Faronics™
Simplifying Computer Management

Faronics
ANTI-VIRUS™

ADVANCED
System Integrity

Guía del usuario

www.faronics.com

Modificado por última vez: enero de 2023

Contenidos

Prólogo

Esta guía del usuario explica cómo instalar y usar Faronics Anti-Virus.

Temas

Información importante

Esta sección contiene información importante acerca de su producto de Faronics.

Acerca de Faronics

Faronics brinda soluciones líderes en el mercado que ayudan a administrar, simplificar y proteger entornos complejos de TI. Nuestros productos garantizan una disponibilidad del 100% para las máquinas y han repercutido notablemente en la vida cotidiana de miles de profesionales de tecnología de la información. Impulsadas por su orientación al mercado, las innovaciones tecnológicas de Faronics benefician a instituciones educativas, centros de salud, bibliotecas, organizaciones gubernamentales y empresas.

Documentación del producto

Los siguientes documentos integran el conjunto de documentación de Faronics Anti-Virus:

- Guía del usuario Faronics Anti-Virus: Este documento le indicará cómo usar el producto.
- Notas de la versión de Faronics Anti-Virus: Este documento enumera las nuevas funciones, los temas conocidos y los temas cerrados.

Soporte Técnico

Hemos puesto todo nuestro esfuerzo para diseñar un software de fácil utilización y que no presente inconvenientes. De presentarse alguno, póngase en contacto con nuestro Soporte Técnico.

Correo electrónico: support@faronics.com

Teléfono: 1-800-943-6422 ó 1-604-637-3333

Horario: De lunes a viernes, de 7:00 a.m. a 5:00 p.m. (Hora del Pacífico)

Información de contacto

- Web: www.faronics.com
- Correo electrónico: sales@faronics.com
- Teléfono: 1-800-943-6422 ó 1-604-637-3333
- Fax: 1-800-943-6488 ó 1-604-637-8188
- Horario: De lunes a viernes, de 7:00 a.m. a 5:00 p.m. (Hora del Pacífico)
- Dirección:

  Faronics Technologies USA Inc.
  5506 Sunol Blvd, Suite 202
  Pleasanton, CA, 94566
  EE.UU.

  Faronics Corporation (Canadá e internacional)
  609 Granville Street, Suite 1400
  Vancouver, BC V7Y 1G5
  Canadá

  Faronics Corporation (Europa)
  8 The Courtyard, Eastern Road,
  Bracknell, Berkshire,
  RG12 2XB, United Kingdom

Definición de términos

Término	Definición
Protección activa	La protección activa (Active Protection, AP) es un método de detección de malware en tiempo real. AP trabaja en segundo plano mientras usted trabaja o navega por Internet, monitoreando constantemente los archivos que se ejecutan sin causar un esfuerzo notorio en su sistema.
Adware	El adware, también conocido como software de publicidad, por lo generall se basa en el contexto o el comportamiento y registra los hábitos de navegación para mostrar publicidades de terceros cuyo destino es el usuario relevante. Las publicidades pueden tener diferentes formas, entre ellas ventanas emergentes, ventanas inferiores, pancartas o enlaces que contienen páginas Web o partes de la interfaz de Windows. Algunas publicidades de adware pueden consistir en publicidades de texto que se muestran dentro de la misma aplicación o dentro de las barras laterales, las barras de búsqueda y los resultados de las búsquedas.
Firewall	Un Firewall proporciona protección bidireccional que lo protege del tránsito entrante y saliente. Un Firewall protege su red de intrusos no autorizados.
Cuarentena	La cuarentena es un lugar seguro de su computadora usa Faronics Anti-Virus para almacenar el malware o los archivos infectados que no se pudieron desinfectar. Si su computadora o los archivos de su computadora no están actuando normalmente luego de haber colocado el elemento ahí, usted tiene la oportunidad de revisar los detalles de un riesgo e investigarlo más y quitarlo de la Cuarentena, restaurarlo a la computadora en su ubicación original. También puede retirar permanentemente los riesgos de la Cuarentena.
Programa de seguridad fraudulento	Un programa de seguridad fraudulento es un software de origen desconocido o cuestionable, o de un valor dudoso. Este tipo de programa suele presentarse en sitios web o correos electrónicos no deseados como advertencias intrusivas que indican que su equipo está infectado y le ofrecen la posibilidad de analizarlo o limpiarlo. Desconfíe siempre de estas advertencias. Las empresas de programas antivirus o antispyware reputadas nunca utilizan este tipo de notificaciones. Un programa de seguridad fraudulento puede parecer un programa antivirus o antimalware normal, pero su único propósito es engañarle para que adquiera el programa malicioso. Si bien algunos programas de seguridad fraudulentos simplemente venden humo sin ocasionar mayores daños, otros pueden tener consecuencias graves como la instalación de malware o el robo de credenciales con el fin de perpetrar delitos de usurpación de identidad. Asimismo, es preciso que tenga cuidado al cerrar o eliminar estas alertas, aunque sepa que son falsas.

Término	Definición
Rootkits	Un software rootkit oculta la presencia de los archivos y los datos para evadir la detección, mientras permite que un atacante controle la máquina sin que el usuario lo sepa. Por lo general, los rootkits son utilizados por los virus, spyware, troyanos y programas encubiertos, para ocultarse del usuario y del software de detección de malware como las aplicaciones anti-virus y anti-spyware. Los rootkits también son utilizados por algunas aplicaciones de adware y DRM (Digital Rights Management, administración de derechos digitales) para evitar que los usuarios eliminen ese software no deseado.
Spyware	El spyware es un software que transmite información a un tercero sin notificárselo a usted. También se lo conoce como trackware, hijackware, scumware, snoopware y thiefware. Algunos defensores de la privacidad incluso lo llaman control de acceso legítimo, filtrado, monitoreo de Internet, recuperación de contraseña, seguridad y software de supervisión *spyware* porque estos se pueden usar sin notificarle a usted.
Troyano	Un troyano se instala en forma fraudulenta o con falsedades y con frecuencia sin que el usuario lo conozca del todo o dé su consentimiento. En otras palabras, lo que puede parecer completamente inofensivo para un usuario, de hecho es dañino porque contiene código malicioso. La mayoría de los troyanos tienen alguna forma de funcionalidad o comportamiento malicioso, hostil o dañino.
Virus	Un virus de computación es un código malicioso que tiene la capacidad de replicarse a sí mismo e invadir otros programas o archivos para extenderse en la máquina infectada. Típicamente, los virus se expanden cuando los usuarios ejecutan los archivos infectados o cargan medios infectados, en especial medios extraíbles como CD-ROM o unidades flash. Los virus también se pueden expandir a través del correo electrónico con adjuntos y archivos infectados. La mayoría de los virus incluyen una *carga* que puede estar en cualquier parte desde molesto o que interrumpe hasta dañino. Los virus pueden causar daños en el sistema, pérdidas de datos valiosos o se pueden utilizar para instalar otro malware.
Gusano	Un gusano es un programa malicioso que se expande sin la intervención de ningún usuario. Los gusanos son similares a los virus porque se auto-replican. Sin embargo, a diferencia de los virus, los gusanos se expanden sin adjuntarse o infectar otros programas y archivos. Un gusano se puede expandir por las redes de computación a través de agujeros de seguridad en las máquinas vulnerables conectadas a la red. Los gusanos también pueden expandirse a través del correo electrónico mediante el envío de copias de sí mismo a todos los contactos de la libreta de direcciones. Un gusano puede consumir una gran cantidad de recursos del sistema y hacer que la máquina se vuelva notablemente más lenta y poco confiable. Algunos gusanos se pueden usar para comprometer a las máquinas infectadas y descargar software malicioso adicional.

Introducción

Faronics Anti-Virus proporciona protección de las amenazas de seguridad sin hacer que las computadoras funcionen con lentitud debido a los tiempo de análisis lentos y espacios de utilización grandes. Construido con tecnología de última generación, Faronics Anti-Virus le proporciona un software anti-virus y anti-spyware poderoso todo en uno que lo protege de las amenazas complejas de malware actuales, mientras que a la vez proporciona una integración perfecta conFaronics Deep Freeze y Faronics Anti-Executable para así conformar una solución de seguridad muy completa en varios niveles.

Temas

Generalidades sobre Faronics Anti-Virus

Faronics Anti-Virus protege a las estaciones de trabajo de las siguientes amenazas:

- Adware
- Programa de seguridad fraudulento
- Rootkits
- Spyware
- Troyano
- Gusanos

Faronics Anti-Virus se puede implementar en múltiples estaciones de trabajo a través de Faronics Core. Para obtener información sobre Faronics Core, consulte la Guía del usuario de Faronics Core. La guía del usuario más reciente está disponible en http://www.faronics.com/library.

Cuando se instala con Deep Freeze, las definiciones Anti-Virus se pueden actualizar en las estaciones de trabajo administradas sin que sea necesario *Reiniciar Thawed* o reiniciar en *Modo mantenimiento*. Para obtener más información consulte la Guía del usuario de Deep Freeze Enterprise. La guía del usuario más reciente está disponible en http://www.faronics.com/library.

Requisitos del sistema

Requisitos de Faronics Anti-Virus

El Loadin de Faronics Anti-Virus tiene los siguientes requisitos:

- Faronics Core 3.7 o superior

El cliente Faronics Anti-Virus en la estación de trabajo requiere cualquiera de los siguientes sistemas operativos:

- Windows XP SP3 (32 bits) o Windows XP SP2 (64 bits)
- Windows 7 (32 bits o 64 bits)
- Windows 8.1 (32 bits o 64 bits)
- Windows 10 hasta la version 22H2 (32 bits o 64 bits)
- Windows 11 hasta la version 22H2
- Windows Server 2008 R2 (64 bits)
- Windows Server 2012 (64 bits)
- Windows Server 2016 (64 bits)
- Windows Server 2019 (64 bits)
- Windows Server 2022 (64 bits)

Se recomienda instalar todos los componentes usando una cuenta de Administrador de Windows.

Requisitos de Faronics Core

Es posible encontrar información sobre los requisitos del sistema en la Guía del usuario de Faronics Core. La guía del usuario más reciente está disponible en http://www.faronics.com/library.

Requisitos de Deep Freeze

Es posible encontrar información sobre los requisitos del sistema de Deep Freeze en la Guía del usuario de Deep Freeze Enterprise. La guía del usuario más reciente está disponible en http://www.faronics.com/library.

Para ejecutar Faronics Anti-Virus en las estaciones de trabajo administradas por Deep Freeze, se necesita Deep Freeze Enterprise 7.0 o superior.

Licencia de Faronics Anti-Virus

La licencia de Faronics Anti-Virus se puede aplicar a través de Faronics Core Console. Realice los siguientes pasos para aplicar la Licencia de Faronics Anti-Virus:

1. Inicie Faronics Core Console.
2. Haga clic con el botón derecho del mouse en *Core Server* y elija *Properties (Propiedades)*.
3. Haga clic en la ficha *Anti-virus*. La ficha Anti-Virus muestra la *Versión*, *Clave de licencia* (si es una versión con licencia), y *Vencimiento de la licencia*.
4. Haga clic en *Editar* e ingrese la *clave de licencia* en el campo *Clave de licencia*.
5. Haga clic en *Apply (Aplicar)*. Haga clic en *OK (Aceptar)*.

Las licencias de Faronics Anti-Virus funcionan de la siguiente forma:

- Core Server (un componente de Faronics Core) envía automáticamente la clave de licencia a las estaciones de trabajo en las que está instalado Faronics Anti-Virus Client (si las computadoras están desconectadas, la clave de licencia se aplicará una vez que las computadoras estén nuevamente en línea).

Si la clave de licencia de Faronics Anti-Virus se ingresó cuando se instaló el Loadin, no es necesario ingresarla nuevamente en la ficha *Propiedades*.

Las definiciones de virus no se pueden descargar si la licencia de Faronics Anti-Virus está vencida.

Instalación de Faronics Anti-Virus

Este capítulo describe cómo instalar Faronics Anti-Virus.

Temas

Descripción general de la instalación

Faronics Anti-Virus tiene dos componentes:

- Faronics Anti-Virus Loadin: se instala en una computadora que tiene Faronics Core.
- Cliente Faronics Anti-Virus: se implementa en una estación de trabajo que será administrada por Faronics Anti-Virus Loadin.

La instalación y configuración de la consola Faronics Anti-Virus implica las siguientes etapas:

- Instalar Faronics Core y generar/implementar Core Agent
- Instalación de Faronics Anti-Virus Loadin
- Implementación del Cliente Faronics Anti-Virus

Instalación de Faronics Core

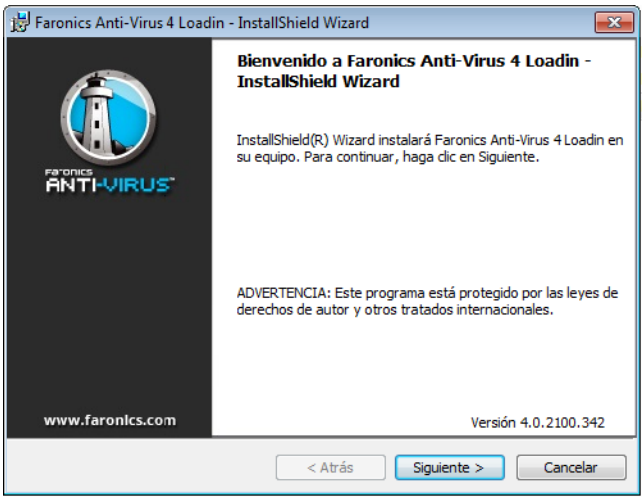
Para obtener información sobre cómo instalar la Faronics Core y generar/implementar el instalador de Core Agent, consulte la guía del usuario de Faronics Core. La guía del usuario más reciente está disponible en http://www.faronics.com/library.

Instalación de Faronics Anti-Virus Loadin

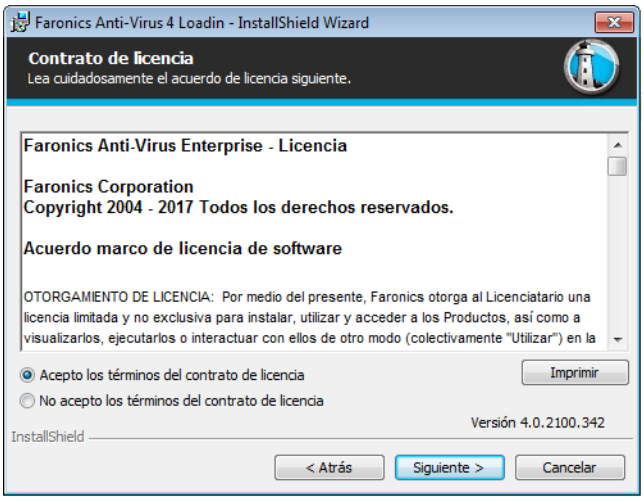
Realice los siguientes pasos para instalar Faronics Anti-Virus Loadin:

No es posible instalar Anti-Virus Loadin en un equipo que no tenga también instalado Faronics Core Console (o Faronics Core Server).

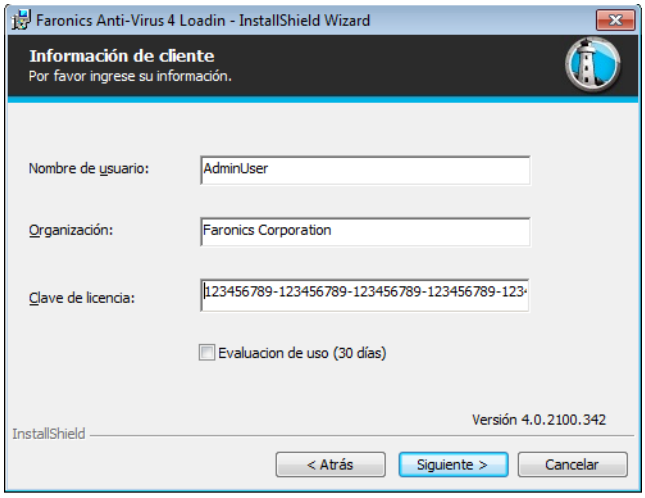
1. Haga doble clic en *Anti-VirusLoadinInstaller.exe*. Haga clic en *Next (Siguiente)*.



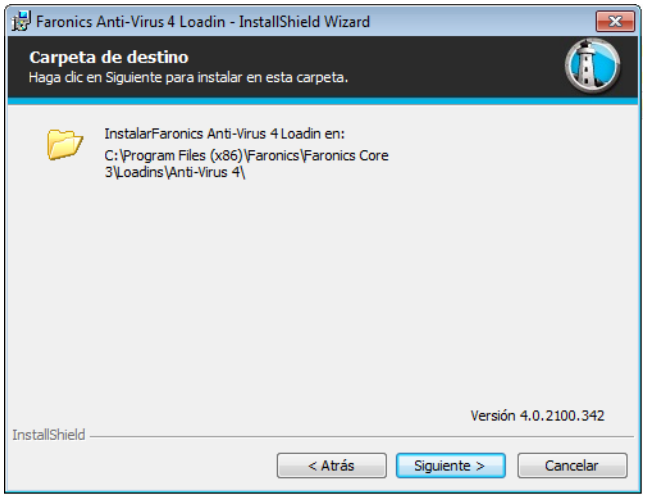
2. Lea y acepte el contrato de licencia. Haga clic en *Next (Siguiente)*.



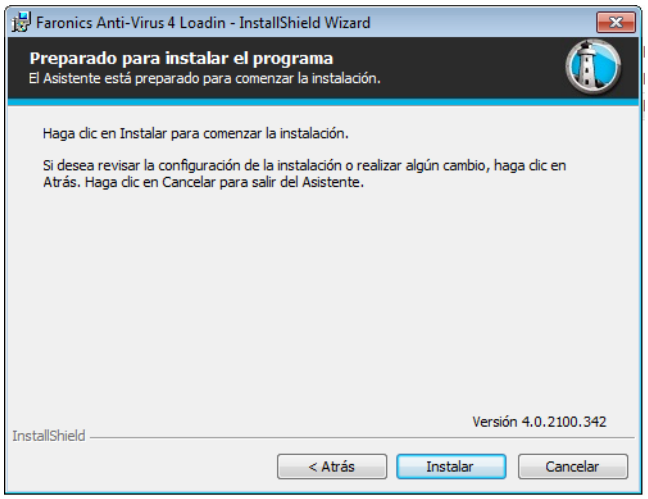
3. Ingrese el *Nombre de usuario*, la *Organización* y la *Clave de licencia*. Alternativamente, seleccione la casilla de verificación *Use Evaluation (Usar evaluación)*. Faronics Anti-Virus caduca luego de 30 días de evaluación. Haga clic en *Next (Siguiente)*.



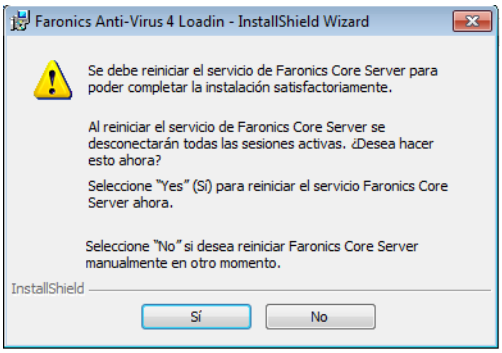
4. La ubicación predeterminada es *C:\Program Files\Faronics\Faronics Core 3\Loadins\Anti-Virus*.



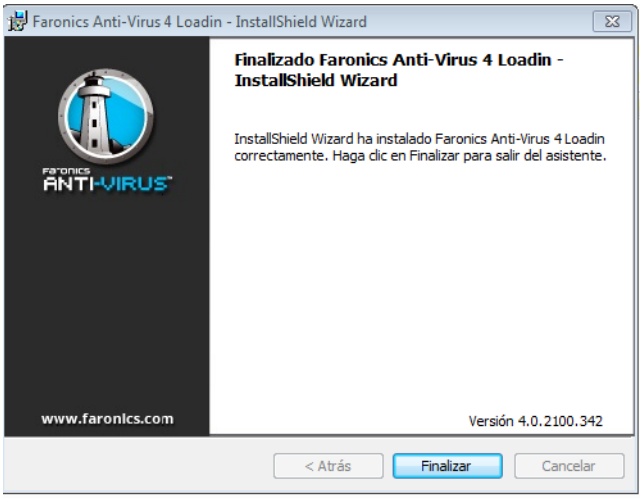
5. Haga clic en *Install (Instalar)* para instalar Faronics Anti-Virus Loadin.



6. Se mostrará el siguiente mensaje. Haga clic en *Yes (Sí)* para reiniciar el servicio Faronics Core Server. Haga clic en *No* para reiniciar manualmente el servicio Faronics Core Server.



7. Haga clic en *Finish (Finalizar)* para completar la instalación.



Instalación o actualización de Faronics Anti-Virus en una estación de trabajo mediante Faronics Core Console

Core Agent, que forma parte de Faronics Core, debe ser instalado en cada estación de trabajo que será administrada por Faronics Anti-Virus. Para más información sobre la instalación de Core Agent, consulte la guía del usuario de Faronics Core. La guía del usuario más reciente está disponible en http://www.faronics.com/library.

Las estaciones de trabajo se detectan en la red después de la instalación de Core Agent y pueden verse en Core Console.

Para instalar o actualizar la versión de Faronics Anti-Virus, seleccione una o varias estaciones de trabajo:

1. Haga clic en Configurar estaciones de trabajo en el panel derecho y seleccione *Avanzado* > *Instalar/Actualizar la versión de Faronics Anti-Virus Client*.
2. Seleccione las siguientes opciones si tiene instalado otro programa antivirus:
   - > Quite cualquier producto antivirus no compatible antes de instalar Faronics Anti-Virus Enterprise Workstation.
   - > Instalar Faronics Anti-Virus incluso si hay otro producto Anti-Virus o si no se pudo quitar.

La estación de trabajo se reinicia después de una instalación o una actualización exitosa.

Si hay más de un Loadin instalado, se puede acceder al menú contextual de Faronics Anti-Virus al hacer clic derecho en una estación de trabajo, seleccionar *Anti-Virus* y luego seleccionar la acción en particular.

Instalación manual de Faronics Anti-Virus en una estación de trabajo

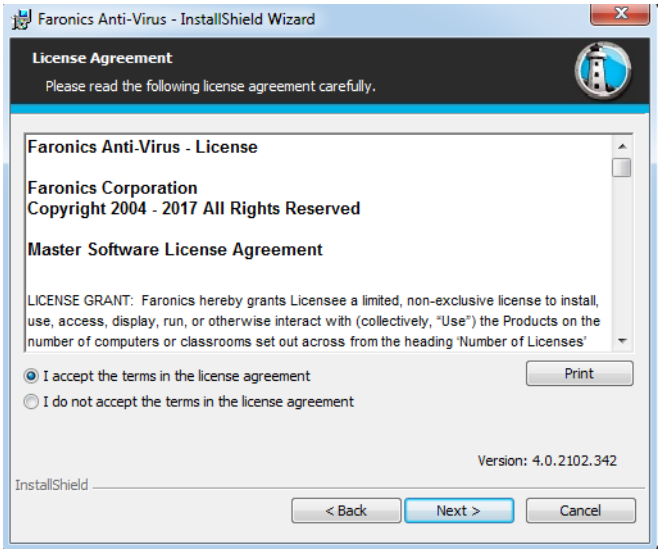
Antes de instalar Faronics Anti-Virus Client en una estación de trabajo, copie el archivo *msi* apropiado desde la ruta *C:\Program Files\Faronics\Faronics Core 3\Loadins\Anti-Virus\Wks Installers* en el equipo donde está instalado Anti-Virus Loadin en una o más estaciones de trabajo.

Repita el proceso en cada estación de trabajo que se protegerá con Faronics Anti-Virus.

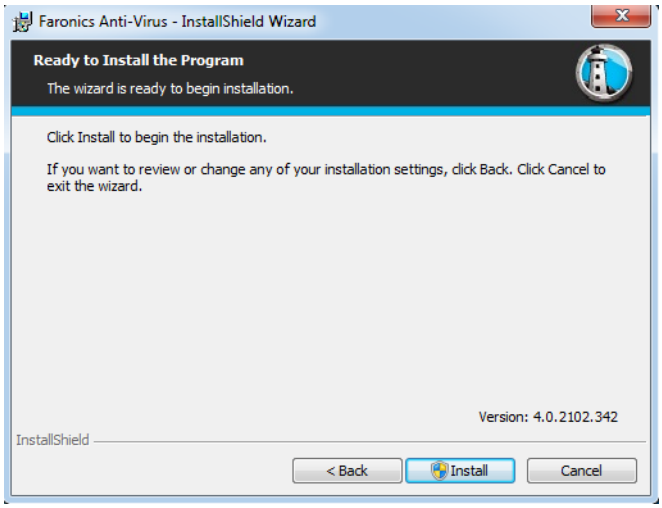
Realice los siguientes pasos para instalar Faronics Anti-Virus en la estación de trabajo:

1. Haga doble clic en *AntiVirus_Ent_32-bit.msi* en un sistema operativo de 32 bits y en *AntiVirus_Ent_64-bit.msi* en un sistema operativo de 64 bits. Haga clic en *Next (Siguiente)*.

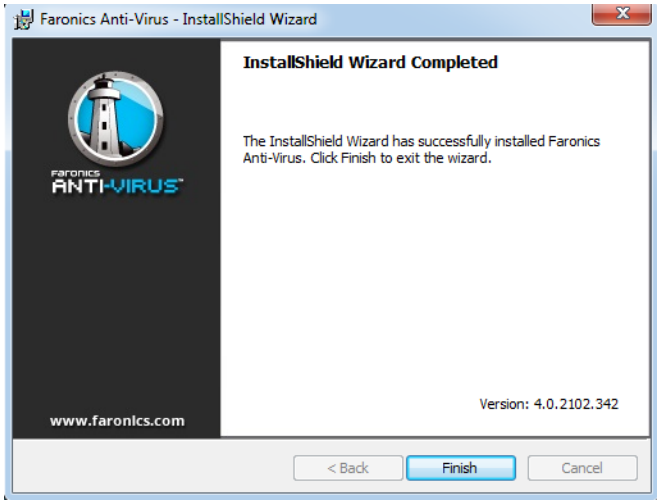
2. Lea y acepte el contrato de licencia. Haga clic en *Next (Siguiente)*.



3. Haga clic en *Install (Instalar)* para instalar Faronics Anti-Virus.



4. Haga clic en *Finish (Finalizar)* para completar la instalación.



Se recomienda reiniciar de inmediato luego de instalar el cliente Anti-Virus en la estación de trabajo.

Uso de Faronics Anti-Virus

Este capítulo describe cómo usar Faronics Anti-Virus.

Temas

Generalidades sobre Faronics Anti-Virus

Faronics Anti-Virus se puede usar de las siguientes formas:

Administración de Faronics Anti-Virus a través de Faronics Core Console:

- Instalación de Faronics Anti-Virus Loadin (para más información, consulte Instalación de Faronics Anti-Virus Loadin)
- Implementar Faronics Anti-Virus Client en las estaciones de trabajo
- Crear, editar, eliminar y aplicar una política anti-virus
- Analizar las estaciones de trabajo a través de Faronics Core Console
- Fabilitar/Deshabilitar el firewall
- Ver el historial de análisis
- Ver y tomar medidas acerca de los archivos en cuarentena
- Actualizar las definiciones anti-virus a través de Faronics Core Console
- Generación de informes
- Habilitar/Deshabilitar protección activa
- Ver logs

Uso de Faronics Anti-Virus en la estación de trabajo

- Inicio de Faronics Anti-Virus en la estación de trabajo
- Análisis de la estación de trabajo
- Actualización de las definiciones anti-virus en la estación de trabajo.
- Habilitar/Deshabilitar protección activa
- Fabilitar/Deshabilitar el firewall
- Ver el historial de análisis
- En cuarentena

Administración de Faronics Anti-Virus a través de Faronics Core Console

Una vez instalado Faronics Anti-Virus Loadin, las estaciones de trabajo se pueden administrar a través de Faronics Core Console. En las siguientes secciones se explican varios aspectos de la administración de Faronics Anti-Virus a través de Faronics Core Console.

Implementación de Faronics Anti-Virus Client en las estaciones de trabajo

Realice los siguientes pasos para implementar Faronics Anti-Virus Client en las estaciones de trabajo:

1. Inicie Faronics Core Console.
2. En el panel Console Tree (Árbol de la consola), vaya a *Faronics Core Console>[Nombre de Core Server]>Workstations (Estaciones de trabajo)>Managed Workstations (Estaciones de trabajo administradas)*.
3. Haga clic con el botón derecho en una o más estaciones de trabajo y seleccione *Configure Workstations (Configurar estaciones de trabajo)>Advanced (Avanzado)>Install/Upgrade Anti-Virus Client (Instalar/Actualizar Anti-Virus Client)*.

Faronics Anti-Virus está instalado en las estaciones de trabajo.

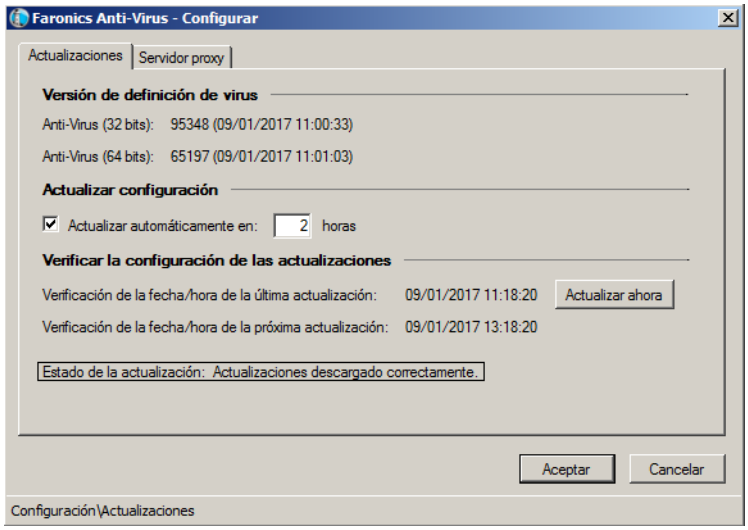
Luego de una implementación satisfactoria, la estación de trabajo tendrá la política Default (Predeterminada) y las últimas definiciones de virus.

Configuración de Faronics Anti-Virus

Realice los siguientes pasos para configurar Faronics Anti-Virus:

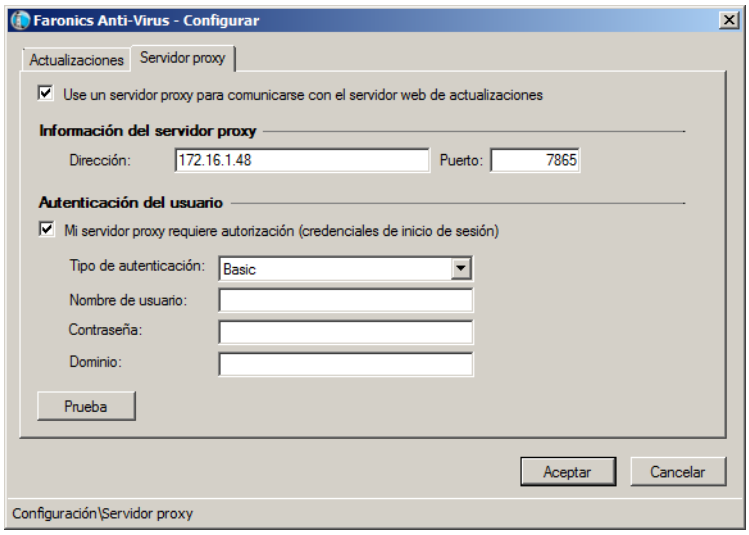
1. Inicie Faronics Core Console.
2. En el panel Console Tree (Árbol de la consola), vaya a *Faronics Core Console>[Nombre de Core Server]>Workstations (Estaciones de trabajo)>Managed Workstations (Estaciones de trabajo administradas)>Anti-Virus*.
3. Haga clic con el botón derecho en Anti-Virus y seleccione *Configure Anti-Virus (Configurar Anti-Virus)*.
4. Aparecerá la ficha Updates (Actualizaciones) en el diálogo Configure Faronics Anti-Virus (Configurar Faronics Anti-Virus).

5. La ficha Updates (Actualizaciones) muestra la versión del motor de análisis y la versión de definición de virus. Especifique las siguientes opciones:



   > Automatically update (in hours) (Actualizar automáticamente (en horas)): seleccione la casilla de verificación para actualizar automáticamente las definiciones de virus.
   > Hours (horas): especifique un valor entre 1 a 77 horas.
   > Update Now (Actualizar ahora): haga clic en este botón para actualizar las definiciones Anti-Virus.

6. Haga clic en la ficha Proxy Server (Servidor proxy) y especifique los valores de las siguientes opciones:



7. Seleccione Use a proxy server to communicate to Updates Web Server (Usar un servidor proxy para comunicarse con el Servidor Web de actualizaciones) y especifique la siguiente información:

   > Dirección: especifique la dirección IP o URL.
   > Puerto: especifique el puerto.

8. Seleccione Use a proxy server to communicate to Updates Web Server (Usar un servidor proxy para comunicarse con el Servidor Web de actualizaciones) y especifique los siguientes ajustes:
   - > Tipo de autenticación
   - > Nombre de usuario
   - > Contraseña
   - > Dominio
9. Haga clic en *Test (Probar)* para probar la conexión. Haga clic en OK (Aceptar) para guardar la configuración del proxy.

Actualización de la configuración de Faronics Anti-Virus

Para obtener los ajustes de una sola estación de trabajo que esté ejecutando Faronics Anti-Virus, realice los siguientes pasos:

1. Inicie Faronics Core Console.
2. En el panel Console Tree (Árbol de la consola), vaya a *Faronics Core Console>[Nombre de Core Server]>Workstations (Estaciones de trabajo)>Managed Workstations (Estaciones de trabajo administradas)*.
3. Haga clic con el botón derecho del mouse en una estación de trabajo y seleccione *Refresh Anti-Virus (Actualizar configuración del Anti-Virus)*.
4. Faronics Anti-Virus se actualizará y se mostrarán las siguientes columnas actualizadas:
   - > Nombre de la política
   - > Estado
   - > % del análisis completado
   - > Versión de las definiciones
   - > Fecha de la última actualización
   - > Fecha del último análisis
   - > Fecha de la última detección de una amenaza
   - > Versión

Política de Faronics Anti-Virus

Una directiva de Anti-Virus contiene todos los ajustes de configuración acerca de cómo se debe ejecutar Anti-Virus en las estaciones de trabajo. Incluye las acciones que debe realizar el programa, las programaciones, los servidores proxy, los informes de error y las funciones permitidas al usuario en la estación de trabajo. En las siguientes secciones se explica cómo crear y aplicar una directiva de Anti-Virus.

Si utiliza Legacy Anti-Virus, siga los pasos descritos a continuación para migrar al nuevo Anti-Virus:

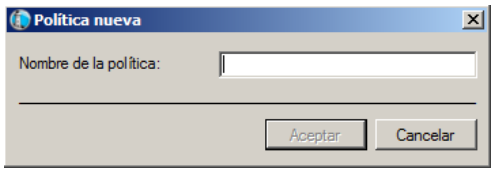
1. Desinstale Legacy Anti-Virus en las estaciones de trabajo administradas.
2. Configure la nueva directiva de Anti-Virus.
3. Instale el nuevo Anti-Virus en las estaciones de trabajo administradas.

Faronics Anti-Virus contiene una directiva *Predeterminada*. La directiva Predeterminada contiene los ajustes de configuración más óptimos para administrar Faronics Anti-Virus.

Creación de directivas de Anti-Virus

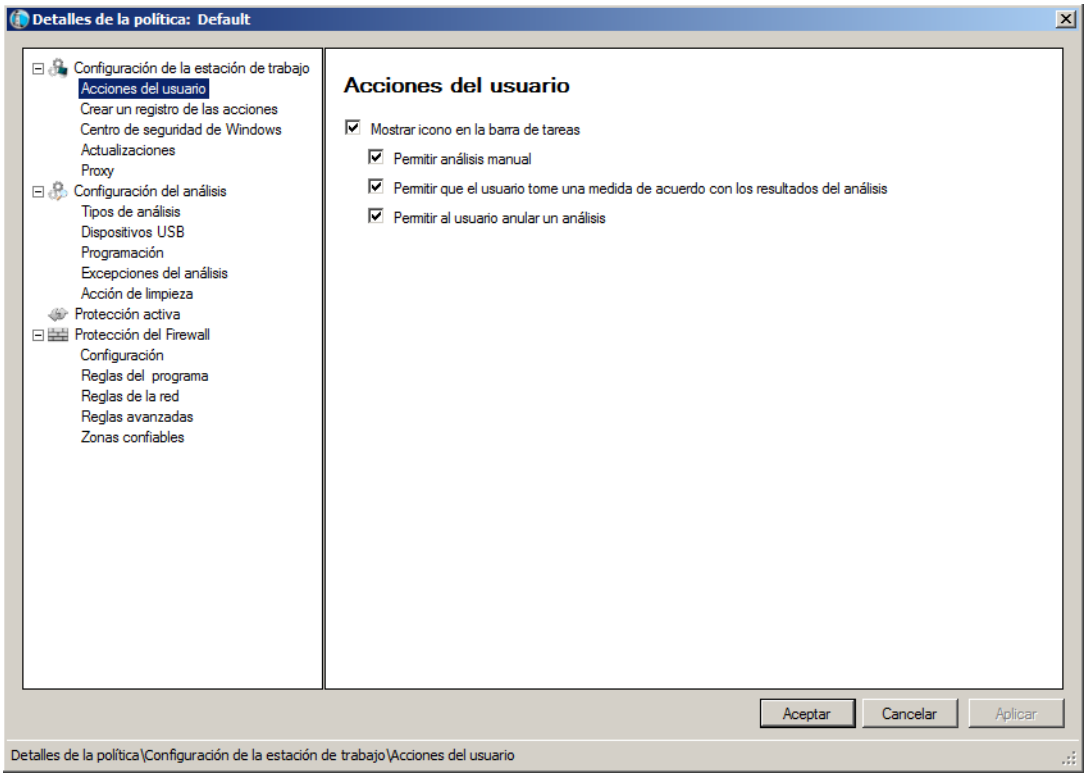
Realice los siguientes pasos para crear una nueva directiva de Anti-Virus:

1. Inicie Faronics Core Console.
2. En el *panel de vista de árbol de la consola*, vaya a *Faronics Core Console>[Nombre de Core Server]>Estaciones de trabajo>Estaciones de trabajo administradas>Anti-Virus*.
3. Haga clic con el botón secundario en *Anti-Virus* y seleccione *Nueva directiva*.
4. Especifique un nombre para la directiva en el cuadro de diálogo *Nueva directiva*. Haga clic en *Aceptar*. Se creará una nueva directiva debajo del nodo *Anti-Virus*. Por ejemplo, puede asignar a la nueva directiva el nombre de *Nueva directiva 1*.



5. Haga clic con el botón secundario en *Nueva directiva 1* y seleccione *Detalles de directiva*. Aparecerá el cuadro de diálogo *Detalles de directiva*.
6. Especifique los ajustes en el nodo *Configuración de estación de trabajo*.

- Panel *Acciones de usuario*



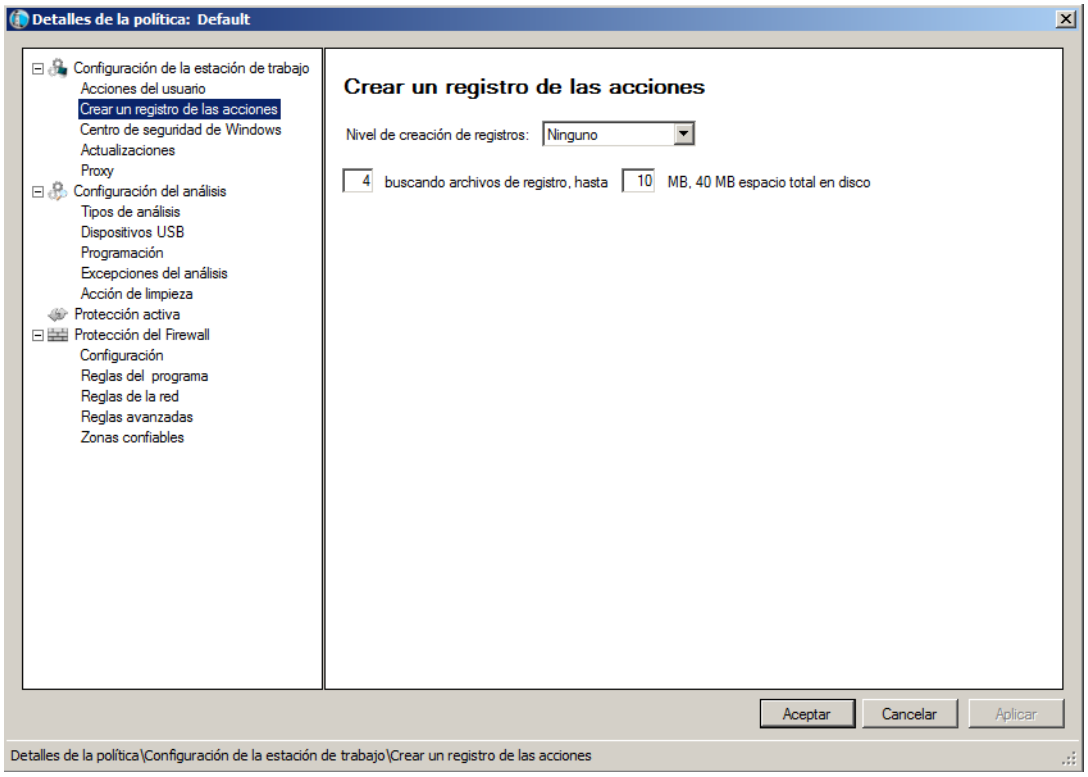
> Mostrar icono de barra de tareas: active esta casilla de verificación para mostrar el icono de Faronics Anti-Virus en la barra de tareas de las estaciones de trabajo. Si no se activa esta casilla de verificación, Faronics Anti-Virus permanecerá oculto para el usuario.

~ Permitir análisis manual: active esta casilla de verificación para permitir a los usuarios iniciar de forma manual el análisis de Faronics Anti-Virus en las estaciones de trabajo.

~ Permitir al usuario tomar medidas sobre los resultados del análisis: active esta casilla de verificación para permitir al usuario de la estación de trabajo tomar medidas en función de los resultados del análisis.

~ Permitir al usuario anular un análisis iniciado localmente: active esta casilla de verificación para permitir a los usuarios anular un análisis iniciado localmente en la estación de trabajo.

- Panel *Crear un registro de las acciones*

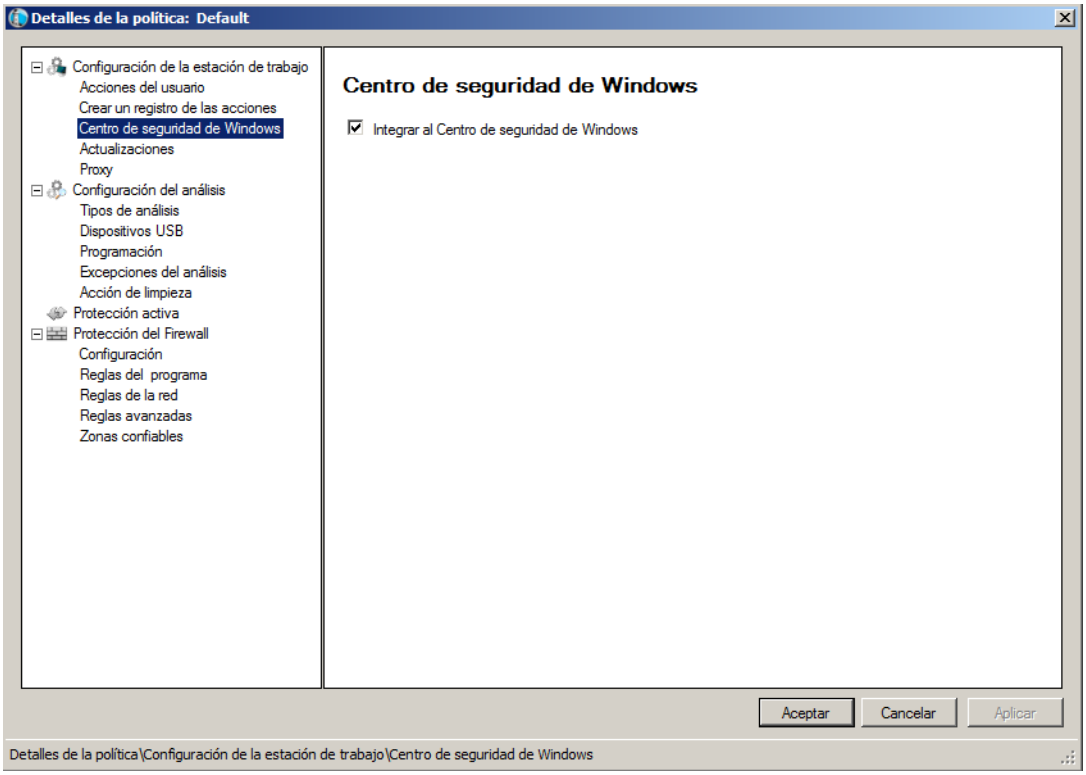


> Nivel de registro: seleccione el nivel de registro. Seleccione *Ninguno* si no desea que se realice ningún tipo de registro. Seleccione *Error* para registrar los mensajes de error. Seleccione *Seguimiento* para realizar un seguimiento. Seleccione *Detallado* si desea que el registro incluya información detallada.

> Número de archivos de registro: especifique el número de archivos de registro. La información de registro se guardará de forma secuencial en los archivos. Por ejemplo, si hay tres archivos A, B y C, Faronics Anti-Virus escribirá primero los registros de error en el archivo A. Una vez que este esté lleno, los escribirá en el archivo B y, por último, en el archivo C. Cuando el archivo C esté lleno, se borrarán los datos en el archivo A y se escribirán los nuevos datos.

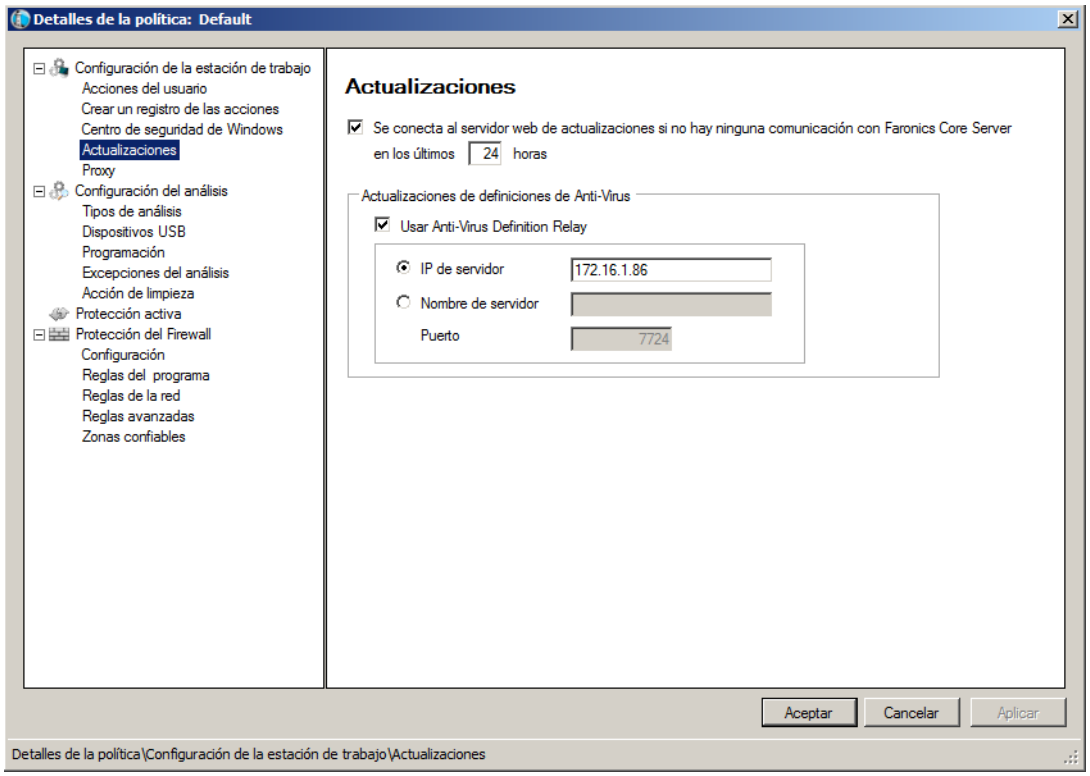
> Tamaño de archivo: seleccione el tamaño de cada uno de los archivos en MB.

- Panel *Centro de seguridad de Windows*



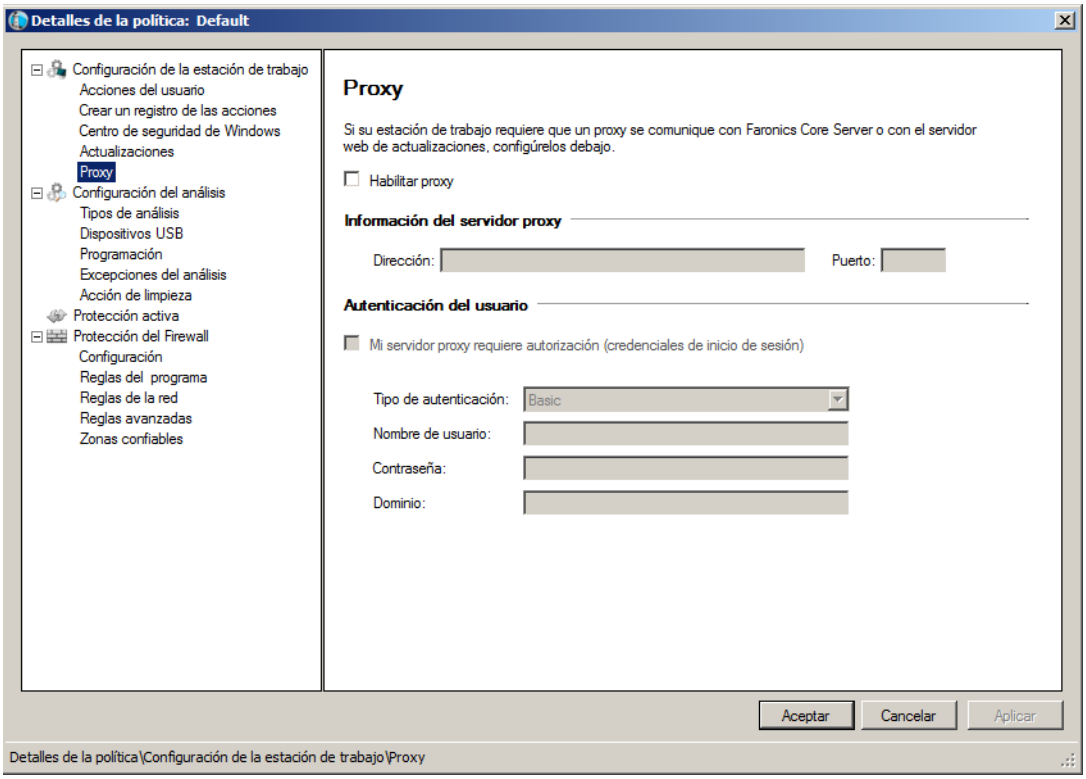
> Integrar en Centro de seguridad de Windows: active esta casilla de verificación para integrar Faronics Anti-Virus en el Centro de seguridad de Windows. El Centro de seguridad de Windows indicará si Faronics Anti-Virus está activo o inactivo en la bandeja del sistema.

- Panel *Actualizaciones*



> Conectar con servidor web de actualizaciones si no hay comunicación con Faronics Core Server en las últimas x horas: seleccione esta opción para conectarse al servidor web de actualizaciones y descargar las definiciones de virus si la estación de trabajo pierde contacto con Faronics Core Server. Si no activa esta casilla de verificación, las definiciones de virus no se actualizarán si la estación de trabajo pierde la conexión con Faronics Core Server.

- Panel *Proxy*



> Habilitar proxy: seleccione la casilla de verificación si las estaciones de trabajo necesitan un proxy para comunicarse con Faronics Core Server o el servidor web de actualizaciones.

> Información del servidor proxy: Especifique la *Dirección* y el *Puerto*.

> Autenticación del usuario

  Mi servidor proxy requiere autorización (credenciales de inicio de sesión): si el servidor requiere autenticación, especifique los valores para los siguientes campos:

  ~ Tipo de autenticación: seleccione el tipo de autenticación.

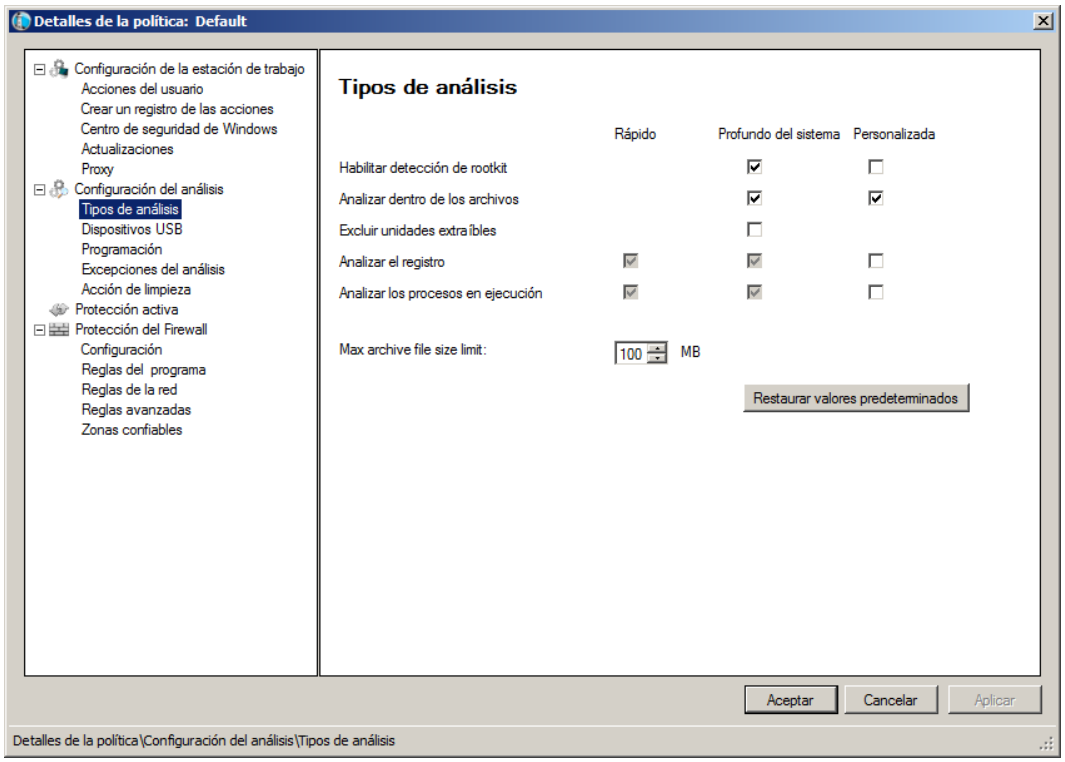
  ~ Nombre de usuario: especifique el nombre de usuario.

  ~ Contraseña: especifique la contraseña.

  ~ Dominio: especifique el dominio.

7. Especifique los ajustes en el nodo *Configuración de análisis*.

- Panel *Tipos de análisis*



Faronics Anti-Virus ofrece tres tipos de análisis:

> Análisis rápido: analiza las áreas comúnmente afectadas de su equipo. Su duración es menor que el análisis a fondo del sistema. El análisis rápido también usa menos memoria que el análisis a fondo del sistema.

> Análisis a fondo del sistema: realiza un análisis minucioso de todas las áreas del equipo. La duración del análisis dependerá del tamaño de la unidad de disco duro.

> Análisis personalizado: realiza un análisis de acuerdo con las selecciones realizadas en cuadro de diálogo *Detalles de directiva*.

Para cada tipo de análisis, seleccione las opciones siguientes (algunas opciones pueden aparecer atenuadas en función del tipo de análisis):

> Habilitar detección de rootkits: detecta si el equipo está infectado con un rootkit.

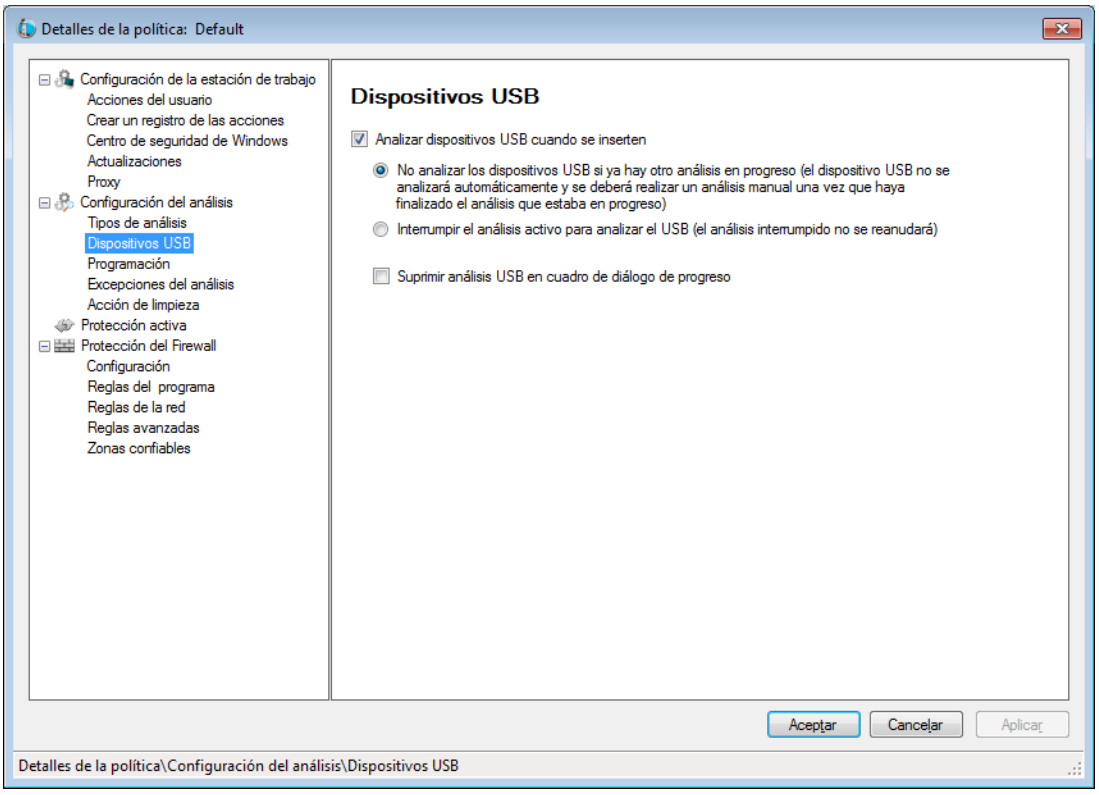
> Analizar dentro de archivos: analiza el contenido de los archivos zip. Seleccione esta opción si también desea que se analicen los archivos de almacenamiento, como .RAR y .ZIP. Si un archivo .RAR contiene un archivo infectado, el archivo .RAR se pondrá en cuarentena. Si un archivo .ZIP contiene un archivo infectado, el archivo infectado se pondrá en cuarentena y será reemplazado por un archivo .TXT con texto que informará al usuario de que el archivo estaba infectado y se ha puesto en cuarentena. Especifique el *Límite de tamaño del archivo*.

> Excluir unidades extraíbles (p.ej., USB): excluye las unidades extraíbles del proceso de análisis. No se analizarán dispositivos como discos externos extraíbles, unidades USB, etc.

> Analizar el registro: analiza el registro.

> Analizar procesos en ejecución: analiza los procesos que se están ejecutando en ese momento.

- Panel *Dispositivos USB*



Analizar unidades USB al insertar: active esta casilla de verificación para analizar las unidades USB cuando se conecten al equipo, y seleccione una de las opciones siguientes:

> No realizar análisis USB si ya hay otro análisis en curso: seleccione esta opción para que el análisis activo no se interrumpa cuando se conecte una unidad USB. Una vez haya finalizado el análisis activo, se deberá iniciar el análisis de la unidad USB manualmente.

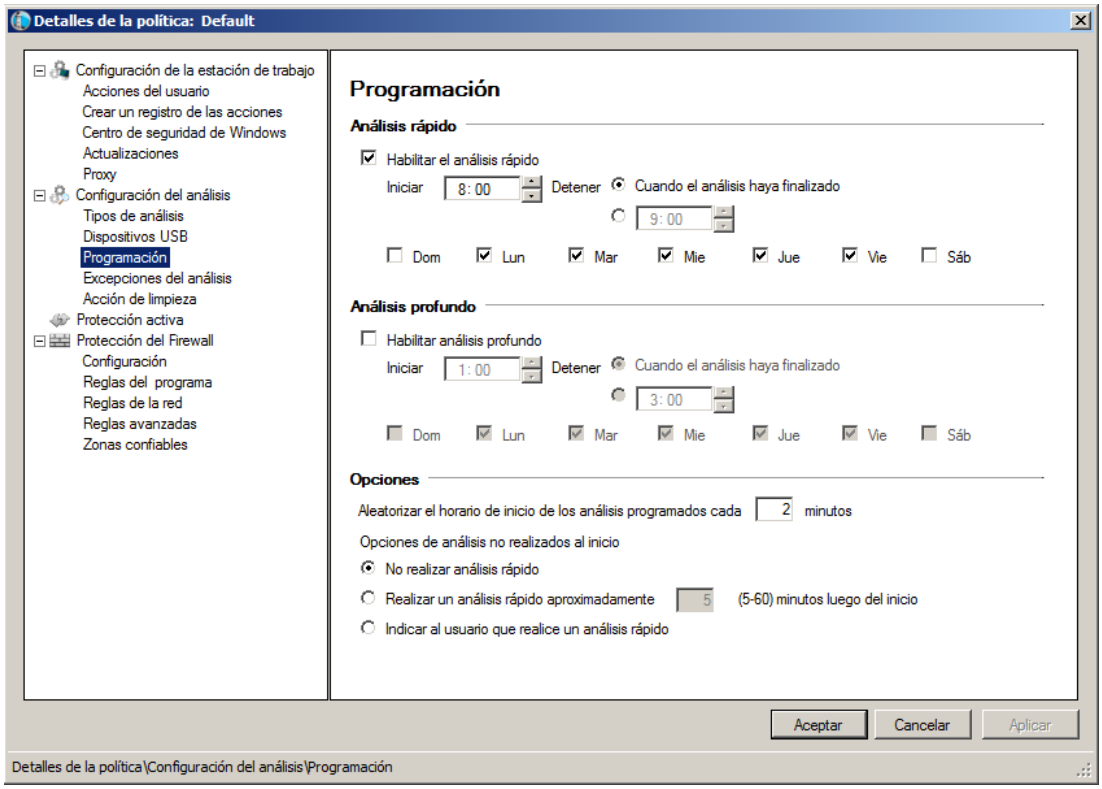
> Interrumpir análisis activo para analizar USB: seleccione esta opción para interrumpir el análisis activo y analizar la unidad USB conectada. Una vez se haya interrumpido el análisis activo, este no se reanudará automáticamente, sino que deberá iniciarse manualmente.

> Suprimir análisis USB en cuadro de diálogo de progreso: seleccione esta opción para ocultar las indicaciones de que Anti-Virus está analizando las unidades USB que se acaban de conectar; no se abrirá ninguna interfaz de Anti-Virus y el icono de la bandeja del sistema no mostrará información sobre herramientas que indique un análisis en curso. Al finalizar el análisis, se informará a los usuarios si se ha detectado un virus; de lo contrario, no se mostrará ninguna notificación conforme se ha realizado el análisis.

  Tenga en cuenta que si no se selecciona la opción Analizar unidades USB al insertar, esta opción no estará disponible.

Si la casilla de selección *Permitir análisis manual* está seleccionada en la ficha *Configuración de estación de trabajo*>panel *Acciones del usuario*, el dispositivo USB se analizará automáticamente. Si la casilla de verificación *Permitir análisis manual* no está seleccionada, el dispositivo USB no se analizará automáticamente.

- Panel *Programación*



Análisis rápido:

> Habilitar análisis rápido: active esta casilla de verificación para habilitar el análisis rápido.

> Inicio: especifique la hora de inicio.

> Finalización: especifique la hora de finalización. El intervalo de tiempo máximo entre la hora de *Inicio* y la hora de *Finalización* es de *23.59* horas. Si se analizan todos los archivos antes de la hora de *Finalización*, finalizará el análisis. Si el análisis no se completa antes de la hora de *Finalización*, se interrumpirá cuando llegue a la hora de *Finalización*. También puede seleccionar *Cuando finalice el análisis* para asegurarse de que termine el análisis.

> Días: seleccione los días en los que se ejecutará el análisis rápido programado.

Análisis a fondo:

> Habilitar análisis a fondo: active esta casilla de verificación para habilitar el análisis a fondo.

> Inicio: especifique la hora de inicio.

> Finalización: especifique la hora de finalización. El intervalo de tiempo máximo entre la hora de *Inicio* y la hora de *Finalización* es de 23.59 horas. Si se analizan todos los archivos antes de la hora de *Finalización*, finalizará el análisis. Si el análisis no se completa antes de la hora de *Finalización*, se interrumpirá cuando llegue a la hora de *Finalización*. También puede seleccionar *Cuando finalice el análisis* para asegurarse de que termine el análisis.

> Días: seleccione los días en los que se ejecutará el análisis a fondo programado.

Opciones:

> Horas de inicio de análisis programados aleatorias cada x minutos: especifique el número de minutos. Los análisis programados se iniciarán de forma aleatoria para reducir el impacto en el tráfico de la red. Faronics Anti-Virus se comunica con Faronics Core cuando se inicia el análisis. Si los análisis de varios sistemas se iniciarán al mismo tiempo, el tráfico de la red podría verse afectado.

Opciones si no se realiza el análisis: seleccione una de las opciones siguientes para especificar cómo se debe realizar el análisis si la estación de trabajo no estaba *ENCENDIDA* durante un análisis programado:

> No realizar análisis rápido: seleccione esta opción si no desea realizar un análisis rápido al inicio.

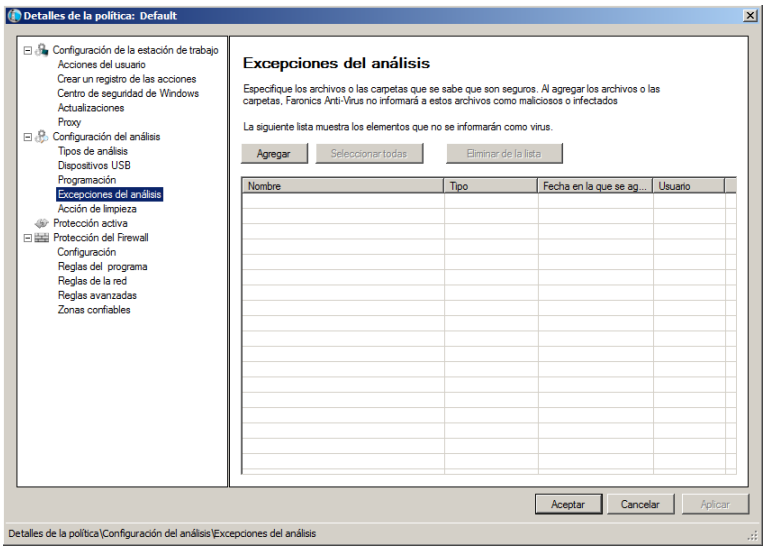
> Realizar análisis rápido aproximadamente x minutos después del inicio: especifique el número de minutos que deben transcurrir desde el inicio para que Faronics Anti-Virus inicie el análisis.

> Preguntar al usuario si desea realizar un análisis rápido: seleccione esta opción para preguntar al usuario si desea realizar un análisis rápido.

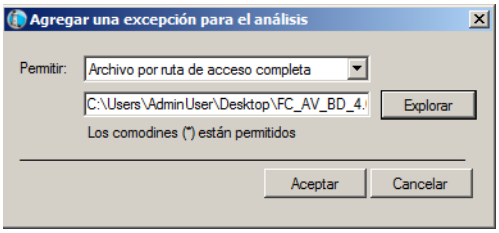
- Panel *Excepciones de análisis*

  La ficha Excepciones de análisis permite agregar carpetas o archivos identificados como seguros. Faronics Anti-Virus siempre analizará los archivos agregados a la ficha Excepciones de análisis. Sin embargo, nunca identificará los archivos como maliciosos o infectados. El administrador nunca recibirá notificaciones de amenazas de los archivos y carpetas especificados como seguros.

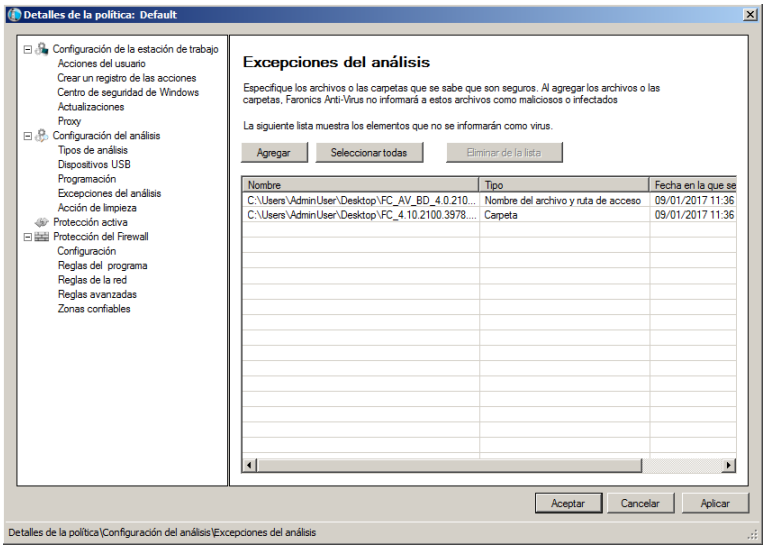
  A. Haga clic en *Agregar*.



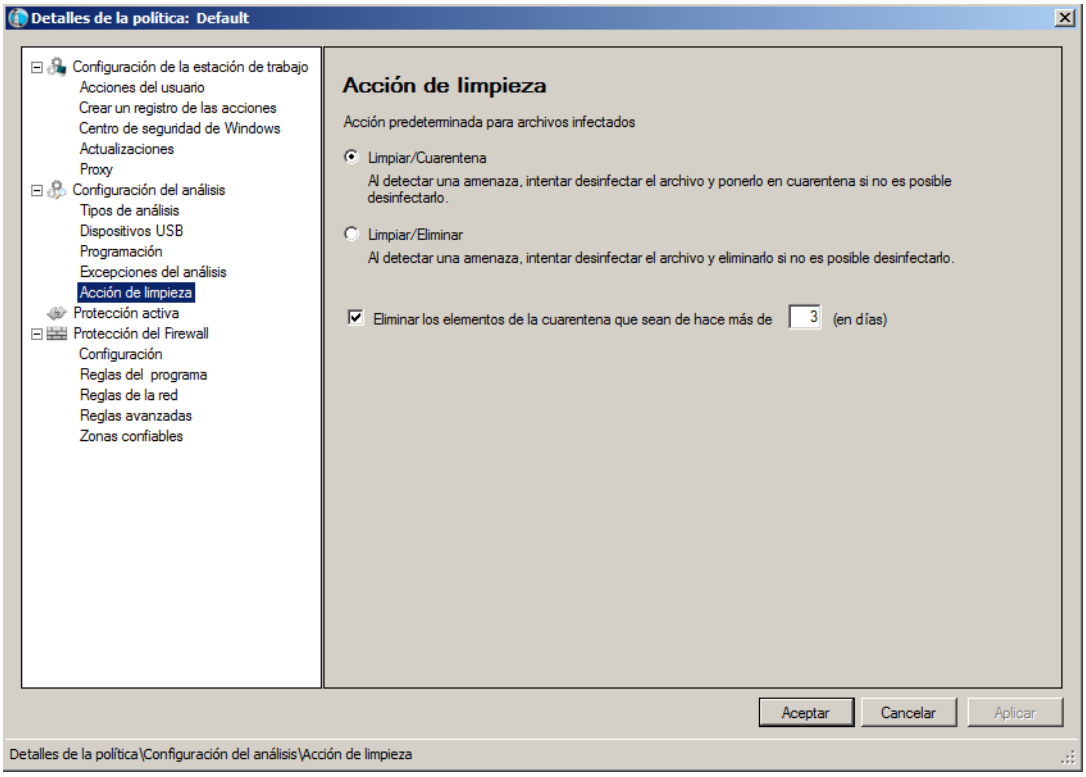
  B. En el cuadro de diálogo *Agregar*, seleccione *Archivo por ruta completa*, o *Toda la carpeta*. Haga clic en Examinar para seleccionar el archivo o carpeta y haga clic en *Aceptar*.



  C. El *Archivo por ruta completa* se agregará a las excepciones de análisis.



- Panel *Acción de limpieza*

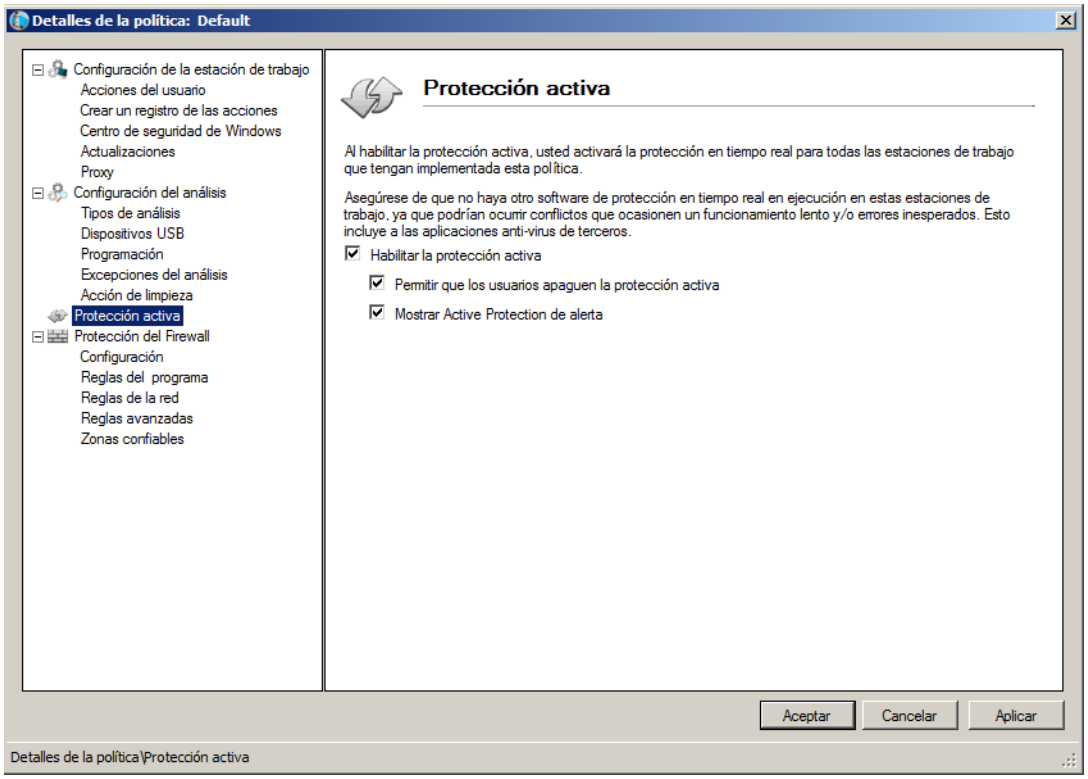


> Limpiar/Cuarentena: al detectar una amenaza, intentar desinfectar el archivo y ponerlo en cuarentena si no es posible desinfectarlo. Si no es posible desinfectar el archivo, se pondrá en cuarentena y no se eliminará.

> Limpiar/Eliminar: al detectar una amenaza, intentar desinfectar el archivo y eliminarlo si no es posible desinfectarlo. Si no es posible desinfectar el archivo, se eliminará del equipo.

> Eliminar elementos en cuarentena que tengan más de: especifique el número de días que se deberán conservar los elementos en cuarentena. El valor predeterminado es 3 días.

8. Especifique los ajustes en el panel *Protección activa*.

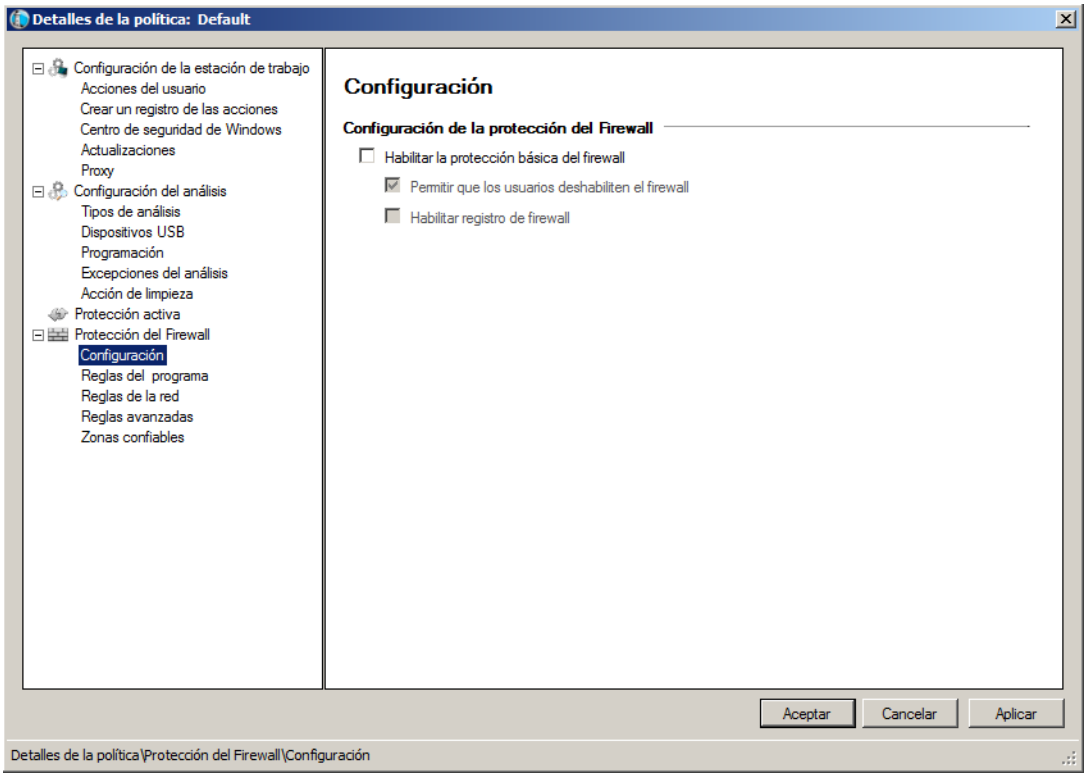


- Habilitar protección activa: seleccione esta opción para habilitar la protección en tiempo real. La protección activa es un análisis en tiempo real que se ejecuta en segundo plano sin comprometer el rendimiento del sistema. Seleccione esta opción si hay riesgo de infección de virus en tiempo real desde Internet.
  - > Permitir al usuario desactivar la protección activa: Seleccione esta opción para permitir a los usuarios desactivar la protección activa. Seleccione esta opción si los usuarios instalan o utilizan software que podría ser identificado de forma errónea como virus (por ejemplo, la ejecución de macros avanzadas en Microsoft Office o archivos por lotes complejos).
  - > Mostrar alerta de protección activa: Seleccione esta opción para mostrar una alerta si se detecta una amenaza durante la protección activa. No active esta casilla de verificación si no desea que se muestre una alerta.

9. Especifique los ajustes en el nodo *Protección de firewall*.

   El nodo Protección de firewall proporciona protección bidireccional, ya que protege el equipo del tráfico entrante y saliente. Puede crear reglas personalizadas para proteger su red. Puede *Permitir* o *Bloquear* la comunicación.

- Panel *Configuración*



Configuración de la protección de firewall

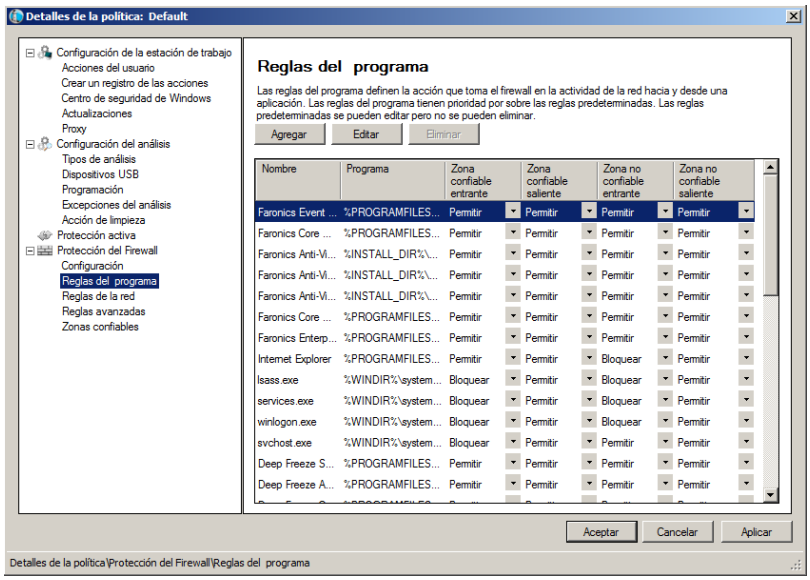
> Habilitar la protección básica de firewall: active esta casilla de verificación para habilitar la protección de firewall. La protección de firewall impide el acceso de hackers o software malicioso a su equipo a través de Internet o la red.

  ~ Permitir que los usuarios deshabiliten el firewall: seleccione esta opción para permitir al usuario deshabilitar el firewall en el equipo.

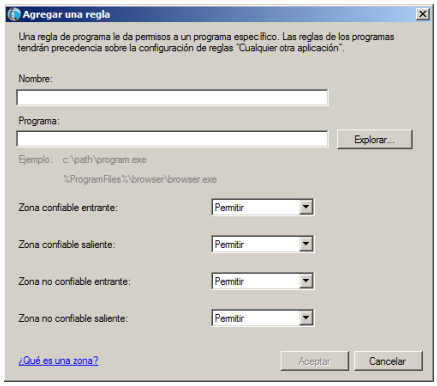
  ~ Habilitar registro de firewall: seleccione esta opción para registrar todas las acciones relacionadas con el firewall.

- Panel *Reglas de programa*

  Las reglas de programa definen las acciones que realizará el firewall en relación con la actividad de red hacia y desde una aplicación. Las reglas de programa tienen prioridad sobre las reglas predeterminadas. Las reglas predeterminadas pueden editarse, pero no pueden eliminarse.



Haga clic en *Agregar* para agregar una regla de programa. Especifique o seleccione las opciones correspondientes y haga clic en *Aceptar*. Se mostrarán los parámetros siguientes:



> Nombre: nombre de la regla.

> Programa: nombre del programa, incluidas su extensión y ruta completa.

> Zona de confianza (Entrada): la acción que se realizará para las comunicaciones entrantes dirigidas al programa en una zona de confianza (*Permitir* o *Bloquear*).

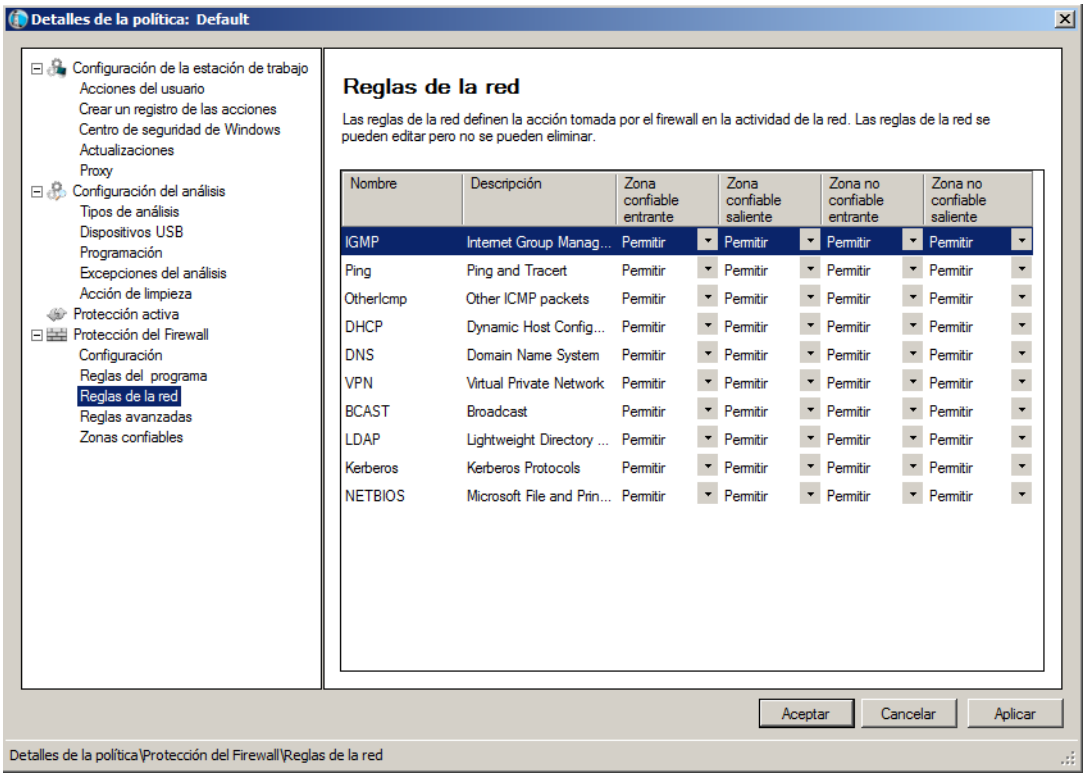
> Zona de confianza (Salida): la acción que se realizará para las comunicaciones salientes procedentes del programa en una zona de confianza (*Permitir* o *Bloquear*).

> Zona de no confianza (Entrada): la acción que se realizará para las comunicaciones entrantes dirigidas al programa en una zona de no confianza (*Permitir* o *Bloquear*).

> Zona de no confianza (Salida): la acción que se realizará para las comunicaciones salientes procedentes del programa en una zona de no confianza (*Permitir* o *Bloquear*).

- Panel *Reglas de red*

  Las reglas de red definen las medidas que tomará el firewall en relación con la actividad de red. Las reglas de red pueden editarse pero no eliminarse.

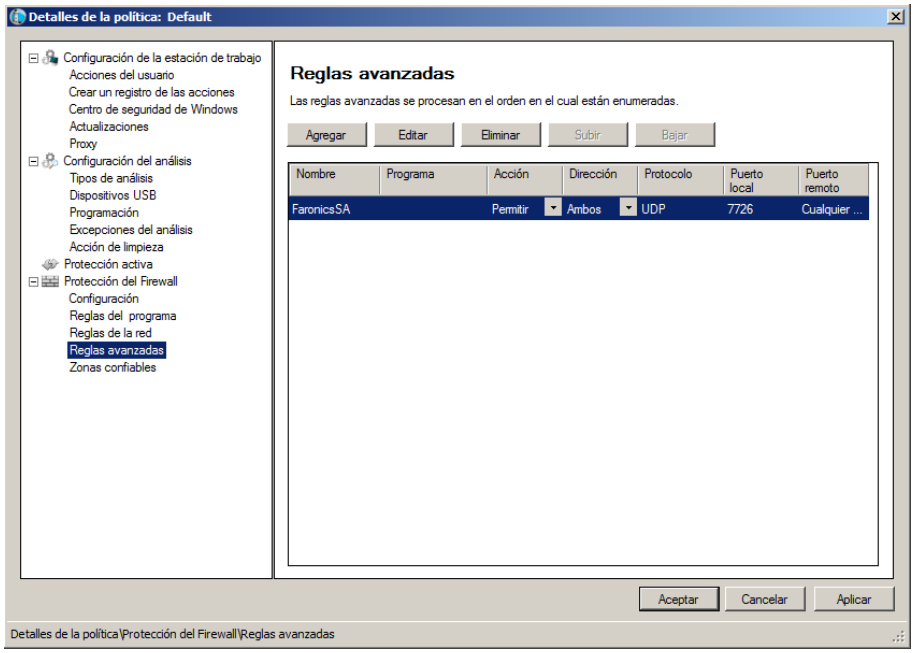


Seleccione las reglas de red para las siguientes opciones:

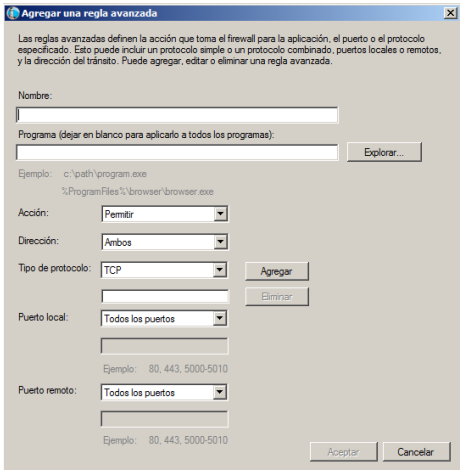
Nombre	Descripción	Zona de confianza (Entrada)	Zona de confianza (Salida)	Zona de no confianza (Entrada)	Zona de no confianza (Salida)
IGMP	Protocolo de administración de grupos de Internet	Seleccione Permitir o Bloquear	Seleccione Permitir o Bloquear	Seleccione Permitir o Bloqu–ear	Seleccione Permitir o Bloquear
Ping	Ping y Traceroute	Seleccione Permitir o Bloquear	Seleccione Permitir o Bloquear	Seleccione Permitir o Bloquear	Seleccione Permitir o Bloquear
OtherIcmp	Otros paquetes ICMP	Seleccione Permitir o Bloquear	Seleccione Permitir o Bloquear	Seleccione Permitir o Bloquear	Seleccione Permitir o Bloquear
DHCP	Protocolo de configuración dinámica de host	Seleccione Permitir o Bloquear	Seleccione Permitir o Bloquear	Seleccione Permitir o Bloquear	Seleccione Permitir o Bloquear
DNS	Sistema de nombres de dominio	Seleccione Permitir o Bloquear	Seleccione Permitir o Bloquear	Seleccione Permitir o Bloquear	Seleccione Permitir o Bloquear
VPN	Red privada virtual	Seleccione Permitir o Bloquear	Seleccione Permitir o Bloquear	Seleccione Permitir o Bloquear	Seleccione Permitir o Bloquear
BCAST	Difusión	Seleccione Permitir o Bloquear	Seleccione Permitir o Bloquear	Seleccione Permitir o Bloquear	Seleccione Permitir o Bloquear
LDAP	Protocolo ligero de acceso a directorios	Seleccione Permitir o Bloquear	Seleccione Permitir o Bloquear	Seleccione Permitir o Bloquear	Seleccione Permitir o Bloquear
Kerberos	Protocolo Kerberos	Seleccione Permitir o Bloquear	Seleccione Permitir o Bloquear	Seleccione Permitir o Bloquear	Seleccione Permitir o Bloquear
NETBIOS	Compartir archivos e impresoras de Microsoft	Seleccione Permitir o Bloquear	Seleccione Permitir o Bloquear	Seleccione Permitir o Bloquear	Seleccione Permitir o Bloquear

- Panel *Reglas avanzadas*

  Las reglas avanzadas definen las medidas que tomará el firewall en relación con una aplicación, puerto o protocolo especificados. Esto puede incluir un solo protocolo o una combinación de protocolo, puertos locales o remotos y dirección de tráfico. Puede agregar, editar o eliminar una regla avanzada.



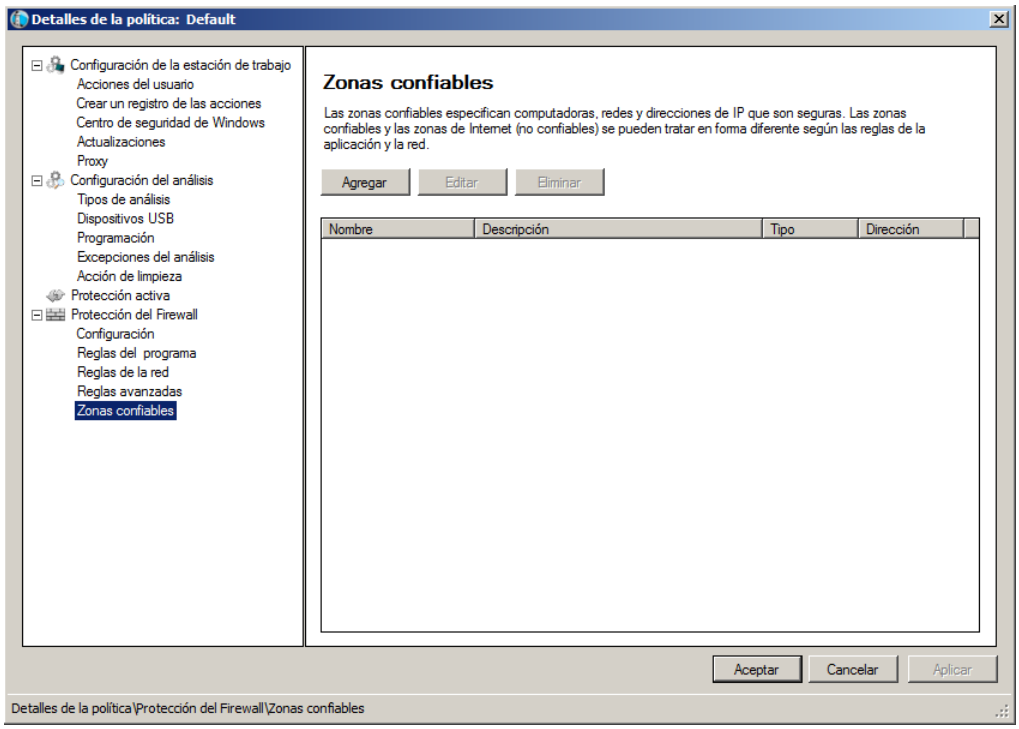
  Haga clic en *Agregar* para agregar una regla avanzada. Especifique o seleccione las opciones correspondientes y haga clic en *Aceptar*. El panel Reglas avanzadas incluye los parámetros siguientes:



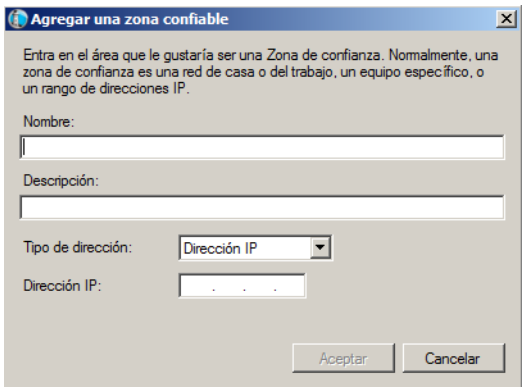
  > Nombre: nombre de la regla.
  > Programa: nombre y ruta del programa.
  > Acción: la acción que realizará el firewall para las comunicaciones procedentes de la aplicación, puerto o protocolo especificados (*Permitir* o *Bloquear*).
  > Dirección: la dirección de la comunicación (*Ambas*, *Hacia dentro* o *Hacia fuera*).
  > Tipo de protocolo: el tipo (ICMP, IGMP, TCP, UDP) y el nombre del protocolo.
  > Puerto local: ajustes del puerto local.
  > Puerto remoto: ajustes del puerto remoto.

- Panel *Zonas de confianza*

  Las zonas de confianza especifican equipos, redes y direcciones IP seguros. Es posible tratar las zonas de confianza e Internet (zona de no confianza) de forma distinta mediante reglas de red y de programa.



  Haga clic en *Agregar* para agregar una zona de confianza. Especifique o seleccione las opciones correspondientes y haga clic en *Aceptar*. Se mostrarán los parámetros siguientes:



  > Nombre: nombre de la zona de confianza.
  > Descripción: descripción de la zona de confianza.
  > Tipo: tipo de zona de confianza (*Dirección IP* o *Red*).

10. Haga clic en *Aceptar*. La nueva directiva, *Nueva directiva 1* se mostrará debajo del nodo*Anti-Virus*.

Aplicación de una directiva de Anti-Virus

Una vez se haya creado la directiva de Anti-Virus, puede aplicarse a una o más estaciones de trabajo con Faronics Core Console. Siga los pasos descritos a continuación para aplicar la directiva:

1. Seleccione una o más estaciones de trabajo. Haga clic con el botón secundario y seleccione *Reasignar directiva*.
2. Se abrirá el cuadro de diálogo *Reasignar estaciones de trabajo a directiva*. Seleccione la directiva en la lista desplegable *Asignar directiva* y haga clic en *Aceptar*.
3. La directiva se aplicará a las estaciones de trabajo seleccionadas.

Visualización o modificación de una directiva de Anti-Virus

Una vez se haya creado la directiva de Anti-Virus, podrá verse o modificarse. Siga los pasos descritos a continuación para ver o modificar una directiva:

1. Inicie Faronics Core Console.
2. En el *panel de vista de árbol de la consola*, vaya a *Faronics Core Console>[Core Server]>Estaciones de trabajo administradas>Anti-Virus>[Nombre de directiva]*.
3. Haga clic con el botón secundario en la directiva y seleccione *Detalles de directiva*.
4. Para editar la directiva, modifique la configuración en las fichas como se explica en Creación de directivas de Anti-Virus.
5. Haga clic en *Aceptar* para aplicar los cambios.
6. Los cambios realizados en la directiva se aplicarán automáticamente a las estaciones de trabajos administradas por la directiva.

Cambio de nombre de una directiva de Anti-Virus

Una vez se haya creado la directiva de Anti-Virus, podrá cambiar su nombre. Siga los pasos descritos a continuación para cambiar el nombre de una directiva:

1. Inicie Faronics Core Console.
2. En el *panel de vista de árbol de la consola*, vaya a *Faronics Core Console>[Core Server]>Estaciones de trabajo administradas>Anti-Virus>[Nombre de directiva]*.
3. Haga clic con el botón secundario en la directiva y seleccione *Cambiar nombre de directiva*. Aparecerá el cuadro de diálogo *Cambiar nombre de directiva*.
4. Introduzca el *nuevo nombre de la directiva* y haga clic en *Aceptar*.

Copiar una directiva

Es posible copiar una directiva existente en una nueva directiva. También se pueden copiar los datos de una directiva existente en otra directiva existente.

Siga los pasos descritos a continuación para copiar una directiva:

1. Inicie Faronics Core Console.
2. En el *panel de vista de árbol de la consola*, vaya a *Faronics Core Console>[Core Server]>Estaciones de trabajo administradas>Anti-Virus>[Nombre de directiva]*.
3. Haga clic con el botón secundario en la directiva y seleccione *Copiar directiva*. Aparecerá el cuadro de diálogo *Copiar directiva*.
4. Seleccione una *Directiva de destino* en la lista desplegable o haga clic en *Nueva* para copiar los datos en una nueva directiva. Especifique un nombre para la nueva directiva.
5. Haga clic en *Copiar datos de directiva ahora*.

Los datos se copiarán en una directiva existente o en una nueva directiva, según la opción especificada en el paso 3.

Eliminación de una directiva de Anti-Virus

Siga los pasos descritos a continuación para eliminar una directiva existente:

1. Inicie Faronics Core Console.
2. En el *panel de vista de árbol de la consola*, vaya a *Faronics Core Console>[Core Server]>Estaciones de trabajo administradas>Anti-Virus>[Nombre de directiva]*.
3. Haga clic con el botón secundario en la directiva y seleccione *Eliminar directiva*. Aparecerá el cuadro de diálogo *Eliminar directiva*.
4. Haga clic en *Sí* para eliminar la directiva.

Si se elimina una directiva asignada a una estación de trabajo, se sustituirá por la directiva predeterminada. No es posible eliminar la directiva predeterminada.

Importación de una directiva de Anti-Virus

Se puede importar una directiva de Anti-Virus configurada previamente en una directiva existente. Esta función permite ahorrar tiempo, ya que no es necesario volver a configurar toda la directiva.

Siga los pasos descritos a continuación para importar una directiva existente:

1. Inicie Faronics Core Console.
2. En el *panel de vista de árbol de la consola*, vaya a *Faronics Core Console>[Core Server]>Estaciones de trabajo administradas>Anti-Virus>[Nombre de directiva]*.
3. Haga clic con el botón secundario en la directiva y seleccione *Importar directiva*. Haga clic en *Sí* para sobrescribir la configuración actual de la directiva existente.
4. Busque y seleccione la directiva que se va a importar. Solo es posible importar directivas exportadas en formato XML.
5. Seleccione una directiva exportada previamente y haga clic en *Abrir*. Se importará la directiva.

Exportación de una directiva de Anti-Virus

Se puede exportar una directiva de Anti-Virus configurada previamente para utilizarla de nuevo. Esta función permite ahorrar tiempo, ya que no es necesario volver a configurar toda la directiva.

Siga los pasos descritos a continuación para exportar una directiva existente:

1. Inicie Faronics Core Console.
2. En el *panel de vista de árbol de la consola*, vaya a *Faronics Core Console>[Core Server]>Estaciones de trabajo administradas>Anti-Virus>[Nombre de directiva]*.
3. Haga clic con el botón secundario en la directiva y seleccione *Exportar directiva*.
4. Busque y seleccione la ubicación.
5. Especifique un nombre de archivo y haga clic en *Guardar*. La directiva se exportará en formato XML.

Análisis mediante Faronics Core Console

El análisis se puede realizar en forma manual, según esté programado en la política Anti-Virus o se puede programar una tarea a través de Faronics Core Console. Realice los siguientes pasos para analizar manualmente las estaciones de trabajo a través de Faronics Core Console:

1. Inicie Faronics Core Console.
2. Vaya al panel *Lista de estaciones de trabajo*.
3. Haga clic en una o más estaciones de trabajo y seleccione *Scan (Analizar)*.
   > Seleccione *Scan (Análisis)*>*Quick (Rápido)* para realizar un análisis rápido.
   > Seleccione *Scan (Análisis)*>*Deep (Profundo)* para realizar un análisis profundo.
   > Seleccione *Fix Now (Arreglar ahora)* para descargar las últimas definiciones de virus y realizar un análisis. Si la Protección activa fue deshabilitada temporalmente por el usuario, se habilitará cuando se seleccione Fix Now (Arreglar ahora).

El progreso del análisis (*% del análisis completado*) se muestra en el panel *Lista de estaciones de trabajo* en Faronics Core Console.

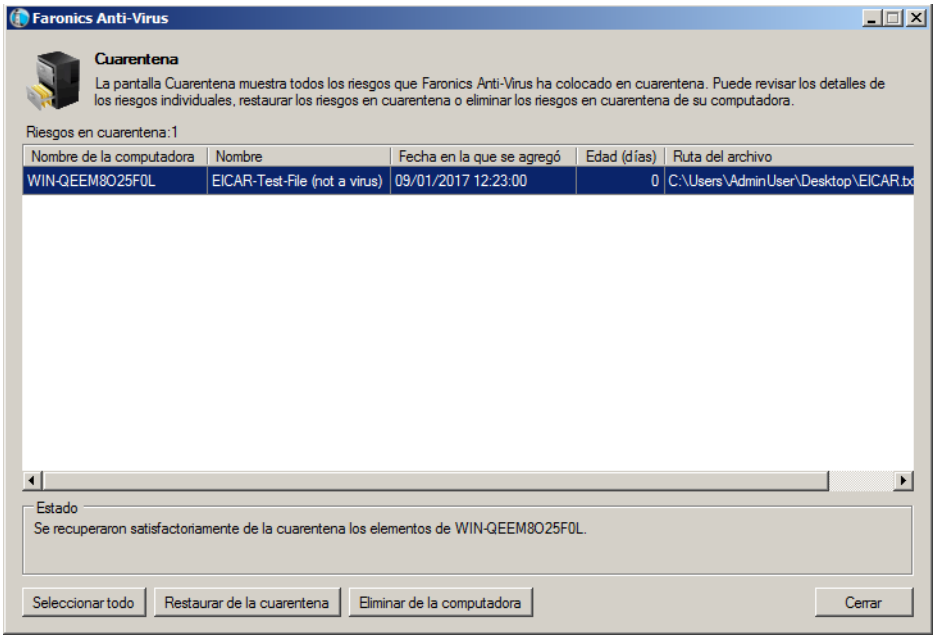
Si hay más de un Loadin instalado, se puede acceder al menú contextual de Faronics Anti-Virus al hacer clic derecho en una estación de trabajo, seleccionar *Faronics Anti-Virus* y luego seleccionar la acción en particular.

La protección activa debe estar habilitada para que la función Fix Now (Arreglar ahora) funcione a través de Faronics Core Console.

Ver y tomar medidas acerca de los archivos en cuarentena

Realice los siguientes pasos para ver los archivos que Faronics Anti-Virus puso en cuarentena:

1. Inicie Faronics Core Console.
2. Vaya al panel *Lista de estaciones de trabajo* .
3. Seleccione la estación de trabajo.
4. Haga clic derecho en la estación de trabajo y seleccione *Ver cuarentena*. Se mostrará la lista de los archivos en cuarentena.



5. Se mostrará la siguiente información acerca de cada archivo infectado:
   - > Nombre de riesgo
   - > Nombre del archivo
   - > Ubicación original
   - > Fecha en la que se agregó
   - > Edad (días)
6. Seleccione las siguientes acciones:
   - > Detalles: seleccione un archivo y haga clic en Detalles para ver los detalles del archivo infectado. Esto también muestra la acción recomendada.
   - > Seleccionar todo: selecciona todos los archivos.
   - > Eliminar del equipo: elimina el archivo seleccionado del equipo.
   - > Restaurar de la cuarentena: restaura el archivo seleccionado del equipo.
   - > Cerrar: cierra el diálogo.

Actualización de Faronics Anti-Virus a través de Faronics Core Console

Las definiciones de Faronics Anti-Virus se pueden actualizar en las estaciones de trabajo a través de Faronics Core Console. Faronics Core actúa como el depósito de actualizaciones del Anti-Virus para las estaciones de trabajo administradas. Faronics Core envía las actualizaciones del Anti-Virus automáticamente a las estaciones de trabajo remotas. Además, Faronics Core Administrator puede actualizar manualmente las definiciones de virus, como se describe a continuación.

Realice los siguientes pasos para actualizar Faronics Anti-Virus en las estaciones de trabajo:

1. Inicie Faronics Core Console.
2. Vaya al panel *Lista de estaciones de trabajo*.
3. Haga clic con el botón derecho del mouse en una o más estaciones de trabajo y seleccione *Update (Actualizar)*.
   > Seleccione *Update (Actualizar)*>*Full Update (Actualización total)*: esto actualiza las definiciones Anti-Virus.
   > Seleccione *Update (Actualizar)*>*Full Force Update (Forzar actualización completa)*: esto elimina las definiciones existentes del Anti-Virus y las actualiza con las últimas definiciones Anti-Virus.

Programación de acciones para Faronics Anti-Virus a través de Faronics Core Console

Es posible programar los eventos de Anti-Virus y de Faronics Core Console para que ocurran en una o más estaciones de trabajo en una fecha y hora convenientes para el administrador. Haga clic en una o más estaciones de trabajo y seleccione *Schedule Action (Programar acción)*. Los submenús que aparecen contienen la siguiente lista de acciones disponibles:

Acciones controladas por Faronics Core Console:

- Apagar
- Reiniciar
- Reactivar

Acciones controladas por Faronics Anti-Virus:

- Habilitar la >protección activa
- Deshabilitar >protección activa
- Análisis > rápido
- Análisis > profundo
- Actualizar > Actualización total
- Actualizar > Forzar actualización completa
- Arreglar ahora
- Instalar/Actualizar el cliente anti-virus
- Desinstalar cliente anti-virus

Al seleccionar una acción aparece un menú *Schedule (Programar)* que le permite al administrador especificar la frecuencia (una sola vez, todos los diariamente, semanalmente, mensualmente). De acuerdo con la frecuencia, podrá seleccionar la hora, el día, la fecha o el mes.

La tarea programada a través de una política Anti-Virus siempre tiene precedencia por sobre una acción programada a través de Faronics Core Console.

Generación de informes

Faronics Anti-Virus proporciona muchos informes para monitorear la actividad de cada estación de trabajo. Hay dos categorías de informes:

- Informes globales: estos informes se basan en todas las estaciones de trabajo protegidas por Faronics Anti-Virus.
- Informes específicos de una estación de trabajo: estos informes son específicos para la estación de trabajo seleccionada.

Informes globales

Realice los siguientes pasos para generar un informe global:

1. Inicie Faronics Core Console.
2. En el panel *Console Tree (Árbol de la consola)*, vaya a *Faronics Core Console>[Nombre de Core Server]>Managed Workstations (Estaciones de trabajo administradas)>Anti-Virus*.
3. En el panel *Action (Acción)*, haga clic en *Global Reports (Informes globales)*.
4. Seleccione el informe e ingrese un rango de fechas en el diálogo que aparece. Haga clic en *OK (Aceptar)*. Estos son los informes disponibles:
   > Amenazas por número de detecciones: se muestran las amenazas detectadas por el número de detecciones en todas las estaciones de trabajo administradas por Faronics Anti-Virus.
   > Resumen de gravedad de las amenazas: se muestra el resumen de la gravedad de las amenazas.
   > Principales 25 máquinas infectadas: se muestran las principales 25 computadoras infectadas.
5. Se muestra el informe seleccionado en el panel *Console Tree (Árbol de la consola)* en el nodo>*Informes*.

Informes específicos de una estación de trabajo

Realice los siguientes pasos para generar un informe específico para una estación de trabajo:

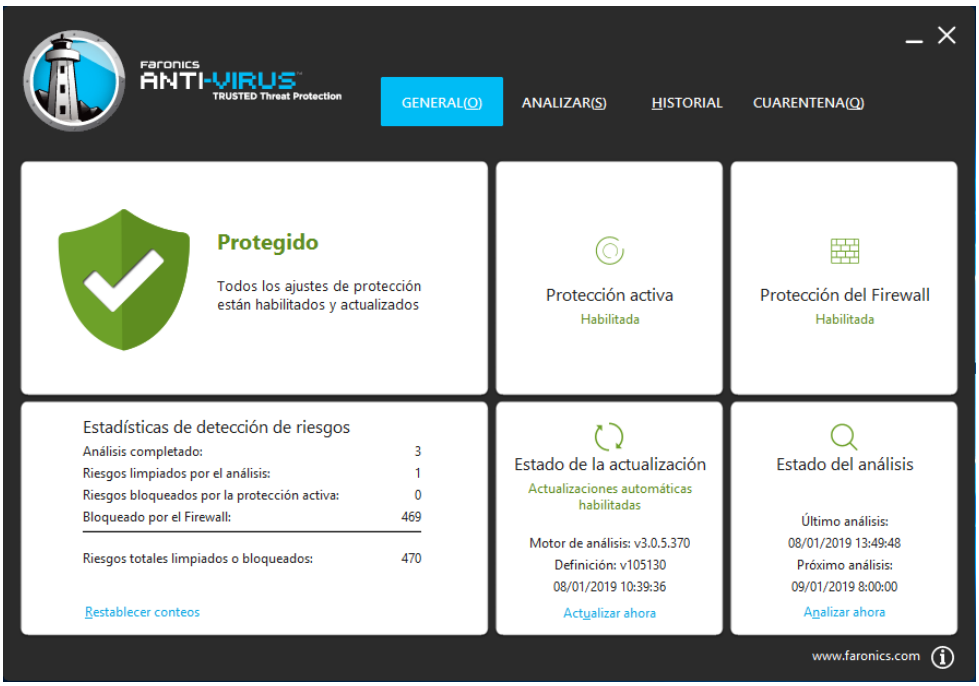
1. Inicie Faronics Core Console.
2. En el panel *Console Tree (Árbol de la consola)*, vaya a *Faronics Core Console>[Nombre de Core Server]>Managed Workstations (Estaciones de trabajo administradas)*.
3. Seleccione la estación de trabajo para la cual desea generar el informe.
4. Haga clic derecho en la estación de trabajo y seleccione *Informes*.
5. Seleccione el informe e ingrese un rango de fechas en el diálogo que aparece. Haga clic en *OK (Aceptar)*. Estos son los informes disponibles:
   > Detalles de la estación de trabajo
   > Último análisis
   > Historial de análisis
   > Historial de protección activa
   > Cuarentena
   > Historial de protección del correo electrónico
   > Mensajes de eventos del sistema
6. Se muestra el informe seleccionado en el panel *Console Tree (Árbol de la consola)* en el nodo>*Informes*.

Uso de Faronics Anti-Virus en la estación de trabajo

Las funciones disponibles en Faronics Anti-Virus en la estación de trabajo dependen completamente de la configuración seleccionada en la política Anti-Virus. Para obtener más información acerca de la política Anti-Virus, consulte Política de Faronics Anti-Virus.

Inicio de Faronics Anti-Virus en la estación de trabajo

Vaya a *Start (Inicio)*>*Programs (Programas)*>*Faronics*>*Anti-Virus Enterprise*>*Faronics Anti-Virus Enterprise*. Como alternativa, puede hacer doble clic en el icono de Faronics Anti-Virus en la bandeja de sistema.



Los siguientes paneles muestran información importante para el usuario:

- *Protected (Protegido)* o *Not Protected (No protegido)* aparece para notificar si el equipo está protegido o no. Si aparece Not Protected (No protegido), haga clic en el botón *Fix Now (Arreglar ahora)* debajo del aviso *Not Protected (No protegido)*.
- *Estado del análisis* muestra cuándo se realizó el último análisis. Para analizar ahora, haga clic en el enlace *Analizar ahora*.
- *Estado de la actualización* muestra cuándo se realizó la última actualización. Para actualizar las definiciones de virus, haga clic en el enlace *Actualizar todo ahora*.
- *Protección activa* muestra si está habilitada la protección en tiempo real.
- *Protección del correo electrónico* muestra si el correo electrónico está protegido por Faronics Anti-Virus.
- La protección del Firewall muestra si la estación de trabajo está protegida por el Firewall.
- *Estadísticas de detención de riesgos* muestra las estadísticas para las acciones que ha realizado Faronics Anti-Virus. Haga clic en *Restablecer conteos* para restablecer los conteos a cero.

Análisis de la estación de trabajo

Realice los siguientes pasos para analizar una estación de trabajo:

1. Vaya a *Start (Inicio)>Programs (Programas)>Faronics>Anti-Virus Enterprise> Faronics Anti-Virus Enterprise*. Como alternativa, puede hacer doble clic en el icono de Faronics Anti-Virus en la bandeja de sistema.

2. En el panel *Estado del análisis*, haga clic en *Analizar ahora*. Se mostrará la ficha *Analizar*. Como alternativa, también puede hacer clic en la ficha *Analizar*.

3. Seleccione una de las siguientes opciones:
   - > Análisis rápido: analiza sólo en busca de las amenazas conocidas.
   - > Análisis profundo del sistema: realiza un análisis detallado de todos los archivos de la estación de trabajo.
   - > Análisis personalizado (seleccione uno de los siguientes):
     - ~ Analizar los procesos en ejecución: analiza los procesos en ejecución en la estación de trabajo.
     - ~ Analizar el registro: analiza el registro.
     - ~ Analizar cookies: analiza los archivos cookies guardados en la estación de trabajo.
     - ~ Especifica las unidades y las carpetas que se analizarán: Haga clic en Browse (Examinar) para seleccionar las carpetas.
4. Haga clic en *Analizar ahora*. El ícono que gira indica que se está realizando un análisis. Los resultados del análisis se muestran luego de que haya finalizado el análisis.
5. Seleccione el archivo y las siguientes opciones estarán disponibles:
   - > Seleccione *Cambiar acción de limpieza*>*Acción recomendada* para realizar la acción recomendada por Faronics Anti-Virus.
   - > Seleccione *Cambiar acción de limpieza*>*Poner en cuarentena/Desinfectar* para poner en cuarentena o desinfectar el archivo.
   - > Seleccione *Cambiar acción de limpieza*>*Eliminar* para eliminar el archivo.
   - > Seleccione *Cambiar acción de limpieza*>*Permitir* para permitir el archivo.
   - > Haga clic en *Seleccionar todo* para seleccionar todos los archivos que se muestran en el *Resultado del análisis*.
   - > Haga clic en *Detalles* para mostrar los detalles del riesgo.
   - > Haga clic en *Cancelar* para cerrar el diálogo sin realizar ninguna acción.
   - > Haga clic en *Limpiar* para eliminar el archivo y cerrar el diálogo.

La acción también se puede realizar a través de Faronics Core Console. Para obtener más información consulte Ver y tomar medidas acerca de los archivos en cuarentena.

Análisis de un archivo o una carpeta con clic del botón derecho

Es muy fácil analizar en busca de virus los archivos o las carpetas (de a uno o varios). Cuando Faronics Anti-Virus está instalado en una estación de trabajo, la opción Analizar en busca de virus se agrega al menú que aparece al hacer clic derecho.

Realice los siguientes pasos para analizar un archivo o una carpeta en el equipo:

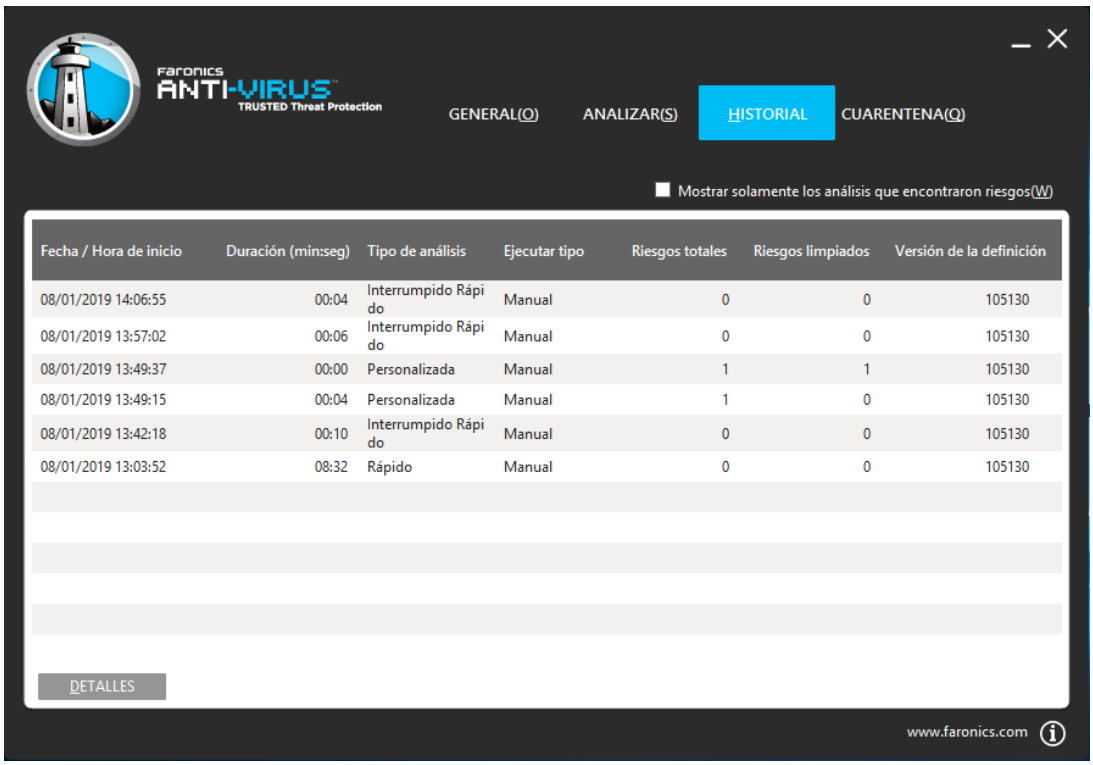
1. Haga clic con el botón derecho en el archivo o la carpeta.
2. Seleccione *Analizar en busca de virus*.

Se realizará el análisis y se mostrarán los resultados.

Ver historial de análisis

Realice los siguientes pasos para ver el historial de análisis:

1. Vaya a *Start (Inicio)>Programs (Programas)>Faronics>Anti-Virus Enterprise>Faronics Anti-Virus Enterprise*. Como alternativa, puede hacer doble clic en el icono de Faronics Anti-Virus en la bandeja de sistema.
2. Haga clic en la ficha *Historial*.

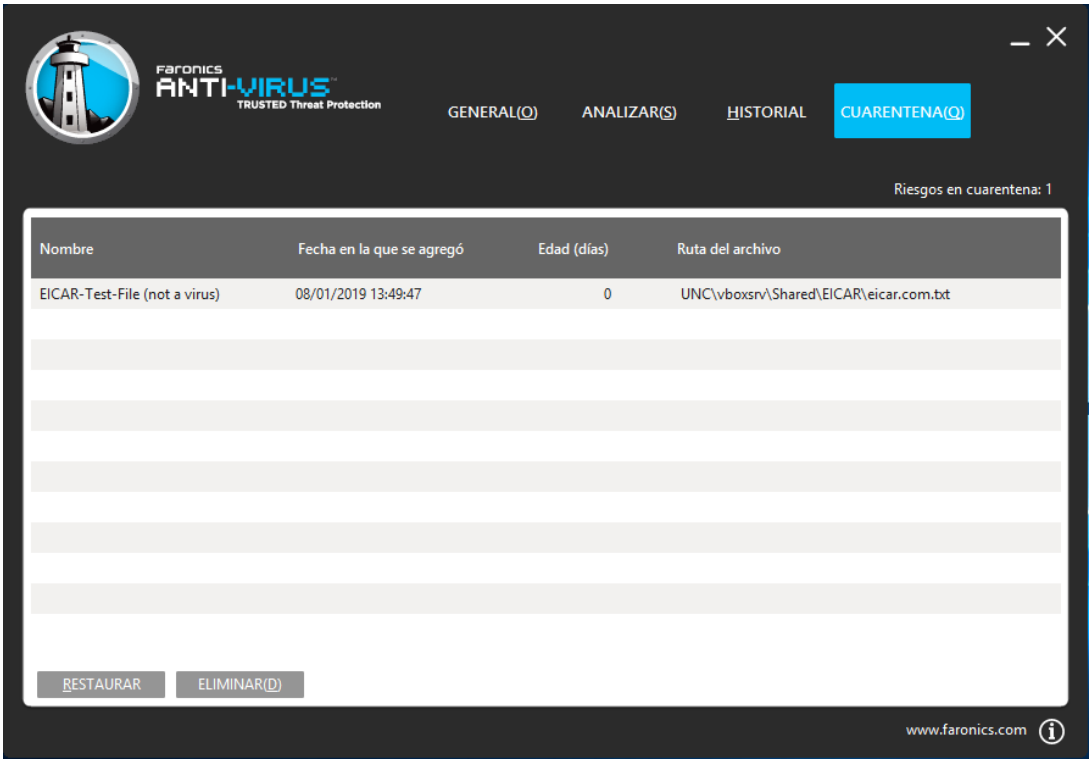


3. Seleccione las siguientes acciones:
   - > Mostrar solamente los análisis que encontraron riesgos: seleccione esta opción para ver solamente los análisis en los que se encontraron riesgos.
   - > Detalles: seleccione una entrada y haga clic en los detalles para ver los detalles del análisis.

Ver y tomar medidas acerca de los archivos en cuarentena

Realice los siguientes pasos para ver Cuarentena:

1. Vaya a *Start (Inicio)*>*Programs (Programas)*>*Faronics*>*Anti-Virus Enterprise*>*Faronics Anti-Virus Enterprise*. Como alternativa, puede hacer doble clic en el icono de Faronics Anti-Virus en la bandeja de sistema.
2. Haga clic en la ficha *Cuarentena*.



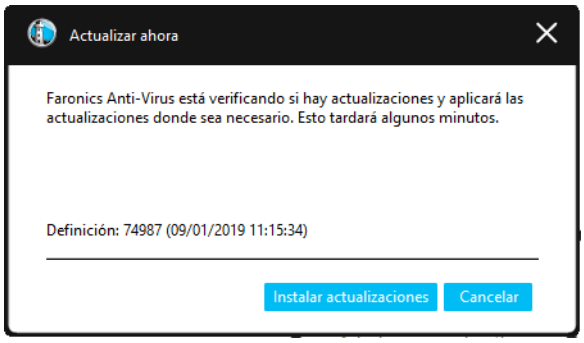
3. Haga clic en *Detalles de los riesgos*. Se mostrará la siguiente información acerca de cada archivo infectado:
   - > Nombre
   - > Categoría de riesgo
   - > Fecha en la que se agregó
   - > Edad (días)
   - > En cuarentena por

Actualización de las definiciones anti-virus en la estación de trabajo

Realice los siguientes pasos para actualizar Faronics Anti-Virus en una estación de trabajo:

1. Vaya a *Start (Inicio)>Programs (Programas)>Faronics>Anti-Virus Enterprise>Faronics Anti-Virus Enterprise*. Como alternativa, puede hacer doble clic en el icono de Faronics Anti-Virus en la bandeja de sistema.

2. En el panel *Estado de la actualización*, haga clic en *Actualizar ahora*. Se mostrará el cuadro de diálogo *Actualizar ahora*.



3. Haga clic en *Instalar actualizaciones*. Se actualizarán las definiciones de virus en la estación de trabajo.

Administración de Faronics Anti-Virus en la estación de trabajo a través de la bandeja de sistema

Faronics Anti-Virus se puede administrar en la estación de trabajo a través de un menú disponible en la bandeja de sistema.

Haga clic derecho en el icono de Faronics Anti-Virus en la bandeja de sistema. Estas son las opciones disponibles:

- Abrir Faronics Anti-Virus: inicia Faronics Anti-Virus en la estación de trabajo.
- Protección activa
  - > *Protección activa>Habilitar la protección activa*: habilita la protección activa.
  - > *Protección activa>Deshabilitar la protección activa>[Seleccione la opción]*: selecciona el tiempo durante el cual la protección activa estará deshabilitada. Seleccione 5 minutos, 15 minutos, 30 minutos, 1 hora, hasta que el equipo se reinicie o permanentemente. Esta opción se muestra sólo si se seleccionó en la política Anti-Virus.
- *Analizar ahora>[Seleccione la opción]*: seleccione Cancelar análisis, Pausar análisis, Reiniciar análisis, Análisis rápido o Análisis profundo. Esta opción se muestra sólo si se seleccionó en la política Anti-Virus.
- *Protección de firewall>Habilitar* o *Deshabilitar*.

Las opciones anteriores están disponibles para el usuario sólo si se especificaron en la política Anti-Virus. Para obtener más información, consulte Creación de directivas de Anti-Virus.

Control de línea de comandos

Este capítulo explica los diversos controles de la línea de comandos disponibles para Faronics Anti-Virus.

Temas

Control de línea de comandos

El control de la línea de comandos de Faronics Anti-Virus ofrece a los administradores de red una mayor flexibilidad en la administración de estaciones de trabajo con Faronics Anti-Virus al permitir el control a través de herramientas de administración de terceros y/o soluciones de administración central.

Realice los siguientes pasos para ejecutar los comandos de Faronics Anti-Virus:

1. En la estación de trabajo vaya al *<directorio del sistema>:\Program Files\Faronics\Faronics Anti-Virus Enterprise* desde la solicitud de comandos.
2. Ingrese `AVECLI/[Command]`

Estos son los comandos disponibles:

Comando	Definición
`definitionversion`	Muestra la versión de la definición de virus.
`scanengineversion`	Muestra la versión del motor de análisis.
`updatedefs`	Actualiza y aplica las definiciones de virus.
`scanquick`	Inicia un análisis rápido.
`scandeep`	Inicia un análisis profundo.
`fixnow`	Descarga la última definición de virus. Habilita la protección activa y la protección del correo electrónico. Realiza el análisis profundo predeterminado
`setlicense[clave]`	Aplica una clave de licencia determinada.
`enableap`	Habilita la protección activa.
`fixnow /quick`	Realiza un análisis rápido si es

Sintaxis:

```
AVECLI/definitionversion
```

Desinstalación de Faronics Anti-Virus

Este capítulo describe cómo desinstalar Faronics Anti-Virus.

Temas

Generalidades sobre la desinstalación

Faronics Anti-Virus Loadin se encuentra instalado en el sistema Faronics Core Console (o Faronics Core Server). Faronics Anti-Virus Client se encuentra instalado en las estaciones de trabajo.

Desinstale Faronics Anti-Virus Client de la estación de trabajo manualmente o a través de Faronics Core Console. Una vez que haya terminado, desinstale Faronics Anti-Virus Loadin del sistema Faronics Core Console (o Faronics Core Server).

El proceso de desinstalación se explica en las siguientes secciones.

Desinstalación de Faronics Anti-Virus Client a través de Faronics Core Console

Realice los siguientes pasos para desinstalar Faronics Anti-Virus Client a través de Faronics Core Console:

1. Inicie Faronics Core Console.
2. En el panel *Console Tree (Árbol de la consola)*, vaya a *Faronics Core Console>[Core Server]>Managed Workstations (Estaciones de trabajo administradas)*.
3. Seleccione las estaciones de trabajo de las que desea desinstalar Faronics Anti-Virus Client.
4. Haga clic con el botón derecho y seleccione *Configure Workstations (Configurar estaciones de trabajo)>Advanced (Avanzado)>Uninstall Anti-Virus Client (Desinstalar Anti-Virus Client)*.

Faronics Anti-Virus Client se desinstalará de las estaciones de trabajo.

Desinstalación de Faronics Anti-Virus Client de una estación de trabajo a través de Add or Remove Programs (Agregar o quitar programas)

Realice los siguientes pasos para desinstalar Faronics Anti-Virus a través de *Add or Remove Programs (Agregar o quitar programas)* en Windows:

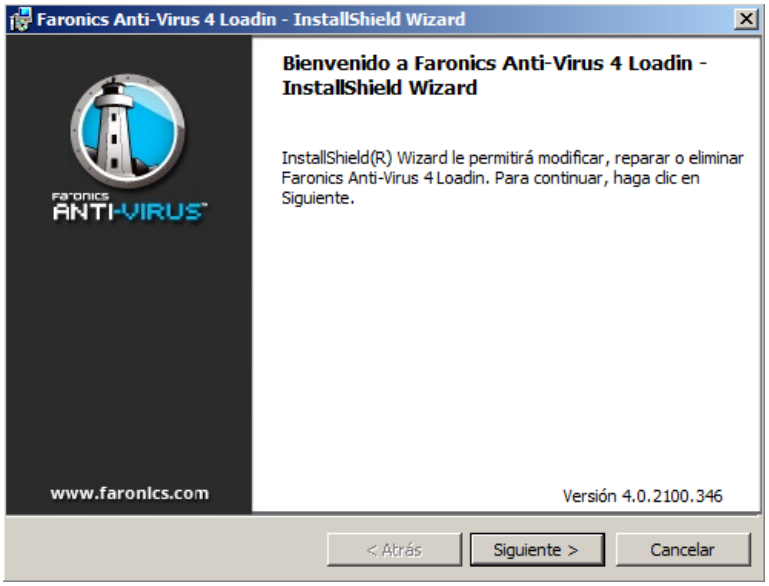
1. Haga clic en *Start (Inicio)*>*Control Panel (Panel de control)*>*Add or Remove Programs (Agregar o quitar programas)*.
2. Seleccione *Faronics Anti-Virus Enterprise Workstation*.
3. Haga clic en *Remove (Quitar)*.

Faronics Anti-Virus Client se desinstalará de la estación de trabajo.

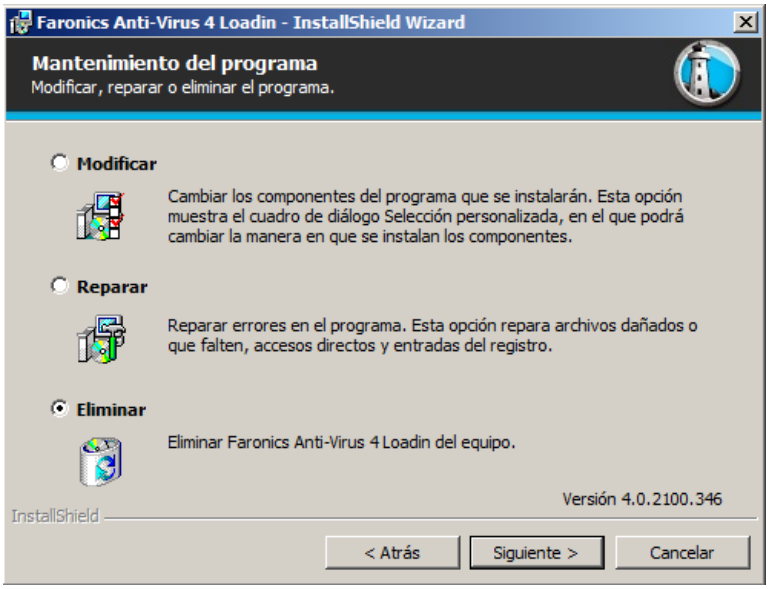
Desinstalación de Faronics Anti-Virus Loadin con el instalador

Realice los siguientes pasos para desinstalar Faronics Anti-Virus Loadin:

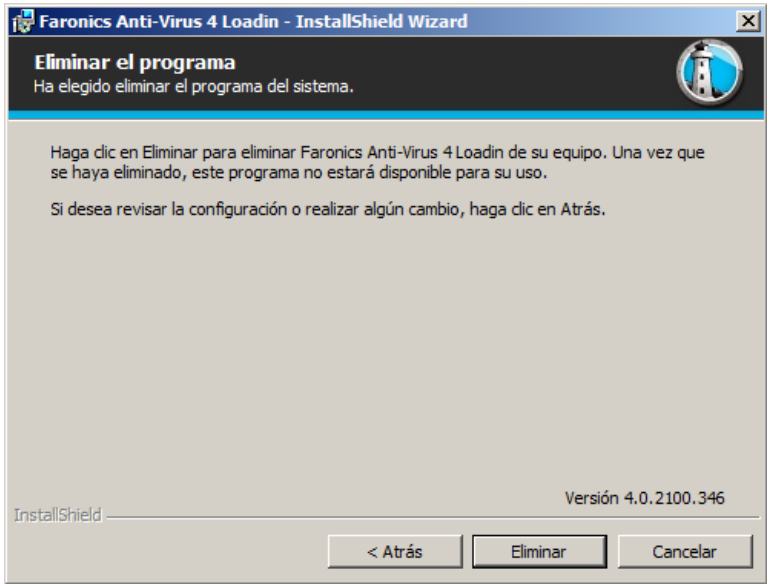
1. Haga doble clic en *Anti-VirusLoadinInstaller.exe*. Haga clic en *Next (Siguiente)*.



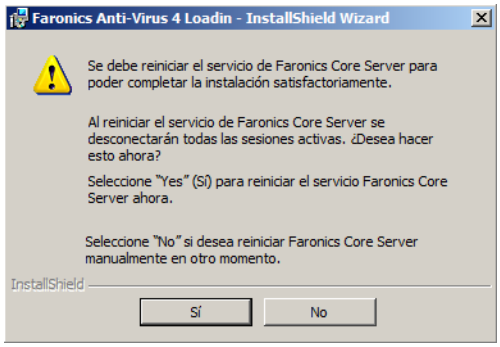
2. Seleccione *Remove (Quitar)*. Haga clic en *Next (Siguiente)*.



3. Haga clic en *Remove (Quitar)*.



4. Se mostrará el siguiente mensaje. Haga clic en *Yes (Sí)* para reiniciar el servicio Faronics Core Server o en *No* para reiniciar manualmente el servicio *Faronics Core Server* en otro momento.



5. Faronics Anti-Virus Loadin se quitará de su equipo. Haga clic en *Finish (Finalizar)* para completar la desinstalación.

Desinstalación de Faronics Anti-Virus a través de Agregar o Quitar Programas

Realice los siguientes pasos para desinstalar Faronics Anti-Virus Loadin a través de *Add or Remove Programs (Agregar o quitar programas)* en Windows:

1. Haga clic en *Start (Inicio)*>*Control Panel (Panel de control)*>*Add or Remove Programs (Agregar o quitar programas)*.
2. Seleccione *Faronics Anti-Virus Loadin*.
3. Haga clic en *Remove (Quitar)*.