de este usuario en el día calendario anterior o siguiente.
Vista de tabla	Muestra una lista de cada URL solicitada, dando la fecha y hora de la solicitud, la categoría y la acción realizada (bloqueada, permitida, u otra).
Vista detallada	Muestra la vista gráfica inicial del informe.
Agrupar accesos similares / Ver todos los accesos	Combina en una sola fila todas las solicitudes que ocurrieron con una diferencia de 10 segundos o menos entre sí y tienen el mismo dominio, categoría y acción. Esto resulta en una vista resumida y más corta de la información. El umbral de tiempo estándar es de 10 segundos. Si necesita cambiar este valor, consulte *Opciones de visualización y formato de salida*, página 339. Después de hacer clic en el enlace, éste se convierte en Ver todos los accesos, lo que restablece la lista original de cada solicitud.
Vista de categorías	Exhibe una lista de cada categoría en el informe actual, mostrando tanto el nombre de la categoría como el icono que la representa. Controle qué categorías aparecerán en el informe marcando las casillas de las categorías a incluir. Luego haga clic en **Aceptar** para actualizar el informe de acuerdo con sus selecciones.

6. Haga clic en **Detalle de actividad del usuario por mes**, arriba del informe, para ver la actividad del mismo usuario en todo el mes. Para obtener más información, consulte *Detalle de actividad del usuario por mes*, página 131.

Detalle de actividad del usuario por mes

Temas relacionados:

- *Informes de investigación*, página 117
- *Informes de Detalle de actividad del usuario*, página 129
- *Detalle de actividad del usuario por día*, página 130
- *Asociar categorías*, página 132

Mientras el informe de Detalle de actividad del usuario por día esté abierto, puede alternar para ver la actividad mensual de ese usuario.

1. Abra un informe de Detalle de actividad del usuario por día. Consulte *Detalle de actividad del usuario por día*, página 130.

2. Haga clic en **Detalle de actividad del usuario por mes** en la parte superior.

   El informe nuevo muestra una imagen de calendario, donde el área de cada día muestra pequeños bloques de color que representan la actividad de Internet del usuario en ese día. Las solicitudes a sitios en categorías personalizadas se muestran como bloques grises.

3. Haga clic en **Leyenda de categorías de base de datos** en la parte superior izquierda para ver cómo los colores representan un riesgo potencial de bajo a alto para el sitio solicitado.

   Las asignaciones de categorías son fijas y no pueden cambiarse. Consulte *Asociar categorías*, página 132.

4. Haga clic en **Anterior** o **Siguiente** para ver la actividad de Internet de este usuario en el mes anterior o siguiente.

Asociar categorías

Temas relacionados:

- *Informes de investigación*, página 117
- *Informes de Detalle de actividad del usuario*, página 129
- *Detalle de actividad del usuario por mes*, página 131

La siguiente lista identifica qué categorías representa cada color en los informes de Actividad del usuario por día y Detalle de actividad del usuario por mes.

Tenga en cuenta que los nombres de las categorías en la base de datos principal están sujetos a cambio. También pueden agregarse o eliminarse categorías en cualquier momento.

Color	Categorías
Gris	Categorías personalizadas Tráfico no HTTP
Azul oscuro	**Negocios y economía** y todas sus subcategorías **Educación** y todas sus subcategorías **Salud** **Tecnología informática**, incluyendo las subcategorías Motores de búsqueda, Portales y Web Hosting **Varios**, incluyendo subcategorías como Redes de entrega de contenido, Contenido dinámico, Imágenes (medios), Servidores de imágenes, y Direcciones IP privadas **Productividad**/Publicidades

Color	Categorías
Celeste	**Drogas**/Medicamentos con receta **Gobierno** y su subcategoría Ejército **Tecnología informática**/Sitios de traducción de URL **Varios**, sólo la categoría principal **Noticias y medios**, sólo la categoría principal **Eventos especiales**
Amarillo Verde	**Aborto** y todas sus subcategorías **Material adulto**/Educación sexual **Ancho de banda**, incluyendo las subcategorías Radio y TV por Internet, Almacenamiento personal y respaldo de seguridad en la red, y Transmisiones multimedia **Entretenimiento**, incluyendo su subcategoría MP3 **Juegos** **Gobierno**/Organizaciones políticas **Tecnología informática**/Seguridad informática **Comunicación por Internet**/Correo electrónico basado en la Web **Varios**/Servidores de descarga de archivos **Varios**/Errores de red **Noticias y medios**/Publicaciones alternativas **Productividad**, incluyendo sus subcategorías Mensajería instantánea, Tableros y clubes de mensajes, y Corretaje en bolsa y comercio de valores en línea **Religión** y sus subcategorías Religiones no tradicionales, Ocultismo y folklore, y Religiones tradicionales **Seguridad**, sólo la categoría principal **Compras** y todas sus subcategorías **Organizaciones sociales** y todas sus subcategorías **Sociedad y estilos de vida**, incluyendo sus subcategorías Interés para gays, lesbianas o bisexuales, Hobbies, Sitios Web personales, y Restaurantes y comida **Deportes** y todas sus subcategorías **Viajes** **Definido por el usuario** **Vehículos**

Color	Categorías
Naranja	**Material adulto**/Desnudos **Grupos de defensa** **Ancho de bnada**/Telefonía por Internet **Drogas** y sus subcategorías Drogas de abuso, Marihuana, y Suplementos y compuestos libres **Tecnología informática**/Elusión con proxy **Comunicación en Internet** y su subcategoría Chat en la Web **Búsqueda de empleo** **Varios**/Sin categorizar **Productividad**, incluyendo las subcategorías Descarga de freeware y software, y Pagar por navegar **Religión** **Sociedad y estilos de vida**, incluyendo las subcategorías Alcohol y tabaco, y Relaciones personales y citas **Mal gusto** **Armas**
Rojo	**Material adulto** y sus subcategorías: Contenido adulto, Lencería y trajes de baño, y Sexo **Ancho de banda**/Intercambio de archivos P2P **Juegos de apuestas** **Ilegal o cuestionable** **Tecnología informática**/Hackers **Militancia y extremistas** **Racismo y odio** **Seguridad**, incluyendo las subcategorías Keyloggers, Sitios Web maliciosos, Phishing y Spyware **Violencia**

Informes estándar

Temas relacionados:

- *Informes de investigación*, página 117
- *Informes de investigación Favoritos*, página 135
- *Programar informes de investigación*, página 138

Los informes estándar le permiten ver rápidamente un conjunto específico de información sin usar el proceso de reducción de resultados.

1. Haga clic en el enlace **Informes estándar** en la página principal de Informes de investigación.

2. Elija el informe que contiene la información deseada. Están disponibles los siguientes informes.

Niveles de actividad más altos
• ¿Qué usuarios tienen el mayor número de accesos? • 10 principales usuarios de las 10 URL más visitadas • Actividad de los 5 principales usuarios en compras, entretenimiento y deportes • 5 principales URL de las 5 categorías más visitadas
Consumo de ancho de banda más alto
• Qué grupos consumen el mayor ancho de banda • Grupos que consumen el mayor ancho de banda en transmisiones multimedia • Informe de URL detallado sobre usuarios por pérdida de ancho de banda de red • 10 principales grupos para categorías de ancho de banda
Mayor tiempo conectados
• Qué usuarios pasaron más tiempo conectados • Qué usuarios pasaron más tiempo en sitios de las categorías de productividad
Los más bloqueados
• ¿Qué usuarios han sido los más bloqueados? • ¿Qué sitios han sido los más bloqueados? • Informe de URL detallado sobre los usuarios bloqueados • 10 principales categorías bloqueadas
Riesgo de seguridad más alto
• Principales categorías que representan un riesgo de seguridad • Principales usuarios de protocolo P2P • Principales usuarios de sitios en categorías de seguridad • URL de las 10 principales máquinas con actividad spyware
Responsabilidad legal
• Riesgo de responsabilidad legal por categoría • Principales usuarios de las categorías de contenido para adultos

3. Vea el informe que aparece.
4. Si desea ejecutarlo en forma periódica, guárdelo como Favorito. Consulte *Informes de investigación Favoritos*, página 135.

Informes de investigación Favoritos

Temas relacionados:

- *Informes de investigación*, página 117
- *Programar informes de investigación*, página 138

Puede guardar la mayoría de los informes de investigación como **Favoritos**. Esto incluye los informes que usted genere reduciendo los resultados a la información específica, los informes estándar y los informes detallados que ha modificado para satisfacer sus necesidades específicas. Luego, ejecute el informe Favorito en cualquier momento, o prográmelo para que se ejecute en ciertos días y horarios específicos.

En las organizaciones que utilizan la administración delegada, el permiso para guardar y programar Favoritos lo establece el superadministrador. Los administradores a los que se les otorga este permiso pueden ejecutar y programar sólo los Favoritos que guardaron; no tienen acceso a los Favoritos guardados por otros administradores.

Para obtener instrucciones detalladas sobre cómo trabajar con los informes favoritos, consulte:

- *Guardar un informe como Favorito*, página 136
- *Generar o eliminar un informe Favorito*, página 137
- *Modificar un informe Favorito*, página 137

Guardar un informe como Favorito

Temas relacionados:

- *Informes de investigación Favoritos*, página 135
- *Modificar un informe Favorito*, página 137

Utilice el siguiente procedimiento para guardar un informe como Favorito.

1. Genere un informe de investigación con el formato y la información deseados.
2. Haga clic en **Informes favoritos**.
3. Acepte o modifique el nombre que muestra Websense Manager.

   El nombre puede contener letras, números y caracteres de subrayado (_). No se pueden utilizar espacios ni otros caracteres especiales.
4. Haga clic en **Agregar**.

   El nombre del informe se agregará a la lista de Favoritos.
5. Seleccione un informe en esta lista y luego seleccione una opción para administrarlo. Dependiendo de la opción que elija, consulte:
   - *Generar o eliminar un informe Favorito*, página 137
   - *Programar informes de investigación*, página 138

Generar o eliminar un informe Favorito

Temas relacionados:

- *Informes de investigación Favoritos*, página 135
- *Modificar un informe Favorito*, página 137

Puede generar un informe Favorito en cualquier momento, o eliminar uno que se ha vuelto obsoleto.

1. Haga clic en **Informes favoritos** para ver una lista de los informes guardados como Favoritos.

   Nota
   Si su organización utiliza la administración delegada, esta lista no incluye los informes favoritos guardados por otros administradores.

2. Seleccione el informe deseado de la lista.

   Si el informe deseado no se ha guardado como Favorito, consulte *Guardar un informe como Favorito*, página 136.

3. Dependiendo de su necesidad:
   - Haga clic en **Ejecutar ahora** para generar y mostrar inmediatamente el informe seleccionado.
   - Haga clic en **Programar** para programar un informe más adelante o en forma periódica. Para obtener más información, consulte *Programar informes de investigación*, página 138.
   - Haga clic en **Eliminar** para quitar el informe de la lista de Favoritos.

Modificar un informe Favorito

Temas relacionados:

- *Informes de investigación*, página 117
- *Informes de investigación Favoritos*, página 135

Puede crear fácilmente un informe Favorito nuevo similar a un informe Favorito existente, de la siguiente manera.

1. Haga clic en **Informes favoritos** para ver una lista de los informes guardados como Favoritos.

   > **Nota**
   > Si su organización utiliza la administración delegada, esta lista no incluye los informes favoritos guardados por otros administradores.

2. Seleccione y ejecute el informe Favorito existente que más se parezca al informe nuevo que desea crear. (Consulte *Generar o eliminar un informe Favorito*, página 137.)
3. Modifique el informe que se muestra según lo desee.
4. Haga clic en **Informes favoritos** para guardar el informe revisado como un informe Favorito con un nombre nuevo. (Consulte *Guardar un informe como Favorito*, página 136.)

Programar informes de investigación

Temas relacionados:

- *Informes de investigación Favoritos*, página 135
- *Guardar un informe como Favorito*, página 136
- *Administrar trabajos programados de informes de investigación*, página 141

Primero debe guardar un informe de investigación como Favorito si luego desea programarlo para que se ejecute en otro momento o en un ciclo de repetición. Cuando se ejecuta el trabajo del informe programado , los informes resultantes se envían por correo electrónico a los destinatarios que usted designe. Al crear trabajos programados, considere si su servidor de correo electrónico podrá manejar el tamaño y la cantidad de archivos de informes adjuntos.

Los archivos de informes programados se almacenan en el siguiente directorio:

```
<install_path>\webroot\Explorer\<name>\
```

La ruta de instalación predeterminada es C:\Program Files\Websense. Si el trabajo programado tiene sólo un destinatario, el <nombre> es la primera parte de la dirección

de correo electrónico (antes de la @). En caso de haber múltiples destinatarios, los informes se guardan en un directorio llamado Otro.

> **Nota**
>
> Los informes guardados a partir de un trabajo de repetición utilizan el mismo nombre de archivo todas las veces. Si desea guardar los archivos por no más de un ciclo, asegúrese de cambiar el nombre del archivo o copie este último en otra ubicación.
>
> Dependiendo del tamaño y el número de informes programados, este directorio podría volverse muy grande. Asegúrese de limpiarlo periódicamente, eliminando los archivos de informes innecesarios.

1. Guarde uno o más informes como Favoritos. (Consulte *Guardar un informe como Favorito*, página 136.)
2. Haga clic en **Informes favoritos** para ver una lista de los informes guardados como Favoritos.

   > **Nota**
   >
   > Si su organización utiliza roles de administración delegada, esta lista no incluye los informes favoritos guardados por otros administradores.

3. Resalte hasta 5 informes para que se ejecuten como parte del trabajo.
4. Haga clic en **Programar** para crear un trabajo de informes programado, y luego complete la información solicitada en la página Programar informe.

   Se aconseja programar los trabajos de informes en diferentes días o a diferentes horas, para evitar la sobrecarga de la base de datos de registro y la disminución del rendimiento a causa de los registros e informes interactivos.

Campo	Descripción
Periodicidad	Seleccione la frecuencia (Una vez, Diaria, Semanal, Mensual) para ejecutar el trabajo de informes.
Fecha de inicio	Elija el día de la semana o la fecha calendario para ejecutar el trabajo la primera (o única) vez.
Hora de ejecución	Establezca la hora del día para ejecutar el trabajo.
Enviar a	Utilice el campo **Direcciones de correo adicionales** para agregar las direcciones apropiadas a esta lista. Resalte una o más direcciones de correo electrónico que deban recibir los informes del trabajo. (Asegúrese de deseleccionar las que no deban recibir los informes.)

Campo	Descripción
Direcciones de correo adicionales	Especifique una dirección de correo electrónico y luego haga clic en **Agregar** para colocarla en la lista **Enviar a**. La nueva dirección de correo electrónico queda automáticamente resaltada con las demás direcciones seleccionadas.
Personalizar asunto y texto del cuerpo del correo electrónico	Marque esta casilla si desea personalizar la línea de asunto y el texto del cuerpo de la notificación. Si esta casilla no está marcada, se utilizarán el asunto y el texto del cuerpo predeterminados.
Asunto del correo electrónico	Ingrese el texto que debe aparecer en la línea de asunto del correo electrónico cuando se distribuyan los informes programados. El asunto predeterminado del correo electrónico dice: Trabajo programado de informes de investigación
Texto del correo electrónico	Ingrese el texto que se debe agregar al mensaje de correo electrónico para la distribución de los informes programados. El correo electrónico dice lo siguiente, y su texto irá en lugar de <TEXTO PERSONALIZADO>. El programador de informes ha generado el o los archivos adjuntos el <fecha hora>. <TEXTO PERSONALIZADO> Para visualizar los informes generados, haga clic en los siguientes enlaces. Nota: El enlace no funcionará si el destinatario no tiene acceso al servidor Web desde el que se ha enviado el trabajo.
Nombre de trabajo programado	Asigne un nombre único para el trabajo programado. El nombre identifica este trabajo en la Cola de trabajos. Consulte *Administrar trabajos programados de informes de investigación*, página 141.
Formato de salida	Elija el formato de archivo para los informes programados: **PDF**: Los archivos Portable Document Format se visualizan en Adobe Reader. **Excel**: Los archivos de hojas de cálculo de Excel se visualizan en Microsoft Excel.
Rango de fechas	Establezca el rango de fechas a cubrir por los informes de este trabajo. **Todas las fechas**: todas las fechas disponibles en la base de datos de registro. **Relativas**: Elija un período de tiempo (Días, Semanas o Meses) y el período específico a incluir (Este, Último, Últimos 2, etc.). **Específicas**: establezca fechas específicas o un rango de fechas para los informes de este trabajo.

5. Haga clic en **Siguiente** para mostrar la página Programar confirmación.

6. Haga clic en **Guardar** para guardar sus selecciones e ir a la página Cola de trabajos (consulte *Administrar trabajos programados de informes de investigación*, página 141).

Administrar trabajos programados de informes de investigación

Temas relacionados:

- *Informes de investigación*, página 117
- *Programar informes de presentación*, página 110

Cuando usted crea un trabajo programado de informes de investigación, aparece la página **Cola de trabajos**, que muestra el trabajo nuevo y una lista de los trabajos programados existentes. También puede acceder a la página haciendo clic en el enlace **Cola de trabajos** en la página principal de informes de investigación.

> **Nota**
> Si su organización utiliza la administración delegada, esta página no muestra los trabajos programados por otros administradores.

La sección **Detalle de informes programados** enumera todos los trabajos programados en el orden en que se crearon, con una descripción general del programa definido y el estado del trabajo. También están disponibles las siguientes opciones.

Opción	Descripción
Editar	Muestra el programa definido para este trabajo y le permite modificarlo, según sea necesario.
Eliminar	Elimina el trabajo y agrega una entrada a la sección registro de estado, mostrando el trabajo como Eliminado.

La sección **Registro de estado** enumera todos los trabajos que se modificaron en alguna forma, mostrando la hora de inicio programada del trabajo, la hora de finalización real, y el estado.

Haga clic en **Borrar registro de estado** para eliminar todas las entradas de esta sección.

Informes de casos atípicos

Temas relacionados:

- *Informes de investigación*, página 117
- *Informes resumidos*, página 119

Un informe de Casos atípicos muestra qué usuarios tienen la actividad de Internet más inusual en la base de datos. El software Websense calcula la actividad promedio de todos los usuarios por categoría, por día, por acción (a veces llamada "disposición") y por protocolo. Luego muestra la actividad de usuario con la variación estadísticamente más importante del promedio. La variación se calcula como el desvío estándar de la media.

1. En la página principal de informes de investigación, genere un informe resumido que muestre la información sobre la cual desee ver casos atípicos. Las selecciones del informe subrayadas y que se muestran en azul al lado del campo Uso de Internet por, se reflejan en el informe de casos atípicos.

   Por ejemplo, para ver los casos atípicos por accesos para una categoría en particular, seleccione **Categoría** en la lista **Uso de Internet por**, y seleccione **Accesos** como la **Medida**.

   > **Nota**
   > No pueden generarse informes de casos atípicos para el tiempo de navegación. Si usted parte de un informe resumido que muestra el tiempo de navegación, el informe de casos atípicos se basa en los accesos.

2. Haga clic en **Ver casos atípicos**.

   Las filas se ordenan en forma descendente, con la variación más alta al comienzo. Cada fila muestra:

   - El total (de accesos o de ancho de banda) para el usuario, la categoría, el protocolo, el día y la acción.
   - El promedio (de accesos o de ancho de banda) para todos los usuarios, para esa categoría, protocolo, día y acción.
   - Variación del promedio para el usuario.

3. Para ver la actividad de un usuario individual en esta categoría en el transcurso del tiempo, haga clic en el nombre de usuario.

   Por ejemplo, si la actividad de un usuario es notablemente alta en un día específico, haga clic en ese nombre de usuario para ver un informe más detallado sobre la actividad general del usuario.

Generar archivo

Temas relacionados:

- *Informes de investigación*, página 117
- *Imprimir informes de investigación*, página 143

Después de generar un informe de investigación, puede usar los botones arriba del informe para guardarlo como un archivo. El botón que elija determinará el formato del archivo.

Opción	Descripción
	Guarda el informe en formato XLS . Si la máquina desde la cual está utilizando Websense Manager tiene instalado Microsoft Excel 2003 o superior, se le preguntará si desea ver o guardar el informe. De lo contrario, se le pedirá que seleccione un directorio y un nombre de archivo para el informe guardado. Utilice las opciones de Microsoft Excel para imprimir, guardar o enviar el informe por correo electrónico.
	Genera un informe en formato PDF. Si la máquina desde la cual está utilizando Websense Manager tiene instalado Adobe Reader v7.0 o superior, se le preguntará si desea ver o guardar el informe. De lo contrario, se le pedirá que seleccione un directorio y un nombre de archivo para el informe guardado. Utilice las opciones de Adobe Reader para imprimir, guardar o enviar el informe por correo electrónico.

Imprimir informes de investigación

Temas relacionados:

- *Informes de investigación*, página 117
- *Generar archivo*, página 142

Puede imprimir los informes de investigación:

- Utilizando la función de impresión del navegador Web mientras se muestra el informe.
- Creando un archivo PDF o XLS y luego utilizando la función de impresión de Adobe Reader o Microsoft Excel (consulte *Generar archivo*, página 142).

Si bien los informes están configurados para imprimirse correctamente desde el navegador, le aconsejamos realizar una impresión de prueba para controlar el resultado.

Los informes de Detalle de actividad del usuario por mes están configurados para imprimirse en modo horizontal. Todos los demás informes están configurados para el modo vertical.

Cuando usted diseña su propio informe (consulte *Informes detallados flexibles*, página 125), los anchos de columna varían según la información incluida. Si el ancho del informe supera las 8 1/2 pulgadas, la orientación de la página cambia a horizontal.

El contenido de la página puede ser de 7 1/2 pulgadas o de 10 pulgadas de ancho. En el caso del tamaño A4, los márgenes son algo más angostos pero se mantienen dentro del rango de impresión. (El tamaño predeterminado del papel es Carta, u 8 1/2 x 11

pulgadas. Si trabaja con papel A4, asegúrese de cambiar esta configuración en el archivo wse.ini. Consulte *Opciones de visualización y formato de salida*, página 339.)

Acceder a ver actividad propia

Temas relacionados:

- *Informes de investigación*, página 117
- *Configuración de las preferencias de informes*, página 310
- *Actividad propia*, página 342

La función de Websense Ver actividad propia le permite evaluar sus propias actividades de navegación en Internet y ajustarlas, según sea necesario, para que cumplan con las pautas de la organización. También responde a las normas gubernamentales que exigen a las empresas que permitan a los usuarios poder ver el tipo de información que se recopila.

Si la función Ver actividad propia está habilitada en su empresa, acceda a la misma desde su navegador:

1. Ingrese la URL provista por su administrador de Websense, o haga clic en el enlace Ver actividad propia en la página principal de inicio de sesión de Websense Manager para acceder a la página de inicio de sesión para ver la actividad propia.
2. Si **Policy Server** muestra una lista desplegable, elija la dirección IP del Policy Server que registra la información de su actividad en Internet.

   Póngase en contacto con el administrador de Websense para obtener ayuda.
3. Ingrese el **Nombre de usuario** y la **Contraseña** que utiliza para iniciar sesión en la red.
4. Haga clic en **Iniciar sesión**.

Websense Manager abre un informe de investigación que muestra su actividad en Internet por clase de riesgo. Haga clic en los distintos enlaces y elementos de la página para acceder a otras opciones de vistas alternativas de la información almacenada sobre su actividad. Si necesita ayuda para trabajar con los informes, consulte el sistema de **Ayuda**.

7 Análisis de contenido con las opciones en tiempo real

Temas relacionados:

- *Opciones de exploración*, página 147
- *Categorización de contenido y exploraciones para detectar amenazas*, página 148
- *Exploración de archivos*, página 149
- *Eliminación de contenido innecesario*, página 151
- *Informes sobre la actividad de exploración en tiempo real*, página 153

El software de filtrado de Websense filtra la actividad de Internet de acuerdo con su política activa y la información almacenada en la base de datos principal. Si está suscrito a Websense Content Gateway o a Websense Web Security Gateway, también puede analizar contenido de sitios Web y archivos en tiempo real.

Según la suscripción que tenga, hay disponibles 2 opciones de análisis en tiempo real: categorización de contenido y exploración en tiempo real de seguridad.

- Utilice la **categorización de contenido** para revisar el contenido de las URL que no estén bloqueadas (en base a su política activa y en la categorización de la base de datos principal de Websense de la URL) y devuelva una categoría para utilizar en el filtrado.
- Si está suscrito a Websense Web Security Gateway, hay disponibles 3 opciones de **exploración en tiempo real de seguridad**.
  - La **exploración de contenido** observa el contenido Web para buscar amenazas a la seguridad como phishing, redireccionamiento de URL, exploits de Web y elusión con proxy.
  - La **exploración de archivos** inspecciona el contenido de los archivos para determinar una categoría de amenaza, como virus, caballos de Troya o gusanos.
  - La **eliminación de contenido innecesario** elimina contenido activo de páginas Web solicitadas.

Cuando se activa alguna de estas opciones, se analizan únicamente los sitios que **no** están bloqueados en base a su política activa y la categorización que tengan en la base

de datos principal de Websense. Para obtener más información, consulte *Opciones de exploración*, página 147.

> **Importante**
>
> Los filtros de acceso limitado y las URL no filtradas reemplazan a la categorización en tiempo real.
>
> Si un usuario solicita un sitio en un filtro de acceso limitado activo (consulte *Cómo restringir usuarios a una lista definida de sitios de Internet*, página 168) o la lista de URL sin filtrar (consulte *Cómo redefinir el filtrado para sitios específicos*, página 182), se permite la solicitud, aún cuando se realiza una exploración en tiempo real y se encuentran amenazas.

Para aprovechar estas funciones de seguridad en tiempo real, ingrese una clave de suscripción que incluya admisión para Websense Content Gateway o Websense Web Security Gateway en 2 lugares:

- En Websense Manager (vaya a **Configuración > Cuenta**).
- En la interfaz de administración de Websense Content Gateway (vaya a la ficha **Configurar > Mi Proxy > Suscripción > Administración de suscripción**).

Lleva varios minutos para que los 2 productos descarguen las bases de datos necesarias, sincronicen y muestren todas las funciones en tiempo real de ambas herramientas de administración.

Opciones en tiempo real de Websense

Las opciones en tiempo real de Websense ayudan a garantizar la seguridad de la red. Utilice estas opciones para explorar el contenido de Internet y asignarlo a una categoría de filtrado. El resultado en tiempo real se envía a Filtering Service, que filtra el sitio basado en la acción asignada a su categorización en tiempo real en la política activa.

Descarga de la base de datos

Las opciones en tiempo real requieren pequeñas bases de datos instaladas con Websense Web Security Gateway, que verifica que se realicen actualizaciones de bases de datos de forma periódica. Las actualizaciones a estas bases de datos ocurren independientemente de todas las actualizaciones de la base de datos principal (incluso las actualizaciones de bases de datos en tiempo real y las actualizaciones de seguridad en tiempo real).

Cada vez que utiliza el comando **./WCGAdmin start** para iniciar Websense Security Gateway, se inicia una descarga de base de datos. Si se produce un error en la

descarga, se intenta realizar una nueva descarga cada 15 minutos hasta que la descarga se realice correctamente.

El intervalo predeterminado para las verificaciones de las actualizaciones de base de datos es 15 minutos. Para cambiar este intervalo, edite el valor **PollInterval** en el archivo **/opt/bin/downloadservice.ini** del equipo donde está Websense Content Gateway.

Luego de editar el archivo **downloadservice.ini**, debe detener y reiniciar Websense Content Gateway desde la línea de comandos.

- Para detenerlo, ingrese: **/opt/WCG/WCGAdmin stop**
- Para reiniciar, ingrese: **/opt/WCG/WCGAdmin start**

Opciones de exploración

Utilice la página **Configuración > Exploración en tiempo real** para activar y configurar opciones en tiempo real. Las opciones de exploración en tiempo real individuales se describen en las secciones siguientes.

- *Categorización de contenido y exploraciones para detectar amenazas*, página 148
- *Exploración de archivos*, página 149
- *Eliminación de contenido innecesario*, página 151

Para cada opción, tiene por lo menos 2 opciones:

- **Desactivado.** No ocurre ninguna exploración ni ningún bloqueo en tiempo real. Esta opción no proporciona seguridad adicional.
- **Recomendado** o bien **Activado.** Si su sitio está configurado para exploraciones en tiempo real, esta configuración le brinda el mejor rendimiento. Las exploraciones se realizan en base a 2 factores:
  - Las listas Explorar siempre y No explorar nunca de la ficha **Configuración > Exploración en tiempo real > Excepciones** (consulte *Limitación de la exploración*, página 152).
  - Si el software de Websense ha identificado que el sitio incluye contenido dinámico. Se exploran los sitios que se indica que incluyen contenido dinámico. El marcador que identifica que un sitio incluye contenido dinámico no puede ser configurado por el usuario.

    No se exploran los sitios con contenido dinámico que aparecen en la lista No explorar nunca.
- **Todos.** Se exploran todas las páginas Web solicitadas. Las únicas excepciones son las enumeradas en la lista No explorar nunca.

Esta opción proporciona la mayor seguridad, pero puede reducir significativamente el rendimiento del sistema.

Advertencia

Los sitios que aparecen en la lista No explorar nunca no son analizados bajo ninguna circunstancia. Si se ve afectado un sitio de la lista No explorar nunca, las opciones en tiempo real no analizan ni detectan el código malicioso.

Categorización de contenido y exploraciones para detectar amenazas

Temas relacionados:

- *Opciones de exploración*, página 147
- *Exploración de archivos*, página 149
- *Eliminación de contenido innecesario*, página 151
- *Limitación de la exploración*, página 152
- *Informes sobre la actividad de exploración en tiempo real*, página 153

El contenido Web cambia rápidamente. Las estadísticas han demostrado que una gran mayoría de contenido Web es dinámica. Además, Internet hospeda más contenido generado por el usuario, como el que se encuentra en los sitios de redes sociales. Este material no está sujeto a las pautas de contenido y estilo que rigen a los sitios Web corporativos.

Cuando la categorización de contenido está activada, los sitios seleccionados se categorizar en tiempo real, y la categoría resultante se reenvía al software de filtrado de Websense para ser bloqueada o permitida en base a la política activa.

Importante

Active el registro de URL completa (consulte *Configuración de registro de URL completa*, página 329) si planifica generar informes de la actividad de exploración en tiempo real. De otro modo, los registros del registro incluyen solamente el dominio (www.dominio.com) del sitio categorizado, y las páginas individuales de un sitio pueden entrar en diferentes categorías.

Si su sitio utiliza WebCatcher para informar URL no categorizadas a Websense, Inc. (consulte *Configuración de WebCatcher*, página 320), las URL categorizadas mediante categorización de contenido se reenvían para ser incluidas en la base de datos principal Master Database.

Si su suscripción incluye Websense Security Gateway, también puede especificar que los sitios se exploren para detectar amenazas a la seguridad.

Utilice la página **Configuración > Exploración en tiempo real > Opciones comunes** para especificar cuándo utilizar la categorización de contenido y la exploración de contenido.

1. En el área Categorización de contenido, seleccione **Desactivado** o **Activado** (valor predeterminado) para determinar si se realizará una exploración. Consulte *Opciones de exploración*, página 147.

   Luego de que se determina la categoría, se aplica cualquier otra opción en tiempo real que usted haya configurado para proporcionar seguridad adicional.
2. (*Websense Security Gateway*) En el área Exploración de contenido, seleccione **Desactivado** (valor predeterminado), **Recomendado** o **Todos** para determinar el nivel de exploración.
3. Realice una de las siguientes acciones:
   - Para agregar sitios a las listas No explorar nunca o Explorar siempre, seleccione la ficha **Excepciones**. Consulte *Limitación de la exploración*, página 152.
   - Para cambiar la configuración de otras opciones en tiempo real, continúe en la página **Opciones comunes**. Consulte *Exploración de archivos*, página 149 y *Eliminación de contenido innecesario*, página 151.
4. Cuando haya terminado, haga clic en **Aceptar** para guardar los cambios en caché. Los cambios no se implementarán hasta que usted haga clic en **Guardar todo**.

Los informes de presentación pueden proporcionar detalles sobre los intentos de acceso a sitios que contienen amenazas. Consulte *Informes de presentación*, página 98, para obtener detalles sobre la ejecución de informes de Websense.

Exploración de archivos

Temas relacionados:

- *Opciones de exploración*, página 147
- *Categorización de contenido y exploraciones para detectar amenazas*, página 148
- *Eliminación de contenido innecesario*, página 151
- *Limitación de la exploración*, página 152
- *Informes sobre la actividad de exploración en tiempo real*, página 153

La exploración de archivos observa el contenido de los archivos de aplicación entrantes que los usuarios intentan descargar o abrir de manera remota. Esta opción en tiempo real devuelve una categoría al software de filtrado de Websense de modo que el archivo se permite o se bloquea según corresponda.

Como práctica recomendada, explore todos los archivos **ejecutables** (por ejemplo, archivos **.exe** y **.dll**). También puede identificar tipos adicionales de archivos para explorar, y definir un tamaño máximo para explorar.

> **Nota**
> Se exploran únicamente los archivos de aplicaciones portátiles de 32 bits de Windows.

Utilice la ficha **Configuración> Exploración en tiempo real> Opciones comunes** para especificar cuándo utilizar la exploración de contenido.

1. En el área Exploración de contenido, seleccione **Desactivado**, **Recomendado** (valor predeterminado) o **Todos** para determinar el nivel de exploración. Consulte *Opciones de exploración*, página 147.
2. Haga clic en **Configuración avanzada**.
3. **Explorar todos los tipos de archivo con contenido ejecutable** está seleccionado de manera predeterminada. Elimine la marca de esta casilla si prefiere enumerar extensiones de archivo individuales para explorar.
4. Para especificar tipos de archivo adicionales para explorar, ingrese la extensión del archivo (como **ppt** o **wmv**) y luego haga clic en **Agregar**. La extensión del archivo puede contener únicamente caracteres alfanuméricos, un carácter de subrayado (_) o un guión (-). No incluya el punto que antecede a la extensión.

   Para quitar una extensión de archivo de la lista de extensiones de archivo seleccionadas, seleccione la extensión y haga clic en **Eliminar**.
5. En Opciones, ingrese el tamaño máximo de los archivos a explorar (en forma predeterminada, 10 MB). Seleccione **Personalizado** para ingresar un tamaño de hasta 4096 MB (4 GB). Los archivos que superen el tamaño especificado no se explorarán.
6. Realice una de las siguientes acciones:
   - Si quiere agregar sitios a las listas No explorar nunca o Explorar siempre, seleccione la ficha **Excepciones**. Consulte *Limitación de la exploración*, página 152.
   - Si quiere cambiar la configuración de otras opciones en tiempo real, continúe en la ficha **Opciones comunes**. Consulte *Categorización de contenido y exploraciones para detectar amenazas*, página 148, y *Eliminación de contenido innecesario*, página 151.
7. Cuando haya terminado, haga clic en **Aceptar** para guardar los cambios en caché. Los cambios no se implementarán hasta que usted haga clic en **Guardar todo**.

Hay varios informes de presentación que proporcionan detalles sobre los intentos de descarga de archivos que contienen riesgos a la seguridad. Consulte *Informes de presentación*, página 98, para obtener instrucciones sobre la ejecución de informes de Websense.

Consulte *Cómo administrar tráfico en función del tipo de archivo*, página 193, para obtener información sobre el bloqueo de archivos en base al tipo y la categoría de la URL.

Eliminación de contenido innecesario

Temas relacionados:

- *Opciones de exploración*, página 147
- *Categorización de contenido y exploraciones para detectar amenazas*, página 148
- *Exploración de archivos*, página 149
- *Limitación de la exploración*, página 152
- *Informes sobre la actividad de exploración en tiempo real*, página 153

Puede haber amenazas a su sistema ocultas en el contenido activo enviado a través de páginas Web. Una manera de preservar la integridad del sistema es asegurarse de que ese tipo de contenido no llegue nunca.

Las opciones en tiempo real de Websense hacen posible especificar que se elimine el contenido de lenguajes de scripts particulares (ActiveX, JavaScript o VB Script) de las páginas Web entrantes. Si la eliminación de contenido innecesario está activada, todo el contenido de los lenguajes de script especificados se elimina de los sitios que se indica que contienen contenido dinámico o que aparecen en la lista Explorar siempre (consulte *Opciones de exploración*, página 147).

El contenido se elimina solamente luego de que las opciones en tiempo real han categorizado el sitio y el software de filtrado de Websense ha determinado qué política se aplica.

Importante

Las páginas Web que requieren contenido activo que se ha eliminado no funcionarán como se espera. Para permitir acceso total a los sitios que requieren contenido activo, desactive la eliminación de contenido innecesario o agregue los sitios a la lista No explorar nunca.

El usuario que solicita una página con contenido activo no recibe ninguna notificación de que se ha eliminado contenido.

Utilice la ficha **Configuración > Exploración en tiempo real > Opciones comunes** para especificar cuándo eliminar contenido innecesario de los sitios con contenido dinámico.

1. En el área Eliminación de contenido innecesario, seleccione los tipos de contenido activo que se deben eliminar de las páginas Web entrantes.
2. Para cambiar la configuración de otras opciones en tiempo real, consulte:
   - *Categorización de contenido y exploraciones para detectar amenazas*, página 148
   - *Exploración de archivos*, página 149.

3. Cuando haya terminado, haga clic en **Aceptar** para guardar los cambios en caché. Los cambios no se implementarán hasta que usted haga clic en **Guardar todo**.

Para desactivar la eliminación de contenido innecesario de un lenguaje seleccionado, elimine la marca de la casilla asociada.

Limitación de la exploración

Temas relacionados:

- *Opciones de exploración*, página 147
- *Categorización de contenido y exploraciones para detectar amenazas*, página 148
- *Exploración de archivos*, página 149
- *Eliminación de contenido innecesario*, página 151

Utilice las listas Explorar siempre y No explorar nunca para personalizar el comportamiento de las opciones de exploración Recomendado y Todo.

- Cuando una opción en tiempo real está configurada en Recomendado o Activado, se explorarán los sitios con contenido dinámico y los sitios que estén en la lista Explorar siempre (consulte *Opciones de exploración*, página 147). Los sitios de la lista No explorar nunca se ignoran.
- Cuando una opción en tiempo real está configurada en Todo, los sitios de la lista No explorar nunca se ignoran. Esto puede mejorar el rendimiento.

Utilice la lista No explorar nunca con precaución. Si un sitio de esta lista está comprometido, Websense Security Gateway no explorará ese sitio para detectar el problema de seguridad.

Utilice la página **Configuración > Exploración en tiempo real > Excepciones** para completar y editar las listas Explorar siempre y No explorar nunca.

Para agregar sitios a la lista Explorar siempre o No explorar nunca:

1. Ingrese los nombres de los sitios en el cuadro **URL**.

   Ingrese solamente el nombre del host (por ejemplo, **estesitio.com**). No es necesario ingresar la URL completa. Asegúrese de ingresar el dominio y la extensión; **estesitio.com** y **estesitio.net** son entradas distintas.

   Puede ingresar más de un nombre de host por vez.
2. En la columna **Opciones**, seleccione las opciones en tiempo real que se aplican a todos los sitios que ha ingresado. Puede seleccionar una o más opciones. Tenga en cuenta que **Amenazas a la seguridad** se refiere únicamente a la exploración de contenido, no de archivos. La exploración de archivos no se ve afectada por las listas Explorar siempre y No explorar nunca.

   Para aplicar diferentes opciones a sitios diferentes, ingrese los sitios por separado.

3. Seleccione **Agregar a Explorar siempre** o **Agregar a No explorar nunca**.

   Un sitio puede aparecer en sólo una de las 2 listas. Usted no puede, por ejemplo, especificar que el mismo sitio se debe explorar siempre para detectar amenazas y no se debe explorar nunca para eliminar contenido innecesario.

   - Para cambiar la lista en la que aparece un sitio, primero seleccione el sitio y luego utilice los botones de flecha derecha (>) y flecha izquierda (>) para mover el sitio a una lista nueva.
   - Para eliminar un sitio de cualquiera de las listas, seleccione el sitio y luego haga clic en **Eliminar**.

4. Cuando haya terminado, haga clic en **Aceptar** para guardar los cambios en caché. Los cambios no se implementarán hasta que usted haga clic en **Guardar todo**.

Para cambiar las opciones de exploración asociadas con un sitio:

1. Seleccione el sitio en la lista Explorar siempre o No explorar nunca y luego haga clic en **Editar**.
2. En el cuadro Reglas de edición, seleccione las nuevas opciones para ese nombre de host:
   - **Sin cambios** mantiene la configuración actual.
   - **Activado** indica que el contenido se explora para detectar la opción especificada, como categorización de contenido.
   - **Desactivado** indica que no se realiza ninguna exploración para detectar la opción especificada. Si una opción está desactivada, el rendimiento puede mejorar pero la seguridad puede verse afectada.
3. Cuando haya terminado de realizar los cambios, haga clic en **Aceptar** en el cuadro Reglas de edición para regresar a la ficha Excepciones.
4. Vuelva a hacer clic en **Aceptar** para guardar los cambios en caché. Los cambios no se implementarán hasta que usted haga clic en **Guardar todo**.

Informes sobre la actividad de exploración en tiempo real

Temas relacionados:

- *Opciones de exploración*, página 147
- *Categorización de contenido y exploraciones para detectar amenazas*, página 148
- *Exploración de archivos*, página 149
- *Eliminación de contenido innecesario*, página 151

Si su suscripción incluye funciones de exploración en tiempo real, usted puede analizar los efectos de estas funciones con informes de presentación e informes de investigación.

En la página Informes de presentación se encuentra disponible un grupo de informes llamado Amenazas de seguridad en tiempo real. Estos informes se concentran específicamente en actividades relacionadas con amenazas. Como con todos los informes de presentación, usted puede copiar un informe de amenazas a la seguridad y editar su filtro de informe para limitar la información que se incluye al generar un informe a partir de esa copia.

Algunos informes de amenazas a la seguridad incluyen una columna llamada ID de amenaza. Puede hacer clic en la ID de la amenaza individual para abrir una página de Websense Security Labs en la que se describe el tipo de amenaza identificada.

Además, otros informes de presentación contienen información sobre actividades de exploración en tiempo real, así como actividades de filtrado estándar. Copie un informe predefinido y edite el filtro del mismo para crear un informe específico para las actividades de exploración en tiempo real.

Importante

Active el registro de URL completa (consulte *Configuración de registro de URL completa*, página 329) para garantizar que los informes de la actividad en tiempo real tengan sentido. De otro modo, los informes pueden mostrar únicamente el dominio (www.dominio.com) del sitio categorizado, aunque las páginas individuales dentro del sitio puedan entrar en diferentes categorías o contener diferentes amenazas.

Por ejemplo, el informe Detalle de URL completas por categoría, que se encuentra en el grupo Actividad de Internet del Catálogo de informes, proporciona una lista detallada de cada URL a la que se accede dentro de cada categoría. Para realizar un informe específico para la exploración en tiempo real, copie el informe Detalle de URL completas por categoría y edite su filtro de informe. En la ficha Acciones, seleccione únicamente acciones permitidas y bloqueadas que se relacionen con la exploración en tiempo real. En la ficha Opciones, cambie el título del catálogo del informe y el nombre del informe para identificarlo como un informe de exploración en tiempo real. Por ejemplo, podría cambiar el nombre y el título a Tiempo real: detalle de URL completas por categoría

Los informes de investigación también se pueden utilizar para comprender las actividades de exploración en tiempo real.

1. En la lista desplegable **Uso de Internet por**, seleccione Acción.
2. En el informe resultante, haga clic en una acción en tiempo real, como Categoría bloqueada en tiempo real, para mostrar una lista de opciones detalladas.
3. Haga clic en la opción detallada que quiera; por ejemplo, Categoría o Usuario.
4. Haga clic en el valor Accesos o en la barra o en cualquier fila para ver los detalles relacionados.
5. Haga clic en **Modificar informe**, en la parte superior de la página, para agregar al informe la columna URL completa.

Consulte *Informes de investigación*, página 117, para obtener detalles sobre la utilización de todas las funciones de los informes de investigación.

Cómo se registra la exploración en tiempo real

Cuando utiliza las opciones de exploración en tiempo real, tenga en cuenta que hay diferencias en la manera en que se registran la actividad de filtrado en la Web estándar y la actividad de exploración en tiempo real.

Para el filtrado en la Web estándar, hay varias opciones para disminuir el tamaño de la base de datos de registro.

- Active las **visitas** para registrar sólo un registro para cada sitio Web solicitado. Consulte *Configuración de los archivos de caché de registro*, página 317.
- Active la **consolidación** para combinar en un solo registro del registro múltiples solicitudes que tengan ciertos elementos comunes. Consulte *Configuración de opciones de consolidación*, página 318.
- Desactive el **registro de URL completa** para registrar únicamente el nombre de dominio (www.dominio.com) para cada solicitud, y no la ruta a la página específica del dominio (/productos/productoA). Consulte *Configuración de registro de URL completa*, página 329.
- Active el **registro de categorías selectivo** para limitar el registro a categorías seleccionadas que sean fundamentales para la empresa. Consulte *Configuración de Filtering Service para el registro*, página 310.

Las funciones de exploración en tiempo real, sin embargo, están vinculadas sólo en parte por esta configuración. Cuando la exploración en tiempo real analiza un sitio, crea 2 registros del registro separados.

- Los **registros de filtro de la Web** aprovechan cualquier parámetro de reducción de tamaño que se haya implementado, y están disponibles para todos los informes de filtros de la Web.
- Los **registros en tiempo real** ignoran la mayoría de los parámetros de reducción de tamaño. Cada acceso separado se registra, las solicitudes a todas las categorías se registran, y no se consolidan registros. Se genera un registro en tiempo real independientemente de si el sitio está bloqueado o permitido como resultado de la exploración en tiempo real. Solamente la configuración de registro de URL completa es recompensada por los registros en tiempo real.

Si ha activado alguna opción de reducción de tamaño de la base de datos de registro Log Database, los números que aparecen en los informes en tiempo real posiblemente **no** coincidan con los que aparecen en los informes de filtrado estándar, aún cuando los informes estén configurados para los mismos usuarios, períodos de tiempo y categorías. Por ejemplo, si ha elegido registrar las visitas y un usuario solicita un sitio analizado por las funciones de exploración en tiempo real, la solicitud de ese usuario aparece como una visita en los informes de filtrado estándar, pero puede aparecer como múltiples accesos en los informes en tiempo real.

Para ver datos comparables de filtrado estándar y en tiempo real, **desactive** los parámetros de reducción de tamaño de la base de datos de registro Log Database.

Como esto puede dar como resultado una base de datos muy grande y de crecimiento rápido, asegúrese de que la máquina de la base de datos de registro Log Database tenga la capacidad adecuada de disco duro, procesamiento y memoria.

Consulte *Administración de informes*, página 305, para obtener más información sobre la configuración de los parámetros de reducción de tamaño. Consulte *Informes de presentación*, página 98, y *Informes de investigación*, página 117, para obtener información sobre la generación de informes.

8 Filtrado de clientes remotos

Temas relacionados:

- *Funcionamiento de Remote Filtering*, página 158
- *Configuración de parámetros de Remote Filtering*, página 164

Muchas empresas tienen usuarios que a veces trasladan sus computadoras portátiles fuera de la red. Para los usuarios remotos que tienen un sistema operativo Microsoft Windows, usted puede filtrar las solicitudes de Internet mediante la implementación de Websense Remote Filtering, una función opcional disponible tanto para Websense Web Security como para Websense Web Filter.

Remote Filtering supervisa el tráfico HTTP, SSL y FTP, aplicando la política asignada al usuario individual o al grupo, o bien la política predeterminada, según la manera en que el usuario inicie sesión en la computadora remota. Remote Filtering no filtra sobre la base de las políticas asignadas a las computadoras o los rangos de red. Consulte *Identificación de usuarios remotos*, página 161 para obtener más información.

El filtrado basado en ancho de banda no está admitido para los clientes remotos (consulte *Cómo utilizar Bandwidth Optimizer para administrar el ancho de banda*, página 191). El ancho de banda generado por el tráfico remoto no está incluido en las mediciones y los informes de ancho de banda.

El filtrado remoto Remote Filtering de solicitudes FTP y SSL, como HTTPS, únicamente se puede bloquear o permitir. Si un usuario remoto solicita un sitio FTP o un sitio HTTPS, por ejemplo, desde una categoría que tiene asignada la acción cuota o confirmar, el sitio estará bloqueado para los clientes de Remote Filtering. Cuando estas computadoras navegan desde dentro de la red, las acciones de filtrado de cuota y confirmar se aplican normalmente.

Para implementar Remote Filtering, debe instalar los siguientes componentes:

- Remote Filtering Server debe estar dentro del firewall más alejado, y las computadoras remotas deben tener permitido comunicarse con él. En general, está instalado en la *zona desmilitarizada*, o DMZ, de la red, fuera del firewall que protege al resto de la red. Puede instalar un máximo de 3 Remote Filtering Servers para que proporcionen capacidades de recuperación de fallos.

- Remote Filtering Client debe estar en cada computadora que tenga un sistema operativo Windows y se utilice fuera de la red.

Notas

Siga atentamente las recomendaciones de la publicación *Deployment Guide* para implementar estos componentes. Consulte la *guía de instalación* para obtener instrucciones para instalarlos.

Si utiliza el software de Websense en modo autónomo (sin un producto de integración), configure Network Agent **para que no** supervise el equipo de Remote Filtering Server (consulte *Cómo establecer la configuración global*, página 348).

Todas las comunicaciones entre Remote Filtering Client y Remote Filtering Server son autenticadas y están cifradas.

Funcionamiento de Remote Filtering

Temas relacionados:

- *Dentro de la red*, página 159
- *Fuera de la red*, página 160
- *Identificación de usuarios remotos*, página 161
- *Cuando no es posible establecer una comunicación con el servidor*, página 162
- *Red Privada Virtual (VPN)*, página 163
- *Configuración de parámetros de Remote Filtering*, página 164

Cada vez que una computadora remota realiza una solicitud HTTP, SSL o FTP, el Remote Filtering Client de ese equipo se comunica con Remote Filtering Server. Remote Filtering Server se comunica con Websense Filtering Service para determinar qué acción se aplica. Remote Filtering Server luego responde a Remote Filtering Client, permitiendo el sitio o bien enviando el mensaje de bloqueo que corresponda.

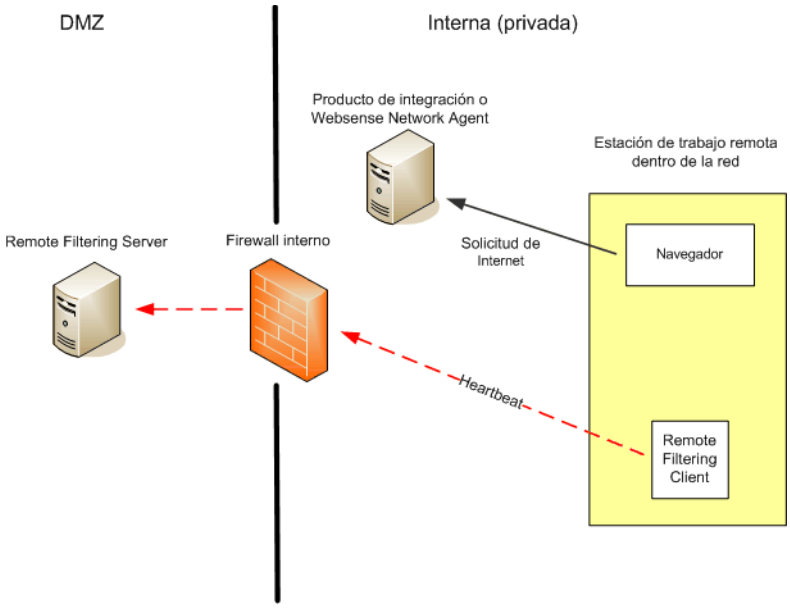
Cuando el navegador de una computadora en la cual se ejecuta Remote Filtering Client realiza una solicitud mediante HTTP, SSL o FTP, Remote Filtering Client debe decidir si consultará a Remote Filtering Server sobre la solicitud. Esta decisión está controlada por la ubicación de la computadora en relación con la red.

Dentro de la red

Temas relacionados:

- *Funcionamiento de Remote Filtering*, página 158
- *Fuera de la red*, página 160
- *Identificación de usuarios remotos*, página 161
- *Cuando no es posible establecer una comunicación con el servidor*, página 162
- *Red Privada Virtual (VPN)*, página 163
- *Configuración de parámetros de Remote Filtering*, página 164

Cuando se inicia una computadora *dentro* de la red, Remote Filtering Client intenta enviar un **heartbeat** a Remote Filtering Server en la DMZ. El heartbeat es exitoso porque el puerto del heartbeat está abierto en el firewall interno.



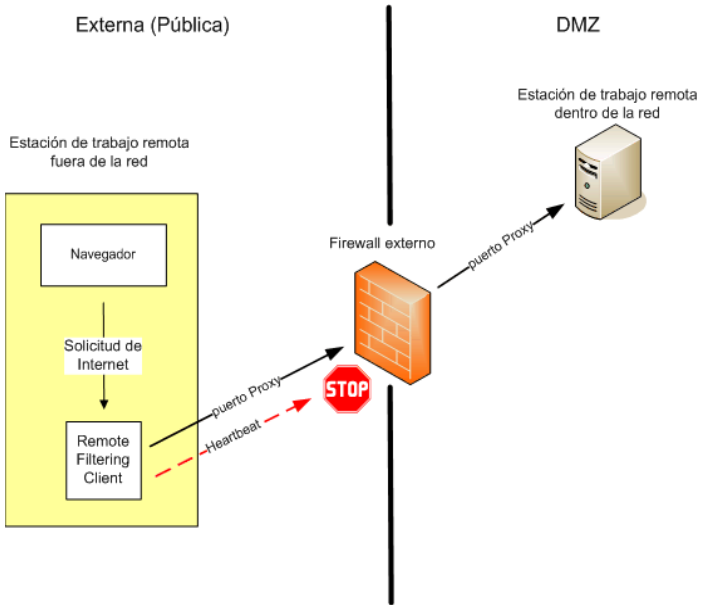
En este caso, Remote Filtering Client se vuelve pasivo y no consulta a Remote Filtering Server sobre las solicitudes de Internet. En cambio, estas solicitudes se traspasan directamente al producto de integración (como Cisco Pix, Microsoft ISA Server) o a Websense Network Agent. La solicitud se filtra como cualquier otra solicitud interna.

Fuera de la red

Temas relacionados:

- *Funcionamiento de Remote Filtering*, página 158
- *Dentro de la red*, página 159
- *Identificación de usuarios remotos*, página 161
- *Cuando no es posible establecer una comunicación con el servidor*, página 162
- *Red Privada Virtual (VPN)*, página 163
- *Configuración de parámetros de Remote Filtering*, página 164

Cuando se inicia una computadora *fuera* de la red, Remote Filtering Client intenta enviar un heartbeat a Remote Filtering Server. El hertbeat no es exitoso porque el puerto del heartbeat está bloqueado en el firewall externo.



Este error de heartbeat le pide a Remote Filtering Client que envíe una consulta sobre cada solicitud HTTP, SSL o FTP por el puerto configurado (valor predeterminado 80) a Remote Filtering Server en la DMZ. Entonces, Remote Filtering Server reenvía la solicitud de filtrado a Websense Filtering Service dentro de la red. Filtering Service evalúa la solicitud y envía una respuesta a Remote Filtering Server. Luego, la respuesta se envía a la computadora remota. Si el sitio está bloqueado, Remote Filtering Client solicita y recibe la página de bloqueo que corresponda, que luego se muestra al usuario.

Remote Filtering Client demora cada solicitud filtrada hasta que recibe una respuesta de Remote Filtering Server. Según la respuesta recibida, Remote Filtering Client permite el sitio o bien muestra la página de bloqueo.

Un archivo de registro realiza el seguimiento de las actividades de Remote Filtering, como ingresar y retirarse de la red, abrir o cerrar si falla y reiniciar el cliente. Remote Filtering Client crea el archivo de registro cuando se inicia por primera vez. Usted controla la presencia y el tamaño de este archivo de registro. Consulte *Configuración de parámetros de Remote Filtering*, página 164.

Identificación de usuarios remotos

Temas relacionados:

- *Funcionamiento de Remote Filtering*, página 158
- *Dentro de la red*, página 159
- *Fuera de la red*, página 160
- *Cuando no es posible establecer una comunicación con el servidor*, página 162
- *Red Privada Virtual (VPN)*, página 163
- *Configuración de parámetros de Remote Filtering*, página 164

La manera en que un usuario inicia sesión en una computadora remota determina la política que se implementará.

Si un usuario inicia sesión utilizando credenciales de dominio guardadas en caché (información de inicio de sesión de directorio de red), Websense Filtering Service puede resolver el nombre de usuario, y aplica a la computadora remota las políticas basadas en grupos y usuarios que corresponda. Además, la actividad de Internet se registra bajo el nombre de usuario de la red.

Si el usuario inicia sesión con una cuenta de usuario que es local para la computadora, Filtering Service no puede resolver el nombre de usuario y, en su lugar, aplica la política predeterminada. La actividad de Internet se registra bajo el nombre de usuario local. Remote Filtering no filtra sobre la base de las políticas asignadas a las computadoras o los rangos de red.

Nota

Los usuarios remotos siempre se filtran de acuerdo con sus credenciales de inicio de sesión, como se describe aquí. Los parámetros de autenticación selectiva no se aplican a estos usuarios.

Cuando no es posible establecer una comunicación con el servidor

Temas relacionados:

- *Funcionamiento de Remote Filtering*, página 158
- *Dentro de la red*, página 159
- *Fuera de la red*, página 160
- *Identificación de usuarios remotos*, página 161
- *Red Privada Virtual (VPN)*, página 163
- *Configuración de parámetros de Remote Filtering*, página 164

El filtrado se realiza cuando Remote Filtering Client, fuera de la red, se comunica correctamente con Remote Filtering Server en la DMZ de la red. Sin embargo, puede haber ocasiones en las que esa comunicación no se realiza.

La acción que realiza Remote Filtering Client si no se puede comunicar con Remote Filtering Server se puede configurar. De manera predeterminada, Remote Filtering Client utiliza el parámetro **abrir si falla**, que permite todas las solicitudes HTTP, SSL y FTP cuando no se puede establecer la comunicación entre estos componentes. Remote Filtering Client continúa intentando comunicarse con Remote Filtering Server. Cuando la comunicación se realiza correctamente, se implementa la política de filtrado que corresponde.

Cuando Remote Filtering Client está configurado en **cerrar si falla**, se aplica un valor de tiempo de espera (valor predeterminado 15 minutos). El reloj comienza a funcionar cuando se inicia la computadora remota. Remote Filtering Client intenta conectarse con Remote Filtering Server inmediatamente y continúa ciclando a través de Remote Filtering Servers disponibles hasta que lo logra.

Si el usuario tiene acceso Web al inicio, no se realiza ningún filtrado (se permiten todas las solicitudes) hasta que Remote Filtering Client se conecta con el Remote Filtering Server. Cuando esto ocurre, se implementa la política de filtrado que corresponde.

Si Remote Filtering Client no se puede conectar dentro del período de espera configurado, se bloquea todo acceso a Internet (cerrar si falla) hasta que se pueda establecer la conexión con Remote Filtering Server.

> **Nota**
> Si Remote Filtering Server no se puede conectar con Websense Filtering Service por cualquier motivo, se devuelve un error al Remote Filtering Client, y el filtrado siempre cierra si falla.

Este período de espera permite a los usuarios que pagan por el acceso a Internet cuando están de viaje iniciar la computadora y organizar para conectarse sin estar bloqueados. Si el usuario no establece acceso Web antes de que finalice el período de

espera de 15 minutos, no se podrá establecer acceso a la Web durante esa sesión. Cuando esto ocurre, el usuario debe reiniciar la computadora para iniciar nuevamente el intervalo de tiempo de espera.

Para cambiar la configuración de abrir/cerrar si falla y cambiar el valor del tiempo de espera, consulte *Configuración de parámetros de Remote Filtering*, página 164.

Red Privada Virtual (VPN)

Temas relacionados:

- *Funcionamiento de Remote Filtering*, página 158
- *Dentro de la red*, página 159
- *Fuera de la red*, página 160
- *Identificación de usuarios remotos*, página 161
- *Cuando no es posible establecer una comunicación con el servidor*, página 162
- *Configuración de parámetros de Remote Filtering*, página 164

Websense Remote Filtering admite conexiones de VPN, incluida la VPN con túnel dividido. Cuando una computadora remota se conecta con la red interna mediante VPN (sin túnel dividido), Remote Filtering Client puede enviar un heartbeat a Remote Filtering Server. Como resultado, Remote Filtering Client se vuelve pasivo y todas las solicitudes HTTP, SSL y FTP de la computadora remota son filtradas por el producto de integración interno o Network Agent, como otras computadoras dentro de la red.

Si la computadora remota se conecta con la red interna mediante un cliente de VPN con túnel dividido, Remote Filtering Client lo detecta y no envía un heartbeat a Remote Filtering Server. Remote Filtering Client supone que está operando externamente y envía solicitudes a Remote Filtering Server para el filtrado.

El software de Websense admite túnel dividido para los siguientes clientes de VPN:

- Checkpoint SecureClient
- Cisco
- Juniper/Netscreen
- Microsoft PPTP
- Nokia
- Nortel
- SonicWALL

Configuración de parámetros de Remote Filtering

Temas relacionados:

- *Funcionamiento de Remote Filtering*, página 158
- *Dentro de la red*, página 159
- *Fuera de la red*, página 160
- *Identificación de usuarios remotos*, página 161
- *Cuando no es posible establecer una comunicación con el servidor*, página 162
- *Red Privada Virtual (VPN)*, página 163

Los superadministradores incondicionales pueden usar la página **Configuración > General > Remote Filtering** para configurar opciones que afectan a todos los Remote Filtering Clients asociados con esta instalación.

Para obtener detalles sobre el funcionamiento de Remote Filtering, consulte *Funcionamiento de Remote Filtering*, página 158.

1. Seleccione la casilla **Cerrar si falla** para bloquear a los Remote Filtering Clients de todo acceso a Internet a menos que la computadora de los mismos se comunique con Remote Filtering Server.

   De manera predeterminada, no está seleccionada, lo que significa que los usuarios remotos tienen acceso sin filtrar a Internet cuando sus computadoras no se pueden comunicar con Remote Filtering Server.

2. Si usted marcó la opción Cerrar si falla, utilice el campo **Tiempo de espera de cerrar si falla** para seleccionar una cantidad de minutos hasta 60 (valor predeterminado 15), o elija **Sin tiempo de espera**.

   Durante el período de espera, se permiten todas las solicitudes HTTP, SSL y FTP.

   Si Remote Filtering Client no se puede comunicar con Remote Filtering Server durante el intervalo de tiempo de espera, se bloqueará todo el acceso a Internet (cerrar si falla).

   Si elige **Sin tiempo de espera**, esto puede bloquear una computadora remota antes de que el usuario pueda establecer una conexión con Internet desde un hotel u otro proveedor de pago por uso. Además, Remote Filtering Client intenta comunicarse con Remote Filtering Server continuamente.

   Advertencia

   Websense, Inc., no recomienda elegir **Sin tiempo de espera** ni definir el período de espera en un número muy bajo.

3. Seleccione un **Tamaño máximo para archivos de registro (en megabytes)** local, hasta 10. Elija **Sin registro** para desactivar la opción de registro.

Controla el tamaño y la existencia del archivo de registro que crea la computadora remota cuando se desconecta inicialmente de Remote Filtering Server. Este archivo de registro realiza el seguimiento de los siguientes eventos:

- La computadora abandona la red
- La computadora se reincorpora a la red
- Remote Filtering Client se reinicia
- Ocurre una condición Abrir si falla
- Ocurre una condición Cerrar si falla
- Remote Filtering Client recibe una actualización de políticas

La computadora retiene los 2 registros más recientes. Estos registros se pueden utilizar para solucionar problemas de conexión u otros problemas con Remote Filtering.

9 Refinar políticas de filtrado

En su nivel más simple, el filtrado de uso de Internet requiere una sola política que aplique un filtro de categorías y un filtro de protocolos las 24 horas del día, los 7 días de la semana. Sin embargo, el software de Websense ofrece herramientas para superar este filtrado básico y lograr el nivel preciso de granularidad necesario para administrar el uso de Internet. Usted puede:

- Crear **filtros de acceso limitado** para bloquear el acceso a todo excepto a una lista específica de sitios para ciertos usuarios (consulte *Cómo restringir usuarios a una lista definida de sitios de Internet*, página 168).
- Crear **categorías personalizadas** para redefinir el método de filtrado de los sitios seleccionados (consulte *Cómo trabajar con categorías*, página 175).
- **Recategorizar URL** para mover sitios específicos de la categoría predeterminada de la base de datos principal a otra categoría personalizada o definida por Websense (consulte *Cómo recategorizar URL*, página 184).
- Definir **URL sin filtrar** para permitir que los usuarios accedan a sitios específicos, aún cuando dichos sitios se asignan a una categoría bloqueada en el filtro de categorías activo (consulte *Cómo definir URL sin filtrar*, página 183).
- Implementar restricciones de **ancho de banda**, para bloquear el acceso de los usuarios a categorías y protocolos permitidos de otro modo cuando el uso del ancho de banda alcanza un umbral específico.
- Definir **palabras clave** utilizadas para bloquear sitios en categorías permitidas de otro modo cuando el bloqueo de palabras clave se encuentra habilitado y activado (consulte *Cómo filtrar según palabras clave*, página 180).
- Definir **tipos de archivo** utilizados para bloquear la descarga de tipos de archivos seleccionados de categorías que estarían permitidas de otro modo cuando se activa el bloqueo por tipo de archivo (consulte *Cómo administrar tráfico en función del tipo de archivo*, página 193).

Cómo restringir usuarios a una lista definida de sitios de Internet

Temas relacionados:

- *Filtros de acceso limitado y prioridad de filtrado*, página 168
- *Cómo crear un filtro de acceso limitado*, página 170
- *Cómo modificar un filtro de acceso limitado*, página 170

Los filtros de acceso limitado proporcionan una forma muy precisa de filtrar el acceso a Internet. Cada filtro de acceso limitado es una lista de sitios Web individuales. Al igual que los filtros de categorías, los filtros de acceso limitado se agregan a las políticas y se implementan durante un período de tiempo específico. Cuando un filtro de acceso limitado se encuentra activo en una política, los usuarios asignados a esa política pueden visitar sitios de la lista únicamente. Todos los demás sitios están bloqueados.

Por ejemplo, si la política del primer año de escuela primaria implementa un filtro de acceso limitado que incluye sólo ciertos sitios educativos y de referencia, los estudiantes regidos por dicha política sólo pueden visitar esos sitios y ningún otro.

Importante

Cuando se aplica un filtro de acceso limitado, el software de Websense verifica que sólo aparezca en el filtro un sitio solicitado. No se realiza ninguna otra verificación.

Esto significa que si un sitio permitido por el filtro se infecta con códigos maliciosos, igual se permiten las solicitudes de los usuarios para ese sitio, independientemente de la categorización de la base de datos principal o la exploración en tiempo real del sitio.

Cuando un filtro de acceso limitado se encuentra activo, se muestra una página de bloqueo por cada URL solicitada que no esté incluida en ese filtro.

El software de Websense puede admitir hasta 2.500 filtros de acceso limitado con 25.000 URL en total.

Filtros de acceso limitado y prioridad de filtrado

En algunos casos, podría aplicarse más de una política de filtrado a un solo usuario. Esto sucede cuando un usuario pertenece a más de un grupo y los grupos se rigen por políticas diferentes. Además, una URL podría tanto aparecer en un filtro de acceso limitado como definirse como una URL sin filtrar.

Cuando se aplican múltiples políticas de grupo a un usuario, el parámetro **Usar bloqueo más restrictivo** (consulte *Orden de filtrado*, página 80) determina el método de filtrado del usuario. De forma predeterminada, este valor está desactivado.

El software de Websense determina qué parámetros de filtrado son menos restrictivos en el nivel de filtro. En los casos en que un usuario pudiera ser filtrado por múltiples políticas, una de las cuales se rige por un filtro de acceso limitado, "menos restrictivo" puede parecer carente de lógica.

Cuando **Usar bloqueo más restrictivo** se encuentra **DESACTIVADO**:

- Si es posible aplicar el filtro de categorías **Bloquear todo** y un filtro de acceso limitado, este último siempre se considera menos restrictivo.
- Si es posible aplicar cualquier otro filtro de categorías y un filtro de acceso limitado, el filtro de categorías se considera menos restrictivo.

  Esto significa que aun cuando el filtro de acceso limitado permite el sitio y el filtro de categorías lo bloquea, el sitio está bloqueado.

Cuando **Usar bloqueo más restrictivo** se encuentra **ACTIVADO**, un filtro de acceso limitado se considera más restrictivo que cualquier otro filtro de categorías excepto Bloquear todo.

La siguiente tabla resume el modo en que el parámetro **Usar bloqueo más restrictivo** afecta el filtrado cuando es posible aplicar múltiples políticas:

	Usar bloqueo más restrictivo **DESACTIVADO**	***Usar bloqueo más restrictivo*** **ACTIVADO**
filtro de acceso limitado +Filtro de categoría **Bloquear todo**	filtro de acceso limitado (solicitud permitida)	**Bloquear todo** (solicitud bloqueada)
filtro de acceso limitado + categoría permitida	filtro de categorías (solicitud permitida)	filtro de acceso limitado (solicitud permitida)
filtro de acceso limitado + categoría bloqueada	filtro de categorías (solicitud bloqueada)	filtro de acceso limitado (solicitud permitida)
filtro de acceso limitado + Cuota/Confirmar categoría	filtro de categorías (solicitud limitada por la opción cuota/confirmar)	filtro de acceso limitado (solicitud permitida)
filtro de acceso limitado + URL sin filtrar	URL sin filtrar (solicitud permitida)	filtro de acceso limitado (solicitud permitida)

Cómo crear un filtro de acceso limitado

Temas relacionados:

- *Cómo trabajar con filtros*, página 48
- *Cómo restringir usuarios a una lista definida de sitios de Internet*, página 168
- *Cómo modificar un filtro de acceso limitado*, página 170

Utilice la página **Agregar filtro Acceso limitado** (a la que se accede mediante la página **Filtros** o **Modificar política**) para dar a su nuevo filtro un nombre y una descripción. Después de crear el filtro, especifique una lista de URL permitidas, asigne el filtro a una política y aplique la política a clientes.

1. Especifique un **Nombre de filtro** único. El nombre debe tener entre 1 y 50 caracteres y no puede contener ninguno de los caracteres siguientes:

   ```
   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

   Los nombres de filtro pueden contener espacios, guiones y apóstrofes.
2. Especifique una **Descripción** corta del filtro. Esta descripción aparece junto al nombre del filtro en la sección Filtros de acceso limitado en la página Filtros, y debe explicar el objetivo del filtro para ayudar a los administradores a administrar políticas a través del tiempo.

   Las restricciones de caracteres que se aplican a los nombres de filtro también se aplican a las descripciones, con dos excepciones: las descripciones pueden incluir puntos (.) y comas (,).
3. Para ver y modificar el filtro nuevo, haga clic en **Aceptar**. Para descartar los cambios y regresar a la página Filtros, haga clic en **Cancelar**.

Cuando crea un nuevo filtro de acceso limitado, dicho filtro se agrega a la lista **Administración de políticas > Filtros > Filtros de acceso limitado**. Haga clic en un nombre de filtro para modificarlo.

Para terminar de personalizar su nuevo filtro, continúe con *Cómo modificar un filtro de acceso limitado*.

Cómo modificar un filtro de acceso limitado

Temas relacionados:

- *Cómo restringir usuarios a una lista definida de sitios de Internet*, página 168
- *Filtros de acceso limitado y prioridad de filtrado*, página 168
- *Cómo crear un filtro de acceso limitado*, página 170
- *Cómo editar una política*, página 77

Un filtro de acceso limitado es una lista de sitios Web (URL o direcciones IP) y expresiones regulares, que se utiliza para identificar sitios específicos a los que pueden acceder los usuarios. Cuando se aplica el filtro a los clientes, dichos clientes no pueden visitar ningún sitio que no se encuentre en la lista.

Importante

Cuando se aplica un filtro de acceso limitado, el software de Websense verifica que sólo aparezca en el filtro un sitio solicitado. No se realiza ninguna otra verificación.

Esto significa que si un sitio permitido por el filtro se infecta con códigos maliciosos, igual se permiten las solicitudes de los usuarios para ese sitio, independientemente de la categorización de la base de datos principal o la exploración en tiempo real del sitio.

Utilice la página **Administración de políticas > Filtros > Modificar el filtro de acceso limitado** para realizar cambios a un filtro de acceso limitado existente. Puede cambiar el nombre y la descripción del filtro, ver una lista de políticas que lo implementan y administrar los sitios incluidos en el filtro.

Al modificar un filtro de acceso limitado, los cambios afectan a todas las políticas que implementan el filtro.

1. Verifique el nombre y la descripción del filtro. Para cambiar el nombre del filtro, haga clic en **Cambiar nombre** y luego ingrese el nuevo nombre. El nombre se actualiza en todas las políticas que implementan el filtro de acceso limitado seleccionado.
2. Utilice el campo **Políticas que utilizan este filtro** para ver cuántas políticas implementan este filtro en un momento dado. Si una o más políticas implementan el filtro, haga clic en **Ver políticas** para que aparezcan listadas.
3. En Agregar o eliminar sitios, ingrese las URL y direcciones IP que desee agregar al filtro de acceso limitado. Especifique una URL o dirección IP por línea.

   No es necesario incluir el prefijo HTTP://.

   Cuando un sitio es filtrado según la categoría de su base de datos principal, el software de Websense asocia la URL con su dirección IP equivalente. Este no es el caso para los filtros de acceso limitado. Para permitir la URL y la dirección IP de un sitio, agréguelas al filtro.
4. Haga clic en el botón de flecha derecha (>) para mover las URL y las direcciones IP a la lista de sitios permitidos.
5. Además de agregar sitios individuales al filtro de acceso limitado, puede agregar expresiones regulares que establezcan coincidencias entre varios sitios. Para crear expresiones regulares, haga clic en **Opciones avanzadas**.
   - Ingrese una expresión regular por línea y luego haga clic en el botón de la flecha derecha para mover las expresiones a la lista de sitios permitidos.
   - Para comprobar que una expresión regular coincide con los sitios pretendidos, haga clic en **Probar**.

- Consulte *Cómo utilizar expresiones regulares*, página 197, para obtener información detallada sobre el uso de expresiones regulares para filtrado.

6. Revise las URL, las direcciones IP y las expresiones regulares en la lista **Sitios permitidos**.
   - Para realizar cambios a un sitio o una expresión, seleccione dicho sitio o expresión y haga clic en **Modificar**.
   - Para eliminar de la lista un sitio o una expresión, seleccione dicho sitio o expresión y haga clic en **Eliminar**.
7. Después de modificar el filtro, haga clic en **Aceptar** para guardar los cambios en caché y regrese a la página Filtros. Los cambios no se implementarán hasta que haga clic en **Guardar todo**.

Cómo agregar sitios de la página Modificar política

Temas relacionados:

- *Cómo restringir usuarios a una lista definida de sitios de Internet*, página 168
- *Filtros de acceso limitado y prioridad de filtrado*, página 168
- *Cómo crear un filtro de acceso limitado*, página 170
- *Cómo editar una política*, página 77

Utilice la página **Políticas > Modificar política > Agregar sitios** para agregar sitios a un filtro de acceso limitado.

Especifique una URL o dirección IP por línea. Si no especifica un protocolo, el software de Websense agregará automáticamente el prefijo **HTTP://**.

Cuando termine de realizar cambios, haga clic en **Aceptar** para regresar a la página Modificar política. También debe hacer clic en **Aceptar** en la página Modificar política para guardar los cambios en caché. Los cambios no se implementarán hasta que haga clic en **Guardar todo**.

Los cambios realizados a un filtro de acceso limitado afectan a todas las políticas que implementan el filtro.

Cómo copiar filtros y políticas a roles

Temas relacionados:

- *Cómo crear un filtro de categorías*, página 49
- *Cómo crear un filtro de protocolos*, página 52
- *Cómo crear un filtro de acceso limitado*, página 170
- *Cómo crear una política*, página 76

Los superadministradores pueden utilizar las páginas **Filtros > Copiar Filtros a rol** y **Políticas > Copiar Políticas a rol** para copiar uno o más filtros o políticas a un rol de administración delegado. Una vez copiado el filtro o la política, los administradores delegados pueden utilizar los filtros o las políticas para filtrar sus clientes administrados.

- En el rol de destino, la etiqueta "(Copiado)" se agrega al final del nombre del filtro o la política. Se agrega un número si se copia el mismo filtro o la misma política muchas veces.
- Los administradores delegados pueden cambiar el nombre de los filtros o las políticas que se han copiado a su rol, o modificarlos.
- Los filtros de categorías copiados a un rol de administración delegado establecen la acción de filtrado a Permitir para las categorías personalizadas creadas en el rol. Los administradores delegados deben actualizar los filtros de categorías copiados con el fin de establecer la acción deseada para sus categorías personalizadas específicas del rol.
- Los cambios realizados por un administrador delegado a un filtro o una política copiados a su rol por un superadministrador no afectan el filtro o la política original del superadministrador, ni cualquier otro rol que haya recibido una copia del filtro o la política.
- Las restricciones de fijación de filtro no afectan el filtro o la política original del superadministrador, pero sí afectan la copia del filtro o de la política del administrador delegado.
- Debido a que los administradores delegados son afectados por restricciones de fijación de filtro, los filtros de categorías y protocolos Permitir todo no se pueden copiar a un rol de administración delegado.

Para copiar un filtro o una política:

1. En la página Copiar filtros a rol o Copiar políticas a rol, compruebe que aparezcan los filtros o las políticas correctos en la lista de la parte superior de la página.
2. Utilice la lista desplegable **Seleccionar un rol** para seleccionar un rol de destino.
3. Haga clic en **Aceptar**.

   Un cuadro de diálogo contextual indica que los filtros o las políticas seleccionados se están copiando. El proceso de copiado puede llevar un tiempo.

Los cambios no se implementarán hasta que haga clic en **Guardar todo**.

Después de finalizado el proceso de copiado, los filtros o las políticas copiados estarán disponibles para los administradores delegados en el rol seleccionado la próxima vez que inicien sesión en Websense Manager. Si un administrador delegado inicia sesión en el rol con política de acceso cuando se copian los filtros o las políticas, no podrá ver los filtros o las políticas nuevos hasta que cierre sesión e inicie sesión nuevamente.

Cómo construir componentes de filtro

Utilice la página **Administración de políticas > Componentes de filtro** para acceder a las herramientas que se utilizan para perfeccionar y personalizar el modo en que el software de Websense implementa las políticas de acceso a Internet de su empresa. Los cuatro botones en la pantalla están asociados con las siguientes tareas:

Modificar categorías	• Recategorice una URL (consulte *Cómo redefinir el filtrado para sitios específicos*, página 182). Por ejemplo, si la categoría Compras está bloqueada por sus políticas de filtrado de Internet, pero desea permitir el acceso a sitios de partners o proveedores específicos, puede mover esos sitios a una categoría permitida, como Comercio y economía. • Defina o modifique categorías personalizadas (consulte *Cómo crear una categoría personalizada*, página 178). Cree subcategorías adicionales dentro de categorías principales definidas por Websense, o dentro de la categoría principal definida por el usuario, y luego asigne URL a las nuevas categorías. • Asigne palabras clave a una categoría (consulte *Cómo filtrar según palabras clave*, página 180). Para recategorizar y bloquear el acceso a sitios cuyas URL contienen una cadena específica, primero defina las plabras clave y luego habilite el bloqueo de palabras clave en un filtro de categorías. • Cree expresiones regulares (consulte *Cómo utilizar expresiones regulares*, página 197), patrones o plantillas que se puedan usar para establecer coincidencias entre varias URL y asígnelos a una categoría.
Modificar protocolos	Defina o modifique definiciones de protocolos personalizados (consulte *Cómo crear un protocolo personalizado*, página 189, y *Cómo modificar protocolos personalizados*, página 186). Por ejemplo, si los miembros de su empresa utilizan una herramienta de mensajería personalizada, puede crear una definición de protocolo personalizado para permitir el uso de dicha herramienta y, al mismo tiempo, bloquear los demás protocolos de mensajería instantánea/chat.

Tipos de archivo	Cree o defina definiciones de tipo de archivo, que se utilizan para bloquear tipos específicos de archivos dentro de categorías que estarían permitidas de otro modo (consulte *Cómo administrar tráfico en función del tipo de archivo*, página 193).
URL sin filtrar	Defina sitios específicos permitidos para todos los clientes, aun cuando pertenecen a una categoría bloqueada (consulte *Cómo definir URL sin filtrar*, página 183). Tenga en cuenta que agregar una URL a esta lista no modifica el filtro de categorías Bloquear todo o el filtro de acceso limitado.

Cómo trabajar con categorías

Temas relacionados:

- *Cómo modificar categorías y sus atributos*, página 175
- *Cómo crear una categoría personalizada*, página 178
- *Cómo filtrar según palabras clave*, página 180
- *Cómo redefinir el filtrado para sitios específicos*, página 182

El software de Websense ofrece múltiples métodos para filtrar sitios que no se encuentran en la base de datos principal, y para cambiar el modo de filtrar sitios individuales en la base de datos principal.

- Cree **categorías personalizadas** para lograr mayor precisión en el filtrado y la generación de informes.
- Utilice **URL recategorizadas** para definir categorías para sitios sin categorizar, o para cambiar la categoría de sitios que aparecen en la base de datos principal.
- Defina **palabras clave** para recategorizar todos los sitios cuya URL contiene una cadena determinada.

Cómo modificar categorías y sus atributos

Temas relacionados:

- *Cómo crear una categoría personalizada*, página 178
- *Cómo revisar todos los atributos de categorías personalizados*, página 177
- *Cómo realizar cambios de filtrado de categoría globales*, página 177
- *Cómo filtrar según palabras clave*, página 180
- *Cómo redefinir el filtrado para sitios específicos*, página 182

Utilice la página **Administración de políticas > Componentes de filtro > Modificar Categorías** para crear y modificar categorías personalizadas, URL recategorizadas y palabras clave.

Las categorías existentes, tanto las definidas por Websense como las personalizadas, aparecen listadas en la parte izquierda del panel de contenido. Para ver las configuraciones personalizadas actuales que están asociadas con una categoría, o para crear nuevas definiciones personalizadas, primero seleccione una categoría de la lista.

Para ver una lista de todas las URL personalizadas, palabras clave y expresiones regulares que están asociadas con todas las categorías, haga clic en **Ver todas las URL personalizadas/palabras clave** en la barra de herramientas de la parte superior de la página. Consulte *Cómo revisar todos los atributos de categorías personalizados*, página 177, para obtener más información.

- Para crear una categoría nueva, haga clic en **Agregar** y luego vaya a *Cómo crear una categoría personalizada*, página 178, para obtener más instrucciones.

  Para eliminar una categoría personalizada existente, selecciónela y luego haga clic **Eliminar**. Usted no puede eliminar categorías definidas por Websense.
- Para cambiar el nombre o la descripción de una categoría personalizada, selecciónela y haga clic en **Cambiar nombre** (consulte *Cómo cambiar el nombre de una categoría personalizada*, página 178).
- Para cambiar la acción de filtrado asociada con una categoría en todos los filtros de categorías, haga clic en **Sustituir acción** (consulte *Cómo realizar cambios de filtrado de categoría globales*, página 177).
- La lista **URL recategorizadas** muestra los sitios recategorizados (URL y direcciones de IP) que han sido asignados a esta categoría.
  - Para agregar un sitio a la lista, haga clic en **Agregar URL**. Consulte *Cómo recategorizar URL*, página 184, para obtener más instrucciones.
  - Para modificar un sitio recategorizado existente, seleccione la URL o la dirección IP y luego haga clic en **Modificar**.
- La lista **Palabras clave** muestra las palabras clave que han sido asociadas con esta categoría.
  - Para definir una palabra clave asociada con la categoría seleccionada, haga clic en **Agregar palabras clave**. Consulte *Cómo filtrar según palabras clave*, página 180, para obtener más instrucciones.
  - Para modificar una definición de palabra clave existente, selecciónela y luego haga clic en **Modificar**.
- Además de URL y palabras clave, puede definir **Expresiones regulares** para la categoría. Cada expresión regular es un patrón o una plantilla que se utiliza para asociar varios sitios con la categoría.

  Para ver o crear expresiones regulares para la categoría, haga clic en **Opciones avanzadas**.
  - Para definir una expresión regular, haga clic en Agregar expresiones (consulte *Cómo utilizar expresiones regulares*, página 197).
  - Para modificar una expresión regular existente, selecciónela y luego haga clic **Modificar**.

- Para eliminar una URL, palabra clave o expresión regular recategorizada, seleccione el elemento a eliminar y luego haga clic en **Eliminar**.

Cuando termine de realizar cambios en la página Modificar categorías, haga clic en **Aceptar** para guardar los cambios en caché y regrese a la página Componentes de filtro. Los cambios no se implementarán hasta que haga clic en **Guardar todo**.

Cómo revisar todos los atributos de categorías personalizados

Utilice la página **Componentes de filtro > Modificar categorías > Ver todas las URL personalizadas y las palabras clave** para revisar las definiciones de URL personalizadas, palabras claves y expresiones regulares. También puede eliminar las definiciones que ya no se necesiten.

La página contiene tres tablas similares, una para cada atributo de categoría: URL personalizadas, palabras clave o expresiones regulares. En cada tabla, el atributo está listado junto al nombre de la categoría con la cual está asociado.

Para eliminar el atributo de una categoría, marque la casilla correspondiente y luego haga clic en **Eliminar**.

Para regresar a la página Modificar categorías, haga clic en **Cerrar**. Si eliminó elementos en la página Ver todas las URL personalizadas y palabras clave, haga clic en **Aceptar** en la página Modificar categorías para guardar los cambios en caché. Los cambios no se implementarán hasta que haga clic en **Guardar todo**.

Cómo realizar cambios de filtrado de categoría globales

Utilice la página **Componentes de filtro > Modificar categorías > Sustituir acción** para cambiar la acción aplicada a una categoría en todos los filtros de categorías existentes. Esto también determina la acción predeterminada aplicada a la categoría en los filtros nuevos.

A pesar de que este cambio sustituye la acción aplicada a la categoría en todos los filtros existentes, los administradores después pueden modificar dichos filtros para aplicar una acción diferente.

Antes de cambiar las configuraciones de filtrado aplicadas a una categoría, verifique primero que aparezca el nombre de categoría correcto junto a **Categoría seleccionada**. A continuación, usted podrá:

1. Elegir una nueva **Acción** (Permitir, Bloquear, Confirmar, o Cuota). Consulte *Acciones de filtrado*, página 44, para obtener más información.

   De modo predeterminado, se selecciona **No cambiar configuración actual** para todas las opciones de la página.
2. Especifique si desea o no **Bloquear palabras clave**. Consulte *Cómo filtrar según palabras clave*, página 180, para obtener más información.
3. Especifique si desea o no **Bloquear tipos de archivo**, y personalice las configuraciones de bloqueo. Consulte *Cómo administrar tráfico en función del tipo de archivo*, página 193, para obtener más información.

4. En **Filtrado avanzado**, especifique si desea o no utilizar Bandwidth Optimizer para administrar el acceso a los sitios HTTP, y personalice las configuraciones de bloqueo. Consulte *Cómo utilizar Bandwidth Optimizer para administrar el ancho de banda*, página 191, para obtener más información.

   Importante

   Los cambios realizados aquí afectan a todos los filtros de categorías existentes, excepto **Bloquear todo** y **Permitir todo**.

5. Haga clic en **Aceptar** para regresar a la página Modificar categorías (consulte *Cómo modificar categorías y sus atributos*, página 175). Los cambios no se guardarán en caché hasta que haga clic en **Aceptar** en la página Modificar categorías.

Cómo cambiar el nombre de una categoría personalizada

Utilice la página **Filtro Componentes > Modificar categorías > Cambiar nombre de categoría** para cambiar el nombre o la descripción asociados con una categoría personalizada.

- Utilice el campo **Nombre de filtro** para modificar el nombre de la categoría. El nuevo nombre debe ser único y no puede superar los 50 caracteres.

  El nombre no puede incluir ninguno de los siguientes caracteres:

  ```
  * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
  ```

- Utilice el campo **Descripción** para modificar la descripción de la categoría. La descripción no puede superar los 255 caracteres.

  Las restricciones de caracteres que se aplican a los nombres de filtro también se aplican a las descripciones, con dos excepciones: las descripciones pueden incluir puntos (.) y comas (,).

Cuando termine de realizar cambios, haga clic en **Aceptar** para regresar a la página Modificar categorías. Los cambios no se guardarán en caché hasta que haga clic en **Aceptar** en la página Modificar categorías.

Cómo crear una categoría personalizada

Temas relacionados:

- *Cómo modificar categorías y sus atributos*, página 175
- *Cómo filtrar según palabras clave*, página 180
- *Cómo redefinir el filtrado para sitios específicos*, página 182

Además de utilizar las más de 90 categorías definidas por Websense en la base de datos principal, puede definir sus propias **categorías personalizadas** para

proporcionar filtrados e informes más precisos. Por ejemplo, cree categorías personalizadas como:

- **Viajes laborales**, para agrupar sitios de proveedores aprobados, que los empleados puedan utilizar para comprar boletos de aerolíneas y realizar reservas de automóviles y en hoteles
- **Materiales de referencia**, para agurpar sitios de diccionarios y enciclopedias considerados apropiados para estudiantes de escuelas primarias
- **Desarrollo profesional**, para agrupar sitios de capacitación y demás recursos que los empleados pueden utilizar para desarrollar sus habilidades laborales

Utilice la página **Administración de políticas > Componentes de filtro > Modificar categorías > Agregar categoría** para agregar categorías personalizadas a cualquier categoría principal. Puede crear hasta 100 categorías personalizadas.

1. Especifique un **Nombre de categoría** único y descriptivo. El nombre no puede incluir ninguno de los siguientes caracteres:

   ```
   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

2. Especifique una **Descripción** para la nueva categoría.

   Las restricciones de caracteres que se aplican a los nombres de filtro también se aplican a las descripciones, con dos excepciones: las descripciones pueden incluir puntos (.) y comas (,).

3. De la lista **Agregar a**, seleccione una categoría principal. De modo predeterminado, se selecciona **Todas las categorías**.
4. Especifique los sitios (URL o direcciones IP) que desea agregar a esta categoría. Consulte *Cómo recategorizar URL*, página 184, para obtener más información.

   También puede modificar esta lista después de crear la categoría.

5. Especifique las palabras clave que desea asociar con esta categoría. Consulte *Cómo filtrar según palabras clave*, página 180, para obtener más información.

   También puede modificar esta lista después de crear la categoría.

6. Defina una **Acción** de filtrado predeterminada para aplicar a esta categoría en todos los filtros de categorías existentes. Luego podrá modificar esta acción en los filtros individuales.

   Nota

   Los filtros de categorías copiados a un rol de administración delegado establecen la acción de filtrado a Permitir para las categorías personalizadas creadas en el rol. Los administradores delegados deben actualizar los filtros de categorías copiados con el fin de establecer la acción deseada para sus categorías personalizadas específicas del rol.

7. Active las acciones de **Filtrado avanzado** (bloqueo de palabras clave, bloqueo de tipos de archivos o bloqueo de ancho de banda) que se deben aplicar a esta categoría en todos los filtros de categorías existentes.

8. Cuando termine de definir la nueva categoría, haga clic en **Aceptar** para guardar los cambios en caché y regresar a la página Modificar categorías. Los cambios no se implementarán hasta que haga clic en **Guardar todo**.

La nueva categoría se incorpora a la lista de Categorías y aparece la información sobre palabra clave y URL personalizada para esa categoría.

Cómo filtrar según palabras clave

Temas relacionados:

- *Cómo recategorizar URL*, página 184
- *Cómo configurar los valores de filtrado de Websense*, página 56
- *Cómo crear un filtro de categorías*, página 49
- *Cómo modificar un filtro de categorías*, página 50
- *Cómo trabajar con categorías*, página 175

Las palabras clave se asocian con categorías y luego se utilizan para ofrecer protección contra sitios que no han sido explícitamente agregados a la base de datos principal o definidos como una URL personalizada. Se necesitan tres pasos para activar el bloqueo por palabra clave:

1. Habilitar el bloqueo de palabras clave a nivel global (consulte *Cómo configurar los valores de filtrado de Websense*, página 56).
2. Definir palabras clave asociadas con una categoría (consulte *Cómo definir palabras clave*, página 181).
3. Habilitar el bloqueo de palabras clave para la categoría en un filtro de categorías activo (consulte *Cómo modificar un filtro de categorías*, página 50).

Cuando se han definido las palabras clave y se ha activado el bloqueo de palabras clave para una categoría específica, el software de Websense bloquea cualquier sitio cuya URL contenga una palabra clave y registra el sitio como perteneciente a la categoría especificada. El sitio se bloquea incluso cuando otras URL en la categoría están permitidas.

Por ejemplo, si la categoría Deportes está permitida en un filtro de categorías activo, pero usted desea bloquear el acceso a sitios de básquetbol, puede asociar la palabra clave “nba” con Deportes y activar el bloqueo por palabra clave. Esto significa que las siguientes URL quedan bloqueadas y registradas como pertenecientes a la categoría Deportes:

- sports.espn.go.com/**nba**/
- moder**nba**kery.com
- moder**nba**biesandchildren.com
- fashio**nba**r.com

Tenga precaución al definir palabras clave para evitar bloqueos no intencionados.

> **Importante**
> Si utiliza Websense Web Security, evite asociar las palabras clave con cualquiera de las subcategorías de Protección Ampliada. No se implementa el bloqueo por palabras clave para estas categorías.

Cuando una solicitud es bloqueada sobre la base de una palabra clave, esto se indica en la página de bloqueo de Websense que el usuario recibe.

Cómo definir palabras clave

Temas relacionados:

- *Cómo modificar un filtro de categorías*, página 50
- *Cómo trabajar con categorías*, página 175
- *Cómo filtrar según palabras clave*, página 180
- *Cómo utilizar expresiones regulares*, página 197

Una palabra clave es una cadena de caracteres (como una palabra, frase o acrónimo) que es posible encontrar en una URL. Asigne palabras clave a una categoría y luego active el bloqueo por palabras clave en un filtro de categorías.

Utilice la página **Administración de políticas > Componentes de filtro > Modificar categorías > Agregar palabras clave** para asociar palabras clave con categorías. Si necesita realizar modificaciones a una definición de palabra clave, utilice la página **Modificar palabras clave**.

Al definir palabras clave, tenga la precaución de evitar bloqueos no intencionados. Por ejemplo, al utilizar la palabra clave “sex” con la intención de bloquear el acceso a sitios con material para adultos, puede terminar bloqueando solicitudes de motores de búsqueda para palabras como sextuplets o City of Essex, y sitios como m**sex**change.org (Tecnología de la información), vega**sex**perience.com (Viajes), y sci.esa.int/mar**sex**press (Instituciones educativas).

Especifique una palabra clave por línea.

- No incluya espacios en las palabras clave. Las cadenas CGI y URL no contienen espacios entre las palabras.
- Incluya una barra invertida (\) antes de caracteres especiales como:

  ```
  . , # ? * +
  ```

  Si no incluye la barra invertida, el software de Websense ignorará el carácter especial.

- Si utiliza Websense Web Security, evite asociar las palabras clave con cualquiera de las subcategorías de Protección Ampliada. No se implementa el bloqueo por palabras clave para estas categorías.

Cuando termine de agregar o modificar palabras clave, haga clic en **Aceptar** para guardar los cambios en caché y regresar a la página Modificar categorías. Los cambios no se implementarán hasta que haga clic en **Guardar todo**.

Para que se implemente el bloqueo por palabra clave, también debe:

1. Activar el bloqueo de palabras clave mediante la página **Configuración > Filtrado** (consulte *Cómo configurar los valores de filtrado de Websense*, página 56).
2. Activar el bloqueo de palabras clave en uno o más filtros de categorías activos (consulte *Cómo modificar un filtro de categorías*, página 50).

Cómo redefinir el filtrado para sitios específicos

Temas relacionados:

- *Cómo crear una categoría personalizada*, página 178
- *Cómo filtrar según palabras clave*, página 180
- *Cómo definir URL sin filtrar*, página 183
- *Cómo recategorizar URL*, página 184

Con las URL personalizadas, usted puede:

- Aplicar filtrado más preciso a sitios que no se encuentran en la base de datos principal de Websense. De modo predeterminado, se utiliza la acción aplicada a la categoría **Varios/Sin categorizar** para filtrar dichos sitios.
- Filtrar sitios en forma diferente que sus categorías de la base de datos principal.

El software de Websense busca definiciones de URL personalizadas para un sitio antes de consultar la base de datos principal y, por lo tanto, filtra el sitio según la categoría asignada a la URL personalizada.

Existen dos tipos de URL personalizadas: sin filtrar y recategorizadas.

- Las URL sin filtrar están permitidas para todos los usuarios que no se rigen por el filtro de categorías Bloquear todo o por un filtro de acceso limitado (consulte *Cómo definir URL sin filtrar*, página 183).
- Las URL recategorizadas han sido movidas de su categoría de la base de datos principal hacia otra categoría personalizada o definida por Websense (consulte *Cómo recategorizar URL*, página 184).

  Una URL recategorizada no se bloquea de manera predeterminada. Se filtra de acuerdo con la acción aplicada a su nueva categoría en cada filtro de categorías activo.

Cuando un sitio es filtrado según la categoría de su base de datos principal, el software de Websense asocia la URL con su dirección IP equivalente. Este no es el caso para las URL personalizadas. Para cambiar el método de filtrado de un sitio, defina su URL y su dirección IP como una URL personalizada.

Si es posible acceder a un sitio mediante múltiples URL, defina cada una de las URL que se pueden utilizar para acceder a dicho sitio como una URL personalizada para asegurarse de que el mismo esté permitido o bloqueado según lo desee.

Si un sitio es movido a un nuevo dominio y se utiliza una redirección de HTTP para enviar usuarios a la nueva URL, la nueva URL no se filtra automáticamente de la misma manera que el sitio que la redirecciona. Para asegurarse de que el sitio sea filtrado correctamente en su nueva dirección, cree una nueva URL personalizada.

Cómo definir URL sin filtrar

Temas relacionados:

- *Cómo trabajar con categorías*, página 175
- *Cómo redefinir el filtrado para sitios específicos*, página 182
- *Cómo recategorizar URL*, página 184

Utilice la página **Política Administración > Componentes de filtro > URL sin filtrar** para definir una lista de sitios a los que cualquier usuario puede acceder, excepto cuando está regido por el filtro de categorías Bloquear todo o un filtro de acceso limitado.

La lista **Sitios permitidos** ubicada en la parte derecha del panel de contenido enumera los sitios sin filtrar (URL y direcciones IP) y las expresiones regulares que usted ha definido (consulte *Cómo utilizar expresiones regulares*, página 197). Cada sitio está asociado con una categoría.

- La URL puede asociarse con la categoría de su base de datos principal, o recategorizarse.
- Cuando un usuario solicita acceso a la URL sin filtrar, la solicitud se registra como una URL personalizada permitida en la categoría a la cual ha sido asignada.

Para agregar una URL sin filtrar:

1. En **Definir URL sin filtrar**, especifique una URL o dirección IP por línea y luego haga clic en el botón de la flecha derecha (>).

   El software de Websense no asocia una URL personalizada con su dirección IP equivalente. Para permitir tanto la dirección de URL como la dirección IP de un sitio, agregue ambas a la lista URL sin filtrar.
2. Para agregar expresiones regulares que establezcan coincidencias entre varios sitios, haga clic en **Opciones avanzadas**. Ingrese una expresión regular por línea y luego haga clic en el botón de la flecha derecha para mover las expresiones a la lista de URL sin filtrar. Para comprobar que un patrón coincide con los sitios pretendidos, haga clic en **Probar**.

Consulte *Cómo utilizar expresiones regulares*, página 197, para obtener más información.

3. Cuando termine, haga clic en **Aceptar** para guardar los cambios en caché y regresar a la página Modificar categorías. Los cambios no se implementarán hasta que haga clic en **Guardar todo**.

Para eliminar un sitio de la lista URL sin filtrar, seleccione la URL, dirección IP o expresión regular y luego haga clic en **Eliminar**.

Cómo recategorizar URL

Temas relacionados:

- *Cómo trabajar con categorías*, página 175
- *Cómo redefinir el filtrado para sitios específicos*, página 182
- *Cómo definir URL sin filtrar*, página 183

Utilice la página **Política Administración > Componentes de filtro > Modificar categorías > Recategorizar URL** para agregar sitios individuales a cualquier categoría. Realice modificaciones a los sitios recategorizados existentes en la página **Modificar URL**.

Recategorice URL para cambiar el modo de filtrar y registrar sitios individuales. Cuando usted agrega sitios recategorizados:

- Ingrese cada URL o dirección IP en una línea por separado.
- Incluya el protocolo para cualquier sitio que no sea HTTP. Si omite el protocolo, el software de Websense filtra el sitio como sitio HTTP.

  Para sitios HTTPS, incluya también el número de puerto (https://63.212.171.196:443/, https://www.onlinebanking.com:443/).
- El software de Websense reconoce las URL personalizadas exactamente como se las especificó. Si la categoría Portales y motores de búsqueda está bloqueada, pero usted recategoriza **www.yahoo.com** en una categoría permitida, el sitio estará permitido sólo si los usuarios escriben la dirección completa. Si un usuario escribe images.search.yahoo.com, o sólo yahoo.com, el sitio igual estará bloqueado. Sin embargo, si usted recategoriza **yahoo.com**, todos los sitios con yahoo.com en la dirección estarán permitidos.

Cuando termine de agregar o modificar sitios recategorizados, haga clic en **Aceptar** para guardar los cambios en caché y regresar a la página Modificar categorías. Los cambios no se implementarán hasta que haga clic en **Guardar todo**.

Después de guardar URL recategorizadas, utilice la herramienta **Categoría de URL** ubicada en el panel de acceso directo a la derecha para comprobar que el sitio se asigne a la categoría correcta. Consulte *Cómo utilizar la Caja de herramientas para comprobar el patrón de filtrado*, página 198.

Cómo trabajar con protocolos

La base de datos principal de Websense incluye definiciones de protocolos utilizadas para filtrar protocolos de Internet que no sean HTTP, HTTPS y FTP. Estas definiciones incluyen aplicaciones de Internet y otros métodos de transferencia de datos como aquellos utilizados para mensajería instantánea, transmisiones multimedia, intercambio de archivos, transferencia de archivos, correo en Internet y otras operaciones de red y base de datos.

Estas definiciones de protocolos también se pueden utilizar para filtrar protocolos o aplicaciones que omiten un firewall mediante el uso de puertos normalmente utilizados para el tráfico HTTP. Por ejemplo, los datos de mensajería instantánea pueden ingresar a una red cuyo firewall bloquea protocolos de mensajería instantánea mediante el uso de puertos HTTP. El software de Websense identifica con exactitud estos protocolos y los filtra de acuerdo con las políticas que configure.

Nota
Es necesario Network Agent para activar el filtrado basado en protocolos.

Además de utilizar definiciones de protocolos definidas por Websense, puede definir protocolos personalizados para filtrado. Las definiciones de protocolos personalizados pueden basarse en direcciones IP o números de puertos, y se pueden modificar.

Para bloquear el tráfico por un puerto específico, asocie dicho número de puerto con un protocolo personalizado, y asigne la acción predeterminada Bloquear a dicho protocolo.

Para trabajar con definiciones de protocolos personalizados, vaya a **Administración de políticas > Componentes de filtro** y luego haga clic en**Protocolos**. Consulte *Cómo modificar protocolos personalizados*, página 186, y *Cómo crear un protocolo personalizado*, página 189, para obtener detalles.

Cómo filtrar protocolos

Temas relacionados:

- *Cómo trabajar con protocolos*, página 185
- *Cómo modificar protocolos personalizados*, página 186
- *Cómo crear un protocolo personalizado*, página 189
- *Cómo agregar o modificar identificadores de protocolos*, página 187
- *Cómo agregar un protocolo definido por Websense*, página 191

Cuando se instala Network Agent, el software de Websense puede bloquear el contenido de Internet transmitido por puertos específicos, o que utilizan direcciones IP

específicas, o indicados por firmas específicas, independientemente de la naturaleza de los datos. De modo predeterminado, el bloqueo de un puerto intercepta todo el contenido de Internet que ingresa a la red por ese puerto, independientemente del origen.

> **Nota**
> En ocasiones, es posible que no se bloquee el tráfico de red interno que se envía por un puerto determinado, incluso cuando el protocolo que utiliza dicho puerto está bloqueado. El protocolo puede enviar datos vía un servidor interno con mayor rapidez que el tiempo que necesita Network Agent para capturar y procesar los datos. Esto no ocurre con los datos que se originan fuera de la red.

Cuando se realiza una solicitud de protocolo, el software de Websense utiliza los siguientes pasos para determinar si debe bloquear o permitir la solicitud:

1. Determina el nombre del protocolo (o la aplicación de Internet).
2. Identifica el protocolo sobre la base de la dirección de destino solicitada.
3. Busca números de puertos o direcciones IP relacionadas en definiciones de protocolos personalizadas.
4. Busca números de puertos, direcciones IP o firmas relacionadas en las definiciones de protocolos definidas por Websense.

Si el software de Websense no puede determinar ninguno de estos datos, se permite todo el contenido asociado con el protocolo.

Cómo modificar protocolos personalizados

Temas relacionados:

- *Cómo trabajar con protocolos*, página 185
- *Cómo crear un protocolo personalizado*, página 189
- *Cómo crear un filtro de protocolos*
- *Cómo modificar un filtro de protocolos*
- *Cómo trabajar con categorías*

Utilice la página **Administración de políticas > Componentes de filtro > Modificar protocolos** para crear y modificar definiciones de protocolo personalizadas y para revisar definiciones de protocolo definidas por Websense. Los protocolos definidos por Websense no pueden modificarse.

La lista Protocolos incluye la totalidad de los protocolos personalizados y definidos por Websense. Haga clic en un protocolo o grupo de protocolos para obtener información acerca del elemento seleccionado en la parte derecha del panel de contenido.

Para agregar un nuevo protocolo personalizado, haga clic en **Agregar protocolo**, y luego continúe con *Cómo crear un protocolo personalizado*, página 189.

Para modificar una definición de protocolo:

1. Seleccione el protocolo en la lista Protocolos. La definición del protocolo aparece a la derecha de la lista.
2. Haga clic en **Sustituir acción** para cambiar la acción de filtrado aplicada a este protocolo en todos los filtros de protocolo (consulte *Cómo realizar cambios de filtrado global de protocolos*, página 188).
3. Haga clic en **Agregar identificador** para definir identificadores de protocolo adicionales para este protocolo (consulte *Cómo agregar o modificar identificadores de protocolos*, página 187).
4. Seleccione un identificador en la lista y haga clic en **Modificar** para realizar cambios al **Puerto**, al **Rango de direcciones IP** o al **Método de transporte** definido por el identificador.
5. Cuando termine, haga clic en **Aceptar** para guardar los cambios en caché. Los cambios no se implementarán hasta que haga clic en **Guardar todo**.

Para eliminar una definición de protocolo, seleccione un elemento en la lista Protocolos y luego haga clic en **Eliminar**.

Cómo agregar o modificar identificadores de protocolos

Utilice la página **Componentes de filtro > Modificar Protocolos > Agregar identificador de protocolo** para definir identificadores de protocolo adicionales para un protocolo personalizado existente. Utilice la página **Modificar identificador de protocolo** para realizar cambios a un identificador definido anteriormente.

Antes de crear o cambiar un identificador, compruebe que el nombre de protocolo correcto aparezca junto a **Protocolo seleccionado**.

Al trabajar con identificadores de protocolos, recuerde que al menos un criterio (puerto, dirección IP o tipo de transporte) debe ser único para cada protocolo.

1. Especifique cuáles son los **Puertos** que están incluidos en este identificador.
   - Si selecciona **Todos los puertos**, ese criterio se superpone con otros puertos o direcciones IP ingresados en otras definiciones de protocolos.
   - Los rangos de puertos no se consideran únicos si se superponen. Por ejemplo, el rango de puertos 80-6000 se superpone con el rango 4000-9000.
   - Tenga precaución al definir un protocolo en el puerto 80 o 8080. Network Agent escucha las solicitudes de Internet en estos puertos.

     Como los protocolos personalizados tienen prioridad sobre los protocolos de Websense, si usted define un protocolo personalizado utilizando el puerto 80, todos los demás protocolos que utilizan el puerto 80 son filtrados y registrados como el protocolo personalizado.
2. Especifique cuáles son las **Direcciones IP** que están incluidas en este identificador.

- Si selecciona **Todas las direcciones IP externas**, ese criterio se superpone con cualquier otra dirección IP ingresada en otras definiciones de protocolos.
- Los rangos de direcciones IP no se consideran únicos si se superponen.

3. Especifique qué método de **Transporte de protocolos** está incluido en este identificador.
4. Haga clic en **Aceptar** para guardar los cambios en caché y regresar a la página Modificar protocolos. Los cambios no se implementarán hasta que haga clic en **Guardar todo**.

Cómo cambiar el nombre de un protocolo personalizado

Utilice la página **Componentes de filtro > Modificar protocolos > Cambiar nombre de protocolo** para cambiar el nombre de un protocolo personalizado, o moverlo a un grupo de protocolos diferente.

- Utilice el campo **Nombre** para modificar el nombre del protocolo. El nuevo nombre no puede superar los 50 caracteres.

  El nombre no puede incluir ninguno de los siguientes caracteres:

  ```
  * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
  ```

- Para mover el protocolo a un grupo de protocolos diferente, seleccione el nuevo grupo del campo **En grupo**.

Cuando termine de realizar cambios, haga clic en **Aceptar** para regresar a la página Modificar protocolos. También debe hacer clic en **Aceptar** en la página Modificar protocolos para guardar los cambios en caché.

Cómo realizar cambios de filtrado global de protocolos

Utilice la página **Componentes de filtro > Modificar protocolos > Sustituir acción** para cambiar el método de filtrado de un protocolo en todos los filtros de protocolos existentes. Esto también determina la acción predeterminada aplicada al protocolo en filtros nuevos.

A pesar de que este cambio sustituye la acción de filtrado aplicada en todos los filtros de protocolos existentes, los administradores después pueden modificar dichos filtros para aplicar una acción diferente.

1. Compruebe que el nombre de protocolo correcto aparezca junto a **Protocolo seleccionado**.
2. Seleccione una nueva **Acción** (Permitir o Bloquear) para aplicar a este protocolo. De modo predeterminado, se selecciona **Sin cambios**. Consulte *Acciones de filtrado*, página 44, para obtener más información.
3. Especifique nuevas opciones de **Registro**. Debe registrar el tráfico de protocolo para que aparezca en los informes y active alertas de uso de protocolos.

4. Especifique si **Bandwidth Optimizer** se utiliza para administrar el acceso a este protocolo. Consulte *Cómo utilizar Bandwidth Optimizer para administrar el ancho de banda*, página 191, para obtener más información.

   Importante

   Los cambios realizados aquí afectan a todos los filtros de protocolos existentes, excepto **Bloquear todo** y **Permitir todo**.

5. Cuando termine, haga clic en **Aceptar** para regresar a la página Modificar protocolos (consulte *Cómo modificar protocolos personalizados*, página 186). También debe hacer clic en **Aceptar** en la página Modificar protocolos para guardar los cambios en caché.

Cómo crear un protocolo personalizado

Temas relacionados:

- *Cómo trabajar con protocolos*, página 185
- *Cómo filtrar protocolos*, página 185
- *Cómo modificar protocolos personalizados*, página 186
- *Cómo agregar un protocolo definido por Websense*, página 191

Utilice la página **Componentes de filtro > Protocolos > Agregar protocolo** para definir un nuevo protocolo personalizado.

1. Ingrese un **Nombre** para el protocolo.

   El nombre no puede incluir ninguno de los siguientes caracteres:

   ```
   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

   Un protocolo personalizado puede tener asignado el mismo nombre que un protocolo definido por Websense, con el fin de expandir la cantidad de direcciones IP o puertos asociados con el protocolo original. Consulte *Cómo agregar un protocolo definido por Websense*, página 191, para obtener más información.

2. Expanda la lista desplegable **Agregar protocolo a este grupo** y luego seleccione un grupo de protocolos. El nuevo protocolo aparece en este grupo en todas las listas de protocolos y filtros.

3. Defina un único **Identificador de protocolo** (conjunto de **puertos**, **direcciones IP** y **métodos de transporte**) para dicho grupo. Después puede agregar identificadores adicionales de la página Modificar protocolo.

   Siga las siguientes pautas para crear identificadores de protocolos:

   - Al menos un criterio (puerto, dirección IP o tipo de transporte) debe ser único para cada identificador de protocolo.

- Si selecciona **Todos los puertos** o **Todas las direcciones IP externas**, ese criterio se superpone con cualquier otra dirección IP o puerto ingresado en otras definiciones de protocolos.
- Los rangos de puertos o rangos de direcciones IP no se consideran únicos si se superponen. Por ejemplo, el rango de puertos 80-6000 se superpone con el rango 4000-9000.

> **Nota**
>
> Tenga precaución al definir un protocolo en el puerto 80 o 8080. Network Agent escucha las solicitudes de Internet en estos puertos.
>
> Como los protocolos personalizados tienen prioridad sobre los protocolos de Websense, si usted define un protocolo personalizado utilizando el puerto 80, todos los demás protocolos que utilizan el puerto 80 son filtrados y registrados como el protocolo personalizado.

Las siguientes tablas proporcionan ejemplos de definiciones de protocolos válidas e inválidas:

Puerto	Dirección IP	Método de transporte	¿Combinación aceptada?
70	CUALQUIERA	TCP	Sí, el número de puerto hace que cada identificador de protocolo sea único.
90	CUALQUIERA	TCP	

Puerto	Dirección IP	Método de transporte	¿Combinación aceptada?
70	CUALQUIERA	TCP	No, las direcciones IP no son únicas. 10.2.1.201 está incluida en la serie “CUALQUIERA”.
70	10.2.1.201	TCP	

Puerto	Dirección IP	Método de transporte	¿Combinación aceptada?
70	10.2.3.212	TCP	Sí, las direcciones IP son únicas.
70	10.2.1.201	TCP	

4. En Acción de filtrado predeterminada, especifique la acción predeterminada (**Permitir** o **Bloquear**) que debe aplicarse a este protocolo en todos los filtros de protocolos activos:
   - Indique si el tráfico que utiliza este protocolo se debe **registrar**. El tráfico de protocolo debe registrarse para que aparezca en informes y active alertas de uso de protocolos.

- Indique si el acceso a este protocolo debe estar regulado por **Bandwidth Optimizer** (consulte *Cómo utilizar Bandwidth Optimizer para administrar el ancho de banda*, página 191).

5. Cuando termine, haga clic en **Aceptar** para regresar a la página Modificar protocolos. La nueva definición de protocolo aparece en la lista Protocolos.
6. Haga clic en **Aceptar** nuevamente para guardar sus cambios en caché. Los cambios no se implementarán hasta que haga clic en **Guardar todo**.

Cómo agregar un protocolo definido por Websense

Usted no puede agregar un número de puerto o dirección IP directamente a un protocolo definido por Websense. Sin embargo, es posible crear un protocolo personalizado con el mismo nombre que el protocolo definido por Websense, y luego agregar puertos o direcciones IP a su definición.

Cuando un protocolo personalizado y un protocolo definido por Websense tienen el mismo nombre, el software de Websense busca tráfico de protocolo en las direcciones IP y los puertos especificados en ambas definiciones.

En los informes, los nombres de protocolos personalizados tienen un prefijo “C_”. Por ejemplo, si usted creó un protocolo personalizado para SQL_NET y especificó números de puertos adicionales, los informes muestran C_SQL_NET cuando el protocolo usa los números de puertos en el protocolo personalizado.

Cómo utilizar Bandwidth Optimizer para administrar el ancho de banda

Temas relacionados:

- *Cómo trabajar con categorías*, página 175
- *Cómo trabajar con protocolos*, página 185
- *Cómo configurar los límites predeterminados de Bandwidth Optimizer*, página 192

Cuando usted crea un filtro de categorías o protocolos, puede optar por limitar el acceso a una categoría o a un protocolo en función del uso del ancho de banda.

- Bloquee el acceso a categorías o protocolos en función del uso total del ancho de banda de red.
- Bloquee el acceso a categorías en función del uso total del ancho de banda por tráfico HTTP.
- Bloquee el acceso a un protocolo específico en función del uso del ancho de banda por ese protocolo.

Por ejemplo:

- Bloquee el protocolo de mensajería instantánea AOL si el uso total del ancho de banda de red supera el 50% del ancho de banda disponible, o si el uso actual del ancho de banda para AIM supera el 10% del ancho de banda de red total.
- Bloquee la categoría Deportes cuando el uso total del ancho de banda de red alcanza el 75%, o cuando el uso del ancho de banda por todo el tráfico HTTP alcanza el 60% del ancho de banda de red disponible.

El uso de ancho de banda de protocolos incluye tráfico por todos los puertos, direcciones IP o firmas definidos para el protocolo. Esto significa que si un protocolo o una aplicación de Internet utiliza múltiples puertos para transferencia de datos, el tráfico por todos los puertos incluidos en la definición de protocolo se cuenta para el total del uso de ancho de banda de ese protocolo. Sin embargo, si una aplicación de Internet utiliza un puerto no incluido en la definición del protocolo, el tráfico por ese puerto no se incluye en las mediciones del uso del ancho de banda.

El software de Websense registra el ancho de banda utilizado por protocolos basados en TCP y UDP filtrados.

Websense, Inc., actualiza regularmente las definiciones de protocolos de Websense para garantizar la precisión de las mediciones del ancho de banda.

Network Agent envía datos de ancho de banda de red a Filtering Service a intervalos predeterminados. Esto asegura que el software de Websense supervise correctamente el uso de ancho de banda y reciba mediciones lo más cercanas al promedio.

Cuando las opciones de filtrado en función del ancho de banda están activas, el software de Websense comienza el filtrado basado en el ancho de banda 10 minutos después de la configuración inicial y 10 minutos después de reiniciado cada Websense Policy Server. Esta demora garantiza la exactitud de la medición de los datos de ancho de banda y el uso de estos datos en el filtrado.

Cuando una solicitud es bloqueada en función de restricciones al ancho de banda, la página de bloqueo de Websense muestra esta información en el campo **Motivo**. Para obtener más información, consulte *Páginas de bloqueo*, página 85.

Cómo configurar los límites predeterminados de Bandwidth Optimizer

Temas relacionados:

- *Cómo modificar un filtro de categorías*, página 50
- *Cómo modificar un filtro de protocolos*, página 52
- *Cómo utilizar Bandwidth Optimizer para administrar el ancho de banda*, página 191

Antes de especificar la configuración de ancho de banda en las políticas, verifique los umbrales de ancho de banda predeterminados que desencadenan los ajustes de filtrado en función del ancho de banda. Los valores definidos por Websense son:

- Ancho de banda predeterminado de la red: **50%**
- Ancho de banda predeterminado por protocolo: **20%**

Los valores de ancho de banda predeterminados son guardados por Policy Server, e implementados por todas las instancias asociadas de Network Agent. Si tiene múltiples Policy Servers, los cambios a los valores de ancho de banda predeterminados en uno de ellos no afectan a los demás.

Para cambiar los valores de ancho de banda predeterminados:

1. En Websense Manager, vaya a **Configuración > Filtrado**.
2. Ingrese los umbrales de uso de ancho de banda que desencadenarán el filtrado en función del ancho de banda, cuando se activa el filtrado de ancho de banda.
   - Cuando una categoría o protocolo es bloqueado en función del tráfico para toda la red, **Ancho de banda predeterminado de la red** define el umbral de filtrado predeterminado.
   - Cuando una categoría o protocolo es bloqueado en función del tráfico para el protocolo, el **Ancho de banda predeterminado por protocolo** define el umbral de filtrado predeterminado.

   Usted puede modificar los valores de umbral predeterminados para cada categoría o protocolo en cualquier filtro de categorías o protocolos.
3. Cuando termine, haga clic en **Aceptar** para guardar los cambios en caché. Los cambios no se implementarán hasta que haga clic en **Guardar todo**.

Cualquier cambio realizado a los valores predeterminados puede afectar a cualquiera de los filtros de categorías o protocolos que implementan restricciones de Bandwidth Optimizer.

- Para administrar el uso de ancho de banda asociado con un protocolo específico, modifique el o los filtros de protocolos activos.
- Para administrar el uso de ancho de banda asociado con una categoría de URL específica, modifique el o los filtros de categorías activos correspondientes.

  Cuando usted filtra categorías en función del uso de ancho de banda HTTP, el software de Websense mide el uso total del ancho de banda HTTP por todos los puertos especificados como puertos HTTP para el software de Websense.

Cómo administrar tráfico en función del tipo de archivo

Cuando crea un filtro de categorías , usted puede definir el filtrado basado en extensiones de archivos, a fin de restringir el acceso a determinados tipos de archivos de sitios en ciertas categorías. Por ejemplo, puede permitir la categoría Deportes pero bloquear los archivos de video de sitios de la categoría Deportes.

El software de Websense proporciona varios tipos de archivos predefinidos, o agrupaciones de extensiones de archivos utilizados para fines similares. Estas definiciones de tipos de archivos se mantienen en la base de datos principal, y pueden cambiar como parte de un proceso de actualización de la base de datos principal.

Puede implementar filtrado usando tipos de archivos predefinidos, modificar las definiciones de tipos de archivos existentes o crear nuevos tipos de archivos. Sin embargo, tenga en cuenta que no puede eliminar tipos de archivos definidos por Websense ni eliminar las extensiones de archivos asociadas con los mismos.

Cuando un usuario solicita un sitio, el software de Websense primero determina la categoría del sitio y luego controla que no existan extensiones de archivos filtradas.

> **Nota**
> Para implementar el filtrado total de medios de video y audio en Internet, combine el filtrado basado en protocolos con el filtrado por tipo de archivo. En este caso, el filtrado de protocolos se encarga de los medios de transmisión, mientras que el filtrado por tipo de archivo se encarga de archivos que se pueden descargar y luego reproducir.

Cuando un usuario intenta acceder a un archivo cuya extensión está bloqueada, el campo **Motivo**de la página de bloqueo de Websense muestra que el tipo de archivo fue bloqueado. Para obtener más información, consulte *Páginas de bloqueo*, página 85.

> **Nota**
> La página de bloqueo estándar no aparece si una imagen GIF o JPEG bloqueada abarca sólo una parte de una página permitida. En su lugar, la región de la imagen aparece en blanco. Esto impide que se pueda mostrar una pequeña parte de una página de bloqueo en múltiples ubicaciones en una página que de lo contrario estaría permitida.

Las definiciones de tipo de archivo pueden contener tantas o tan pocas extensiones de archivos como sean útiles para propósitos de filtrado. Por ejemplo, los tipos de archivos definidos por Websense incluyen las siguientes extensiones de archivos:

Audio	Archivos comprimidos		Ejecutables	Vídeo	
.aif	.ace	.mim	.bat	.asf	.mpg
.aifc	.arc	.rar	.exe	.asx	.mpv2
.aiff	.arj	.tar		.avi	.qt
.m3u	.b64	.taz		.ivf	.ra
.mid	.bhx	.tgz		.m1v	.ram
.midi	.cab	.tz		.mov	.wm
.mp3	.gz	.uu		.mp2	.wmp

Audio	Archivos comprimidos		Ejecutables	Vídeo	
.ogg	.gzip	.uue		.mp2v	.wmv
.rmi	.hqx	.xxe		.mpa	.wmx
.snd	.iso	.z		.mpe	.wxv
.wav	.jar	.zip			
.wax	.lzh				
.wma					

Cualquiera de las extensiones de archivos asociadas con un tipo de archivo definido por Websense se puede agregar a un tipo de archivo personalizado. Luego la extensión del archivo se filtra y registra de acuerdo con las configuraciones asociadas con el tipo de archivo personalizado.

Para ver las definiciones de tipo de archivos existentes, modificar tipos de archivos o crear tipos de archivos personalizados, vaya a **Administración de políticas > Componentes de filtro**, y luego haga clic en **Tipos de archivo**. Consulte *Cómo trabajar con tipos de archivos*, página 195, para obtener más información.

Cómo trabajar con tipos de archivos

Temas relacionados:

- *Cómo administrar tráfico en función del tipo de archivo*, página 193
- *Cómo modificar un filtro de categorías*, página 50
- *Filtrado de un sitio*, página 81

Utilice la página **Administración de políticas > Componentes de filtro > Modificar Tipos de archivo** para crear y administrar hasta 32 **tipos de archivo**. Los tipos de archivo son grupos de extensiones de archivos que pueden ser expresamente bloqueados en filtros de categorías (consulte *Cómo administrar tráfico en función del tipo de archivo*, página 193).

- Haga clic en un tipo de archivo para ver las extensiones de archivo asociadas con ese tipo.
- Para agregar extensiones al tipo de archivo seleccionado, haga clic en **Agregar extensión** y luego consulte *Cómo agregar extensiones de archivo a un tipo de archivo*, página 196, para obtener más instrucciones.
- Para crear un tipo de archivo nuevo, haga clic en **Agregar tipo de archivo** y luego consulte *Cómo agregar tipos de archivos personalizados*, página 196, para obtener más instrucciones.
- Para eliminar un tipo o una extensión de archivo personalizado, seleccione un elemento y luego haga clic en **Eliminar**.

No puede eliminar tipos de archivos definidos por Websense ni eliminar las extensiones de archivos asociadas con los mismos.

Sin embargo, puede agregar extensiones de archivos asociadas con un tipo de archivo definido por Websense a un tipo de archivo personalizado. Luego la extensión del archivo se filtra y registra de acuerdo con las configuraciones asociadas con el tipo de archivo personalizado. No puede agregar la misma extensión a varios tipos de archivos personalizados.

Cuando termine de realizar cambios a las definiciones de tipos de archivos, haga clic en **Aceptar**. Los cambios no se implementarán hasta que haga clic en **Guardar todo**.

Cómo agregar tipos de archivos personalizados

Utilice la página **Componentes de filtro > Modificar tipos de archivo > Agregar tipo de archivo** para definir tipos de archivos personalizados.

1. Especifique un **Nombre de tipo de archivo** único.

   Puede crear un tipo de archivo personalizado con el mismo nombre que un tipo de archivo definido por Websense para agregar extensiones de archivo adicionales al tipo de archivo existente.
2. Ingrese las extensiones de archivo, una por línea, en la lista **Extensiones de archivo**. No es necesario incluir un punto (“.”) antes de cada extensión.
3. Haga clic en **Aceptar** para regresar a la pantalla Modificar tipos de archivo. El nuevo tipo de archivo aparece en la lista Tipos de archivo.
4. Cuando termine de trabajar con definiciones de tipo de archivo, haga clic en **Aceptar** en la página Modificar tipos de archivo. Los cambios no se implementarán hasta que haga clic en **Guardar todo**.

Cómo agregar extensiones de archivo a un tipo de archivo

Utilice la página **Componentes de filtro > Modificar tipos de archivo > Agregar extensiones de archivo** para agregar extensiones de archivos al tipo de archivo seleccionado.

1. Compruebe que el nombre del tipo de archivo previsto aparezca junto a **Tipo de archivo seleccionado**.
2. Ingrese las extensiones de archivo, una por línea, en la lista **Extensiones de archivo**. No es necesario incluir un punto (“.”) antes de cada extensión.
3. Haga clic en **Aceptar** para regresar a la pantalla Modificar tipos de archivo. Las nuevas extensiones de archivo aparecen en la lista Extensiones de archivo personalizadas.
4. Cuando termine de trabajar con definiciones de tipo de archivo, haga clic en **Aceptar** en la página Modificar tipos de archivo. Los cambios no se implementarán hasta que haga clic en **Guardar todo**.

Cómo utilizar expresiones regulares

Una **expresión regular** es una plantilla o un patrón que se utiliza para establecer coincidencias entre varias cadenas o grupos de caracteres. Puede utilizar expresiones regulares en filtros de acceso limitado o para definir palabras clave o URL personalizadas. Luego Websense filtering intenta establecer coincidencia con el patrón general, en vez de con una palabra clave o URL única y específica.

Analice esta expresión regular simple:

```
dominio.(com|org|net)
```

Este patrón de expresión coincide con las URL:

- dominio.com
- dominio.org
- dominio.net

Utilice expresiones regulares con precaución. Proporcionan una poderosa herramienta de filtrado, pero fácilmente pueden bloquear o permitir sitios inesperados. Además, las expresiones regulares construidas deficientemente pueden generar filtrado excesivo.

Importante

El uso de expresiones regulares como criterios de filtrado puede aumentar el uso de la CPU. Está demostrado que con 100 expresiones regulares, el uso promedio de la CPU en el equipo de Filtering Service se incrementa en un 20%.

El software de Websense admite, en su mayoría, la sintaxis de expresiones regulares, con unas pocas excepciones: Algunas de las sintaxis no admitidas no sirven para vincular cadenas que se pueden encontrar en una URL.

Las sintaxis de expresiones regulares no admitidas incluyen:

```
(?<=patrón)cadena
\N{nombre}
(?(condición)pat1)
(?(condición)pat1|pat2)
(?{código})
(?<!patrón)cadena
(?imsx-imsx)
\pP
\PP
??{código})
```

Para obtener más ayuda con expresiones regulares, consulte:

en.wikipedia.org/wiki/Regular_expression

www.regular-expressions.info/

Cómo utilizar la Caja de herramientas para comprobar el patrón de filtrado

El panel derecho de acceso directo en Websense Manager incluye una **Caja de herramientas** que le permite realizar comprobaciones rápidas de su configuración de filtrado.

Haga clic en el nombre de una herramienta para acceder a la misma. Haga clic en el nombre nuevamente para ver la lista de herramientas. Para obtener más información acerca del uso de una herramienta, consulte:

- *Categoría de URL*, página 198
- *Comprobar política*, página 198
- *Probar filtrado*, página 199
- *Acceso a URL*, página 199
- *Investigar usuario*, página 200

También puede hacer clic en **Portal de soporte** para acceder al sitio Web de Soporte técnico de Websense en una nueva ventana o ficha de navegador. Desde el Portal de soporte, usted puede utilizar Knowledge Base para acceder a tutoriales, sugerencias, artículos y documentación.

Categoría de URL

Para descubrir cómo se categoriza un sitio en un momento dado:

1. Haga clic en **Categoría de URL** en la Caja de herramientas.
2. Especifique una URL o dirección IP.
3. Haga clic en **Ir**.

La categoría actual del sitio aparece en una ventana emergente. Si su empresa ha recategorizado la URL, se muestra la nueva categoría.

La categorización del sitio puede depender de la versión de la base de datos principal (incluyendo actualizaciones en tiempo real) que usted está utilizando.

Comprobar política

Utilice esta herramienta para determinar qué políticas se aplican a un cliente específico. Los resultados son específicos para la hora y el día actual.

1. Haga clic en **Comprobar política** en la Caja de herramientas.
2. Para identificar un directorio o cliente de equipo, especifique:
   - Un nombre de usuario totalmente calificado

Para examinar el árbol de directorios con el fin de identificar al usuario, haga clic en **Buscar usuario** (consulte *Cómo identificar un usuario para comprobar política o probar filtrado*, página 200).

- Una dirección IP

3. Haga clic en **Ir**.

El nombre de una o más políticas aparece en una ventana emergente. Aparecen múltiples políticas únicamente cuando no se ha asignado ninguna política al usuario, sino que se han asignado políticas a múltiples grupos, dominios o unidades organizativas a las cuales el usuario pertenece.

Incluso cuando aparecen múltiples políticas, sólo una se implementa para un usuario en un momento determinado (consulte *Orden de filtrado*, página 80).

Probar filtrado

Para descubrirqué sucede cuando un cliente específico solicita un sitio determinado:

1. Haga clic en **Probar filtrado** en la Caja de herramientas.
2. Para identificar un directorio o cliente de equipo, especifique:
   - Un nombre de usuario totalmente calificado

     Para examinar el árbol de directorios con el fin de identificar al usuario, haga clic en **Buscar usuario** (consulte *Cómo identificar un usuario para comprobar política o probar filtrado*, página 200).
   - Una dirección IP
3. Ingrese la URL o dirección IP del sitio que desea revisar.
4. Haga clic en **Ir**.

La categoría del sitio, la acción aplicada a la categoría y el motivo de la acción aparecen en una ventana emergente.

Acceso a URL

Para ver si los usuarios han intentado acceder a un sitio en las últimas dos semanas, incluido el día de hoy:

1. Haga clic en **Acceso a URL** en la Caja de herramientas.
2. Ingrese, total o parcialmente, la URL o dirección IP del sitio que desea revisar.
3. Haga clic en **Ir**.

Un informe de investigación muestra si se ha accedido al sitio, y cuándo.

Usted podría utilizar esta herramienta después de recibir una alerta de seguridad para saber si su empresa ha sido expuesta a phishing o a sitios infectados con virus.

Investigar usuario

Para revisar el historial de uso de Internet de un cliente de las últimas dos semanas, sin incluir el día de hoy:

1. Haga clic en **Investigar usuario** en la Caja de herramientas.
2. Especifique, total o parcialmente, el nombre de un usuario o la dirección IP de un equipo.
3. Haga clic en **Ir**.

Un informe de investigación muestra el historial de uso del cliente.

Cómo identificar un usuario para comprobar política o probar filtrado

Utilice la página **Buscar usuario** para identificar un cliente de usuario (directorio) para la herramienta Comprobar política o Probar filtrado.

La página se abre con la opción **Usuario** seleccionada. Expanda la carpeta **Entradas de directorio** para desplazarse por el directorio, o haga clic en **Buscar**. La función de búsqueda sólo esta disponible si usted utiliza un servicio de directorio basado en LDAP.

Para buscar un usuario en el directorio:

1. Ingrese, total o parcialmente, el **Nombre** del usuario.
2. Expanda el árbol **Entradas de directorio** y desplácese para identificar un contexto de búsqueda.

   Debe hacer clic en una carpeta (DC, OU o CN) del árbol para especificar el contexto. Esto llena el campo debajo del árbol.
3. Haga clic en **Buscar**. Las entradas que coinciden con el término de su búsqueda aparecen listadas en **Resultados de la búsqueda**.
4. Haga clic en un nombre de usuario para seleccionar un usuario, o haga clic en **Buscar de nuevo** para ingresar un nuevo término o contexto de búsqueda.

   Para volver a navegar por el directorio, haga clic en **Cancelar búsqueda**.
5. Cuando el nombre correcto de un usuario totalmente calificado aparezca en el campo **Usuario**, haga clic en**Ir**.

Si está utilizando la herramienta Probar filtrado, asegúrese de que la URL o dirección IP aparezca en el campo **URL** antes de hacer clic en **Ir**.

Para identificar un cliente de equipo en vez de un usuario, haga clic en **Dirección IP**.

10 Identificación de usuarios

Para aplicar las políticas a usuarios y grupos, el software de Websense debe poder identificar al usuario que realiza una solicitud, dada la dirección IP de origen. Hay diversos métodos de identificación disponibles:

- Una aplicación o dispositivo de integración identifica y autentica los usuarios, y luego pasa la información sobre los mismos al software de Websense. Para obtener más información, consulte la *Guía de instalación*.
- Un agente de identificación transparente de Websense trabaja en segundo plano para comunicarse con un servicio de directorio e identificar usuarios (consulte *Identificación transparente*).
- El software de Websense solicita a los usuarios sus credenciales de red y les indica que deben iniciar sesión cuando abren un navegador de Internet (consulte *Autenticación manual*, página 203).

Identificación transparente

Temas relacionados:

- *Autenticación manual*, página 203
- *Cómo configurar métodos de identificación de usuarios*, página 204

En general, la **identificación transparente** describe cualquier método que el software de Websense utiliza para identificar usuarios en el servicio de directorio sin solicitarles información de inicio de sesión. Esto incluye la integración del software de Websense con un dispositivo o una aplicación que proporcione información de los usuarios para utilizarla en el filtrado, o el uso de agentes opcionales de identificación transparente de Websense.

- Websense *DC Agent*, página 213, se utiliza con un servicio de directorio basado en Windows. El agente consulta periódicamente a los controladores de dominio sobre las sesiones de inicio de sesión de los usuarios y sondea los equipos cliente para verificar el estado de inicio de sesión. Se ejecuta en un servidor Windows y se puede instalar en cualquier dominio de la red.

- Websense *Logon Agent*, página 216, identifica a los usuarios a medida que inician sesiones en dominios de Windows. El agente se ejecuta en un servidor Linux o Windows, pero su aplicación de inicio de sesión asociada se ejecuta únicamente en equipos Windows.
- Websense *RADIUS Agent*, página 219, puede utilizarse junto con servicios de directorio basados en Windows o LDAP. El agente funciona con un servidor y un cliente RADIUS para identificar a los usuarios que inician sesión desde ubicaciones remotas.
- Websense *eDirectory Agent*, página 225, se utiliza con Novell eDirectory. El agente utiliza autenticación de Novell eDirectory para asignar los usuarios a direcciones IP.

Para obtener instrucciones sobre cómo instalar cada agente, consulte la *Guía de instalación*. El agente puede utilizarse solo o en determinadas combinaciones (consulte *Cómo configurar múltiples agentes*, página 231).

Notas

Si utiliza un dispositivo NetCache integrado, NetCache debe enviar nombres de usuarios al software de Websense en formato WinNT, LDAP o RADIUS para que la identificación transparente funcione.

Si tiene un servidor proxy y utiliza un agente de identificación transparente, lo óptimo es utilizar autenticación anónima en su servidor proxy.

Tanto la configuración general de identificación de usuarios y los agentes específicos de identificación transparente se configuran en Websense Manager. Haga clic en la ficha **Configuración** ubicada en el panel de navegación izquierdo, y luego haga clic en **Identificación de usuarios**.

Consulte *Cómo configurar métodos de identificación de usuarios*, página 204, para obtener instrucciones más detalladas sobre configuración.

En algunos casos, es posible que el software de Websense no pueda obtener información sobre usuarios de un agente de identificación transparente. Esto puede ocurrir si se ha asignado más de un usuario al mismo equipo, o si un usuario es un invitado o usuario anónimo, o por otros motivos. En estos casos, puede solicitar al usuario que inicie sesión mediante el navegador (consulte *Autenticación manual*, página 203).

Identificación transparente de usuarios remotos

En ciertas configuraciones, el software de Websense puede identificar de forma transparente a los usuarios que incian sesión en su red desde ubicaciones remotas:

- Si usted ha implementado Websense Remote Filtering Server y Remote Filtering Client, el software de Websense puede identificar a cualquier usuario remoto que inicie sesión en un dominio guardado en caché usando una cuenta de dominio. Para obtener más información, consulte *Filtrado de clientes remotos*, página 157.

- Si ha implementado DC Agent, y los usuarios remotos inician sesión directamente en dominios de Windows designados de su red, DC Agent puede identificar a dichos usuarios (consulte *DC Agent*, página 213).
- Si usted utiliza un servidor RADIUS para autenticar a los usuarios que incian sesión desde ubicaciones remotas, RADIUS Agent puede identificar de forma transparente a esos usuarios para que pueda aplicar políticas de filtrado sobre la base de usuarios o grupos (consulte *RADIUS Agent*, página 219).

Autenticación manual

Temas relacionados:

- *Identificación transparente*, página 201
- *Cómo establecer reglas de autenticación para equipos específicos*, página 206
- *Autenticación manual segura*, página 209
- *Cómo configurar métodos de identificación de usuarios*, página 204

La identificación transparente no siempre está disponible o es conveniente en todos los entornos. Para las empresas que no utilizan identificación transparente, o en los casos en que la identificación transparente no está disponible, igual es posible filtrar sobre la base de políticas basadas en usuarios o en grupos utilizando **autenticación manual**.

La autenticación manual exige a los usuarios que ingresen un nombre de usuario y una contraseña la primera vez que acceden a Internet a través de un navegador. El software de Websense luego confirma la contraseña con el servicio de directorio admitido, y luego recupera la información de la política de dicho usuario.

Usted puede configurar el software de Websense para activar la autenticación manual cada vez que la identificación transparente no esté disponible (consulte *Cómo configurar métodos de identificación de usuarios*, página 204), o crear una lista de equipos específicos con configuraciones de autenticación personalizadas en las cuales se solicita a los usuarios que inicien sesisión cuando abren un navegador (consulte *Cómo establecer reglas de autenticación para equipos específicos*, página 206).

Cuando se activa la autenticación manual, es posible que los usuarios reciban errores HTTP y no puedan acceder a Internet si:

- Han intentado ingresar una contraseña tres veces en forma fallida. Esto ocurre cuando el nombre de usuario o la contraseña no son válidos.
- Hacen clic en **Cancelar** para omitir la solicitud de autenticación.

Cuando se activa la autenticación manual, se impide la navegación por Internet a los usuarios que no es posible identificar.

Cómo configurar métodos de identificación de usuarios

Temas relacionados:

- *Identificación transparente*, página 201
- *Autenticación manual*, página 203
- *Cómo trabajar con usuarios y grupos*, página 62

Utilice la página **Configuración > Identificación de usuarios** para administrar cuándo y cómo el software de Websense intenta identificar a los usuarios de la red con el fin de aplicar políticas basadas en usuarios y grupos.

- Configure Policy Server para que se comunique con agentes de identificación transparente.
- Revise y actualice las configuraciones de los agentes de identificación transparente.
- Establezca una regla global para determinar el modo en que el software de Websense responde cuando los usuarios no pueden ser identificados por un agente de identificación transparente o un dispositivo de integración.
- Identifique los equipos de su red sobre los que no se aplican reglas globales de identificación de usuarios, y especifique si los usuarios de dichos equipos deben ser autenticados, y cómo.

Si utiliza agentes de identificación transparente de Websense, los agentes aparecen listados en **Agentes de identificación transparente**:

- **Servidor** muestra la dirección IP o el nombre del equipo que hospeda al agente de identificación transparente.
- **Puerto** indica el puerto que el software de Websense utiliza para comunicarse con el agente.
- **Tipo** indica si la instancia específica es DC Agent, Logon Agent, RADIUS Agent, o eDirectory Agent. (Consulte *Identificación transparente*, página 201, para una introducción a cada tipo de agente.)

Para agregar un nuevo agente a la lista, seleccione el tipo de agente de la lista desplegable **Agregar agente**. Para obtener instrucciones sobre configuración, haga clic en uno de los siguientes enlaces:

- *Cómo configurar DC Agent*, página 214
- *Cómo configurar Logon Agent*, página 217
- *Cómo configurar RADIUS Agent*, página 222
- *Cómo configurar eDirectory Agent*, página 227

Para eliminar de la lista una instancia de agente, marque la casilla de verificación que se encuentra junto a la información del agente en la lista y luego haga clic en **Eliminar**.

En **Opciones de autenticación adicionales**, especifique la respuesta predeterminada del software de Websense cuando los usuarios no están identificados de forma transparente (por un agente o una integración):

- Haga clic en **Aplicar una política de red o equipo** para ignorar políticas basadas en usuarios y grupos a favor de políticas basadas en equipos y redes, o la política predeterminada.
- Haga clic en **Solicitar al usuario información de inicio de sesión** para solicitar a los usuarios que proporcionen credenciales de inicio de sesión cuando abren un navegador. Luego es posible aplicar políticas basadas en usuarios y grupos (consulte *Autenticación manual*, página 203).
- Especifique el dominio predeterminado **Contexto** que el software de Websense debe utilizar cada vez que se solicita a un usuario las credenciales de inicio de sesión. Este es el dominio en el que las credenciales de los usuarios son válidas.

  Si usted utiliza la lista Excepciones para especificar los equipos en los que se solicita a los usuarios información de inicio de sesión, debe proporcionar un contexto de dominio predeterminado, aún cuando la regla global sea aplicar una política basada en equipos o redes.

Después de establecer la regla general que determina cuándo y cómo los usuarios son identificados por el software de Websense, usted puede crear excepciones a la regla.

Por ejemplo, si utiliza un agente de identificación transparente o un producto de integración para identificar usuarios, y ha habilitado la autenticación manual para solicitar credenciales a los usuarios cuando no se los puede identificar de forma transparente, usted puede identificar equipos específicos en los cuales:

- A los usuarios que no pueden ser identificados nunca se les solicita sus credenciales. En otras palabras, cuanda falla la identificación transparente, no se intenta la autenticación manual, y se aplica la política de equipos o redes, o la política predeterminada.
- La información sobre usuarios siempre es ignorada, aún cuando está disponible, y siempre se solicita a los usuarios sus credenciales.
- La información sobre usuarios siempre es ignorada, aún cuando está disponible, y nunca se solicita a los usuarios sus credenciales (siempre se aplica la política de equipos o redes, o la política predeterminada).

Para crear una excepción, haga clic en **Excepciones** y luego consulte *Cómo establecer reglas de autenticación para equipos específicos*, página 206.

Cuando termine de realizar cambios en esta página, haga clic en **Aceptar** para guardarlos. Para evitar guardar los cambios, haga clic en **Cancelar**.

Cómo establecer reglas de autenticación para equipos específicos

Temas relacionados:

- *Cómo configurar métodos de identificación de usuarios*, página 204
- *Autenticación manual*, página 203
- *Autenticación manual segura*, página 209

La autenticación selectiva le permite determinar si a los usuarios que solicitan acceso a Internet desde un equipo cliente específico (identificado por dirección IP) se les indica que proporcionen sus credenciales de inicio de sesión mediante el navegador. Esto se puede utilizar para:

- Establecer reglas de autenticación diferentes para un equipo en una cabina pública de acceso a Internet que para los empleados de la empresa que provee la cabina.
- Garantizar que los usuarios de la máquina en una sala de exámenes médicos siempre se identifiquen antes de obtener acceso a Internet.

Los equipos a los que se aplican configuraciones especiales de identificación de usuarios aparecen listados en la página **Configuración > Identificación de usuarios**. Haga clic en **Excepciones** para establecer configuraciones específicas de identificación de usuarios para algunos equipos de su red, o controlar si se han definido configuraciones especiales para un equipo específico.

Para agregar un equipo a la lista, haga clic en **Agregar** y luego consulte*Cómo definir excepciones a las configuraciones de identificación de usuarios*, página 206, para obtener más instrucciones.

Cuando termine de agregar equipos o rangos de red a la lista, haga clic en **Aceptar**. Los cambios no se implementarán hasta que haga clic en **Guardar todo**.

Cómo definir excepciones a las configuraciones de identificación de usuarios

Temas relacionados:

- *Identificación transparente*, página 201
- *Autenticación manual*, página 203
- *Cómo configurar métodos de identificación de usuarios*, página 204

Utilice la página **Configuración > Identificación de usuarios > Agregar dirección IP** para identificar equipos a los que se les debe aplicar reglas específicas de identificación de usuarios.

1. Especifique una **Dirección IP** o un **Rango de direcciones IP** para identificar los equipos a los cuales aplicar un método de autenticación específico, y luego haga clic en el botón de flecha derecha para agregarlos a la lista **Selección**.

Si las mismas reglas deben aplicarse a múltiples equipos, agréguelos todos a la lista.

2. Seleccione cualquier entrada en la lista desplegable **Identificación de usuarios** para indicar si el software de Websense debe intentar identificar de forma transparente a los usuarios de esos equipos.
   - Seleccione **Intentar identificar al usuario de forma transparente** para solicitar información del usuario desde un agente de identificación transparente o un dispositivo de integración.
   - Seleccione **Ignorar la información del usuario** para evitar usar cualquier método transparente para identificar usuarios.
3. Indique si a los usuarios se les debe solicitar que proporcionen credenciales de inicio de sesión mediante el navegador. Esta configuración se aplica cuando la información de usuario no se encuentra disponible, ya sea porque falló otra identificación o porque la información del usuario fue ignorada.
   - Seleccione **Solicitar al usuario información de inicio de sesión** para solicitar a los usuarios que prorpocionen credenciales de inicio de sesión.

     Si también se selecciona **Intentar identificar al usuario de forma transparente**, los usuarios reciben una solicitud del navegador sólo si no están identificados de forma transparente.
   - Seleccione **Aplicar una política de red o equipo** para asegurarse de que a los usuarios nunca se les solicite proporcionar credenciales de inicio de sesión.

     Si también se selecciona **Intentar identificar al usuario de forma transparente**, los usuarios cuyas credenciales pueden verificarse de forma transparente son filtrados por la política basada en usuarios que corresponda.
4. Haga clic en **Aceptar** para regresar a la página Identificación de usuarios.
5. Cuando termine de actualizar la lista Excepciones, haga clic en **Aceptar** para guardar los cambios en caché. Los cambios no se implementarán hasta que haga clic en **Guardar todo**.

Cómo revisar las excepciones a la configuración de identificación de usuarios

Temas relacionados:

- *Identificación transparente*, página 201
- *Autenticación manual*, página 203
- *Cómo configurar métodos de identificación de usuarios*, página 204

Utilice la página **Configuración > Identificación de usuarios > Modificar dirección IP** para realizar cambios a las entradas de la lista Excepciones. Los cambios realizados en esta página afectan a todos los equipos (identificados por rango o dirección IP) que aparecen en la lista Selección.

1. Seleccione cualquier entrada en la lista desplegable **Identificación de usuarios** para indicar si el software de Websense debe intentar identificar de forma transparente a los usuarios de esos equipos.
   - Seleccione **Intentar identificar al usuario de forma transparente** para solicitar información del usuario desde un agente de identificación transparente o un dispositivo de integración.
   - Seleccione **Ignorar la información del usuario** para evitar usar cualquier método transparente para identificar usuarios.
2. Indique si a los usuarios se les debe solicitar que proporcionen credenciales de inicio de sesión mediante el navegador. Esta configuración se aplica cuando la información del usuario no se encuentra disponible, ya sea porque la identificación transparente falló o porque fue ignorada.
   - Seleccione **Solicitar al usuario información de inicio de sesión** para solicitar a los usuarios que prorpocionen credenciales de inicio de sesión.

     Si también se selecciona **Intentar identificar al usuario de forma transparente**, los usuarios reciben una solicitud por navegador sólo si no han sido notificados de forma transparente.
   - Seleccione **Aplicar una política de red o equipo** para asegurarse de que a los usuarios nunca se les solicite proporcionar las credenciales de inicio de sesión.

     Si también se selecciona **Intentar identificar usuario de forma transparente**, los usuarios cuyas credenciales pueden verificarse de forma transparente son filtrados por la política basada en usuarios que corresponda.
3. Haga clic en **Aceptar** para regresar a la página Identificación de usuarios.
4. Cuando termine de actualizar la lista Excepciones, haga clic en **Aceptar** para guardar los cambios en caché. Los cambios no se implementarán hasta que haga clic en **Guardar todo**.

Autenticación manual segura

Temas relacionados:

- *Cómo configurar métodos de identificación de usuarios*, página 204
- *Autenticación manual*, página 203
- *Cómo establecer reglas de autenticación para equipos específicos*, página 206
- *Cómo activar la autenticación manual segura*, página 210

La autenticación manual segura de Websense utiliza el cifrado de Secure Sockets Layer (SSL) para proteger los datos de autenticación que se transmiten entre equipos cliente y software de Websense. Un servidor SSL incorporado en Filtering Service proporciona el cifrado de nombres de usuarios y contraseñas transmitidos entre equipos cliente y Filtering Service. De modo predeterminado, la autenticación manual segura está deshabilitada.

Nota

La autenticación manual segura no puede utilizarse con Remote Filtering. Remote Filtering Server no puede servir páginas de bloqueo a los clientes si está asociado con una instancia de Filtering Service que tiene habilitada la autenticación manual segura.

Para habilitar esta funcionalidad, debe llevar a cabo los siguientes pasos:

1. Generar claves y certificados SSL, y colocarlos en una ubicación a la que pueda acceder el software de Websense y que pueda ser leída por Filtering Service (consulte *Cómo generar claves y certificados*, página 209).
2. Habilitar la autenticación manual segura (consulte *Cómo activar la autenticación manual segura*, página 210) y la comunicación segura con el servicio de directorio.
3. Importar certificados al navegador (consulte *Cómo aceptar el certificado dentro del navegador cliente*, página 211).

Cómo generar claves y certificados

Temas relacionados:

- *Autenticación manual*, página 203
- *Cómo establecer reglas de autenticación para equipos específicos*, página 206
- *Autenticación manual segura*, página 209
- *Cómo activar la autenticación manual segura*, página 210
- *Cómo aceptar el certificado dentro del navegador cliente*, página 211

Un certificado consta de una clave pública, que se utiliza para cifrar datos, y una clave privada, que se utiliza para descifrar datos. Los certificados son emitidos por una Autoridad de Certificación (CA). Puede generar un certificado de un servidor de certificado interno, u obtener un certificado de cliente de cualquier autoridad certificadora tercera, como VeriSign.

La CA que emite el certificado de cliente debe ser de confianza para el software de Websense. En general, esto está determinado por un parámetro de configuración del navegador.

- Para obtener respuestas a preguntas comunes sobre las claves privadas, CSR y certificados, consulte httpd.apache.org/docs/2.2/ssl/ssl_faq.html#aboutcerts.
- Para aprender más acerca de cómo generar su clave privada, CSR, y certificado propios, consulte www.akadia.com/services/ssh_test_certificate.html.

Existen muchas herramientas que puede utilizar para generar un certificado con firma personal, incluido OpenSSL toolkit (disponible en www.openssl.org).

Independientemente del método que elija para generar el certificado, utilice los siguientes pasos generales.

1. Generar una clave privada (**server.key**).
2. Generar una solicitud de firma de certificado (CSR) con la clave privada.

   Importante
   Cuando se le solicite el nombre común, especifique la dirección IP del equipo Filtering Server. Si saltea este paso, los navegadores del cliente mostrarán un error de certificado de seguridad.

3. Utilice la CSR para crear un certificado con firma personal (**server.crt**).
4. Guarde los archivos **server.crt** y **server.key** en una ubicación a la que el software de Websense pueda acceder, y donde puedan ser leídos por Filtering Service.

Cómo activar la autenticación manual segura

Temas relacionados:

- *Autenticación manual*, página 203
- *Cómo establecer reglas de autenticación para equipos específicos*, página 206
- *Autenticación manual segura*, página 209
- *Cómo generar claves y certificados*, página 209
- *Cómo aceptar el certificado dentro del navegador cliente*, página 211

1. Detenga Websense Filtering Service (consulte *Cómo detener e iniciar los servicios Websense*, página 286).

2. Naveque hacia el directorio de instalación de Websense en el equipo Filtering Service (en forma predeterminada, **C:\Program Files\Websense\bin** o **/opt/Websense/bin/**).
3. Localice **eimserver.ini** y realice una copia de respaldo del archivo en otro directorio.
4. Abra el archivo INI original en un editor de texto.
5. Encuentre la sección **[WebsenseServer]**, y luego agregue la línea:

   ```
   SSLManualAuth=on
   ```

6. Debajo de la línea anterior, agregue lo siguiente:

   ```
   SSLCertFileLoc=[ruta]
   ```

   Reemplace **[ruta]** con la ruta completa al certificado SSL, incluyendo el nombre de archivo del certificado (por ejemplo, C:\secmanauth\server.crt).
7. Agregue también:

   ```
   SSLKeyFileLoc=[ruta]
   ```

   Reemplace **[ruta]** con la ruta completa a la clave SSL, incluyendo el nombre de archivo de la clave (por ejemplo, C:\secmanauth\server.key).
8. Guarde y cierre **eimserver.ini**.
9. Inicie Websense Filtering Service.

Una vez iniciado, Filtering Service escucha las solicitudes en el puerto HTTP seguro predeterminado (**15872**).

Los pasos anteriores garantizan la comunicación segura entre el equipo cliente y el software de Websense. Para asegurar también la comunicación entre el software de Websense y el servicio de directorio, asegúrese de seleccionar **Usar SSL** en la página **Configuración > Servicios de directorio**. Consulte *Configuración de directorio avanzada*, página 65, para más información.

Cómo aceptar el certificado dentro del navegador cliente

Temas relacionados:

- *Autenticación manual*, página 203
- *Cómo establecer reglas de autenticación para equipos específicos*, página 206
- *Autenticación manual segura*, página 209
- *Cómo generar claves y certificados*, página 209
- *Cómo activar la autenticación manual segura*, página 210

La primera vez que intente navegar a un sitio Web, el navegador mostrará una advertencia acerca del certificado de seguridad. Para evitar ver este mensaje en el futuro, instale el certificado en el almacén de certificados.

Microsoft Internet Explorer (Versión 7)

1. Abra el navegador y vaya a un sitio Web.

   Aparecerá una advertencia indicando que existe un problema con el certificado de seguridad del sitio.
2. Haga clic en **Continuar a este sitio Web (no recomendado)**.

   Si recibe una solicitud de autenticación, haga clic en **Cancelar**.
3. Haga clic en el cuadro **Error de certificado** situado a la derecha de la barra de direcciones (en la parte superior de la ventana del navegador), y luego haga clic en **Ver certificados**.
4. En la ficha General del cuadro de diálogo Certificado, haga clic en **Instalar certificado**.
5. Seleccione **Seleccionar automáticamente el almacén de certificados según el tipo de certificado**, y luego haga clic en **Siguiente**.
6. Haga clic en **Finalizar**.
7. Cuando se le pregunte si va a instalar el certificado, haga clic en **Sí**.

Los usuarios ya no recibirán advertencias de seguridad de certificados relacionadas con Filtering Service en este equipo.

Mozilla Firefox (Versión 2.x)

1. Abra el navegador y vaya a un sitio Web.

   Aparecerá un mensaje de advertencia.
2. Haga clic en **Aceptar el certificado de forma permanente**.
3. Ingrese sus credenciales si así se le solicita.
4. Vaya a **Herramientas > Opciones**, y luego haga clic en **Opciones avanzadas**.
5. Seleccione la ficha **Cifrado** y luego haga clic en **Ver certificados**.
6. Seleccione la ficha **Sitios Web** y compruebe que el certificado figure en la lista.

Los usuarios ya no recibirán advertencias de seguridad de certificados relacionadas con Filtering Service en este equipo.

Mozilla Firefox (Versión 3.x)

1. Abra el navegador y vaya a un sitio Web.

   Aparecerá un mensaje de advertencia.
2. Haga clic en **O puede agregar una excepción**.
3. Haga clic en **Agregar excepción**.
4. Asegúrese de **seleccionar Guardar esta excepción de forma permanente**, y luego haga clic en **Confirmar excepción de seguridad**.

Los usuarios ya no recibirán advertencias de seguridad de certificados relacionadas con Filtering Service en este equipo.

DC Agent

Temas relacionados:

- *Identificación transparente*, página 201
- *Cómo configurar DC Agent*, página 214
- *Cómo establecer diferentes configuraciones para una instancia de agente*, página 233

Websense DC Agent se ejecuta en Windows y detecta los usuarios de una red Windows que ejecutan servicios de red NetBIOS, WINS o DNS.

DC Agent y User Service recopilan datos de los usuarios de la red y los envían a Websense Filtering Service. Diversas variables determinan la velocidad de la transmisión de los datos, incluyendo el tamaño de la red y la cantidad de tráfico de red existente.

Para habilitar la identificación transparente con DC Agent:

1. Instale DC Agent. Para más información, consulte *Cómo instalar los componentes de Websense en forma independiente* en la *Guía de instalación*.

   Nota

   Ejecute DC Agent utilizando privilegios de administrador de dominio. La cuenta de administrador de dominio también debe ser miembro del grupo Administradores en el equipo DC Agent.

   Esto es requisito para que DC Agent recupere información de inicio de sesión de los usuarios del controlador de dominio. Si no puede instalar DC Agent con tales privilegios, configure privilegios de administrador para estos servicios después de la instalación. Para obtener más información, consulte *El software Websense no está aplicando las políticas de usuarios o de grupos*, página 369.

2. Configure DC Agent para que se comunique con otros componentes de Websense y con controladores de dominio en su red (consulte *Cómo configurar DC Agent*).
3. Use Websense Manager para agregar usuarios y grupos para filtrarlos (consulte *Cómo agregar un cliente*, página 68).

El software de Websense puede solicitar a los usuarios que se identifiquen si DC Agent no puede identificarlos de forma transparente. Para obtener más información, consulte *Autenticación manual*, página 203.

Cómo configurar DC Agent

Temas relacionados:

- *Identificación transparente*
- *Autenticación manual*
- *Cómo configurar métodos de identificación de usuarios*
- *DC Agent*
- *Cómo configurar múltiples agentes*

Utilice la página**Configuración > Identificación de usuarios > DC Agent** para configurar una nueva instancia de DC Agent, y también para establecer las configuraciones globales que se aplican a todas las instancias de DC Agent.

Para agregar una nueva instancia de DC Agent, primero proporcione información básica acerca de dónde está instalado el agente y cómo Filtering Service debe establecer comunicación con el mismo. Estas configuraciones pueden ser únicas para cada instancia de agente.

1. En Configuración básica de agente, ingrese la dirección IP o el nombre del **Servidor** donde se encuentra instalado el agente.

   Nota

   Los nombres de máquina deben comenzar con un carácter alfabético (a-z), no con un carácter numérico o especial.

   Los nombres de máquinas que contienen ciertos caracteres ASCII extendidos pueden no resolverse correctamente. Si usted utiliza una versión del software de Websense en idiomas distintos del inglés, ingrese una dirección IP en vez del nombre de una máquina.

2. Especifique el **Puerto** que DC Agent debe utilizar para comunicarse con otros componentes de Websense. El valor predeterminado es 30600.
3. Para establecer una conexión autenticada entre Filtering Service y DC Agent, marque **Activar autenticación** e ingrese una **Contraseña** para establecer conexión.

A continuación, personalice las configuraciones globales de comunicación de DC Agent y solución de problemas, del sondeo de controlador de dominio y del sondeo de equipos. De forma predeterminada, los cambios que usted realice aquí afectarán a todas las instancias de DC Agent. Sin embargo, las configuraciones marcadas con un asterisco (*), pueden modificarse en el archivo de configuración de un agente para personalizar el patrón de esa instancia de agente (consulte *Cómo establecer diferentes configuraciones para una instancia de agente*, página 233).

1. En Comunicación de DC Agent, especifique el **Puerto de comunicaciones** a utilizarse para establecer comunicación entre DC Agent y otros componentes de Websense. El valor predeterminado es 30600.

   A menos que se lo indique el soporte técnico de Websense, no realice cambios a la configuración del **Puerto de diagnóstico**. El valor predeterminado es 30601.

2. En Sondeo de controlador de dominio, marque **Activar sondeo de controlador de dominio** para permitir que DC Agent consulte a los controladores de dominio sobre las sesiones iniciadas de los usuarios.

   Puede especificar qué controladores de dominio sondea cada instancia de DC Agent en el archivo de configuración del agente. Consulte *Cómo configurar múltiples agentes*, página 231, para más información.

3. Utilice el campo **Intervalo de consulta** para especificar con qué frecuencia (en segundos) DC Agent consulta a los controladores de dominio.

   El hecho de reducir el intervalo de consulta puede brindar mayor exactitud en la captura de inicios de sesión, pero también aumenta el tráfico general de la red. El hecho de aumentar el intervalo de consulta reduce el tráfico de red, pero también puede demorar o evitar la captura de incios de sesión. El valor predeterminado es 10 segundos.

4. Utilice el campo **Tiempo de espera de entrada de usuario** para especificar con qué frecuencia (en horas) DC Agent actualiza las entradas del usuario en su mapa. El valor predeterminado es 24 horas.

5. En Sondeo de equipos, marque **Activar sondeo de equipos** para permitir que DC Agent consulte a los equipos sobre los inicios de sesión de los usuarios. Esto puede incluir equipos que se encuentran fuera de los dominios que el agente ya ha consultado.

   DC Agent utiliza WMI (Windows Management Instruction) para sondeo de equipos. Si usted activa el sondeo de equipos, configure el Firewall de Windows en equipos cliente para permitir la comunicación en el puerto **135**.

6. Ingrese un **Intervalo de verificación del mapa de usuarios** para especificar con qué frecuencia DC Agent se comunica con los equipos cliente para verificar cuáles usuarios han iniciado sesión. El valor predeterminado es 15 minutos.

   DC Agent compara los resultados de la consulta con los pares nombre de usuario/dirección IP en el mapa de usuarios que envía a Filtering Service. Si reduce este intervalo, puede lograr mayor exactitud en el mapa de usuarios, pero aumentará el tráfico de red. Aumentar el intervalo reduce el tráfico de red, pero también puede reducir la exactitud.

7. Ingrese un período **Tiempo de espera de entrada de usuario** para especificar con qué frecuencia DC Agent actualiza las entradas obtenidas mediante sondeo de equipos en su mapa de usuarios. El valor predeterminado es 1 hora.

   DC Agent quita cualquier entrada de nombre de usuario/dirección IP que sea anterior a este período de espera y que DC Agent no pueda verificar con los usuarios que han iniciado sesión en ese momento. Al aumentar este intervalo, es

posible que el mapa de usuarios pierda exactitud, porque el mapa podrá conservar nombres de usuarios viejos durante más tiempo.

> **Nota**
> No haga que el intervalo de tiempo de espera de entrada de usuario sea más corto que el intervalo de verificación del mapa de usuarios. Esto podría provocar la eliminación de nombres de usuarios del mapa de usuarios antes de ser verificados.

8. Haga clic en **Aceptar** para guardar e implementar inmediatamente los cambios.

Logon Agent

Temas relacionados:

- *Identificación transparente*, página 201
- *Cómo configurar Logon Agent*, página 217
- *Cómo establecer diferentes configuraciones para una instancia de agente*, página 233

Websense Logon Agent identifica usuarios en tiempo real a medida que inician sesión en los diversos dominios. Esto elimina la posibilidad de perder el inicio de sesión de un usuario debido a un problema con el tiempo de espera de una consulta.

Logon Agent (también llamado Servidor de autenticación) puede residir en un equipo Windows o Linux. El agente funciona con la aplicación de inicio de sesión de Websense (LogonApp.exe) en equipos Windows cliente para identificar a los usuarios a medida que inician sesión en dominios de Windows.

En la mayoría de los casos, es suficiente con usar ya sea DC Agento o Logon Agent, pero puede utilizar ambos agentes simultáneamente. En este caso, Logon Agent tiene prioridad sobre DC Agent. DC Agent sólo comunica un inicio de sesión a Filtering Service en el caso poco probable de que Logon Agent lo haya pasado por alto.

Instale Logon Agent y luego implemente la aplicación de inicio de sesión en los equipos cliente desde una ubicación central. Para obtener más información, consulte la *Guía de instalación*.

Después de la instalación, configure el agente para que se comunique con los equipos cliente y con Websense Filtering Service (consulte *Cómo configurar Logon Agent*).

> **Nota**
> Si usted utiliza Windows Active Directory (modo nativo) y User Service está instalado en un equipo Linux, consulte*User Service con Linux*, página 376, para informarse sobre los pasos de configuración adicionales.

Cómo configurar Logon Agent

Temas relacionados:

- *Identificación transparente*, página 201
- *Autenticación manual*, página 203
- *Cómo configurar métodos de identificación de usuarios*, página 204
- *Logon Agent*, página 216
- *Cómo configurar múltiples agentes*, página 231

Utilice la página**Configuración > Identificación de usuarios > Logon Agent** para configurar una nueva instancia de Logon Agent, y también para establecer las configuraciones globales que se aplican a todas las instancias de Logon Agent.

Para agregar una nueva instancia de Logon Agent:

1. En Configuración básica de agente, ingrese la dirección IP o el nombre del **Servidor** donde se encuentra instalado el agente.

   > **Nota**
   > Los nombres de máquina deben comenzar con un carácter alfabético (a-z), no con un carácter numérico o especial.
   >
   > Los nombres de máquinas que contienen ciertos caracteres ASCII extendidos pueden no resolverse correctamente. Si usted utiliza una versión del software de Websense en idiomas distintos del inglés, ingrese una dirección IP en vez del nombre de una máquina.

2. Especifique el **Puerto** que Logon Agent debe utilizar para comunicarse con otros componentes de Websense. El valor predeterminado es 30602.
3. Para establecer una conexión autenticada entre Filtering Service y Logon Agent, marque **Activar autenticación** e ingrese una **Contraseña** para establecer conexión.
4. Haga clic en **Aceptar** para guardar sus cambios o continúe a la siguiente sección de la pantalla para ingresar información adicional de configuración.

Luego personalice la configuración global de comunicación de Logon Agent. De forma predeterminada, los cambios que usted realice aquí afectarán a todas las instancias de Logon Agent.

1. En Comunicación de Logon Agent, especifique el **Puerto de comunicaciones** que debe utilizarse para establecer comunicación entre Logon Agent y otros componentes de Websense. El valor predeterminado es 30602.
2. A menos que se lo indique el soporte técnico de Websense, no realice cambios a la configuración del **Puerto de diagnóstico**. El valor predeterminado es 30603.
3. En Comunicación de la aplicación de inicio de sesión, especifique el **Puerto de conexión** que la aplicación de inicio de sesión utiliza para comunicarse con Logon Agent. El valor predeterminado es 15880.
4. Especifique el **Número máximo de conexiones** que cada instancia de Logon Agent permite. El valor predeterminado es 200.

   Si su red es grande, es posible que necesite aumentar este número. Al aumentar el número, aumenta el tráfico de red.
5. Haga clic en **Aceptar** para guardar sus cambios o continúe a la siguiente sección de la pantalla para ingresar información adicional de configuración.

Para establecer las configuraciones predeterminadas que establecen el modo en que se determina la validez de la entrada de usuario, primero debe decidir si Logon Agent y la aplicación de inicio de sesión del cliente funcionarán en **modo persistente** o en **modo no persistente** (predeterminado).

El modo no persistente se activa incluyendo el parámetro /NOPERSIST cuando se inicia **LogonApp.exe**. (Hay más información disponible en el archivo **LogonApp_ReadMe.txt** que viene incluido con la instalación de Logon Agent.)

- En modo persistente, la aplicación de inicio de sesión se comunica periódicamente con Logon Agent para transmitir información de inicio de sesión de los usuarios.

  Si usted utiliza el modo persistente, especifique un **Intervalo de consulta** para determinar con qué frecuencia la aplicación de inicio de sesión transmite información de inicio de sesión.

  > **Nota**
  > En caso de cambiar este valor, dicho cambio no se hará efectivo hasta que haya transcurrido el período de intervalo anterior. Por ejemplo, si cambia el intervalo de 15 minutos a 5 minutos, el actual intervalo de 15 minutos deberá finalizar antes de que la consulta comience a ocurrir cada 5 minutos.

- En modo no persistente, la aplicación de inicio de sesión envía información de inicio de sesión de los usuarios a Logon Agent sólo una vez para cada inicio de sesión.

  Si usted utiliza el modo no persistente, especifique un período de tiempo de **Caducidad de entradas de usuario**. Cuando se alcance este período de tiempo, la entrada de usuario se eliminará del mapa de usuarios.

Cuando termine de realizar cambios de configuración, haga clic en **Aceptar** para guardarlos.

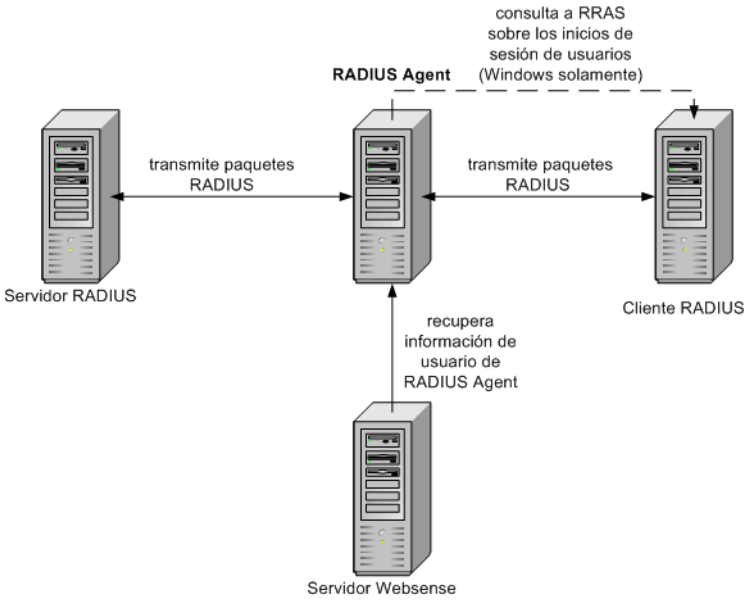
RADIUS Agent

Temas relacionados:

- *Identificación transparente*, página 201
- *Cómo procesar el tráfico de RADIUS*, página 220
- *Cómo configurar el entorno de RADIUS*, página 221
- *Cómo configurar RADIUS Agent*, página 222
- *Cómo configurar el cliente de RADIUS*, página 223
- *Cómo configurar el servidor RADIUS*, página 224
- *Cómo establecer diferentes configuraciones para una instancia de agente*, página 233

Websense RADIUS Agent le permite aplicar políticas basadas en usuarios y grupos utilizando autenticación proporcionada por un servidor RADIUS. RADIUS Agent permite la identificación transparente de usuarios que acceden a su red utilizando una conexión por vía telefónica, red privada virtual (VPN), línea de suscripción digital (DSL), u otra conexión remota (según su configuración).

RADIUS Agent trabaja en conjunto con el servidor RADIUS y el cliente de RADIUS en su red para procesar y realizar el seguimiento del tráfico de protocolo de servicio de usuario de acceso telefónico de autenticación remota (RADIUS). Esto le permite asignar políticas de filtrado determinadas a usuarios o grupos que acceden de forma remota a su red, además de a usuarios locales.



Cuando usted instala RADIUS Agent, el agente se integra con los componentes de Websense existentes. Sin embargo, RADIUS Agent, su servidor RADIUS y su cliente de RADIUS deben configurarse correctamente (consulte *Cómo configurar RADIUS Agent*, página 222).

Cómo procesar el tráfico de RADIUS

Websense RADIUS Agent actúa como un proxy que reenvía mensajes de RADIUS entre un cliente de RADIUS y un servidor RADIUS (o múltiples clientes y servidores).

RADIUS Agent no autentica a los usuarios directamente. En cambio, el agente identifica los usuarios remotos y los asocia con direcciones IP de modo que un servidor RADIUS pueda autenticar esos usuarios. Idealmente, el servidor RADIUS pasa solicitudes de autenticación a un servicio de directorio basado en LDAP.

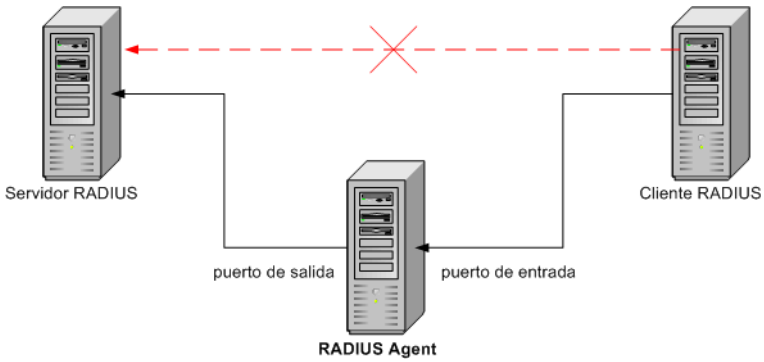
RADIUS Agent almacena pares de nombre de usuario-dirección IP en un mapa de usuarios. Si su cliente de RADIUS admite contabilidad (o seguimiento de incio de sesión de usuarios), y la misma está habilitada, RADIUS Agent obtiene más detalles acerca de los inicios de sesión de los usuarios desde los mensajes de RADIUS que recibe.

Cuando está correctamente configurado, Websense RADIUS Agent captura y procesa todos los paquetes de protocolo RADIUS de los siguientes tipos:

- **Access-Request**: Enviado por un cliente de RADIUS para solicitar autorización para un intento de conexión de acceso a la red.
- **Access-Accept**: Enviado por un servidor RADIUS en respuesta a un mensaje Access-Request; comunica al cliente de RADIUS que la conexión está autorizada y autenticada.
- **Access-Reject**: Enviado por un servidor RADIUS en respuesta a un mensaje Access-Request; comunica al cliente de RADIUS que la conexión ha sido rechazada.
- **Accounting-Stop-Request**: Enviado por un cliente de RADIUS para indicar al servidor RADIUS que debe detener el seguimiento de la actividad del usuario.

Cómo configurar el entorno de RADIUS

Websense RADIUS Agent sirve de proxy entre un cliente de RADIUS y un servidor RADIUS. Este diagrama muestra una vista simplificada del modo en que el uso de RADIUS Agent difiere de una configuración de RADIUS estándar.



RADIUS Agent y el servidor RADIUS deben instalarse en equipos diferentes. El agente y el servidor no pueden tener la misma dirección IP y deben utilizar puertos diferentes.

Después de instalar RADIUS Agent, configúrelo en Websense Manager (consulte *Cómo configurar RADIUS Agent*, página 222). También debe:

- Configurar el cliente de RADIUS (generalmente un servidor de acceso a la red [NAS]) para que se comunique con RADIUS Agent en vez de hacerlo directamente con su servidor RADIUS.
- Configurar el servidor RADIUS para que utilice RADIUS Agent como proxy (consulte la documentación del servidor RADIUS). Si tiene múltiples servidores RADIUS, configure cada uno por separado.

Nota

Si utiliza Lucent RADIUS Server y RRAS, debe configurar el servidor RADIUS para que utilice un protocolo de autenticación por contraseña (PAP) y el servidor RRAS para que acepte solicitudes de PAP únicamente. Para más información, consulte la documentación relacionada del producto.

Cómo configurar RADIUS Agent

Temas relacionados:

- *Identificación transparente*, página 201
- *Autenticación manual*, página 203
- *Cómo configurar métodos de identificación de usuarios*, página 204
- *RADIUS Agent*, página 219
- *Cómo configurar múltiples agentes*, página 231

Utilice la página**Configuración > Identificación de usuarios > RADIUS Agent** para configurar una nueva instancia de RADIUS Agent, y también para establecer las configuraciones globales que se aplican a todas las instancias de RADIUS Agent.

Para agregar una nueva instancia de RADIUS Agent:

1. En Configuración básica de agente, ingrese la dirección IP o el nombre del **Servidor** donde se encuentra instalado el agente.

   Nota

   Los nombres de máquina deben comenzar con un carácter alfabético (a-z), no con un carácter numérico o especial.

   Los nombres de máquinas que contienen ciertos caracteres ASCII extendidos pueden no resolverse correctamente. Si usted utiliza una versión del software de Websense en idiomas distintos del inglés, ingrese una dirección IP en vez del nombre de una máquina.

2. Especifique el **Puerto** que RADIUS Agent debe utilizar para comunicarse con otros componentes de Websense. El valor predeterminado es 30800.
3. Para establecer una conexión autenticada entre Filtering Service y RADIUS Agent, marque **Activar autenticación** e ingrese una **Contraseña** para establecer conexión.
4. Haga clic en **Aceptar** para guardar sus cambios o continúe a la siguiente sección de la pantalla para ingresar información adicional de configuración.

Luego personalice la configuración global de RADIUS Agent. De forma predeterminada, los cambios que usted realice aquí afectarán a todas las instancias de RADIUS Agent. Sin embargo, las configuraciones marcadas con un asterisco (*), pueden modificarse en el archivo de configuración de un agente para personalizar el patrón de esa instancia de agente (consulte *Cómo establecer diferentes configuraciones para una instancia de agente*, página 233).

1. Especifique el **Puerto de comunicaciones** utilizado para establecer comunicación entre RADIUS Agent y otros componentes de Websense. El valor predeterminado es 30800.

2. A menos que se lo indique el soporte técnico de Websense, no realice cambios a la configuración del **Puerto de diagnóstico**. El valor predeterminado es 30801.
3. En el servidor RADIUS, ingrese el **nombre o IP de RADIUS**. RADIUS Agent reenvía solicitudes de autenticación al servidor RADIUS y debe conocer la identidad de este equipo.
4. Si Microsoft RRAS se encuentra en uso, ingrese la dirección IP del **equipo RRAS**. El software de Websense consulta a este equipo para iniciar sesiones de usuarios.
5. Especifique un intervalo de **Tiempo de espera de entrada de usuario**, que se utiliza para determinar la frecuencia con la que RADIUS Agent actualiza su mapa de usuarios. Por lo general, el valor óptimo de consulta es el predeterminado (24 horas).
6. Utilice las configuraciones de **Puertos de autenticación** y **Puertos de contabilidad** para especificar los puertos que RADIUS Agent utiliza para enviar y recibir solicitudes de autenticación y de contabilidad. Para cada tipo de comunicación, puede especificar qué puerto se utiliza para establecer comunicación entre:
   - RADIUS Agent y el servidor RADIUS
   - RADIUS Agent y el cliente de RADIUS
7. Cuando termine, haga clic en **Aceptar** para guardar inmediatamente los cambios en caché.

Cómo configurar el cliente de RADIUS

Su cliente de RADIUS debe configurarse para transmitir solicitudes de autenticación y contabilidad al servidor RADIUS mediante RADIUS Agent.

Modifique la configuración de su cliente de RADIUS para que:

- El cliente de RADIUS envíe solicitudes de autenticación al equipo y al puerto donde RADIUS Agent escucha las solicitudes de autenticación. Este es el **Puerto de autenticación** especificado durante la configuración de RADIUS Agent.
- El cliente de RADIUS envíe solicitudes de contabilidad al equipo y al puerto donde RADIUS Agent escucha las solicitudes de contabilidad. Este es el **Puerto de contabilidad** especificado durante la configuración de RADIUS Agent.

El procedimiento exacto para configurar un cliente de RADIUS difiere según el tipo de cliente. Para más detalles, consulte la documentación de su cliente de RADIUS.

> **Nota**
> El cliente de RADIUS debe incluir los atributos **User-Name** y **Framed-IP-Address** en los mensajes de autenticación y contabilidad que envía. RADIUS Agent utiliza los valores de estos atributos para interpretar y almacenar los pares nombre de usuario/dirección IP. Si su cliente de RADIUS no genera esta información de forma predeterminada, configúrelo para que lo haga (consulte la documentación del cliente de RADIUS).

Cómo configurar el servidor RADIUS

Para habilitar la comunicación adecuada entre Websense RADIUS Agent y su servidor RADIUS:

- Agregar la dirección IP del equipo RADIUS Agent a la lista de clientes de su servidor RADIUS. Para más detalles, consulte la documentación de su servidor RADIUS.
- Defina los secretos compartidos entre el servidor RADIUS y todos los clientes de RADIUS que utilizan el agente para establecer comunicación con el servidor RADIUS. Los secretos compartidos generalmente se especifican como opciones de seguridad y autenticación.

  La configuración de un secreto compartido para clientes de RADIUS y el servidor de RADIUS proporciona la transmisión segura de mensajes de RADIUS. Por lo general, el secreto compartido es una cadena de texto común. Para más detalles, consulte la documentación de su servidor RADIUS.

  > **Nota**
  > El servidor RADIUS debe incluir los atributos **User-Name** y **Framed-IP-Address** en los mensajes de autenticación y contabilidad que envía. RADIUS Agent utiliza los valores de estos atributos para interpretar y almacenar los pares nombre de usuario/dirección IP. Si su servidor RADIUS no genera esta información de forma predeterminada, configúrelo para que lo haga (consulte la documentación del servidor RADIUS).

eDirectory Agent

Temas relacionados:

- *Identificación transparente*, página 201
- *Cómo configurar eDirectory Agent*, página 227
- *Cómo establecer diferentes configuraciones para una instancia de agente*, página 233

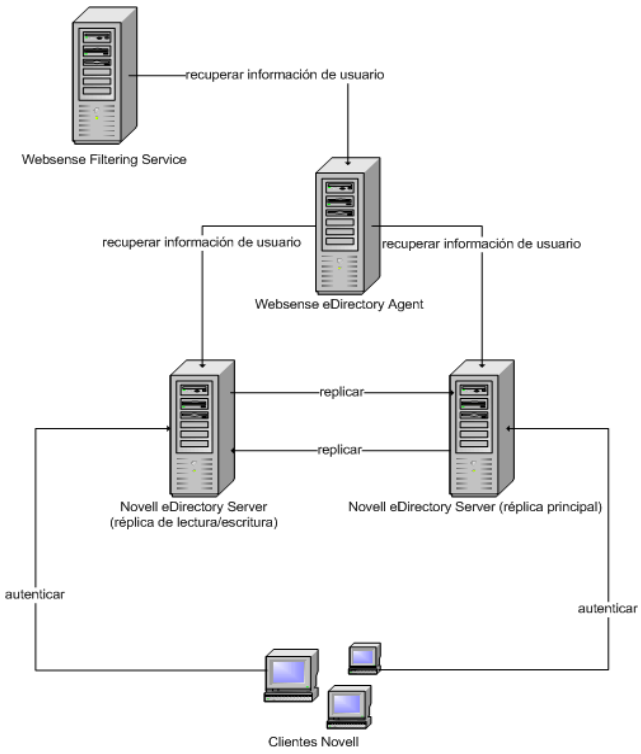
Websense eDirectory Agent trabaja junto con Novell eDirectory para identificar de forma transparente a los usuarios, de modo que el software de Websense pueda filtrarlos de acuerdo con las políticas asignadas a usuarios, grupos, dominios o unidades organizativas.

eDirectory Agent recopila información sobre inicio de sesión de usuarios desde Novell eDirectory, que autentica a los usuarios que inician sesión en la red. Luego el agente asocia cada usuario autenticado con una dirección IP y registra los pares nombre de usuario-dirección IP en un mapa de usuario local. Entonces eDirectory Agent comunica esta información a Filtering Service.

Nota

Desde un cliente de Novell que se ejecuta en Windows, múltiples usuarios pueden iniciar sesión en un único servidor Novell eDirectory. Esto asocia una dirección IP con múltiples usuarios. En este caso, el mapa de usuarios de eDirectory Agent únicamente retiene el par nombre de usuario/dirección IP para el último usuario que inició sesión desde una dirección IP determinada.

Una instancia de Websense eDirectory Agent puede admitir un Novell eDirectory principal además de cualquier número de réplicas de Novell eDirectory.



Consideraciones especiales de configuración

- Si usted tiene Cisco Content Engine v5.3.1.5 o superior integrado con el software de Websense:
  - Ejecute los siguientes servicios Websense en el mismo equipo que Cisco Content Engine:

    Websense eDirectory Agent
    Websense User Service
    Websense Filtering Service
    Websense Policy Server
  - Asegúrese de que todas las réplicas de Novell eDirectory se agreguen al archivo **wsedir.ini** en el mismo equipo.
  - Elimine el archivo **eDirAgent.bak**.

  Ejecute los servicios de las herramientas de generación de informes de Websense en un equipo **independiente** de Cisco Content Engine y el software de Websense.
- El software de Websense admite el uso de NMAS con eDirectory Agent. Para utilizar eDirectory Agent con NMAS habilitado, eDirectory Agent debe instalarse en un equipo que también ejecute el cliente de Novell.

Cómo configurar eDirectory Agent

Temas relacionados:

- *Identificación transparente*, página 201
- *Autenticación manual*, página 203
- *Cómo configurar métodos de identificación de usuarios*, página 204
- *eDirectory Agent*, página 225
- *Cómo configurar eDirectory Agent para que utilice LDAP*, página 229
- *Cómo configurar múltiples agentes*, página 231

Utilice la página**Configuración > Identificación de usuarios > eDirectory Agent** para configurar una nueva instancia de eDirectory Agent, y también para establecer las configuraciones globales que se aplican a todas las instancias de eDirectory Agent.

Para agregar una nueva instancia de eDirectory Agent:

1. En Configuración básica de agente, ingrese la dirección IP o el nombre del **Servidor** donde se encuentra instalado el agente.

   Nota

   Los nombres de máquina deben comenzar con un carácter alfabético (a-z), no con un carácter numérico o especial.

   Los nombres de máquinas que contienen ciertos caracteres ASCII extendidos pueden no resolverse correctamente. Si usted utiliza una versión del software de Websense en idiomas distintos del inglés, ingrese una dirección IP en vez del nombre de una máquina.

2. Especifique el **Puerto** que eDirectory Agent debe utilizar para comunicarse con otros componentes de Websense. El valor predeterminado es 30700.
3. Para establecer una conexión autenticada entre Filtering Service y eDirectory Agent, marque **Activar autenticación** e ingrese una **Contraseña** para establecer conexión.
4. Haga clic en **Aceptar** para guardar sus cambios o continúe a la siguiente sección de la pantalla para ingresar información adicional de configuración.

Luego personalice la configuración global de comunicación de eDirectory Agent. De forma predeterminada, los cambios que usted realice aquí afectarán a todas las instancias de eDirectory Agent. Sin embargo, las configuraciones marcadas con un asterisco (*), pueden modificarse en el archivo de configuración de un agente para personalizar el patrón de esa instancia de agente (consulte *Cómo establecer diferentes configuraciones para una instancia de agente*, página 233).

1. Especifique el **Puerto de comunicaciones** utilizado para establecer comunicación entre eDirectory Agent y otros componentes de Websense. El valor predeterminado es 30700.
2. A menos que se lo indique el soporte técnico de Websense, no realice cambios a la configuración del **Puerto de diagnóstico**. El valor predeterminado es 30701.
3. En eDirectory Server, especifique una **Base de búsqueda** (contexto root) para que eDirectory Agent utilice como punto de inicio cuando busque información sobre usuarios en el directorio.
4. Proporcione la información de cuenta de usuario administrativo que eDirectory Agent debe utilizar para comunicarse con el directorio.
   a. Ingrese el **Nombre distinguido de administrador** para una cuenta de usuario administrativo de Novell eDirectory.
   b. Especifique la **Contraseña** utilizada por dicha cuenta.
   c. Especifique un intervalo de **Tiempo de espera de entrada de usuario** para indicar por cuánto tiempo las entradas permanecen en el mapa de usuarios del agente.

      Este intervalo debe ser aproximadamente un 30% más prolongado que el del inicio de sesión de un usuario típico. Esto ayuda a evitar que las entradas de usuarios sean eliminadas del mapa antes de que los usuarios hayan terminado de navegar.

      Por lo general, se recomienda el valor predeterminado (24 horas).

      Nota

      En algunos entornos, en vez de utilizar el intervalo de Tiempo de espera de entrada de usuario para determinar la frecuencia con que eDirectory Agent actualiza su mapa de usuarios, puede resultar útil consultar eDirectory Server a intervalos regulares para actualizar inicios de sesión de usuarios. Consulte *Cómo habilitar consultas completas a eDirectory Server*, página 230.

5. Agregue el eDirectory Server principal, además de cualquier número de réplicas, a la lista **Réplicas de eDirectory**. Para agregar un eDirectory Server principal o una réplica a la lista, haga clic en **Agregar** y siga las instrucciones que figuran en *Cómo agregar una réplica de eDirectory Server*, página 228.

Cuando termine de realizar cambios de configuración, haga clic en **Aceptar** para guardarlos.

Cómo agregar una réplica de eDirectory Server

Una instancia de Websense eDirectory Agent puede admitir un Novell eDirectory principal además de cualquier número de réplicas de Novell eDirectory que se ejecutan en equipos diferentes.

eDirectory Agent debe poder comunicarse con cada equipo donde se ejecuta una réplica del servicio de directorio. Esto asegura que el agente obtenga información

actualizada de inicio de sesión a la mayor brevedad posible, y que no espere a que se produzca la replicación de eDirectory.

Novell eDirectory replica el atributo que identifica de un modo único a los usuarios que han iniciado sesión cada 5 minutos. A pesar de esta demora en la replicación, eDirectory Agent registra los nuevos inicios de sesión apenas el usuario inicia sesión en cualquier réplica de eDirectory.

Para configurar la instalación de eDirectory con el fin de establecer comunicación con eDirectory:

1. En la pantalla de réplica Agregar eDirectory, especifique la dirección IP o el nombre para eDirectory **Server** (principal o réplica).
2. Especifique el **Puerto** que eDirectory Agent utiliza para comunicarse con el equipo eDirectory.
3. Haga clic en **Aceptar** para regresar a la página eDirectory. La nueva entrada aparece en la lista Réplicas de eDirectory.
4. Repita el proceso para todos los equipos con servidor eDirectory adicionales.
5. Haga clic en **Aceptar** para guardar los cambios en caché, y luego haga clic en **Guardar todo**.
6. Detenga e inicie eDirectory Agent para que el agente pueda comenzar a comunicarse con la nueva réplica. Consulte *Cómo detener e iniciar los servicios Websense*, página 286, para obtener instrucciones.

Cómo configurar eDirectory Agent para que utilice LDAP

Websense eDirectory Agent puede utilizar el protocolo principal Netware (NCP) o el protocolo de acceso ligero a directorio (LDAP) para obtener información de inicio de sesión de los usuarios de Novell eDirectory. De modo predeterminado, eDirectory Agent en Windows utiliza NCP. En Linux, eDirectory Agent debe utilizar LDAP.

Si usted está ejecutando eDirectory Agent en Windows, pero desea que el agente utilice LDAP para consultar Novell eDirectory, configure el agente para que utilice LDAP en vez de NCP. Por lo general, NCP proporciona un mecanismo de consulta más eficaz.

Para configurar eDirectory Agent en Windows para que utilice LDAP:

1. Asegúrese de tener al menos una réplica de Novell eDirectory que contenga todos los objetos de directorio para controlar y filtrar en su red.
2. Detenga el servicio Websense eDirectory Agent (consulte *Cómo detener e iniciar los servicios Websense*, página 286).
3. Navegue al directorio de instalación de eDirectory Agent (de modo predeterminado, **\Program Files\Websense\bin**), y luego abra el archivo **wsedir.ini** en un editor de texto.
4. Modifique la entrada **QueryMethod** de la siguiente manera:

   ```
   QueryMethod=0
   ```

   Esto configura al agente para que utilice LDAP para consultar Novell eDirectory. (El valor predeterminado es 1, para NCP.)

5. Guarde y cierre el archivo.
6. Reinicie el servicio Websense eDirectory Agent.

Cómo habilitar consultas completas a eDirectory Server

En redes pequeñas, usted puede configurar Websense eDirectory Agent para que consulte al servidor de eDirectory para todos los usuarios que han iniciado sesión a intervalos regulares. Esto permite al agente detectar tanto los usuarios que han iniciado sesión recientemente como a los usuarios que han cerrado sesión desde la última consulta, y actualizar su mapa de usuarios local según corresponda.

Importante

Para redes más grandes, no se recomienda configurar eDirectory Agent para utilizar consultas completas, porque la cantidad de tiempo requerida para regresar resultados de consulta depende del número de usuarios que hayan iniciado sesión. Cuantos más usuarios hayan iniciado sesión, mayor será el impacto en el rendimiento.

Cuando usted habilita consultas completas para eDirectory Agent, el intervalo **Tiempo de espera de entrada de usuario** no se utiliza porque los usuarios que han cerrado sesión son identificados por la consulta. De modo predeterminado, la consulta se realiza cada 30 segundos.

Activar esta función aumenta el tiempo de procesamiento de eDirectory Agent de dos maneras:

- El tiempo necesario para recuperar los nombres de usuarios que han iniciado sesión cada vez que se realiza una consulta
- El tiempo requerido para procesar la información de nombre de usuario, eliminar entradas obsoletas del mapa de usuarios local y agregar nuevas entradas en función de la consulta más reciente

eDirectory Agent examina todo el mapa de usuarios local después de cada consulta, en vez de identificar únicamente los nuevos inicios de sesión. El tiempo requerido para este proceso depende del número de usuarios devueltos por cada consulta. Por lo tanto, el proceso de consulta puede afectar a los tiempos de respuesta tanto de eDirectory Agent como de Novell eDirectory Server.

Para habilitar consultar completas:

1. En el equipo eDirectory Agent, navegue al directorio **bin** Websense (de modo predeterminado, C:\Program Files\Websense\bin or /opt/Websense/bin).
2. Localice el archivo **wsedir.ini** y realice una copia de respaldo en otro directorio.
3. Abra **wsedir.ini** en un editor de texto (como Notepad o vi).
4. Vaya a la sección **[eDirAgent]** del archivo y busque la siguiente entrada:

   ```
   QueryMethod=<N>
   ```

Tome nota de este valor de QueryMethod, en caso de que desee volver a la configuración predeterminada más tarde.

5. Actualice el valor **QueryMethod** de la siguiente manera:
   - Si el valor actual es 0 (comuníquese con el directorio mediante LDAP), cambie el valor a **2**.
   - Si el valor actual es 1 (comuníquese con el directorio mediante NCP), cambie el valor a **3**.

   Nota
   Si cambiar este valor de consulta reduce el rendimiento del sistema, regrese la entrada QueryMethod a su valor anterior.

6. Si el intervalo de consulta predeterminado (30 segundos) no es el adecuado para su entorno, modifique el valor **PollInterval** como corresponda.

   Tenga en cuenta que el tiempo de intervalo está configurado en **milisegundos**.
7. Guarde y cierre el archivo.
8. Reinicie el servicio Websense eDirectory Agent (consulte *Cómo detener e iniciar los servicios Websense*, página 286).

Cómo configurar múltiples agentes

Temas relacionados:

- *DC Agent*, página 213
- *Logon Agent*, página 216
- *RADIUS Agent*, página 219
- *eDirectory Agent*, página 225

Es posible combinar múltiples agentes de identificación transparente dentro de la misma red. Si la configuración de su red requiere múltiples agentes, lo óptimo es instalar cada agente en un equipo aparte. Sin embargo, en algunos casos puede configurar el software de Websense para que funcione con múltiples agentes en un solo equipo.

Las siguientes combinaciones de agentes de identificación transparente son compatibles:

Combinación	¿Mismo equipo?	¿Misma red?	Configuración requerida
Múltiples DC Agents	No	Sí	Asegúrese de que todas las instancias de DC Agent puedan comunicarse Filtering Service.
Múltiples RADIUS Agents	No	Sí	Configure cada instancia para que se comunique con Filtering Service.
Múltiples eDirectory Agents	No	Sí	Configure cada instancia para que se comunique con Filtering Service.
Múltiples Logon Agents	No	Sí	Configure cada instancia para que se comunique con Filtering Service.
DC Agent + RADIUS Agent	Sí	Sí	Instale estos agentes en directorios separados. Configure cada agente para que se comunique con Filtering Service utilizando un puerto de comunicación diferente.
DC Agent + eDirectory Agent	No	No	El software de Websense no admite la comunicación con servicios de directorio de Windows y de Novell en la misma implementación. Sin embargo, usted puede tener ambos agentes instalados y sólo uno de ellos activo.
DC Agent + Logon Agent	Sí	Sí	Configure ambos agentes para que se comuniquen con Filtering Service. De forma predeterminada, cada agente utiliza un puerto único, de modo que los conflictos de puertos no representen un problema a menos que dichos puertos se cambien.
eDirectory Agent + Logon Agent	No	No	El software de Websense no admite la comunicación con servicios de directorio de Windows y de Novell en la misma implementación. Sin embargo, usted puede tener ambos agentes instalados y sólo uno de ellos activo.

Combinación	¿Mismo equipo?	¿Misma red?	Configuración requerida
RADIUS Agent + eDirectory Agent	Sí	Sí	Configure cada agente para que se comunique con Filtering Service utilizando un puerto de comunicación diferente.
DC Agent + Logon Agent + RADIUS Agent	Sí	Sí	A pesar de que esta combinación raramente es requerida, es compatible. Instale cada agente en un directorio separado. Configure todos los agentes para que se comuniquen con Filtering Service utilizando puertos de comunicación diferentes.

Cómo establecer diferentes configuraciones para una instancia de agente

Los valores de configuración de los agentes de identificación transparente de Websense Manager son globales y se aplican a todas las instancias del agente que usted ha instalado. Sin embargo, si usted tiene múltiples instancias de cualquier agente, puede configurar una instancia independientemente de las otras.

Las configuraciones únicas que usted especifica para una instancia de agente determinada modifican las configuraciones globales en el cuadro de diálogo Configuración. Las configuraciones que pueden modificarse están marcadas con un asterisco (*).

1. Detenga el servicio de agente de identificación transparente (consulte *Cómo detener e iniciar los servicios Websense*, página 286).
2. En el equipo donde se ejecuta la instancia de agente, navegue al directorio de instalación de agentes y abra el archivo que corresponda en un editor de texto:
   - para DC Agent: **transid.ini**
   - para Logon Agent: **authserver.ini**
   - para eDirectory Agent: **wsedir.ini**
   - para RADIUS Agent: **wsradius.ini**
3. Localice el parámetro a cambiar para esta instancia de agente (consulte *Parámetros de archivo INI*, página 234).

   Por ejemplo, usted puede activar una conexión autenticada entre esta instancia de agente y otros servicios Websense. Para hacerlo, especifique un valor para el parámetro **contraseña** en el archivo INI:

   ```
   contraseña=[xxxxxx]
   ```
4. Modifique los demás valores como desee.
5. Guarde y cierre el archivo INI.

6. Si usted realiza un cambio en las configuraciones de **DC Agent**, debe eliminar dos archivos del directorio **bin** de Websense (de modo predeterminado, C:\Program Files\Websense\bin):
   a. Detenga todos los servicios Websense en el equipo DC Agent (consulte *Cómo detener e iniciar los servicios Websense*, página 286).
   b. Elimine los siguientes archivos:

      ```
      Journal.dat
      XidDcAgent.bak
      ```

      Estos archivos son recreados cuando usted inicia el servicio Websense DC Agent.
   c. Reinicie los servicios Websense (incluyendo DC Agent), y luego continúe con el **paso 8**.
7. Reinicie el servicio de agente de identificación transparente.
8. Actualice las configuraciones de los agentes en Websense Manager:
   a. Vaya a **Configuración >** Identificación de usuarios.
   b. En **Agentes de identificación transparente**, seleccione el agente y haga clic en **Modificar**.

      Nota
      Si usted modificó el valor **puerto** para esta instancia de agente, elimine el agente y luego vuelva a agregarlo. Primero seleccione la entrada del agente existente y haga clic en **Eliminar**; y luego haga clic en **Agregar agente**.

   c. Verifique el **Nombre o IP de servidor** y el **Puerto** que esta instancia de agente utiliza. Si usted especificó un número de puerto único en el archivo INI, asegúrese de que su entrada coincida con ese valor.
   d. Si especificó una contraseña de autenticación única en el archivo INI, asegúrese de que la entrada de la **Contraseña** que aparece aquí sea la correcta.
   e. Haga clic en **Aceptar** para guardar sus cambios en caché. Los cambios no se implementarán hasta que haga clic en **Guardar todo**.

Parámetros de archivo INI

Etiqueta del campo Websense Manager	Nombre de parámetro .ini	Descripción
Puerto de comunicaciones (*todos los agentes*)	puerto	El puerto por donde el agente se comunica con otros servicios Websense.
Puerto de diagnóstico (*todos los agentes*)	DiagServerPort	El puerto por donde la herramienta de solución de problemas del agente escucha los datos del agente.

Contraseña (*todos los agentes*)	contraseña	La contraseña que el agente utiliza para autenticar conexiones a otros servicios Websense. Especifique una contraseña para activar la autenticación.
Intervalo de consulta (*DC Agent*)	QueryInterval	El intervalo al cual DC Agent consulta los controladores de dominio.
Nombre o IP de servidor Puerto (*eDirectory Agent*)	Server=IP:port	La dirección IP y el número de puerto del equipo donde se ejecuta eDirectory Agent.
Base de búsqueda (*eDirectory Agent*)	SearchBase	El contexto root del servidor Novel eDirectory.
Nombre distinguido de administrador (*eDirectory Agent*)	DN	El nombre del usuario administrativo para el servidor Novell eDirectory.
Contraseña (*eDirectory Agent*)	PW	La contraseña para el usuario administrativo del servidor Novell eDirectory.
Nombre o IP de servidor RADIUS	RADIUSHost	La dirección IP o el nombre del equipo de su servidor RADIUS.
IP de máquina RRAS (sólo Windows) (*RADIUS Agent*)	RRASHost	La dirección IP del equipo donde se ejecuta RRAS. Websense consulta a este equipo para iniciar sesiones de usuarios.
Puertos de autenticación: Entre RADIUS Agent y el servidor RADIUS	AuthOutPort	El puerto donde el servidor RADIUS escucha las solicitudes de autenticación.
Puertos de autenticación: Entre clientes RADIUS y RADIUS Agent	AuthInPort	El puerto por donde RADIUS Agent acepta solicitudes de autenticación.
Puertos de contabilidad: Entre RADIUS Agent y el servidor RADIUS	AccOutPort	El puerto por donde el servidor RADIUS escucha los mensajes de contabilidad de RADIUS.
Puertos de contabilidad: Entre clientes RADIUS y RADIUS Agent	AccInPort	El puerto por donde RADIUS Agent acepta solicitudes de contabilidad.

Cómo configurar un agente para que ignore determinados nombres de usuarios

Usted puede configurar un agente de identificación transparente para que ignore los nombres de inicio de sesión que no estén asociados a usuarios reales. Esta función se utiliza a menudo para ocuparse del modo en que algunos servicios Windows 200x y XP se comunican con los controladores de dominio en la red.

Por ejemplo, **usuario1** inicia sesión en la red y es identificado por el controlador de dominio como **equipo/usuario1**. Ese usuario es filtrado por una política de Websense asignada a **usuario1**. Si un servicio se inicia en el equipo del usuario que asume la identidad **equipoA/nombredeservicio** para comunicarse con el controlador de dominio, esto puede ocasionar problemas de filtrado. El software de Websense trata a **equipo/nombredeservicio** como un usuario nuevo sin ninguna política asignada, y filtra a este usuario según la política del equipo o según la política**Predeterminada**.

Para abordar este error:

1. Detenga el servicio del agente (consulte *Cómo detener e iniciar los servicios Websense*, página 286).
2. Navegue al directorio **\Websense\bin** y abra el archivo **ignore.txt** en un editor de texto.
3. Especifique cada nombre de usuario en una línea por separado. No incluya caracteres comodines, como "*":

   ```
   maran01
   WindowsServiceName
   ```

   El software de Websense ignora estos nombres de usuarios, independientemente del equipo con el que están asociados.

   Para indicar al software de Websense que ignore un nombre de usuario dentro de un dominio específico, utilice el formato **nombredeusuario, dominio**.

   ```
   aperez, engineering1
   ```
4. Cuando termine, guarde y cierre el archivo.
5. Reinicie el servicio de agente.

El agente ignora los nombres de usuario especificados, y el software de Websense no considera estos nombres para el filtrado.

11 Administración delegada

Temas relacionados:

- *Introducción a los roles administrativos*, página 238
- *Introducción a los administradores*, página 238
- *Introducción a los roles administrativos*, página 243
- *Cómo permitir el acceso a Websense Manager*, página 250
- *Cómo utilizar la administración delegada*, página 254
- *Varios administradores que acceden a Websense Manager*, página 265
- *Cómo definir restricciones de filtrado para todos los roles*, página 266

La administración delegada ofrece métodos potentes y flexibles para la administración del filtrado de Internet y la generación de informes para determinados grupos de clientes. Es una forma eficaz de distribuir la responsabilidad de la administración del acceso a Internet y la generación de informes entre diferentes administradores, cuando todos los usuarios tienen una ubicación central. Es especialmente eficaz en organizaciones grandes que incluyen varios lugares y regiones geográficas, ya que permite que los administradores locales administren el acceso a Internet e informen sobre la actividad de filtrado para los usuarios de sus regiones.

La implementación de la administración delegada implica la creación de un rol administrativo para cada grupo de clientes que será administrado por los mismos administradores. A los diferentes administradores de cada rol se les pueden otorgar permisos para administrar políticas o generar informes para sus clientes, o para ambas tareas. Consulte *Introducción a los roles administrativos*, página 243.

El rol de superadministrador viene preinstalado e incluye el usuario administrativo predeterminado: WebsenseAdministrator. Los superadministradores tienen acceso a un rango más amplio de parámetros de configuración y políticas que los administradores de otros roles. Consulte *Los superadministradores*, página 239.

Introducción a los roles administrativos

Temas relacionados:

- *Introducción a los administradores*, página 238
- *Introducción a los roles administrativos*, página 243

El rol administrativoes un grupo de clientes administrados (usuarios, grupos, dominios, unidades organizativas, equipos y rangos de red), que son administrados por uno o másadministradores. Usted le otorga a los diferentes administradores permisos para aplicar políticas a los clientes del rol, generar informes o para ambas tareas.

El software de Websense trae un rol de superadministradorpredefinido. También tiene un usuariopredeterminado, WebsenseAdministrator, que es un miembro automático del rol de superadministrador. Usted puede agregar administradores a este rol pero no puede eliminar el administrador predeterminado.

Importante

No se puede eliminar el rol de superadministradorpredefinido. El usuario predeterminado, WebsenseAdministrator, es un administrador del rol de superadministrador pero no se encuentra en la lista del rol. No se pueden eliminar ni cambiar los permisos para WebsenseAdministrator.

Cree la cantidad de roles necesaria para su organización. Por ejemplo, puede crear un rol para cada departamento, con el gerente de departamento como administrador y los miembros del departamento como clientes administrados. En una organización distribuida geográficamente, puede crear un rol para cada lugar y designar a todos los usuarios del lugar como clientes administrados de ese rol. Luego, designe una o más personas del lugar como administradores.

Consulte *Introducción a los administradores*, página 238,para obtener información sobre las opciones disponibles para definir los administradores.

Consulte *Cómo utilizar la administración delegada*, página 254,para obtener instrucciones sobre cómo crear roles y configurar permisos.

Introducción a los administradores

Los administradores son las personas que pueden obtener acceso a Websense Manager para administrar políticas o generar informes para un grupo de clientes. Los permisos específicos disponibles dependen del tipo de rol.

- EL superadministrador es un rol especial predefinido en Websense Manager. Este rol ofrece una gran flexibilidad para definir los permisos de acceso. Consulte *Los superadministradores*, página 239.
- Los roles de administración delegada deben ser creados por un superadministrador. Los administradores de estos roles tienen permisos de acceso más limitados. Consulte *Administradores delegados*, página 241.

Asimismo, usted puede crear algunos roles de administración delegada para informes únicamente, lo que permite a diferentes personas generar informes sin tener la responsabilidad de administrar políticas.

Usted puede asignar administradores a roles mediante el uso de sus credenciales de inicio de sesión de red o crear cuentas especiales que se utilizan sólo para acceder a Websense Manager. Consulte *Cómo permitir el acceso a Websense Manager*, página 250.

Los superadministradores

Temas relacionados:

- *Introducción a los administradores*, página 238
- *Administradores delegados*, página 241
- *Administradores en varios roles*, página 242

El rol de superadministrador se crea durante la instalación. El usuario predeterminado,WebsenseAdministrator, es asignado automáticamente a este rol. Por lo tanto, la primera vez que inicia sesión con ese nombre de usuario y la contraseñaestablecida durante la instalación, usted tiene acceso administrativo total a todas las políticas, informes y parámetros de configuración de Websense Manager.

Para preservar el acceso total para esta cuenta, WebsenseAdministrator no aparece en la lista de administradores para el rol de superadministrador. No se lo puede eliminar y sus permisos no se pueden modificar.

Usted puede agregar administradores al rol de superadministrador, según sea necesario. A cada administrador se le pueden otorgar permisos de la siguiente manera:

- Los permisos para **políticas** permiten a los superadministradores crear y modificar roles de administración delegada y copiar filtros y políticas a estos roles, según corresponda. También pueden crear y modificar componentes de filtrado, filtros y políticas, y aplicar políticas a clientes que no son administrados por ningún otro rol.

  Asimismo, los superadministradores con permisos para políticas pueden ver el registro de auditoría y se les permite el acceso a la configuración de Websense y a otras opciones de la siguiente manera:

- **Permisos**incondicionalespermiten al superadministrador el acceso a todos los parámetros de configuración del sistema para la instalación de Websense, como parámetros de cuenta, Policy Server y Remote Filtering Server, asignaciones de clase de riesgo y opciones de registro.

  Los superadministradores incondicionales tienen la opción de crear una fijación de filtro que bloquea determinadas categorías y protocolos para todos los usuarios administrados por roles de administración delegada. Consulte *Cómo definir restricciones de filtrado para todos los roles*, página 266,para obtener más información.

  Los superadministradores incondicionales pueden modificar el rol de superadministrador, al agregar o eliminar administradores, según sea necesario. También pueden eliminar roles de administración delegada o administradores o clientes de esos roles.

- **Los permisos**condicionales permiten alsuperadministrador el acceso a la descarga de la base de datos, servicios de directorio, identificación de usuarios y parámetros de configuración de Network Agent. Los superadministradores condicionales que también tienen permisos para informes pueden obtener acceso a parámetros de configuración para las herramientas de generación de informes.

  Los superadministradores condicionales pueden agregar cuentas de usuario de Websense, pero no pueden eliminarlas. Pueden crear y modificar roles de administración delegada pero no pueden eliminar roles ni los administradores o clientes administrados asignados a ellos. Tampoco pueden eliminar administradores del rol de superadministrador.

- **Los permisos**para informes permiten a los superadministradores acceder a todas las funciones de generación de informes y generar informes sobre todos los usuarios. A los superadministradores incondicionales se les otorgan permisos para informes automáticamente.

  Si a un administradorsólo se le otorgan permisos para informes, las opciones Crear política, Recategorizar URL y Desbloquear URL de la lista de Tareas comunes no se encuentran disponibles. Asimismo, la opción Comprobar política de la caja de herramientas no se encuentra disponible.

La creación de varios superadministradores incondicionales asegura que si el superadministrador principal no se encuentra disponible, otro administrador tiene acceso a todas las políticas y los parámetros de configuración de Websense.

Recuerde que no pueden iniciar sesión 2 administradores a la vez para administrar políticas para el mismo rol. Consulte *Varios administradores que acceden a Websense Manager*, página 265, para obtener información sobre cómo prevenir conflictos.

Los privilegios únicos del rol de superadministrador permiten que un administrador del rol acceda a todos los roles. Para cambiar a otro rol después de haber iniciado sesión, vaya a la lista desplegable **Roles** del anuncio y elija un rol.

Después de haber cambiado a otro rol, sus permisos para políticas se limitan a los que se encuentran disponibles para el rol de administración delegada. Los filtros y las políticas que usted crea se encuentran disponibles únicamente para los

administradores de ese rol. Sólo se pueden aplicar a los clientes administrados de ese rol. Consulte *Administradores delegados*, página 241.

Los permisos para informes son acumulativos, lo que significa que usted obtiene los permisos combinados de todos los roles en los que es administrador. Los superadministradores incondicionales tienen permisos para informes completos, independientemente de a qué rol obtienen acceso.

Administradores delegados

Temas relacionados:

- *Introducción a los administradores*, página 238
- *Los superadministradores*, página 239
- *Administradores en varios roles*, página 242

Los administradores delegados administran clientes asignados a un rol específico. Asigne a cada administrador permisos para políticas, permisos para informes o para ambos.

Los administradores delegados que cuentan con permisos para **políticas** aplican políticas a los clientes asignados a su rol y de ese modo determinan el acceso a Internet disponible para cada cliente. Como parte de esta responsabilidad, los administradores delegados pueden crear, editar y eliminar políticas y filtros, los que están sujetos a las limitaciones de la fijación de filtro establecida por el superadministrador. Consulte *Cómo definir restricciones de filtrado para todos los roles*, página 266.

Nota

Los administradores delegados ejercen un control importante sobre las actividades en Internet de sus clientes administrados. Para asegurar que este control se ejerza con responsabilidad y de acuerdo a las políticas de uso aceptables de su organización, los superadministradores deben utilizar la página de registro de auditoría para supervisar los cambios realizados por los administradores. Consulte *Visualización y exportación del registro de auditoría*, página 284.

Los administradores delegados no pueden eliminar la política predeterminada.

Los administradores delegados pueden modificar los componentes de filtro, con algunas limitaciones. Consulte *Crear políticas y filtros*, página 248,para obtener más información.

Los administradores con permisos para políticas que inician sesión en Websense Manager con una cuenta de usuario de Websense también pueden cambiar sus propias contraseñas de Websense. (Consulte *Cuentas de usuario de Websense*, página 252.)

Las opciones disponibles para administradores delegados con permisos para **informes**varían según la manera en que se configura el rol. Es posible que sólo puedan realizar informes sobre aquellos clientes administrados por su rol o posiblemente se les permita realizar informes sobre todos los clientes. Es posible que tengan acceso a todas las funciones de generación de informes o que su acceso a la generación de informes sea más limitado. Consulte *Cómo modificar roles*, página 256,para obtener más información.

Un administrador que sólo tiene permisos para informes tiene limitadas las opciones disponibles en el panel de accesos directos (Tareas comunes y Caja de herramientas).

Administradores en varios roles

Temas relacionados:

- *Introducción a los administradores*, página 238
- *Los superadministradores*, página 239
- *Administradores delegados*, página 241

Según las necesidades de su organización, un mismo administrador puede ser designado para varios roles. Los administradores designados para varios roles deben elegir un solo rol para administrar en el inicio de sesión.

Después del inicio de sesión, sus permisos son los siguientes:

- **Política**: usted puede agregar y modificar filtros y políticas para el rol seleccionado al iniciar sesión y aplicar políticas a los clientes administrados de ese rol. La página Administración delegada contiene una lista de todos los roles para los que es designado, lo que le permite ver los clientes administrados de cada rol y los permisos para informes.
- **Informes**: usted tiene los permisos para informes combinados de todos sus roles. Por ejemplo, supongamos que se le asignan 3 roles, con permisos para informes de la siguiente manera:
  - Rol 1: sin informes.
  - Rol 2: sólo informes sobre clientes administrados e informes de investigación.
  - Rol 3: informes sobre todos los clientes, acceso completo a todas la funciones de generación de informes.

  En esta situación, independientemente del rol que elija durante el inicio de sesión, se le permite ver informes de la páginas Hoy e Historial y generar informes sobre todos los clientes, con todas la funciones de generación de informes.

  Si inicia sesión únicamente para informes, el campo Rol de la barra de anuncios indica si usted tiene permisos para informes completos (informes sobre todos los clientes) o limitados (únicamente informes sobre clientes administrados).

Introducción a los roles administrativos

Temas relacionados:

- *Introducción a los roles administrativos*, página 238
- *Cómo notificar a los administradores*, página 245
- *Tareas de los administradores delegados*, página 246

La introducción a la administración delegadarequiere que el superadministrador lleve a cabo las siguientes tareas:

- Decida de qué forma los administradores iniciarán sesión en Websense Manager. Consulte *Cómo permitir el acceso a Websense Manager*, página 250.
- Agregue roles y configúrelos. Consulte *Cómo utilizar la administración delegada*, página 254.
- Informe a los administradores sobre sus responsabilidades y opciones. Consulte *Cómo notificar a los administradores*, página 245.

Además de estas tareas requeridas, existen tareas opcionales asociadas con la administración delegada.

Cómo crear la fijación de filtro

Los superadministradores incondicionales pueden crear una fijación de filtro, la cual designa categorías y protocolos específicos como bloqueados para clientes administrados de todos los roles de administración delegada. Estas restricciones se aplican automáticamente para todos los filtros creados en un rol de administración delegada o copiados a él y no pueden ser modificados por el administrador delegado.

> **Nota**
> La fijación de filtro no se aplica a clientes administrados por el rol de superadministrador.

La fijación de filtro también puede bloquear y fijar tipos de archivos y palabras clave asociadas con categorías seleccionadas y aplicar el registro de protocolos seleccionado. Consulte *Cómo crear una fijación de filtro*, página 267.

Cómo mover clientes

Al agregar un cliente a la página Clientes cuando ha iniciado sesión como superadministrador, usted asigna a ese cliente al rol de superadministrador. Ese cliente no puede ser agregado a un rol de administración delegada en la página Modificar rol. Lo ideal sería que usted agregue los clientes directamente al rol, en lugar de asignar una política dentro del rol de superadministrador. Sin embargo, esto no siempre es posible.

Para transferir clientes desde el rol de superadministrador a otro rol, utilice la opción **Mover a rol**de la página Clientes. Consulte *Cómo mover clientes a roles*, página 70.

Como parte del movimiento, la política aplicada en el rol de superadministrador se copia al rol de administración delegada. También se copian los filtros que aplica esa política. Durante este proceso de copiado, los filtros se actualizan para aplicar la restricciones de la fijación de filtro, si estas existen.

En el rol de destino, se agrega la etiqueta "(Copied)" al final del nombre del filtro o política. Los administradores para ese rol pueden identificar claramente el nuevo elemento y actualizarlo según corresponda.

> **Nota**
>
> Cada vez que se copia un filtro o una política en el mismo rol, la etiqueta (Copied) recibe un número que aumenta con cada copia nueva: (Copied 1), (Copied 2), etcétera. Cada uno se convierte en un filtro o una política separados dentro del rol.
>
> Sugiera a los administradores del rol que cambien los nombres de los filtros y las políticas y que los editen según sea necesario, para aclarar sus configuraciones y minimizar la cantidad de duplicados. Esos cambios pueden simplificar trabajos de mantenimiento futuros.

Los filtros Permitir todo del rol de Superadministrador permiten el acceso a todas las categorías o protocolos y no se pueden modificar. Para preservar la capacidad del superadministrador de implementar una fijación de filtro, estos filtros no se pueden copiar a un rol de administración delegada.

Si la política asignada al cliente que se está moviendo aplica un filtro Permitir todo, el cliente no puede ser movido hasta que usted aplica una política que utilice un filtro Permitir todo.

Una vez que el cliente ha sido movido al nuevo rol, sólo un administrador de ese rol puede modificar la política del cliente o los filtros que aplica. Los cambios en la política original o en los filtros del rol de superadministrador no afectan a las copias de la política o los filtros de los roles de administración delegada.

Cómo copiar filtros y políticas

Inicialmente, los filtros y las políticas creados por un superadministradorse encuentran disponibles sólo para los administradores del rol de superadministrador. Usted puede utilizar la opción **Copiar a rol**para copiar filtros y políticas a un rol de administración delegada sin mover un cliente a ese rol. Consulte *Cómo copiar filtros y políticas a roles*, página 173.

Cuando se copian filtros y políticas directamente, se utilizan las mismas restricciones que se aplican cuando los filtros y las políticas se copian como parte del movimiento de un cliente.

- Las restricciones de fijación de filtro se implementan durante el copiado.

- Los filtros de la categoría Permitir todo y de protocolo no se pueden copiar.
- Los filtros y las políticas copiados están identificados en el rol con la etiqueta (Copied) en el nombre.

Considere modificar las descripciones de las políticas antes de comenzar la copia, con el fin de asegurar que tengan sentido para los administradores de los roles de destino.

Cómo aplicar políticas a los clientes restantes

Los clientes que no son asignados específicamente a un rol de administración delegadason administrados por superadministradores. Para el rol de superadministrador, no existe una lista de clientes administrados.

Para aplicar políticas a estos clientes, agréguelos a la página Administración de políticas >Clientes. Consulte *Cómo agregar un cliente*, página 68. Los clientes que no han sido asignados a una política específica se rigen por la política predeterminada para su rol.

Es posible que existan ocasiones en las que usted no pueda agregar clientes a la página Clientes. Esto puede suceder cuando el cliente es miembro de una red, grupo, dominio o unidad organizativa asignado a otro rol. Si el administrador del otro rol ha aplicado una política para miembros individuales de la red o grupo, esos clientes no pueden ser agregados al rol de superadministrador.

Cómo notificar a los administradores

Temas relacionados:

- *Introducción a los roles administrativos*, página 238
- *Introducción a los roles administrativos*, página 243

Después de designar personas como administradores en cualquier rol administrativo, asegúrese de proporcionarles la siguiente información.

- La URL para iniciar sesión en Websense Manager. Predeterminada:

  ```
  https://<ServerIP>:9443/mng/
  ```

  En lugar de <ServerIP>, utilice la dirección IP del equipo que está ejecutando Websense Manager.
- Qué Policy Server elegir durante el inicio de sesión, si corresponde. En un entorno con muchos Policy Servers, los administradores deben optar por un Policy Server durante el inicio de sesión. Deben elegir el Policy Server que está configurado para comunicarse con el servicio de directorio que autentica a sus clientes administrados.
- Si deben utilizar su cuenta de inicio de sesión de red o una cuenta de usuario de Websense al iniciar sesión en Websense Manager. Si los administradores inician sesión con cuentas de usuario de Websense, proporcióneles el nombre de usuario y la contraseña.

- Sus permisos, ya sea para crear y aplicar políticas a clientes del rol o para generar informes, o para ambas tareas.

  Recomiende a los administradores que tienen tanto permisos para políticas como para informes que consideren qué actividades planean realizar durante la sesión. Si el único plan consiste en generar informes, recomiéndeles que vayan al campo**Rol** del anuncio y elijan **Liberar Políticas Permisos**. Esto libera los permisos para políticas para el rol, lo que permite que otro administrador obtenga acceso a Websense Manager y controle la política para ese rol.
- Cómo encontrar la lista de clientes administrados por su rol. Los administradores pueden ir a Administración de políticas > Administración delegada y luego hacer clic en el nombre de su rol para visualizar la página Modificar rol, que incluye una lista de clientes administrados.
- Limitaciones impuestas por la fijación de filtros, si algunas categorías o protocolos han sido bloqueados y fijados.
- Las tareas que generalmente realizan los administradores. Consulte *Tareas de los administradores delegados*, página 246.

Asegúrese de notificar a los administradores delegados cuando agregue o modifique tipos de archivos y protocolos personalizados. Estos componentes aparecen automáticamente en filtros y políticas para todos los roles. Por lo tanto, es importante que esos administradores sean informados cuándo se han realizado cambios.

Tareas de los administradores delegados

Temas relacionados:

- *Introducción a los roles administrativos*, página 238
- *Introducción a los roles administrativos*, página 243
- *Cómo notificar a los administradores*, página 245

Los administradores delegados que tienen permisos para **políticas** pueden realizar las siguientes tareas.

- *Ver su cuenta de usuario*, página 247
- *Ver la definición de su rol.*, página 247
- *Agregar clientes a la página Clientes*, página 248
- *Crear políticas y filtros*, página 248
- *Cómo aplicar políticas a clientes*, página 250

Los permisos para informes pueden otorgarse a nivel individual. Los permisos para informes específicos otorgados a su rol determinan cuál de las siguientes tareas se encuentran disponibles para los administradores con permisos para informes. Consulte *Generar informes*, página 250.

Ver su cuenta de usuario

Temas relacionados:

- *Tareas de los administradores delegados*, página 246
- *Ver la definición de su rol.*, página 247
- *Agregar clientes a la página Clientes*, página 248
- *Crear políticas y filtros*, página 248
- *Cómo aplicar políticas a clientes*, página 250

Si inicia sesión en Websense Manager con credenciales de red, los cambios de contraseña se gestionan a través de su servicio de directorio de red. Comuníquese con el administrador del sistema para recibir asistencia.

Si se le ha asignado un nombre de usuario y una contraseña de Websense, consulte la información sobre su cuenta y cambie su contraseña en Websense Manager.

1. Vaya a **Administración de políticas >Administración delegada**.
2. Haga clic en **Administrar cuentas de usuario de Websense**, en la parte superior de la página.
3. Haga clic en **Cambiar contraseña**si desea cambiar su contraseña. Consulte *Cómo cambiar una contraseña de usuario de Websense*, página 254.
4. Haga clic en **Ver**para visualizar la lista de roles en los que usted es administrador.

Ver la definición de su rol.

Temas relacionados:

- *Tareas de los administradores delegados*, página 246
- *Ver su cuenta de usuario*, página 247
- *Agregar clientes a la página Clientes*, página 248
- *Crear políticas y filtros*, página 248
- *Cómo aplicar políticas a clientes*, página 250

Abra la página Administración delegada y haga clic en el nombre de su rol para visualizar la página Modificar rol, la cual proporciona una lista de los clientes administrados del rol. Esta página también muestra las funciones de generación de informes disponibles para los administradores que tienen permisos para informes en este rol.

Los administradores que tienen permisos para informes únicamente no pueden visualizar esta página. Sólo las funciones de generación de informes especificadas se encuentran disponibles para estos administradores.

Agregar clientes a la página Clientes

Temas relacionados:

- *Tareas de los administradores delegados*, página 246
- *Ver su cuenta de usuario*, página 247
- *Ver la definición de su rol.*, página 247
- *Crear políticas y filtros*, página 248
- *Cómo aplicar políticas a clientes*, página 250

Los superadministradores asignan clientes administrados a un rol, pero los administradores delegados deben agregarlos a la página Clientes antes de aplicar políticas. Consulte *Cómo agregar un cliente*, página 68,para obtener instrucciones.

Ni bien se agregan los clientes a la lista de clientes administrados del rol, son filtrados por la política predeterminada de éste. Los clientes que fueron movidos al rol desde la página Clientes del Superadministrador se rigen por la política que aplicó el superadministrador, la cual fue copiada al rol cuando se movió al cliente.

Los clientes que se detallan en la lista de la página Administración delegada > Modificar rol para su rol se pueden agregar a la página Clientes y se les puede asignar una política. También se pueden agregar diferentes usuarios y equipos que son miembros de un grupo, dominio, unidad organizativa o rango de red asignado como cliente administrado del rol.

Debido a que un usuario puede ser parte de varios grupos, dominios o unidades organizativas, si se agregan personas de una agrupación de clientes más grande se pueden crear conflictos cuando los diferentes roles administran grupos, dominios o unidades organizativas con miembros en común. Si los administradores de diferentes roles obtienen acceso a Websense Manager al mismo tiempo, pueden agregar al mismo cliente (miembro individual de un grupo, por ejemplo) a su página Clientes. Dada esa situación, el filtrado de Internet para ese cliente está regido por la prioridad establecida para cada rol. Consulte *Cómo manejar conflictos de roles*, página 263.

Crear políticas y filtros

Temas relacionados:

- *Tareas de los administradores delegados*, página 246
- *Ver su cuenta de usuario*, página 247
- *Ver la definición de su rol.*, página 247
- *Agregar clientes a la página Clientes*, página 248
- *Cómo aplicar políticas a clientes*, página 250

Cuando se creó su rol, heredó automáticamente la política predeterminada, el filtro de categorías y el filtro de protocolos preinstalados, según se definió en ese momento. Es posible que existan también políticas y filtros que el superadministrador ha elegido copiar a su rol.

Además de las políticas y filtros, usted también hereda los tipos de archivos personalizados y los protocolos creados por el superadministrador.

Usted tiene la libertad de modificar las políticas y los filtros que heredó del superadministrador. Los cambios que usted realiza afectan sólo a su rol. Los cambios que realiza el superadministrador en las políticas y los filtros que heredó previamente no afectan a su rol.

Nota

Los cambios que realiza el superadministrador en los tipos de archivos y protocolos personalizados afectan automáticamente a los filtros y las políticas de su rol.

Cuando su superadministrador le informe sobre cambios en estos componentes, revise sus filtros y políticas para asegurarse de que se manejen adecuadamente.

También puede crear tantos filtros y políticas nuevos como necesite. Los filtros y las políticas creados por un administrador delegado sólo se encuentran disponibles para los administradores que iniciaron sesión en su rol. Para obtener instrucciones sobre cómo crear políticas, consulte *Cómo trabajar con políticas*, página 75. Para obtener instrucciones sobre cómo crear filtros, consulte *Cómo trabajar con filtros*, página 48.

Usted puede modificar los componentes de filtro para su rol, con algunas limitaciones.

- **Categorías**: agregue categorías personalizadas y modifique tanto las categorías de la base de datos principal como las personalizadas, con la definición de las URL recategorizadas y las palabras clave para su uso dentro del rol. Cambie la acción y la opción de filtrado avanzado aplicadas en forma predeterminada en los filtros de categorías que crean. (Los cambios en la acción predeterminada de una categoría sólo se implementan si la categoría no está bloqueada por la fijación de filtros.)
- **Protocolos**: cambie la acción y las opciones de filtrado avanzado aplicadas en forma predeterminada en los filtros de protocolos que crean. (Los cambios en una acción predeterminada de un protocolo sólo se implementan si el protocolo no está bloqueado por la fijación de filtro. Los administradores delegados no pueden agregar ni eliminar definiciones de protocolos.
- **Tipos de archivos**: observe las extensiones de archivos asignadas a cada tipo de archivo. Los administradores delegados no pueden agregar tipos de archivos ni cambiar las extensiones asignadas a un tipo de archivo.
- **URL sin filtrar**: agregue URL y agregue extensiones regulares que representen los sitios que estarán permitidos para todos los clientes administrados únicamente en sus roles.

Para obtener más información, consulte *Cómo construir componentes de filtro*, página 174.

Si un superadministrador ha implementado restricciones de fijación de filtro, puede haber categorías o protocolos que se bloqueen automáticamente y no se puedan cambiar en los filtros que usted cree y edite. Consulte *Cómo definir restricciones de filtrado para todos los roles*, página 266.

Cómo aplicar políticas a clientes

Temas relacionados:

- *Tareas de los administradores delegados*, página 246
- *Ver su cuenta de usuario*, página 247
- *Ver la definición de su rol.*, página 247
- *Agregar clientes a la página Clientes*, página 248
- *Crear políticas y filtros*, página 248

Después de crear una política, usted puede aplicar esa política directamente a los clientes que ya hayan sido agregados a la página Clientes. Para ello debe hacer clic en el botón **Aplicar a clientes**. Consulte *Cómo asignar una política a clientes*, página 79.

Otra opción es que vaya a la página Clientes y agregue los clientes que deberán regirse por esta política. Consulte *Cómo trabajar con clientes*, página 60.

Generar informes

Si cuenta con permisos para informes, las opciones de informes específicas que se encuentran disponibles son establecidas por el superadministrador. Para saber qué funciones puede utilizar, vaya a la página Administración delegada y haga clic en el nombre del rol. La página Modificar rol muestra las funciones de generación de informes para las cuales tiene permisos. Consulte *Cómo modificar roles*, página 256,para obtener más información.

Cómo permitir el acceso a Websense Manager

Cuando configura los roles de administración delegada, usted determina a qué funciones de Websense Manager pueden tener acceso los administradores. Para asegurar que se encuentren disponibles las funciones correctas para las personas que inicien sesión en Websense Manager, cada persona debe iniciar sesión con un nombre de usuario y una contraseña. Se pueden utilizar dos tipos de cuentas:

- **Las cuentas de red** utilizan las credenciales que ya están establecidas en su servicio de directorio de red (ver *Cuentas de directorio*, página 251).
- **Las cuentas de usuarios de Websense** le permiten crear un nombre de usuario y una contraseña específicamente para uso dentro de Websense Manager (ver *Cuentas de usuario de Websense*, página 252).

Cuentas de directorio

Temas relacionados:

- *Cómo permitir el acceso a Websense Manager*, página 250
- *Cuentas de usuario de Websense*, página 252

Los superadministradores incondicionales pueden utilizar la página **Configuración > General >Directorio de inicio de sesión** para ingresar la información de servicio de directorio necesaria para permitir que los administradores inicien sesión en Websense Manager con sus credenciales de la red.

Nota

Esta información se utiliza únicamente para autenticar a usuarios de Websense Manager. No se aplica a clientes de filtrado. La información del servicio de directorio de clientes se configura en la página Configuraciones >Servicios de directorio (ver *Servicios de directorio*, página 62).

Las credenciales de la red de los usuarios de Websense Manager deben ser autenticadas en un único servicio de directorio. Si su red incluye varios servicios de directorio, debe existir una relación de confianza entre el servicio de directorio de inicio de sesión que usted configure en Websense Manager y los demás.

Si no es posible definir un servicio de directorio único para su uso con Websense Manager, considere la creación de cuentas de usuario de Websense para los administradores (ver *Cuentas de usuario de Websense*, página 252).

Para definir el servicio de directorio que debería utilizar Websense Manager para autenticar administradores, primero verifique que la casilla para utilizar un servicio de directorio para autenticar administradores esté seleccionada y luego elija un tipo de **Servicio de directorio** de la lista.

Si elije el predeterminado, **Directorio de Windows NT / Active Directory (modo mixto)**, no se necesitan otras configuraciones. Haga clic en **Aceptar** para guardar los cambios. Los cambios no se implementan hasta que usted haya hecho clic en **Guardar todo**.

Si elige **Active Directory (modo nativo)** u **otro Directorio LDAP**, proporcione la siguiente información adicional:

1. Especifique la dirección IP o el nombre del equipo donde está instalado el servicio de directorio.

   Si utiliza Active Directory (modo nativo) y ha configurado sus servidores de catálogo global para recuperación de fallos, puede, en lugar de eso, ingresar el nombre de dominio DNS.

2. Especifique el **Puerto** utilizado para la comunicación con el servicio de directorio.
3. Para cifrar la comunicación con el servicio de directorio, marque **Usar SSL**.
4. Especifique el **Nombre distinguido de usuario** y la **Contraseña** que debe utilizar el software de Websense para conectarse con el servicio de directorio.
5. Especifique el **Contexto de dominio predeterminado** que debe utilizar el software de Websense cuando autentique administradores.
   - Si utiliza Active Directory (modo nativo), la configuración ha finalizado. Haga clic en **Aceptar** para guardar los cambios. Los cambios no se implementan hasta que usted haya hecho clic en **Guardar todo**.
   - Si usa otro servicio de directorio basado en LDAP, continúe.
6. Proporcione los **Atributos de ID de inicio de sesión de usuario** y el **Filtro de búsqueda de usuario**, si lo hubiera, que el software de Websense debe usar para aumentar la velocidad de autenticación de usuarios.

   Esta información también aparece en la página **Configuración > Servicios de directorio**, bajo **Configuración de directorio avanzada**. Si es necesario, puede copiar y pegar los valores.
7. Bajo Opciones de grupo, especifique si su esquema de LDAP incluye al atributo de **miembro** o no:
   - Si no se utiliza el atributo de miembro, especifique el **Filtro de búsqueda de grupo de usuario** que debe aplicar el software de Websense para autenticar administradores.
   - Si se utiliza el atributo de miembro, especifique el **Atributo de grupo** que debe aplicarse.
8. Si su esquema de LDPA incluye grupos anidados, marque **Realizar búsqueda adicional de grupo anidado**.
9. Si su servicio de directorio utiliza referencias LDAP, indique si el software de Websense debe utilizar o ignorar las referencias.
10. Haga clic en **Aceptar** para guardar los cambios. Los cambios no se implementan hasta que usted haya hecho clic en **Guardar todo**.

Cuentas de usuario de Websense

Temas relacionados:

- *Cómo permitir el acceso a Websense Manager*, página 250
- *Cómo agregar cuentas de usuario de Websense*, página 253

Los superadministradores utilizan la página **Administración delegada > Administrar cuentas de usuarios de Websense** para crear cuentas con el fin de que los administradores accedan a Websense Manager sin ingresar credenciales de directorio de red. Esta página también permite que los superadministradores cambien

la contraseña para las cuentas de usuario de Websense y visualicen los roles a los que se asigna a los usuarios de Websense como administradores.

Los superadministradores incondicionales también pueden eliminar cuentas de usuarios de Websense de esta página.

Los administradores delegados utilizan esta página para cambiar sus contraseñas de Websense y visualizar los roles a los que son asignados como administradores.

Opción	Descripción
Agregar	Abre la página para crear una cuenta de usuario de Websense nueva. Consulte *Cómo agregar cuentas de usuario de Websense*, página 253.
Cambiar contraseña	Abre la página para cambiar la contraseña para la cuenta asociada. Consulte *Cómo cambiar una contraseña de usuario de Websense*, página 254.
Ver	Muestra la lista de roles a los que se asigna a este usuario como administrador.
Eliminar	Marque la casilla para una o más cuentas de usuarios obsoletas, luego haga clic en este botón para borrarlos.
Cerrar	Vuelve a la página Administración delegada.

Cómo agregar cuentas de usuario de Websense

Temas relacionados:

- *Cómo permitir el acceso a Websense Manager*, página 250
- *Cuentas de usuario de Websense*, página 252
- *Cómo cambiar una contraseña de usuario de Websense*, página 254

Utilice la página **Administración delegada > Administrar cuentas de usuario de Websense > Agregar usuario de Websense** para agregar cuentas de usuario de Websense.

1. Especifique un **Nombre de usuario** único con 50 caracteres como máximo.

   El nombre debe tener entre 1 y 50 caracteres y no puede incluir ninguno de los siguientes caracteres:

   ```
   * < > ' { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

   Los nombres de usuarios pueden incluir espacios y guiones.

2. Especifique y confirme una Contraseña (4-255 caracteres) para este usuario.

   Se recomienda utilizar contraseñas completas: de 8 caracteres o más, que incluyan por lo menos una de las siguientes características:

   - letra mayúscula
   - letra minúscula
   - número

- carácter especial (como guiones, subrayado o espacios en blanco)

3. Cuando termine de realizar los cambios, haga clic en **Aceptar** para guardar los cambios y volver a la página Administrar cuentas de usuarios de Websense. Los cambios no se implementan hasta que usted haya hecho clic en **Guardar todo**.

Cómo cambiar una contraseña de usuario de Websense

Temas relacionados:

- *Cómo permitir el acceso a Websense Manager*, página 250
- *Cuentas de usuario de Websense*, página 252
- *Cómo agregar cuentas de usuario de Websense*, página 253

La página **Administración delegada > Administrar cuentas de usuario de Websense > Cambiar contraseña** permite a los administradores delegados cambiar las contraseñas de sus propias cuentas de usuario de Websense. Los superadministradores pueden utilizar esta página para cambiar la contraseña de cualquier cuenta de usuario de Websense.

1. Verifique que aparezca el **Nombre de usuario** correcto en la parte superior de la página.
2. Especifique y confirme una **Contraseña** nueva (4-255 caracteres) para este usuario.

   Se recomienda utilizar contraseñas completas: de 8 caracteres o más, que incluyan por lo menos una de las siguientes características:

   - letra mayúscula
   - letra minúscula
   - número
   - carácter especial (como guiones, subrayado o espacios en blanco)
3. Cuando haya terminado de realizar los cambios, haga clic en **Aceptar** para guardar los cambios y volver a la página Administrar cuentas de usuario de Websense. Los cambios no se implementan hasta que usted haya hecho clic en **Guardar todo**.

Cómo utilizar la administración delegada

Temas relacionados:

- *Introducción a los roles administrativos*, página 238
- *Cómo manejar conflictos de roles*, página 263

La página **Administración de políticas > Administración delegada** ofrece diferentes opciones que dependen de quién la mire, un superadministrador o un administrador delegado.

Los superadministradores ven una lista de todos los roles definidos actualmente y tienen disponibles las siguientes opciones.

Opción	Descripción
Agregar	Haga clic en agregar un rol nuevo. Consulte *Cómo agregar roles*, página 256.
Rol	Haga clic para ver o configurar el rol. Consulte *Cómo modificar roles*, página 256.
Eliminar	Haga clic en eliminar los roles de la lista que estén marcados. Esta opción se encuentra disponible únicamente para los superadministradores incondicionales. Consulte *Consideraciones especiales*, página 263,para obtener información sobre cómo se administran los clientes de un rol una vez que su rol fue eliminado.
Avanzado	Haga clic aquí para acceder a la función Administrar prioridad de roles.
Administrar prioridad de roles	Haga clic para especificar qué configuraciones de política de rol se utilizan cuando el mismo cliente existe en varios grupos que son administrados por diferentes roles. Consulte *Cómo manejar conflictos de roles*, página 263.
Administrar cuentas de usuario de Websense	Haga clic en agregar, editar y eliminar nombres de usuario y contraseñas para cuentas usadas únicamente para obtener acceso a Websense Manager. Consulte *Cuentas de usuario de Websense*, página 252.
Administrar grupos LDAP personalizados	Haga clic en agregar, editar y eliminar grupos LDAP personalizados, los que se pueden asignar como clientes administrados en roles de administración delegada. Consulte *Cómo trabajar con grupos LDAP personalizados*, página 66. Esta opción no se encuentra disponible si el servicio de directorio configurado es Windows NT/Active Directory (modo mixto).

Los administradores delegados ven únicamente los roles en los que son administradores y tienen acceso a opciones más limitadas.

Opción	Descripción
Rol	Haga clic para ver los clientes asignados al rol y los permisos específicos para informes otorgados. Consulte *Cómo modificar roles*, página 256.
Administrar cuentas de usuario de Websense	Haga clic para acceder a las opciones para cambiar su contraseña de Websense Manager y ver sus roles asignados. Consulte *Cuentas de usuario de Websense*, página 252.

Cómo agregar roles

Temas relacionados:

- *Cómo modificar roles*, página 256
- *Consideraciones especiales*, página 263

Utilice la página **Administración delegada > Agregar rol** para proporcionar un nombre y una descripción para el nuevo rol.

1. Especifique un **Nombre** para el nuevo rol.

   El nombre debe tener entre 1 y 50 caracteres y no puede incluir ninguno de los siguientes caracteres:

   ```
   * < > ' { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

   Los nombres de roles pueden incluir espacios y guiones.
2. Especifique una **Descripción** para el nuevo rol.

   La descripción debe tener 255 caracteres como máximo. Las restricciones de caracteres que se aplican a los nombres de los roles también se aplican a las descripciones pero con 2 excepciones: las descripciones pueden incluir puntos (.) y comas (,).
3. Haga clic en **Aceptar** para visualizar la página **Modificar rol** y definir las características de este rol. Consulte *Cómo modificar roles*, página 256.

   El nuevo rol se agrega a la lista desplegable de roles del anuncio cuando usted vuelve a iniciar sesión en Websense Manager.

Cómo modificar roles

Temas relacionados:

- *Cómo utilizar la administración delegada*, página 254
- *Cómo agregar roles*, página 256
- *Cómo manejar conflictos de roles*, página 263

Los administradores delegados pueden utilizar la página **Administración delegada > Modificar rol** para ver la lista de clientes administrados por su rol y los permisos para informes específicos otorgados.

Los superadministradores pueden utilizar esta página para seleccionar los administradores y clientes para un rol y para configurar permisos para administradores como se describe a continuación. Sólo los superadministradores incondicionales pueden eliminar administradores y clientes de un rol.

1. Cambiar el **Nombre** y la **Descripción** del rol, según sea necesario.

   > **Nota**
   > El nombre del rol de superadministrador no se puede cambiar.

2. Agregar y eliminar administradores para este rol. (Disponible para los superadministradores solamente, esta sección no aparece si usted inicia sesión como administrador delegado.)

Elemento	Descripción
Nombre de usuario	Nombre de usuario del administrador.
Tipo de cuenta	Indica si el usuario está definido en el servicio de directorio de red (Directorio) o como cuenta de usuario de Websense (Websense).
Informes	Marque esta casilla para otorgar al administrador permiso para utilizar herramientas de generación de informes.
Política	Marque esta casilla para otorgar al administrador permiso para crear filtros y políticas y para aplicar políticas a los clientes administrados del rol. En el rol de superadministrador, los administradores con permisos para políticas también pueden administrar determinados parámetros de configuración de Websense. Consulte *Los superadministradores*, página 239.
Incondicional	Disponible sólo para el rol de superadministrador, marque esta casilla para otorgar al administrador permisos para administrar todos los parámetros de configuración de Websense y la fijación de filtro. Sólo los superadministradores incondicionales pueden otorgar permisos incondicionales a un nuevo administrador.
Agregar	Abre la página **Agregar administradores**. Consulte *Cómo agregar administradores*, página 259.
Eliminar	Retira del rol a todos los administradores marcados en la lista de administradores. (Disponible únicamente para los superadministradores incondicionales.)

3. Agregar y eliminar **Clientes administrados** para el rol. (Sólo los superadministradores pueden realizar los cambios. Los administradores delegados pueden visualizar los clientes asignados a sus roles.)

Elemento	Descripción
<Nombre>	Muestra el nombre de cada cliente asignado expresamente al rol. Los administradores del rol deben agregar los clientes a la página Clientes antes de que se puedan a aplicar políticas. Consulte *Tareas de los administradores delegados*, página 246.

Elemento	Descripción
Agregar	Abre la página **Agregar clientes administrados**. Consulte *Cómo agregar clientes administrados*, página 261.
Eliminar	Disponible únicamente para los superadministradores incondicionales, este botón retira del rol todos los clientes marcados en la lista de clientes administrados. Algunos clientes no pueden ser eliminados directamente de la lista de clientes administrados. Consulte *Consideraciones especiales*, página 263,para obtener más información.

4. Utilice el área de **Permisos para informes** para elegir las funciones disponibles para los administradores de este rol que tienen acceso a informes.

   a. Elija el nivel general de los permisos para informes.

Opción	Descripción
Informe sobre todos los clientes	Elija esta opción para otorgar a los administradores permiso para generar informes sobre todos los usuarios de la red. Utilice las opciones restantes del área de Permisos para informes para configurar los permisos específicos para los administradores de este rol.
Informes sobre clientes administrados únicamente	Seleccione esta opción para limitar a los administradores a informes sobre los clientes administrados asignados a este rol. Luego, elija las funciones de informes de investigación a las que pueden acceder estos administradores. Los administradores limitados a la generación de informes sobre clientes administrados únicamente, no pueden acceder a informes de presentación ni a informes basados en usuarios en las páginas Hoy e Historial. Tampoco pueden administrar la configuración de base de datos de registro.

   b. Marque la casilla para cada función de generación de informes que se le permite utilizar a los administradores correspondientes del rol.

Opción	Descripción
Acceder a los informes de presentación	Permite el acceso a las funciones de informes de presentación. Esta opción sólo se encuentra disponible cuando los administradores pueden generar informes sobre todos los clientes. Consulte *Informes de presentación*, página 98.
Ver informes en las páginas Hoy e Historial	Permite mostrar gráficos que muestran la actividad de Internet en esas páginas. Consulte *Hoy: Estado, Seguridad y Utilidad desde medianoche*, página 21y *Historial: últimos 30 días*, página 24. Si se deselecciona esta opción, los administradores pueden ver sólo las áreas de Alertas de estado y Utilidad de la página Hoy y las Estimaciones de utilidad de la página Historial.

Opción	Descripción
Acceder a los informes de investigación	Permite el acceso a las funciones de informes de investigación básicas. Cuando se selecciona esta opción, se pueden seleccionar también funciones de informes de investigación adicionales. Consulte *Informes de investigación*, página 117.
Ver nombres de usuario en informes de investigación	Permite a los administradores de este rol ver los nombres de usuario, siempre y cuando estén registrados. Consulte *Configuración de Filtering Service para el registro*, página 310. Deseleccione esta opción para mostrar sólo códigos de identificación generados por el sistema, en lugar de nombres. Esta opción sólo se encuentra disponible cuando los administradores obtienen acceso a informes de investigación.
Guardar informes de investigación como favoritos	Permite a los administradores de este rol crear informes de investigación favoritos. Consulte *Informes de investigación Favoritos*, página 135. Esta opción sólo se encuentra disponible cuando los administradores obtienen acceso a informes de investigación.
Programar informes de investigación	Permite a los administradores de este rol programar informes de investigación para ejecutarlos en el futuro o en un ciclo repetitivo. Consulte *Programar informes de investigación*, página 138. Esta opción sólo se encuentra disponible cuando los administradores tienen permisos para guardar informes de investigación como favoritos.
Administrar la base de datos de registro	Permite a los administradores acceder a la página Configuración > Base de datos de registro. Consulte *Configuración de administración de la base de datos de registro.*, página 326. Esta opción sólo se encuentra disponible cuando los administradores pueden generar informes sobre todos los clientes.

5. Cuando termine de realizar los cambios, haga clic en **Aceptar** para guardar los cambios y volver a la página Administración delegada. Los cambios no se implementan hasta que usted haya hecho clic en **Guardar todo**.

Cómo agregar administradores

Temas relacionados:

- *Cómo modificar roles*, página 256
- *Cómo permitir el acceso a Websense Manager*, página 250

Los superadministradores pueden utilizar la página **Administración delegada > Editar rol** > **Agregar administradores** para especificar qué personas son administradores para un rol.

> **Nota**
> Los administradores pueden ser agregados a varios roles. Estos administradores deben optar por un rol durante el inicio de sesión. En esta situación, el administrador recibe los permisos para informes combinados para todos los roles.

Los administradores delegados ejercen un control importante sobre las actividades de Internet de sus clientes administrados. Para asegurar que este control se ejerza con responsabilidad y de acuerdo a las políticas de uso aceptables de su organización, los superadministradores deben utilizar la página de registro de auditoría para supervisar los cambios realizados por los administradores. Consulte *Visualización y exportación del registro de auditoría*, página 284.

1. Si planea agregar cuentas de directorio como administradores delegados, asegúrese de estar registrado en el Policy Server cuya configuración de servicio de directorio (ver *Servicios de directorio*, página 62) coincida con la configuración del directorio de inicio de sesión (ver *Cuentas de directorio*, página 251).

   Si sólo está agregando cuentas de usuario de Websense como administradores, puede estar registrado en cualquier Policy Server.

2. En **Cuentas de directorio**, marque la casilla para uno o más usuarios y luego haga clic en el botón de flecha derecha (>) para moverlos a la lista **Selección**.

   > **Nota**
   > Los grupos LDAP personalizados no pueden ser agregados como administradores.

   Si su entorno utiliza Active Directory (modo nativo) u otro servicio de directorio basado en LDAP, usted puede revisar el directorio para buscar nombres de usuarios, grupos, dominios o unidades organizativas específicos. Consulte *Cómo buscar el servicio de directorio*, página 69.

3. En **Cuentas de usuario de Websense**, marque la casilla para uno o más usuarios y luego haga clic en el botón de flecha derecha (>) para mover los usuarios resaltados a la lista **Selección**.

4. Configurar los **Permisos** para los administradores de este rol.

Opción	Descripción
Política	Marque esta opción para permitir que los administradores de este rol apliquen políticas a sus clientes administrados. Esto también permite el acceso a determinados parámetros de configuración de Websense.
Incondicional	Marque esta opción para permitir el acceso a todos los parámetros de configuración de Websense. Esta opción sólo se encuentra disponible cuando un superadministrador incondicional agrega administradores al rol de superadministrador con permisos para políticas.
Informes	Marque esta opción para permitir el acceso a herramientas de generación de informes. Utilice la página Modificar rol para configurar las funciones de informes específicas permitidas.

5. Cuando haya terminado de realizar los cambios, haga clic en **Aceptar** para volver a la página Modificar rol.
6. Para guardar los cambios, haga clic en **Aceptar** en la página Modificar rol. Los cambios no se implementan hasta que usted haya hecho clic en **Guardar todo**.

Cómo agregar clientes administrados

Temas relacionados:

- *Cómo utilizar la administración delegada*, página 254
- *Cómo modificar roles*, página 256

Los clientes administrados son los usuarios y equipos asignados a un rol, cuyas políticas configuran los administradores del rol. Los equipos, redes y clientes del directorio (usuarios, grupos, dominios y unidades organizativas) se pueden definir todos como clientes administrados.

Los superadministradores pueden utilizar la página **Administración delegada > Modificar rol >Agregar clientes administrados** para agregar tantos clientes como sea necesario a un rol. Cada cliente puede ser asignado a sólo un rol.

Si asigna un rango de red como cliente administrado de un rol, no puede asignar direcciones IP individuales de ese rango a ningún otro rol. Asimismo, no se puede asignar específicamente un usuario, grupo, dominio o unidad organizativa a 2 roles diferentes. Sin embargo, usted puede asignar un usuario a un rol y luego asignar un

grupo, dominio o unidad organizativa en el cual el usuario es miembro a un rol diferente.

> **Nota**
> Si un grupo es un cliente administrado de un rol y el administrador de ese rol aplica una política a cada miembro del grupo, los usuarios individuales de ese grupo no pueden ser asignados a otro rol más adelante.

Cuando agregue clientes administrados, considere qué tipos de clientes incluir. Si agrega direcciones IP a un rol, los administradores para ese rol pueden generar informes sobre **todas** las actividades para los equipos especificados. Si agrega usuarios a un rol, los administradores pueden generar informes sobre todas las actividades para esos usuarios, independientemente del equipo en el que se produjo la actividad.

Los administradores no se incluyen automáticamente como clientes administrados en los roles que administran, ya que esto les permitiría configurar sus propias políticas. Para permitir que los administradores visualicen el propio uso de Internet, active ver actividad propia (ver *Actividad propia*, página 342).

Si su organización ha implementado diferentes Policy Servers y estos se conectan con diferentes directorios, asegúrese de seleccionar el Policy Server conectado con el directorio que contiene los clientes que usted desea agregar.

> **Nota**
> Las mejores prácticas recomiendan que todos los clientes administrados del mismo rol sean del mismo servicio de directorio.

1. Seleccionar clientes para el rol:
   - En **Directorio**, marque la casilla para uno o más usuarios.

     Si su entorno utiliza Active Directory (modo nativo) u otro servicio de directorio basado en LDAP, usted puede revisar el directorio para buscar nombres de usuarios, grupos, dominios o unidades organizativas específicos. Consulte *Cómo buscar el servicio de directorio*, página 69.
   - En **Equipo**, especificar la dirección IP de un equipo que desee agregar a este rol.
   - En **Red**, especifique la primera y la última direcciones IP del rango de equipos que desee agregar como unidad.
2. Haga clic en el botón de flecha derecha (>), que se encuentra junto al tipo de cliente, para mover los clientes a la lista **Selección**.
3. Cuando haya terminado de realizar los cambios, haga clic en **Aceptar** para volver a la página Modificar rol.
4. Para guardar los cambios, haga clic en **Aceptar** en la página Modificar rol. Los cambios no se implementan hasta que usted haya hecho clic en **Guardar todo**.

Cómo manejar conflictos de roles

Temas relacionados:

- *Cómo utilizar la administración delegada*, página 254
- *Cómo agregar clientes administrados*, página 261

Los servicios de directorio permiten que el mismo usuario pertenezca a varios grupos. Como resultado de esto, un solo usuario puede existir en grupos que son administrados por diferentes roles de administración delegada. La misma situación se presenta con dominios y unidades organizativas.

Asimismo, es posible que un usuario sea administrado por un rol y pertenezca a un grupo, dominio o unidad organizativa administrado por un rol diferente. Si los administradores para ambos roles inician sesión simultáneamente, el administrador responsable del usuario podría aplicar políticas a ese usuario al mismo tiempo que el administrador responsable del grupo aplica políticas a los diferentes miembros del grupo.

Utilice la página **Administración delegada > Configurar Rol Prioridad** para indicarle al software de Websense qué hacer si se aplican diferentes políticas al mismo usuario debido a una superposición. Cuando se produce un conflicto, el software de Websense aplica la política de filtrado del rol que aparece más arriba en la lista.

1. Seleccione cualquier rol de la lista, excepto el de superadministrador.

   Nota
   El rol de superadministrador siempre aparece primero en esta lista. No se puede mover.

2. Haga clic en **Subir** o **Bajar** para cambiar su posición en la lista.
3. Repita los pasos 1 y 2 hasta que todos los roles tengan la prioridad deseada.
4. Cuando haya terminado de realizar los cambios, haga clic en **Aceptar** para guardar los cambios y volver a la página Administración delegada. Los cambios no se implementan hasta que usted haya hecho clic en **Guardar todo**.

Consideraciones especiales

Temas relacionados:

- *Cómo utilizar la administración delegada*, página 254
- *Cómo modificar roles*, página 256

Antes de eliminar roles de administración delegada o clientes administrados de un rol, revise la siguiente información.

Cómo liminar roles

En la página **Administración delegada**, los superadministradores incondicionales pueden eliminar cualquier rol que haya quedado obsoleto.

Al eliminar un rol, también se quitan todos los clientes que los administradores del rol han agregado a la página Clientes. Una vez que se borró el rol, si esos clientes pertenecen a alguna red, grupo o dominio administrado por otros roles, se rigen por la política correspondiente aplicada en esos roles (ver *Orden de filtrado*, página 80). De otro modo, se rigen por la política predeterminada del superadministrador.

1. En la página **Administración delegada**, marque la casilla que se encuentra junto a cada rol que desee eliminar.

   Nota
   No se puede eliminar el rol de superadministrador.

2. Haga clic en **Eliminar**.
3. Confirme la solicitud de eliminar para quitar los roles seleccionados de la página Administración delegada. Los cambios no son permanentes hasta que usted haya hecho clic en **Guardar todo**.

   Cuando usted vuelve a iniciar sesión en Websense Manager, el rol borrado ha desaparecido de la lista desplegable de roles del anuncio.

Cómo eliminar clientes administrados

No se pueden eliminar directamente los clientes de la lista de clientes administrados (Administración delegada >Modificar rol) si:

- el administrador ha aplicado una política al cliente.
- el administrador ha aplicado una política a uno o más de los miembros de una red, grupo, dominio o unidad organizativa.

También pueden surgir problemas si, durante el inicio de sesión en Websense Manager, el superadministrador elige un Policy Server distinto del que se comunica con el servicio de directorio que contiene los clientes que desea eliminar. Dado este caso, Policy Server y el servicio de directorio actuales no reconocen los clientes.

El superadministrador incondicional puede asegurarse de que se puedan eliminar los clientes correspondientes de la siguiente manera:

1. Inicie sesión en Websense Manager. Para ello elija el Policy Server cuyo servicio de directorio contenga los clientes administrados que desea eliminar. Debe iniciar sesión con permisos de superadministrador incondicional.
2. Abra la lista **Rol** del anuncio y elija el rol del que se van a eliminar clientes administrados.
3. Vaya a **Administración de políticas > Clientes** para ver una lista de todos los clientes a los que el administrador delegado ha asignado una política expresamente.

Esto puede incluir tanto a clientes que se identifican específicamente en la lista de clientes administrados del rol como a clientes que son miembros de redes, grupos, dominios o unidades organizativas de la lista de clientes administrados.

4. Elimine los clientes que corresponda.
5. Haga clic en **Aceptar** para guardar los cambios.
6. Abra la lista **Rol** del anuncio y seleccione el rol de **Superadministrador**.
7. Vaya a **Administración de políticas >Administración delegada > Editar rol**.
8. Elimine los clientes correspondientes de la lista de clientes administrados y luego haga clic en **Aceptar** para confirmar la solicitud de eliminar.
9. Para guardar los cambios, haga clic en **Aceptar** en la página Modificar rol. Los cambios no se implementan hasta que usted haya hecho clic en **Guardar todo**.

Varios administradores que acceden a Websense Manager

Temas relacionados:

- *Introducción a los administradores*, página 238
- *Cómo permitir el acceso a Websense Manager*, página 250

Los administradores de diferentes roles pueden obtener acceso a Websense Manager simultáneamente para realizar cualquier actividad permitida por los permisos de sus roles. Por ejemplo, los administradores del Rol A y del Rol B que cuentan con permisos para políticas pueden iniciar sesión en Websense Manager al mismo tiempo. Dado que administran diferentes clientes, pueden crear y aplicar políticas sin conflicto.

La situación es diferente si los administradores que tienen permisos para políticas en el mismo rol inician sesión al mismo tiempo. Para preservar la integridad de la estructura y las asignaciones de la política, sólo un administrador de un rol puede acceder a Websense Manager con permisos para políticas por vez. Si un segundo administrador con permisos para políticas para el mismo rol intenta iniciar sesión y el primer administrador continúa registrado, el segundo administrador debe elegir.

- Iniciar sesión para generar informes solamente, si el administrador tiene permisos para informes.
- Iniciar sesión en un rol diferente, si el administrador está asignado a otros roles.
- Intentar nuevamente después, cuando el primer administrador haya cerrado sesión.

Cuando los administradores que tienen tanto permisos para políticas como para informes inician sesión para generar informes, deben liberar sus permisos para políticas de inmediato para que otros administradores del rol puedan desempeñar actividades de administración de políticas.

- Vaya a la lista deslizable **Rol** del anuncio y elija **Liberar permisos para políticas**.

Un método alternativo consiste en crear una cuenta de usuario de Websense especial (ver *Cuentas de usuario de Websense*, página 252) para cada rol y otorgar a ese usuario sólo permisos para informes. Otorgar esas credenciales para inicio de sesión (nombre de usuario y contraseña) a los administradores del rol que tienen tanto permisos para políticas como para informes. Cuando los administradores necesiten generar informes, pueden iniciar sesión como este administrador de informes y dejar el acceso a políticas abierto para otro administrador.

Cómo definir restricciones de filtrado para todos los roles

Temas relacionados:

- *Introducción a los administradores*, página 238
- *Cómo crear una fijación de filtro*, página 267

El software de Websense permite a los superadministradores incondicionales establecer una fijación de filtro que bloquee categorías y protocolos para todos los clientes administrados por roles de administración delegada. Consulte *Cómo crear una fijación de filtro*, página 267,para obtener más información.

Los administradores de esos roles tienen la libertad de aplicar cualquier acción de filtrado a otras categorías y protocolos en sus políticas, pero aquellas categorías y protocolos bloqueados en la fijación de filtro no se pueden permitir.

Los cambios en la fijación de filtro se implementan para todos los clientes administrados tan pronto como se guardan los cambios. Los administradores delegados que se encuentren trabajando en Websense Manager cuando los cambios surtan efecto no verán los cambios en sus filtros hasta que vuelvan a iniciar sesión.

Nota

Cuando se copia un filtro del rol de superadministrador a otro rol, la copia adopta las restricciones de la fijación de filtro.

Los superadministradores no se encuentran limitados por la fijación de filtro. Pueden definir políticas que permiten el acceso a categorías y protocolos bloqueados y fijados para roles de administración delegada. Por lo tanto, las personas que requieren derechos de acceso especiales deben ser administradas por el rol de superadministrador.

Cómo crear una fijación de filtro

Temas relacionados:

- *Cómo definir restricciones de filtrado para todos los roles*, página 266
- *Cómo fijar categorías*, página 267
- *Cómo fijar protocolos*, página 268

La página **Administración de políticas > Fijación de filtro** le da la opción de modificar las categorías o protocolos que se bloquearán para todos los clientes administrados en los roles de administración delegada. Toda función de categoría o protocolo que se bloquee en la fijación de filtro se considera **bloqueada y fijada**.

- Haga clic en el botón **Categorías** para bloquear y fijar categorías o elementos de categorías específicos (palabras clave y tipos de archivo). Consulte *Cómo fijar categorías*, página 267.
- Haga clic en el botón **Protocolos** para bloquear y fijar protocolos o el registro para protocolos. Consulte *Cómo fijar protocolos*, página 268.

Cómo fijar categorías

Temas relacionados:

- *Cómo definir restricciones de filtrado para todos los roles*, página 266
- *Cómo crear una fijación de filtro*, página 267
- *Cómo fijar protocolos*, página 268

Utilice la página **Administración de políticas > Fijación de filtro > Categorías** para seleccionar las categorías que se bloquearán y fijarán para todos los miembros de roles de administración delegada. También se pueden bloquear y fijar palabras clave y tipos de archivo para una categoría.

1. Seleccione una categoría del árbol.

   Los roles de administración delegada no tienen acceso a categorías personalizadas creadas por los superadministradores. Por lo tanto, las categorías personalizadas no aparecen en este árbol.
2. Configure las restricciones para esta categoría en el cuadro que aparece junto al árbol de categorías.

Opción	Descripción
Fijar categoría	Bloquea y fija los accesos a sitios de esta categoría.
Fijar palabras clave	Bloquea y fija el acceso en base a palabras clave definidas para esta categoría en cada rol.

Opción	Descripción
Fijar tipos de archivos	Bloquea y fija los tipos de archivo seleccionados para sitios de esta categoría. Asegúrese de marcar la casilla para cada tipo de archivo que desea bloquear y fijar. Los tipos de archivo personalizados creados por el superadministrador se incluyen en esta lista porque se encuentran disponibles para los roles de administración delegada.
Aplicar a subcategorías	Aplica la misma configuración a todas las subcategorías de esta categoría.

Puede bloquear y fijar elementos seleccionados para todas las categorías de una sola vez, si corresponde. Seleccione **Todas las categorías** en el árbol y luego seleccione los elementos que desea bloquear para todas las categorías. Luego, haga clic en **Aplicar a subcategorías**.

3. Cuando haya terminado de realizar los cambios, haga clic en **Aceptar** para guardar los cambios y volver a la página Fijación de filtro. Los cambios no se implementan hasta que usted haya hecho clic en **Guardar todo**.

Cómo fijar protocolos

Temas relacionados:

- *Cómo definir restricciones de filtrado para todos los roles*, página 266
- *Cómo crear una fijación de filtro*, página 267
- *Cómo fijar categorías*, página 267

Utilice la página **Administración de políticas > Fijación de filtro > Protocolos** para bloquear y fijar el acceso a o bloquear el registro de protocolos seleccionados para todos los clientes administrados por los roles de administración delegada.

Nota

El registro de protocolo se asocia con las alertas de uso de protocolos. No se pueden generar alertas de uso para un protocolo a menos que esté configurado para registrar por lo menos un filtro de protocolo. La habilitación de la opción **Fijar registro de protocolo** a través de la fijación de filtro asegura que se generen alertas de uso para el protocolo. Consulte *Configuración de alertas de uso de protocolos*, página 292.

1. Seleccione un protocolo del árbol.

Los roles de administración delegada tienen acceso a protocolos personalizados creados por el superadministrador. Por lo tanto, los protocolos personalizados no aparecen en este árbol.

2. Configure las restricciones para este protocolo en el cuadro que aparece junto al árbol de protocolos.

Opción	Descripción
Fijar protocolo	Bloquea y fija accesos a aplicaciones y sitios Web mediante el uso de este protocolo.
Fijar registro de protocolo	Registra información sobre el acceso a este protocolo y evita que los administradores delegados desactiven el registro.
Aplicar a grupo	Aplica la misma configuración a todos los protocolos del grupo.

3. Cuando termine de realizar los cambios, haga clic en **Aceptar** para guardar los cambios y volver a la página Fijación de filtro. Los cambios no se implementan hasta que usted haya hecho clic en **Guardar todo**.

12 Administración de Websense Server

Temas relacionados:

- *Componentes del producto Websense*, página 272
- *Cómo trabajar con Policy Server*, página 278
- *Visualización y exportación del registro de auditoría*, página 284
- *Cómo detener e iniciar los servicios Websense*, página 286
- *Alertas*, página 287
- *Cómo hacer una copia de seguridad y restaurar los datos de Websense*, página 295

El filtrado del uso de Internet requiere la interacción entre varios componentes de software de Websense:

- Las solicitudes de los usuarios para el acceso a Internet las recibe Network Agent o un producto de integración de terceros.
- Las solicitudes se envían a Websense Filtering Service para ser procesadas.
- Filtering Service se comunica con Policy Server y Policy Broker para aplicar la política correspondiente en respuesta a la solicitud.

En la mayoría de los entornos, una sola base de datos Policy Database retiene información de cliente, filtro, política y configuración general, tanto si hay un solo Policy Server como si hay múltiples Policy Server.

Cada instancia de Websense Manager está asociada con una sola base de datos Policy Database, y se puede utilizar para configurar cada Policy Server asociado con esa base de datos.

Como la configuración de políticas realizada en Websense Manager se almacena en la base de datos central, la información sobre políticas está disponible automáticamente para todos los Policy Server asociados con esa base de datos Policy Database.

Componentes del producto Websense

Temas relacionados:

- *Componentes de filtrado*, página 273
- *Componentes de informes*, página 275
- *Componentes de identificación de usuarios*, página 276
- *Cómo trabajar con Policy Server*, página 278
- *Cómo detener e iniciar los servicios Websense*, página 286
- *Cómo revisar el estado actual del sistema*, página 294

El software de Websense está formado por varios componentes que trabajan en conjunto para proporcionar capacidades de identificación de usuarios, filtrado de Internet y realización de informes. Esta sección brinda información general sobre cada componente para ayudar a comprender y administrar el entorno de filtrado.

Los principales componentes de Websense incluyen:

- Policy Database
- Policy Broker
- Policy Server
- Filtering Service
- Network Agent
- Master Database
- Websense Manager
- Usage Monitor
- User Service
- Log Server
- Log Database

El software de Websense también incluye agentes de identificación transparente opcionales:

- DC Agent
- RADIUS Agent
- eDirectory Agent
- Logon Agent

Otros componentes opcionales incluyen:

- Remote Filtering Server
- Remote Filtering Client
- Websense Content Gateway

Componentes de filtrado

Componente	Descripción
Policy Database	Almacena los parámetros del software de Websense y la información de políticas.
Policy Broker	Administra solicitudes de los componentes de Websense para información de configuración general y de políticas.
Policy Server	• Identifica y realiza el seguimiento de la ubicación y el estado de otros componentes de Websense. • Almacena información de configuración específica de una sola instancia de Policy Server. • Comunica datos de configuración a Filtering Service, para utilizar en el filtrado de las solicitudes de Internet. Configure los parámetros de Policy Server en Websense Manager (consulte *Cómo trabajar con Policy Server*, página 278). Los parámetros de políticas y la mayoría de los parámetros de configuración se comparten entre Policy Server que comparten una base de datos Policy Database (consulte *Cómo trabajar en un entorno de múltiples Policy Server*, página 279).
Filtering Service	Proporciona filtrado de Internet junto con Network Agent o un producto de integración de terceros. Cuando un usuario solicita un sitio, Filtering Service recibe la solicitud y determina qué política se aplica. • Filtering Service debe estar en ejecución para poder filtrar y registrar las solicitudes de Internet. • Cada instancia de Filtering Service descarga su propia copia de la base de datos principal de Websense. Configure el comportamiento del filtrado y de Filtering Service en Websense Manager (consulte *Filtros para el uso de Internet*, página 37, y *Cómo configurar los valores de filtrado de Websense*, página 56).
Network Agent	• Mejora las funciones de filtrado y registros • Permite la administración de protocolos • Permite el filtrado en un entorno autónomo Para obtener más información, consulte *Configuración de redes*, página 345.
Master Database	• Incluye más de 36 millones de sitios Web, ordenados en más de 90 categorías y subcategorías. • Contiene más de 100 definiciones de protocolos para utilizar en protocolos de filtrado. Descargue la base de datos principal de Websense para activar el filtrado de Internet, y asegúrese de que la base de datos se mantiene actualizada. Si Master Database tiene más de 2 semanas de antigüedad, no puede realizarse el filtrado. Consulte *Base de datos principal de Websense*, página 31, para obtener más información.

Componente	Descripción
Websense Manager	Cumple la función de interfaz de configuración y administración para el software de Websense. Utilice Websense Manager para definir y personalizar las políticas de acceso a Internet, agregar o quitar clientes de filtrado, configurar componentes del software de Websense, etcétera. Consulte *Uso de Websense Manager*, página 17, para obtener más información.
Usage Monitor	Permite emitir alertas en base al uso de Internet. Usage Monitor realiza el seguimiento del acceso a protocolos y categorías URL y genera mensajes de alerta según el comportamiento de alerta que se haya configurado. Consulte *Alertas*, página 287, para obtener más información.
Remote Filtering Client	• Reside en equipos cliente fuera del ámbito del firewall de la red. • Identifica a los equipos como clientes para filtrar y se comunica con Remote Filtering Server. Consulte *Filtrado de clientes remotos*, página 157, para obtener más información.
Remote Filtering Server	• Permite el filtrado de clientes fuera del ámbito de un firewall de red. • Se comunica con Filtering Service para proporcionar la administración del acceso a Internet de los equipos remotos. Consulte *Filtrado de clientes remotos*, página 157, para obtener más información.
Websense Content Gateway	• Proporciona una robusta plataforma de proxy y caché. • Puede analizar el contenido de sitios Web y archivos en tiempo real para categorizar sitios previamente no categorizados. Consulte *Análisis de contenido con las opciones en tiempo real*, página 145.
Websense Security Gateway	Además de la función estándar de Websense Content Gateway: • Analiza código HTML para buscar amenazas a la seguridad (por ejemplo, phishing, redireccionamiento de URL, exploits de Web y elusión con proxy). • Inspecciona el contenido de los archivos para asignar una categoría de amenaza (por ejemplo, virus, caballos de Troya o gusanos). • Elimina contenido activo innecesario de ciertas páginas Web. Consulte *Análisis de contenido con las opciones en tiempo real*, página 145.

Componentes de informes

Componente	Descripción
Log Server	Registra datos de solicitudes de Internet, como: • El origen de la solicitud • La categoría o el protocolo asociados con la solicitud • Si la solicitud se permitió o se bloqueó • Si se aplicaron bloqueo de palabra clave, bloqueo de tipo de archivo, asignaciones de cuota, niveles de ancho de banda o protección mediante contraseña Con Network Agent y algunos productos de integración, Log Server también almacena información sobre la cantidad de ancho de banda utilizada Log Server debe instalarse en un equipo con Windows para permitir realizar informes de investigación y de presentación, y gráficos de páginas Hoy e Historial, en Websense Manager. Luego de instalar Log Server, configure Filtering Service para que traspase datos de registro a la ubicación correcta (consulte *Configuración de Filtering Service para el registro*, página 310).
Log Database	Almacena datos de solicitudes de Internet reunidos por Log Server para que los utilicen las herramientas de informes de Websense.

Componentes de identificación de usuarios

Componente	Descripción
User Service	• Se comunica con el servicio de directorio. • Transmite información relacionada con el usuario, como relaciones de usuario a grupo y de usuario a dominio, a Policy Server y Filtering Service, para utilizar en la aplicación de las políticas de filtrado. Si se ha instalado y configurado un agente de identificación transparente de Websense (consulte *Identificación transparente*, página 201), User Service ayuda a interpretar la información de inicio de sesión de los usuarios, y utiliza esta información para proporcionarle a Filtering Service asociaciones de nombre de usuario a dirección IP. Cuando usted agrega usuarios y grupos como clientes de Websense (consulte *Cómo agregar un cliente*, página 68), User Service proporciona información de nombre y ruta de acceso del servicio de directorio a Websense Manager. Para obtener información sobre la configuración del acceso al servicio de directorio, consulte *Servicios de directorio*, página 62.
DC Agent	• Ofrece identificación de usuario transparente para los usuarios en un servicio de directorio basado en Windows. • Se comunica con User Service para suministrarle información actualizada de inicio de sesión de los usuarios al software de Websense para que pueda utilizarla en el filtrado. Para obtener más información, consulte *DC Agent*, página 213.
Logon Agent	• Proporciona exactitud sin precedentes en la identificación de usuario transparente en redes Linux y Windows. • No requiere un servicio de directorio ni otro intermediario al capturar inicios de sesión de usuarios. • Detecta los inicios de sesión de usuarios a medida que ocurren. Logon Agent se comunica con la aplicación de inicio de sesión en equipos cliente para asegurar que los inicios de sesión de usuarios individuales sean capturados y procesados directamente por el software de Websense. Para obtener más información, consulte *Logon Agent*, página 216.

Componente	Descripción
eDirectory Agent	• Trabaja junto con Novell eDirectory para identificar a los usuarios de manera transparente. • Reúne información de inicio de sesión de usuarios de Novell eDirectory, que autentica a los usuarios que inician sesión en la red. • Asocia a cada usuario autenticado con una dirección IP, y luego trabaja junto con User Service para proporcionarle la información a Filtering Service. Para obtener más información, consulte *eDirectory Agent*, página 225.
RADIUS Agent	Permite la identificación transparente de los usuarios que utilizan conexión de acceso telefónico, Red Privada Virtual (VPN), Línea de Abonado Digital (DSL) u otro tipo de conexión remota para acceder a la red. Para obtener más información, consulte *RADIUS Agent*, página 219.

Información general sobre Policy Database

Websense Policy Database almacena tanto los datos de política (como parámetros de clientes, filtros, componentes de filtro y administración delegada) y los parámetros de configuración global especificados en Websense Manager. Los parámetros específicos de una sola instancia de Policy Server se almacenan por separado.

En la mayoría de los múltiples entornos de Policy Server, una sola base de datos Policy Database retiene datos de política y configuración general para múltiples Policy Server.

1. Al inicio, cada componente de Websense le solicita a la base de datos Policy Database la información de configuración que corresponda a través de Policy Broker.
2. Los componentes en ejecución con frecuencia controlan si hay cambios en la base de datos Policy Database.
3. Policy Database se actualiza cada vez que los administradores realizan cambios en Websense Manager y hacen clic en Guardar todo.
4. Luego de un cambio en Policy Database, cada componente solicita y recibe los cambios que afectan a su funcionamiento.

Realice copias de seguridad de la base de datos Policy Database con regularidad para salvaguardar información importante de configuración y políticas. Consulte *Cómo hacer una copia de seguridad y restaurar los datos de Websense*, página 295, para obtener más información.

Cómo trabajar con Policy Server

Policy Server es el componente del software de Websense que administra información de políticas y se comunica con Filtering Service para ayudar en la aplicación de políticas. Policy Server también es responsable de identificar otros componentes y realizar el seguimiento de sus ubicaciones y estados.

Cuando se inicia sesión en Websense Manager, se está iniciando sesión en una interfaz gráfica de Policy Server.

- Usted no puede iniciar sesión en Websense Manager hasta que este esté configurado para comunicarse con Policy Server.
- Si la instalación del software de Websense incluye múltiples Policy Server, se puede elegir entre instancias de Policy Server en el momento de iniciar sesión.
- Puede agregar y quitar instancias de Policy Server dentro de Websense Manager.

De modo predeterminado, la comunicación entre Websense Manager y una instancia central de Policy Server se establece durante la instalación de Websense Manager.

La mayoría de los entornos requieren un solo Policy Server. Un solo Policy Server se puede comunicar con múltiples instancias de Filtering Service y Network Agent para equilibrar las cargas. En empresas muy grandes (10.000 o más usuarios), sin embargo, puede ser de ayuda instalar múltiples instancias de Policy Server. Si instala Policy Server adicionales, agregue cada instancia a Websense Manager (consulte *Cómo agregar y editar instancias de Policy Server*, página 278).

Cómo agregar y editar instancias de Policy Server

Utilice la página **Configuración > Policy Server** para agregar instancias de Policy Server a Websense Manager, o para configurar o quitar Policy Server existentes.

Para agregar una instancia de Policy Server:

1. Haga clic en **Agregar**. Se abrirá la página Agregar Policy Server.
2. Ingrese la dirección IP o el nombre de host del equipo de Policy Server en el campo **Nombre o IP de servidor**.
3. Ingrese el **Puerto** que Websense Manager debe utilizar para comunicarse con esa instancia de Policy Server. El número predeterminado es **55806**.
4. Haga clic en **Aceptar** para volver a la página de Policy Server. La nueva instancia de Policy Server aparecerá en la lista.
5. Haga clic en **Aceptar** para guardar en caché todos los cambios realizados en la página de Policy Server. Los cambios no se implementarán hasta que usted haga clic en **Guardar todo**.

Para editar una instancia de Policy Server (por ejemplo, si cambian el nombre o la dirección IP del equipo de Policy Server), seleccione una dirección IP o nombre de host en la lista de Policy Server y luego haga clic en **Editar**.

Para eliminar una instancia de Policy Server, seleccione una dirección IP o nombre de host de la lista de Policy Server y luego haga clic en **Eliminar**. Al hacer clic en Eliminar, se quita la instancia de Policy Server de Websense Manager, pero no se desinstala ni se detiene el servicio Websense Policy Server. Si sólo hay una instancia de Policy Server en la lista, no puede eliminarla.

Cómo trabajar en un entorno de múltiples Policy Server

En algunos entornos distribuidos con una gran cantidad de usuarios, puede ser apropiado instalar múltiples Policy Server. Esto implica algunas consideraciones especiales.

- Si usted implementa una configuración que permita que el mismo cliente sea administrado por diferentes Policy Server, dependiendo de la carga actual, **no** implemente acciones de política por tiempo:
  - Acceso con contraseña
  - Confirmar
  - Cuota

  La información de tiempo asociada con estas funciones no se comparte entre Policy Server, y los clientes podrían tener permitido más o menos acceso a Internet del que usted pretende.

  Recuerde que la política predeterminada se implementa cada vez que no se aplica ninguna otra política a un cliente. Si los clientes pueden estar regidos por más de un Policy Server, asegúrese de que la política predeterminada no aplique filtros de categoría que aplican acciones por tiempo.
- Como la información de políticas se almacena en la base de datos Policy Database, los cambios a las políticas se comparten automáticamente entre todos los Policy Server al hacer clic en **Guardar todo**.
- Muchos parámetros de configuración global (como definiciones de clases de riesgo y opciones de alerta) también se comparten entre Policy Server.
- Los parámetros de configuración específicos de un solo Policy Server (como sus conexiones de Filtering Service y Network Agent) son almacenados localmente por cada Policy Server y no distribuidos.

Para cambiar entre Policy Server en Websense Manager para revisar o configurar parámetros que se aplican a una sola instancia de Policy Server:

1. En el anuncio de Websense, expanda la lista de **Policy Server** y seleccione una dirección IP.
2. Si hay cambios sin guardar en la instancia actual de Policy Server, aparece una lista de cambios. Realice una de las siguientes acciones:
   - Haga clic en **Guardar todo y finalizar sesión** para guardar los cambios y finalizar la sesión en el Policy Server actual.
   - Haga clic en **Cancelar cambios y finalizar sesión** para descartar los cambios y finalizar la sesión en el Policy Server actual.
   - Haga clic en **Volver** para continuar configurando el Policy Server actual.

Si no hay cambios no guardados, pasará directamente a la pantalla de inicio de sesión.

3. En la pantalla de inicio de sesión, ingrese un nombre de usuario y contraseña para iniciar la sesión en el Policy Server seleccionado, y luego haga clic en **Iniciar sesión**.

Cómo cambiar la dirección IP de Policy Server

Antes de cambiar la dirección IP del equipo de Policy Server, **detenga todos los servicios Websense** en el equipo. Si Websense Manager también está instalado en el equipo, esto incluye los servicios Apache2Websense y ApacheTomcatWebsense.

Luego de cambiar la dirección IP, debe actualizar manualmente los archivos de configuración de Websense utilizados por Websense Manager, Policy Server y otros servicios Websense antes de reanudar el filtrado.

Paso 1: Actualice la configuración de Websense Manager

Actualice Websense Manager para que utilice la nueva dirección IP para conectarse con Policy Server.

1. En el equipo de Websense Manager, detenga los servicios **Apache2Websense** y **ApacheTomcatWebsense** (si es necesario).

   Si Websense Manager y Policy Server están instalados en este mismo equipo, los servicios Apache ya se deberían haber detenido.
2. Navegue hasta el siguiente directorio:
   - Windows:

     ```
     C:\Archivos de programa\Websense\tomcat\conf\Catalina\localhost\
     ```
   - Linux:

     ```
     /opt/Websense/tomcat/conf/Catalina/localhost/
     ```
3. Ubique el archivo **mng.xml** y luego realice una copia de seguridad del archivo en otro directorio.
4. Abra **mng.xml** en un editor de texto (como Notepad o vi) y reemplace cada instancia de la antigua dirección IP de Policy Server con la nueva.

   La dirección IP de Policy Server aparece dos veces: como el valor **ps/default/host** y como el valor **psHosts**.
5. Cuando haya terminado, guarde y cierre el archivo.

No reinicie los servicios Apache hasta que haya completado las actualizaciones de configuración restantes de esta sección.

Paso 2: Actualice la configuración de Policy Server

Actualice el archivo de configuración de Policy Server y el archivo de inicialización utilizado para configurar la comunicación entre los componentes de Websense.

1. Si aún no lo ha hecho, detenga todos los servicios Websense en el equipo de Policy Server (consulte *Cómo detener e iniciar los servicios Websense*, página 286).
2. Navegue hasta el directorio **bin** de Websense.
   - Windows:

     `C:\Archivos de programa\Websense\bin`
   - Linux:

     `/opt/Websense/bin`
3. Ubique el archivo **config.xml** y luego realice una copia de seguridad del archivo en otro directorio.
4. Abra **config.xml** en un editor de texto y reemplace cada instancia de la antigua dirección IP de Policy Server con la nueva.
5. Cuando haya terminado, guarde y cierre el archivo.
6. En el directorio **bin**, ubique el archivo **websense.ini** y luego realice una copia de seguridad en otro directorio.
7. Abra **websense.ini** en un editor de texto y reemplace cada instancia de la antigua dirección IP de Policy Server con la nueva.
8. Cuando haya terminado, guarde y cierre el archivo.

Paso 3: Verifique la conexión de Log Database

Utilice el administrador de orígenes de datos ODBC de Windows en el equipo de Policy Server para verificar la conexión ODBC con Log Database.

1. Vaya a **Inicio > Configuración > Panel de control > Herramientas administrativas > Orígenes de datos (ODBC)**.
2. En la ficha **System DSN**, seleccione el nombre del origen de datos adecuado (de manera predeterminada, **wslogdb70**), y luego haga clic en **Configurar**.
3. Verifique que esté seleccionado el equipo del servidor de la base de datos correcto y luego haga clic en **Siguiente**.
4. Ingrese las credenciales utilizadas para conectarse con la base de datos y luego haga clic en **Siguiente**.
5. Acepte los valores predeterminados en las siguientes 2 pantallas y luego haga clic en **Probar origen de datos**.

Nota

Si la prueba produce un error, verifique el nombre del equipo del servidor de la base de datos y vuelva a intentarlo.

Si el nombre del equipo es correcto pero la prueba sigue produciendo un error, verifique que se esté utilizando el puerto de conexión correcto y que el firewall permita la comunicación en el puerto seleccionado.

Paso 4: Reinicie los servicios Websense

1. Reinicie el equipo de Policy Server. Asegúrese de que todos los servicios Websense del equipo se reinicien normalmente.
2. Si el Websense Manager utilizado para configurar este Policy Server está instalado en otro equipo, reinicie los servicios **Apache2Websense** y **ApacheTomcatWebsense** en ese equipo.

Nota

Si Websense Manager está instalado en el mismo equipo que Policy Server, los administradores deben utilizar la nueva dirección IP para iniciar sesión.

Cómo trabajar con Filtering Service

Filtering Service es el componente del software de Websense que funciona con Network Agent o un producto de integración de terceros para filtrar la actividad de Internet. Cuando un usuario solicita un sitio, Filtering Service recibe la solicitud, determina qué política se aplica y utiliza la política aplicable para determinar de qué manera se filtra el sitio.

Cada instancia de Filtering Service descarga su propia copia de la base de datos principal de Websense para utilizarla al determinar cómo filtrar las solicitudes de Internet.

Filtering Service también envía información sobre la actividad en Internet a Log Server, de modo que se pueda registrar y utilizar para crear informes.

Cuando usted inicia sesión en Websense Manager, un **Resumen de Filtering Service** en la página Estado > Hoy enumera la dirección IP y el estado actual de cada instancia de Filtering Service asociada con el Policy Server actual. Haga clic en una dirección IP de Filtering Service para obtener información más detallada sobre el Filtering Service seleccionado.

Revisión de detalles de Filtering Service

Utilice la página **Estado > Hoy > Detalles de Filtering Service** para revisar el estado de una instancia individual de Filtering Service.

En la página se enumera:

- La dirección IP de Filtering Service
- Si la instancia seleccionada se está ejecutando o no
- La versión de Filtering Service

  Esta debe coincidir con la versión que tiene del software de Websense, con todas las revisiones que se hayan aplicado.
- El sistema operativo que se ejecuta en el equipo de Filtering Service

- La plataforma de software de Websense

  Esto indica si el software de Websense se está ejecutando en modo autónomo o integrado con un producto de terceros.
- La dirección IP y el estado de todas las instancias de Network Agent con las cuales se comunica el Filtering Service seleccionado

Haga clic en **Cerrar** para volver a la página Hoy.

Revisión del estado de descarga de la base de datos principal

Cada instancia de Filtering Service de la red descarga su propia copia de la base de datos principal. Cuando trabaje en Websense Manager, en Resumen de alertas de estado de la página Estado > Hoy aparece un mensaje de estado cuando se está descargando una base de datos principal o si falla un intento de descarga.

Para obtener información detallada sobre las descargas de base de datos recientes o corrientes, haga clic en **Descarga de base de datos** en la barra de herramientas de la página Hoy. La página Descarga de base de datos incluye una entrada por cada instancia de Filtering Service asociada con el Policy Server actual.

Inicialmente, la página Descarga de base de datos muestra un resumen rápido de descarga, en el que se muestra dónde se descargó la base de datos, qué versión de la base de datos se descargó y si la descarga fue exitosa. A partir de esta vista de resumen, usted puede:

- Iniciar una descarga de base de datos para un solo Filtering Service (haga clic en **Actualizar**).
- Iniciar descargas de base de datos para todas las instancias de Filtering Service enumeradas (haga clic en **Actualizar todo**).
- Cancelar una o todas las actualizaciones corrientes.

Haga clic en una dirección IP de la lista de la derecha para revisar un estado más detallado de la descarga de base de datos del Filtering Service seleccionado.

- Si el Filtering Service seleccionado ha tenido problemas de descarga, posiblemente aparezca una recomendación para ocuparse del problema.
- Para iniciar manualmente una descarga de la base de datos para el Filtering Service seleccionado, haga clic en **Actualizar**.

Durante la descarga de la base de datos, la pantalla de estado muestra información detallada del progreso en cada etapa del proceso de descarga. Haga clic en **Cerrar** para ocultar la información de progreso y continuar trabajando en Websense Manager.

Reanudación de descargas de la base de datos principal Master Database

Si se interrumpe la descarga de una base de datos Master Database, el software de Websense intenta reanudar la descarga automáticamente. Si Filtering Service puede

reconectarse con el servidor de descarga, la descarga se reanuda desde donde se interrumpió.

Puede reiniciar manualmente una descarga con errores o interrumpida. Esto no reinicia la descarga desde el punto de interrupción, sino que reinicia el proceso desde el principio.

1. En Websense Manager, vaya a **Estado > Hoy** y haga clic en **Descargas de base de datos**.
2. Haga clic en **Detener todas las actualizaciones** para detener el proceso interrumpido.
3. Seleccione una instancia de Filtering Service y haga clic en **Actualizar**, o haga clic en **Actualizar todo**, para reiniciar el proceso de descarga desde el principio.

Visualización y exportación del registro de auditoría

El software de Websense proporciona una secuencia de auditoría que muestra cuáles administradores han accedido a Websense Manager, así como todos los cambios realizados a las políticas y los parámetros. Esta información está disponible únicamente para los superadministradores a quienes se les concedieron permisos de políticas (consulte *Los superadministradores*, página 239).

Los administradores delegados cuentan con un alto grado de control sobre las actividades de Internet de los clientes que administran. Monitorear sus cambios a través del registro de auditoría le permite a usted asegurarse de que este control se maneje con responsabilidad y de acuerdo con las políticas de uso aceptable de su empresa.

Utilice la página **Estado > Registro de auditoría** para ver el registro de auditoría y para exportar partes seleccionadas del mismo a un archivo de hoja de cálculo de Excel (XLS), si así lo desea.

Los registros de auditoría se guardan durante 60 días. Para preservar registros de auditoría durante más de 60 días, utilice la opción de exportación para exportar el registro con regularidad. Al exportar, no se eliminan registros del registro de auditoría.

Cuando se abre la página Registro de auditoría, aparecen los registros más recientes. Utilice la barra de desplazamiento y los botones de paginación que están arriba del registro para ver registros más antiguos.

El registro muestra la siguiente información. Si un elemento está truncado, haga clic en la entrada parcial para ver el registro completo en un cuadro de diálogo emergente.

Columna	Descripción
Fecha	Fecha y hora del cambio, ajustada por husos horarios. Para asegurar datos coherentes en el registro de auditoría, asegúrese de que los parámetros de fecha y hora de todas las máquinas que ejecuten componentes de Websense estén sincronizados.
Usuario	Nombre del usuario del administrador que realizó el cambio.
Servidor	Dirección IP o nombre del equipo que ejecuta el Policy Server afectado por el cambio. Este aparece solamente para los cambios que afectan al Policy Server, como los cambios realizados en la ficha Configuración.
Rol	Rol de administración delegada afectado por el cambio. Cuando un cambio afecta a un cliente explícitamente asignado como cliente administrado en el rol de administrador delegado, ese cambio se muestra como afectando al rol del superadministrador. Si el cambio afecta a un cliente que es miembro de un rango de red, un grupo, un dominio o una unidad organizativa asignados al rol, el cambio se muestra como afectando al rol del administrador delegado.
Tipo	Elemento de configuración que se modificó, como política, filtro de categorías o inicio/cierre de sesión.
Elemento	Identificador del objeto específico modificado, como el nombre del filtro de categorías o el nombre del rol.
Acción	Tipo de cambio realizado, como agregar, eliminar, cambiar, iniciar sesión, etcétera.
Anterior	Valor anterior al cambio.
Actual	Nuevo valor luego del cambio.

No se muestran todos los elementos de todos los registros. Por ejemplo, el rol no aparece en los registros de inicio de sesión y cierre de sesión.

Para exportar registros del registro de auditoría:

1. Seleccione un período de tiempo de la lista **Rango de exportación**.

   Elija **Últimos 60 días** para exportar el archivo de registro de auditoría completo.
2. Haga clic en **Ir**.

   Si Microsoft Excel está instalado en el equipo donde se ejecuta Websense Manager, se abrirá el archivo exportado. Utilice las opciones de Excel para guardar o imprimir el archivo.

   Si Microsoft Excel no está instalado en el equipo donde se ejecuta Websense Manager, siga las instrucciones de la pantalla para ubicar el software o guardar el archivo.

Cómo detener e iniciar los servicios Websense

Los servicios Websense están configurados para iniciarse cada vez que se reinicia el equipo. Sin embargo, en algunos casos es necesario detener o iniciar uno o más componentes del producto en forma independiente del reinicio de un equipo.

> **Nota**
> Si Filtering Service se encuentra en proceso de descarga de la base de datos principal Master Database, no deja de ejecutarse hasta que se completa la descarga.

Cuando detenga todos los servicios Websense, finalice siempre con los siguientes servicios, en el orden que aparece a continuación:

1. Websense Policy Server
2. Websense Policy Broker
3. Websense Policy Database

Tenga en cuenta que, a menos que un problema pertenezca específicamente a Policy Broker o a la base de datos Policy Database, es muy poco común que sea necesario reiniciar estos servicios. Evite reiniciar estos servicios cuando sea posible.

Cuando inicie todos los servicios Websense, comience siempre con los siguientes servicios, en el orden que aparece a continuación:

1. Websense Policy Database
2. Websense Policy Broker
3. Websense Policy Server

Windows

1. Abra el cuadro de diálogo de servicios de Windows (**Inicio > Configuración > Panel de control > Herramientas administrativas > Servicios**).
2. Haga clic con el botón secundario en el nombre del servicio Websense y seleccione **Detener** o **Iniciar**.

Linux:

En equipos con Linux, todos los servicios se detienen y se inician juntos cuando se utiliza este procedimiento.

1. Vaya al directorio **/opt/Websense**.
2. Compruebe el estado de los servicios Websense con el comando:
   - `./WebsenseAdmin status`
3. Detenga, inicie o reinicie todos los servicios Websense con los comandos:
   - `./WebsenseAdmin stop`
   - `./WebsenseAdmin start`

- `./WebsenseAdmin restart`

Advertencia

No utilice el comando **kill** para detener un servicio Websense, ya que puede dañar el servicio.

Alertas

Temas relacionados:

- *Control de desbordamiento*, página 288
- *Configuración de opciones generales de alerta*, página 288
- *Configuración de alertas del sistema*, página 290
- *Configuración de alertas de uso de categorías*, página 291
- *Configuración de alertas de uso de protocolos*, página 292

Para facilitar el seguimiento y la administración del software de Websense y la actividad en Internet del cliente, los superadministradores pueden configurar alertas para enviar cuando ocurren eventos seleccionados.

- **Alertas del sistema**: Notificación sobre el estado de la suscripción y la actividad de la base de datos principal Master Database.
- **Alertas de uso**: Notificación cuando la actividad de Internet para categorías o protocolos particulares alcanza umbrales configurados.

Se pueden enviar alertas a destinatarios seleccionados por correo electrónico, mensajes emergentes en la pantalla (mensajes **net send** en Windows) o mensajes SNMP.

Nota

Las alertas emergentes en la pantalla no se pueden enviar a equipos con Linux. Sin embargo, se pueden enviar desde un equipo con Linux donde se ejecute Policy Server a equipos con Windows, siempre que el cliente Samba esté instalado en el equipo con Linux. Consulte la publicación *Deployment Guide*.

Las alertas de uso se pueden generar para protocolos o categorías personalizados y definidos por Websense.

Control de desbordamiento

Temas relacionados:

- *Alertas*, página 287
- *Configuración de opciones generales de alerta*, página 288
- *Configuración de alertas de uso de categorías*, página 291
- *Configuración de alertas de uso de protocolos*, página 292

Hay controles incorporados para alertas de uso para evitar generar cantidades excesivas de mensajes de alerta. Utilice el parámetro **Máximo de alertas diarias por tipo de uso** para especificar un límite para la cantidad de alertas que se envían como respuesta a las solicitudes de los usuarios para categorías y protocolos particulares. Consulte *Configuración de opciones generales de alerta*, página 288, para obtener más información.

También se puede configurar límites de umbral para cada alerta de uso de categorías y protocolos. Por ejemplo, si configura un límite de umbral de 10 para una categoría determinada, se genera una alerta luego de 10 solicitudes para esa categoría (realizadas por cualquier combinación de clientes). Consulte *Configuración de alertas de uso de categorías*, página 291, y *Configuración de alertas de uso de protocolos*, página 292, para obtener más información.

Suponga que el parámetro máximo de alertas diarias es 20, y el umbral de alerta de categoría es 10. Los administradores solamente reciben alertas las primeras 20 veces que las solicitudes de categoría superan el umbral. Eso quiere decir que sólo los primeros 200 casos dan como resultado mensajes de alerta (umbral de 10 multiplicado por límite de alertas de 20).

Configuración de opciones generales de alerta

Temas relacionados:

- *Alertas*, página 287
- *Configuración de alertas del sistema*, página 290
- *Configuración de alertas de uso de categorías*, página 291
- *Configuración de alertas de uso de protocolos*, página 292

El software de Websense puede notificarles a los administradores sobre varios tipos de eventos del sistema, como actualizaciones a las categorías de la base de datos principal Master Database y problemas de suscripción, así como del uso de Internet que supera los umbrales definidos.

Utilice la página **Configuración > Alertas y notificaciones > Alertas** para seleccionar y configurar los métodos de notificación deseados, según se describe a

continuación. Luego, utilice las otras páginas de la sección Configuración > Alertas y notificaciones para activar las alertas que quiere recibir.

1. Ingrese un número en el campo **Máximo de alertas diarias por tipo de uso** para limitar la cantidad total de alertas generadas diariamente para cada alerta de uso de categorías y protocolos.

   Por ejemplo, podría configurar las alertas de uso para que se envíen cada 5 veces (umbral) que alguien solicite un sitio en la categoría Deportes. Según la cantidad de usuarios y sus patrones de uso de Internet, eso podría generar cientos de alertas por día.

   Si usted ingresa 10 como el máximo de alertas diarias por tipo de uso, se generan sólo 10 mensajes de alerta por día para la categoría Deportes. En este ejemplo, estos mensajes lo alertan sobre las primeras 50 solicitudes de sitios de Deportes (5 solicitudes por alerta multiplicadas por 10 alertas).

2. Marque la casilla **Activar alertas por correo electrónico** para enviar alertas y notificaciones por correo electrónico. Luego, configure estos parámetros de correo electrónico.

IP o nombre de servidor SMTP	Dirección IP o nombre del servidor SMTP a través del cual se deben enrutar las alertas de correo electrónico.
Dirección de correo electrónico De	Direcciones de correo electrónico a utilizar como remitente para las alertas enviadas por correo electrónico.
Dirección de correo electrónico de administrador (Para)	Dirección de correo electrónico del destinatario principal de las alertas enviadas por correo electrónico.
Direcciones de correo electrónico de destinatarios (Cc)	Direcciones de correo electrónico de hasta 50 destinatarios adicionales. Cada dirección debe estar en una línea por separado.

3. Marque la casilla **Activar alertas emergentes** para mostrar mensajes emergentes en computadoras específicas. Luego, ingrese la dirección IP o el nombre del equipo para un máximo de 50 **Destinatarios**, cada una en una línea por separado.

> **Nota**
>
> Las alertas emergentes no se pueden enviar a equipos con Linux. Sin embargo, se pueden enviar desde un equipo con Linux donde se ejecute Policy Server a equipos con Windows, siempre que el cliente Samba esté instalado en el equipo con Linux. Consulte la publicación *Deployment Guide*.

4. Marque la casilla **Activar alertas SNMP** para enviar mensajes de alerta a través de un sistema de captura SNMP instalado en su red. Luego, proporcione información sobre su sistema de captura SNMP.

Nombre de comunidad	Nombre de la comunidad de captura de su servidor de captura SNMP.
Nombre o IP de servidor	Dirección IP o nombre del servidor de captura SNMP.
Puerto	Número de puerto que utilizan los mensajes SNMP.

5. Cuando haya terminado, haga clic en **Aceptar** para guardar los cambios en caché. Los cambios no se implementarán hasta que usted haga clic en **Guardar todo**.

Configuración de alertas del sistema

Temas relacionados:

- *Alertas*, página 287
- *Configuración de opciones generales de alerta*, página 288
- *Cómo revisar el estado actual del sistema*, página 294

Websense Manager muestra información detallada del estado del sistema a través de la página **Estado > Alertas** (información detallada), que se describe en *Cómo revisar el estado actual del sistema*, página 294.

Para asegurarse de que los administradores reciban notificaciones sobre los eventos importantes del sistema, como un error de descarga de la base de datos o una suscripción a punto de caducar, cuando no hayan iniciado sesión con Websense Manager, configure las alertas del sistema Websense para que se distribuyan mediante correo electrónico, mensajes emergentes o a través del sistema de captura SNMP.

En la ficha Configuración, utilice la página **Alertas y notificaciones > Sistema** para seleccionar el método utilizado para enviar estas alertas a los administradores de Websense, así como qué alertas enviar.

1. Para cada alerta, marque los métodos de entrega a utilizar. Según qué métodos estén activados en la página Alertas, puede elegir los métodos **Correo electrónico**, **Emergentes** y **SNMP**.

   Nota
   Además de generar una alerta, en el visor de sucesos de Windows (sólo Windows) y en el archivo Websense.log (Windows y Linux) se registra información sobre los errores en la descarga de la base de datos principal Master Database y los niveles de suscripción excedida.

   Hay disponibles alertas para eventos tales como:

- La suscripción caduca dentro de una semana.
- Han cambiado los motores de búsqueda admitidos de Search Filtering.
- Error al descargar la base de datos principal de Websense.
- Se agregó o se quitó una categoría o un protocolo de la base de datos principal Master Database.
- La cantidad de usuarios actuales supera el nivel de suscripción.
- La cantidad de usuarios actuales ha alcanzado el 90% del nivel de suscripción.
- La suscripción caducará dentro de un mes.
- La base de datos principal Master Database de Websense se ha actualizado.

2. Cuando haya terminado, haga clic en **Aceptar** para guardar los cambios en caché. Los cambios no se implementarán hasta que usted haga clic en **Guardar todo**.

Configuración de alertas de uso de categorías

Temas relacionados:

- *Alertas*, página 287
- *Control de desbordamiento*, página 288
- *Configuración de opciones generales de alerta*, página 288
- *Cómo agregar alertas de uso de categorías*, página 292

El software de Websense puede notificarle cuando la actividad en Internet de categorías URL particulares alcanza un umbral definido. Usted puede definir alertas para solicitudes permitidas o para solicitudes bloqueadas para la categoría.

Por ejemplo, posiblemente quiera recibir alertas cada vez que se hayan permitido 50 solicitudes de sitios en la categoría Compras para decidir si debe colocar restricciones en esa categoría. O posiblemente quiera recibir una alerta cada vez que se hayan bloqueado 100 solicitudes de sitios en la categoría Entretenimiento, para ver si los usuarios se están adaptando a una nueva política de uso de Internet.

En la ficha Configuración, utilice la página **Alertas y notificaciones > Uso de categorías** para ver las alertas que ya se han establecido y para agregar o eliminar alertas de uso de categorías.

1. Vea las listas **Alertas de uso de categorías permitidas** y **Alertas de uso de categorías bloqueadas** para saber cuáles categorías están configuradas para alertas, el umbral de cada una y los métodos de alerta seleccionados.
2. Haga clic en **Agregar** debajo de la lista correspondiente para abrir la página Agregar alertas de uso de categorías (consulte *Cómo agregar alertas de uso de categorías*, página 292) y configurar categorías URL adicionales para enviar alertas.
3. Marque la casilla de las categorías que quiera eliminar de la lista y luego haga clic en **Eliminar** debajo de la lista correspondiente.

4. Cuando haya terminado, haga clic en **Aceptar** para guardar los cambios en caché y volver a la página Alertas de uso de categorías. Los cambios no se implementarán hasta que usted haga clic en **Guardar todo**.

Cómo agregar alertas de uso de categorías

Temas relacionados:

- *Alertas*, página 287
- *Configuración de opciones generales de alerta*, página 288
- *Configuración de alertas de uso de categorías*, página 291

La página **Agregar alertas de uso de categorías** aparece al hacer clic en Agregar en la página Alertas de uso de categorías. Aquí, puede seleccionar nuevas categorías para las alertas de uso, establecer el umbral de estas alertas y seleccionar los métodos de alerta.

1. Marque la casilla al lado de cada categoría que quiera agregar con el mismo umbral y los mismos métodos de alerta.

   Nota
   No puede agregar alertas de uso de ninguna categoría excluida del registro. Consulte *Configuración de Filtering Service para el registro*, página 310.

2. Para configurar el **Umbral**, seleccione la cantidad de solicitudes que hacen que se genera una alerta.
3. Marque la casilla de cada método de alerta que quiera (**Correo electrónico**, **Emergente**, **SNMP**) para estas categorías.

   Sólo los métodos de alerta activados en la página Alertas (consulte *Configuración de opciones generales de alerta*, página 288) están disponibles para seleccionar.
4. Haga clic en **Aceptar** para guardar los cambios en caché y volver a la página Alertas de uso de categorías (consulte *Configuración de alertas de uso de categorías*, página 291). Los cambios no se implementarán hasta que usted haga clic en **Guardar todo**.

Configuración de alertas de uso de protocolos

Temas relacionados:

- *Alertas*, página 287
- *Control de desbordamiento*, página 288
- *Configuración de opciones generales de alerta*, página 288
- *Cómo agregar alertas de uso de protocolos*, página 293

El software de Websense puede notificarle cuando la actividad de Internet de un protocolo en particular alcanza un umbral definido. Usted puede definir alertas para solicitudes permitidas o bloqueadas del protocolo seleccionado.

Por ejemplo, posiblemente quiera recibir alertas cada vez que se hayan permitido 50 solicitudes de un protocolo de mensajería instantánea en particular para decidir si debe colocar restricciones en ese protocolo. O posiblemente quiera recibir una alerta cada vez que se hayan bloqueado 100 solicitudes de un protocolo de compartición de archivos P2P, para ver si los usuarios se están adaptando a una nueva política de uso de Internet.

En la ficha Configuración, utilice la página **Alertas y notificaciones > Alertas de uso de protocolos** para ver las alertas que ya se han establecido y para agregar o eliminar alertas de uso de protocolos.

1. Vea las listas **Alertas de uso de protocolos permitidos** y **Alertas de uso de protocolos bloqueados** para saber cuáles protocolos están configurados para alertas, el umbral de cada uno y los métodos de alerta seleccionados.
2. Haga clic en **Agregar** debajo de la lista correspondiente para abrir la página Agregar alertas de uso de protocolos (consulte*Cómo agregar alertas de uso de protocolos*, página 293) y configurar protocolos adicionales para enviar alertas.
3. Marque la casilla de los protocolos que quiera eliminar y luego haga clic en **Eliminar** debajo de la lista correspondiente.
4. Cuando haya terminado, haga clic en **Aceptar** para guardar los cambios en caché y volver a la página Alertas de uso de protocolos. Los cambios no se implementarán hasta que usted haga clic en **Guardar todo**.

Cómo agregar alertas de uso de protocolos

Temas relacionados:

- *Alertas*, página 287
- *Configuración de opciones generales de alerta*, página 288
- *Configuración de alertas de uso de protocolos*, página 292

Utilice la página **Alertas de uso de protocolos > Agregar alertas de uso de protocolos** para seleccionar nuevos protocolos para alertas de uso, establecer el umbral de estas alertas y seleccionar los métodos de alerta.

1. Marque la casilla al lado de cada protocolo que quiera agregar con el mismo umbral y los mismos métodos de alerta.

   Notas

   No puede seleccionar un protocolo para enviar una alerta a menos que esté configurado para iniciar sesión en uno o más filtros de protocolos.

   Las alertas de protocolos sólo reflejan el uso de los clientes regidos por un filtro de protocolos que registra el protocolo.

2. Para configurar el **Umbral**, seleccione la cantidad de solicitudes que hacen que se genera una alerta.
3. Seleccione cada método de alerta que quiera (**Correo electrónico**, **Emergente**, **SNMP**) para estos protocolos.

   Sólo los métodos de alerta activados en la página Alertas (consulte *Configuración de opciones generales de alerta*, página 288) están disponibles para seleccionar.
4. Haga clic en **Aceptar** para guardar los cambios en caché y volver a la página Alertas de uso de protocolos (consulte *Configuración de alertas de uso de protocolos*, página 292). Los cambios no se implementarán hasta que usted haga clic en **Guardar todo**.

Cómo revisar el estado actual del sistema

Utilice la página **Estado > Alertas** para buscar información sobre los problemas que afectan al estado del software de Websense, obtener ayuda para solucionar problemas y revisar los detalles de las actualizaciones recientes en tiempo real realizadas a la base de datos principal de Websense.

La lista **Alertas activas** muestra el estado de los componentes supervisados del software de Websense.

- Para obtener información detallada sobre cuáles componentes se supervisan, haga clic en **¿Qué se está supervisando?** arriba de la lista de mensajes de alerta.
- Para solucionar un problema, haga clic en el botón **Soluciones** que está al lado del mensaje de error o advertencia.
- Para ocultar un mensaje de alerta, haga clic en **Avanzado**. Si su empresa no utiliza Log Server, Network Agent o User Service, o si usted no tiene pensado activar WebCatcher, marque una casilla para ocultar la alerta asociada. Cuando haya terminado, haga clic en **Aceptar** para hacer efectivo el cambio.

  Vuelva a hacer clic en **Avanzado** para ocultar las opciones avanzadas.

La lista **Actualizaciones de base de datos en tiempo real** proporciona información sobre actualizaciones de emergencia a la base de datos principal de Websense, y muestra:

- Cuándo ocurrió la actualización
- El tipo de actualización
- El número de versión de la nueva base de datos
- El motivo de la actualización
- La dirección IP de la instancia de Filtering Service que recibió la actualización

Estas actualizaciones complementarias ocurren además de las actualizaciones regulares planificadas de la base de datos principal Master Database y se pueden utilizar, por ejemplo, para recategorizar un sitio que ha sido temporalmente categorizado incorrectamente. El software de Websense verifica que se realicen actualizaciones a la base de datos cada hora.

Para los usuarios de Websense Web Security, la página Alertas incluye una tercera lista: **Actualizaciones de seguridad en tiempo real**. Esta lista tiene el mismo formato que la lista Actualizaciones de la base de datos en tiempo real, pero específicamente muestra actualizaciones de la base de datos relacionadas con la seguridad.

Si se instalan actualizaciones de seguridad tan pronto como se crean, se elimina la vulnerabilidad ante amenazas, como que haya nuevos mensajes fraudulentos o phishing (fraude de identidad), aplicaciones malintencionadas o código malicioso que infecten a una aplicación o un sitio Web dominante.

Para obtener más información sobre las actualizaciones de seguridad en tiempo real, consulte *Real-Time Security Updates™*, página 32.

Utilice el botón **Imprimir**, arriba de la página, para abrir una ventana secundaria con una versión para imprimir del área Alertas. Utilice las opciones del navegador para imprimir esta página, que omite todas las opciones de navegación que aparecen en la ventana principal de Websense Manager.

Cómo hacer una copia de seguridad y restaurar los datos de Websense

Temas relacionados:

- *Planificación de realización de copias de seguridad*, página 298
- *Ejecución de copias de seguridad inmediatas*, página 299
- *Mantenimiento de las copias de seguridad de archivos*, página 300
- *Restauración de los datos de Websense*, página 301
- *Cómo discontinuar la realización de copias de seguridad planificadas*, página 302
- *Referencia de comandos*, página 302

La utilidad de copias de seguridad Websense Backup Utility facilita la manera de realizar copias de seguridad de los parámetros del software de Websense y los datos de políticas, y de volver a una configuración anterior. Los datos que guarda la utilidad también se pueden utilizar para importar información de configuración de Websense luego de una actualización.

La utilidad de copias de seguridad Backup Utility guarda:

- Información de configuración global, que incluye datos de clientes y de políticas, almacenada en la base de datos Policy Database.
- Información de configuración local, como parámetros de Filtering Service y Log Server, almacenada por cada Policy Server.
- Archivos de inicialización y configuración de los componentes de Websense.

El proceso de realización de copias de seguridad funciona de la siguiente manera:

1. Usted inicia una copia de seguridad inmediata (consulte *Ejecución de copias de seguridad inmediatas*, página 299) o define una planificación para realizar copias de seguridad (consulte *Planificación de realización de copias de seguridad*, página 298).
   - Active manualmente la realización de una copia de seguridad en cualquier momento.
   - Las copias de seguridad de los archivos se almacenan en un directorio que usted especifica cuando ejecuta o planifica la realización de copias de seguridad.
2. La utilidad de copias de seguridad Backup Utility verifica todos los componentes de Websense del equipo, reúne los datos elegibles para realizar la copia de seguridad y crea un archivo. El nombre del archivo tiene el siguiente formato:

   `wsbackup_yyyy-mm-dd_hhmmss.tar.gz`

   Aquí, *yyyy-mm-dd_hhmmss* representa la fecha y hora de la realización de la copia de seguridad. **tar.gz** es un formato de archivo comprimido portátil.

   Sólo el root (Linux) y los miembros del grupo de administradores (Windows) pueden acceder a las copias de seguridad de los archivos.

Ejecute la utilidad de copias de seguridad Websense Backup Utility en cada equipo que incluya componentes de Websense. La herramienta identifica y guarda cualquiera de los siguientes archivos que encuentra en el equipo actual:

Ruta	Nombre de archivo
\Program Files\Websense\bin *o* **/opt/Websense/bin**	authserver.ini BrokerService.cfg config.xml eimserver.ini LogServer.ini netcache.conf securewispproxy.ini transid.ini upf.conf websense.ini WebUI.ini wsauthserver.ini wscitrix.ini WSE.ini wsedir.ini wsradius.ini wsufpserver.ini
bin/i18n	i18n.ini
bin/postgres/data	postgresql.conf pg_hba.conf
BlockPages/*/Custom	Todos los parámetros de las páginas de bloqueo personalizadas
tomcat/conf/Catalina/Localhost	mng.xml
Windows\system32	isa_ignore.txt
Windows\system32\bin	ignore.txt
/etc/wsLib	wsSquid.ini

Guarde las copias de seguridad de los archivos de Websense en un lugar seguro. Estos archivos deben formar parte de los procesos habituales de realización de copias de seguridad de su empresa.

Para volver a una configuración anterior:

1. Recupere las copias de seguridad de los archivos del sitio donde las guardó.
2. Copie cada copia de seguridad de archivo en el equipo Websense en el que lo creó.

3. Ejecute la utilidad de copias de seguridad Backup Utility en modo de restauración.

> **Importante**
> Siempre utilice la utilidad de copias de seguridad Backup Utility para restaurar una configuración de software de Websense. No extraiga los archivos del archivo con otras utilidades de extracción.
>
> Si la copia de seguridad del archivo está dañada, no podrá restaurar la configuración.

Durante el proceso de restauración, cualquier mensaje de error o advertencia aparecerá en el equipo en que se está ejecutando la restauración.

Planificación de realización de copias de seguridad

Temas relacionados:

- *Ejecución de copias de seguridad inmediatas*, página 299
- *Mantenimiento de las copias de seguridad de archivos*, página 300
- *Restauración de los datos de Websense*, página 301
- *Cómo discontinuar la realización de copias de seguridad planificadas*, página 302
- *Referencia de comandos*, página 302

Para planificar la realización de copias de seguridad, abra una línea de comandos y navegue al directorio bin de Websense (**C:\Program Files\Websense\bin** o **opt/Websense/bin**, de manera predeterminada). Ingrese el siguiente comando:

```
wsbackup -s -t "<m> <h> <día_del_mes> <mes>
   <día_de_la_semana>" -d <directory>
```

Tenga en cuenta que la información de hora utiliza el formato **crontab** y es obligatorio usar las comillas y los espacios.

En lugar de las variables que aparecen en el ejemplo, proporcione la siguiente información:

Variable	Información
<m>	0 - 59 Especifique el minuto preciso para comenzar a hacer la copia de seguridad.
<h>	0 - 23 Especifique la hora general del día para comenzar a hacer la copia de seguridad.

Variable	Información
<día_del_mes>	1 - 31 Especifique la fecha para realizar la copia de seguridad. Si planifica la realización de una copia de seguridad para los días 29 - 31, la utilidad utiliza el procedimiento de sustitución estándar del sistema operativo en los meses que no incluyen esa fecha.
<mes>	1 - 12 Especifique el mes para realizar la copia de seguridad.
<día_de_la_semana>	0 - 6 Especifique un día de la semana. 0 representa el domingo.

Cada campo puede contener un número, un asterisco o una lista de parámetros. Consulte cualquier referencia de **crontab** para obtener detalles.

Ejecución de copias de seguridad inmediatas

Temas relacionados:

- *Planificación de realización de copias de seguridad*, página 298
- *Mantenimiento de las copias de seguridad de archivos*, página 300
- *Restauración de los datos de Websense*, página 301
- *Cómo discontinuar la realización de copias de seguridad planificadas*, página 302
- *Referencia de comandos*, página 302

Para ejecutar la realización de una copia de seguridad inmediata, abra una línea de comandos y navegue al directorio bin de Websense (**C:\Program Files\Websense\bin** o **opt/Websense/bin**, de manera predeterminada). Ingrese el siguiente comando:

```
wsbackup -b -d <directory>
```

Aquí, *directory* indica el directorio de destino de la copia de seguridad del archivo.

Advertencia

No guarde copias de seguridad de archivos en el directorio **bin** de Websense. Este directorio es eliminado si usted desinstala el software de Websense.

Cuando inicie una copia de seguridad inmediata, cualquier mensaje de error y notificación aparecerá en la consola del equipo en que se está ejecutando la realización de la copia de seguridad.

Mantenimiento de las copias de seguridad de archivos

Temas relacionados:

- *Planificación de realización de copias de seguridad*, página 298
- *Ejecución de copias de seguridad inmediatas*, página 299
- *Restauración de los datos de Websense*, página 301
- *Cómo discontinuar la realización de copias de seguridad planificadas*, página 302
- *Referencia de comandos*, página 302

Cuando realiza un a copia de seguridad, se crea un archivo de configuración (**WebsenseBackup.cfg**) que se almacena con la copia de seguridad del archivo. Este archivo de configuración especifica:

- Durante cuánto tiempo se guardará la copia de seguridad del archivo en el directorio de copias de seguridad
- La cantidad máxima de espacio en disco que pueden consumir todas las copias de seguridad de archivos en el directorio

Edite el archivo **WebsenseBackup.cfg** en cualquier editor de texto para cambiar cualquiera de estos parámetros:

Parámetro	Valor
KeepDays	Cantidad de días que los archivos deben permanecer en el directorio de copias de seguridad. El valor predeterminado es 365.
KeepSize	Cantidad de bytes asignados para las copias de seguridad de archivos. El valor predeterminado es 10857600.

Todos los archivos más antiguos que el valor de **KeepDays** se eliminarán del directorio de copias de seguridad. Si se sobrepasa la cantidad de espacio en disco asignada, los archivos más antiguos se eliminarán del directorio de copias de seguridad para dejar espacio para los archivos más recientes.

Restauración de los datos de Websense

Temas relacionados:

- *Planificación de realización de copias de seguridad*, página 298
- *Ejecución de copias de seguridad inmediatas*, página 299
- *Mantenimiento de las copias de seguridad de archivos*, página 300
- *Cómo discontinuar la realización de copias de seguridad planificadas*, página 302
- *Referencia de comandos*, página 302

Al restaurar datos de configuración de Websense, asegúrese de restaurar los datos de los componentes que existen en el equipo actual.

Para iniciar el proceso de restauración, abra una línea de comandos y navegue al directorio bin de Websense (**C:\Program Files\Websense\bin** o **opt/Websense/bin**, de manera predeterminada). Ingrese el siguiente comando:

```
wsbackup -r -f archive_file.tar.gz
```

Importante

El proceso de restauración puede tardar unos minutos. No detenga el proceso durante la restauración.

Durante el proceso de restauración, la utilidad de copias de seguridad Backup Utility detiene todos los servicios Websense. Si la utilidad no puede detener los servicios, envía un mensaje en el cual le pide al usuario que los detenga manualmente. Los servicios se deben detener en el orden que se describe en *Cómo detener e iniciar los servicios Websense*, página 286.

La utilidad de copias de seguridad Backup Utility guarda algunos archivos utilizados para la comunicación con productos de integración de terceros. Dado que estos archivos residen fuera de la estructura del directorio de Websense, deberá restaurarlos manualmente, copiando cada archivo en el directorio que corresponda.

Los archivos que se deben restaurar manualmente incluyen:

Nombre de archivo	Restaurar a
isa_ignore.txt	**Windows\system32**
ignore.txt	**Windows\system32\bin**
wsSquid.ini	**/etc/wsLib**

Cómo discontinuar la realización de copias de seguridad planificadas

Temas relacionados:

- *Planificación de realización de copias de seguridad*, página 298
- *Ejecución de copias de seguridad inmediatas*, página 299
- *Mantenimiento de las copias de seguridad de archivos*, página 300
- *Restauración de los datos de Websense*, página 301
- *Referencia de comandos*, página 302

Para borrar la planificación de copias de seguridad y detener la ejecución de las copias de seguridad planificadas actualmente, abra una línea de comandos y navegue al directorio bin de Websense (**C:\Program Files\Websense\bin** o **opt/Websense/bin**, de manera predeterminada). Ingrese el siguiente comando:

```
wsbackup -u
```

Referencia de comandos

Temas relacionados:

- *Planificación de realización de copias de seguridad*, página 298
- *Ejecución de copias de seguridad inmediatas*, página 299
- *Mantenimiento de las copias de seguridad de archivos*, página 300
- *Restauración de los datos de Websense*, página 301
- *Cómo discontinuar la realización de copias de seguridad planificadas*, página 302

Sólo el root (Linux) y los miembros del grupo de administradores (Windows) pueden ejecutar la utilidad de copias de seguridad Backup Utility.

Para ver una lista completa de opciones de comandos de la utilidad de copias de seguridad Backup Utility en cualquier momento, ingrese:

```
wsbackup -h
```

o

```
wsbackup --help
```

El comando **wsbackup** toma las siguientes opciones:

- `-b` *o* `--backup`
- `-d` *directory_path* *o* `--dir` *directory_path*
- `-f` *full_file_name* *o* `--file` *full_file_name*
- `-h` *o* `--help` *o* `-?`

- `-r` *o* `--restore`
- `-s` *o* `--schedule`
- `-t` *o* `--time`
- `-u` *o* `--unschedule`
- `-v` *o* `--verbose [0...3]`

13 Administración de informes

Temas relacionados:

- *Planificación de su configuración*, página 306
- *Administración del acceso a herramientas de generación de informes*, página 306
- *Configuración básica*, página 307
- *utilidad Log Server Configuration*, página 312
- *Administración de la base de datos de registro*, página 326
- *Configuración de los informes de investigación*, página 337
- *Actividad propia*, página 342

Para utilizar los informes de presentación y los informes de investigación de Websense, debe instalar Websense Manager y los componentes de generación de informes en un servidor de Windows. También debe configurar el software de Websense para que registre la actividad de filtrado de Internet.

El proceso envía registros al Log Server de Websense, que los procesa en una base de datos de registro que debe instalarse en un motor de base de datos admitido: Microsoft SQL Server Desktop Engine (normalmente denominado MSDE en este documento) o Microsoft SQL Server Enterprise o Standard Editions (ambos normalmente denominados Microsoft SQL Server). Consulte la *guía de instalación* de Websense para obtener más información acerca de la instalación de estos componentes de generación de informes.

Cuando genera un informe, Websense Manager muestra información de la base de datos de registro según el filtro que usted defina para el reporte.

Las organizaciones que instalan Websense Manager en un servidor de Linux, o que prefieren usar Linux para sus informes, pueden instalar el Websense Explorer aparte para productos Linux para generar informes. Este producto funciona en forma independiente del Websense Manager. Consulte la *guía del administrador de Websense Explorer para Linux* para ver las instrucciones sobre la instalación y el uso del programa.

Planificación de su configuración

Según el volumen del tráfico de Internet en su red, la base de datos de registro puede ponerse muy grande. Para ayudar a determinar una estrategia de registro y generación de informes que resulte eficaz para su organización, considere estas preguntas:

- ¿Cuándo es más intenso el tráfico en la red?

  Considere programar los trabajos en la base de datos que utilizan muchos recursos y los trabajos de generación de informes en un horario en el que el volumen de tráfico sea menor. Esto mejora el rendimiento del registro y de la generación de informes durante los horarios de mucha actividad. Consulte *Configuración de las opciones de tiempo de navegación por Internet*, página 330, y *Configuración de las opciones de mantenimiento de la base de datos de registro*, página 331.

- ¿Durante cuánto tiempo se debe guardar la información de registro como respaldo del historial de informes?

  Considere eliminar las particiones automáticamente después de que cumplan con este período. Esto reduce la cantidad de espacio en el disco que necesita la base de datos de registro. Consulte *Configuración de las opciones de mantenimiento de la base de datos de registro*, página 331.

- ¿Qué cantidad de datos detallados en realidad necesita?

  Considere qué opciones de registro debe activar: registrar URL y accesos completos aumenta el tamaño de la base de datos de registro. Para disminuir el tamaño de la base de datos de registro, considere:

  - desactivar el registro de URL completa (consulte *Configuración de registro de URL completa*, página 329)
  - registrar visitas en lugar de accesos (consulte *Configuración de los archivos de caché de registro*, página 317)
  - activar la consolidación (consulte *Configuración de opciones de consolidación*, página 318)
  - activar registro de categorías selectivo (consulte *Configuración de Filtering Service para el registro*, página 310)

La implementación satisfactoria de la generación de informes se consigue con equipos que satisfacen o superan los requisitos de carga prevista y retención prevista de datos en el historial.

Administración del acceso a herramientas de generación de informes

Cuando Websense Manager y los componentes de generación de informes están instalados en servidores de Windows, las opciones de informes aparecen dentro de Websense Manager y la utilidad Log Server Configuration.

Cuando instala los componentes de generación de informes, Log Server se conecta a un Policy Server específico. Debe seleccionar ese Policy Server durante el inicio de sesión a Websense Manager para tener acceso a las funciones de generación de informes. Si inicia sesión en un Policy Server diferente, no podrá tener acceso a los informes de presentación o los informes de investigación en la ficha Principal, ni a la sección Informes completa en la ficha Configuración.

En las organizaciones que utilizan únicamente la cuenta de inicio de sesión de WebsenseAdministrator, toda persona que use Websense Manager tiene acceso a todas las opciones de generación de informes en Websense Manager, incluidos los informes de presentación, los informes de investigación y las configuraciones de las herramientas de generación de informes.

En las organizaciones que usan administración delegada, el acceso a las herramientas de generación de informes en Websense Manager está controlado por WebsenseAdministrator y los miembros del rol de superadministrador. Cuando crea un rol, el superadministrador indica si ese rol tiene acceso o no a las opciones de generación de informes específicas.

Consulte *Cómo modificar roles*, página 256, para obtener información sobre la configuración del acceso a las herramientas de generación de informes.

La utilidad Log Server Configuration se abre en el menú Inicio de Windows. Sólo quienes tengan acceso a la máquina de instalación pueden abrir esta utilidad y modificar la configuración de Log Server. Consulte *utilidad Log Server Configuration*, página 312.

Si su organización instaló Websense Manager en un servidor de Linux, o prefiere el programa de generación de informes Websense Explorer para Linux en lugar de los componentes de generación de informes que se ejecutan en Windows, las opciones de generación de informes no aparecen en Websense Manager. No se pueden mostrar gráficos de filtrado de Internet en las páginas Hoy e Historial. Consulte la *guía del administrador de Explorer para Linux* para obtener más información acerca de cómo instalar este programa y utilizarlo para ejecutar informes.

Configuración básica

Temas relacionados:

- *Configuración de Filtering Service para el registro*, página 310
- *Asignación de categorías a las clases de riesgo*, página 308
- *Configuración de las preferencias de informes*, página 310
- *utilidad Log Server Configuration*, página 312
- *Administración de la base de datos de registro*, página 326

Puede usar una variedad de opciones de configuración para adaptar los informes a su entorno.

La base de datos principal de Websense organiza categorías en **clases de riesgo**. Las clases de riesgo sugieren los tipos o niveles posibles de vulnerabilidad que presentan los sitios de esas categorías. Utilice la página Clases > de riesgo generales, que se abre en la ficha Configuración, para personalizar las clases de riesgo para su organización. Consulte *Asignación de categorías a las clases de riesgo*, página 308.

Utilice la página Preferencias > de informes, que se abre en la ficha Configuración, para configurar el servidor de correo electrónico que utilizará para distribuir informes, y para activar la función de informes propios. Consulte *Configuración de las preferencias de informes*, página 310.

El registro es el proceso de almacenar información acerca de las actividades de filtrado de Websense en una base de datos de registro de modo que pueda generar informes.

Utilice la página Registro > general, que se abre en la ficha Configuración, para activar el registro, seleccionar las categorías que se deben registrar y determinar qué información del usuario se registra. Consulte *Configuración de Filtering Service para el registro*, página 310, para obtener más información.

Utilice la utilidad Log Server Configuration para administrar el modo en que se procesan los registros y las conexiones a la base de datos de registro. Consulte *utilidad Log Server Configuration*, página 312, para obtener más información.

Utilice la página Base > de datos de registro de informes, que se abre en la ficha Configuración, para administrar la base de datos de registro, incluidos los controles de tiempo de navegación de Internet, las opciones de partición de la base de datos y los registros de errores. Consulte *Administración de la base de datos de registro*, página 326, para obtener más información.

Asignación de categorías a las clases de riesgo

Temas relacionados:

- *Clases de riesgo*, página 41
- *Páginas de bloqueo*, página 85
- *Uso de los informes para evaluar las políticas de filtrado*, página 95

La base de datos principal de Websense organiza categorías en **clases de riesgo**. Las clases de riesgo sugieren los tipos o niveles posibles de vulnerabilidad que presentan los sitios de esas categorías.

Las clases de riesgo se utilizan principalmente en la generación de informes. Las páginas Hoy e Historial ofrecen gráficos en los que se realiza un seguimiento de la actividad en Internet por clase de riesgo, usted puede generar informes de presentación o de investigación organizados por clase de riesgo.

Los superadministradores incondicionales pueden ver o cambiar las categorías que comprende cada clase de riesgo en la página **Clases de riesgo >** en Configuración. Por

ejemplo, algunas empresas pueden considerar que los sitios de video publicados por usuarios entran en las clases de riesgo de responsabilidad legal, pérdida de ancho de banda de red y pérdida de productividad. Sin embargo, si su compañía se dedica a investigaciones de mercado sobre ciertos grupos demográficos, debe considerarlos parte de la clase de riesgo del Uso relacionado con el trabajo.

> **Nota**
> La página de bloqueo de seguridad aparece para los sitios bloqueados en las categorías predeterminadas de clase de riesgo de Seguridad. Los cambios en las categorías en la clase de riesgo de seguridad afectan a la generación de informes, pero no inciden en las páginas de bloqueo. Consulte *Páginas de bloqueo*, página 85.

La información de clase de riesgo en los informes de Websense refleja las asignaciones que usted realiza en esta página.

1. Seleccione una entrada en la lista **Clases de riesgo**.
2. Revise la lista de **Categorías** para ver qué categorías están incluidas en esa clase de riesgo.

   Una marca de verificación indica que la categoría está asignada a la clase de riesgo seleccionada. El icono W azul indica que las categorías están incluidas en la clase de riesgo en forma predeterminada.
3. Coloque una marca o elimínela en el árbol de categorías para incluir o excluir una categoría de la clase de riesgo seleccionado. Las categorías pueden pertenecer a más de una clase de riesgo.

   Otras opciones son:

Opción	Descripción
Seleccionar todo	Selecciona todas las categorías del árbol.
Borrar todo	Quita la selección de todas las categorías del árbol.
Valores predeterminados	Restaura las categorías elegidas para la clase de riesgo seleccionada a las categorías provistas por el software de Websense. Un icono W azul indica una categoría predeterminada.

4. Repita este proceso para cada clase de riesgo.
5. Haga clic en **Aceptar** para almacenar los cambios. Los cambios no se implementan hasta que haga clic en **Guardar todo**.

Configuración de las preferencias de informes

Temas relacionados:

- *Actividad propia*, página 342
- *Programar informes de presentación*, página 110
- *Programar informes de investigación*, página 138

Cuando programa que los informes de presentación o investigación se ejecuten en un momento posterior o en un ciclo repetitivo, los informes se distribuyen por correo electrónico a destinatarios específicos. Utilice la página **Informes > Preferencias**, que se abre en la ficha Configuración, para proporcionar los datos para estos mensajes de correo electrónico.

Esta página también se utiliza para activar los informes propios, donde las personas pueden generar informes de investigación sobre su propia actividad en Internet.

1. Ingrese la **dirección de correo electrónico** que debe aparecer en el campo del remitente cuando los informes programados se distribuyen por correo electrónico.
2. Ingrese el **nombre o IP del servidor SMTP** para el servidor de correo electrónico utilizado para distribuir los informes programados por correo electrónico.
3. Marque la casilla de verificación **Permitir que los usuarios vean su propia actividad** para permitir que los usuarios finales de su organización tengan acceso a Websense Manager y ejecuten informes de investigación sobre su propia actividad en Internet. Consulte *Actividad propia*, página 342.
4. Haga clic en **Guardar ahora** para implementar los cambios.

Configuración de Filtering Service para el registro

Temas relacionados:

- *Introducción a la base de datos de registro*, página 324
- *utilidad Log Server Configuration*, página 312

Utilice la página **Registro >** en la ficha Configuración para proporcionar la dirección IP y el puerto para enviar los registros a Log Server. Esta página también le permite seleccionar qué información de usuario y categorías de URL Websense Filtering Service debe enviar a Log Server y dejar disponibles para los informes y las alertas de uso de categorías (consulte *Configuración de alertas de uso de categorías*, página 291).

En un entorno con varios Policy Servers, configure la página general Registro > en forma separada para cada uno. Todos los Filtering Services asociados con el Policy Server activo envían sus registros al Log Server identificado en esta página.

Cuando trabaje con varios Policy Servers, tenga en cuenta lo siguiente:

- Si la dirección IP y el puerto del Log Server están en blanco en cualquier Policy Server, los Filtering Services asociados a ese Policy Server no pueden registrar ningún tipo de tráfico para la presentación de informes o las alertas.
- Cada Filtering Service registra el tráfico según la configuración del Policy Server al que está conectado. Si cambia la información del usuario o las selecciones de registro de categorías para diferentes Policy Servers, los informes que se generen de los usuarios asociados a los diferentes Policy Servers pueden resultar incoherentes.

Si su entorno incluye tanto varios Policy Servers como varios Log Servers, asegúrese de iniciar sesión en cada Policy Server por separado y verifique que se está comunicando con el Log Server correcto.

1. Para registrar información de identificación en las máquinas con acceso a Internet, coloque una marca en **Registrar direcciones IP**.
2. Para registrar información de identificación para los usuarios con acceso a Internet, coloque una marca en **Registrar nombres de usuario.**

   Nota
   Si no registra las direcciones IP o los nombres de usuario, no puede haber datos de usuarios en sus informes. Esto a veces se denomina **registro anónimo**.

3. Especifique la dirección IP o el nombre de la máquina donde se instaló Log Server en el campo **Nombre o dirección IP de Log Server**.

   Importante
   Si el Log Server se instala en otra máquina desde Policy Server, esta entrada puede ser la predeterminada para el host local. Si esto sucede, ingrese la dirección IP correcta del equipo de Log Server para habilitar que se muestren los cuadros en las páginas Hoy e Historial, así como otras funciones de generación de informes.

4. Especifique el número de **Puerto** para enviar registros a Log Server.
5. Haga clic en **Comprobar estado** para determinar si Websense Manager puede comunicarse con el Log Server especificado.

   Un mensaje indica si pasó la prueba de conexión. Si es necesario, actualice la dirección IP o el nombre y puerto de la máquina hasta que el resultado de la prueba sea satisfactorio.
6. Haga clic en el botón **Registro de categorías selectivo** para abrir el área donde se debe indicar qué categorías URL registrar.

Las selecciones que haga aquí se aplican a todos los filtros de categorías en todas las políticas activas.

> **Notas**
>
> Si desactiva el registro para las categorías que tienen configuradas alertas de uso (consulte *Configuración de alertas de uso de categorías*, página 291), no se pueden enviar alertas de uso.
>
> Los informes no pueden incluir información sobre categorías que no están registradas.

a. Puede expandir o contraer las categorías principales como desee para ver las categorías que le interesan.

b. Para seleccionar cada categoría que debe registrarse, coloque una marca en la casilla de verificación correspondiente.

   Debe seleccionar o quitar la selección de cada categoría por separado. La selección de una categoría principal no se aplica automáticamente a las subcategorías que ésta comprende. Utilice **Seleccionar todo** y **Borrar todo** para facilitar la selección.

7. Haga clic en **Aceptar** para almacenar los cambios. Los cambios no se implementan hasta que haga clic en **Guardar todo**.

utilidad Log Server Configuration

Temas relacionados:

- *Administración del acceso a herramientas de generación de informes*, página 306
- *Configuración básica*, página 307
- *Cómo detener e iniciar Log Server*, página 323

Durante la instalación, usted configura ciertos aspectos de la operación de Log Server, incluido cómo el Log Server interactúa con los componentes de filtrado de Websense.

La utilidad Log Server Configuration le permite cambiar esta configuración cuando sea necesario y configurar otros detalles acerca de la operación de Log Server. Esta utilidad está instalada en la misma máquina que el Log Server.

1. En el menú Inicio de Windows, seleccione **Programas > Websense > Utilidades > Log Server Configuration**.

   Se abre la utilidad Log Server Configuration.

2. Seleccione una ficha para mostrar sus opciones y realice cualquier cambio necesario. Para obtener instrucciones detalladas, consulte:

- *Configuración de las conexiones de Log Server*, página 313
- *Configuración de las opciones de la base de datos de Log Server*, página 314
- *Configuración de los archivos de caché de registro*, página 317
- *Configuración de opciones de consolidación*, página 318
- *Configuración de WebCatcher*, página 320

3. Haga clic en **Aplicar** para guardar los cambios.
4. Utilice la ficha **Conexión** para detener y reiniciar Log Server para que los cambios surtan efecto.

IMPORTANTE

Después de hacer los cambios en cualquier ficha de Log Server Configuration, haga clic en **Aplicar**. Luego, **debe** detener y reiniciar Log Server para que los cambios surtan efecto. Para evitar reiniciar Log Server varias veces, realice todos los cambios en Log Server Configuration antes de reiniciar Log Server.

Configuración de las conexiones de Log Server

Temas relacionados:

- *utilidad Log Server Configuration*, página 312
- *Configuración de las opciones de la base de datos de Log Server*, página 314
- *Configuración de los archivos de caché de registro*, página 317
- *Configuración de opciones de consolidación*, página 318
- *Configuración de WebCatcher*, página 320
- *Cómo detener e iniciar Log Server*, página 323

La ficha **Conexión** de la utilidad Log Server Configuration contiene las opciones para crear y mantener una conexión entre Log Server y los componentes de filtrado de Websense.

1. Acepte el **puerto de entrada de Log Server** predeterminado (55805) o establezca otro puerto disponible.

   Éste es el puerto por el cual el Log Server se comunica con Filtering Service. El puerto que se especifique aquí debe coincidir con el puerto que se especificó en la página Registro > general (ficha Configuración) en Websense Manager.
2. Ingrese un número de horas como el **Intervalo de actualización de usuarios/grupos** para especificar la frecuencia con la que el Log Server debe ponerse en contacto con el servicio de directorio para actualizarse.

   Log Server se pone en contacto con el servicio de directorio para obtener información actualizada, como nombre del usuario completo y asignaciones de grupos, relacionada con los usuarios con registros en la base de datos de registro.

La actividad para un usuario cuyo grupo cambió continúa informándose con el grupo anterior hasta que se produzca la próxima actualización. Las organizaciones que actualizan su servicio de directorio con frecuencia o tienen un gran número de usuarios deben considerar actualizar la información de usuario/grupo con más frecuencia que la predeterminada de 12 horas.

3. Haga clic en **Aplicar** para guardar los cambios.
4. Utilice el botón en el área de Estado del servicio para **Iniciar** o **Detener** Log Server. La etiqueta del botón cambia para indicar la acción que se producirá cuando haga clic sobre éste.

> **Nota**
> No es posible registrar la actividad de Internet cuando Log Server está detenido.

Los cambios que se realicen en la utilidad Log Server Configuration no surten efecto hasta que detiene y reinicia Log Server.

Configuración de las opciones de la base de datos de Log Server

Temas relacionados:

- *utilidad Log Server Configuration*, página 312
- *Configuración de las conexiones de Log Server*, página 313
- *Configuración de la conexión a la base de datos*, página 316
- *Configuración de los archivos de caché de registro*, página 317
- *Configuración de opciones de consolidación*, página 318
- *Configuración de WebCatcher*, página 320
- *Cómo detener e iniciar Log Server*, página 323

Abra la ficha **Base de datos** de la utilidad Log Server Configuration para configurar cómo funciona Log Server con la base de datos de registro.

1. Elija un **Método de inserción de registro** entre las siguientes opciones.
   - Open Database Connectivity (ODBC): Inserta registros en la base de datos de a uno, mediante un controlador de base de datos para administrar la información entre Log Server y la base de datos de registro.
   - Bulk Copy Program (BCP) *(recomendado)*: Inserta registros en la base de datos de registro en grupos denominados lotes. Se recomienda esta opción porque ofrece más eficacia que la inserción de ODBC.

> **Nota**
> La opción BCP está disponible sólo si instala las herramientas del cliente SQL Server en la máquina de Log Server.

2. Haga clic en el botón **Conexión** para seleccionar la base de datos de registro para almacenar la nueva información de acceso a Internet de Websense. Consulte *Configuración de la conexión a la base de datos*, página 316.

   El Nombre del origen de datos ODBC (DSN) y el **Nombre de inicio de sesión ODBC** muestran la configuración que se estableció para la conexión a la base de datos.

3. Si elige BCP como el método de inserción de registro en el paso 1, configure las opciones siguientes. Si elige ODBC como el método de inserción de registro, omita este paso.

Opción	Descripción
Ubicación de ruta de archivos de BCP	Ruta del directorio para almacenar archivos BCP. Debe ser una ruta donde Log Server tenga acceso para leer y escribir. Esta opción está disponible sólo si se instala Log Server en la máquina de la base de datos de registro, o si las herramientas del cliente SQL Server están instaladas en la máquina de Log Server.
Frecuencia de creación de archivos de BCP	Cantidad máxima de minutos que el Log Server pasa colocando registros en un archivo de lote antes de cerrar ese archivo de lote y crear uno nuevo. Esta configuración trabaja en combinación con la configuración del tamaño de lote: Log Server crea un nuevo archivo de lote tan pronto como se llega a uno de los límites.
Tamaño máximo de lote de BCP	Cantidad máxima de registros antes de que se cree un nuevo archivo de lote. Esta configuración trabaja en combinación con la configuración de la frecuencia de creación: Log Server crea un nuevo archivo de lote tan pronto como se llega a uno de los límites.

4. Configure las **Máximas conexiones permitidas** para indicar cuántas conexiones internas pueden hacerse entre Log Server y el motor de base de datos. Las opciones disponibles dependen del motor de base de datos que se utilice.
   - **MSDE**: Este valor está predeterminado en 4 y no puede modificarse.
   - **SQL Server**: Configure en un valor de 4 a 50, según corresponda para su licencia de SQL Server. La cantidad mínima de conexiones depende del método de inserción de registro seleccionado.

   Nota

   El hecho de aumentar el número de conexiones puede incrementar la velocidad de procesamiento de los registros, pero podría incidir en otros procesos de la red que utilizan el mismo SQL Server. En la mayoría de los casos, debe configurar el número de conexiones en un valor menor de 20. Comuníquese con el administrador de su base de datos para solicitar ayuda.

5. Marque o desmarque la opción **Registro avanzado** para activarla o desactivarla, esta opción controla el modo en que Log Server reanuda el registro después de una detención.

   Cuando esta opción está desactivada (como en la configuración predeterminada), Log Server inicia el procesamiento al comienzo del archivo de caché de registro más antiguo después de una detención. Esto podría generar entradas duplicadas en la base de datos de registro, pero agiliza el procesamiento de Log Server.

   Cuando esta opción está activada, Log Server realiza un seguimiento de su ubicación en el archivo de caché de registro activo. Después de reiniciar, Log Server reanuda el procesamiento adonde se detuvo. El registro avanzado puede ocasionar demoras en el procesamiento de Log Server.
6. Haga clic en **Aplicar** para guardar los cambios, luego detenga y reinicie Log Server (consulte *Cómo detener e iniciar Log Server*, página 323).

Configuración de la conexión a la base de datos

Temas relacionados:

- *Configuración de las conexiones de Log Server*, página 313
- *Configuración de las opciones de la base de datos de Log Server*, página 314

El botón **Conexión** en la ficha Base de datos de la utilidad Log Server Configuration le permite seleccionar la base de datos de registro para almacenar la información de acceso a Internet entrante desde Websense. Se configura automáticamente durante la instalación, pero puede modificarse siempre que lo necesite para cambiar la base de datos para su registro. (La base de datos ya debe existir antes de establecer una conexión.)

1. En el cuadro de diálogo Origen de datos, seleccione la ficha **Origen de datos de máquina**.
2. Seleccione la conexión ODBC para la base de datos donde se registrará la información nueva.
3. Haga clic en **Aceptar** para mostrar el cuadro de diálogo Inicio de sesión de SQL.
4. Si la opción **Utilizar conexión de confianza** está disponible, asegúrese de que esté configurada correctamente según el entorno.

   Usuarios de MSDE: Desmarque la opción Conexión de confianza.

   Usuarios de SQL Server: Comuníquese con el administrador de su base de datos para solicitar ayuda.

   Nota

   Si usa una conexión de confianza para las comunicaciones con SQL Server, puede necesitar configurar varios servicios Websense con el nombre y la contraseña del usuario de confianza. Para obtener más detalles, consulte la *guía de instalación* de Websense.

5. Ingrese el **ID** y la **contraseña de inicio de sesión** especificados durante la creación de la base de datos. Normalmente es el mismo ID y la misma contraseña que ingresó durante la instalación de Log Server y la creación de la base de datos.
6. Después de este paso y de cualquier otro cambio en la utilidad Log Server Configuration, detenga y reinicie Log Server mediante la ficha **Conexión**.

Configuración de los archivos de caché de registro

Temas relacionados:

- *utilidad Log Server Configuration*, página 312
- *Configuración de las conexiones de Log Server*, página 313
- *Configuración de las opciones de la base de datos de Log Server*, página 314
- *Configuración de opciones de consolidación*, página 318
- *Configuración de WebCatcher*, página 320
- *Cómo detener e iniciar Log Server*, página 323

La ficha **Configuración** de la utilidad Log Server Configuration le permite administrar las opciones de creación de archivo de caché de registro, y especificar si Log Server realiza un seguimiento de los archivos individuales que conforman cada sitio Web solicitado o únicamente del sitio Web.

1. Especifique la ruta para guardar archivos de caché de registro en el campo **Ubicación de ruta de archivo de registro**. La ruta predeterminada es **<directorio de instalación>\bin\Cache**. (El directorio de instalación predeterminado es C:\Archivos de Programa\Websense\).
2. Para la **frecuencia de creación de archivo de caché**, indique la cantidad máxima de minutos que el Log Server debe dedicar al envío de información de acceso a Internet a un archivo de caché de registro (**log*n*.tmp**) antes de cerrarlo y crear un archivo nuevo.

   Esta configuración trabaja en combinación con la configuración del tamaño: Log Server crea un nuevo archivo de caché de registro tan pronto como se llega a uno de los límites.
3. Para el **tamaño de creación de archivo de caché**, especifique el tamaño que debe tener un archivo de caché de registro antes de que el Log Server lo cierre y cree un archivo nuevo.

   Esta configuración trabaja en combinación con la configuración de la frecuencia de creación: Log Server crea un nuevo archivo de caché de registro tan pronto como se llega a uno de los límites.

4. Marque **Activar visitas** para crear un registro por cada sitio Web visitado.

   Nota
   Administrar el tamaño de la base de datos de registro es una preocupación importante en las redes con un volumen alto. Habilitar el registro de las visitas es una manera de controlar el tamaño y el crecimiento de la base de datos.

   Cuando esta opción está desactivada, se crea un registro separado para cada solicitud HTTP generado para mostrar los diferentes elementos de la página, como gráficos y anuncios. También denominada accesos de registro, esta opción crea una base de datos de registro de mayor tamaño que crece rápidamente.

   Cuando está opción está activada, Log Server combina los elementos individuales que crean la página Web (como gráficos y anuncios) en un único registro.

   Si instaló Websense Web Security Gateway, la actividad de exploración en tiempo real siempre se informa en accesos a los informes que son específicos a la exploración en tiempo real, incluso cuando está activado el registro de las visitas. En esta situación, los números que se muestran en los informes de filtrado Web que incluyen tráfico bloqueado por exploración en tiempo real serán menores que los números que se muestran en los informes de exploración en tiempo real.

   Nota
   Es mejor crear una nueva partición de la base de datos antes de cambiar el método de registro entre las visitas y los accesos. Consulte la página Base de > datos de registro de informes (ficha Configuración) en Websense Manager para crear una nueva partición de la base de datos.

5. Haga clic en **Aplicar** para guardar los cambios, luego detenga y reinicie Log Server (consulte *Cómo detener e iniciar Log Server*, página 323).

Configuración de opciones de consolidación

Temas relacionados:

- *utilidad Log Server Configuration*, página 312
- *Configuración de las conexiones de Log Server*, página 313
- *Configuración de las opciones de la base de datos de Log Server*, página 314
- *Configuración de los archivos de caché de registro*, página 317
- *Configuración de WebCatcher*, página 320
- *Cómo detener e iniciar Log Server*, página 323

Utilice la ficha **Consolidación** de la utilidad Log Server Configuration para activar la consolidación y establecer las preferencias de consolidación.

> **Nota**
> Administrar el tamaño de la base de datos de registro es una preocupación importante en las redes con un volumen alto. Habilitar la consolidación es una manera de controlar el tamaño y el crecimiento de la base de datos.

La consolidación disminuye el tamaño de su base de datos de registro al combinar las solicitudes de Internet que comparten los siguientes elementos:

- Nombre de dominio (por ejemplo: www.websense.com)
- Categoría
- Palabra clave
- Acción (por ejemplo: Categoría bloqueada)
- Usuario/estación de trabajo

Los informes se ejecutan más rápidamente cuando la base de datos de registro es más pequeña. Sin embargo, consolidar los datos de registro puede disminuir la exactitud de algunos informes detallados, dado que se pueden perder registros separados para el mismo nombre de dominio.

> **Importante**
> Si se habilita la consolidación, se puede desvirtuar la exactitud de algunos datos del informe, como los cálculos del tiempo de navegación por Internet.

1. Marque **Consolidar registros** para activar la consolidación, que combina varias solicitudes a Internet similares en un único registro.

   Cuando esta opción no está marcada, como en la configuración predeterminada, la base de datos de registro conserva accesos completos o detalles de visitas para cada solicitud de Internet (según su selección en la ficha Configuraciones, consulte *Configuración de los archivos de caché de registro*, página 317). Esto ofrece un mayor detalle en los informes, pero también genera una base de datos de registro más grande.

   Si se selecciona esta opción, se crea una base de datos más pequeña con informes menos detallados.

   > **Importante**
   > Para garantizar la coherencia entre los informes, considere crear una nueva partición de la base de datos cada vez que active o desactive la consolidación. Además, recuerde generar informes de las particiones con la misma configuración de consolidación.

Si instaló Websense Web Security Gateway, la actividad de exploración en tiempo real siempre se informa en accesos individuales a los informes que son específicos a la exploración en tiempo real, incluso cuando está activada la consolidación. En esta situación, los números que se muestran en los informes de filtrado Web que incluyen tráfico bloqueado por exploración en tiempo real serán menores que los números que se muestran en los informes de exploración en tiempo real.

2. Para el **Intervalo de tiempo de consolidación**, especifique el tiempo máximo entre el primer y el último registro que se van a combinar.

   Esto representa la mayor diferencia de tiempo entre el primer y el último registro combinados para hacer un registro de consolidación.

   Disminuya el intervalo para incrementar la granularidad de los informes. Incremente el intervalo para maximizar la consolidación. Tenga en cuenta que un intervalo mayor también puede incrementar el uso de los recursos del sistema, como la memoria, CPU y espacio de disco.

   Si habilitó la opción URL completa en la página Base > de datos de registro de informes (ficha Configuración) en Websense Manager, el registro consolidado contendrá la ruta completa (hasta 255 caracteres) del primer sitio coincidente con que se encuentre Log Server.

   Por ejemplo, suponga que un usuario visitó los siguientes sitios y todos corresponden a la categoría sitios de compras.

   - www.domain.com/shoeshopping
   - www.domain.com/purseshopping
   - www.domain.com/jewelryshopping

   Con la URL completa activada, la consolidación podría crear una única entrada de registro bajo la URL www.domain.com/shoeshopping.

3. Haga clic en **Aplicar** para guardar los cambios, luego detenga y reinicie Log Server (consulte *Cómo detener e iniciar Log Server*, página 323).

Configuración de WebCatcher

Temas relacionados:

- *utilidad Log Server Configuration*, página 312
- *Configuración de las conexiones de Log Server*, página 313
- *Configuración de las opciones de la base de datos de Log Server*, página 314
- *Configuración de los archivos de caché de registro*, página 317
- *Configuración de opciones de consolidación*, página 318
- *Configuración de WebCatcher*, página 320
- *Autenticación de WebCatcher*, página 322
- *Cómo detener e iniciar Log Server*, página 323

WebCatcher es una función opcional que recopila URL no reconocidas y URL de seguridad y las envía a Websense, Inc., donde se analizan para su categorización y en busca de riesgos de seguridad y responsabilidad. (No se requiere un registro de URL completa para el procesamiento de WebCatcher.) Websense, Inc. analiza la información y actualiza la base de datos principal con las URL recientemente categorizadas, lo que deriva en un mejor filtrado.

Elija los tipos de URL que va a enviar y configure el tamaño de archivo y el tiempo de procesamiento en la ficha **WebCatcher** de la utilidad Log Server Configuration.

> **Nota**
> En un entorno con varios Log Servers, WebCatcher se activa para un Log Server únicamente. Una vez que se ha activado, esta ficha no está disponible cuando se ejecute la herramienta Log Server Configuration para otras instancias de Log Server.

La información enviada a Websense, Inc., contiene únicamente URL y no incluye la información de usuarios.

En el siguiente ejemplo se ilustra la información que se enviaría si usted activara WebCatcher. La dirección IP de este ejemplo refleja la dirección de la máquina host de la URL, no la dirección IP de quien realiza la solicitud.

```
<URL HREF="http://www.ack.com/uncategorized/" CATEGORY="153"
IP_ADDR="200.102.53.105" NUM_HITS="1" />
```

Los datos de WebCatcher se envían a Websense, Inc. a través de HTTP Post. Es posible que deba crear roles o realizar otros cambios en su servidor proxy o firewall para permitir el tráfico saliente de HTTP. Consulte el servidor proxy o documentación de firewall para ver las instrucciones.

1. Seleccione una de las siguientes opciones:
   - **Sí, enviar sólo las URL especificadas a Websense** activa el procesamiento de WebCatcher. Debe indicar qué URL se deben enviar. Continúe con el paso 2.
   - **No, no enviar información a Websense** desactiva el procesamiento de WebCatcher. No se deben realizar más entradas si elige esta opción.
2. Marque **Enviar URL sin categorizar** para enviar una lista de todas las URL sin categorizar que se encuentran en su base de datos de registro.

   Websense, Inc. analiza las URL sin categorizar que recibe y las agrega a las categorías de la base de datos principal, según corresponda. Esto mejora la precisión del filtrado en todas las organizaciones.

   > **Nota**
   > Los sitios de intranet no se envían por WebCatcher. Esto incluye todos los sitios con direcciones IP de los rangos 10.xxx.xxx.xxx, 172.16.xxx.xxx y 192.168.xxx.xxx.

3. Marque **Enviar URL de seguridad** para enviar una lista de las URL de seguridad que se encuentran en su base de datos de registro.

   Las URL de seguridad recibidas y analizadas por Websense, Inc. para determinar la actividad de las categorías keyloggers, sitios Web maliciosos, phishing y otros fraudes, y Spyware.

4. En **Seleccione el país o la región que mejor refleje su ubicación**, seleccione el país donde se registra la mayor parte de la actividad.
5. Marque la opción **Guardar una copia de los datos enviados a Websense** para guardar una copia de los datos que se envían a Websense, Inc.

   Cuando esta opción está habilitada, WebCatcher guarda los datos como archivos XML no cifrados en el directorio Websense\Reporter. Estos archivos contienen una marca de fecha y tiempo.

6. En **Máximo tamaño de archivo a transferir**, indique qué tamaño puede alcanzar el archivo (de 4096 KB a 8192 KB) antes de enviarlo a Websense.

   Asegúrese de que el sistema pueda publicar un archivo de este tamaño por HTTP Post.

7. Para **Hora de inicio diaria (mínimo)**, configure la hora de inicio para que WebCatcher envíe el archivo si el umbral de tamaño no se alcanzó ese día.

   Esto garantiza que la información se envíe y se borre de su sistema al menos una vez al día.

8. Haga clic en el botón **Autenticación** si la máquina de Log Server debe autenticarse para acceder a Internet.

   Consulte *Autenticación de WebCatcher*, página 322, para obtener información acerca de el cuadro de diálogo **Autenticación** que aparece.

9. Haga clic en **Aplicar** para guardar los cambios, luego detenga y reinicie Log Server (consulte *Cómo detener e iniciar Log Server*, página 323).

Autenticación de WebCatcher

Temas relacionados:

- *utilidad Log Server Configuration*, página 312
- *Configuración de WebCatcher*, página 320
- *Cómo detener e iniciar Log Server*, página 323

Al hacer clic en Autenticación de la ficha WebCatcher, se muestra el cuadro de diálogo **Autenticación**.

1. Marque la opción **Usar servidor proxy** si la máquina de Log Server abre Internet a través de un servidor proxy, y luego proporcione la información requerida.

Campo	Descripción
Nombre de servidor proxy	Especifique la dirección IP o el nombre de la máquina del servidor proxy que utiliza Log Server para acceder a Internet.
Puerto de servidor proxy	Especifique el número de puerto a través del cual se comunica el servidor proxy.

2. Marque la opción **Usar autenticación básica** si la máquina de Log Server debe autenticarse para acceder a Internet, y luego escriba el nombre de usuario y la contraseña para autenticación.
3. Haga clic en **Aceptar** para guardar los cambios y volver a la ficha de WebCatcher.

Cómo detener e iniciar Log Server

Temas relacionados:

- *utilidad Log Server Configuration*, página 312
- *Configuración de las conexiones de Log Server*, página 313

Log Server recibe información de Filtering Service y la almacena en la base de datos de registro para luego utilizarla en la generación de informes. Se ejecuta como servicio de Windows, por lo general se inicia durante la instalación, y se inicia cada vez que usted reinicia la máquina.

Los cambios que haga en la utilidad Log Server Configuration surten efecto únicamente después de detener y reiniciar Log Server. Esto puede hacerse fácilmente en la ficha Conexión en la utilidad Log Server Configuration.

1. En el menú de Inicio de Windows, seleccione **Programas > Websense > Utilidades > Log Server Configuration**.
2. En la ficha **Conexiones**, haga clic en **Detener**.
3. Espere unos segundos y luego haga clic en **Iniciar** para reiniciar el servicio de Log Server.
4. Haga clic en **Aceptar** para cerrar la utilidad Log Server Configuration.

Nota

Websense no puede registrar el acceso a Internet que se produce mientras Log Server se encuentra detenido.

Introducción a la base de datos de registro

Temas relacionados:

- *Trabajos en la base de datos*, página 325
- *Administración de la base de datos de registro*, página 326

La base de datos de registro almacena los registros de la actividad de Internet y las acciones de filtrado de Websense asociadas. La instalación crea la base de datos de registro con una base de datos de catálogo y una partición de la base de datos.

La **base de datos de catálogo** proporciona un único punto de conexión para los diferentes componentes de Websense que necesitan acceder a la base de datos de registro: páginas de Estado, Log Server, informes de presentación e informes de investigación. Contiene información de soporte para las particiones de la base de datos, que incluye la lista de nombres de categorías, definiciones de clases de riesgo, la asignación de usuarios a grupos, los trabajos en la base de datos, etc. La base de datos del catálogo también lleva una lista de todas las particiones de la base de datos disponibles.

Las particiones de la base de datos se almacenan en registros individuales para la actividad en Internet. Para usuarios de MSDE, se crean nuevas particiones según las reglas de reinicio de datos por tamaño establecidas por el software de Websense. Los usuarios de Microsoft SQL Server pueden configurar la base de datos de registro para iniciar una nueva partición según el tamaño de la partición o un intervalo de fecha (consulte *Configuración de opciones de reinicio de datos*, página 327, para obtener más información).

Nota

Las particiones por fecha están disponibles únicamente cuando el software de Websense utiliza Microsoft SQL Server como el motor de base de datos.

Cuando las particiones se basan en el tamaño, todos los registros entrantes se insertan en la partición activa más reciente que cumple con la regla de tamaño. Cuando la partición alcanza el tamaño máximo designado, se crea una nueva partición para insertar nuevos registros.

Cuando las particiones se basan en la fecha, se crean nuevas particiones según el ciclo establecido. Por ejemplo, si la opción de reinicio de datos es mensual, se crea una nueva partición tan pronto se reciban registros para el nuevo mes. Los registros entrantes se insertan en la partición correspondiente según la fecha.

Las particiones de la base de datos brindan ventajas de flexibilidad y rendimiento. Por ejemplo, puede generar informes de una única partición para limitar el alcance de datos que deben analizarse para localizar la información solicitada.

Trabajos en la base de datos

Los siguientes trabajos en la base de datos se instalan junto con la base de datos de registro. El SQL Server Agent debe estar ejecutándose en la máquina donde se ejecuta el motor de base de datos (MSDE o Microsoft SQL Server).

- El trabajo Extraer, transformar y cargar (ETL) se ejecuta continuamente, recibiendo datos del Log Server, procesándolos y luego insertándolos en la base de datos de partición. El trabajo ETL debe estar ejecutándose para procesar los registros en la base de datos de registro.
- El trabajo de mantenimiento de la base de datos realiza tareas de mantenimiento de la base de datos y conserva el rendimiento óptimo. Este trabajo se ejecuta, en forma predeterminada, todas las noches.
- El trabajo de cálculo de Tiempo de navegación por Internet analiza los datos recibidos y calcula el tiempo de navegación para cada cliente. El trabajo de la base de datos de tiempo de navegación por Internet utiliza gran cantidad de recursos, afecta a la mayoría de los recursos de la base de datos. Este trabajo se ejecuta, en forma predeterminada, todas las noches.

Ciertos aspectos de estos trabajos en la base de datos pueden configurarse en la página Configuración de la > base de datos de registro. Consulte *Configuración de administración de la base de datos de registro.*, página 326, para obtener más información.

Cuando configure la hora de inicio para el trabajo de mantenimiento y el trabajo Tiempo de navegación por Internet, considere los recursos del sistema y el tráfico de la red. Estos trabajos utilizan muchos recursos y pueden ocasionar demoras en el rendimiento del registro y de la generación de informes.

Administración de la base de datos de registro

Temas relacionados:

- *Configuración de administración de la base de datos de registro.*, página 326
- *Configuración de opciones de reinicio de datos*, página 327
- *Configuración de las opciones de tiempo de navegación por Internet*, página 330
- *Configuración de registro de URL completa*, página 329
- *Configuración de las opciones de mantenimiento de la base de datos de registro*, página 331
- *Configuración de la creación de particiones en la base de datos de registro*, página 333
- *Configuración de las particiones disponibles*, página 335
- *Cómo visualizar los registros de errores*, página 336

La administración de la base de datos de registro implica el control de numerosos aspectos de las operaciones de la base de datos, entre ellos:

- Qué operaciones realizan los trabajos en la base de datos y cuándo se ejecutan.
- Las condiciones para crear nuevas particiones en la base de datos.
- Qué particiones están disponibles para la generación de informes.

Éstas y otras opciones le brindan un control significativo a la persona que administra la base de datos de registro. Consulte *Configuración de administración de la base de datos de registro.*, página 326.

El superadministrador designa quién puede administrar la base de datos de registro cuando crea los roles. Consulte *Cómo modificar roles*, página 256.

Nota

Es aconsejable limitar el número de administradores con permiso para cambiar la configuración de la base de datos de registro.

Configuración de administración de la base de datos de registro.

Temas relacionados:

- *Administración de la base de datos de registro*, página 326

La página **Base de datos > de registro de informes**, que se abre desde la ficha Configuración, le permite administrar diferentes aspectos de las operaciones de la base de datos de registro. Las opciones están agrupadas en secciones lógicas que se describen por separado.

Debe hacer clic en el botón Guardar ahora en una sección para activar los cambios correspondientes a esa sección. Si hace clic en **Guardar ahora**, los cambios en esa sección se registran inmediatamente. (No es necesario hacer clic también en Guardar todo.)

La parte superior de la página muestra el nombre de la base de datos de registro activa y un enlace para **Actualizar**. Este enlace Actualizar muestra nuevamente la información que se encuentra actualmente en la página de la base de datos de registro. Se perderá cualquier cambio que no se haya aplicado con el botón Guardar ahora correspondiente.

Para obtener instrucciones detalladas sobre cómo usar cada sección, haga clic en el enlace correspondiente de abajo.

- Opciones de reinicio de datos de la base de datos *Configuración de opciones de reinicio de datos*, página 327.
- Registro de URL completa *Configuración de registro de URL completa*, página 329.
- Configuración del tiempo de navegación por Internet: *Configuración de las opciones de tiempo de navegación por Internet*, página 330.
- Configuración de mantenimiento: *Configuración de las opciones de mantenimiento de la base de datos de registro*, página 331.
- Creación de partición de base de datos: *Configuración de la creación de particiones en la base de datos de registro*, página 333.
- Particiones disponibles: *Configuración de las particiones disponibles*, página 335.
- Actividad de registro de errores: *Cómo visualizar los registros de errores*, página 336.

Configuración de opciones de reinicio de datos

Temas relacionados:

- *Configuración de administración de la base de datos de registro.*, página 326
- *Configuración de las opciones de tiempo de navegación por Internet*, página 330
- *Configuración de registro de URL completa*, página 329
- *Configuración de las opciones de mantenimiento de la base de datos de registro*, página 331
- *Configuración de la creación de particiones en la base de datos de registro*, página 333
- *Configuración de las particiones disponibles*, página 335
- *Cómo visualizar los registros de errores*, página 336

Utilice la sección **Opciones de reinicio de datos de la base de datos** de la página Base de datos de registro de > informes (ficha Configuración) para especificar cuándo desea que la Base de datos de registro cree una nueva partición de la base de datos (reinicio de datos).

1. Utilice las opciones de **Reinicio de datos cada** para indicar si las particiones de la base de datos deben reiniciarse según el tamaño (MB) o la fecha (semanas o meses), según el motor de la base de datos que se utilice.

   Los usuarios de MSDE deben usar la opción de reinicio de datos por tamaño. Los usuarios de Microsoft SQL Server pueden elegir entre tamaño o fecha.

   - Para reinicios de datos por fecha, seleccione **semanas** o **meses** como unidad de medida y especifique cuántas semanas o meses calendario completos se deben mantener en una partición de base de datos antes de crear una nueva.
   - Para reinicios de datos por tamaño, seleccione **MB** y especifique la cantidad de megabytes que debe alcanzar la base de datos para que comience el reinicio de datos.

     Los usuarios de Microsoft SQL Server pueden configurar un tamaño de hasta 204800 MB.

     Los usuarios de MSDE pueden configurar un tamaño entre 100 MB y 1536 MB.

     Nota

     Si el reinicio de datos comienza durante un horario del día con mucha actividad, el rendimiento durante el proceso de reinicio de datos puede ser bajo.

     Para evitar que esto suceda, algunos entornos utilizan configurar el reinicio de datos automático a un período extenso o un tamaño máximo. Luego, realizan reinicios de datos manuales periódicos para impedir que se produzca un reinicio de datos automático. Consulte *Configuración de la creación de particiones en la base de datos de registro*, página 333, para obtener información sobre reinicios manuales.

     Recuerde que no se recomiendan las particiones individuales extremadamente grandes. El rendimiento del reinicio de datos puede ser lento si los datos no están divididos en varias particiones más pequeñas.

   Cuando se crea una nueva partición de la base de datos, automáticamente se activa el reinicio de datos para esa partición (consulte *Configuración de las particiones disponibles*, página 335).

2. Haga clic en **Guardar ahora** para activar los cambios en las opciones de reinicio de datos en la base de datos.

Configuración de registro de URL completa

Temas relacionados:

- *Configuración de administración de la base de datos de registro.*, página 326
- *Configuración de opciones de reinicio de datos*, página 327
- *Configuración de las opciones de tiempo de navegación por Internet*, página 330
- *Configuración de las opciones de mantenimiento de la base de datos de registro*, página 331
- *Configuración de la creación de particiones en la base de datos de registro*, página 333
- *Configuración de las particiones disponibles*, página 335
- *Cómo visualizar los registros de errores*, página 336

La sección **Registro de URL completa** de la página > Base de datos de registro de informes (ficha Configuración) le permite decidir qué porción de la URL se registra para cada solicitud de Internet.

Nota

Administrar el tamaño de la base de datos de registro es una preocupación importante en las redes con un volumen alto. Deshabilitar la opción de registro de URL completa es una manera de controlar el tamaño y el crecimiento de la base de datos.

1. Marque **Registrar la URL completa de cada sitio solicitado** para registrar la URL completa, incluido el dominio (www.domain.com) y la ruta a la página en particular (/products/productA.html).

   Importante

   Habilite el registro de URL completa si planea generar informes de actividad de escaneo en tiempo real (consulte *Informes sobre la actividad de exploración en tiempo real*, página 153). De lo contrario, los informes pueden mostrar sólo el dominio (www.domain.com) del sitio categorizado, aun cuando las páginas individuales dentro del sitio puedan ser de categorías diferentes o contener amenazas diferentes.

   Si esta opción no está marcada, sólo se registran los nombres de los dominios. Esta opción da como resultado una base de datos más pequeña, pero proporciona menos detalle.

Registrar URL completas genera una base de datos de registro más grande, pero a cambio ofrece un mayor detalle.

Si activa el registro de URL completas cuando está activada la consolidación, el registro consolidado contiene la URL completa del primer registro en el grupo de consolidación. Consulte *Configuración de opciones de consolidación*, página 318, para obtener más información.

2. Haga clic en **Guardar ahora** para activar los cambios en las opciones de registro de URL completas.

Configuración de las opciones de tiempo de navegación por Internet

Temas relacionados:

- *Configuración de administración de la base de datos de registro.*, página 326
- *Configuración de opciones de reinicio de datos*, página 327
- *Configuración de registro de URL completa*, página 329
- *Configuración de las opciones de mantenimiento de la base de datos de registro*, página 331
- *Configuración de la creación de particiones en la base de datos de registro*, página 333
- *Configuración de las particiones disponibles*, página 335
- *Cómo visualizar los registros de errores*, página 336

Los informes del tiempo de navegación por Internet brindan una visión de la cantidad de tiempo que los usuarios pasan en Internet. Un trabajo de la base de datos que se ejecuta todas las noches calcula el tiempo de navegación para cada cliente sobre la base de los registros nuevos que se recibieron ese día. Consulte las opciones de tiempo de navegación en la sección **Configuración del tiempo de navegación por Internet** en la página Configuración > de la base de datos de registro.

1. Elija un **Hora de inicio de trabajo** para el trabajo en la base de datos de tiempo de navegación por Internet.

   Los recursos de tiempo y sistema requeridos por este trabajo varían según el volumen de datos registrados cada día. Es conveniente ejecutar este trabajo en otro momento diferente que el trabajo de mantenimiento nocturno (consulte *Configuración de las opciones de mantenimiento de la base de datos de registro*, página 331) y seleccionar un tiempo con menor actividad en la red para minimizar cualquier impacto en la generación de informes.

   El trabajo de la base de datos de tiempo de navegación por Internet utiliza gran cantidad de recursos, afecta a la mayoría de los recursos de la base de datos. Si activa este trabajo, configure un tiempo de inicio de manera que no intervenga con la capacidad del sistema de la base de datos de procesar informes programados y

otras operaciones importantes. Además, supervise el trabajo para determinar si necesita un hardware más robusto con capacidad para todas las necesidades de procesamiento.

2. Para el umbral de tiempo de **Lectura**, configure una cantidad promedio de minutos para leer un sitio Web específico.

   Este umbral de tiempo de lectura define las sesiones de navegación con el fin de generar informes de tiempo de navegación por Internet. Cuando se abre un navegador se genera tráfico HTTP. Esto representa el comienzo de una sesión de navegación. La sesión está abierta siempre que se siga generando continuamente tráfico HTTP dentro del tiempo que se establece aquí. La sesión de navegación se considera cerrada una vez que se cumple este período sin tráfico HTTP. Una nueva sesión de navegación comienza tan pronto como se genere tráfico HTTP nuevamente.

   Nota

   Es mejor cambiar el Umbral de tiempo de lectura con la menor frecuencia posible y comenzar una nueva partición de la base de datos siempre que realice un cambio.

   Para evitar la falta de coherencia de datos en los informes, genere informes de cálculo de tiempo de navegación por Internet a partir de particiones de base de datos que utilicen el mismo valor para el Umbral de tiempo de lectura.

   Tenga en cuenta que algunos sitios Web usan una técnica de actualización automática para actualizar la información con frecuencia. Un ejemplo es un sitio de noticias que muestra una pantalla que va cambiando con las últimas noticias. Esta actualización genera nuevo tráfico HTTP. Por lo tanto, cuando se deja abierto este tipo de sitios, se generan nuevos registros cada vez que el sitio se actualiza. No hay intervalo en el tráfico HTTP, de modo que la sesión de navegación no está cerrada.

3. Configure un valor **Último tiempo de lectura** para que represente el tiempo de lectura del último sitio Web antes del final de una sesión de navegación.

   Cuando el intervalo de tiempo de tráfico HTTP es mayor que el umbral de tiempo de lectura, la sesión finaliza y el valor del Último tiempo de lectura se agrega al tiempo de la sesión.

4. Haga clic en **Guardar ahora** para activar los cambios en la configuración del tiempo de navegación de Internet.

Configuración de las opciones de mantenimiento de la base de datos

de registro

Temas relacionados:

- *Configuración de administración de la base de datos de registro.*, página 326
- *Configuración de opciones de reinicio de datos*, página 327
- *Configuración de las opciones de tiempo de navegación por Internet*, página 330
- *Configuración de registro de URL completa*, página 329
- *Configuración de la creación de particiones en la base de datos de registro*, página 333
- *Configuración de las particiones disponibles*, página 335
- *Cómo visualizar los registros de errores*, página 336

Utilice la sección **Configuración de mantenimiento** de la página Base de datos de registro > de informes (ficha Configuración) para controlar ciertos aspectos del procesamiento de la base de datos, como el tiempo para ejecutar el trabajo de mantenimiento de la base de datos, algunas de las tareas que realiza este trabajo, y borrar particiones de base de datos y registros de errores.

1. Para **Hora de inicio de mantenimiento**, seleccione la hora del día para ejecutar el trabajo de mantenimiento de la base de datos.

   Los recursos de tiempo y sistema requeridos por este trabajo varían según las tareas que seleccione en esta área. Para minimizar cualquier impacto en otras actividades y sistemas, es mejor ejecutar este trabajo durante un horario con poca actividad en la red, que no sea el horario establecido para el trabajo del Tiempo de navegación por Internet (consulte *Configuración de las opciones de tiempo de navegación por Internet*, página 330).

2. Marque **Eliminar particiones automáticamente** y luego especifique el número de días (de 2 a 365) después del cual deben borrarse las particiones.

   Advertencia

   Después de que una partición se eliminó, los datos no pueden recuperarse. Consulte *Configuración de las particiones disponibles*, página 335, para ver una manera alternativa de eliminar particiones.

3. Marque **Activar la reindexación automática** y luego seleccione un día de la semana para que este proceso se ejecute automáticamente todas las semanas.

Reindexar la base de datos de registro es importante para mantener la integridad de la base de datos y optimizar la velocidad de generación de informes.

Importante

Es mejor realizar este proceso durante un horario tranquilo en la red. La reindexación de particiones de la base de datos es un trabajo que consume tiempo y utiliza muchos recursos. No se deben ejecutar informes durante el proceso.

4. Marque **Número de días antes de eliminar los lotes con errores** y luego especifique una cantidad de días (de 0 a 90) después de la cual se borrarán los lotes con errores.

   Si esta opción no está marcada, los lotes con errores se conservan por tiempo indefinido para procesos futuros.

   Si hay espacio insuficiente en disco o permisos de base de datos inadecuados para insertar registros en la base de datos, los registros se marcan como un **lote con errores**. Por lo general, estos lotes se reprocesan satisfactoriamente y se insertan en la base de datos durante el trabajo de mantenimiento de la base de datos nocturno.

   Sin embargo, este reprocesamiento no puede ser satisfactorio si el problema de espacio en disco o del permiso no se ha resuelto. Además, si no está seleccionado **Procesar los lotes sin procesar**, los lotes con errores nunca se reprocesan. Se eliminan después del tiempo especificado aquí.

5. Marque **Procesar los lotes sin procesar** para que el trabajo de mantenimiento de la base de datos nocturno reprocese los lotes con errores.

   Si esta opción no está marcada, los lotes con errores no se reprocesarán nunca. Se eliminan después del tiempo especificado más arriba, si corresponde.

6. Marque **Número de días antes de eliminar el registro de errores y** luego especifique una cantidad de días (de 0 a 90) después de la cual se borrarán los registros de errores de la base de datos de la base de datos de catálogo.

   Si esta opción no está marcada, los registros de errores se guardan por tiempo indefinido.

7. Haga clic en **Guardar ahora** para activar los cambios en las opciones de la configuración de mantenimiento.

Configuración de la creación de particiones en la base de datos de

registro

Temas relacionados:

- *Configuración de administración de la base de datos de registro.*, página 326
- *Configuración de opciones de reinicio de datos*, página 327
- *Configuración de las opciones de tiempo de navegación por Internet*, página 330
- *Configuración de registro de URL completa*, página 329
- *Configuración de las opciones de mantenimiento de la base de datos de registro*, página 331
- *Configuración de las particiones disponibles*, página 335
- *Cómo visualizar los registros de errores*, página 336

Utilice la sección **Creación de partición de base de datos** en la página Base de datos de registro > de informes (ficha Configuración) para definir las características de las nuevas particiones en la base de datos, como opciones de ubicación y tamaño. Esta área también le permite crear una nueva partición inmediatamente, antes de esperar el reinicio de datos programado (consulte *Configuración de opciones de reinicio de datos*, página 327).

1. Especifique la **Ruta de archivo** para crear los archivos **Datos** y **Registro** para nuevas particiones de la base de datos.
2. En **Tamaño inicial** configure el tamaño de archivo inicial (de 100 a 204800 MB) de los archivos **Datos** y **Registro** para las nuevas particiones en la base de datos.

   Usuarios de Microsoft SQL Server: El rango aceptable es de 100 a 204800

   Usuarios de MSDE: El rango aceptable es de 100 a 1500

   Nota

   La mejor práctica recomienda calcular el tamaño de partición promedio durante un período. Luego, actualizar el tamaño inicial a este valor. Este método minimiza la cantidad de veces que se deberá ampliar una partición, y libera recursos para procesar datos en las particiones.

3. En **Crecimiento** configure el incremento por el cual aumentar el tamaño, en megabytes (MB), de los archivos **Datos** y **Registro** de una partición cuando se necesita espacio adicional.

   Usuarios de Microsoft SQL Server: El rango aceptable es de 1 a 999999

   Usuarios de MSDE: El rango aceptable es de 1 a 450
4. Haga clic en **Guardar ahora** para implementar los cambios ingresados en la ruta, el tamaño y el crecimiento.

Las particiones de la base de datos creada después de estos cambios utilizan la nueva configuración

5. Haga clic en **Crear ahora** para crear una nueva partición la próxima vez que se ejecute un trabajo ETL (consulte *Trabajos en la base de datos*, página 325), independientemente de la configuración del reinicio de datos automático. Por lo general, este proceso toma unos pocos minutos.

   Para que la nueva partición utilice los cambios que se hicieron en esta sección, recuerde hacer clic en **Guardar ahora** antes de hacer clic en **Crear ahora**.

   Cada cierto tiempo, haga clic en el enlace Actualizar en el panel de contenido. El área de las Particiones disponibles mostrará la nueva partición una vez que el proceso de creación finalice.

Configuración de las particiones disponibles

Temas relacionados:

- *Configuración de administración de la base de datos de registro.*, página 326
- *Configuración de opciones de reinicio de datos*, página 327
- *Configuración de las opciones de tiempo de navegación por Internet*, página 330
- *Configuración de registro de URL completa*, página 329
- *Configuración de las opciones de mantenimiento de la base de datos de registro*, página 331
- *Configuración de la creación de particiones en la base de datos de registro*, página 333
- *Cómo visualizar los registros de errores*, página 336

La sección **Particiones disponibles** de la página Base de datos de registro > de informes (ficha Configuración) enumera en una lista todas las particiones de la base de datos disponibles para la generación de informes. La lista muestra las fechas cubiertas, así como el tamaño y el nombre de cada partición.

Utilice esta lista para controlar qué particiones de base de datos están incluidas en los informes y para seleccionar las particiones que se deben eliminar.

1. Marque **Activar** junto a cada partición que se deba incluir en los informes.

   Utilice las opciones **Todas** y **Ninguna** que figuran arriba de la lista, según corresponda.

   Debe activar al menos una partición para la generación de informes. Utilice la opción **Ninguna** para desactivar todas las particiones de una vez de manera que luego pueda activar sólo algunas.

Utilice estas opciones para administrar cuántos datos deben analizarse cuando se generan informes y acelerar el procesamiento de informes. Por ejemplo, si planea generar una serie de informes para junio, quite la marca en todas las particiones excepto en aquellas con fecha en junio.

Importante

Esta selección afecta tanto a los informes programados como a los informes que se ejecutan en forma interactiva. Para evitar generar informes sin datos, compruebe que las particiones pertinentes estén activadas cuando los informes están programados para ejecutarse.

2. Haga clic en la opción **Eliminar** junto al nombre de la partición si ya no necesita esa partición. La partición se eliminará la próxima vez que se ejecute el trabajo de mantenimiento de la base de datos nocturno.

Advertencia

Utilice esta opción con cuidado. No podrá recuperar las particiones eliminadas.

Eliminar las particiones obsoletas reduce la cantidad de particiones en la base de datos de registro, lo que mejora el rendimiento de la base de datos y de la generación de informes. Utilice esta opción Eliminar para eliminar las particiones individuales según sea necesario. Consulte *Configuración de las opciones de mantenimiento de la base de datos de registro*, página 331, si prefiere eliminar las particiones más antiguas según una programación.

3. Haga clic en **Guardar ahora** para activar los cambios en las opciones de particiones disponibles.

Cómo visualizar los registros de errores

Temas relacionados:

- *Configuración de administración de la base de datos de registro.*, página 326
- *Configuración de opciones de reinicio de datos*, página 327
- *Configuración de las opciones de tiempo de navegación por Internet*, página 330
- *Configuración de registro de URL completa*, página 329
- *Configuración de las opciones de mantenimiento de la base de datos de registro*, página 331
- *Configuración de la creación de particiones en la base de datos de registro*, página 333
- *Configuración de las particiones disponibles*, página 335

Utilice la sección **Actividad del registro de errores** de la página Base de datos de registro > de informes (ficha Configuración) para ver los registros de los errores que se produjeron durante la ejecución de trabajos en la base de datos de registro de Websense (consulte *Trabajos en la base de datos*, página 325). Esta información puede ser útil para solucionar problemas.

Seleccione una de las siguientes opciones.

- Elija un número en la lista desplegable para mostrar la cantidad de entradas del registro de errores.
- Elija **Ver todas** para mostrar todas las entradas del registro de errores.
- Elija **No ver ninguna** para ocultar todas las entradas del registro de errores.

Configuración de los informes de investigación

Temas relacionados:

- *Opciones predeterminadas para la conexión de la base de datos y los informes*, página 338
- *Opciones de visualización y formato de salida*, página 339

Los informes de investigación le permiten explorar en forma interactiva la información sobre el uso de Internet en su organización. Consulte *Informes de investigación*, página 117.

El enlace Opciones en la página principal de los informes de investigación le brinda la oportunidad de modificar qué base de datos de registro se utiliza para los informes. También le permite modificar la vista predeterminada de los informes detallados. Consulte *Opciones predeterminadas para la conexión de la base de datos y los informes*, página 338.

El archivo **wse.ini** le permite configurar ciertas vistas predeterminadas para los informes de resumen y de múltiples niveles. Además, le brinda la posibilidad de elegir el tamaño de la página predeterminado que se utiliza cuando un informe se presenta con formato de salida en PDF. Consulte *Opciones de visualización y formato de salida*, página 339.

Opciones predeterminadas para la conexión de la base de datos y los informes

Temas relacionados:

- *Configuración de los informes de investigación*, página 337
- *Opciones de visualización y formato de salida*, página 339
- *Informes resumidos*, página 119
- *Informes resumidos de múltiples niveles*, página 124

Utilice la página de **Informes de investigación > Opciones** para conectarse a la base de datos de registro deseada y controlar las opciones predeterminadas para la visualización de los detalles de los informes de investigación.

Los cambios realizados en esta página se reflejan en sus informes. Otros administradores, o incluso usuarios que inicien sesión para informes propios, pueden cambiar estos valores para sus propias actividades de generación de informes.

1. Elija la base de datos de registro que debe utilizar para los informes de investigación.
   - Haga clic en **Ver la base de datos de catálogo** para conectarse a la base de datos de registro donde se está registrando Log Server. Continúe con el paso 2.
   - Para acceder a una base de datos de registro diferente:
     a. Desmarque la opción **Ver la base de datos de catálogo**.
     b. Especifique la siguiente información para identificar la base de datos de registro deseada. (Los informes de investigación pueden generarse desde una base de datos v6.3.x o v7.0.)

Campo	Descripción
Servidor	Especifique el nombre de la máquina o la dirección IP donde se encuentra la base de datos de registro.
Base de datos	Especifique el nombre de la base de datos de registro.
ID de usuario	Especifique el ID de usuario para una cuenta que tiene permiso para acceder a la base de datos. Deje en blanco si Log Server se instaló para usar una conexión de confianza para acceder a la base de datos de registro. Si no está seguro, escriba **sa**. Es el ID de usuario predeterminado para MSDE y el ID de administrador predeterminado en Microsoft SQL Server.
Contraseña	Ingrese la contraseña para el ID de usuario especificado. Deje en blanco para una conexión de confianza.

2. Seleccione los siguientes valores predeterminados para los informes detallados.

Campo	Descripción
Seleccione rango de fechas de informes de investigación predeterminados	Elija el rango de fechas para el informe de resumen inicial.
Seleccione el formato del informe detallado predeterminado	Elija **Selección de columnas inteligentes** para mostrar informes detallados con las columnas predeterminadas configuradas para la información que se está presentando. Elija **Selección personalizada de columnas** para especificar las columnas exactas que deben aparecer en la presentación inicial de todos los informes detallados. Utilice la lista de Columnas disponibles para hacer sus elecciones. Los usuarios pueden modificar las columnas que se muestran después de generar el informe.
Seleccionar tipo de informe	Elija si desea abrir los informes detallados que inicialmente muestran: • **Detalle**: cada registro aparece en una fila separada, se puede mostrar la hora. • **Resumen**: combina en una única entrada todos los registros que comparten un elemento en común. El elemento específico varía, según la información presentada. Por lo general, la columna de la derecha antes de la medida muestra el elemento resumido. No es posible mostrar la hora.
Columnas disponibles/ Informe actual	Seleccione un nombre de columna en la lista de Columnas disponibles y haga clic en la flecha correspondiente para moverla a la lista de Informe actual. La lista de Informe actual puede contener hasta siete columnas. Una vez que la lista de Informe actual tenga todas las columnas para los informes detallados iniciales, establezca el orden de las columnas. Seleccione una entrada en la lista y use los botones de las flechas hacia arriba y hacia abajo para cambiar la posición.

3. Haga clic en **Guardar opciones** para guardar los cambios inmediatamente.

Opciones de visualización y formato de salida

Temas relacionados:

- *Configuración de los informes de investigación*, página 337
- *Opciones predeterminadas para la conexión de la base de datos y los informes*, página 338
- *Generar archivo*, página 142

Puede hacer ajustes en la manera en que ciertas opciones de informes y resultados de informes se muestran en informes de investigación de múltiples niveles y resumen, y especificar el tamaño de página predeterminada cuando los informes se presentan en formato de salida PDF.

Estas opciones de configuración de informes de investigación se establecen en el archivo **wse.ini**. La ubicación predeterminada es:

```
C:\Archivos de programa\Websense\webroot\Explorer\wse.ini
```

La siguiente tabla enumera los parámetros que afectan la visualización y el formato de salida de los informes de investigación, qué controla cada uno, y su valor predeterminado. (NO modifique ninguna otra configuración en el archivo wse.ini.)

Parámetro	Descripción
maxUsersMenu	La base de datos debe tener una cantidad de usuarios menor que este valor (en forma predeterminada, 5000) para mostrar Usuario como opción de informe en Uso de Internet por lista.
maxGroupsMenu	La base de datos debe tener una cantidad de grupos menor que este valor (en forma predeterminada, 3000) para mostrar Grupo como opción de informe en Uso de Internet por lista. **Nota:** Debe haber dos o más grupos para que el Grupo aparezca en el Uso de Internet por lista. Debe haber dos o más dominios para que el Dominio aparezca en el Uso de Internet por lista. No se aplica ningún valor máximo para la cantidad de dominios.
maxUsersDrilldown	Trabaja con el parámetro warnTooManyHits para controlar cuándo la opción Usuario se muestra en rojo. Las letras rojas indican que la selección de Usuario producirá un informe muy grande, que podría demorar en generarse. Si la cantidad de usuarios supera este valor (en forma predeterminada, 5000) y más accesos que el valor warnTooManyHits, la opción Usuario se muestra en rojo en las diferentes listas desplegables y listas de valores. Si la cantidad de usuarios supera este valor, pero hay menos accesos que el valor warnTooManyHits, la opción Usuario se muestra en el color normal, ya que el informe resultante tendrá un tamaño más razonable.
maxGroupsDrilldown	Si el informe propuesto incluye una cantidad de grupos mayor que esta cifra (de forma predeterminada, 2000), la opción Grupo se muestra en color rojo durante la reducción de resultados. Las letras rojas indican que la selección de Grupo producirá un informe muy grande, que podría demorar en generarse.

Parámetro	Descripción
warnTooManyHits	Trabaja con el parámetro maxUsersDrilldown para controlar cuándo la opción Usuario se muestra en rojo. Si existen más usuarios que el valor maxUsersDrilldown pero menos accesos que este valor (de forma predeterminada, 10000), la opción Usuario *no* se mostrará en rojo. Si existen más usuarios que el valor maxUsersDrilldown y más accesos que este valor, la opción Usuario se mostrará en rojo. El color rojo indica que la selección de Usuario producirá un informe muy grande, que podría demorar en generarse.
hitsPerPage	Determina el número máximo de elementos (en forma predeterminada, 100) que se muestra por página. (No incide en los informes impresos.)
maxOutputBufferSize	Es la cantidad máxima de datos (en bytes) que pueden mostrarse en la página principal de los informes de investigación. Si los datos solicitados superan este límite (en forma predeterminada, 4000000, o 4 millones de bytes), aparece un mensaje en rojo al final del informe que indica que algunos resultados no se muestran. Los valores más grandes le permiten mostrar cantidades mayores de datos en un informe, si esto es lo que desea. Sin embargo, si se presentan errores en la memoria, considere la posibilidad de disminuir este valor.
sendMulti	Esta opción se encuentra deshabilitada (0) en forma predeterminada. Configúrela en 1 (habilitada) para dividir informes detallados programados que sean muy grandes en varios archivos de 10,000 filas cada uno. Los archivos que representan un informe se comprimen y se envían a los destinatarios de correo electrónico. Los archivos de informe pueden extraerse con las utilidades de compresión de archivos más comunes.
maxSlices	Es la cantidad máxima de sectores en que se divide un gráfico circular (en forma predeterminada, 6), incluido el sector Otro, que combina todos los valores que no tienen un sector propio.
timelineCompressionThreshold	Esta opción se utiliza sólo para la Actividad del usuario por día o mes, cuando la opción Agrupar accesos similares/Ver todos los accesos está disponible. El informe contrae todos los accesos con la misma categoría que se produce dentro de la cantidad de segundos establecida aquí (en forma predeterminada, 10).
PageSize	Los resultados del informe de investigación pueden tener el formato de salida Portable Document Format (PDF) para facilitar su distribución e impresión. El tamaño de la página (en forma predeterminada, carta) puede ser: • A4 (8.27 x 11.69 pulgadas) • Carta (8.5 x 11 pulgadas)

Actividad propia

Temas relacionados:

- *Configuración de las preferencias de informes*, página 310
- *Acceder a ver actividad propia*, página 144
- *Informes de investigación*, página 117

La actividad propia es una función que puede habilitar para permitir a los usuarios ver informes de investigación de su propia actividad en Internet. Esto les permite ver qué clase de información relacionada con ellos se recopila y se supervisa, y respeta las normas oficiales en muchos países. Además, si los usuarios ven su propia actividad pueden sentirse alentados a modificar sus hábitos de navegación para cumplir con la política de Internet de la organización.

Nota

La actividad propia está disponible únicamente cuando Websense Manager y los componentes de informes están instalados en un sistema operativo de Windows. Consulte la *Guía de implementación* para obtener información adicional.

Para habilitar la actividad propia:

1. Vaya a **Configuración >General > Servicios de directorio** y configure el servicio de directorio que se utiliza para autenticar usuarios que tienen acceso a Websense Manager con sus credenciales de red. Esto puede hacerse antes para activar el filtrado por usuario y nombres de grupo. Consulte *Servicios de directorio*, página 62.

   Si su instalación incluye varios Policy Servers, debe iniciar sesión en cada uno y configurar la página Servicios de directorio con información para el servicio de directorio correspondiente.
2. Vaya a **Configuración > Informes > Preferencias** y marque la casilla de verificación **Permitir que los usuarios vean su propia actividad**. Consulte *Configuración de las preferencias de informes*, página 310.

Después de activar esta opción, recuerde dar a los usuarios la información que necesitan para ejecutar los informes:

- La URL para acceder a la interfaz de actividad propia. Recuerde a los usuarios que pueden agregar la URL a su lista de sitios favoritos para volver a utilizarla en el futuro.

  Continúe leyendo si desea información detallada acerca de la URL.
- Qué Policy Server elegir durante el inicio de sesión.

En las redes con sólo un Policy Server, esto no se necesita. Si su red incluye varios Policy Servers, comunique a los usuarios la dirección IP del Policy Server configurada para comunicarse con el servicio de directorio que autentica su inicio de sesión en la red. Es también el Policy Server especificado cuando instaló Log Server.

- Qué nombre de usuario y contraseña se debe usar durante el inicio de sesión.

  Los usuarios de actividad propia deben ingresar su nombre de usuario de red y la contraseña durante el inicio de sesión.

La **URL** para acceder a la interfaz de actividad propia es.

```
https://<ServerIP>:9443/mng/login/pages/
   selfReportingLogin.jsf
```

En lugar de <ServerIP> use la dirección IP de la máquina que ejecuta Websense Manager.

Los administradores y usuarios también pueden acceder a la página de inicio de la actividad propia si abren la página de inicio de Websense Manager y hacen clic en el enlace Ver actividad propia.

Si su red incluye **varios Policy Servers**, debe informar a los usuarios cuál deben elegir durante el inicio de sesión de actividad propia.

14 Configuración de redes

Temas relacionados:

- *Configuración de hardware*, página 346
- *Configuración de Network Agent*, página 347
- *Cómo verificar la configuración de Network Agent*, página 354

Al ejecutar el software de Websense de modo autónomo (no integrado con un producto de proxy o firewall), Websense Network Agent permite:

- Filtrado de contenido de Internet
- Administración de protocolos y aplicaciones de Internet
- Administración de ancho de banda
- Registro de bytes transferidos

En una implementación del software de Websense, un producto de terceros puede administrar la tarea de enrutar solicitudes de los usuarios al software de Websense para filtrar y enrutar páginas de bloqueo de regreso al cliente. En este entorno, Network Agent aún se puede utilizar para filtrar solicitudes no http, ofrecer un detalle de registro mejorado o ambas opciones.

Network Agent supervisa continuamente el uso de red en general, incluidos los bytes transferidos por la red. Agent envía resúmenes de uso al software de Websense a intervalos predefinidos. Cada resumen incluye una hora de inicio y finalización, bytes utilizados en general y bytes utilizados por protocolo.

De manera predeterminada, Network Agent también proporciona datos de uso de ancho de banda a Policy Server, y datos de registro de filtrado a Filtering Service.

Network Agent generalmente se configura para ver todo el tráfico en la red. Agent distingue entre:

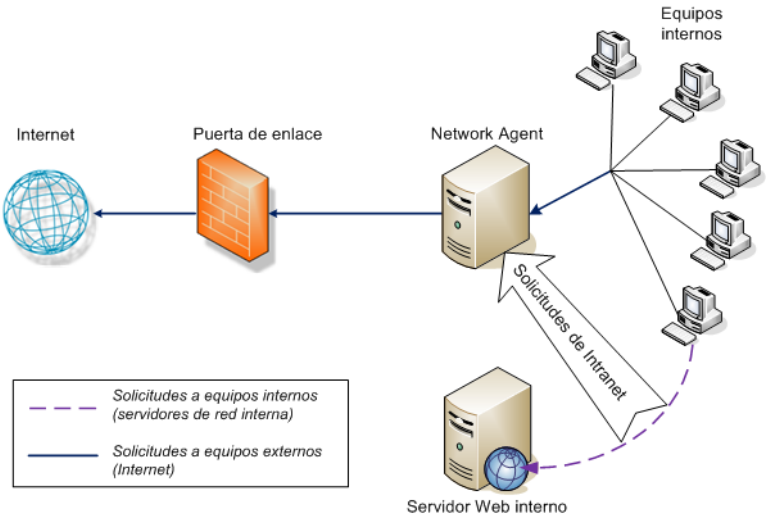
- Las solicitudes enviadas de equipos internos a equipos internos (accesos a un servidor de intranet, por ejemplo)
- Las solicitudes enviadas de equipos internos a equipos externos como servidores Web (solicitudes de Internet por parte de usuarios, por ejemplo)

Éstas últimas representan la principal inquietud en la supervisión del uso de Internet por parte de los empleados.

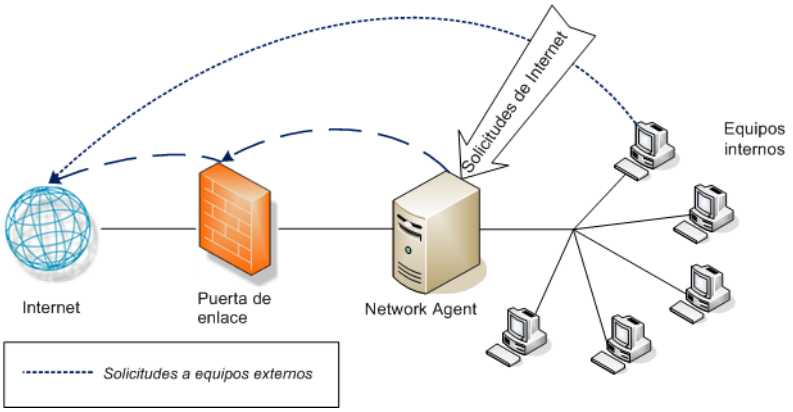
Configuración de hardware

Cada instancia de Network Agent supervisa el tráfico **desde** los equipos que identifica como pertenecientes a su red. De forma predeterminada, supervisa el tráfico **a** sólo esos equipos internos que especifica (por ejemplo, servidores Web internos).

Puede personalizar los equipos internos (segmentos de red) que cada instancia de Network Agent o, incluso cada tarjeta de interfaz de red (NIC), supervisará en un equipo de Network Agent.



Cómo supervisar solicitudes a equipos internos



Cómo supervisar solicitudes a equipos externos

Cada instancia de Network Agent debe:

- Posicionarse adecuadamente en la red para detectar tráfico hacia y desde todos los equipos supervisados.

- Tener al menos 1 NIC dedicada a supervisar el tráfico.

Network Agent se puede instalar en un equipo con múltiples NIC y puede utilizar varias NIC tanto para supervisar solicitudes como para enviar páginas de bloqueo. Si agrega una nueva NIC al equipo de Network Agent, reinicie el servicio de Network Agent y configure la nueva NIC (consulte *Cómo establecer la configuración de NIC*, página 351).

> **Nota**
> Para determinar si Network Agent puede ver el tráfico en un segmento de red, utilice la utilidad Detector de tráfico de la red. Consulte *Cómo verificar la configuración de Network Agent*, página 354.

Para obtener más información sobre la ubicación de Network Agent y los requisitos de NIC, consulte la *guía de instalación*.

Para obtener información sobre cómo configurar Network Agent para supervisar las solicitudes de red interna, utilice NIC específicas y realice un registro mejorado. Para ello, consulte *Configuración de Network Agent*, página 347.

Configuración de Network Agent

Temas relacionados:

- *Configuración de hardware*, página 346
- *Cómo establecer la configuración global*, página 348
- *Cómo establecer la configuración local*, página 349
- *Cómo establecer la configuración de NIC*, página 351
- *Cómo agregar o editar direcciones IP*, página 353

Después de instalar Network Agent, utilice Websense Manager para configurar su comportamiento de supervisión de red. La configuración de Network Agent se divide en dos áreas principales:

- **Configuración global** afecta todas las instancias de Network Agent. Utilice esta configuración para:
  - Identificar los equipos de la red.
  - Enumerar equipos en la red que Network Agent deba supervisar para solicitudes **entrantes** (por ejemplo, servidores Web internos).
  - Especificar el cálculo del ancho de banda y el comportamiento de registro de protocolos.
- **Configuración local** se aplica sólo a la instancia seleccionada de Network Agent. Utilice esta configuración para:

- Identificar la instancia de Filtering Service asociada con cada Network Agent.
- Advertir proxys y cachés utilizados por los equipos que este Network Agent supervisa.
- Configurar cómo se usa cada tarjeta de red (NIC) en el equipo de Network Agent (para supervisar solicitudes, enviar páginas de bloqueo o ambas opciones).

  La configuración de la tarjeta de red determina el segmento de la red que supervisa cada instancia de Network Agent.

Cómo establecer la configuración global

Temas relacionados:

- *Configuración de hardware*, página 346
- *Cómo establecer la configuración local*, página 349
- *Cómo establecer la configuración de NIC*, página 351
- *Cómo agregar o editar direcciones IP*, página 353

Utilice la página **Configuración > Network Agent > Global** para definir el comportamiento básico de supervisión y registro de todas las instancias de Network Agent.

La lista **Definición de red interna** identifica los equipos que forman parte de la red. De forma predeterminada, Network Agent no supervisa el tráfico (comunicaciones de la red interna) enviado entre estos equipos.

Se proporciona un conjunto inicial de entradas de forma predeterminada. Puede agregar entradas adicionales o editar o eliminar entradas existentes.

La lista **Tráfico interno que se debe supervisar** incluye cualquier equipo incluido en Definición de red interna para la que **desee** que Network Agent supervise el tráfico. Esto puede incluir servidores Web internos, por ejemplo, para ayudarlo a realizar un seguimiento de las conexiones internas.

Se supervisa cualquier solicitud enviada desde cualquier lugar de la red a los equipos internos especificados. De forma predeterminada, esta lista está en blanco.

- Haga clic en **Agregar** para agregar una dirección IP o rango a la lista adecuada. Consulte *Cómo agregar o editar direcciones IP*, página 353, para obtener más información.
- Para editar una entrada en la lista, haga clic en la dirección IP o rango. Consulte *Cómo agregar o editar direcciones IP*, página 353, para obtener más información.
- Para quitar una entrada de la lista, marque la casilla de verificación junto a una dirección IP o rango y haga clic en **Eliminar**.

Las opciones de **Configuración adicional** permiten determinar la frecuencia con la que Network Agent calcula el uso del ancho de banda, si se registra el tráfico de protocolo y con qué frecuencia:

Campo	Procedimientos
Intervalo de cálculo del ancho de banda	Ingrese un número entre 1 y 300 para especificar la frecuencia, en segundos, con la que Network Agent debe calcular el uso del ancho de banda. Una entrada de 300, por ejemplo, indica que Network Agent calculará el ancho de banda cada 5 minutos. El valor predeterminado es 10 segundos.
Registrar el tráfico de protocolos periódicamente	Marque esta opción para habilitar el campo Intervalo de registro.
Intervalo de registro	Ingrese un número entre 1 y 300 para especificar la frecuencia, en minutos, con la que Network Agent registra los protocolos. Una entrada de 60, por ejemplo, indica que Network Agent escribirá en el archivo de registro cada hora. El valor predeterminado es 1 minuto.

Cuando termine de realizar los cambios, haga clic en **Aceptar** para almacenar los cambios en caché. Los cambios no se implementan hasta que haga clic en **Guardar todo**.

Cómo establecer la configuración local

Temas relacionados:

- *Configuración de hardware*, página 346
- *Cómo establecer la configuración global*, página 348
- *Cómo establecer la configuración de NIC*, página 351

Utilice la página **Configuración > Network Agent > Configuración local** para establecer el comportamiento de filtrado, la información del proxy y otras opciones de configuración para la instancia seleccionada de Network Agent. La dirección IP de la instancia seleccionada de Network Agent aparece en la barra de título del panel de contenido y está resaltada en el panel izquierdo de navegación.

Utilice la configuración **Definición de Filtering Service** para especificar el Filtering Service asociado con la instancia seleccionada de Network Agent y cómo responder a las solicitudes de Internet si Filtering Service no está disponible.

Campo	Procedimientos
Dirección IP de Filtering Service	Seleccione el Filtering Service asociado con este Network Agent.
Si Filtering Service no está disponible	Seleccione **Permitir** para permitir todas las solicitudes o **Bloquear** para bloquear todas las solicitudes hasta que Filtering Service esté disponible nuevamente. La opción predeterminada es Permitir.

Para garantizar que las solicitudes de los usuarios se supervisen, filtren y registren correctamente, utilice la lista **Proxys y cachés** para especificar la dirección IP de cualquier servidor proxy o caché que se comunique con Network Agent.

- Haga clic en **Agregar** para agregar una dirección IP o rango a la lista. Consulte *Cómo agregar o editar direcciones IP*, página 353, para obtener más información.
- Para editar una entrada en la lista, haga clic en la dirección IP o rango.
- Para quitar una entrada de la lista, marque la casilla de verificación junto a una dirección IP o rango y haga clic en **Eliminar**.

Utilice la lista **Tarjetas de interfaz de red** para configurar NIC individuales. Haga clic en una NIC en la columna **Nombre** y consulte *Cómo establecer la configuración de NIC*, página 351, para obtener más instrucciones.

Si las solicitudes HTTP en la red pasan por un puerto no estándar, haga clic en **Configuración avanzada de Network Agent** para proporcionar los puertos correctos que Network Agent debe supervisar. De forma predeterminada, los **Puertos utilizados para tráfico HTTP** son **8080, 80**.

La otra configuración en esta sección no se debe cambiar a menos que el Soporte técnico de Websense lo indique.

Campo	Descripción
Modo	• Ninguno (predeterminado) • General • Error • Detalle • Ancho de banda
Salida	• Archivo (predeterminado) • Ventana
Puerto	55870 (predeterminado)

Cuando termine de realizar los cambios, haga clic en **Aceptar** para almacenar los cambios en caché. Los cambios no se implementan hasta que haga clic en **Guardar todo**.

Cómo establecer la configuración de NIC

Temas relacionados:

- *Configuración de hardware*, página 346
- *Configuración de Network Agent*, página 347
- *Cómo establecer la configuración de supervisión de una NIC*, página 352
- *Cómo agregar o editar direcciones IP*, página 353

Utilice la página **Network Agent > Configuración local > Configuración de NIC** para especificar cómo Network Agent debe usar cada tarjeta de interfaz de red (NIC) disponible para supervisar y administrar el uso de la red.

El área **Información de NIC** ofrece el contexto para los cambios que realiza, de modo de mostrar la **dirección IP**, una **descripción** breve de NIC y el **nombre** de la tarjeta. Utilice esta información para garantizar que esté configurando la NIC correcta.

Supervisión

En una configuración de múltiples NIC, puede identificar una NIC para que supervise el tráfico de la red y otra NIC para que envíe páginas de bloqueo. Se debe usar al menos una NIC para supervisar y más de una pueden supervisar el tráfico.

Utilice la sección **Supervisión** para indicar si debe **Utilizar esta NIC para supervisar el tráfico**.

- Si esta NIC no se utiliza para la supervisión, desactive la casilla de verificación y continúe con la siguiente sección.
- Si la NIC sí se utiliza para la supervisión, active la casilla de verificación y haga clic en **Configurar**. Será dirigido a la página Configurar comportamiento de supervisión. Consulte *Cómo establecer la configuración de supervisión de una NIC*, página 352, para obtener instrucciones.

Otras opciones de NIC

Además de configurar las opciones de supervisión, también puede determinar otros comportamientos de NIC:

1. En la sección Bloqueo, asegúrese de que se muestre la NIC adecuada en el campo **Bloqueo de NIC**. Si configurará varias NIC, la configuración para cada una debe mostrar el mismo valor en este campo. En otras palabras, sólo una NIC se utiliza para el bloqueo.
2. Si ejecuta el software de Websense en modo **Autónomo**, la opción **Solicitudes http de filtrado y registro** estará seleccionada y no se podrá cambiar.

3. Si cuenta con un software de Websense con un dispositivo o aplicación de terceros, utilice las opciones **Integraciones** para indicar cómo este Network Agent debe filtrar las solicitudes HTTP de filtrado y registro. Las opciones que no correspondan a su entorno se encontrarán deshabilitadas.
   - Seleccione **Solicitudes HTTP de registro** para mejorar la precisión de los informes de Websense.
   - Seleccione **Filtrar todas las solicitudes de protocolos no enviadas a través de puertos HTTP** para que Network Agent filtre sólo las solicitudes HTTP no enviadas mediante el producto de integración.
4. En la sección Protocolo Management, indique si Network Agent debe utilizar esta NIC para filtrar protocolos no HTTP:
   - Marque la opción **Filtrar peticiones de protocolo no HTTP** para activar la función de administración de protocolos. Esto permite que el software de Websense filtre aplicaciones de Internet y métodos de transferencia de datos como aquellos utilizados para la mensajería instantánea, transmisiones multimedia, intercambio de archivos, transferencia de archivos, correo en Internet, etc. Consulte *Protocolos y categorías de filtrado*, página 38, y *Cómo trabajar con protocolos*, página 185, para obtener más información.
   - Marque la opción **Medir uso de ancho de banda por protocolo** para activar la función Bandwidth Optimizer. Network Agent utiliza esta NIC para realizar un seguimiento del uso de ancho de banda de la red por cada protocolo o aplicación. Consulte *Cómo utilizar Bandwidth Optimizer para administrar el ancho de banda*, página 191, para obtener más información.

Cómo establecer la configuración de supervisión de una NIC

Utilice la página **Configuración local > Configuración de NIC >Lista de supervisión** para especificar los equipos que Network Agent supervisa mediante la tarjeta de interfaz de red (NIC) seleccionada.

1. En la sección Lista de supervisión, especifique las solicitudes que Network Agent debe supervisar:
   - **Todas**: Network Agent supervisa las solicitudes de todos los equipos que detecta con la NIC seleccionada. Por lo general, esto incluye todos los equipos del mismo segmento de red que el equipo Network Agent o la NIC actual.
   - **Ninguna**: Network Agent no supervisa ninguna solicitud.
   - **Específica**: Network Agent supervisa sólo los segmentos de red incluidos en la lista de supervisión.

2. Si seleccionó Específica, haga clic en **Agregar** y luego especifique las direcciones IP de los equipos que Network Agent debe supervisar. Consulte *Cómo agregar o editar direcciones IP*, página 353, para obtener más información.

   Nota
   No puede ingresar rangos de direcciones IP que se superpongan. Si los rangos se superponen, es posible que las mediciones del ancho de banda de red no sean exactas y que el filtrado en función del ancho de banda no se aplique correctamente.

   Para quitar una dirección IP o rango de redes de la lista, marque el elemento de lista adecuado y haga clic en **Eliminar**.

3. En Excepciones de lista de supervisión, identifique cualquier equipo interno que Network Agent deba excluir de la supervisión.

   Por ejemplo, Network Agent podría ignorar las solicitudes realizadas por CPM Server. De esta manera, las solicitudes de CPM Server no desorganizarán los datos de registro de Websense o ninguno de los supervisores del estado.

   a. Para identificar un equipo, haga clic en **Agregar** e ingrese su dirección IP.

   b. Repita el proceso para identificar equipos adicionales.

4. Haga clic en **Aceptar** para almacenar los cambios en caché y regrese a la página Configuración de NIC. Los cambios no se implementan hasta que haga clic en **Guardar todos**.

Cómo agregar o editar direcciones IP

Temas relacionados:

- *Cómo establecer la configuración global*, página 348
- *Cómo establecer la configuración local*, página 349
- *Cómo establecer la configuración de NIC*, página 351

Utilice la página **Agregar direcciones IP** o **Editar direcciones IP** para realizar cambios en cualquiera de las siguientes listas de Network Agent: Definición de red interna, Tráfico interno que se debe supervisar, Proxys y cachés, Lista de supervisión o Excepciones de lista de supervisión.

- Al agregar o editar un rango de direcciones IP, asegúrese de que no se superpongan con ninguna entrada existente (dirección IP o rango únicos) en la lista.
- Al agregar o editar una dirección IP única, asegúrese de que no se encuentre en el rango que ya aparece en la lista.

Para agregar una dirección IP o rango:

1. Seleccione el botón de opción **Dirección IP** o **Rango de direcciones IP**.

2. Ingrese una dirección IP o rango.
3. Haga clic en **Aceptar** para volver a la página anterior Configuración de Network Agent. La nueva dirección IP o rango aparece en la tabla adecuada.

   Para volver a la página anterior sin almacenar los cambios en caché, haga clic en **Cancelar**.
4. Repita este proceso para direcciones IP adicionales, si es necesario.

Al editar una dirección IP o rango existentes, la página Editar direcciones IP muestra el elemento seleccionado con el botón de opción correcto ya seleccionado. Realice los cambios necesarios y haga clic en **Aceptar** para volver a la página anterior.

Cuando termine de agregar o editar direcciones IP, haga clic en **Aceptar** en la página Configuración de Network Agent. Los cambios no se implementan hasta que haga clic en **Guardar todos**.

Cómo verificar la configuración de Network Agent

Después de configurar Network Agent en Websense Manager, utilice el detector de tráfico de la red para asegurarse de que los equipos en la red estén visibles para el software de Websense.

1. Vaya a **Inicio > Programas > Websense > Utilidades >Detector de tráfico de la red** para iniciar la herramienta.
2. Seleccione una tarjeta de red de la lista desplegable **Adaptador de red**.
3. Controle las direcciones que aparecen en la lista **Rangos de red supervisados** para verificar que se muestren todas las subredes pertinentes.
4. Utilice los botones **Agregar subred** y **Eliminar subred** para cambiar las partes de la red que se analizan.
5. Haga clic en **Iniciar supervisión**.

   El detector de tráfico de la red detecta los equipos de la red al supervisar la información que envían a través de ésta. La lista **Nº de equipos detectados** muestra el conteo actual de equipos detectados.
6. Para obtener información específica sobre los equipos detectados por la herramienta, seleccione una subred en la lista Rangos de red supervisados y haga clic en **Ver equipos detectados**.

   Si no figura un equipo específico, verifique que el mismo esté generando tráfico en la red. Para esto, abra un navegador de Internet en el equipo y visite un sitio Web. Luego regrese al detector de tráfico de la red y compruebe que el equipo figure en el cuadro de diálogo **Equipos detectados**.
7. Cuando haya terminado de comprobar la visibilidad del tráfico de la red, haga clic en **Detener supervisión**.

Si algunos equipos no están visibles:

- Analice la configuración de la red y los requisitos de ubicación de red (consulte *Configuración de hardware*, página 346).

- Analice la información de red mas detallada en la *guía de instalación* para el software de Websense.
- Verifique que haya configurado adecuadamente la supervisión de NIC (*Cómo establecer la configuración de NIC*, página 351).

15 Solución de problemas

Use esta sección para encontrar las soluciones a problemas comunes antes de ponerse en contacto con el soporte técnico.

El sitio Web de Websense posee una Knowledge Base con amplia información, disponible en www.websense.com/global/en/SupportAndKB/. Busque los temas mediante palabras clave o números de referencia, o navegue por los artículos más populares.

Las instrucciones para la solución de problemas se agrupan en las siguientes secciones:

Problemas de instalación y suscripción

El estado de Websense indica un problema de suscripción

Para descargar la base de datos principal de Websense y realizar el filtrado de Internet se requiere una clave de suscripción válida. Cuando la suscripción caduca o es

inválida, y cuando la base de datos principal de Websense no ha sido descargada por más de 2 semanas, el supervisor Websense Health muestra una advertencia.

- Verifique que haya ingresado su clave de suscripción exactamente como la recibió. La clave distingue entre mayúsculas y minúsculas.
- Asegúrese de que su suscripción no haya caducado. Vea *Clave de suscripción*, página 360.
- Asegúrese de que la base de datos principal no haya sido correctamente descargada en las últimas 2 semanas. Puede verificar el estado de descarga desde el Websense Manager: Haga clic en **Descarga de base de datos** en la página Estado > Hoy.

  Vea *No se descarga la base de datos principal*, página 360, para obtener información sobre la solución de problemas de descarga de la base de datos.

Si ha ingresado la clave en forma correcta pero continúa recibiendo un mensaje de error de estado, o si la suscripción ha caducado, comuníquese con Websense, Inc., o con su revendedor autorizado.

Cuando caduca la suscripción, la configuración de Websense Manager determina si todos los usuarios recibirán acceso a Internet sin filtrar o si se bloquearán todas las solicitudes de Internet. Consulte *Suscripción*, página 28, para más información.

Luego de realizar la actualización, los usuarios no aparecen en el Websense Manager

Si está definido como Directorio activo como su servicio de directorio, luego de una actualización del software de Websense, los nombres de usuario podrían no aparecer en el Websense Manager. Esto sucede cuando los nombres de usuario incluyen caracteres que no son parte del juego de caracteres UTF-8.

A fin de soportar LDAP 3.0, el instalador de Websense cambia el juego de caracteres de MBCS a UTF-8 durante la actualización. Como resultado, los nombres de usuario que incluyen caracteres diferentes a los UTF-8 no son reconocidos correctamente.

Para solucionar el problema, cambie manualmente el juego de caracteres por MBCS:

1. En Websense Manager, vaya a **Configuración** > **Servicios de Directorio**.
2. Asegúrese de que **Active Directory (modo nativo)** esté seleccionado en Directorios, próximo a la parte superior de la página.
3. Haga clic en **Configuración de directorio avanzada**.
4. En la sección Juego de caracteres, haga clic en **MBCS**. Para poder visualizar esta opción, navegue por la página.
5. Haga clic en **Aceptar** para implementar el cambio. Los cambios no se producirán hasta que no haga clic en **Guardar todo**.

Problemas de la base de datos principal

Se está utilizando la base de datos de filtrado inicial

La base de datos principal de Websense contiene las definiciones de categorías y protocolos que representan las bases para el filtrado del contenido de Internet.

Una versión parcial de la base de datos principal se instala con su software de Websense en cada una de las máquinas Filtering Service. Esta base de datos parcial se utiliza para habilitar la funcionalidad de filtrado básico a partir del momento que se ingresa la clave de suscripción.

Es necesario descargar la base de datos entera para poder efectuar un filtrado completo. Consulte *Base de datos principal de Websense*, página 31, para más información.

El proceso de descarga de la base de datos completa podría insumir unos minutos o más de 60 minutos, dependiendo de factores tales como la velocidad de conexión de Internet, el ancho de banda, la memoria disponible y el espacio libre en disco.

La base de datos principal tiene más de una semana de antigüedad

La base de datos principal de Websense contiene las definiciones de categorías y protocolos que representan las bases para el filtrado del contenido de Internet. El software de Websense descarga los cambios en la base de datos principal según la programación definida en Websense Manager. De manera predeterminada, la descarga está programada para que se realice una vez al día.

Para iniciar manualmente una descarga de la base de datos:

1. En Websense Manager, diríjase a la página **Estado > Hoy** y haga clic en **Descarga de base de datos**.

2. Haga clic en **Actualizar** al lado del Filtering Service que corresponda para iniciar la descarga de la base de datos, o en **Actualizar todo** para iniciar la descarga en todas las máquinas Filtering Service.

   Nota
   Tras descargar las actualizaciones de la base de datos principal, el uso de CPU puede ser del 90% o superior por unos minutos, mientras se carga la base de datos en la memoria local. Una buena idea es realizar la descarga en horarios de menor actividad.

3. Para continuar trabajando mientras se descarga la base de datos, haga clic en **Cerrar**.

   Haga clic en el botón **Descarga de base de datos** en cualquier momento para visualizar el estado de la descarga.

Si una nueva versión de la base de datos principal agrega o elimina categorías o protocolos, los administradores que realicen tareas de gestión de políticas relacionadas con la categoría o protocolo (como editar un juego de categorías) podrán recibir errores al momento de la descarga. Si bien tales actualizaciones no son comunes, a modo de buena práctica, intente evitar realizar cambios relacionados con la categoría y el protocolo mientras se está actualizando la base de datos.

No se descarga la base de datos principal

En caso de que no pueda descargar la base de datos principal de Websense correctamente:

- Asegúrese de haber ingresado la clave de suscripción correctamente en Websense Manager, y de que la clave no haya caducado (*Clave de suscripción*, página 360).
- Verifique que el equipo Filtering Service tenga acceso a Internet (*Acceso a Internet*, página 361).
- Controle las Configuración de firewall y de servidor proxy para asegurarse de que Filtering Service pueda conectarse al servidor de descarga de Websense (*Verifique las Configuración de firewall y del servidor Proxy.*, página 362).
- Asegúrese de que haya espacio suficiente en disco (*Espacio en disco insuficiente*, página 363) y memoria (*Memoria insuficiente*, página 363) en el equipo de descarga.
- Busque cualquier aplicación o dispositivo de la red, como software anti-virus, que pudiera impedir la conexión de descarga (*Aplicaciones restrictivas*, página 364).

Clave de suscripción

Para verificar que la clave de suscripción haya sido ingresada correctamente y que no haya caducado:

1. En Websense Manager, vaya a **Configuración >Cuenta**.

2. Compare la clave otorgada por Websense, Inc., o su revendedor con el campo **Clave de suscripción**. La clave debe utilizar las mismas mayúsculas y minúsculas que en su documento.
3. Verifique la fecha que se encuentra junto a **La clave caduca**. Si la fecha caducó, póngase en contacto con su revendedor autorizado o con Websense, Inc. para renovar la suscripción.
4. En caso de haber incorporado cambios de clave en el cuadro de diálogo Configuración, haga clic en **Aceptar** para activar la clave y habilitar la descarga de la base de datos.

Para iniciar una descarga de la base de datos manualmente o para verificar el estado de la descarga más reciente de la base de datos, haga clic en **Descarga de base de datos** en la barra de herramientas que se encuentra en la parte superior de la página Estado > Hoy.

Acceso a Internet

Para descargar la base de datos principal, el equipo Filtering Service envía un comando **HTTP post** a los servidores de descarga a las siguientes URL:

download.websense.com
ddsdom.websense.com
ddsint.websense.com
portal.websense.com
my.websense.com

Para verificar que Filtering Service tenga el acceso a Internet necesario para comunicarse con el servidor de descarga:

1. Abra un navegador en el Filtering Service que se ejecuta en el equipo.
2. Ingrese la siguiente URL:

   http://download.websense.com/

   Si el equipo puede abrir una conexión HTTP en el sitio, se visualiza una página de redireccionamiento y luego el navegador muestra la página de inicio de Websense.

   En caso contrario, asegúrese de que el equipo:

   - Pueda comunicarse mediante el puerto 80 o el puerto designado en su red para el tráfico HTTP
   - Está configurado para realizar consultas de DNS correctamente
   - Está configurado para utilizar cualquier servidor proxy necesario (ver *Verifique las Configuración de firewall y del servidor Proxy.*, página 362)

   Asimismo, asegúrese que su puerta de enlace no incluya ninguna regla que bloquee el tráfico HTTP del equipo Filtering Service.
3. Use uno de los siguientes métodos para confirmar que el equipo pueda comunicarse con el sitio de descarga:
   - Desde el símbolo del sistema, ingrese el siguiente comando:

     ```
     ping download.websense.com
     ```

Verifique que el ping reciba una respuesta del servidor de descarga.

- Use telnet para conectarse a **download.websense.com 80**. Si ve un cursor y no aparece un mensaje de error, puede conectarse al servidor de descarga.

Verifique las Configuración de firewall y del servidor Proxy.

Si la base de datos principal se descarga mediante un firewall o servidor proxy que requiera autenticación, asegúrese de que un navegador en el equipo Filtering Service pueda cargas correctamente las páginas Web. Si las páginas abren normalmente, pero la base de datos principal no se descarga, verifique la configuración del servidor Proxy de su navegador Web.

Microsoft Internet Explorer:

1. Seleccione **Herramientas > Opciones de Internet**.
2. Abra la ficha **Conexiones**.
3. Haga clic en **Configuración de red**. Se visualiza la configuración del servidor proxy debajo de **Servidor proxy**.

   Tome nota de la configuración del Proxy.

Mozilla Firefox:

1. Seleccione **Herramientas > Opciones > Opciones avanzadas**.
2. Seleccione la ficha **Red**.
3. Haga clic en **Configuración**. El cuadro de diálogo Configuración de conexión indica si el navegador está configurado para conectarse con un servidor Proxy.

   Tome nota de la configuración del Proxy.

Luego, asegúrese de que el software de Websense esté configurado para usar el mismo servidor proxy para realizar la descarga.

1. En Websense Manager, vaya a **Configuración > Descarga de base de datos**.
2. Verifique que **Usar servidor proxy o firewall** esté seleccionado y que el servidor y el puerto correcto aparezcan en la lista.
3. Asegúrese de que las Configuración de **Autenticación** sean correctas. Verifique el nombre de usuario y la contraseña, verifique la ortografía y el uso de mayúsculas.

   Si el software de Websense debe proporcionar información de autenticación, el firewall o servidor proxy debe estar configurado para aceptar texto no cifrado o autenticación básica. En Knowledge Base de Websense encontrará información de autenticación básica.

Si el firewall restringe el acceso a Internet en el momento en que el software de Websense normalmente descarga la base de datos, o si restringe el tamaño de los archivos que se pueden transferir vía HTTP, el software de Websense no puede descargar la base de datos. Para determinar si el firewall está provocando una falla de descarga, busque una regla en el firewall que pudiera estar bloqueando la descarga y cambie los tiempos de descarga en Websense Manager (*Configuración de descargas de la base de datos*, página 33), en caso de ser necesario.

Espacio en disco insuficiente

La Base de datos principal de Websense está almacenada en el directorio **binario** (/opt/Websense/bin o C:\Archivos de programa\Websense\bin, por defecto). La unidad que contiene este directorio debe tener espacio suficiente para descargar la base de datos comprimida y espacio suficiente para descomprimir la base de datos.

El equipo debe tener como mínimo 2 veces el tamaño de la base de datos principal de espacio libre en disco. A medida que incrementan las entradas en la base de datos principal, el tamaño requerido para lograr la descarga también incrementa. Como regla general, Websense, Inc. recomienda como mínimo 3 GB de espacio libre en disco en la unidad de descarga.

En Windows, use Windows Explorer para verificar el espacio disponible en disco:

1. Abra **Mi PC** en Windows Explorer (no en Internet Explorer).
2. Seleccione la unidad en la que está instalado el software Websense. De forma predeterminada, el software de Websense está instalado en la unidad C.
3. Haga clic con el botón secundario y seleccione **Propiedades** del menú emergente.
4. En la ficha General, verifique que haya como mínimo 3 GB de espacio libre disponible. Si el espacio libre en la unidad es insuficiente, elimine los archivos que sea necesario para liberar el espacio requerido.

Con los sistemas Linux, use el comando **df** para verificar la cantidad de espacio disponible en el sistema de archivos en el cual está instalado el software de Websense:

1. Abra una sesión de terminal.
2. Cuando aparece la solicitud, ingrese:

   ```
   df -h /opt
   ```

   Generalmente, el software de Websense está instalado en el directorio /opt/Websense/bin. En caso de que esté instalado en otro directorio, use esa ruta.
3. Asegúrese de tener, como mínimo, 3 GB de espacio libre disponible. Si el espacio libre en la unidad es insuficiente, elimine los archivos que sea necesario para liberar el espacio requerido.

Si verifica que el espacio en disco es suficiente, pero aún tienen problemas de descarga, intente detener todos los servicios de de Websense (consulte *Cómo detener e iniciar los servicios Websense*, página 286), eliminando los archivos **Websense.xfr** y **Websense** (sin extensión), iniciando los servicios y descargando manualmente una nueva base de datos.

Memoria insuficiente

La memoria necesaria para ejecutar el software de Websense y descargar la base de datos principal varía según el tamaño de la red. Por ejemplo, en caso de una red pequeña, se recomiendan 2 GB de memoria para todas las plataformas.

Consulte la *Guía de implementación* para obtener recomendaciones del sistema.

Para verificar la memoria del sistema Windows:

1. Abra el Administrador de tareas.
2. Seleccione la ficha **Rendimiento**.
3. Verifique la memoria **Memoria física** total disponible.
4. En caso de que haya menos de 2 GB instalados, actualice la RAM del equipo.

También puede seleccionar **Panel de control > Herramientas administrativas > Rendimiento** para capturar información.

Para verificar la memoria de un sistema Linux:

1. Abra una sesión de terminal.
2. Cuando aparece la solicitud, ingrese:

   ```
   top
   ```
3. Calcule la memoria total disponible sumando **Mem: av** y **Swap: av**.
4. En caso de que haya menos de 2 GB instalados, actualice la RAM del equipo.

Aplicaciones restrictivas

Algunas aplicaciones restrictivas, como las herramientas antivirus o las aplicaciones que limitan tamaños o los sistemas de detección de intrusión, pueden interferir con las descargas de la base de datos. Idealmente, configure el software Websense para ingresar directamente a la última puerta de enlace de modo que no se conecte con estas aplicaciones o dispositivos. Alternativamente:

1. Desactive las restricciones relacionadas con el equipo Filtering Service y la ubicación de descarga de la base de datos principal.

   Consulte la documentación del dispositivo o software para obtener las instrucciones para cambiar la configuración del dispositivo.
2. Intente descargar la base de datos principal.

Si el cambio no tiene efecto, reconfigure la aplicación o el dispositivo para incluir el equipo que ejecuta Filtering Service.

La descarga de la base de datos principal no se produce en el horario correcto

Es posible que no se haya determinado correctamente la fecha y la hora del sistema en el equipo Filtering Service. El software de Websense utiliza el reloj del sistema para determinar el horario adecuado para la descarga de la base de datos principal.

Si no se produce la descarga, consulte *No se descarga la base de datos principal*, página 360.

Cómo contactar al soporte técnico para resolver problemas relativos a la descarga de la base de datos

Si aún tiene problemas para descargar la base de datos principal luego de completar los pasos para la solución de problemas en esta sección de Ayuda, envíe la siguiente información al soporte técnico de Websense:

1. El mensaje de error exacto que aparece en el cuadro de diálogo de Descarga de base de datos
2. Las direcciones de IP externas de las máquinas en las que se intenta descargar la base de datos
3. Su clave de suscripción de Websense
4. Fecha y hora del último intento de descarga
5. Cantidad de bytes transferidos, en caso de que corresponda
6. Abra el símbolo del sistema y realice una **nslookup** en **download.websense.com**. En caso de lograr la conexión con el servidor de descarga, envíe las direcciones de IP al soporte técnico.
7. Abra el símbolo del sistema y realice una **tracert** en **download.websense.com**. En caso de lograr la conexión con el servidor de descarga, envíe la ruta al soporte técnico.
8. Paquete de seguimiento o paquete de captura realizado en el servidor de descarga de Websense durante un intento de descarga.
9. Paquete de seguimiento o paquete de captura realizado en la puerta de enlace de la red durante el mismo intento de descarga.
10. Los siguientes archivos del directorio **binario** de Websense: **websense.ini**, **eimserver.ini** y **config.xml**.

Ingrese en www.websense.com/SupportPortal/default.aspx para obtener la información de contacto del soporte técnico.

Problemas de filtrado

- *El software Websense no está aplicando las políticas de usuarios o de grupos*, página 369
- *Los usuarios remotos no son filtrados por la política correcta*, página 369

Filtering Service no está en ejecución

Cuando Filtering Service no está en ejecución, no es posible filtrar ni registrar solicitudes de Internet.

Filtering Service puede detenerse si:

- No hay espacio suficiente en el equipo de Filtering Service.
- Se produce una falla en una descarga de la base de datos principal debido a falta de espacio en disco (consulte *No se descarga la base de datos principal*, página 360).
- Falta el archivo **websense.ini** o el archivo está corrupto.
- Usted detiene el servicio (después de crear páginas de bloqueo personalizadas, por ejemplo) y no lo reinicia.

Filtering Service también podría haberse detenido en caso de haber reiniciado múltiples servicios de Websense, y de no haberlo hecho en el orden correcto. Cuando reinicia múltiples servicios, recuerde iniciar Policy Database, Policy Broker y Policy Server antes de iniciar otros servicios de Websense.

Para solucionar estos problemas:

- Verifique que haya, como mínimo, 3 GB de espacio libre en disco en el equipo Filtering Service. Es posible que deba eliminar archivos no utilizados o agregar capacidad adicional.
- Ingrese al directorio **binario** de Websense (C:\Archivos de programa\Websense\bin o /opt/Websense/bin, por defecto) y verifique que puede abrir **websense.ini** en un editor de texto. Si este archivo estuviera corrupto, reemplácelo con un archivo de respaldo.
- Verifique el visor de sucesos de Windows o el archivo **websense.log** para determinar si existen mensajes de error de Filtering Service (consulte *Herramientas para la solución de problemas*, página 401).
- Cierre la sesión de Websense Manager, reinicie Websense Policy Server y luego reinicie Websense Filtering Service (consulte *Cómo detener e iniciar los servicios Websense*, página 286).

  Espere 1 minuto antes de iniciar sesión en Websense Manager nuevamente.

User Service no está disponible.

Cuando User Service no se está ejecutando, o cuando Policy Server no puede comunicarse con User Service, el software Websense no puede aplicar correctamente las políticas de filtrado basadas en usuarios.

Es posible que se detenga User Service si usted reinició Policy Server después de reiniciar otros servicios de Websense. Para corregir este problema:

1. Reinicie el servicio Websense Policy Server (consulte *Cómo detener e iniciar los servicios Websense*, página 286).
2. Inicie o reinicie Websense User Service.
3. Cierre Websense Manager.

   Espere 1 minuto antes de iniciar sesión en Websense Manager nuevamente.

Si los pasos anteriores no resuelven el problema:

- Verifique el visor de sucesos de Windows o el archivo **websense.log** para determinar si existen mensajes de error de User Service (consulte *Herramientas para la solución de problemas*, página 401).
- Ingrese al directorio **binario** de Websense (C:\Archivos de programa\Websense\bin o /opt/websense/bin, por defecto) y verifique que puede abrir **websense.ini** en un editor de texto. Si este archivo estuviera corrupto, reemplácelo con un archivo de respaldo.

Los sitios están incorrectamente categorizados como tecnología informática

Las versiones 4.0 y posteriores de Internet Explorer tienen capacidad para aceptar búsquedas desde la barra de Direcciones. Cuando esta opción está habilitada, si un usuario ingresa únicamente un nombre de dominio en la barra de direcciones (**websense** en lugar de **http://www.websense.com**, por ejemplo), Internet Explorer lo considera una solicitud de búsqueda, no una solicitud de un sitio. Muestra el sitio con mayores probabilidades que esté buscando el usuario, junto con una lista de sitios posibles.

Como resultado, el software de Websense permite, bloquea o limita la solicitud sobre la base del estado de las categorías Tecnología informática/Portales y motores de búsqueda en la política activa —no en la categoría del sitio solicitado. Para que el software de Websense filtre sobre la base de la categoría del sitio solicitado, desactive la búsqueda desde la barra de direcciones:

1. Seleccione **Herramientas > Opciones de Internet**.
2. Vaya a la ficha **Avanzado**.
3. En el área Buscar desde la barra de direcciones, seleccione **No buscar desde la barra de direcciones**.
4. Haga clic en **Aceptar**.

> **Nota**
>
> Estos pasos son válidos para las versiones 5, 6 y 7 de Internet Explorer.

No se bloquean las palabras clave

Los 2 posibles motivos de este problema son: **Desactivar bloqueo de palabra clave** está seleccionado o el sito cuya URL contiene la palabra clave usa **post** para enviar datos a su servidor Web.

Para asegurarse de que el bloqueo de palabra clave esté activado:

1. En Websense Manager, vaya a **Configuración >Filtrado**.
2. En Filtrado general, seleccione la lista **de opciones de búsqueda por palabra clave**. Si aparece **Desactivar bloque de palabra clave**, seleccione otra opción de la lista. Consulte *Cómo configurar los valores de filtrado de Websense*, página 56, para más información sobre las opciones disponibles.
3. Haga clic en **Aceptar** para implementar el cambio. Los cambios no se producirán hasta que no haga clic en **Guardar todo**.

Si el sitio usa **post** para enviar datos a su servidor Web, el software Websense no reconoce la configuración de filtrado por palabra clave para la URL. Salvo que su producto de integración reconozca los datos enviados vía post, los usuarios aún pueden acceder a las URL que contengan palabras clave bloqueadas.

Para controlar si un sitio Web utiliza un comando post, vea el código fuente del sitio desde su navegador. Si el código fuente contiene una cadena como **<method=post>**, entonces se utiliza post para cargar ese sitio.

Las URL con filtro de acceso personalizado o limitado no están filtradas como se espera

Si una URL HTTPS de una lista de URL con filtro de acceso limitado o personalizado (recategorizada o no filtrada) no está filtrada como se espera, puede ocurrir que un producto de integración esté convirtiendo la URL a un formato que Filtering Service no puede reconocer.

Los productos de integración por no proxy convierten las URL de formato de dominio a formato IP. Por ejemplo, la URL **https://<domain>** se lee como **https://<IP address>:443**. En este caso, Filtering Service no puede hacer coincidir la URL proveniente del producto de integración con una URL con filtro de acceso limitado o personalizado, y no filtra el sitio correctamente.

Para solucionar este problema, agregue la dirección de IP y las URL de los sitios que desea filtrar usando las URL personalizadas o los filtros de acceso limitado.

Un usuario no puede acceder a un protocolo o aplicación como era previsto

Si su red incluye Microsoft ISA Server, ciertas Configuración del método de autenticación podrán provocar caídas de las conexiones de las aplicaciones de mensajería.

Si se ha activado cualquier método distinto de Autenticación anónima, los intentos del servidor proxy por identificar paquetes de datos recibidos cuando los usuarios solicitan conexiones con aplicaciones. El servidor proxy no puede identificar el paquete de datos y se interrumpe la conexión. Esto puede desviar la actividad de filtrado de protocolos de Websense.

También es posible que no se pueda acceder a un protocolo o aplicación de Internet si el puerto utilizado por la aplicación está bloqueado. Esto podría ocurrir si:

- El puerto está bloqueado por un firewall.
- Un protocolo personalizado bloqueado incluye un puerto (como un puerto único o como parte de un rango de puertos) en cualquiera de sus identificadores.

Un solicitud de FTP no está bloqueada como se esperaba

Cuando se integra con los firewalls Check Point®, el software Websense requiere que **vista de carpeta** esté activado en el navegador del cliente para poder reconocer y filtrar las solicitudes de FTP.

Cuando la vista de carpeta no está activada, las solicitudes de FTP enviadas al proxy Firewall-1 son enviadas al software Websense con un prefijo “http://”. Como resultado, el software Websense filtra estas solicitudes como solicitudes HTTP, en lugar de solicitudes FTP.

El software Websense no está aplicando las políticas de usuarios o de grupos

Si el software Websense está aplicando políticas de equipos o de redes, o la política **predeterminada**, incluso luego de la asignación de políticas de usuario o grupo, consulte *Problemas de identificación de usuarios*, página 372. Podrá obtener información adicional vía la Knowledge Base.

Los usuarios remotos no son filtrados por la política correcta

Si un usuario remoto accede a la red iniciando sesión mediante credenciales de dominio en caché (información de inicio de sesión de red), el software Websense aplica la política asignada a ese usuario o al grupo de usuarios o de dominio, según corresponda. En caso de no haber una política asignada al usuario, grupo o dominio, o si el usuario inicia sesión en un equipo con una cuenta de usuario local, el software Websense aplica la política predeterminada.

Ocasionalmente, el usuario no está filtrado por la política de usuario o grupo o la política predeterminada. Esto se produce cuando el usuario inicia sesión en un equipo remoto con una cuenta de usuario local y la última porción de la dirección de Control de Acceso de Medios (MAC) del equipo remoto se superpone con una dirección IP de red interna a la cual se asignó una política. En este caso, la política asignada a esa dirección IP en particular se aplica al usuario remoto.

Problemas de Network Agent

Network Agent no está instalado

Network Agent es necesario para activar el filtrado de protocolo. Con algunas integraciones, Network Agent también proporciona un registro más preciso.

Si está ejecutando un producto de integración y no requiere filtrado de protocolo Network Agent o inicio de sesión, puede ocultar el mensaje de estado "No hay ningún Network Agent instalado". Consulte *Cómo revisar el estado actual del sistema*, página 294,para obtener instrucciones.

Para instalaciones autónomas, Network Agent debe estar instalado de modo que pueda supervisar y filtrar el tráfico de red. Consulte la *Guía de instalación* para obtener instrucciones sobre la instalación y luego consulte *Configuración de Network Agent*, página 347.

Network Agent no está en ejecución

Network Agent es necesario para activar el filtrado de protocolo. Con algunas integraciones, Network Agent también proporciona un registro más preciso.

Para instalaciones autónomas, Network Agent debe estar ejecutándose para supervisar y filtrar el tráfico de red.

Para solucionar este problema:

1. Seleccione el cuadro de diálogo Servicios de Windows (consulte *El cuadro de diálogo de Windows Services*, página 402) para verificar que el servicio **Websense Network Agent** se haya iniciado.
2. Reinicie los servicios **Policy Broker de Websense** y **Policy Server de Websense** (consulte *Cómo detener e iniciar los servicios Websense*, página 286).
3. Inicie o reinicie el servicio **Network Agent de Websense**.
4. Cierre Websense Manager.
5. Aguarde un minuto y luego inicie sesión en Websense Manager nuevamente.

Si no se corrige el problema:

- Verifique **el visor de sucesos de Windows** para controlar que no existan mensajes de error de Network Agent (consulte *El visor de sucesos de Windows*, página 402).
- Controle el archivo **Websense.log** para determinar si existen mensajes de error de Network Agent (consulte *El archivo de registro Websense*, página 402).

Network Agent no está supervisando ninguna NIC

Network Agent debe estar asociado con, por lo menos, una tarjeta de interfaz de red (NIC) para supervisar el tráfico de red.

Si agregó o eliminó tarjetas de red del equipo de Network Agent, debe actualizar la configuración de Network Agent.

1. En Websense Manager, vaya a **Configuración**.
2. En el panel izquierdo de navegación, en Network Agent, seleccione la dirección IP del equipo Network Agent.
3. Verifique que todas las NIC para el equipo seleccionado aparezcan en la lista.
4. Verifique que al menos una NIC esté configurada para supervisar el tráfico de la red.

Consulte *Configuración de Network Agent*, página 347, para más información.

Network Agent no puede comunicarse con Filtering Service

Network Agent debe poder comunicarse con Filtering Service para aplicar las políticas de uso de Internet.

- ¿Cambió la dirección IP del equipo Filtering Service o reinstaló Filtering Service?

  En tal caso, consulte *Actualización de la dirección IP o información UID de Filtering Service*, página 371.
- ¿Tiene más de 2 tarjetas de interfaz de red (NIC) en el equipo de Network Agent?

  Si la respuesta es afirmativa, consulte *Configuración de redes*, página 345,para verificar la configuración de Websense.
- ¿Ha reconfigurado el switch conectado el equipo de Network Agent?

  Si la respuesta es afirmativa, consulte la *Guía de instalación* para verificar la configuración de su hardware y consulte *Configuración de Network Agent*, página 347,para verificar la configuración de Websense.

Si no se aplica ninguna de estas posibilidades, consulte *Cómo establecer la configuración local*, página 349,para obtener información sobre cómo asociar Network Agent y Filtering Service.

Actualización de la dirección IP o información UID de Filtering Service

Cuando Filtering Service fue instalado y reinstalado, Network Agent no actualiza automáticamente el identificador interno (UID) para el Filtering Service. Websense Manager intenta consultar Filtering Service usando el viejo UID, que ya no existe.

Del mismo modo, cuando cambia la dirección IP del equipo Filtering Service, este cambio no se registra automáticamente.

Para reestablecer conexión con Filtering Service:

1. Abra Websense Manager.

Un mensaje de estado le indica que una instancia Network Agent no puede conectarse con Filtering Service.

2. Haga clic en **Configuración** en la parte superior del panel de navegación de la izquierda.
3. En el panel izquierdo de navegación, en Network Agent, seleccione la dirección IP del equipo Network Agent.
4. En la parte superior de la página, en Definición de Filtering Service, abra la lista **Dirección IP del servidor** y seleccione la dirección IP del equipo de Filtering Service.
5. Haga clic en **Aceptar** en la parte inferior de la página para implementar la actualización. Los cambios no se producirán hasta que no haga clic en **Guardar todo**.

Problemas de identificación de usuarios

Temas relacionados:

- *Problemas de filtrado*, página 365
- *No se solicita a los usuarios remotos que realicen autenticación manual*, página 382
- *Los usuarios remotos no están siendo correctamente filtrados*, página 382

Si Websense está usando políticas de equipos o de redes o la política **Predeterminada**, para filtrar solicitudes de Internet, incluso luego de haber asignado políticas basadas en usuarios o grupos, o si se está aplicando una política de usuario o de grupo incorrecta, aplique los siguientes pasos para detectar el problema:

- Si está usando Microsoft ISA Server y cambió su método de autenticación, asegúrese de que el servicio proxy Web haya sido reiniciado.
- Si está utilizando grupos anidados en Windows Active Directory, las políticas asignadas a un grupo principal se aplican a los usuarios que pertenecen a un subgrupo, y no directamente al grupo principal. Para obtener información sobre jerarquías de usuarios y grupos, consulte la documentación del servicio de directorio.
- Es posible que el caché de User Service esté desactualizado. User Service almacena en caché desde los nombres de usuario hasta los mapeos de direcciones IP durante 3 horas. Puede hacer que la memoria caché de User Service se actualice guardando cualquier cambio de Websense Manager y haciendo clic en **Guardar todo**.
- Si el usuario que está siendo filtrado en forma incorrecta se encuentra en una máquina con Windows XP SP2, el problema puede deberse a Windows Internet Connection Firewall (ICF), incluido y habilitado de forma predeterminada en

Windows XP SP2. Para obtener más información sobre Windows ICF, consulte el artículo 320855 de la base de información de Microsoft.

Para que DC Agent o Logon Agent reciba información de inicio de sesión de los usuarios de una máquina con Windows XP SP2:

1. En el equipo cliente, seleccione el menú **Inicio** de Windows, **Configuración** > **Panel de control** > **Centro de seguridad** > **Firewall de Windows**.
2. Vaya a la ficha **Excepciones**.
3. Seleccione **Compartir archivos e impresora**.
4. Haga clic en **Aceptar** para cerrar el cuadro de diálogo ICF y cierre cualquier otra ventana abierta.

Si está usando un agente de identificación transparente de Websense, consulte la sección de solución de problemas correspondiente:

- *Solución de problemas de DC Agent*, página 373.
- *Solución de problemas de Logon Agent*, página 375.
- *Solución de problemas de eDirectory Agent*, página 378.
- *Solución de problemas de RADIUS Agent*, página 380.

Solución de problemas de DC Agent

Para solucionar problemas de identificación relacionados con DC Agent:

1. Verifique las conexiones de red.
2. Controle que no existan mensajes de error del visor de sucesos de Windows (consulte *El visor de sucesos de Windows*, página 402).
3. Controle el archivo de registro Websense (Websense.log) para obtener información de error detallada (consulte *El archivo de registro Websense*, página 402).

Entre las causas comunes de problemas de identificación de usuario de DC Agent se encuentran:

- Los servicios Network o Windows se están comunicando con un controlador de dominio de modo que DC Agent considera al servicio como un nuevo usuario a quien no se le ha definido ninguna política. Vea *Los usuarios no están siendo filtrados correctamente por la política predeterminada*, página 374.
- Es posible que DC Agent o User Service hayan sido instalados como servicios utilizando la cuenta de invitado, equivalente a un usuario anónimo para el controlador de dominio. Si se configuró el controlador de dominio para que no entregue la lista de usuarios y grupos a un usuario anónimo, DC Agent no puede descargar la lista. Vea *Cómo cambiar los permisos de DC Agent y User Service manualmente*, página 374.
- El caché de User Service esté desactualizado. User Service almacena en caché los mapeos de nombre de usuario y dirección IP durante 3 horas, de forma predeterminada. La memoria también se actualiza cada vez que efectúa cambios y hace clic en **Guardar todo** en Websense Manager.

Los usuarios no están siendo filtrados correctamente por la política predeterminada

Cuando alguna red o Microsoft Windows 200x se pone en contacto con el controlador de dominio, el nombre de la cuenta que usan puede provocar que Websense interprete que un usuario no identificado está accediendo a Internet desde un equipo filtrado. Dado que no se ha asignado una política basada en usuarios o grupos para este usuario, se aplica la política del equipo, de redes, o la política predeterminada

- Los servicios de red podrían requerir privilegios de dominio para acceder a datos en la red y utilizar el nombre de usuario de dominio que están aplicando para contactar al controlador de dominio.

  Para obtener información sobre este problema, consulte *Cómo configurar un agente para que ignore determinados nombres de usuarios*, página 235.

- Los servicios Windows 200x se comunican periódicamente con un controlador de dominio con un nombre de usuario que se forma a partir del nombre del equipo seguido por un signo de dólar (jdoe-equipo$). DC Agent interpreta el servicio como un usuario nuevo, para el cual no hay ninguna política asignada.

  Para obtener información sobre este problema, configure DC Agent para que ignore cualquier inicio de sesión del estilo **computer$**.

  1. En el equipo DC Agent, ingrese en el directorio **binario** Websense (por defecto, **C:\Program Files\Websense\bin**).
  2. Abra el archivo **transid.ini** en un editor de texto.
  3. Agregue la siguiente entrada al archivo:

     ```
     IgnoreDollarSign=true
     ```

  4. Guarde y cierre el archivo.
  5. Reinicie DC Agent (consulte *Cómo detener e iniciar los servicios Websense*, página 286).

Cómo cambiar los permisos de DC Agent y User Service manualmente

En el equipo que ejecuta el controlador de dominio:

1. Cree una cuenta de usuario con la denominación **Websense**. Puede utilizar una cuenta existente, pero es preferible usar una cuenta Websense de modo que pueda configurar la contraseña para que no caduque. No se requieren privilegios especiales.

   Configure la contraseña para que no caduque nunca. Esta cuenta sólo proporciona un contexto de seguridad para acceder a objetos de directorio.

   Tome nota del nombre de usuario y de la contraseña definidas para esta cuenta, dado que debe ingresarlas en los pasos 6 y 7.
2. Abra el cuadro de diálogo Windows Services en cada uno de los equipos Websense DC Agent (vaya a **Inicio > Programas > Herramientas administrativas > Servicios**).
3. Seleccione la entrada **Websense DC Agent** y haga clic en **Detener**.
4. Haga doble clic en la entrada **Websense DC Agent**.

5. En la ficha **Iniciar sesión**, seleccione la opción **Esta cuenta**.
6. Ingrese el nombre de usuario de la cuenta Websense DC Agent creada en el paso 1. Por ejemplo: **DomainName\websense**.
7. Especifique y confirme la contraseña de Windows para esta cuenta.
8. Haga clic en **Aceptar** para cerrar el cuadro de diálogo.
9. Seleccione la entrada **Websense DC Agent** en el cuadro de diálogo Servicios y haga clic en **Inicio**.
10. Repita este procedimiento para cada instancia de Websense User Service.

Solución de problemas de Logon Agent

Si alguno de los usuarios de su red son filtrados por la política **predeterminada** porque Logon Agent no es capaz de identificarlos:

- Asegúrese de que los objetos de la política de grupos de Windows (GPO) esté siendo aplicado correctamente en los equipos de los usuarios (consulte *Objetos de la política de grupos*, página 375).
- Si User Service está instalado en un equipo con Linux y está usando Windows Active Directory (modo nativo), verifique la configuración para el servicio de directorio (consulte *User Service con Linux*, página 376).
- Verifique que el equipo cliente pueda conectarse con el controlador de dominio desde el cual se ejecuta la secuencia de comandos de inicio de sesión (consulte *Visibilidad del controlador de dominio*, página 376).
- Asegúrese de que NetBIOS esté habilitado en el equipo cliente (consulte *NetBIOS*, página 377).
- Asegúrese de que el perfil de usuario en el equipo cliente no esté corrupto (consulte *Problemas de perfil de usuario*, página 377).

Objetos de la política de grupos

Luego de comprobar que su entorno cumple con los prerrequisitos que se describen en la *Guía de instalación* de Websense, asegúrese de que los objetos de la política de grupos sean correctamente aplicados:

1. En el equipo Active Directory, abra Panel de control y vaya a **Herramientas administrativas Tools > Active Directory Users y Computers**.
2. Haga clic con el botón secundario en la entrada de dominio y seleccione **Propiedades**.
3. Haga clic en la ficha **Política de grupo** y luego seleccione la política de dominio de la lista Group Domain Policy Objects Links.
4. Haga clic en **Editar**y expanda el nodo Configuración de usuario del árbol de directorios.
5. Expanda el nodo Configuración de Windows y seleccione **Scripts**.
6. En el panel de la derecha, haga doble clic en **Inicio de sesión**, y verifique que **logon.bat** aparezca en el cuadro de diálogo Propiedades de inicio de sesión.

Esta secuencia de comandos es requerida por la aplicación de inicio de sesión del cliente.

- Si **logon.bat** no está en la secuencia de comandos, consulte el capítulo *Configuración inicial* de la*Guía de instalación*de Websense.
- Si **logon.bat** aparece en la secuencia de comandos, pero Logon Agent no funciona, aplique los pasos adicionales para la solución de problemas de esta sección para verificar que no haya problemas de conectividad de redes, o consulte Knowledge Base de Websense.

User Service con Linux

Cuando usa Logon Agent para la identificación transparente de usuarios, y User Service está instalado en un equipo con plataforma Linux, deberá configurar temporariamente Websense para que se conecte con Active Directory en Modo mixto.

1. En Websense Manager, vaya a **Configuración > Servicios de directorio**.
2. Tome nota de las Configuración de su directorio actual.
3. En Directorios, seleccione **Windows NT Directory / Active Directory (Modo mixto**.
4. Haga clic en **Aceptar** para guardar los cambios y haga clic en **Guardar todo**.
5. En Directories, seleccione **Active Directory (modo nativo)**. Si su configuración original no aparece, use las notas efectuadas en el paso 2 para recrear las Configuración del directorio. Consulte *Windows Active Directory (modo nativo)*, página 63, para obtener instrucciones detalladas.
6. Una vez que termine con los cambios de configuración, haga clic en **Aceptar** y luego en **Guardar todo**.

Visibilidad del controlador de dominio

Para verificar que el equipo cliente pueda comunicarse con el controlador de dominio :

1. Intento de encontrar el mapa de una unidad en el equipo cliente hacia la unidad de raíz compartida del controlador de dominio. Aquí es donde normalmente se ejecuta la secuencia de comandos de sesión de inicio y donde reside **LogonApp.exe**.
2. En el equipo cliente, abra un símbolo del sistema Windows y ejecute el siguiente comando:

   ```
   net view /domain:<domain name>
   ```

Si alguno de estas pruebas falla, consulte la documentación relativa al sistema operativo Windows para obtener posibles soluciones. Hay un problema de conectividad con la red no relacionado con Websense.

NetBIOS

NetBIOS para TCP/IP debe estar habilitado y el servicio TCP/IP NetBIOS Helper debe estar funcionando para que la secuencia de comandos de inicio de sesión de Websense se ejecute en el equipo del usuario.

Para asegurarse de que NetBIOS para TCP/IP esté habilitado en el equipo cliente:

1. Haga clic con el botón secundario en **Mis sitios de red** y luego seleccione **Propiedades**.
2. Haga clic con el botón secundario en **Conexión de área local** y luego seleccione **Propiedades**.
3. Seleccione **Protocolo Internet (TCP/IP)** y luego haga clic en **Propiedades**.
4. Haga clic en **Opciones avanzadas**.
5. Seleccione la ficha **WINS** y verifique que se haya seleccionado la opción correcta de NetBIOS.
6. Si realiza un cambio, haga clic en **Aceptar** y luego en **Aceptar** dos veces más para cerrar los diferentes cuadros de diálogo de Propiedades y guardar los cambios.

   Si no fue necesario efectuar ningún cambio, haga clic en **Cancelar** para cerrar los cuadros de diálogo sin realizar cambios.

Use el cuadro de diálogo de Windows Services para verificar que el servicio **TCP/IP NetBIOS Helper** se esté ejecutando en el equipo cliente (consulte *El cuadro de diálogo de Windows Services*, página 402). El servicio TCP/IP NetBIOS Helper se ejecuta en Windows 2000, Windows XP, Windows Server 2003 y Windows NT.

Problemas de perfil de usuario

Si el perfil de usuario en el equipo cliente está corrupto, la secuencia de comandos de inicio de sesión de Websense (y las Configuración de Windows GPO) no puede ejecutarse. Este problema puede resolverse creando el perfil de usuario.

Cuando vuelve a crear un perfil de usuario, la carpeta Mis documentos, Favoritos y otros datos y Configuración personalizados existentes del usuario no se transfieren de forma automática al nuevo perfil. No elimine el perfil existente, corrupto hasta que haya verificado que el nuevo perfil resolvió el problema y copiado los datos existentes en un nuevo perfil.

Para volver a crear un perfil de usuario:

1. Inicie sesión en el equipo cliente como administrador local.
2. Asigne un nuevo nombre al directorio que contiene el perfil de usuario:

   ```
   C:\Documents and Settings\<user name>
   ```

3. Reinicie el equipo.
4. Inicie sesión en el equipo como usuario filtrado. Se crea automáticamente un nuevo perfil de usuario.
5. Verifique para asegurarse de que el usuario esté filtrado como se esperaba.

6. Copie los datos personalizados (como el contenido de la carpeta Mis documentos) del perfil viejo al nuevo. Evite usar el Asistente de transferencias de archivos y Configuración, ya que podría transferir la corrupción al nuevo perfil.

Solución de problemas de eDirectory Agent

Temas relacionados:

- *Habilitación de diagnóstico de eDirectory*, página 379
- *eDirectory Agent cometió un error al calcular las conexiones eDirectory Server*, página 379
- *Cómo ejecutar eDirectory Agent en el modo consola*, página 380

Un usuario podría no ser filtrado correctamente si el nombre del usuario no fue transferido a eDirectory Agent. Si un usuario no inicia sesión en el servidor Novell eDirectory, eDirectory Agent no puede detectar el inicio de sesión. Esto sucede porque:

- Un usuario inicia sesión en un dominio que no está incluido en el contexto root predeterminado para los inicios de sesión del usuario. Este contexto se especifica durante la instalación y debe coincidir con el contexto root especificado para Novell eDirectory en la página **Configuración** > **Servicios de directorio**.
- Un usuario trata de omitir la solicitud de inicio de sesión para sortear el filtrado de Websense.
- Un usuario no tiene cuenta configurada en el servidor eDirectory.

Si un usuario no inicia sesión en el servidor eDirectory, las políticas específicas de usuario no pueden aplicarse a ese usuario. En cambio, opera la política **predeterminada**. Si hay estaciones de trabajo compartidas en la red en las cuales los usuarios inician sesión de forma anónima, defina una política de filtrado para esos equipos en particular.

Para determinar si eDirectory Agent está recibiendo un nombre de usuario e identificando al usuario:

1. Active el inicio de sesión eDirectory Agent como se describe en *Habilitación de diagnóstico de eDirectory*, página 379.
2. Abra el archivo de registro especificado en un editor de texto.
3. Busque una entrada correspondiente al usuario que no esté siendo correctamente filtrado.
4. Cualquiera de las entradas que aparecen a continuación indican que eDirectory Agent identificó un usuario:

   ```
   WsUserData::WsUserData()
   Usuario: cn=Admin,o=novell (10.202.4.78)
   WsUserData::~WsUserData()
   ```

   En el ejemplo de arriba, el usuario **Admin** inició sesión en el servidor eDirectory y fue correctamente identificado.

5. Si un usuario es identificado, pero todavía no está siendo filtrado como se esperaba, controle la configuración de su política para verificar que se esté aplicando la política correspondiente al usuario y que el nombre de usuario de Websense Manager corresponda con el nombre de usuario de Novell eDirectory.

   Si el usuario *no* está siendo identificado, verifique que:

   - El usuario tenga una cuenta Novell eDirectory.
   - Un usuario está iniciando sesión en un dominio que está incluido en el contexto root predeterminado para los inicios de sesión de usuario eDirectory.
   - El usuario no está omitiendo una solicitud de inicio de sesión.

Habilitación de diagnóstico de eDirectory

eDirectory Agent tiene capacidades internas de diagnóstico, pero no están activadas de forma predeterminada. Podrá activar el inicio de sesión y la depuración durante la instalación, o en cualquier otro momento.

1. Detenga DC Agent (consulte *Cómo detener e iniciar los servicios Websense*, página 286).
2. En el equipo eDirectory Agent, vaya al directorio de instalación eDirectory Agent.
3. Abra el archivo **wsedir.ini** en un editor de texto.
4. Localice la sección **[eDirAgent]**.
5. Para activar el inicio de sesión y la depuración, cambie el valor **DebugMode** por **On**:

   ```
   DebugMode=On
   ```

6. Para especificar el nivel de detalle del registro, modifique la siguiente línea:

   ```
   DebugLevel=<N>
   ```

   N puede ser un valor de 0 a 3, donde 3 indica el mayor nivel de detalle.

7. Modifique la línea **LogFile** para especificar el nombre del archivo de salida de registro:

   ```
   LogFile=filename.txt
   ```

   De forma predeterminada, la salida del registro es enviada a la consola eDirectory Agent. Si está ejecutando el agente en el modo consola (consulte *Cómo ejecutar eDirectory Agent en el modo consola*, página 380), podrá mantener el valor predeterminado.

8. Guarde y cierre el archivo **wsedir.ini**.
9. Inicie el servicio eDirectory Agent (consulte *Cómo detener e iniciar los servicios Websense*, página 286).

eDirectory Agent cometió un error al calcular las conexiones eDirectory Server

Si eDirectory Agent está controlando a más de 1000 usuarios de su red, pero muestra sólo 1000 conexiones al servidor Novell eDirectory, podría estar produciéndose una

limitación de Windows API que transfiere información del servidor eDirectory al Websense eDirectory Agent. Esto ocurre muy rara vez.

Para resolver esta limitación, agregue un parámetro al archivo **wsedir.ini** que cuente las conexiones del servidor correctamente (sólo en Windows):

1. Detenga el servicio eDirectory Agent de Websense (consulte *Cómo detener e iniciar los servicios Websense*, página 286).
2. Vaya al directorio **binario** de Websense (de forma predeterminada, **C:\Archivos de programa\Websense\bin**).
3. Abra el archivo **wsedir.ini** en un editor de texto.
4. Inserte una línea en blanco y luego ingrese:

   ```
   MaxConnNumber = <NNNN>
   ```

   Aquí, <*NNNN*> es el valor máximo de conexiones posibles con el servidor Novell eDirectory. Por ejemplo, si la red tiene 1.950 usuarios, podría ingresar 2000 como cantidad máxima.
5. Guarde el archivo.
6. Reinicie eDirectory Agent.

Cómo ejecutar eDirectory Agent en el modo consola

1. Proceda con uno de los siguientes pasos:
   - En el símbolo del sistema Windows (**Start > Run > cmd**), ingrese el comando:

     ```
     eDirectoryAgent.exe -c
     ```
   - En la interfaz de línea de comandos de Linux, ingrese el comando:

     ```
     eDirectoryAgent -c
     ```
2. Cuando esté listo para detener el agente, presione **Enter**. Esta operación podría tardar unos segundos antes de que el agente se detenga.

Solución de problemas de RADIUS Agent

RADIUS Agent tiene capacidades internas de diagnóstico, pero no están activadas de forma predeterminada. Para activar el inicio de sesión y la depuración de RADIUS Agent:

1. Detenga el servidor RADIUS Agent (consulte *Cómo detener e iniciar los servicios Websense*, página 286).
2. En el equipo RADIUS Agent, vaya al directorio de instalación del agente (de forma predeterminada, **Websense\bin**).
3. Abra el archivo **wsradius.ini** en un editor de texto.
4. Localice la sección **[RADIUSAgent]**.
5. Para activar el inicio de sesión y la depuración, cambie el valor **DebugMode** por **On**:

   ```
   DebugMode=On
   ```

6. Para especificar el nivel de detalle del registro, modifique la siguiente línea:

   ```
   DebugLevel=<N>
   ```

   N puede ser un valor de 0 a 3, donde 3 indica el mayor nivel de detalle.

7. Modifique la línea **LogFile** para especificar el nombre del archivo de salida:

   ```
   LogFile=filename.txt
   ```

   De forma predeterminada, la salida del registro es enviada a la consola RADIUS Agent. Si está ejecutando el agente en el modo consola (consulte *Cómo ejecutar RADIUS Agent en el modo consola*, página 381), podrá, de forma optativa, mantener el valor predeterminado.

8. Guarde y cierre el archivo **wsradius.ini**.

9. Inicie el servicio RADIUS Agent (consulte *Cómo detener e iniciar los servicios Websense*, página 286).

Si hay usuarios remotos que no están siendo identificados y filtrados como se espera, la posible causa son los problemas de comunicación entre RADIUS Agent y su servidor RADIUS. Controle los registros de RADIUS Agent para detectar si hay errores y así determinar la causa.

Cómo ejecutar RADIUS Agent en el modo consola

Para iniciar RADIUS Agent en el modo consola (como una aplicación), ingrese lo siguiente:

- Abra un símbolo del sistema Windows:

  ```
  RadiusAgent.exe -c
  ```

- En la interfaz de línea de comandos de Linux:

  ```
  ./RadiusAgent -c
  ```

Para detener el agente en cualquier momento, presione **Enter** nuevamente. Esta operación podría tardar unos segundos antes de que el agente se detenga.

RADIUS Agent acepta los siguientes parámetros de la línea de comandos:

> **Nota**
> En Linux, Websense, Inc., recomienda usar la secuencia de comandos provista para iniciar o detener RADIUS Agent de Websense (**WsRADIUSAgent start|stop**), en lugar de los parámetros -r y -s.

Parámetro	Descripción
-i	Instala RADIUS Agent service/daemon.
-r	Ejecuta RADIUS Agent service/daemon.
-s	Detiene RADIUS Agent service/daemon.

Parámetro	Descripción
-c	Ejecuta RADIUS Agent como un proceso de aplicación en lugar de un servicio o daemon. En el modo consola, RADIUS Agent puede configurarse para enviar una salida de registro a la consola o a un archivo de texto.
-v	Muestra el número de versión de RADIUS Agent.
-? -h -ayuda <*sin opción*>	Muestra la información sobre el uso en la línea de comando. Detalla y describe todos los parámetros posibles de la línea de comandos.

No se solicita a los usuarios remotos que realicen autenticación manual

Si configuró los usuarios remotos para que realicen la autenticación manualmente al acceder a Internet, en algunas ocasiones, podría suceder que no se solicite la autenticación de usuarios individuales. Esto puede suceder en situaciones en las cuales algunas direcciones IP de la red fueron configuradas para omitir la autenticación manual.

Cuando un usuario remoto accede a la red, Websense lee la última porción de la dirección de Control de Acceso de Medios (MAC) del equipo. Si ésta coincide con la dirección IP de la red que fue configurada para omitir la autenticación manual, no se le pedirá al usuario remoto que realice la autenticación manual al acceder a Internet.

Una solución es reconfigurar la dirección IP de la red interna para utilizar la autenticación manual. Una solución alternativa es activar el requisito de autenticación manual para el usuario remoto afectado.

Los usuarios remotos no están siendo correctamente filtrados

Si los usuarios remotos no están siendo filtrados o no están siendo filtrados por las políticas particulares asignadas a ellos, controle los registros de RADIUS Agent para ver si existen mensajes de **Error de recepción provenientes del servidor: 10060** (Windows) o **Error de recepción desde el servidor: 0** (Linux).

Esto generalmente se produce cuando el servidor RADIUS no reconoce al RADIUS Agent como cliente (fuente de solicitudes RADIUS). Asegúrese de que su servidor RADIUS esté correctamente configurado (consulte *Cómo configurar el entorno de RADIUS*, página 221).

Puede usar la herramienta interna de diagnóstico de RADIUS Agent para solucionar problemas de filtrado (consulte *Solución de problemas de RADIUS Agent*, página 380).

Si implementó la función Remote Filtering (consulte *Filtrado de clientes remotos*, página 157), los usuarios remotos no pueden ser filtrados si e Remote Filtering Client no logra conectarse con Remote Filtering Server dentro de la red.

Para obtener instrucciones sobre cómo configurar Remote Filtering, consulte los documentos técnicos *Remote Filtering*.

Problemas de bloqueo de mensajes

No aparece ninguna página de bloqueo para un tipo de archivo bloqueado

Cuando se usa un bloqueo de tipo de archivo, el mensaje de bloqueo no siempre podría estar visible para el usuario. Por ejemplo, cuando un archivo descargable se encuentra dentro de un marco interno (IFRAME) en un sitio permitido, el mensaje de bloqueo enviado a ese marco no puede verse porque el tamaño del marco es cero.

Esto es un problema de visualización solamente; el usuario no puede acceder ni descargar el archivo bloqueado.

El usuario recibe un mensaje de error del navegador en lugar de página bloqueada

Si los usuarios reciben un mensaje de error en lugar de una página bloqueada, las 2 causas más probables son:

- El navegador del usuario está configurado para usar un proxy externo. En la mayoría de los navegadores existe un parámetro que permite usar un proxy externo. Verifique que el navegador no esté configurado para usar un proxy externo.
- Hay un problema para identificar o conectarse con el equipo Filtering Service.

Si las Configuración del navegador del usuario son correctas, asegúrese de que la dirección IP del equipo Filtering Service está correctamente enumerada en el archivo **eimserver.ini**.

1. Detenga **Websense Filtering Service** (consulte *Cómo detener e iniciar los servicios Websense*, página 286).
2. Vaya al directorio **binario** de Websense (de forma predeterminada, C:\Archivos de programa\Websense\bin or /opt/Websense/bin).

3. Abra el archivo **eimserver.ini** en un editor de texto.
4. En [WebsenseServer], agregue una línea en blanco e ingrese lo siguiente:

   ```
   BlockMsgServerName = <Filtering Service IP address>
   ```

   Por ejemplo, si la dirección IP de Filtering Service es 10.201.72.15, ingrese:

   ```
   BlockMsgServerName = 10.201.72.15
   ```

5. Guarde y cierre el archivo.
6. Reinicie Filtering Service.

Si el equipo Filtering Service tiene más de una NIC y la página de bloqueo aún no se visualiza correctamente luego de editar el archivo **eimserver.ini**, intente con las direcciones IP de los otras NIC en el parámetro **BlockMsgServerName**.

Si la página de bloqueo aún no se visualiza, asegúrese de que los usuarios hayan leído el acceso a los archivos en los directorios de la página de bloqueo de Websense:

- Websense\BlockPages\en\Default
- Websense\BlockPages\en\Custom

Si el problema con la página de bloque persiste, consulte Knowledge Base de Websense para obtener información adicional para la solución de problemas.

En lugar una página de bloqueo se muestra una página en blanco

Cuando se bloquean los anuncios, o cuando un navegador no detecta correctamente el cifrado asociado con una página de bloqueo, los usuarios podrían visualizar una página en blanco en lugar de una página de bloqueo. Las causas de esta conducta son:

- Cuando se encuentra bloqueada la categoría Publicidad, en ocasiones el software de Websense interpreta una solicitud de un archivo gráfico como una solicitud de un anuncio, y muestra una página en blanco en lugar de un mensaje de bloqueo (método normal para bloquear anuncios). Si la URL solicitada termina en .gif o de manera similar, el usuario debe ingresar nuevamente la URL sin la parte *.gif.
- Es posible que algunos navegadores antiguos no detecten el cifrado de las páginas de bloqueo. Para habilitar la detección adecuada de caracteres, configure el navegador para que muestre el juego de caracteres apropiado (UTF-8 para francés, alemán, italiano, español, portugués de Brasil, chino simplificado, chino tradicional o coreano; y Shift_JIS para japonés). Consulte la documentación del navegador para obtener instrucciones o actualizar el navegador a una versión más reciente.

No aparecen correctamente los mensajes de bloqueo de protocolo

Los mensajes de bloqueo de protocolo podrían no aparecer o aparecer de forma tardía por cualquiera de las siguientes causas:

- User Service debe estar instalado en el equipo Windows para que los mensajes de bloqueo de protocolo se visualicen correctamente. Para obtener más información, consulte la *Guía de instalación*.
- Los mensajes de bloqueo de protocolo podrían no llegar a los equipos cliente si Network Agent está instalado en un equipo con múltiples tarjetas de interfaz de red (NIC) y una NIC está controlando un segmento de red diferente que Filtering Service. Asegúrese de que el equipo Filtering Service tenga acceso de los protocolos NetBIOS y Server Message Block a los equipos cliente y de que el puerto 15871 no esté bloqueado.
- El mensaje de bloqueo de protocolo puede presentar un leve retraso o aparecer en un equipo interno donde se originaron los datos del protocolo solicitado (en lugar del equipo cliente) si Network Agent está configurado para supervisar solicitudes **enviadas a** a equipos internos.
- Si el cliente filtrado o el equipo de filtrado Websense está ejecutando Windows 200x, el servicio **Mensajero** de Windows debe estarse ejecutando para que se visualice el mensaje de bloqueo de protocolo. Utilice el cuadro de diálogo Windows Services del equipo cliente o servidor para verificar que se esté ejecutando el servicio Mensajero (consulte *El cuadro de diálogo de Windows Services*, página 402). Si bien el mensaje de bloqueo no aparece, las solicitudes de protocolo aún están bloqueadas.

Se visualiza un mensaje de bloqueo de protocolo en lugar de una página de bloqueo

Si su producto de integración no envía información HTTPS a Websense o si Websense se está ejecutando en modo autónomo, Network Agent podría interpretar una solicitud de sitio HTTPS que está bloqueada por medio de las Configuración de categoría como una solicitud de protocolo. Como resultado, se visualiza un mensaje de bloqueo de protocolo. La solicitud HTTPS también está registrada como solicitud de protocolo.

Problemas de registro, mensaje de estado y alerta

¿Dónde encuentro mensajes de error para los componentes de Websense?

En caso de error o advertencia relacionada con los componentes clave de Websense, se visualizan breves mensajes de alerta en la lista **Resumen de alertas de estado** en la parte superior de la página **Estado > Hoy** de Websense Manager (consulte *Alertas de Websense Health*, página 386).

- Haga clic en el mensaje de alerta para ver más información en la página **Estado > Alertas**.
- Haga clic en **Soluciones** junto al mensaje de la página Estado > Alertas para obtener asistencia para la solución de problemas.

Los errores, las advertencias y los mensajes de los componentes de Websense y los mensajes de estado de descarga de la base de datos se registran en el archivo **websense.log** del directorio **binario** de Websense (de forma predeterminada, C:\Archivos de programa\Websense\bin o /opt/Websense/bin). Vea *El archivo de registro Websense*, página 402.

Para los componentes de Websense instalados en los equipos Windows, también puede verificar el visor de sucesos de Windows . Vea *El visor de sucesos de Windows*, página 402.

Alertas de Websense Health

El resumen de alertas de estado de Websense proporciona una lista de los posibles problemas que puedan presentar los componentes supervisados de Websense. Entre ellos se incluyen:

- Filtering Service no está en ejecución
- User Service no está disponible
- Log Server no está en ejecución
- No hay ningún Log Server configurado para una Policy Server
- La base de datos de registro no está disponible
- Network Agent no está en ejecución
- No hay ningún Network Agent configurado para una Policy Server
- No se ha configurado ninguna NIC de supervisión para un Network Agent
- No se ha configurado ningún Filtering Service para un Network Agent
- La base de datos de filtrado inicial está en uso
- La base de datos principal se está descargando por primera vez
- La base de datos principal está siendo actualizada
- La base de datos principal tiene más de una semana de antigüedad
- No se descargó correctamente la base de datos principal
- WebCatcher no se ha activado
- Hay un problema de suscripción
- La clave de está suscripción está a punto de caducar
- No se ha especificado la clave de suscripción

Las páginas de alerta proporcionan información básica sobre cualquier situación de error o advertencia. Haga clic en **Soluciones** para obtener información sobre cómo solucionar este problema.

En algunos casos, si está recibiendo mensajes de error o estado sobre un componente que no está usando, o que está desactivado, podrá optar por ocultar los mensajes de alerta. Consulte *Cómo revisar el estado actual del sistema*, página 294, para más información.

Se generan dos registros para una misma solicitud

Cuando Windows QoS Packet Scheduler está instalado en el mismo equipo que Network Agent, se generan 2 registros para cada solicitud de HTTP o protocolo ingresada desde un equipo Network Agent. (Esta duplicación no ocurre con solicitudes efectuadas por los equipos cliente dentro de la red).

Para solucionar el problema, desactive Windows QoS Packet Scheduler en el equipo Network Agent.

Este problema no se produce si utiliza Network Agent para todos los inicios de sesión. Consulte *Cómo establecer la configuración de NIC*, página 351, para más información.

Problemas de Policy Server y Policy Database

Olvidé mi contraseña

Si usted es Super Administrator o administrador delegado y utiliza una cuenta de usuario Websense para iniciar sesión en Policy Server vía Websense Manager, cualquier Super Administrador incondicional puede restaurar la contraseña.

- La contraseña WebsenseAdministrator se define desde la página **Configuración > Cuentas**.
- Otras contraseñas de cuenta de administrador se definen desde la página **Administración delegada > Administrar cuentas de usuario de Websense**.

Si no está usando administración delegada y olvidó su contraseña de WebsenseAdministrator, inicie sesión en MyWebsense para restaurar la contraseña.

- La clave de suscripción asociada con la cuenta MyWebsense debe coincidir con su clave de suscripción Websense Web Security o Websense Web Filter actual.
- Si tiene múltiples claves de suscripción, debe seleccionar la clave apropiada de Websense Web Security o Websense Web Filter para que el proceso de restauración de contraseña sea satisfactorio.
- Debe tener acceso al equipo Websense Manager para completar el proceso de restauración.

No puedo iniciar sesión en Policy Server

Verifique que la dirección IP de Policy Server seleccionada sea correcta. Si la dirección del equipo Policy Server cambió desde que se agregó Policy Server a Websense Manager, deberá iniciar sesión en un Policy Server diferente, eliminar la vieja dirección IP de Websense Manager y agregar una nueva dirección IP de Policy Server. Vea *Cómo agregar y editar instancias de Policy Server*, página 278.

Si Websense Manager deja de funcionar inesperadamente, o bien ha sido detenido mediante los comandos kill (Linux) o End Task (Windows), espere unos minutos antes de volver a iniciar sesión. Websense detecta y cierra la sesión finalizada dentro de los 3 minutos.

El servicio Websense Policy Database no se inicia

La Websense Policy Database se ejecuta como una cuenta especial: **WebsenseDBUser**. Si esta cuenta presenta problema de inicio de sesión, la Policy Database no puede iniciarse.

Para resolver este problema, cambie la contraseña WebsenseDBUser.

1. Inicie sesión en el equipo Policy Database como administrador local.
2. Vaya a **Inicio > Programas > Herramientas administrativas > Administración de equipos**.
3. En el panel de navegación, en Herramientas del sistema, expanda **Grupos y usuarios locales** y luego seleccione **Usuarios**. En el panel de contenido se muestra la información de usuario.
4. Haga clic con el botón secundario en **WebsenseDBUser** y seleccione **Set Password**.
5. Especifique y confirme la nueva contraseña para esta cuenta de usuario y haga clic en **Aceptar**.
6. Cierre el cuadro de diálogo Administración de equipos.
7. Vaya a **Inicio > Programas > Herramientas administrativas > Servicios**.
8. Haga clic con el botón secundario en **Websense Policy Database** y seleccione **Propiedades**.
9. En la ficha de Iniciar sesión del cuadro de diálogo Properties, ingrese la nueva información de la contraseña WebsenseDBUser y haga clic en **Aceptar**.
10. Haga clic nuevamente con el botón secundario en Websense Policy Database y seleccione **Inicio**.

    Una vez iniciado el servicio, cierre el cuadro de diálogo Servicios.

Problemas de administración delegada

- *Los clientes administrados no pueden ser eliminados del rol*, página 389

Los clientes administrados no pueden ser eliminados del rol

Los clientes no pueden ser eliminados directamente de la lista de clientes administrados de la página moficar rol de Administración delegada >si:

- el administrador aplicó una política al cliente
- el administrador aplicó una política a uno o más miembros de una red, grupo, dominio o unidad organizativa

También puede haber problemas si, durante el inicio de sesión de Websense Manager, el Super Administrator opta por un Policy Server diferente que el que se conecta con el servicio de directorio que contiene los clientes que deben eliminarse. En este caso, el Policy Server y el servicio de directorio actuales no reconocen a los clientes.

Para obtener ayuda sobre cómo eliminar clientes administrados, consulte *Cómo eliminar clientes administrados*, página 264.

El error de inicio de sesión indica que otra persona inició sesión en Mi PC

Cuando intenta iniciar sesión en Websense Manager podría recibir el mensaje de error “Error en el inicio de sesión. El rol <nombre de rol> fue utilizado por <nombre de usuario>, desde<fecha, hora>, en el equipo 127.0.0.1.” La dirección de IP 127.0.0.1 también es denominada dirección bucle y típicamente indica que se trata del equipo local.

Este mensaje indica que alguien inició sesión en el equipo de instalación Websense Manager, con el mismo rol que usted está solicitando. Puede seleccionar un rol diferente (si administra roles múltiples), iniciar sesión únicamente para emitir informes o esperar hasta que el otro administrador cierre la sesión.

Algunos usuarios no pueden acceder a un sitio de la lista de URL sin filtrar

Las URL sin filtrarsólo afectan a los clientes administrados por el rol al cual se agregan las URL. Por ejemplo, si un superadministrador agrega URL sin filtrar, los clientes administrados por los roles de administración delegados no obtienen acceso a esos sitios.

Para que el sitio esté disponible para clientes de otros roles, el superadministrador no puede cambiar a cada rol y agregar los sitios relevantes a esa lista de URL sin filtrar del rol.

Los sitios recategorizados son filtrados según la categoría incorrecta

Las URL recategorizadas sólo afectan a los clientes administrados por el rol al cual se agregan las URL. Por ejemplo, cuando un superadministrador recategoriza las URL, los clientes administrados por los roles de administración delegados continúan siendo filtrados según la categoría de Master Database para esos sitios.

Para aplicar la recategorización a los clientes en otros roles, el superadministrador puede cambiar cada uno de los roles y recategorizar los sitios para ese rol.

No puedo crear un protocolo personalizado

Sólo los superadministradores pueden crear protocolos personalizados. Sin embargo, los administradores delegados pueden definir acciones de filtrado para los protocolos personalizados.

Cuando los superadministradores crean protocolos personalizados deben definir las acciones predeterminadas adecuadas para la mayoría de los clientes. Luego, deberá informar a los administradores delegados sobre el nuevo protocolo de modo que puedan actualizar los filtros para sus roles, según corresponda.

Problemas de emisión de informes

Log Server no está en ejecución.

Si Log Server no está en ejecución o si otros componentes de Websense no pueden comunicarse con Log Server, no se almacena la información de uso de Internet y es posible que no pueda generar informes sobre el uso de Internet.

Es posible que Log Server no esté disponible si:

- No hay espacio suficiente en el disco del equipo Log Server.
- Cambió la contraseña de Microsoft SQL Server o MSDE sin actualizar la configuración de ODBC o Log Server.
- Han transcurrido más de 14 días desde que la base de datos principal se descargó correctamente.
- Falta el archivo logserver.ini o el archivo está corrupto.
- Detuvo el servicio de Log Server para evitar registrar información sobre el uso de Internet.

Para solucionar el problema:

- Verifique la cantidad de espacio libre en disco y, si hace falta, elimine archivos innecesarios.
- Si considera que el problema se debe a un cambio de contraseña, consulte *Cómo actualizar la contraseña de la conexión de Log Server*, página 395.
- Ingrese al directorio **binario** de Websense (C:\Archivos de programa\Websense\bin, por defecto) y verifique que puede abrir **logserver.ini** en un editor de texto. Si este archivo estuviera corrupto, reemplácelo con un archivo de respaldo.
- Controle el cuadro de diálogo Servicios de Windows para verificar que se haya iniciado Log Server y reinicie el servicio si fuera necesario (consulte *Cómo detener e iniciar los servicios Websense*, página 286).
- Verifique el visor de sucesos de Windows y el archivo **websense.log** para determinar si existen mensajes de error de Log Server (consulte *Herramientas para la solución de problemas*, página 401).

No hay ningún Log Server instalado para un Policy Server

Log Server de Websense recolecta y almacena información de uso de Internet en la Log Database para ser utilizada en informes de investigación, informes de

presentación y cuadros y resúmenes de las páginas Hoy e Historial de Websense Manager.

Log Server debe estar instalado para que se produzca la generación de informes.

Podría ver este mensaje si:

- Log Server está instalado en un equipo diferente que Policy Server y la dirección IP de Log Server está incorrectamente definida para actuar como host local de Websense Manager.
- Log Server está instalado en el equipo Linux.
- No está usando las herramientas de generación de informes de Websense.

Para verificar que la dirección IP definida para Log Server en Websense Manager sea correcta:

1. Seleccione la ficha **Configuración** del panel de navegación de la izquierda y luego vaya a **Registro > General**.
2. Ingrese la dirección IP del equipo Log Server en el campo **Nombre o Dirección IP del Log Server**.
3. Haga clic en **Aceptar** para guardar los cambios y haga clic en **Guardar todo**.

Si el Log Server está instalado en un equipo Linux, o si no está usando las herramientas de generación de informes de Websense, puede ocultar el mensaje de alerta de Websense Manager.

1. En la ficha Principal del panel de navegación de la izquierda, vaya a **Estado > Alertas**.
2. En Alertas activas, haga clic en **Opciones avanzadas**.
3. Marque **Ocultar esta alerta** para el mensaje "No hay instalado un Log Server".
4. Haga clic en **Guardar ahora**. El cambio se implementa inmediatamente.

La base de datos de registro no fue creada

A veces, el instalador no puede crear la base de datos de registro. La siguiente lista describe la mayoría de las causas y soluciones comunes.

Problema:	Existe un archivo o algunos archivos que usan los nombres que Websense usa para la base de datos de registro (wslogdb70 y wslogdb70_1), pero los archivos no están correctamente conectados al motor de la base de datos, de modo que no pueden ser usados por el instalador de Websense.
Solución:	Eliminar o renombrar los archivos existentes y luego ejecute nuevamente el instalador.
Problema:	La cuenta usada para iniciar la sesión para la instalación tiene permisos inadecuados en la unidad en la cual se está instalando la base de datos.

Solución:	Actualice la cuenta de inicio de sesión para tener permisos de lectura y escritura para la ubicación de instalación o iniciar sesión con una cuenta diferente que ya tiene estos permisos. A continuación, ejecute de nuevo el instalador.
Problema:	No hay espacio suficiente en disco disponible para crear y mantener la base de datos de registro en la ubicación especificada.
Solución:	Libere espacio en el disco seleccionado para instalar y mantener la base de datos de registro. A continuación, ejecute de nuevo el instalador. De lo contrario, elija otra ubicación.
Problema:	La cuenta utilizada para iniciar la sesión para la instalación tiene permisos SQL Server inadecuados para crear la base de datos.
Solución:	Actualice la cuenta de inicio de sesión o inicie sesión con una cuenta que ya tenga los permisos requeridos. A continuación, ejecute de nuevo el instalador. Los permisos requeridos dependen de la versión de Microsoft SQL Server: ■ SQL Server 2000 o MSDE: permisos **dbo** (propietario de la base de datos) requeridos ■ SQL Server 2005: permisos **dbo** y **SQLServerAgentReader** requeridos

La base de datos de registro no está disponible

La base de datos de registro de Websense almacena información de uso de Internet para ser utilizada en informes de presentación, informes de investigación y cuadros y resúmenes en las páginas Hoy e Historial de Websense Manager.

Si Websense no puede conectarse a la base de datos de registro, verifique en primera instancia que el motor de la base de datos (Microsoft SQL Server o Microsoft SQL Server Desktop Engine [MSDE]) esté ejecutándose en el equipo base de datos de registro.

1. Abra el cuadro de diálogo Servicios de Windows (consulte *El cuadro de diálogo de Windows Services*, página 402) y verifique que los siguientes servicios estén ejecutándose:
   - Microsoft SQL Server:
     - MSSQLSERVER
     - SQLSERVERAGENT
   - Microsoft SQL Desktop Engine (MSDE):
     - MSSQL$WEBSENSE (si adquirió MSDE de Websense, Inc.)
     - SQLAgent$WEBSENSE
2. Si el servicio se ha detenido, haga clic con el botón secundario en el nombre del servicio y haga clic en **Inicio**.

Si el servicio no se reinicia, verifique el visor de sucesos de Windows (consulte *El visor de sucesos de Windows*, página 402) para Microsoft SQL Server o MSDE para controlar que no existan mensajes de error o advertencia.

Si el motor de la base de datos está ejecutándose:

- Asegúrese de que SQL Server Agent esté ejecutándose en el equipo que opera el motor de la base de datos.
- Use el cuadro de diálogo Windows Services para verificar que el servicio **Websense Log Server** se esté ejecutando.
- Si Log Server y la base de datos de registro están instalados en diferentes equipos, asegúrese de que ambos equipos estén funcionando y de que la conexión de red entre los equipos no haya sido afectada.
- Asegúrese de tener espacio suficiente en el disco del equipo base de datos de registro y de que la base de datos de registro tenga cantidad de espacio asignado en disco suficiente (consulte *Log Server no está grabando datos en la base de datos de registro*, página 394).
- Asegúrese de que no se hayan cambiado las contraseñas de Microsoft SQL Server o MSDE. Si la contraseña cambia deberá actualizar la información de la contraseña que usa Log Server para conectarse con la base de datos. Vea *Cómo actualizar la contraseña de la conexión de Log Server*, página 395.

Tamaño de la base de datos de registro

El tamaño de la base de datos de registro siempre es un problema. Si viene generando informes Websense de forma adecuada y nota que los informes ahora tardan más tiempo en aparecer, o comienza a recibir mensajes de caducidad de tiempo del navegador Web, considere desactivar algunas de las particiones de la base de datos.

1. En Websense Manager, vaya a **Configuración > Informes >Base de datos de registro**.
2. Ubique la sección **Particiones disponibles** de la página.
3. Elimine del cuadro de diálogo **Activar** cualquier partición que no sea requerida por las operaciones de generación de informes actuales.
4. Haga clic en **Guardar ahora** para implementar el cambio.

Log Server no está grabando datos en la base de datos de registro

Generalmente, cuando Log Server no puede escribir datos en la base de datos de registro se debe a que la base de datos no tiene espacio suficiente en disco. Esto se puede producir si la unidad de disco está llena, o en caso de que Microsoft SQL Server, si hay un tamaño máximo establecido para el incremento de la base de datos.

Si la unidad de disco que alberga la base de datos de registro está llena, deberá liberar espacio en disco para que la máquina pueda reestablecer el registro.

Si su administrador de base de datos de SQL Server definió un tamaño máximo de incremento para la base de datos individual dentro de Microsoft SQL Server, aplique alguno de los siguientes procedimientos:

- Contacte a su administrador de base de datos de SQL Server para incrementar el máximo.
- Encuentre cuál es el tamaño máximo y vaya a **Configuración > Informes >Base de datos de registro** para configurar la base de datos de registro para que reinicie cuando alcance aproximadamente el 90% del tamaño máximo. Vea *Configuración de opciones de reinicio de datos*, página 327.

Si el departamento de Tecnología informática definió una cantidad máxima de espacio en disco para las operaciones de SQL Server, contáctese con soporte.

Cómo actualizar la contraseña de la conexión de Log Server

Si cambia la contraseña de la cuenta que Websense usa para conectarse con la base de datos de registro, también debe actualizar Log Server para que use la nueva contraseña.

1. En el equipo Log Server, vaya a **Inicio > Programas > Websense >Utilitidades > Configuración de Log Server**. Se abre la utilidad Configuración de Log Server.
2. Haga clic en la ficha **Base de datos** y verifique que la base de datos correcta (de forma predeterminada, **wslogdb70**) se visualice en el campo ODBC Data Source Name (DSN).
3. Haga clic en **Conexión**. Se abre el cuadro de diálogo Seleccionar origen de datos.
4. Haga clic en la ficha **Origen de datos de máquina** y luego doble clic en **wslogdb70** (o su nombre de base de datos de registro). Se abre el cuadro de diálogo Inicio de sesión de SQL Server.
5. Asegúrese de que el campo LoginID contenga el nombre de cuenta correcto (generalmente, **sa**) y luego ingrese la nueva contraseña.
6. Haga clic en **Aceptar**, a continuación, en el cuadro de diálogo Configuración de Log Server, haga clic en **Aplicar**.
7. Seleccione la ficha **Conexión** y detenga y reinicie Log Server.
8. Cuando Log Server esté ejecutándose nuevamente, haga clic en **Aceptar** para cerrar la utilidad.

Cómo configurar los permisos de usuario para Microsoft SQL Server 2005

Microsoft SQL Server 2005 define los roles SQL Server Agent que controlan la accesibilidad del entorno de la tarea. Las tareas de SQL Server Agent para SQL Server 2005 se almacenan en la base de datos msdb SQL Server.

Para instalar correctamente Log Server de Websense, la cuenta de usuario que es propietaria de la base de datos Websense debe guardar pertenencia a uno de los siguientes roles de la base de datos msdb:

- SQLAgentUserRole
- SQLAgentReader Role
- SQLAgentOperator Role

> **Nota**
> La cuenta de usuario SQL también debe guardar pertenencia con el rol del servidor fijo *DBCreator*.

Ingrese en Microsoft SQL Server 2005 para otorgar los permisos necesarios a la cuenta de usuario SQL Server para instalar correctamente los componentes de generación de informes Websense.

1. En el equipo SQL Server, vaya a **Inicio > Programas > Microsoft SQL Server 2005 > Microsoft SQL Server Management Studio**.
2. Seleccione el árbol **Explorador de objetos**.
3. Seleccione **Seguridad > Inicios de sesión**.
4. Seleccione la cuenta de inicio de sesión a ser utilizada durante la instalación.
5. Haga clic con el botón secundario en la cuenta de inicio de sesión y seleccione **Propiedades** para este usuario.
6. Seleccione **Asignación de usuario** y siga estos pasos:
   a. Seleccione **msdb** en el mapa de la base de datos.
   b. Otorgue pertenencia a uno de estos roles:
      - SQLAgentUserRole
      - SQLAgentReader Role
      - SQLAgentOperator Role
   c. Haga clic en **Aceptar** para guardar los cambios.
7. Seleccione **Funciones de servidor** y luego **dbcreator**. Se crea el rol dbcreator.
8. Haga clic en **Aceptar** para guardar los cambios.

Log Server no puede conectarse con el servicio de directorio

Si se produce alguno de los errores que se detallan abajo, Log Server no podrá acceder al servicio de directorio, que es necesario para actualizar los mapas usuario a grupo para los informes. Estos errores se visualizan en el visor de sucesos de Windows (consulte *El visor de sucesos de Windows*, página 402).

- EVENT ID:4096 - No es posible inicializar Directory Service. Puede que Websense Server esté desactivado o sea inaccesible.
- EVENT ID:4096 – No pudo conectarse con el servicio de directorio. Los grupos para este usuario no se resolverán en este momento. Verifique que este proceso pueda acceder al servicio de directorio.

La causa más común es que Websense Log Server y Websense User Service están en diferentes lados de un firewall que está limitando el acceso.

Para resolver este problema, configure el firewall para permitir el acceso sobre los puertos utilizados para la comunicación entre estos componentes.

Los datos de los informes de tiempo del navegador de Internet están desviados

Tenga en cuenta que la consolidación podría desviar los datos para los informes de tiempo del navegador de Internet. Estos informes muestran el tiempo que los usuarios tardaron en acceder a Internet y pueden incluir detalles sobre el tiempo que estuvo navegando en cada sitio. El tiempo de navegación en Internet se calcula usando un algoritmo especial y el hecho de permitir la consolidación podría desviar la precisión de los cálculos de estos informes.

El ancho de banda es mayor de lo esperado

Muchas, pero no todas, las integraciones de Websense proporcionan información de ancho de banda. Si su integración no proporciona información de ancho de banda, puede configurar Network Agent para que realice el registro de modo que incluya la información sobre el ancho de banda.

Cuando un usuario solicita la descarga permitida de un archivo, el producto de integración o Network Agent envía el tamaño total del archivo, que Websense registra como bytes recibidos.

Si el usuario posteriormente cancela la descarga actual, o el archivo no se descarga completamente, el valor de los bytes recibidos en la base de datos de registro aún representa el tamaño total del archivo. En estas circunstancias, los bytes registrados como recibidos superarán la cantidad de bytes efectivamente recibidos.

Esto también afecta a los valores de ancho de banda registrados, que representan una combinación de los bytes recibidos y los bytes enviados.

No se están registrando algunas solicitudes de protocolos

Algunos protocolos, como los que utilizan ICQ y AOL, les solicitan a los usuarios que se inicie sesión en un servidor con una dirección IP y luego envían un número de puerto y una dirección IP de identificación diferentes al cliente para fines de mensajería. En este caso, es posible que no todos los mensajes enviados y recibidos sean supervisados y registrados por Websense Network Agent, dado que el servidor de mensajería es desconocido en el momento en que se intercambian los mensajes.

Como resultado, es posible que la cantidad de solicitudes registradas no coincida con la cantidad real de solicitudes enviadas. Esto influye en la exactitud de los informes generados por las herramientas de generación de informes de Websense.

Todos los informes están vacíos

Si no hay datos para ninguno de sus informes asegúrese de que:

- Las particiones de la base de datos activa incluye información para las fechas incluidas en los informes. Vea *Particiones de la base de datos*, página 398.
- La tarea de SQL Server Agent está activa en Microsoft SQL Server o MSDE. Vea *tarea de SQL Server Agent*, página 398.
- Log Server está correctamente configurado para recibir información de registro de Filtering Service. Vea *Configuración de Log Server*, página 398.

Particiones de la base de datos

Los informes de registro de Websense están almacenados en particiones dentro de la base de datos. Se pueden crear nuevas particiones basadas en el tamaño y la fecha, dependiendo de su configuración y motor de base de datos.

Puede activar o desactivar particiones individuales en Websense Manager. Si intenta generar un informe sobre la base de información almacenada en particiones desactivadas, no encontrará información y el informe estará vacío.

Para asegurarse de que las particiones de la base de datos apropiada están activas:

1. Vaya a **Configuración > Informes >Base de datos de registro**.
2. Navegue por la sección **Particiones disponibles**.
3. Marque el cuadro de diálogo **Activar** para cada partición que contenga datos a ser incluidos en los informes.
4. Haga clic en **Guardar ahora** para implementar el cambio.

tarea de SQL Server Agent

Es posible que la tarea de la base de datos SQL Server Agent haya sido desactivada. Esta tarea debe estar siendo ejecutada para que los informes de registro sea procesados en la base de datos por la tarea de base de datos ETL.

Si está ejecutando MSDE:

1. Vaya a **Inicio > Herramientas administrativas > Servicios**.
2. Asegúrese de que ambos servicios, SQL Server y SQL Server Agent, hayan sido iniciados. Si obtuvo MSDE de Websense, Inc., estos servicios se denominan MSSQL$WEBSENSE y SQLAgent$WEBSENSE.

Si está ejecutando Microsoft SQL Server completo, pídale a su Administrador de la base de datos que se asegure de que la tarea SQL Server Agent se esté ejecutando.

Configuración de Log Server

Las Configuración de Configuracióndeben ser correctas para que Websense Manager y Log Server se aseguren de que Log Server recibe información de registro de

Filtering Service. De lo contrario, los datos de registro nunca son procesados en la base de datos de registro.

En primer lugar, verifique que Websense Manager esté correctamente conectado con Log Server.

1. Inicie sesión en Websense Manager con permisos de superadministrador incondicionales.
2. Vaya a **Inicio > General >Registro**.
3. Ingrese en **nombre del equipo** o **dirección IP** donde está ubicado Log Server.
4. Ingrese en el **puerto** que Log Server está oyendo en (el predeterminado es 55805).
5. Haga clic en **Comprobar estado** para determinar si Websense Manager puede comunicarse con el Log Server especificado.

   Un mensaje indica si la prueba de conexión es satisfactoria. Actualice la dirección IP o el nombre del equipo y el puerto, si fuera necesario, hasta que la prueba sea correcta.
6. Cuando haya terminado, haga clic en **Aceptar** para guardar los cambios. Los cambios no se producirán hasta que no haga clic en **Guardar todo**.

Luego, verifique las Configuración de la utilidad Configuración de Log Server.

1. En el equipo en el que se está ejecutando Log Server, vaya a **Inicio > Programas > Websense >Utilidades > Configuración de Log Server**.
2. En la ficha **Conexiones**, verifique que el puerto coincida con el valor ingresado en Websense Manager.
3. Haga clic en **Aceptar** para guardar los cambios.
4. Use el botón de la ficha **Conexiones** para detener y luego iniciar Log Server.
5. Haga clic en **Salir** para cerrar la utilidad Configuración de Log Server.

No aparece ningún cuadro en las páginas Hoy o Historial

En aquellas organizaciones que usan administración delegada, revise los permisos de generación de informes para el rol de administrador delegado. Si **Ver informes en las páginas Hoy e Historial** no está seleccionado, este cuadro no aparece con respecto a los administradores delegados en ese rol.

En entornos que usan múltiples Policy Servers, el Log Server está instalado para comunicarse con un único Policy Server. Deberá iniciar sesión en ese Policy Server para ver los cuadros en las páginas Hoy e Historial, o para acceder a otras funciones de la generación de informes.

No puede acceder a ciertas funciones de generación de informes

Si su navegador Web tiene bloqueo de elementos emergentes con una configuración muy estricta, podría bloquear ciertas funciones de la generación de informes. Para

usar esas funciones, deberá disminuir el nivel de bloqueo o desactivar completamente el bloqueo de elementos emergentes.

Faltan algunos datos de informe para la salida de Microsoft Excel

La mayor cantidad de filas que pueden abrirse en una hoja de cálculo de Microsoft Excel es de 65.536. Si exporta un informe con más de 65.536 registros a formato Microsoft Excel, el registro número 65.537 y los siguientes no estarán disponibles en esta hoja de cálculo.

Para asegurarse de poder acceder a toda la información del informe exportado, siga uno de los siguientes pasos:

- Para la presentación de informes, edite el filtro informe para definir un informe más pequeño, quizás estableciendo un rango de fecha más corto, seleccionando menos usuarios o grupos o seleccionando menos acciones.
- Para los informes de investigación, reduzca los datos para definir un informe más pequeño.
- Seleccione un formato de exportación diferente.

Cómo guardar la salida de los informes de presentación en HTML

Si genera un informe directamente desde la página Generación de informes > Informes de presentación, puede seleccionar alguno de los 3 formatos de visualización que aparecen a continuación: HTML, PDF y XLS. Si selecciona el formato de visualización HTML, podrá ver el informe en la ventana de Websense Manager.

No es recomendable imprimir y guardar informes de presentación desde el navegador. La salida impresa incluye la totalidad de la ventana del navegador y, al abrirla, un archivo almacenado abre Websense Manager.

Para imprimir o guardar informes de forma más efectiva, seleccione PDF o XLS como formato de salida. Puede abrir estos tipos de archivo inmediatamente si el software para visualizarlos (Adobe Reader o Microsoft Excel) está instalado en el equipo local. También puede guardar el archivo en un disco (la única opción si el software de visualización no está disponible).

Luego de abrir un informe en Adobe Reader o Microsoft Excel, use el mismo programa para imprimir y guardar las opciones para obtener la salida final deseada.

Problemas de búsqueda de los informes de investigación

Hay dos problemas potenciales relacionados con la búsqueda de informes de investigación.

- No se pueden ingresar caracteres extendidos de ASCII

- Puede no encontrarse el patrón de búsqueda

Caracteres ASCII extendidos

Los campos Buscar que se encuentran arriba del cuadro de barra en la página principal de informes de investigación le permite buscar un término o cadena de texto específico en el elemento de cuadro seleccionado.

Si está usando Mozilla Firefox en un servidor Linux para acceder a Websense Manager, no podrá ingresar caracteres ASCII extendidos en estos campos. Esto se conoce como limitación de Firefox en Linux.

Si necesita buscar un informe de investigación para una cadena de texto que incluye caracteres ASCII extendidos, acceda a Websense Manager desde un servidor Windows usando cualquier navegador compatible.

Patrón de búsqueda no encontrado

En algunos casos, los informes de investigación no logran encontrar las URL asociadas con un patrón ingresado en los campos Search de la página principal de informes de investigación. Si esto ocurre, y si tiene razonable certeza de que el patrón existe dentro de la URL registrada, intente ingresar un patrón diferente que también pueda encontrar la URL deseada.

Problemas generales con los informes de investigación

- Algunas consultas demoran mucho tiempo. Es posible que la pantalla se ponga en blanco o que se muestre un mensaje indicando que se ha excedido el tiempo de espera de la consulta. Esto puede ocurrir por los siguientes motivos:
  - Caducó el tiempo del servidor Web
  - Caducó el tiempo de MSDE o Microsoft SQL Server
  - Caducó el tiempo de espera del servidor proxy y caché

  Es posible que deba aumentar manualmente el límite del tiempo de espera para estos componentes.
- Si los usuarios no corresponden a ningún grupo, tampoco figurarán en un dominio. Las opciones Grupo y Dominio estarán inactivas.
- Aunque Log Server esté registrando visitas en lugar de accesos, los informes de investigación clasificarán la información como **Hits**.

Herramientas para la solución de problemas

- *El cuadro de diálogo de Windows Services*, página 402
- *El visor de sucesos de Windows*, página 402
- *El archivo de registro Websense*, página 402

El cuadro de diálogo de Windows Services

En los equipos Microsoft Windows, Filtering Service, Network Agent, Policy Server, User Service y todos los agentes de identificación transparente Websense se ejecutan como servicios. Puede usar el cuadro de diálogo de Windows Services para verificar el estado de estos servicios.

1. En Windows Control Panel, abra la carpeta **Herramientas administrativas**.
2. Haga doble clic en **Servicios**.
3. Navegue por la lista de servicios para encontrar el servicio para el cual requiere solución de problemas.

   La entrada de servicio incluye el nombre del servicio, una breve descripción del servicio, el estado del servicio (iniciado o detenido), cómo se inicia el servicio y qué cuenta usa el servicio para realizar estas tareas.
4. Haga doble clic en un nombre de servicio para abrir un cuadro de diálogo de propiedades con información más detallada sobre el servicio.

El visor de sucesos de Windows

El visor de sucesos de Windows registra mensajes de error sobre los eventos de Windows, incluidas las actividades de servicio. Estos mensajes pueden ayudarlo a identificar los errores de red o servicio que podrían estar causando un filtrado de Internet o problemas de identificación de usuarios.

1. En el panel de control de Windows, abra la carpeta **AHerramientas administrativas**.
2. Haga doble clic en **Visor de sucesos de Windows**.
3. En el visor de sucesos, haga clic en **Aplicación** para obtener un lista de mensajes de error, advertencias y mensajes informativos.
4. Navegue por la lista para identificar los errores o advertencias de los servicios Websense.

El archivo de registro Websense

Websense escribe los mensajes de error en el archivo **websense.log**, ubicado en el directorio **binario** Websense (de forma predeterminada, C:\Archivos de programa\Websense\bin o /opt/Websense/bin).

La información de este archivo es comparable con la que se encuentra en el Visor de sucesos de Windows. En los entornos Windows, el Visor de sucesos presenta mensajes en un formato más amigable para el usuario. No obstante, el archivo **websense.log**, está disponible en los sistemas Linux, y puede ser enviado al soporte técnico de Websense si necesita ayuda para resolver un problema.

Índice

B

C

D

E

G

H

I

N

O

P

R

S

T

U

V

W