Instrucciones de instalación del antivirus de Mac-Lab/CardioLab (ES)

Software Mac-Lab/CardioLab, versión 6.9.6

Introducción

El software antivirus resulta útil para las instalaciones en el cumplimiento de reglamentos de privacidad, como por ejemplo, HIPAA.

Uso del documento

Utilice este documento para instalar el software antivirus validado para el sistema Mac-Lab/CardioLab v6.9.6.

Historial de las revisiones

Revisión	Fecha	Comentarios
A	16 de febrero del 2016	Versión pública inicial.
B	9 de junio de 2016	Actualización de Trend Micro para admitir CO_2.
C	16 de mayo del 2017	Actualizaciones a McAfee ePolicy Ochestrator, Trend Micro y Symantec.
D	10 de julio del 2017	Actualizaciones para Symantec 12.1.6 MP5, Trend Micro 11.0 SP1, McAfee ePO 5.9 y McAfee VSE 8.8 Patch 9.
E	14 de agosto del 2017	Eliminar referencias a McAfee ePolicy Orchestrator 5.9 y McAfee VirusScan Enterprise 8.8 Patch 9. Agregar idiomas para la interfaz de usuario de 6.9.6 R3.
F	25 de septiembre de 2017	Adición de McAfee ePO 5.9 y McAfee VSE 8.8 Patch 9. Actualización de los enlaces para Trend Micro 11 y 12.

Primeros pasos

Requisitos del antivirus

ADVERTENCIA: **INSTALACIÓN DE SOFTWARE ANTIVIRUS OBLIGATORIA**

El sistema se suministra sin protección antivirus. Antes de conectarse a ninguna red, asegúrese de instalar un antivirus autorizado en el sistema. La falta de una protección antivirus autorizada podría tener como consecuencia el fallo o la falta de estabilidad del sistema.

Tenga en cuenta los siguientes requisitos:

- El software antivirus no se proporciona con el sistema Mac-Lab/CardioLab y es obligación del cliente obtenerlo, instalarlo y mantenerlo.
- Corre por cuenta del cliente la obligación de actualizar los archivos de definición de antivirus.
- Si se encuentra un virus, será necesario comunicarse con el administrador del sistema de la institución y con el departamento de soporte técnico de GE.
- Instale solo los paquetes de software antivirus que se recogen en la sección Software antivirus validado.
- Inicie sesión como administrador o como miembro de ese grupo para llevar a cabo las actividades que se mencionan en este documento.
- Si es posible, utilice una versión del software antivirus en el mismo idioma que el sistema operativo. En caso de que no haya ninguna versión del software antivirus en el mismo idioma del sistema operativo, instale la versión en inglés del antivirus.

Software antivirus validado

ADVERTENCIA: **INESTABILIDAD DEL SISTEMA**

No instale ni use software antivirus que no esté validado (incluidas versiones no homologadas). Si lo hace, podría provocar el fallo o la inestabilidad del sistema. Use únicamente software antivirus validado en el idioma apropiado.

NOTA: Si no está disponible el software antivirus en el idioma apropiado, instale la versión en inglés del software antivirus.

Se ha comprobado que los sistemas Mac-Lab/CardioLab v6.9.6 funcionan con el software incluido en la siguiente tabla.

Software antivirus compatible	Idiomas compatibles con MLCL	Versión de software antivirus compatible
McAfee VirusScan Enterprise	Inglés, francés, alemán, italiano, español, sueco, noruego, danés, neerlandés, chino y japonés.	8.8, parche 3 8.8, parche 4 8.8, parche 8 8.8, parche 9
McAfee ePolicy Orchestrator (con McAfee VirusScan Enterprise)	Inglés, francés, alemán, italiano, español, sueco, noruego, danés, neerlandés, chino y japonés.	v5.0 v5.3.2 v5.9
Symantec EndPoint Protection	Inglés, francés, alemán, italiano, español, sueco, noruego, danés, neerlandés, chino y japonés.	12.1.2, 12.1.6 MP5, 14.0 MP1
Trend Micro OfficeScan Client/Server Edition	Inglés, francés, alemán, italiano, español, sueco, noruego, danés, neerlandés, chino y japonés.	10.6 SP2, 11.0 SP1, XG 12.0

El software antivirus compatible está disponible en los idiomas enumerados en la siguiente tabla.

Versión MLCL	Idiomas compatibles con MLCL
M6.9.6 R1	Inglés
M6.9.6 R2	Inglés, francés y alemán.
M6.9.6 R3	Inglés, francés, alemán, italiano, español, sueco, noruego, danés, neerlandés, chino y japonés.

Configuración del servidor de la consola de administración del antivirus

Es necesario que la consola de administración del antivirus esté instalada en el servidor de la consola de administración del antivirus.

La comunicación entre el servidor de la consola de administración del antivirus y los dispositivos Mac-Lab/CardioLab puede establecerse de distintas formas en función del entorno:

1. Entorno del controlador de dominio de INW: en el servidor de la consola de administración del antivirus, no en el dominio de INW Server
   - Tipo de comunicación: 1 <misma red con la misma máscara de subred>
   - Tipo de comunicación: 2 <red diferente con máscara de subred distinta>
2. Entorno del controlador de dominio del hospital: en el servidor de la consola de administración del antivirus, no en el dominio del controlador de dominio del hospital
   - Tipo de comunicación: 1 <red diferente con máscara de subred distinta>
3. Entorno del controlador de dominio del hospital: servidor de la consola de administración del antivirus en el dominio del controlador de dominio del hospital
   - Tipo de comunicación: 1 <misma red con la misma máscara de subred>

NOTA: El servidor de la consola de administración del antivirus debe tener dos puertos de red. Un puerto de red para la conexión a la red Centricity Cardiology INW y un segundo puerto de red para la conexión a la red del hospital.

Diagrama de bloques del entorno del controlador de dominio de INW

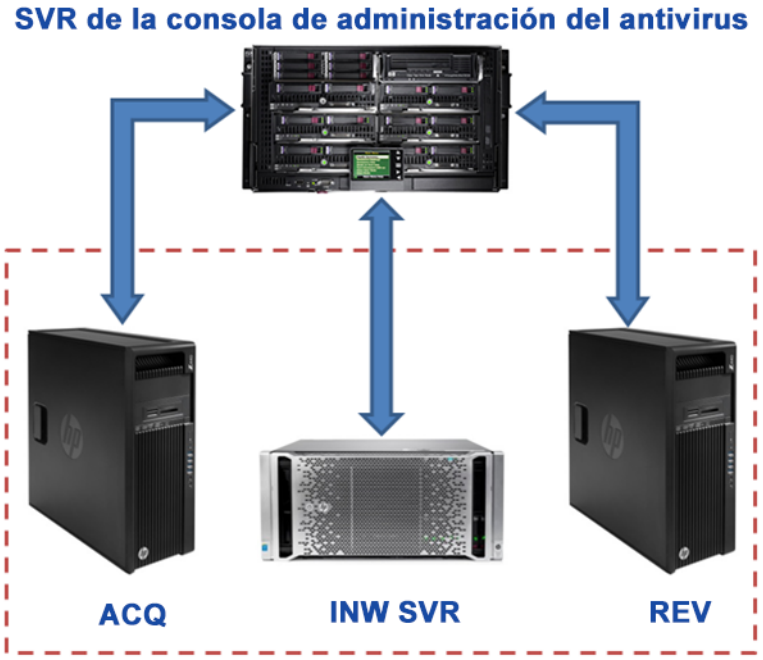
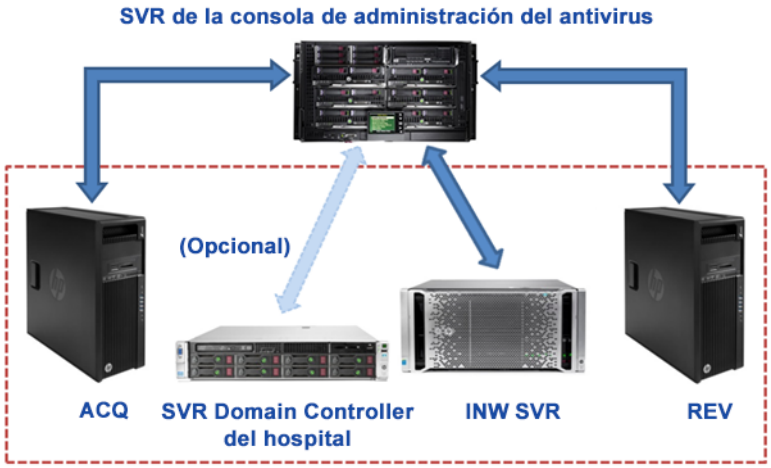
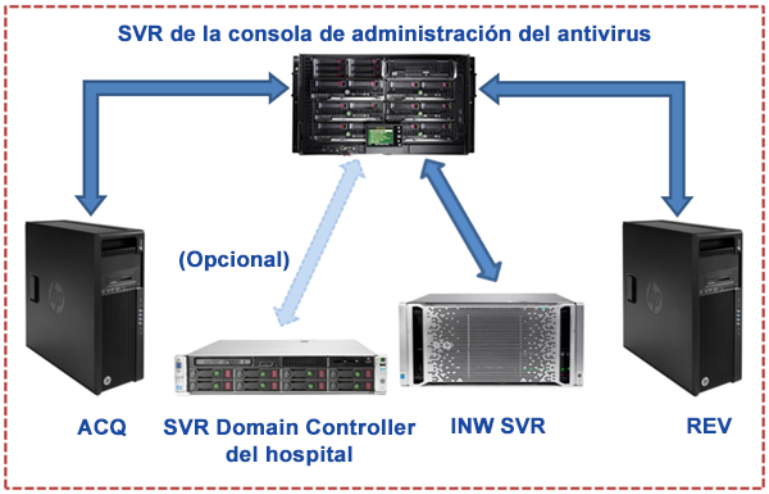


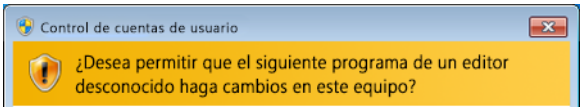
Diagrama de bloques del entorno del controlador de dominio del hospital





Control de cuentas de usuario

El control de cuentas de usuario es una función de Windows que evita que se realicen cambios no autorizados en un equipo. Durante algunos de los procedimientos que se describen en este manual, se muestra un mensaje de control de cuentas de usuario.



Es seguro continuar cuando se muestre este mensaje por haber seguido los procedimientos de este manual.

Instrucciones de instalación del antivirus

Haga clic en el software antivirus que desea instalar:

Procedimientos de instalación habituales del software antivirus

Utilice los procedimientos de esta sección cuando se haga referencia a ellos en las instrucciones de instalación del antivirus.

Desactivar la conexión de bucle invertido

En un sistema de adquisición conectado al entorno de Mac-Lab/CardioLab, desactive la conexión de bucle invertido para ver todos los sistemas del cliente con la misma máscara de subred en el dominio.

1. Inicie sesión como **Administrator** (Administrador) o como miembro de ese grupo.
2. En el escritorio, haga clic con el botón derecho en ***Network*** (Red) y seleccione ***Properties*** (Propiedades).
3. Haga clic en ***Change adapter settings*** (Cambiar configuración del adaptador).
4. Haga clic con el botón derecho en ***Loopback Connection*** (Conexión de bucle invertido) y seleccione ***Disable*** (Desactivar).
5. Reinicie el sistema de adquisición.

NOTA: Es necesario desactivar la conexión de bucle invertido en el sistema de adquisición para detectar todos los sistemas del cliente con la misma máscara de subred en el dominio.

Activar la conexión de bucle invertido

En los sistemas de adquisición conectados al entorno de Mac-Lab/CardioLab, active la conexión de bucle invertido mediante los pasos siguientes.

1. Inicie sesión como **Administrator** (Administrador) o como miembro de ese grupo.
2. En el escritorio, haga clic con el botón derecho en ***Network*** (Red) y seleccione ***Properties*** (Propiedades).
3. Haga clic en ***Change adapter settings*** (Cambiar configuración del adaptador).
4. Haga clic con el botón derecho en ***Loopback Connection*** (Conexión de bucle invertido) y seleccione ***Enable*** (Activar).
5. Reinicie el sistema de adquisición.

Configurar el servicio de Explorador de equipos antes de instalar el antivirus

Compruebe la configuración del servicio de Explorador de equipos en los sistemas de adquisición y revisión para asegurarse de que está configurado correctamente.

1. Haga clic en ***Start > Control Panel > Network and Sharing Center*** (Inicio > Panel de control > Centro de redes y recursos compartidos).
2. Haga clic en ***Change advanced sharing settings*** (Cambiar configuración de uso compartido avanzado).
3. Expanda ***Home or Work*** (Casa o trabajo).
4. Asegúrese de que se ha seleccionado la opción ***Turn on file and printer sharing*** (Activar el uso compartido de archivos e impresoras).
5. Haga clic en ***Save Changes*** (Guardar cambios).
6. Haga clic en ***Start > Run*** (Inicio > Ejecutar).
7. Escriba **services.msc** y pulse **Enter** (Intro).
8. Haga doble clic en el servicio de ***Computer Browser*** (Explorador de equipos).
9. Asegúrese de que la opción ***Startup type*** (Tipo de inicio) se ha establecido en ***Automatic*** (Automático). Si no está establecido en Automatic (Automático), cambie la configuración y haga clic en ***Enter*** (Intro).
10. Haga clic en ***OK*** (Aceptar).
11. Cierre la ventana ***Services*** (Servicios).

Configurar el servicio del Explorador de equipos después de instalar el antivirus

Tras instalar el software antivirus, compruebe la configuración del servicio del Explorador de equipos en los sistemas de adquisición y revisión para asegurarse de que está configurado correctamente.

1. Haga clic en ***Start > Run*** (Inicio > Ejecutar).
2. Escriba **services.msc** y pulse **Enter** (Intro).
3. Haga doble clic en el servicio de ***Computer Browser*** (Explorador de equipos).
4. Cambie el ***Tipo de inicio*** a ***Automático***.
5. Haga clic en ***OK*** (Aceptar).
6. Cierre la ventana ***Services*** (Servicios).

Symantec EndPoint Protection (12.1.2, 12.1.6 MP5 o 14.0 MP1)

Descripción de la instalación

Instale Symantec EndPoint Protection solo en un entorno de red de Mac-Lab/CardioLab. En un sistema en red, Symantec EndPoint Protection se debe instalar en el servidor de la consola de administración del antivirus e implementar en el servidor Centricity Cardiology INW y en las estaciones de trabajo de adquisición y revisión como clientes. Utilice las siguientes instrucciones para instalar y configurar ***Symantec EndPoint Protection***.

Las actualizaciones de virus son responsabilidad de la institución. Actualice las definiciones con regularidad para asegurar que el sistema cuente con la protección antivirus más reciente.

Pautas previas a la instalación

1. Se espera que la consola de administración del antivirus Symantec se instale de acuerdo con las instrucciones de Symantec y que funcione de manera correcta.
2. Inicie sesión como **Administrator** (Administrador) o como miembro de ese grupo en todos los sistemas del cliente (adquisición, revisión y INW Server) para instalar el software antivirus.
3. Abra el símbolo del sistema en modo ***Run As Administrator*** (Ejecutar como administrador).
4. Vaya a C:\Program Files\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec.

NOTA: Para configurar INW Server, vaya a C:\Program Files (x86)\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec.

5. Escriba **UpdateRegSymantec.ps1** y pulse ***Enter*** (Intro).
6. Confirme que el script se ha ejecutado de forma correcta.

   Si no se encuentra la ruta de la carpeta mencionada con anterioridad, realice los siguientes pasos para todos los sistemas MLCL, excepto para MLCL 6.9.6R1 INW Server (sistema operativo del servidor: Windows Server 2008R2).

   a. Haga clic en el botón de ***Start*** (Inicio) y, a continuación, en ***Run*** (Ejecutar).

   b. Escriba **Regedit.exe** y haga clic en ***OK*** (Aceptar).

   c. Vaya a ***HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing***.

   d. Localice y haga doble clic en el registro ***State*** (Estado).

   e. Cambie la ***Base*** a ***Decimal***.

   f. Cambie el ***Value data*** (Datos de valor) a ***146432***.

   g. Haga clic en ***OK*** (Aceptar) y cierre el registro.

7. Desactive la conexión de bucle invertido. Para obtener más información, consulte Desactivar la conexión de bucle invertido en la página 6.
8. Configure el servicio del Explorador de equipos. Para obtener más información, consulte Configurar el servicio de Explorador de equipos antes de instalar el antivirus en la página 7.

Symantec EndPoint Protection: pasos para la implementación de una nueva instalación (método preferido de instalación forzada)

1. Haga clic en ***Start > All Programs > Symantec EndPoint Protection Manager > Symantec Endpoint Protection Manager*** (Inicio > Todos los programas > Symantec EndPoint Protection Manager > Symantec Endpoint Protection Manager).
2. Introduzca el nombre de usuario y la contraseña para iniciar sesión en Symantec Endpoint Protection Manager. Haga clic en ***Yes*** (Sí) si se muestra un aviso de seguridad.
3. Marque la opción ***Do not show this Welcome Page again*** (No volver a mostrar esta página principal) y, a continuación, haga clic en ***Close*** (Cerrar) para salir de la pantalla de bienvenida.

NOTA: En la versión 14.0 MP1, haga clic en ***Close*** (Cerrar) para salir de la pantalla ***Getting Started on Symantec EndPoint Protection*** (Introducción a Symantec EndPoint Protection).

4. Haga clic en ***Admin*** en la ventana ***Symantec EndPoint Protection Manager***.
5. Haga clic en ***Install Packages*** (Instalar paquetes) en el panel inferior.
6. Haga clic en ***Client Install Feature Set*** (Conjunto de funciones de instalación del cliente) en el panel superior.
7. Haga clic con el botón derecho en la ventana ***Client Install Feature Set*** (Conjunto de funciones de instalación del cliente) y seleccione ***Add*** (Agregar). Aparece la ventana Add Client Install Feature Set (Agregar conjunto de funciones de instalación del cliente).
8. Introduzca el nombre adecuado y regístrelo para utilizarlo después.
9. Asegúrese de que la ***versión del conjunto de funciones*** es ***12.1 RU2 y posteriores***.
10. Seleccione solo las siguientes funciones y anule la selección de las demás.
    - ***Virus, Spyware, and Basic Download Protection*** (Virus, spyware y protección de descarga básica).
    - ***Advanced Download Protection*** (Protección de descarga avanzada).
11. En el cuadro de mensaje, haga clic en ***OK*** (Aceptar).
12. Solo en las versiones 12.1.2 y 12.1.6 MP5, haga clic en ***OK*** (Aceptar) para cerrar la ventana ***Add Client Install Feature Set*** (Agregar conjunto de funciones de instalación del cliente).
13. Haga clic en ***Home*** (Inicio) en la ventana ***Symantec Endpoint Protection Manager***.
14. En función de la versión del software, realice una de las siguientes acciones:
    - **Versiones 12.1.2 y 12.1.6 MP5:** Seleccione la opción ***Install protection client to computers*** (Instalar cliente de protección en equipos) de la lista desplegable ***Common Tasks*** (Tareas comunes) situada en la parte superior derecha de la ventana ***Home*** (Inicio). Aparece la pantalla Client Deployment Type (Tipo de implementación del cliente).
    - **Versión 14.0 MP1:** Haga clic en ***Clients*** (Clientes) en la ventana ***Symantec Endpoint Protection Manager***. Haga clic en ***Install a client*** (Instalar un cliente) en ***Tasks*** (Tareas). Aparece la pantalla ***Client Deployment wizard*** (Asistente de implementación del cliente).

15. Seleccione ***New Package Deployment*** (Implementación de paquete nuevo) y haga clic en ***Next*** (Siguiente).

16. Seleccione el nombre de los conjuntos de funciones creado en el paso 8. Mantenga el resto de configuraciones como predeterminadas y haga clic en ***Next*** (Siguiente).

NOTA: En la versión 14.1 MP1, en ***Scheduled Scans*** (Escaneos programados) desmarque ***Delay scheduled scans when running on batteries and Allow user-defined scheduled scans to run when scan author is not logged on*** (Retrasar los escaneos programados cuando se utilice la batería y Permitir la ejecución de los escaneos programados definidos por un usuario cuando el autor del escaneo no haya iniciado sesión).

17. Seleccione ***Remote push*** (Forzado remoto) y haga clic en ***Next*** (Siguiente). Espere a que aparezca la pantalla ***Computer selection*** (Selección de equipo).

18. Expanda ***<Domain>*** (<Dominio>) (por ejemplo: INW). Los sistemas conectados al dominio se muestran en la ventana de ***Computer selection*** (Selección de equipo).

NOTA: Si no se reconocen todos los sistemas, haga clic en ***Search Network*** (Buscar red) y, a continuación, en ***Find Computers*** (Buscar equipos). Utilice el método de detección ***Search by IP address*** (Buscar por dirección IP) para identificar los sistemas del cliente (adquisición, revisión y INW Server).

19. Seleccione todos los equipos cliente Mac-Lab/CardioLab conectados al dominio y haga clic en **>>**. Aparece la pantalla ***Login Credentials*** (Credenciales de inicio de sesión).

20. Introduzca el nombre de usuario, la contraseña y el dominio o el nombre del equipo, y haga clic en ***OK*** (Aceptar).

21. Asegúrese de que todos los equipos seleccionados aparecen en ***Install Protection Client*** (Instalar cliente de protección) y haga clic en ***Next*** (Siguiente).

22. Haga clic en ***Send*** (Enviar) y espere a que el software antivirus Symantec se implemente en todos los sistemas del cliente (adquisición, revisión y INW Server). Cuando finalice, aparecerá la pantalla ***Deployment Summary*** (Resumen de implementación).

23. Haga clic en ***Next*** (Siguiente) y, a continuación, haga clic en ***Finish*** (Finalizar) para completar el asistente de implementación del cliente.

24. Espere a que el icono de Symantec se muestre en la bandeja del sistema y, a continuación, reinicie todos los equipos cliente (adquisición, revisión y INW Server). Inicie sesión como administrador o como miembro de ese grupo en todos los equipos cliente después de reiniciar.

Configuraciones de la consola del servidor de Symantec EndPoint Protection

1. Seleccione ***Start > All Programs > Symantec EndPoint Protection Manager > Symantec EndPoint Protection Manager*** (Inicio > Todos los programas > Symantec EndPoint Protection Manager > Symantec EndPoint Protection Manager). Se abre la ventana de inicio de sesión de Symantec EndPoint Protection Manager.

2. Escriba la contraseña de la consola de Symantec Endpoint Protection Manager y haga clic en ***Log On*** (Iniciar sesión).

3. Seleccione la pestaña ***Policies*** (Directivas) y haga clic en ***Virus and Spyware Protection*** (Protección contra virus y spyware) en ***Policies*** (Directivas). Se abre la ventana ***Virus and Spyware Protection Policies*** (Directivas de protección contra virus y spyware).

4. Haga clic en ***Add a Virus and Spyware Protection*** (Agregar protección contra virus y spyware) en ***Tasks*** (Tareas). Se abre la ventana ***Virus and Spyware Protection*** (Protección contra virus y spyware).

5. En ***Windows Settings > Scheduled Scans*** (Configuración de Windows > Escaneos programados), haga clic en ***Administrator-Defined Scans*** (Escaneos definidos por el administrador).

6. Seleccione ***Daily Scheduled Scan*** (Escaneo programado diario) y haga clic en ***Edit*** (Editar). Aparece la ventana ***Edit Scheduled Scan*** (Editar escaneo programado).

7. Cambie el nombre y la descripción del escaneo a ***Weekly Scheduled Scan*** (Escaneo programado semanal) y ***Weekly Scan at 00:00*** (Escaneo semanal a las 00:00), respectivamente.

8. Seleccione ***Scan type*** (Tipo de escaneo) como ***Full Scan*** (Escaneo completo).

9. Seleccione la pestaña ***Schedule*** (Programar).

10. En ***Scanning Schedule***, (Programa de escaneos) seleccione ***Weekly*** (Semanal) y cambie la hora a ***00:00***.

11. En ***Scan Duration*** (Duración de escaneo), desmarque ***Randomize scan start time within this period (recommended in VMs)*** (Aleatorizar la hora de inicio del escaneado dentro de este período [se recomienda en VM]) y seleccione ***Scan until finished (recommended to optimize scan performance)*** (Escanear hasta que haya finalizado [recomendado para optimizar el rendimiento del escaneo]).

12. En ***Missed scheduled Scans*** (Escaneos programados no ejecutados), desmarque ***Retry the scan within*** (Reintentar el escaneo en).

13. Seleccione la pestaña ***Notifications*** (Notificaciones).

14. Desmarque la opción ***Display a notification message on the infected computer*** (Mostrar notificación en el equipo infectado) y haga clic en ***OK*** (Aceptar).

15. Seleccione la pestaña ***Advanced*** (Avanzado) en la ventana ***Administrator-Defined Scans*** (Escaneos definidos por el administrador).

16. En ***Scheduled Scans*** (Escaneos programados), desmarque ***Delay scheduled scans when running on batteries*** (Retrasar los escaneos programados cuando se utilice la batería), ***Allow user-defined scheduled scans to run when scan author is not logged on*** (Permitir la ejecución de los escaneos programados definidos por un usuario cuando el autor del escaneo no haya iniciado sesión) y ***Display notifications about detections when the user logs on*** (Mostrar notificaciones sobre detecciones cuando el usuario inicie sesión).

NOTA: En la versión 14.0 MP1, en ***Scheduled Scans*** (Escaneos programados) desmarque ***Delay scheduled scans when running on batteries and Allow user-defined scheduled scans to run when scan author is not logged on*** (Retrasar los escaneos programados cuando se utilice la batería y Permitir la ejecución de los escaneos programados definidos por un usuario cuando el autor del escaneo no haya iniciado sesión).

17. En ***Startup and Triggered Scans*** (Escaneos desencadenados y de inicio), desmarque ***Run an Active Scan when new definitions arrive*** (Ejecutar un escaneo activo cuando lleguen nuevas definiciones).

18. En ***Windows Settings > Protection Technology*** (Configuración de Windows > Tecnología de protección), haga clic en ***Auto-Protect*** (Autoproteccíón).

19. Seleccione las pestaña ***Scan Details*** (Detalles de escaneo) y seleccione y bloquee ***Enable Auto-Protect*** (Activar Autoprotección).

20. Seleccione la pestaña ***Notifications*** (Notificaciones), desmarque y bloquee ***Display a notification message on the infected computer*** (Mostrar notificación en el equipo infectado) y ***Display the Auto-Protect results dialog on the infected Computer*** (Mostrar el diálogo de resultados de autoprotección en el equipo infectado).

21. Seleccione la pestaña ***Advanced*** (Avanzado) y en ***Auto-Protect Reloading and Enablement*** (Recarga y activación de la autoprotección) bloquee la opción ***When Auto-Protect is disabled, Enable after:*** (Cuando la protección automática esté desactivada, activar después de:).

22. En ***Additional options*** (Opciones adicionales), haga clic en ***File Cache*** (Caché de archivos). Se abre la ventana ***File Cache*** (Caché de archivos).

23. Desmarque ***Rescan cache when new definitions load*** (Volver a escanear la caché cuando se carguen nuevas definiciones) y haga clic en ***OK*** (Aceptar).

24. En ***Windows Settings > Protection Technology*** (Configuración de Windows > Tecnología de protección), haga clic en ***Download Protecion*** (Descargar protección).

25. Seleccione la pestaña ***Notifications*** (Notificaciones), desmarque y bloquee ***Display a notification message on the infected computer*** (Mostrar notificación en el equipo infectado).

26. En ***Windows Settings > Protection Technology*** (Configuración de Windows > Tecnología de protección), haga clic en ***SONAR***.

27. Seleccione la pestaña ***SONAR Settings*** (Ajustes de SONAR), desmarque y bloquee ***Enable SONAR*** (Activar SONAR).

28. En ***Windows Settings > Protection Technology*** (Configuración de Windows > Tecnología de protección), haga clic en ***Early Launch Anti-Malware Driver*** (Controlador antimalware de inicio temprano).

29. Desmarque y bloquee ***Enable Symantec early lauch anti-malware*** (Activar antimalware de inicio temprano de Symantec).

30. En ***Windows Settings > Email Scans*** (Configuración de Windows > Escaneos de correo electrónico), haga clic en ***Internet Email Auto-Protect*** (Autoprotección de correo electrónico de Internet).

31. Seleccione la pestaña ***Scan Details*** (Detalles de escaneo), desmarque y bloquee ***Enable Internet Email Auto-Protect*** (Activar autoprotección de correo electrónico de Internet).

32. Seleccione la pestaña ***Notifications*** (Notificaciones), desmarque y bloquee ***Display a notification message on the infected computer*** (Mostrar notificación en el equipo infectado), ***Display a Progress indicator when email is being sent*** (Mostrar indicador de progreso durante el envío de un correo electrónico), ***Display a notification area icon*** (Mostrar icono del área de notificación).

33. En ***Windows Settings > Email Scans*** (Configuración de Windows > Escaneos de correo electrónico), haga clic en ***Microsoft Outlook Auto-Protect*** (Autoprotección de Microsoft Outlook).

34. Seleccione la pestaña ***Scan Details*** (Detalles de escaneo), desmarque y bloquee ***Enable Microsoft Outlook Auto-Protect*** (Activar autoprotección de Microsoft Outlook).

35. Seleccione la pestaña ***Notifications*** (Notificaciones), desmarque y bloquee ***Display a notification message on the infected computer*** (Mostrar notificación en el equipo infectado).

36. En ***Windows Settings > Email Scans*** (Configuración de Windows > Escaneos de correo electrónico), haga clic en ***Lotus Notes Auto-Protect*** (Autoprotección de Lotus Notes).

37. Seleccione la pestaña ***Scan Details*** (Detalles de escaneo), desmarque y bloquee ***Enable Lotus Notes Auto-Protect*** (Activar autoprotección de Lotus Notes).

38. Seleccione la pestaña ***Notifications*** (Notificaciones), desmarque y bloquee ***Display a notification message on the infected computer*** (Mostrar notificación en el equipo infectado).

39. En ***Windows Settings > Advanced Options*** (Configuración de Windows > Opciones avanzadas), haga clic en ***Global Scan Options*** (Opciones de escaneo global).

40. En ***Bloodhound(™) Detection Settings*** (Configuración de detección de Bloodhound[™]), desmarque y bloquee ***Enable Bloodhound(™) heuristic virus detection*** (Activar detección heurística de virus Bloodhound[™]).

41. En ***Windows Settings > Advanced Options*** (Configuración de Windows > Opciones avanzadas), haga clic en ***Quarantine*** (Cuarentena).

42. Seleccione la pestaña ***General*** en ***When New Virus Definitions Arrive*** (Cuando lleguen nuevas definiciones de virus) y marque la opción ***Do nothing*** (No hacer nada).

43. En ***Windows Settings > Advanced Options*** (Configuración de Windows > Opciones avanzadas), haga clic en ***Miscellaneous*** (Miscelánea).

44. Seleccione la pestaña ***Notifications*** (Notificaciones) y desmarque ***Display a notification message on the client computer when definitions are outdated*** (Mostrar notificación en el equipo del cliente cuando las definiciones estén atrasadas), ***Display a notification message on the client computer when Symantec Endpoint Protection is running without virus definitions*** (Mostrar notificación en el equipo del cliente cuando Symantec Endpoint Protection se ejecute sin definiciones de virus) y ***Display error messages with a URL to a solution*** (Mostrar mensajes de error con URL para una solución).

45. Haga clic en ***OK*** (Aceptar) para cerrar la ventana de directivas ***Virus and Spyware Protection*** (Protección contra virus y spyware).

46. Haga clic en ***Yes*** (Sí) en el cuadro de mensaje ***Assign Policies*** (Asignar directivas).

47. Seleccione ***My Company*** (Mi compañía) y haga clic en ***Assign*** (Asignar).

48. Haga clic en ***Yes*** (Sí) en el cuadro de mensaje.

49. En ***Policies*** (Directivas) haga clic en ***Firewall***.

50. Haga clic en ***Firewall policy*** (Directiva de firewall) de ***Firewall policies*** (Directivas de firewall) y seleccione ***Edit the policy*** (Editar la directiva) en ***Tasks*** (Tareas).

51. Seleccione la pestaña ***Policy Name*** (Nombre de la directiva) y desmarque ***Enable this policy*** (Activar esta directiva).
52. Haga clic en ***OK*** (Aceptar).
53. En ***Policies*** (Directivas), haga clic en ***Intrusion Prevention*** (Prevención de intrusiones).
54. Haga clic en la directiva ***Intrusion Prevention*** (Prevención de intrusiones) en ***Intrusion Prevention Policies*** (Directivas de prevención de intrusiones) y seleccione ***Edit the policy*** (Editar la directiva) en ***Tasks*** (Tareas).
55. Seleccione la pestaña ***Policy Name*** (Nombre de la directiva) y desmarque ***Enable this policy*** (Activar esta directiva).
56. En función de la versión del software, realice una de las siguientes acciones:
    - **Versión 12.1.2:** Haga clic en la opción ***Settings*** (Configuración) situada en el panel izquierdo.
    - **Versiones 12.1.6 MP5 y 14.0 MP1:** Haga clic en la opción ***Intrusion Prevention*** (Prevención de intrusión) situada en el panel izquierdo.
57. Desmarque y bloquee ***Enable Network Intrusion Prevention*** (Activar la prevención de intrusiones de red) y ***Enable Browser Intrusion Prevention for Windows*** (Activar la prevención de intrusiones del explorador para Windows).
58. Haga clic en ***OK*** (Aceptar).
59. En ***Policies*** (Directivas), haga clic en ***Application and Device Control*** (Control de aplicaciones y dispositivos).
60. Haga clic en ***Application and Device Control Policy*** (Directiva de control de aplicaciones y dispositivos) en ***Application and Device Control Policies*** (Directivas de control de aplicaciones y dispositivos) y seleccione ***Edit the policy*** (Editar la directiva) en ***Tasks*** (Tareas).
61. Seleccione la pestaña ***Policy Name*** (Nombre de la directiva) y desmarque ***Enable this policy*** (Activar esta directiva).
62. Haga clic en ***OK*** (Aceptar).
63. En ***Policies*** (Directivas), haga clic en ***LiveUpdate***.
64. Seleccione ***LiveUpdate Settings policy*** (Directiva de configuración de LiveUpdate) y, en ***Tasks*** (Tareas), haga clic en ***Edit the policy*** (Editar la directiva).
65. En ***Overview > Windows Settings*** (Descripción general > Configuración de Windows), haga clic en ***Server Settings*** (Configuración del servidor).
66. En ***Internal or External LiveUpdate Server*** (Servidor interno o externo de LiveUpdate), asegúrese de que la opción ***Use the default management server*** (Utilizar el servidor de administración predeterminado) está seleccionada y desmarque ***Use a LiveUpdate server*** (Utilizar un servidor de LiveUpdate).
67. Haga clic en ***OK*** (Aceptar).
68. En ***Policies*** (Directivas), haga clic en ***Exceptions*** (Excepciones).
69. Haga clic en ***Exceptions Policy*** (Directiva de excepciones) y, a continuación, en ***Tasks*** (Tareas) seleccione ***Edit the policy*** (Editar la directiva).
70. En función de la versión del software, realice una de las siguientes acciones:

- **Versiones 12.1.2 y 12.1.6 MP5:** Haga clic en ***Exceptions > Add > Windows Exceptions > Folder*** (Excepciones > Agregar > Excepciones de Windows > Carpeta).
- **Versión 14.0 MP1:** Haga clic en la lista desplegable ***Add*** (Agregar) y seleccione ***Windows Exceptions > Folder*** (Excepciones de Windows > Carpeta).

71. Introduzca las siguientes rutas de carpeta una a una **C:\Program Files (x86)\GE Healthcare\MLCL**, **C:\Program Files\GE Healthcare\MLCL, D:\GEData\Studies**, **E:**, **G:** y realice lo siguiente:

    a. Asegúrese de que la opción ***Include subfolders*** (Incluir subcarpetas) está seleccionada.

NOTA: Haga clic en ***Yes*** (Sí) en caso de que aparezca el cuadro de mensaje ***Are you sure you want to exclude all subfolders from protection?*** (¿Está seguro de que desea excluir de la protección todas las subcarpetas?).

    b. Seleccione ***All*** (Todos) en ***Specify the type of scan that excludes this folder*** (Especificar el tipo de escaneo que excluye esta carpeta).

    c. En la versión 14.0 MP1, haga clic en ***OK*** (Aceptar) para agregar la excepción.

72. Haga clic en ***OK*** (Aceptar).
73. Haga clic en ***Assign the policy*** (Asignar la directiva) en ***Tasks*** (Tareas).
74. Seleccione ***My Company*** (Mi compañía) y haga clic en ***Assign*** (Asignar).
75. Haga clic en ***Yes*** (Sí).
76. Haga clic en la opción ***Clients*** (Clientes) situada en el panel izquierdo y seleccione la pestaña ***Policies*** (Directivas).
77. En ***My company*** (Mi compañía), seleccione ***Default Group*** (Grupo predeterminado) y desmarque ***Inherit policies and settings from parent group "My Company"*** (Heredar directivas y ajustes del grupo principal en "Mi compañía") y haga clic en ***Communication Settings*** (Configuración de comunicaciones) en ***Location-Independent policies and settings*** (Directivas y ajustes independientes de lugar).

NOTA: Si aparece un mensaje de advertencia, haga clic en ***OK*** (Aceptar) y vuelva a seleccionar ***Communications Settings*** (Configuración de comunicaciones) en ***Location-Independent Policies and Settings*** (Directivas y ajustes independientes de lugar).

78. En ***Download*** (Descargar), asegúrese de que se han marcado las opciones ***Download policies and content from the management server*** (Descargar directivas y contenido del servidor de administración) y ***Push mode*** (Modo forzado).
79. Haga clic en ***OK*** (Aceptar).
80. Haga clic en ***General Settings*** (Configuración general), en ***Location-independent Policies and Settings*** (Directivas y ajustes independientes de lugar).
81. Seleccione la pestaña ***Tamper Protection*** (Protección contra sabotaje), desmarque y bloquee ***Protect Symantec security software from being tampered with or shut down*** (Proteger el software de seguridad Symantec contra sabotaje o apagón).
82. Haga clic en ***OK*** (Aceptar).
83. Haga clic en ***Admin*** y seleccione ***Servers*** (Servidores).
84. En el menú ***Servers*** (Servidores), seleccione ***Local Site (My Site)*** (Sitio local [Mi sitio]).

85. En ***Tasks*** (Tareas), seleccione ***Edit Site Properties*** (Editar propiedades del sitio). Se abre la ventana ***Site Properties for Locate Site (My Site)*** (Propiedades del sitio para localizar sitio [Mi sitio]).

86. Seleccione la pestaña ***LiveUpdate*** y asegúrese de que en ***Download Schedule*** (Descargar programa) el programa se ha establecido en ***Every 4 hour(s)*** (Cada 4 horas).

87. Haga clic en ***OK*** (Aceptar).

88. Haga clic en ***Log Off*** (Cerrar sesión) y cierre la consola de Symantec EndPoint Protection Manager. Asegúrese de que las directivas de Symantec Endpoint Protection se han insertado en los sistemas de los clientes.

Pautas posteriores a la instalación de Symantec EndPoint Protection

1. Active la conexión de bucle invertido. Para obtener más información, consulte Activar la conexión de bucle invertido en la página 6.

2. Configure el servicio del Explorador de equipos. Para obtener más información, consulte Configurar el servicio del Explorador de equipos después de instalar el antivirus en la página 7.

3. Abra el símbolo del sistema en modo ***Run As Administrator*** (Ejecutar como administrador).

4. Vaya a C:\Program Files\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec.

NOTA: Para configurar INW Server, vaya a C:\Program Files (x86)\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec.

5. Escriba **RestoreRegSymantec.ps1** y pulse ***Enter*** (Intro).

6. Confirme que el script se ha ejecutado de forma correcta.
   Nota: Debe confirmar que el script **RestoreRegSymantec.ps1** se ha ejecutado correctamente antes de continuar.

   Si no se encuentra la ruta de la carpeta mencionada con anterioridad, realice los siguientes pasos para todos los sistemas MLCL, excepto para MLCL 6.9.6R1 INW Server (sistema operativo del servidor: Windows Server 2008R2).

   a. Haga clic en el botón de ***Start*** (Inicio) y, a continuación, en ***Run*** (Ejecutar).

   b. Escriba **Regedit.exe** y haga clic en ***OK*** (Aceptar).

   c. Vaya a ***HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing***.

   d. Localice y haga doble clic en el registro ***State*** (Estado).

   e. Cambie la ***Base*** a ***Decimal***.

   f. Cambie el ***Value data*** (Datos de valor) a ***65536***.

   g. Haga clic en ***OK*** (Aceptar) y cierre el registro.

McAfee VirusScan Enterprise

Descripción de la instalación

McAfee VirusScan Enterprise debe estar instalado en un sistema Mac-Lab/CardioLab independiente y se debe gestionar aparte. Utilice las siguientes instrucciones para instalar y configurar McAfee VirusScan Enterprise.

Las actualizaciones de virus son responsabilidad de la institución. Actualice las definiciones con regularidad para asegurar que el sistema cuente con la protección antivirus más reciente.

Procedimiento de instalación de McAfee VirusScan Enterprise

1. Inicie sesión como **Administrator** (Administrador) o como miembro de ese grupo.
2. Inserte los CD de **McAfee VirusScan Enterprise 8.8 Patch 3**, **McAfee VirusScan Enterprise 8.8 Patch 4**, **McAfee VirusScan Enterprise 8.8 Patch 8** o **McAfee VirusScan Enterprise 8.8 Patch 9** en la unidad de CD.
3. Haga doble clic en ***SetupVSE.Exe***. Aparece el cuadro de diálogo de Windows Defender.
4. Haga clic en ***Yes*** (Sí). Se muestra la pantalla de configuración de McAfee VirusScan Enterprise.
5. Haga clic en ***Next*** (Siguiente). Aparece la pantalla McAfee End User License Agreement (Contrato de licencia para el usuario final McAfee).
6. Lea el contrato de licencia, complete los campos necesarios y haga clic en ***OK*** (Aceptar) cuando haya terminado. Aparece la pantalla Select Setup Type (Seleccionar tipo de configuración).
7. Seleccione ***Typical*** (Típico) y haga clic en ***Next*** (Siguiente). Aparece la pantalla Select Access Protection Level (Seleccionar nivel de protección de acceso).
8. Seleccione ***Standard Protection*** (Protección estándar) y haga clic en ***Next*** (Siguiente). Se muestra la pantalla Ready to Install (Preparado para instalar).
9. Haga clic en ***Install*** (Instalar) y espere a que finalice la instalación. Después de instalar correctamente McAfee VirusScan Enterprise, aparece la pantalla ***McAfee Virus Scan Enterprise Setup has completed successfully*** (La configuración de McAfee Virus Scan Enterprise ha finalizado correctamente).
10. Desmarque la casilla de verificación ***Run On-Demand Scan*** (Ejecutar escaneo a demanda) y haga clic en ***Finish*** (Finalizar).
11. Si aparece la ventana ***Update in Progress*** (Actualización en curso), haga clic en ***Cancel*** (Cancelar).
12. Si se muestra un cuadro de mensaje para reiniciar el sistema, haga clic en ***OK*** (Aceptar).
13. Reinicie el sistema.
14. Inicie sesión como **Administrator** (Administrador) o como miembro de ese grupo.

Configuración de McAfee VirusScan Enterprise

1. Haga clic en ***Start > All Programs > McAfee > VirusScan Console*** (Inicio > Todos los programas > McAfee > Consola de VirusScan). Aparecerá la pantalla ***VirusScan Console*** (Consola de VirusScan).
2. Haga clic con el botón derecho en ***Access Protection*** (Protección de acceso) y seleccione ***Properties*** (Propiedades). Aparece la pantalla ***Access Protection*** (Protección de acceso) de Properties (Propiedades).
3. Haga clic en la pestaña ***Access Protection*** (Protección de acceso) y desmarque ***Enable access protection*** (Activar protección de acceso) y ***Prevent McAfee services from being stopped*** (Evitar que los servicios de McAfee se detengan).
4. Haga clic en ***OK*** (Aceptar).
5. Haga clic en ***Buffer Overflow Protection*** (Protección de desbordamiento de memoria intermedia) y seleccione ***Properties*** (Propiedades). Aparece la pantalla ***Buffer Overflow Protection*** (Protección de desbordamiento de memoria intermedia).
6. Haga clic en la pestaña ***Buffer Overflow Protection*** (Protección de desbordamiento de memoria intermedia) y desmarque ***Show the messages dialog box when a buffer overflow is detected under Buffer overflow settings*** (Mostrar el cuadro de diálogo de mensajes cuando se detecte un desbordamiento de la memoria intermedia mientras esté activa la configuración del desbordamiento de memoria intermedia).
7. Desmarque ***Enable buffer overflow protection*** (Activar protección de desbordamiento de memoria intermedia) en ***Buffer overflow settings*** (Configuración del desbordamiento de memoria intermedia).
8. Haga clic en ***OK*** (Aceptar).
9. Haga clic con el botón derecho en ***On-Delivery Email Scanner*** (Escáner de correo electrónico al llegar) y seleccione ***Properties*** (Propiedades). Aparece la pantalla ***On-Delivery Email Scanner Properties*** (Propiedades del escáner de correo electrónico al llegar).
10. Haga clic en la pestaña ***Scan items*** (Escanear elementos) y desmarque las opciones siguientes en ***Heuristics*** (Heurística):
    - ***Find unknown program threats and trojans*** (Buscar troyanos y amenazas de programas desconocidos).
    - ***Find unknown macro threats*** (Buscar amenazas macro desconocidas).
    - ***Find attachments with multiple extensions*** (Buscar adjuntos con varias extensiones).
11. Desmarque ***Detect unwanted programs*** (Detectar programas no deseados) en ***Unwanted programs detection*** (Detección de programas no deseados).
12. Seleccione ***Disabled*** (Desactivado) para la opción ***Sensitivity level*** (Nivel de sensibilidad) de ***Artemis (Heuristic network check for suspicious files)*** (Artemis [Comprobación de red heurística para archivos sospechosos]).
13. Haga clic en ***OK*** (Aceptar).
14. Haga clic con el botón derecho en ***On-Delivery Email Scanner*** (Escáner de correo electrónico al llegar) y seleccione ***Disable*** (Desactivar).

15. Haga clic con el botón derecho en ***On-Access Scanner*** (Escáner al abrir) y seleccione ***Properties*** (Propiedades). Aparece la pantalla ***On-Access Scan Properties*** (Propiedades de escaneo al abrir).

16. Haga clic en la pestaña ***General*** y seleccione ***Disabled*** (Desactivado) para la opción ***Sensitivity level*** (Nivel de sensibilidad) de ***Artemis (Heuristic network check for suspicious files)*** (Artemis [Comprobación de red heurística para archivos sospechosos]).

17. Haga clic en la pestaña ***ScriptScan*** (Escaneo de scripts) y desmarque ***Enable scanning of scripts*** (Activar escaneo de scripts).

18. Haga clic en la pestaña ***Blocking*** (Bloqueo) y desmarque ***Block the connection when a threat is detected in a shared folder*** (Bloquear la conexión cuando se detecte una amenaza en una carpeta compartida).

19. Haga clic en la pestaña ***Messages*** (Mensajes) y desmarque ***Show the messages dialog box when a threat is detected and display the specified text in the message*** (Mostrar mensaje cuando se detecte una amenaza y mostrar el texto especificado en el mensaje).

20. Haga clic en la opción ***All Processes*** (Todos los procesos) situada en el panel izquierdo.

21. Haga clic en la pestaña ***Scan Items*** (Escanear elementos) y desmarque las opciones siguientes en Heuristics (Heurística).

    - ***Find unknown unwanted programs and trojans*** (Buscar troyanos y programas no deseados desconocidos).
    - ***Find unknown macro threats*** (Buscar amenazas macro desconocidas).

22. Desmarque ***Detect unwanted programs*** (Detectar programas no deseados) en ***Unwanted programs detection*** (Detección de programas no deseados).

23. Haga clic en la pestaña ***Exclusions*** (Exclusiones) y seleccione ***Exclusions*** (Exclusiones). Aparece la pantalla ***Set Exclusions*** (Definir exclusiones).

24. Haga clic en ***Add*** (Agregar). Aparece la pantalla ***Add Exclusion Item*** (Agregar elemento de exclusión).

25. Seleccione ***By name/location*** (Por nombre/ubicación) y haga clic en ***Browse*** (Buscar). Aparece la pantalla ***Browse for Files or Folders*** (Buscar archivos o carpetas).

26. Vaya a las carpetas ***C:\Program Files\GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:***, ***G:*** una por una y seleccione ***OK*** (Aceptar).

27. Seleccione ***Also exclude subfolders*** (Excluir también subcarpetas) en la ventana ***Add Exclusion Item*** (Agregar elemento de exclusión) y haga clic en ***OK*** (Aceptar).

28. Asegúrese de que las carpetas C:\Program Files\GE Healthcare\MLCL\, D:\GEData\Studies\, E:\, G:\ están presentes en la ventana Set Exclusions (Definir exclusiones).

29. Haga clic en ***OK*** (Aceptar).

30. Haga clic con el botón derecho en ***AutoUpdate*** (Actualización automática) y seleccione ***Properties*** (Propiedades). Aparece la pantalla McAfee AutoUpdate Properties – AutoUpdate (Propiedades de actualización automática de McAfee – Actualización automática).

31. Desmarque las siguientes opciones de ***Update Options*** (Opciones de actualización):

    - ***Get new detection engine and dats if available*** (Obtener un nuevo motor de detección y datos si los hubiera).

- ***Get other available updates (service packs, upgrades, etc.)*** (Obtener otras actualizaciones disponibles [paquetes de servicios, actualizaciones, etc.]).

32. Haga clic en ***Schedule*** (Programar). Aparece la pantalla Schedule Settings (Ajustes de programación).
33. Desmarque ***Enable (scheduled task runs at specified time)*** (Activar [la tarea programada se ejecuta a la hora especificada]) en ***Schedule Settings*** (Ajustes de programación).
34. Haga clic en ***OK*** (Aceptar).
35. Haga clic en ***OK*** (Aceptar).
36. Haga clic con el botón derecho en la ventana ***VirusScan Console*** (Consola de VirusScan) y seleccione ***New On-Demand Scan Task*** (Nueva tarea de escaneo a demanda).
37. Cambie el nombre del nuevo escaneo a ***Weekly Scheduled Scan*** (Escaneo programado semanal). Aparece la pantalla ***On-Demand Scan Properties - Weekly Scheduled Scan*** (Propiedades de escaneado a demanda - Escaneo programado semanal).
38. Haga clic en la pestaña ***Scan Items*** (Escanear elementos) y desmarque ***Detect unwanted programs*** (Detectar programas no deseados) en ***Opciones*** (Opciones).
39. Desmarque las siguientes opciones en ***Heuristics*** (Heurística):
    - ***Find unknown programs threats*** (Buscar amenazas de programas desconocidos).
    - ***Find unknown macro threats*** (Buscar amenazas macro desconocidas).
40. Haga clic en la pestaña ***Exclusions*** (Exclusiones) y seleccione ***Exclusions*** (Exclusiones). Aparece la pantalla ***Set Exclusions*** (Definir exclusiones).
41. Haga clic en ***Add*** (Agregar). Aparece la pantalla ***Add Exclusion Item*** (Agregar elemento de exclusión).
42. Seleccione ***By name/location*** (Por nombre/ubicación) y haga clic en ***Browse*** (Buscar). Aparece la pantalla ***Browse for Files or Folders*** (Buscar archivos o carpetas).
43. Vaya a las carpetas ***C:\Program Files\GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:***, ***G:*** una por una y seleccione ***OK*** (Aceptar).
44. Seleccione ***Also exclude subfolders*** (Excluir también subcarpetas) en la ventana ***Add Exclusion Item*** (Agregar elemento de exclusión) y haga clic en ***OK*** (Aceptar).
45. Asegúrese de que las carpetas ***C:\Program Files\GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:***, ***G:*** están presentes en la ventana ***Set Exclusions*** (Definir exclusiones).
46. Haga clic en ***OK*** (Aceptar).
47. Haga clic en la pestaña ***Performance*** (Rendimiento) y seleccione ***Disabled*** (Desactivado) para la opción ***Sensitivity level*** (Nivel de sensibilidad) de ***Artemis (Heuristic network check for suspicious files)*** (Artemis [Comprobación de red heurística para archivos sospechosos]).
48. Haga clic en ***Schedule*** (Programar). Aparece la pantalla ***Schedule Settings*** (Ajustes de programación).
49. Haga clic en la pestaña ***Task*** (Tarea) y seleccione ***Enable (scheduled task runs at specified time)*** (Activar [la tarea programada se ejecuta a la hora especificada]) en ***Schedule Settings*** (Ajustes de programación).

50. Haga clic en la pestaña ***Schedule*** (Programar) y seleccione lo siguiente:
    a. Run task (Ejecutar tarea): Weekly (Semanal).
    b. Start Time (Hora inicio): 12:00 AM.
    c. Every (Cada): 1 Weeks, Sunday (1 semana, domingo).
51. Haga clic en ***OK*** (Aceptar).
52. Haga clic en ***OK*** (Aceptar).
53. Haga clic en ***Tools > Alerts*** (Herramientas > Alertas) en la ventana ***VirusScan Console*** (Consola de VirusScan). Aparece la pantalla Alert Properties (Propiedades de alerta).
54. Desmarque las casillas de verificación ***On-Access Scan*** (Escaneo al abrir), ***On-Demand Scan and scheduled scans*** (Escaneos a demanda y con horario), ***Email Scan*** (Escaneo de correo electrónico) y ***AutoUpdate*** (Actualización automática).
55. Haga clic en ***Destination*** (Destino). Aparece la pantalla ***Alert Manager Client Configuration*** (Configuración de cliente de administrador de alertas).
56. Seleccione la casilla de verificación ***Disable alerting*** (Desactivar alertas).
57. Haga clic en ***OK*** (Aceptar). Aparece la pantalla ***Alert Properties*** (Propiedades de alerta).
58. Seleccione la pestaña ***Additional Alerting Options*** (Otras opciones de alerta).
59. Seleccione la opción ***Suppress all alerts (severities 0 to 4)*** (Suprimir todas las alertas [gravedad 0 a 4]) en la lista desplegable de ***Severity Filter*** (Filtro de gravedad).
60. Seleccione la pestaña ***Alert Manager Alerts*** (Alertas del administrador de alertas).
61. Desmarque la casilla de verificación ***Access Protection*** (Protección de acceso).
62. Haga clic en ***OK*** (Aceptar) para cerrar la ventana ***Alert Properties*** (Propiedades de alerta).
63. Cierre la ventana ***VirusScan Console*** (Consola de VirusScan).

McAfee ePolicy Orchestrator

Descripción de la instalación

Instale McAfee ePolicy Orchestrator solo en un entorno de red de Mac-Lab/CardioLab. McAfee ePolicy Orchestrator se debe instalar en un servidor de la consola de administración del antivirus y McAfee VirusScan Enterprise se debe implementar en el servidor Centricity Cardiology INW y en las estaciones de trabajo de adquisición y revisión como un cliente. Utilice las siguientes instrucciones para instalar y configurar McAfee ePolicy Orchestrator.

Las siguientes instrucciones para instalar y configurar McAfee VirusScan Enterprise son compatibles con los parches 3, 4, 8 y 9.

Las actualizaciones de virus son responsabilidad de la institución. Actualice las definiciones con regularidad para asegurar que el sistema cuente con la protección antivirus más reciente.

Pautas previas a la instalación

1. Se espera que la consola de administración del antivirus McAfee se instale de acuerdo con las instrucciones de McAfee y que funcione de manera correcta.
2. Inicie sesión como **Administrator** (Administrador) o como miembro de ese grupo en todos los sistemas del cliente (adquisición, revisión y INW Server) para instalar el software antivirus.
3. Desactive la conexión de bucle invertido. Para obtener más información, consulte Desactivar la conexión de bucle invertido en la página 6.
4. Para activar McAfee VirusScan Enterprise 8.8 Patch 9, póngase en contacto con McAfee para instalar el certificado raíz UTN-USERFirst-Object y el certificado raíz universal VeriSign solo en INW Server. Reinicie el sistema una vez tenga instalados los certificados.

NOTA: Si el certificado raíz UTN-USERFirst-Object y el certificado raíz universal VeriSign Universal no están instalados, no se podrá instalar McAfee VirusScan Enterprise 8.8 Patch 9 en INW Server.

5. Para una nueva instalación, agregue la siguiente versión del agente al repositorio maestro de McAfee ePolicy Orchestrator en la consola de McAfee ePolicy Orchestrator: ***- McAfee Agent v5.0.5.658***
6. Para una nueva instalación, agregue el siguiente paquete al repositorio maestro de McAfee ePolicy Orchestrator en la consola de McAfee ePolicy Orchestrator:
   - McAfee VirusScan Enterprise 8.8 Patch 3: VSE880LMLRP3.ZIP (v8.8.0.1128).
   - McAfee VirusScan Enterprise 8.8 Patch 4: VSE880LMLRP4.ZIP (v8.8.0.1247).
   - McAfee VirusScan Enterprise 8.8 Patch 8: VSE880LMLRP8.ZIP (v8.8.0.1599).
   - McAfee VirusScan Enterprise 8.8 Patch 9: VSE880MLRP9.ZIP (v8.8.0.1804).

NOTA: El archivo VSE880LMLRP3.zip contiene los paquetes de instalación de los parches 2 y 3. El parche 2 es para Windows 7 y la plataforma del sistema operativo Windows Server 2008, mientras que el parche 3 es para Windows 8 y la plataforma del sistema operativo Windows Server 2012. El instalador de McAfee instala el parche correcto tras identificar la versión del sistema operativo de Windows.

7. Para una nueva instalación, agregue las siguientes extensiones a la tabla de extensiones de McAfee ePolicy Orchestrator en la consola de McAfee ePolicy Orchestrator:
   - McAfee VirusScan Enterprise 8.8 Patch 3: VIRUSSCAN8800 v8.8.0.348 y VIRUSSCANREPORTS v1.2.0.228
   - McAfee VirusScan Enterprise 8.8 Patch 4: VIRUSSCAN8800 v8.8.0.368 y VIRUSSCANREPORTS v1.2.0.236
   - McAfee VirusScan Enterprise 8.8 Patch 8: VIRUSSCAN8800 v8.8.0.511 y VIRUSSCANREPORTS v1.2.0.311
   - McAfee VirusScan Enterprise 8.8 Patch 9: VIRUSSCAN8800 v8.8.0.548 y VIRUSSCANREPORTS v1.2.0.346

NOTA: Los archivos VIRUSSCAN8800(348).zip y VIRUSSCANREPORTS120(228).zip se encuentran en el paquete de McAfee VirusScan Enterprise 8.8 Patch 3.

Los archivos VIRUSSCAN8800(368).zip y VIRUSSCANREPORTS120(236).zip se encuentran en el paquete de McAfee VirusScan Enterprise 8.8 Patch 4.

Los archivos VIRUSSCAN8800(511).zip y VIRUSSCANREPORTS120(311).zip se encuentran en el paquete de McAfee VirusScan Enterprise 8.8 Patch 8.

Los archivos VIRUSSCAN8800(548).zip y VIRUSSCANREPORTS120(346).zip se encuentran en el paquete de McAfee VirusScan Enterprise 8.8 Patch 9.

McAfee ePolicy Orchestrator 5.0 o 5.3.2: pasos para la implementación de una nueva instalación (método preferido de instalación forzada)

1. En función de la versión del software, seleccione ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.0.0 Console*** (Inicio > Todos los programas > McAfee > ePolicy Orchestrator > Ejecutar Consola de McAfee ePolicy Orchestrator 5.0.0) o ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.3.2 Console*** (Inicio > Todos los programas > McAfee > ePolicy Orchestrator > Ejecutar Consola de McAfee ePolicy Orchestrator 5.3.2) para iniciar sesión en la consola de ePolicy Orchestrator.

NOTA: Haga clic en ***Continue with this website*** (Continuar en este sitio web) si aparece el cuadro de mensaje ***Security Alert*** (Alerta de seguridad).

2. Introduzca el nombre de usuario y contraseña, y haga clic en ***Log On*** (Iniciar sesión).
3. Seleccione ***Menu > System > System Tree*** (Menú > Sistema > Árbol del sistema). Aparece la ventana System Tree (Árbol del sistema).
4. Haga clic en ***My Organization*** (Mi organización) y, con el enfoque en ***My Organization*** (Mi organización), haga clic en ***System Tree Actions > New Systems*** (Acciones del árbol del sistema > Nuevos sistemas) en la esquina inferior izquierda de la pantalla.
5. Seleccione ***Push agents and add systems to the current group (My Organization)*** (Forzar instalación de los agentes y agregar sistemas al grupo actual [Mi organización]) y haga clic en ***Browse*** (Buscar) en los sistemas objetivo.
6. Introduzca el nombre de usuario y la contraseña del **dominio/administrador local** y haga clic en ***OK*** (Aceptar).
7. Seleccione el dominio ***INW*** de la lista desplegable ***Domain*** (Dominio).
8. Seleccione los equipos cliente (adquisición, revisión y INW Server) conectados al dominio y haga clic en ***OK*** (Aceptar).

NOTA: Si el nombre de dominio no aparece en la lista desplegable ***Domain*** (Dominio), haga lo siguiente:

- En la ventana ***Browse for Systems*** (Buscar sistemas), haga clic en ***Cancel*** (Cancelar).
- En la ventana ***New Systems*** (Sistemas nuevos), introduzca el nombre del sistema de los equipos cliente (adquisición, revisión y INW Server) en el campo ***Target systems*** (Sistemas objetivo) y continúe con los siguientes pasos.

9. Seleccione ***Agent Version*** (Versión del agente) como ***McAfee Agent for Windows 4.8.0 (Current)*** (McAfee Agent para Windows 4.8.0 [Actual]) o como ***McAfee Agent for Windows 5.0.4 (Current)*** (McAfee Agent para Windows 5.0.4. [Actual]). Introduzca el nombre de usuario y la contraseña del **administrador del dominio** y haga clic en ***OK*** (Aceptar).

10. Confirme que los directorios se crean correctamente en los equipos cliente (adquisición, revisión y INW Server), dependiendo de la versión del parche:

    - Para los parches 3 y 4, compruebe que el directorio ***C:\Program Files\McAfee\Common Framework*** está presente y que McAfee Agent se ha instalado en el mismo directorio.

NOTA: En INW Server, asegúrese de que el directorio ***C:\Program Files (x86)\McAfee\Common Framework*** está presente y que McAfee Agent se ha instalado en el mismo directorio.

    - Para el parche 8, compruebe que el directorio ***C:\Program Files\McAfee\Agent*** está presente y que McAfee Agent se ha instalado en el mismo directorio.

NOTA: En INW Server, asegúrese de que el directorio ***C:\Program Files (x86)\McAfee\Common Framework*** está presente.

11. Reinicie los equipos cliente (adquisición, revisión y INW Server) e inicie sesión como **administrador del dominio** o como miembro de ese grupo.

12. En función de la versión del software, haga clic en ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.0.0 Console*** (Inicio > Todos los programas > McAfee > ePolicy Orchestrator > Ejecutar Consola de McAfee ePolicy Orchestrator 5.0.0) o ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.3.2 Console*** (Inicio > Todos los programas > McAfee > ePolicy Orchestrator > Ejecutar Consola de McAfee ePolicy Orchestrator 5.3.2).

13. Introduzca el nombre de usuario y contraseña, y haga clic en ***Log On*** (Iniciar sesión).

14. Seleccione ***Menu > Systems > Systems Tree*** (Menú > Sistemas > Árbol de los sistemas).

15. Haga clic en ***My Organization*** (Mi organización) y, con el enfoque en ***My organization*** (Mi organización), haga clic en la pestaña ***Assigned Client Tasks*** (Tareas asignadas del cliente).

16. Haga clic en el botón ***Actions > New Client Task Assignment*** (Acciones > Asignación de tareas nuevas del cliente) en la parte inferior de la pantalla. Aparece la pantalla Client Task Assignment Builder (Generador de asignación de tareas del cliente).

17. Seleccione lo siguiente:

    a. **Product (Producto):** McAfee Agent

    b. **Task Type (Tipo de tarea):** Product Deployment (Implementación del producto)

    c. **Task name (Nombre de la tarea):** Create New Task (Crear nueva tarea)

18. En la pantalla ***Client Task Catalog: New Task- McAfee Agent: Product Deployment*** (Catálogo de tareas del cliente: Nueva tarea: McAfee Agent: Implementación del producto), complete los campos de la siguiente manera:

    a. **Task Name (Nombre de la tarea):** Introduzca el nombre de la tarea

    b. **Target platforms (Plataformas objetivo):** Windows

c. **Products and components (Productos y componentes):** VirusScan Enterprise, versión validada para v6.9.6

d. **Options (Opciones):** Ejecutar con cada aplicación de directivas (solo Windows) si ***Options*** (Opciones) está disponible

19. Haga clic en ***Save*** (Guardar).
20. En la pantalla ***1 Select Task*** (1 Seleccionar tarea), seleccione lo siguiente:

    a. **Product (Producto):** McAfee Agent

    b. **Task Type (Tipo de tarea):** Product Deployment (Implementación del producto)

    c. **Task Name (Nombre de la tarea):** Nombre de la tarea recién creada

21. Haga clic en ***Next*** (Siguiente). Aparece la pantalla 2 Schedule (2 Programa).
22. Seleccione ***Run immediately*** (Ejecutar de inmediato) en la lista desplegable ***Schedule type*** (Tipo de programa).
23. Haga clic en ***Next*** (Siguiente). Aparece la pantalla 3 Summary (3 Resumen).
24. Haga clic en ***Save*** (Guardar). Aparece la pantalla ***System Tree*** (Árbol del sistema).
25. Seleccione la pestaña ***Systems*** (Sistemas) y, a continuación, seleccione todos los equipos cliente (adquisición, revisión y INW Server) que estén conectados al dominio.
26. Haga clic en ***Wake up Agents*** (Despertar agentes) en la parte inferior de la ventana.
27. Mantenga la configuración predeterminada y haga clic en ***OK*** (Aceptar).
28. Espere a que el icono de McAfee se muestre en la bandeja del sistema y, a continuación, reinicie todos los equipos cliente (adquisición, revisión y INW Server) e inicie sesión como **Administrator** (Administrador) o como miembro de ese grupo en todos los equipos cliente.
29. Haga clic en el enlace ***Log off*** (Cerrar sesión) para salir de la consola de McAfee ePolicy Orchestrator.

McAfee ePolicy Orchestrator 5.9.0: pasos para la implementación de una nueva instalación (método preferido de instalación forzada)

1. Haga clic en ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.9.0 Console*** (Inicio > Todos los programas > McAfee > ePolicy Orchestrator > Iniciar consola de McAfee ePolicy Orchestrator 5.9.0) para iniciar sesión en la consola de ePolicy Orchestrator.

NOTA: Haga clic en ***Continue with this website*** (Continuar en este sitio web) si aparece el cuadro de mensaje ***Security Alert*** (Alerta de seguridad).

2. Introduzca el nombre de usuario y contraseña, y haga clic en ***Log On*** (Iniciar sesión).
3. Seleccione ***Menu > System > System Tree*** (Menú > Sistema > Árbol del sistema). Aparece la ventana ***System Tree*** (Árbol del sistema).
4. Haga clic en ***My Organization*** (Mi organización) y, con el enfoque en ***My Organization*** (Mi organización), haga clic en ***New Systems*** (Nuevos sistemas) en la parte superior de la pantalla.

5. Seleccione ***Push agents and add systems to the current group (My Organization)*** (Forzar instalación de los agentes y agregar sistemas al grupo actual [Mi organización]) y haga clic en ***Browse*** (Buscar) en los sistemas objetivo.
6. Introduzca el nombre de usuario y la contraseña del **dominio/administrador local** y haga clic en ***OK*** (Aceptar).
7. Seleccione el dominio ***INW*** de la lista desplegable ***Domain*** (Dominio).
8. Seleccione los equipos cliente (adquisición, revisión y INW Server) conectados al dominio y haga clic en ***OK*** (Aceptar).

NOTA: Si el nombre de dominio no aparece en la lista desplegable ***Domain*** (Dominio), haga lo siguiente:

- En la ventana ***Browse for Systems*** (Buscar sistemas), haga clic en ***Cancel*** (Cancelar).
- En la ventana ***New Systems*** (Nuevos sistemas), introduzca el nombre del sistema de los equipos cliente (adquisición, revisión e INW Server) separados manualmente por una coma en el campo ***Target systems*** (Sistemas objetivo) y continúe con los siguientes pasos.

9. Seleccione ***Agent Version*** (Versión del agente) como ***McAfee Agent for Windows 5.0.5 (Current)*** (McAfee Agent para Windows 5.0.5 [Actual]). Introduzca el nombre de usuario y la contraseña del **administrador del dominio** y haga clic en ***OK*** (Aceptar).
10. En los equipos cliente (adquisición, revisión e INW Server), confirme que los directorios ***C:\Program Files\McAfee\Agent*** se crean correctamente.
11. Reinicie los equipos cliente (adquisición, revisión y INW Server) e inicie sesión como **administrador del dominio** o como miembro de ese grupo.
12. Haga clic en ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.9.0 Console*** (Inicio > Todos los programas > McAfee > ePolicy Orchestrator > Iniciar consola de McAfee ePolicy Orchestrator 5.9.0) para iniciar sesión en la consola de ePolicy Orchestrator.
13. Introduzca el nombre de usuario y contraseña, y haga clic en ***Log On*** (Iniciar sesión).
14. Seleccione ***Menu > Systems > Systems Tree*** (Menú > Sistemas > Árbol de los sistemas).
15. Haga clic en ***My Organization*** (Mi organización) y, con el enfoque en ***My organization*** (Mi organización), haga clic en la pestaña ***Assigned Client Tasks*** (Tareas asignadas del cliente).
16. Haga clic en el botón ***Actions > New Client Task Assignment*** (Acciones > Asignación de tareas nuevas del cliente) en la parte inferior de la pantalla. Aparece la pantalla ***Client Task Assignment Builder*** (Generador de asignación de tareas del cliente).
17. Seleccione lo siguiente:
    a. **Product (Producto):** McAfee Agent
    b. **Task Type (Tipo de tarea):** Product Deployment (Implementación del producto)
18. Haga clic en ***Task Actions > Create New Task*** (Acciones de tareas > Crear nueva tarea). Se mostrará la pantalla ***Create New Task*** (Crear nueva tarea).
19. En la pantalla ***Create New Task*** (Crear nueva tarea), complete los campos como se indica:

a. **Task Name (Nombre de la tarea):** Introduzca el nombre de la tarea

b. **Target platforms (Plataformas objetivo):** Windows (desmarque el resto de opciones)

c. **Products and components (Productos y componentes):** VirusScan Enterprise 8.8.0.1804

20. Haga clic en ***Save*** (Guardar). Aparece la pantalla ***Client Task Assignment Builder*** (Generador de asignación de tareas del cliente).

21. En la pantalla ***Client Task Assignment Builder*** (Generador de asignación de tareas del cliente), seleccione lo siguiente:

    a. **Product (Producto):** McAfee Agent

    b. **Task Type (Tipo de tarea):** Product Deployment (Implementación del producto)

    c. **Task Name (Nombre de la tarea):** Nombre de la tarea recién creada

    d. **Schedule Type (Tipo de programa):** Ejecución inmediata

22. Haga clic en ***Save*** (Guardar). Aparece la pantalla ***Assigned Client Tasks*** (Tareas asignadas del cliente).

23. Seleccione la pestaña ***Systems*** (Sistemas) y, a continuación, seleccione todos los equipos cliente (adquisición, revisión y INW Server) que estén conectados al dominio.

24. Haga clic en ***Wake up Agents*** (Despertar agentes) en la parte inferior de la ventana.

25. Mantenga la configuración predeterminada y haga clic en ***OK*** (Aceptar).

26. Espere a que el icono de McAfee se muestre en la bandeja del sistema y, a continuación, reinicie todos los equipos cliente (adquisición, revisión y INW Server) e inicie sesión como **Administrator** (Administrador) o como miembro de ese grupo en todos los equipos cliente.

27. Haga clic en el enlace ***Log off*** (Cerrar sesión) para salir de la consola de McAfee ePolicy Orchestrator.

Configuración de la consola del servidor McAfee ePolicy Orchestrator 5.0 y 5.3.2

1. En función de la versión del software, haga clic en ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.0.0 Console*** (Inicio > Todos los programas > McAfee > ePolicy Orchestrator > Ejecutar Consola de McAfee ePolicy Orchestrator 5.0.0) o ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.3.2 Console*** (Inicio > Todos los programas > McAfee > ePolicy Orchestrator > Ejecutar Consola de McAfee ePolicy Orchestrator 5.3.2).

2. Introduzca el nombre de usuario y contraseña, y haga clic en ***Log On*** (Iniciar sesión).

3. Seleccione ***Menu > Systems > Systems Tree*** (Menú > Sistemas > Árbol de los sistemas).

4. Haga clic en ***My Organization*** (Mi organización) y, con el enfoque en My organization (Mi organización), haga clic en la pestaña ***Assigned Client Tasks*** (Tareas asignadas del cliente).

5. Haga clic en el botón ***Actions > New Client Task Assignment*** (Acciones > Asignación de tareas nuevas del cliente) en la parte inferior de la pantalla. Aparece la pantalla ***Client Task Assignment Builder*** (Generador de asignación de tareas del cliente).

6. Seleccione lo siguiente:

    a. ***Product (Producto):*** VirusScan Enterprise 8.8.0

    b. ***Task Type (Tipo de tarea):*** On Demand Scan (Escaneo a demanda)

    c. ***Task name (Nombre de la tarea):*** Create New Task (Crear nueva tarea)

7. En la pantalla ***Client Task Catalog: New Task - VirusScan Enterprise 8.8.0: On Demand Scan*** (Catálogo de tareas del cliente: Nueva tarea: VirusScan Enterprise 8.8.0: Escaneo a demanda), complete los campos de la siguiente manera:

    a. ***Task Name (Nombre de la tarea):*** Weekly Scheduled Scan (Escaneo programado semanal)

    b. ***Descripción:*** Weekly Scheduled Scan (Escaneo programado semanal)

8. Haga clic en la pestaña ***Scan Items*** (Escanear elementos). Aparece la pantalla ***Scan Items*** (Escanear elementos).

9. Desmarque ***Detect unwanted programs*** (Detectar programas no deseados) en ***Options*** (Opciones).

10. Desmarque las siguientes opciones en Heuristics (Heurística):

    - ***Find unknown program threats (Buscar amenazas de programas desconocidos).***
    - ***Find unknown macro threats (Buscar amenazas macro desconocidas).***

11. Haga clic en la pestaña ***Exclusions*** (Exclusiones). Aparece la pantalla ***Exclusions*** (Exclusiones).

12. Haga clic en ***Add*** (Agregar). Aparece la pantalla ***Add/Edit Exclusion Item*** (Agregar/Editar elemento de exclusión).

13. Seleccione ***By pattern*** (Según diseño) e introduzca las carpetas **C:\Program Files\GE Healthcare\MLCL**, **C:\Program Files (x86)\GE Healthcare\MLCL\, D:\GEData\Studies**, **E:**, **G:** de una en una. A continuación, seleccione Also exclude subfolders (Excluir también subcarpetas). Haga clic en ***OK*** (Aceptar).

14. Haga clic en la pestaña ***Performance*** (Rendimiento). Aparece la pantalla ***Performance*** (Rendimiento).

15. Seleccione ***Disabled*** (Desactivado) en ***Artemis (Heuristic network check for suspicious files)*** (Artemis [Comprobación de red heurística para archivos sospechosos]).

16. Haga clic en ***Save*** (Guardar).

17. En la pantalla ***1 Select Task*** (1 Seleccionar tarea), seleccione lo siguiente:

    - ***Product (Producto):*** VirusScan Enterprise 8.8.0
    - ***Task Type (Tipo de tarea):*** On Demand Scan (Escaneo a demanda)
    - ***Task Name (Nombre de la tarea):*** Weekly Scheduled Scan (Escaneo programado semanal)

18. Haga clic en ***Next*** (Siguiente). Aparece la pantalla ***2 Schedule*** (2 Programa).

19. Seleccione ***Weekly*** (Semanal) en la lista desplegable ***Schedule type*** (Tipo de programa). A continuación, seleccione ***Sunday*** (Domingo).

20. Establezca la ***Start time*** (Hora inicio) en ***12:00 AM*** y seleccione ***Run Once at that time*** (Ejecutar una vez a esa hora).

21. Haga clic en ***Next*** (Siguiente). Aparece la pantalla ***3 Summary*** (3 Resumen).
22. Haga clic en ***Save*** (Guardar). Aparece la pantalla ***System Tree*** (Árbol del sistema).
23. Seleccione la pestaña ***Assigned Policies*** (Directivas asignadas). Aparece la pantalla ***Assigned Policies*** (Directivas asignadas).
24. En la lista desplegable ***Product*** (Producto), seleccione ***VirusScan Enterprise 8.8.0***.
25. Haga clic en ***My Default*** (Mi configuración predeterminada) para ***On-Access General Policies*** (Directivas generales de acceso). Aparece la pantalla ***VirusScan Enterprise 8.8.0 > On-Access General Policies > My Default*** (VirusScan Enterprise 8.8.0 > Directivas generales de acceso > Mi configuración predeterminada).
26. Seleccione ***Workstation*** (Estación de trabajo) en la lista desplegable ***Settings for*** (Configuración de) y seleccione la pestaña ***General***. Aparece la pantalla ***General***.
27. Seleccione ***Disabled*** (Desactivado) en ***Artemis (Heuristic network check for suspicious files)*** (Artemis [Comprobación de red heurística para archivos sospechosos]).
28. Haga clic en la pestaña ***ScriptScan*** (Escaneo de scripts). Aparece la pantalla ***ScriptScan*** (Escaneo de scripts).
29. Desmarque ***Enable scanning of scripts*** (Activar escaneo de scripts).
30. Haga clic en la pestaña ***Blocking*** (Bloqueo). Aparece la pantalla ***Blocking*** (Bloqueo).
31. Desmarque ***Block the connection when a threatened file is detected in a shared folder*** (Bloquear la conexión cuando se detecte un archivo amenazado en una carpeta compartida).
32. Seleccione la pestaña ***Messages*** (Mensajes). Aparece la pantalla ***Messages*** (Mensajes).
33. Desmarque ***Show the messages dialog box when a threat is detected and display the specified text in the message*** (Mostrar mensaje cuando se detecte una amenaza y mostrar el texto especificado en el mensaje).
34. Seleccione ***Server*** (Servidor) en la lista desplegable ***Settings for*** (Configuración de) y seleccione la pestaña ***General***. Aparece la pantalla ***General***.
35. Seleccione ***Disabled*** (Desactivado) en ***Artemis (Heuristic network check for suspicious files)*** (Artemis [Comprobación de red heurística para archivos sospechosos]).
36. Seleccione la pestaña ***ScriptScan*** (Escaneo de scripts). Aparece la pantalla ***Script Scan*** (Escaneo de scripts).
37. Asegúrese de que ***Enable scanning of scripts*** (Activar el escaneo de scripts) está desmarcada.
38. Haga clic en la pestaña ***Blocking*** (Bloqueo). Aparece la pantalla ***Blocking*** (Bloqueo).
39. Desmarque ***Block the connection when a threatened file is detected in a shared folder*** (Bloquear la conexión cuando se detecte un archivo amenazado en una carpeta compartida).
40. Seleccione la pestaña ***Messages*** (Mensajes). Aparece la pantalla ***Messages*** (Mensajes).
41. Desmarque ***Show the messages dialog box when a threat is detected and display the specified text in the message*** (Mostrar mensaje cuando se detecte una amenaza y mostrar el texto especificado en el mensaje).

42. Haga clic en ***Save*** (Guardar).
43. Haga clic en ***My Default*** (Mi configuración predeterminada) para ***On-Access Default Processes Policies*** (Directivas de procesos predeterminados al abrir). Aparece la pantalla ***VirusScan Enterprise 8.8.0 > On-Access Default Processes Policies > My Default*** (VirusScan Enterprise 8.8.0 > Directivas de procesos predeterminados al abrir > Mi configuración predeterminada).
44. Seleccione ***Workstation*** (Estación de trabajo) en la lista desplegable ***Settings for*** (Configuración de).
45. Haga clic en la pestaña ***Scan Items*** (Escanear elementos). Aparece la pantalla ***Scan Items*** (Escanear elementos).
46. Desmarque las siguientes opciones en ***Heuristics*** (Heurística):
    - ***Find unknown unwanted programs and trojans (Buscar troyanos y programas no deseados desconocidos).***
    - ***Find unknown macro threats (Buscar amenazas macro desconocidas).***
47. Desmarque ***Detect unwanted programs*** (Detectar programas no deseados) en ***Unwanted programs detection*** (Detección de programas no deseados).
48. Haga clic en la pestaña ***Exclusions*** (Exclusiones). Aparece la pantalla ***Exclusions*** (Exclusiones).
49. Haga clic en ***Add*** (Agregar). Aparece la pantalla ***Add/Edit Exclusion Item*** (Agregar/Editar elemento de exclusión).
50. Seleccione ***By pattern*** (Según diseño) e introduzca las carpetas **C:\Program Files\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:**, **G:** de una en una. A continuación, seleccione ***Also exclude subfolders*** (Excluir también subcarpetas). Haga clic en ***OK*** (Aceptar).
51. Seleccione ***Server*** (Servidor) en la lista desplegable ***Settings for*** (Configuración de) y haga clic en la pestaña ***Scan Items*** (Escanear elementos). Aparece la pantalla ***Scan Items*** (Escanear elementos).
52. Desmarque las siguientes opciones en ***Heuristics*** (Heurística):
    - ***Find unknown unwanted programs and trojans (Buscar troyanos y programas no deseados desconocidos).***
    - ***Find unknown macro threats (Buscar amenazas macro desconocidas).***
53. Desmarque ***Detect unwanted programs*** (Detectar programas no deseados) en ***Unwanted programs detection*** (Detección de programas no deseados).
54. Haga clic en la pestaña ***Exclusions*** (Exclusiones). Aparece la pantalla ***Exclusions*** (Exclusiones).
55. Haga clic en ***Add*** (Agregar). Aparece la pantalla ***Add/Edit Exclusion Item*** (Agregar/Editar elemento de exclusión).
56. Seleccione ***By pattern*** (Según diseño) e introduzca las carpetas **C:\Program Files (x86)\GE Healthcare\MLCL**, **D:\GEData\Studies** de una en una. A continuación, seleccione ***Also exclude subfolders*** (Excluir también subcarpetas). Haga clic en ***OK*** (Aceptar).
57. Haga clic en ***Save*** (Guardar).
58. Haga clic en ***My Default*** (Mi configuración predeterminada) para ***On-Access Low-Risk Processes Policies*** (Directivas de procesos de bajo riesgo al abrir). Aparece la pantalla

VirusScan Enterprise 8.8.0 > On-Access Low-Risk Processes Policies > My Default (VirusScan Enterprise 8.8.0 > Directivas de procesos de bajo riesgo al abrir > Mi configuración predeterminada).

59. Seleccione ***Workstation*** (Estación de trabajo) en la lista desplegable ***Settings for*** (Configuración de).
60. Haga clic en la pestaña ***Scan Items*** (Escanear elementos). Aparece la pantalla ***Scan Items*** (Escanear elementos).
61. Desmarque las siguientes opciones en ***Heuristics*** (Heurística):
    - ***Find unknown unwanted programs and trojans (Buscar troyanos y programas no deseados desconocidos).***
    - ***Find unknown macro threats (Buscar amenazas macro desconocidas).***
62. Desmarque ***Detect unwanted programs*** (Detectar programas no deseados) en ***Unwanted programs detection*** (Detección de programas no deseados).
63. Haga clic en la pestaña ***Exclusions*** (Exclusiones). Aparece la pantalla ***Exclusions*** (Exclusiones).
64. Haga clic en ***Add*** (Agregar). Aparece la pantalla ***Add/Edit Exclusion Item*** (Agregar/Editar elemento de exclusión).
65. Seleccione ***By pattern*** (Según diseño) e introduzca las carpetas **C:\Program Files\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:**, **G:** de una en una. A continuación, seleccione ***Also exclude subfolders*** (Excluir también subcarpetas). Haga clic en ***OK*** (Aceptar).
66. Seleccione ***Server*** (Servidor) en la lista desplegable ***Settings for*** (Configuración de) y haga clic en la pestaña ***Scan Items*** (Escanear elementos). Aparece la pantalla ***Scan Items*** (Escanear elementos).
67. Desmarque las siguientes opciones en ***Heuristics*** (Heurística):
    - ***Find unknown unwanted programs and trojans (Buscar troyanos y programas no deseados desconocidos).***
    - ***Find unknown macro threats (Buscar amenazas macro desconocidas).***
68. Desmarque ***Detect unwanted programs*** (Detectar programas no deseados) en ***Unwanted programs detection*** (Detección de programas no deseados).
69. Haga clic en la pestaña ***Exclusions*** (Exclusiones). Aparece la pantalla ***Exclusions*** (Exclusiones).
70. Haga clic en ***Add*** (Agregar). Aparece la pantalla ***Add/Edit Exclusion Item*** (Agregar/Editar elemento de exclusión).
71. Seleccione ***By pattern*** (Según diseño) e introduzca las carpetas **C:\Program Files (x86)\GE Healthcare\MLCL**, **D:\GEData\Studies** de una en una. A continuación, seleccione ***Also exclude subfolders*** (Excluir también subcarpetas). Haga clic en ***OK*** (Aceptar).
72. Haga clic en ***Save*** (Guardar).
73. Haga clic en ***My Default*** (Mi configuración predeterminada) para ***On-Access High-Risk Processes Policies*** (Directivas de procesos de alto riesgo al abrir). Aparece la pantalla ***VirusScan Enterprise 8.8.0 > On-Access High-Risk Processes Policies > My Default*** (VirusScan Enterprise 8.8.0 > Directivas de procesos de alto riesgo al abrir > Mi configuración predeterminada).

74. Seleccione ***Workstation*** (Estación de trabajo) en la lista desplegable ***Settings for*** (Configuración de).
75. Haga clic en la pestaña ***Scan Items*** (Escanear elementos). Aparece la pantalla ***Scan Items*** (Escanear elementos).
76. Desmarque las siguientes opciones en ***Heuristics*** (Heurística):
    - ***Find unknown unwanted programs and trojans (Buscar troyanos y programas no deseados desconocidos).***
    - ***Find unknown macro threats (Buscar amenazas macro desconocidas).***
77. Desmarque ***Detect unwanted programs*** (Detectar programas no deseados) en ***Unwanted programs detection*** (Detección de programas no deseados).
78. Haga clic en la pestaña ***Exclusions*** (Exclusiones). Aparece la pantalla ***Exclusions*** (Exclusiones).
79. Haga clic en ***Add*** (Agregar). Aparece la pantalla ***Add/Edit Exclusion Item*** (Agregar/Editar elemento de exclusión).
80. Seleccione ***By pattern*** (Según diseño) e introduzca las carpetas **C:\Program Files\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:**, **G:** de una en una. A continuación, seleccione ***Also exclude subfolders*** (Excluir también subcarpetas). Haga clic en ***OK*** (Aceptar).
81. Seleccione ***Server*** (Servidor) en la lista desplegable ***Settings for*** (Configuración de) y haga clic en la pestaña ***Scan Items*** (Escanear elementos). Aparece la pantalla ***Scan Items*** (Escanear elementos).
82. Desmarque las siguientes opciones en ***Heuristics*** (Heurística):
    - ***Find unknown unwanted programs and trojans (Buscar troyanos y programas no deseados desconocidos).***
    - ***Find unknown macro threats (Buscar amenazas macro desconocidas).***
83. Desmarque ***Detect unwanted programs*** (Detectar programas no deseados) en ***Unwanted programs detection*** (Detección de programas no deseados).
84. Haga clic en la pestaña ***Exclusions*** (Exclusiones). Aparece la pantalla ***Exclusions*** (Exclusiones).
85. Haga clic en ***Add*** (Agregar). Aparece la pantalla ***Add/Edit Exclusion Item*** (Agregar/Editar elemento de exclusión).
86. Seleccione By pattern (Según diseño) e introduzca las carpetas **C:\Program Files (x86)\GE Healthcare\MLCL**, **D:\GEData\Studies** de una en una. A continuación, seleccione ***Also exclude subfolders*** (Excluir también subcarpetas). Haga clic en ***OK*** (Aceptar).
87. Haga clic en ***Save*** (Guardar).
88. Haga clic en ***My Default*** (Mi configuración predeterminada) para ***On-Delivery Email Scan Policies*** (Directivas de escáner de correo electrónico a demanda). Aparece la pantalla ***VirusScan Enterprise 8.8.0 > On Delivery Email Scan Policies > My Default*** (VirusScan Enterprise 8.8.0 > Directivas de escáner de correo electrónico a demanda > Mi configuración predeterminada).
89. Seleccione ***Workstation*** (Estación de trabajo) en la lista desplegable ***Settings for*** (Configuración de).

90. Haga clic en la pestaña ***Scan Items*** (Escanear elementos). Aparece la pantalla ***Scan Items*** (Escanear elementos).
91. Desmarque las siguientes opciones en ***Heuristics*** (Heurística).
    - ***Find unknown program threats and trojans (Buscar troyanos y amenazas de programas desconocidos).***
    - ***Find unknown macro threats (Buscar amenazas macro desconocidas).***
    - ***Find attachments with multiple extensions (Buscar adjuntos con varias extensiones).***
92. Desmarque ***Detect unwanted programs*** (Detectar programas no deseados) en ***Unwanted programs detection*** (Detección de programas no deseados).
93. Seleccione ***Disabled*** (Desactivado) en ***Artemis (Heuristic network check for suspicious files)*** (Artemis [Comprobación de red heurística para archivos sospechosos]).
94. Desmarque ***Enable on-delivery email scanning*** (Activar escaneo de correo electrónico al llegar) en ***Scanning of email*** (Escaneo de correo electrónico).
95. Seleccione ***Server*** (Servidor) en la lista desplegable ***Settings for*** (Configuración de).
96. Haga clic en la pestaña ***Scan Items*** (Escanear elementos). Aparece la pantalla ***Scan Items*** (Escanear elementos).
97. Desmarque las siguientes opciones en ***Heuristics*** (Heurística):
    - ***Find unknown program threats and trojans (Buscar troyanos y amenazas de programas desconocidos).***
    - ***Find unknown macro threats (Buscar amenazas macro desconocidas).***
    - ***Find attachments with multiple extensions (Buscar adjuntos con varias extensiones).***
98. Desmarque ***Detect unwanted programs*** (Detectar programas no deseados) en ***Unwanted programs detection*** (Detección de programas no deseados).
99. Seleccione ***Disabled*** (Desactivado) en ***Artemis (Heuristic network check for suspicious files)*** (Artemis [Comprobación de red heurística para archivos sospechosos]).
100. Desmarque ***Enable on-delivery email scanning*** (Activar escaneo de correo electrónico al llegar) en ***Scanning of email*** (Escaneo de correo electrónico).
101. Haga clic en ***Save*** (Guardar).
102. Haga clic en ***My Default*** (Mi configuración predeterminada) para ***General Options Policies*** (Directivas de opciones generales). Aparece la pantalla ***VirusScan Enterprise 8.8.0 > General Options Policies > My Default*** (VirusScan Enterprise 8.8.0 > Directivas de opciones generales > Mi configuración predeterminada).
103. Seleccione ***Workstation*** (Estación de trabajo) en la lista desplegable ***Settings for*** (Configuración de).
104. Haga clic en la pestaña ***Display Options*** (Opciones de pantalla). Aparece la pantalla ***Display Options*** (Opciones de pantalla).
105. Seleccione las siguientes opciones en ***Console options*** (Opciones de la consola):
    - ***Display managed tasks in the client console (Mostrar las tareas administradas en la consola del cliente).***

- ***Disable default AutoUpdate task schedule (Desactivar el programa predeterminado de las tareas de actualización automática).***

106. Seleccione ***Server*** (Servidor) en la lista desplegable ***Settings for*** (Configuración de).
107. Haga clic en la pestaña ***Display Options*** (Opciones de pantalla). Aparece la pantalla ***Display Options*** (Opciones de pantalla).
108. Seleccione las siguientes opciones en ***Console options*** (Opciones de la consola):
    - ***Display managed tasks in the client console (Mostrar las tareas administradas en la consola del cliente).***
    - ***Disable default AutoUpdate task schedule (Desactivar el programa predeterminado de las tareas de actualización automática).***
109. Haga clic en ***Save*** (Guardar).
110. Haga clic en ***My Default*** (Mi configuración predeterminada) para ***Alert Policies*** (Directivas de alertas). Aparece la pantalla ***VirusScan Enterprise 8.8.0 > Alter Policies > My Default*** (VirusScan Enterprise 8.8.0 > Directivas de alertas > Mi configuración predeterminada).
111. Seleccione ***Workstation*** (Estación de trabajo) en la lista desplegable ***Settings for*** (Configuración de).
112. Seleccione la pestaña ***Alert Manager Alerts*** (Alertas del administrador de alertas). Aparece la pantalla ***Alert Manager Alerts*** (Alertas del administrador de alertas).
113. Desmarque ***On-Access Scan*** (Escaneo al abrir), ***On-Demand Scan and scheduled scans*** (Escaneos a demanda y con horario), ***Email Scan*** (Escaneo de correo electrónico) y ***AutoUpdate*** (Actualización automática) en ***Components that generate alerts*** (Componentes que generan alertas).
114. Seleccione ***Disable alerting*** (Desactivar alertas) en las opciones ***Alert Manager*** (Administrador de alertas).
115. Desmarque ***Access Protection*** (Protección de acceso) en ***Components that generate alerts*** (Componentes que generan alertas).
116. Haga clic en ***Additional Alerting Options*** (Otras opciones de alerta). Aparece la pantalla ***Additional Alerting Options*** (Otras opciones de alerta).
117. En el menú desplegable ***Severity Filters*** (Filtros de gravedad), seleccione ***Suppress all alerts (severities 0 to 4)*** (Suprimir todas las alertas [gravedad 0 a 4]).
118. Seleccione ***Server*** (Servidor) en la lista desplegable ***Settings for*** (Configuración de) y seleccione la pestaña ***Alert Manager Alerts*** (Alertas del administrador de alertas). Aparece la pantalla ***Alert Manager Alerts*** (Alertas del administrador de alertas).
119. Desmarque ***On-Access Scan*** (Escaneo al abrir), ***On-Demand Scan and scheduled scans*** (Escaneos a demanda y con horario), ***Email Scan*** (Escaneo de correo electrónico) y ***AutoUpdate*** (Actualización automática) en ***Components that generate alerts*** (Componentes que generan alertas).
120. Marque ***Disable alerting*** (Desactivar alertas) en las opciones ***Alert Manager*** (Administrador de alertas).
121. Desmarque ***Access Protection*** (Protección de acceso) en ***Components that generate alerts*** (Componentes que generan alertas).

122. Haga clic en ***Additional Alerting Options*** (Otras opciones de alerta). Aparece la pantalla Additional Alerting Options (Otras opciones de alerta).

123. En el menú desplegable ***Severity Filters*** (Filtros de gravedad), seleccione ***Suppress all alerts (severities 0 to 4)*** (Suprimir todas las alertas [gravedad 0 a 4]).

124. Haga clic en ***Save*** (Guardar).

125. Haga clic en ***My Default*** (Mi configuración predeterminada) para ***Access Protection Policies*** (Directivas de protección de acceso). Aparece la pantalla ***VirusScan Enterprise 8.8.0 > Access Protection Policies > My Default*** (VirusScan Enterprise 8.8.0 > Directivas de protección de acceso > Mi configuración predeterminada).

126. Seleccione ***Workstation*** (Estación de trabajo) en la lista desplegable ***Settings for*** (Configuración de).

127. Haga clic en la ficha ***Access Protection*** (Protección de acceso). Aparece la pantalla ***Access Protection*** (Protección de acceso).

128. Desmarque las siguientes opciones en ***Access protection settings*** (Configuración de protección de acceso):

    - ***Enable access protection (Activar protección de acceso).***
    - ***Prevent McAfee services from being stopped (Evitar que los servicios de McAfee se detengan).***

129. Seleccione ***Server*** (Servidor) en la lista desplegable ***Settings for*** (Configuración de).

130. Haga clic en la ficha ***Access Protection*** (Protección de acceso). Aparece la pantalla ***Access Protection*** (Protección de acceso).

131. Desmarque las siguientes opciones en ***Access protection settings*** (Configuración de protección de acceso):

    - ***Enable access protection (Activar protección de acceso).***
    - ***Prevent McAfee services from being stopped (Evitar que los servicios de McAfee se detengan).***

132. Haga clic en ***Save*** (Guardar).

133. Seleccione ***My Default*** (Mi configuración predeterminada) para ***Buffer Overflow Protection Policies*** (Directivas de protección de desbordamiento de memoria intermedia). Aparece la pantalla ***VirusScan Enterprise 8.8.0 > Buffer Overflow Protection Policies > My Default*** (VirusScan Enterprise 8.8.0 > Directivas de protección de desbordamiento de memoria intermedia > Mi configuración predeterminada).

134. Seleccione ***Workstation*** (Estación de trabajo) en la lista desplegable ***Settings for*** (Configuración de).

135. Haga clic en la pestaña ***Buffer Overflow Protection*** (Protección de desbordamiento de memoria intermedia). Aparece la ventana ***Buffer Overflow Protection*** (Protección de desbordamiento de memoria intermedia).

136. Desmarque ***Show the message dialog box when a buffer overflow is detected*** (Mostrar el cuadro de diálogo de mensajes cuando se detecte un desbordamiento de memoria intermedia) y haga clic en ***Client system warning*** (Advertencia del sistema del cliente).

137. Desmarque ***Enable buffer overflow protection*** (Activar protección de desbordamiento de memoria intermedia) en ***Buffer overflow settings*** (Configuración del desbordamiento de memoria intermedia).

138. Seleccione ***Server*** (Servidor) en la lista desplegable ***Settings for*** (Configuración de).

139. Haga clic en la pestaña ***Buffer Overflow Protection*** (Protección de desbordamiento de memoria intermedia). Aparece la ventana ***Buffer Overflow Protection*** (Protección de desbordamiento de memoria intermedia).

140. Desmarque ***Show the message dialog box when a buffer overflow is detected*** (Mostrar el cuadro de diálogo de mensajes cuando se detecte un desbordamiento de memoria intermedia) y haga clic en ***Client system warning*** (Advertencia del sistema del cliente).

141. Desmarque ***Enable buffer overflow protection*** (Activar protección de desbordamiento de memoria intermedia) en ***Buffer overflow settings*** (Configuración del desbordamiento de memoria intermedia).

142. Haga clic en ***Save*** (Guardar).

143. En el menú desplegable ***Product*** (Producto), seleccione ***McAfee Agent***. Aparece la ventana ***Policies*** (Directivas) de McAfee Agent.

144. Haga clic en ***My Default*** (Mi configuración predeterminada) para ***Repository*** (Repositorio). Aparece la pantalla ***McAfee Agent > Repository > My Default*** (McAfee Agent > Repositorio > Mi configuración predeterminada).

145. Haga clic en la pestaña ***Proxy***. Aparece la pantalla ***Proxy***.

146. Seleccione ***Use Internet Explorer settings (For Windows)/System Preferences settings (For Mac OSX)*** (Usar ajustes de Internet Explorer [para Windows]/Configuración de preferencias del sistema [para Mac OSX]) en ***Proxy settings*** (Configuración de proxy).

147. Haga clic en ***Save*** (Guardar).

148. Haga clic en la pestaña ***Systems*** (Sistemas).

149. Seleccione todos los sistemas del cliente (adquisición, revisión y servidor Centricity Cardiology INW) en los que se vayan a implantar las directivas configuradas.

150. Seleccione ***Wake Up Agents*** (Despertar agentes). Aparece la pantalla ***Wake Up Agent*** (Despertar agente).

151. Haga clic en ***OK*** (Aceptar).

152. Termine la sesión en ePolicy Orchestrator.

Configuración de la consola del servidor de McAfee ePolicy Orchestrator 5.9.0

1. Dependiendo de la versión de software, seleccione ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.9.0 Console*** (Inicio > Todos los programas> McAfee > ePolicy Orchestrator > Ejecutar consola de McAfee ePolicy Orchestrator 5.9.0).

2. Introduzca el nombre de usuario y contraseña, y haga clic en ***Log On*** (Iniciar sesión).

3. Seleccione ***Menu > Systems > Systems Tree*** (Menú > Sistemas > Árbol de los sistemas).

4. Haga clic en ***My Organization*** (Mi organización) y, con el enfoque en My organization (Mi organización), haga clic en la pestaña ***Assigned Client Tasks*** (Tareas asignadas del cliente).

5. Haga clic en el botón ***Actions > New Client Task Assignment*** (Acciones > Asignación de tareas nuevas del cliente) en la parte inferior de la pantalla. Aparece la pantalla ***Client Task Assignment Builder*** (Generador de asignación de tareas del cliente).
6. Seleccione lo siguiente:
    a. ***Product (Producto):*** VirusScan Enterprise 8.8.0
    b. ***Task Type (Tipo de tarea):*** On Demand Scan (Escaneo a demanda)
7. Haga clic en ***Create New Task*** (Crear nueva tarea) en ***Task Actions*** (Acciones de tareas). Aparece la pantalla ***Create New Task*** (Crear nueva tarea).
8. En la pantalla ***Create New Task*** (Crear nueva tarea), complete los campos como se indica:
    a. ***Task Name (Nombre de la tarea):*** Weekly Scheduled Scan (Escaneo programado semanal)
    b. ***Descripción:*** Weekly Scheduled Scan (Escaneo programado semanal)
9. Haga clic en la pestaña ***Scan Items*** (Escanear elementos). Aparece la pantalla ***Scan Items*** (Escanear elementos).
10. Desmarque ***Detect unwanted programs*** (Detectar programas no deseados) en ***Options*** (Opciones).
11. Desmarque las siguientes opciones en Heuristics (Heurística):
    - ***Find unknown program threats (Buscar amenazas de programas desconocidos).***
    - ***Find unknown macro threats (Buscar amenazas macro desconocidas).***
12. Haga clic en la pestaña ***Exclusions*** (Exclusiones). Aparece la pantalla ***Exclusions*** (Exclusiones).
13. Haga clic en ***Add*** (Agregar). Aparece la pantalla ***Add/Edit Exclusion Item*** (Agregar/Editar elemento de exclusión).
14. Seleccione ***By pattern*** (Según diseño) e introduzca las carpetas **C:\Program Files\GE Healthcare\MLCL**, **C:\Program Files (x86)\GE Healthcare\MLCL\, D:\GEData\Studies**, **E:**, **G:** de una en una. A continuación, seleccione Also exclude subfolders (Excluir también subcarpetas). Haga clic en ***OK*** (Aceptar).
15. Haga clic en la pestaña ***Performance*** (Rendimiento). Aparece la pantalla ***Performance*** (Rendimiento).
16. Seleccione ***Disabled*** (Desactivado) en ***Artemis (Heuristic network check for suspicious files)*** (Artemis [Comprobación de red heurística para archivos sospechosos]).
17. Haga clic en ***Save*** (Guardar). Aparece la pantalla ***Client Task Assignment Builder*** (Generador de asignación de tareas del cliente).
18. En la pantalla ***Client Task Assignment Builder*** (Generador de asignación de tareas del cliente), seleccione lo siguiente:
    - ***Product (Producto):*** VirusScan Enterprise 8.8.0
    - ***Task Type (Tipo de tarea):*** On Demand Scan (Escaneo a demanda)
    - ***Task Name (Nombre de la tarea):*** Weekly Scheduled Scan (Escaneo programado semanal)

19. Seleccione ***Weekly*** (Semanal) en la lista desplegable ***Schedule type*** (Tipo de programa). A continuación, seleccione ***Sunday*** (Domingo).
20. Establezca la ***Start time*** (Hora inicio) en ***12:00 AM*** y seleccione ***Run Once at that time*** (Ejecutar una vez a esa hora).
21. Haga clic en ***Save*** (Guardar). Aparece la pantalla ***Assigned Client Tasks*** (Tareas asignadas del cliente).
22. Seleccione la pestaña ***Assigned Policies*** (Directivas asignadas). Aparece la pantalla ***Assigned Policies*** (Directivas asignadas).
23. En la lista desplegable ***Product*** (Producto), seleccione ***VirusScan Enterprise 8.8.0***.
24. Haga clic en ***My Default*** (Mi configuración predeterminada) para ***On-Access General Policies*** (Directivas generales de acceso). Aparece la pantalla ***VirusScan Enterprise 8.8.0 > On-Access General Policies > My Default*** (VirusScan Enterprise 8.8.0 > Directivas generales de acceso > Mi configuración predeterminada).
25. Seleccione ***Workstation*** (Estación de trabajo) en la lista desplegable ***Settings for*** (Configuración de) y seleccione la pestaña ***General***. Aparece la pantalla ***General***.
26. Seleccione ***Disabled*** (Desactivado) en ***Artemis (Heuristic network check for suspicious files)*** (Artemis [Comprobación de red heurística para archivos sospechosos]).
27. Haga clic en la pestaña ***ScriptScan*** (Escaneo de scripts). Aparece la pantalla ***ScriptScan*** (Escaneo de scripts).
28. Desmarque ***Enable scanning of scripts*** (Activar escaneo de scripts).
29. Haga clic en la pestaña ***Blocking*** (Bloqueo). Aparece la pantalla ***Blocking*** (Bloqueo).
30. Desmarque ***Block the connection when a threatened file is detected in a shared folder*** (Bloquear la conexión cuando se detecte un archivo amenazado en una carpeta compartida).
31. Seleccione la pestaña ***Messages*** (Mensajes). Aparece la pantalla ***Messages*** (Mensajes).
32. Desmarque ***Show the messages dialog box when a threat is detected and display the specified text in the message*** (Mostrar mensaje cuando se detecte una amenaza y mostrar el texto especificado en el mensaje).
33. Seleccione ***Server*** (Servidor) en la lista desplegable ***Settings for*** (Configuración de) y seleccione la pestaña ***General***. Aparece la pantalla ***General***.
34. Seleccione ***Disabled*** (Desactivado) en ***Artemis (Heuristic network check for suspicious files)*** (Artemis [Comprobación de red heurística para archivos sospechosos]).
35. Seleccione la pestaña ***ScriptScan*** (Escaneo de scripts). Aparece la pantalla ***Script Scan*** (Escaneo de scripts).
36. Asegúrese de que ***Enable scanning of scripts*** (Activar el escaneo de scripts) está desmarcada.
37. Haga clic en la pestaña ***Blocking*** (Bloqueo). Aparece la pantalla ***Blocking*** (Bloqueo).
38. Desmarque ***Block the connection when a threatened file is detected in a shared folder*** (Bloquear la conexión cuando se detecte un archivo amenazado en una carpeta compartida).

39. Seleccione la pestaña ***Messages*** (Mensajes). Aparece la pantalla ***Messages*** (Mensajes).
40. Desmarque ***Show the messages dialog box when a threat is detected and display the specified text in the message*** (Mostrar mensaje cuando se detecte una amenaza y mostrar el texto especificado en el mensaje).
41. Haga clic en ***Save*** (Guardar). Aparece la pantalla Assigned Policies (Directivas asignadas).
42. Haga clic en ***My Default*** (Mi configuración predeterminada) para ***On-Access Default Processes Policies*** (Directivas de procesos predeterminados al abrir). Aparece la pantalla ***VirusScan Enterprise 8.8.0 > On-Access Default Processes Policies > My Default*** (VirusScan Enterprise 8.8.0 > Directivas de procesos predeterminados al abrir > Mi configuración predeterminada).
43. Seleccione ***Workstation*** (Estación de trabajo) en la lista desplegable ***Settings for*** (Configuración de).
44. Haga clic en la pestaña ***Scan Items*** (Escanear elementos). Aparece la pantalla ***Scan Items*** (Escanear elementos).
45. Desmarque las siguientes opciones en ***Heuristics*** (Heurística):
    - ***Find unknown unwanted programs and trojans (Buscar troyanos y programas no deseados desconocidos).***
    - ***Find unknown macro threats (Buscar amenazas macro desconocidas).***
46. Desmarque ***Detect unwanted programs*** (Detectar programas no deseados) en ***Unwanted programs detection*** (Detección de programas no deseados).
47. Haga clic en la pestaña ***Exclusions*** (Exclusiones). Aparece la pantalla ***Exclusions*** (Exclusiones).
48. Haga clic en ***Add*** (Agregar). Aparece la pantalla ***Add/Edit Exclusion Item*** (Agregar/Editar elemento de exclusión).
49. Seleccione ***By pattern*** (Según diseño) e introduzca las carpetas **C:\Program Files\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:**, **G:** de una en una. A continuación, seleccione ***Also exclude subfolders*** (Excluir también subcarpetas). Haga clic en ***OK*** (Aceptar).
50. Seleccione ***Server*** (Servidor) en la lista desplegable ***Settings for*** (Configuración de) y haga clic en la pestaña ***Scan Items*** (Escanear elementos). Aparece la pantalla ***Scan Items*** (Escanear elementos).
51. Desmarque las siguientes opciones en ***Heuristics*** (Heurística):
    - ***Find unknown unwanted programs and trojans (Buscar troyanos y programas no deseados desconocidos).***
    - ***Find unknown macro threats (Buscar amenazas macro desconocidas).***
52. Desmarque ***Detect unwanted programs*** (Detectar programas no deseados) en ***Unwanted programs detection*** (Detección de programas no deseados).
53. Haga clic en la pestaña ***Exclusions*** (Exclusiones). Aparece la pantalla ***Exclusions*** (Exclusiones).
54. Haga clic en ***Add*** (Agregar). Aparece la pantalla ***Add/Edit Exclusion Item*** (Agregar/Editar elemento de exclusión).

55. Seleccione ***By pattern*** (Según diseño) e introduzca las carpetas **C:\Program Files (x86)\GE Healthcare\MLCL**, **D:\GEData\Studies** de una en una. A continuación, seleccione ***Also exclude subfolders*** (Excluir también subcarpetas). Haga clic en ***OK*** (Aceptar).

56. Haga clic en ***Save*** (Guardar). Aparece la pantalla ***Assigned Policies*** (Directivas asignadas).

57. Haga clic en ***My Default*** (Mi configuración predeterminada) para ***On-Access Low-Risk Processes Policies*** (Directivas de procesos de bajo riesgo al abrir). Aparece la pantalla ***VirusScan Enterprise 8.8.0 > On-Access Low-Risk Processes Policies > My Default*** (VirusScan Enterprise 8.8.0 > Directivas de procesos de bajo riesgo al abrir > Mi configuración predeterminada).

58. Seleccione ***Workstation*** (Estación de trabajo) en la lista desplegable ***Settings for*** (Configuración de).

59. Haga clic en la pestaña ***Scan Items*** (Escanear elementos). Aparece la pantalla ***Scan Items*** (Escanear elementos).

60. Desmarque las siguientes opciones en ***Heuristics*** (Heurística):

    - ***Find unknown unwanted programs and trojans (Buscar troyanos y programas no deseados desconocidos).***
    - ***Find unknown macro threats (Buscar amenazas macro desconocidas).***

61. Desmarque ***Detect unwanted programs*** (Detectar programas no deseados) en ***Unwanted programs detection*** (Detección de programas no deseados).

62. Haga clic en la pestaña ***Exclusions*** (Exclusiones). Aparece la pantalla ***Exclusions*** (Exclusiones).

63. Haga clic en ***Add*** (Agregar). Aparece la pantalla ***Add/Edit Exclusion Item*** (Agregar/Editar elemento de exclusión).

64. Seleccione ***By pattern*** (Según diseño) e introduzca las carpetas **C:\Program Files\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:**, **G:** de una en una. A continuación, seleccione ***Also exclude subfolders*** (Excluir también subcarpetas). Haga clic en ***OK*** (Aceptar).

65. Seleccione ***Server*** (Servidor) en la lista desplegable ***Settings for*** (Configuración de) y haga clic en la pestaña ***Scan Items*** (Escanear elementos). Aparece la pantalla ***Scan Items*** (Escanear elementos).

66. Desmarque las siguientes opciones en ***Heuristics*** (Heurística):

    - ***Find unknown unwanted programs and trojans (Buscar troyanos y programas no deseados desconocidos).***
    - ***Find unknown macro threats (Buscar amenazas macro desconocidas).***

67. Desmarque ***Detect unwanted programs*** (Detectar programas no deseados) en ***Unwanted programs detection*** (Detección de programas no deseados).

68. Haga clic en la pestaña ***Exclusions*** (Exclusiones). Aparece la pantalla ***Exclusions*** (Exclusiones).

69. Haga clic en ***Add*** (Agregar). Aparece la pantalla ***Add/Edit Exclusion Item*** (Agregar/Editar elemento de exclusión).

70. Seleccione ***By pattern*** (Según diseño) e introduzca las carpetas **C:\Program Files (x86)\GE Healthcare\MLCL**, **D:\GEData\Studies** de una en una. A continuación, seleccione ***Also exclude subfolders*** (Excluir también subcarpetas). Haga clic en ***OK*** (Aceptar).

71. Haga clic en ***Save*** (Guardar). Aparece la pantalla ***Assigned Policies*** (Directivas asignadas).
72. Haga clic en ***My Default*** (Mi configuración predeterminada) para ***On-Access High-Risk Processes Policies*** (Directivas de procesos de alto riesgo al abrir). Aparece la pantalla ***VirusScan Enterprise 8.8.0 > On-Access High-Risk Processes Policies > My Default*** (VirusScan Enterprise 8.8.0 > Directivas de procesos de alto riesgo al abrir > Mi configuración predeterminada).
73. Seleccione ***Workstation*** (Estación de trabajo) en la lista desplegable ***Settings for*** (Configuración de).
74. Haga clic en la pestaña ***Scan Items*** (Escanear elementos). Aparece la pantalla ***Scan Items*** (Escanear elementos).
75. Desmarque las siguientes opciones en ***Heuristics*** (Heurística):
    - ***Find unknown unwanted programs and trojans (Buscar troyanos y programas no deseados desconocidos).***
    - ***Find unknown macro threats (Buscar amenazas macro desconocidas).***
76. Desmarque ***Detect unwanted programs*** (Detectar programas no deseados) en ***Unwanted programs detection*** (Detección de programas no deseados).
77. Haga clic en la pestaña ***Exclusions*** (Exclusiones). Aparece la pantalla ***Exclusions*** (Exclusiones).
78. Haga clic en ***Add*** (Agregar). Aparece la pantalla ***Add/Edit Exclusion Item*** (Agregar/Editar elemento de exclusión).
79. Seleccione ***By pattern*** (Según diseño) e introduzca las carpetas **C:\Program Files\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:**, **G:** de una en una. A continuación, seleccione ***Also exclude subfolders*** (Excluir también subcarpetas). Haga clic en ***OK*** (Aceptar).
80. Seleccione ***Server*** (Servidor) en la lista desplegable ***Settings for*** (Configuración de) y haga clic en la pestaña ***Scan Items*** (Escanear elementos). Aparece la pantalla ***Scan Items*** (Escanear elementos).
81. Desmarque las siguientes opciones en ***Heuristics*** (Heurística):
    - ***Find unknown unwanted programs and trojans (Buscar troyanos y programas no deseados desconocidos).***
    - ***Find unknown macro threats (Buscar amenazas macro desconocidas).***
82. Desmarque ***Detect unwanted programs*** (Detectar programas no deseados) en ***Unwanted programs detection*** (Detección de programas no deseados).
83. Haga clic en la pestaña ***Exclusions*** (Exclusiones). Aparece la pantalla ***Exclusions*** (Exclusiones).
84. Haga clic en ***Add*** (Agregar). Aparece la pantalla ***Add/Edit Exclusion Item*** (Agregar/Editar elemento de exclusión).
85. Seleccione By pattern (Según diseño) e introduzca las carpetas **C:\Program Files (x86)\GE Healthcare\MLCL**, **D:\GEData\Studies** de una en una. A continuación, seleccione ***Also exclude subfolders*** (Excluir también subcarpetas). Haga clic en ***OK*** (Aceptar).
86. Haga clic en ***Save*** (Guardar). Aparece la pantalla ***Assigned Policies*** (Directivas asignadas).
87. Haga clic en ***My Default*** (Mi configuración predeterminada) para ***On-Delivery Email Scan Policies*** (Directivas de escáner de correo electrónico a demanda). Aparece la pantalla

VirusScan Enterprise 8.8.0 > On Delivery Email Scan Policies > My Default (VirusScan Enterprise 8.8.0 > Directivas de escáner de correo electrónico a demanda > Mi configuración predeterminada).

88. Seleccione ***Workstation*** (Estación de trabajo) en la lista desplegable ***Settings for*** (Configuración de).
89. Haga clic en la pestaña ***Scan Items*** (Escanear elementos). Aparece la pantalla ***Scan Items*** (Escanear elementos).
90. Desmarque las siguientes opciones en ***Heuristics*** (Heurística).
    - ***Find unknown program threats and trojans (Buscar troyanos y amenazas de programas desconocidos).***
    - ***Find unknown macro threats (Buscar amenazas macro desconocidas).***
    - ***Find attachments with multiple extensions (Buscar adjuntos con varias extensiones).***
91. Desmarque ***Detect unwanted programs*** (Detectar programas no deseados) en ***Unwanted programs detection*** (Detección de programas no deseados).
92. Seleccione ***Disabled*** (Desactivado) en ***Artemis (Heuristic network check for suspicious files)*** (Artemis [Comprobación de red heurística para archivos sospechosos]).
93. Desmarque ***Enable on-delivery email scanning*** (Activar escaneo de correo electrónico al llegar) en ***Scanning of email*** (Escaneo de correo electrónico).
94. Seleccione ***Server*** (Servidor) en la lista desplegable ***Settings for*** (Configuración de).
95. Haga clic en la pestaña ***Scan Items*** (Escanear elementos). Aparece la pantalla ***Scan Items*** (Escanear elementos).
96. Desmarque las siguientes opciones en ***Heuristics*** (Heurística):
    - ***Find unknown program threats and trojans (Buscar troyanos y amenazas de programas desconocidos).***
    - ***Find unknown macro threats (Buscar amenazas macro desconocidas).***
    - ***Find attachments with multiple extensions (Buscar adjuntos con varias extensiones).***
97. Desmarque ***Detect unwanted programs*** (Detectar programas no deseados) en ***Unwanted programs detection*** (Detección de programas no deseados).
98. Seleccione ***Disabled*** (Desactivado) en ***Artemis (Heuristic network check for suspicious files)*** (Artemis [Comprobación de red heurística para archivos sospechosos]).
99. Desmarque ***Enable on-delivery email scanning*** (Activar escaneo de correo electrónico al llegar) en ***Scanning of email*** (Escaneo de correo electrónico).
100. Haga clic en ***Save*** (Guardar). Aparece la pantalla ***Assigned Policies*** (Directivas asignadas).
101. Haga clic en ***My Default*** (Mi configuración predeterminada) para ***General Options Policies*** (Directivas de opciones generales). Aparece la pantalla ***VirusScan Enterprise 8.8.0 > General Options Policies > My Default*** (VirusScan Enterprise 8.8.0 > Directivas de opciones generales > Mi configuración predeterminada).
102. Seleccione ***Workstation*** (Estación de trabajo) en la lista desplegable ***Settings for*** (Configuración de).

103. Haga clic en la pestaña ***Display Options*** (Opciones de pantalla). Aparece la pantalla ***Display Options*** (Opciones de pantalla).

104. Seleccione las siguientes opciones en ***Console options*** (Opciones de la consola):

    - ***Display managed tasks in the client console (Mostrar las tareas administradas en la consola del cliente).***
    - ***Disable default AutoUpdate task schedule (Desactivar el programa predeterminado de las tareas de actualización automática).***

105. Seleccione ***Server*** (Servidor) en la lista desplegable ***Settings for*** (Configuración de).

106. Haga clic en la pestaña ***Display Options*** (Opciones de pantalla). Aparece la pantalla ***Display Options*** (Opciones de pantalla).

107. Seleccione las siguientes opciones en ***Console options*** (Opciones de la consola):

    - ***Display managed tasks in the client console (Mostrar las tareas administradas en la consola del cliente).***
    - ***Disable default AutoUpdate task schedule (Desactivar el programa predeterminado de las tareas de actualización automática).***

108. Haga clic en ***Save*** (Guardar). Aparece la pantalla ***Assigned Policies*** (Directivas asignadas).

109. Haga clic en ***My Default*** (Mi configuración predeterminada) para ***Alert Policies*** (Directivas de alertas). Aparece la pantalla ***VirusScan Enterprise 8.8.0 > Alter Policies > My Default*** (VirusScan Enterprise 8.8.0 > Directivas de alertas > Mi configuración predeterminada).

110. Seleccione ***Workstation*** (Estación de trabajo) en la lista desplegable ***Settings for*** (Configuración de).

111. Seleccione la pestaña ***Alert Manager Alerts*** (Alertas del administrador de alertas). Aparece la pantalla ***Alert Manager Alerts*** (Alertas del administrador de alertas).

112. Desmarque ***On-Access Scan*** (Escaneo al abrir), ***On-Demand Scan and scheduled scans*** (Escaneos a demanda y con horario), ***Email Scan*** (Escaneo de correo electrónico) y ***AutoUpdate*** (Actualización automática) en ***Components that generate alerts*** (Componentes que generan alertas).

113. Seleccione ***Disable alerting*** (Desactivar alertas) en las opciones ***Alert Manager*** (Administrador de alertas).

114. Desmarque ***Access Protection*** (Protección de acceso) en ***Components that generate alerts*** (Componentes que generan alertas).

115. Haga clic en ***Additional Alerting Options*** (Otras opciones de alerta). Aparece la pantalla ***Additional Alerting Options*** (Otras opciones de alerta).

116. En el menú desplegable ***Severity Filters*** (Filtros de gravedad), seleccione ***Suppress all alerts (severities 0 to 4)*** (Suprimir todas las alertas [gravedad 0 a 4]).

117. Seleccione ***Server*** (Servidor) en la lista desplegable ***Settings for*** (Configuración de) y seleccione la pestaña ***Alert Manager Alerts*** (Alertas del administrador de alertas). Aparece la pantalla ***Alert Manager Alerts*** (Alertas del administrador de alertas).

118. Desmarque ***On-Access Scan*** (Escaneo al abrir), ***On-Demand Scan and scheduled scans*** (Escaneos a demanda y con horario), ***Email Scan*** (Escaneo de correo electrónico) y ***AutoUpdate*** (Actualización automática) en ***Components that generate alerts*** (Componentes que generan alertas).

119. Marque ***Disable alerting*** (Desactivar alertas) en las opciones ***Alert Manager*** (Administrador de alertas).

120. Desmarque ***Access Protection*** (Protección de acceso) en ***Components that generate alerts*** (Componentes que generan alertas).

121. Haga clic en ***Additional Alerting Options*** (Otras opciones de alerta). Aparece la pantalla Additional Alerting Options (Otras opciones de alerta).

122. En el menú desplegable ***Severity Filters*** (Filtros de gravedad), seleccione ***Suppress all alerts (severities 0 to 4)*** (Suprimir todas las alertas [gravedad 0 a 4]).

123. Haga clic en ***Save*** (Guardar). Aparece la pantalla ***Assigned Policies*** (Directivas asignadas).

124. Haga clic en ***My Default*** (Mi configuración predeterminada) para ***Access Protection Policies*** (Directivas de protección de acceso). Aparece la pantalla ***VirusScan Enterprise 8.8.0 > Access Protection Policies > My Default*** (VirusScan Enterprise 8.8.0 > Directivas de protección de acceso > Mi configuración predeterminada).

125. Seleccione ***Workstation*** (Estación de trabajo) en la lista desplegable ***Settings for*** (Configuración de).

126. Haga clic en la ficha ***Access Protection*** (Protección de acceso). Aparece la pantalla ***Access Protection*** (Protección de acceso).

127. Desmarque las siguientes opciones en ***Access protection settings*** (Configuración de protección de acceso):

    - ***Enable access protection (Activar protección de acceso).***
    - ***Prevent McAfee services from being stopped (Evitar que los servicios de McAfee se detengan).***
    - ***Enable Enhanced Self-Protection. (Activar protección automática mejorada.)***

128. Seleccione ***Server*** (Servidor) en la lista desplegable ***Settings for*** (Configuración de).

129. Haga clic en la ficha ***Access Protection*** (Protección de acceso). Aparece la pantalla ***Access Protection*** (Protección de acceso).

130. Desmarque las siguientes opciones en ***Access protection settings*** (Configuración de protección de acceso):

    - ***Enable access protection (Activar protección de acceso).***
    - ***Prevent McAfee services from being stopped (Evitar que los servicios de McAfee se detengan).***
    - ***Enable Enhanced Self-Protection. (Activar protección automática mejorada.)***

131. Haga clic en ***Save*** (Guardar). Aparece la pantalla ***Assigned Policies*** (Directivas asignadas).

132. Seleccione ***My Default*** (Mi configuración predeterminada) para ***Buffer Overflow Protection Policies*** (Directivas de protección de desbordamiento de memoria intermedia). Aparece la pantalla ***VirusScan Enterprise 8.8.0 > Buffer Overflow Protection Policies > My Default*** (VirusScan Enterprise 8.8.0 > Directivas de protección de desbordamiento de memoria intermedia > Mi configuración predeterminada).

133. Seleccione ***Workstation*** (Estación de trabajo) en la lista desplegable ***Settings for*** (Configuración de).

134. Haga clic en la pestaña ***Buffer Overflow Protection*** (Protección de desbordamiento de memoria intermedia). Aparece la ventana ***Buffer Overflow Protection*** (Protección de desbordamiento de memoria intermedia).

135. Desmarque ***Show the message dialog box when a buffer overflow is detected*** (Mostrar el cuadro de diálogo de mensajes cuando se detecte un desbordamiento de memoria intermedia) y haga clic en ***Client system warning*** (Advertencia del sistema del cliente).

136. Desmarque ***Enable buffer overflow protection*** (Activar protección de desbordamiento de memoria intermedia) en ***Buffer overflow settings*** (Configuración del desbordamiento de memoria intermedia).

137. Seleccione ***Server*** (Servidor) en la lista desplegable ***Settings for*** (Configuración de).

138. Haga clic en la pestaña ***Buffer Overflow Protection*** (Protección de desbordamiento de memoria intermedia). Aparece la ventana ***Buffer Overflow Protection*** (Protección de desbordamiento de memoria intermedia).

139. Desmarque ***Show the message dialog box when a buffer overflow is detected*** (Mostrar el cuadro de diálogo de mensajes cuando se detecte un desbordamiento de memoria intermedia) y haga clic en ***Client system warning*** (Advertencia del sistema del cliente).

140. Desmarque ***Enable buffer overflow protection*** (Activar protección de desbordamiento de memoria intermedia) en ***Buffer overflow settings*** (Configuración del desbordamiento de memoria intermedia).

141. Haga clic en ***Save*** (Guardar). Aparece la pantalla ***Assigned Policies*** (Directivas asignadas).

142. En el menú desplegable ***Product*** (Producto), seleccione ***McAfee Agent***. Aparece la ventana ***Policies*** (Directivas) de McAfee Agent.

143. Haga clic en ***My Default*** (Mi configuración predeterminada) para ***Repository*** (Repositorio). Aparece la pantalla ***McAfee Agent > Repository > My Default*** (McAfee Agent > Repositorio > Mi configuración predeterminada).

144. Haga clic en la pestaña ***Proxy***. Aparece la pantalla ***Proxy***.

145. Asegúrese de que ***Use Internet Explorer settings (For Windows)/System Preferences settings (For Mac OSX)*** (Usar ajustes de Internet Explorer [para Windows]/Configuración de preferencias del sistema [para Mac OSX]) está seleccionada en ***Proxy settings*** (Configuración de proxy).

146. Haga clic en ***Save*** (Guardar). Aparece la pantalla ***Assigned Policies*** (Directivas asignadas).

147. Haga clic en la pestaña ***Systems*** (Sistemas).

148. Seleccione todos los sistemas del cliente (adquisición, revisión y Centricity Cardiology INW server) en los que se vayan a implantar las directivas configuradas.

149. Seleccione ***Wake Up Agents*** (Despertar agentes). Aparece la pantalla ***Wake Up Agent*** (Despertar agente).

150. Haga clic en ***OK*** (Aceptar).

151. Termine la sesión en ePolicy Orchestrator.

Pautas posteriores a la instalación de McAfee ePolicy Orchestrator

Active la conexión de bucle invertido. Para obtener más información, consulte Activar la conexión de bucle invertido en la página 6.

Trend Micro OfficeScan Client/Server Edition 10.6 SP2

Descripción de la instalación

Instale Trend Micro OfficeScan Client/Server Edition solo en un entorno de red de Mac-Lab/CardioLab. Trend Micro OfficeScan se debe instalar en el servidor de la consola de administración del antivirus e implementar en el servidor Centricity Cardiology INW y en las estaciones de trabajo de adquisición y revisión como clientes. Utilice las siguientes instrucciones para instalar ***Trend Micro OfficeScan Client/Server Edition***.

Las actualizaciones de virus son responsabilidad de la institución. Actualice las definiciones con regularidad para asegurar que el sistema cuente con la protección antivirus más reciente.

Pautas previas a la instalación

1. Se espera que la consola de administración del antivirus Trend Micro se instale de acuerdo con las instrucciones de Trend Micro y que funcione de manera correcta.
2. Durante la instalación de Trend Micro OfficeScan lleve a cabo los siguientes pasos en el servidor de la consola de administración del antivirus:
    a. Desmarque ***Enable firewall*** (Activar firewall) en la ventana ***Anti-virus Feature*** (Función de antivirus).
    b. Seleccione ***No, Please do not enable assessment mode*** (No activar el modo de evaluación) en la ventana ***Anti-spyware Feature*** (Función de antispyware).
    c. Desmarque ***Enable web reputation policy*** (Activar directiva de reputación web) en la ventana ***Web Reputation Feature*** (Función de reputación web).
3. No se recomienda Trend Micro OfficeScan cuando se utiliza la función ***CO_2*** con PDM en sistemas Mac-Lab/CardioLab.
4. Si se requiere Trend Micro OfficeScan:
    a. Se recomienda configurar un servidor de la consola de administración del antivirus Trend Micro para los sistemas Mac-Lab/CardioLab. Es necesario realizar un cambio global en la configuración del antivirus para utilizar la función de ***CO_2*** con PDM en sistemas Mac-Lab/CardioLab.
    b. Si no se puede configurar un servidor de la consola de administración del antivirus de Trend Micro, será necesario un cambio en la configuración global del servidor de la consola de administración del antivirus Trend Micro después de la instalación. Este cambio afectará a todos los sistemas del cliente conectados al servidor de la consola de administración del antivirus Trend Micro y se debe consultar con el personal de TI antes de continuar.

5. Inicie sesión como **Administrator** (Administrador) o como miembro de ese grupo en todos los sistemas del cliente (adquisición, revisión y INW Server) para instalar el software antivirus.
6. Desactive la conexión de bucle invertido. Para obtener más información, consulte Desactivar la conexión de bucle invertido en la página 6.
7. Configure el servicio del Explorador de equipos. Para obtener más información, consulte Configurar el servicio de Explorador de equipos antes de instalar el antivirus en la página 7.

Trend Micro OfficeScan: pasos para la implementación de una nueva instalación (método preferido de instalación forzada)

1. Haga clic en ***Start > All Programs > TrendMicro OfficeScan server - <server name> > Office Scan Web Console*** (Inicio > Todos los programas > servidor de TrendMicro OfficeScan - <nombre de servidor> > Consola de Office Scan Web).

NOTA: Para seguir, seleccione ***Continue to this website (not recommended)*** (Continuar en este sitio web [no recomendado]). En la ventana Security Alert (Alerta de seguridad), active ***In the future, do not show this warning*** (No mostrar esta advertencia en el futuro) y haga clic en ***OK*** (Aceptar).

2. Si recibe un error de certificado que indique que el sitio no es de confianza, gestione sus certificados para incluir Trend Micro OfficeScan.
3. Si se le solicita, instale los complementos ***AtxEnc***. Aparece una pantalla de Security Warning (Advertencia de seguridad).
4. Haga clic en ***Install*** (Instalar).
5. Introduzca el nombre de usuario y contraseña, y haga clic en ***Log On*** (Iniciar sesión).
6. Si se le solicita, haga clic en ***Update Now*** (Actualizar ahora) para instalar nuevos widgets. Espere a que se actualicen los nuevos widgets. Aparecerá una pantalla para indicar que la actualización se ha completado.
7. Haga clic en ***OK*** (Aceptar).
8. En la barra de menú del lado izquierdo, haga clic en ***Networked Computers > Client Installation > Remote*** (Equipos en red > Instalación del cliente > Remota).
9. Si se le solicita, instale los complementos ***AtxConsole***. Aparece una pantalla de Security Warning (Advertencia de seguridad).
10. Haga clic en ***Install*** (Instalar).
11. Haga doble clic en ***My Company*** (Mi compañía) en la ventana de ***Remote installation*** (Instalación remota). Todos los dominios se mostrarán en ***My Company*** (Mi compañía).
12. Expanda el dominio de la lista (por ejemplo: INW). Todos los sistemas conectados al dominio aparecerán.
13. Si hay dominios o sistemas que no aparecen en la ventana ***Domains and Computers*** (Dominios y equipos), realice lo siguiente en cada uno de los sistemas del cliente (adquisición, revisión y INW Server):
    a. Inicie sesión como Administrator (Administrador) o como miembro de ese grupo en todos los equipos cliente.

b. Haga clic en ***Start > Run*** (Inicio > Ejecutar).

c. Escriba ***<Anti-Virus Management Console_server_IP_address>*** y pulse ***Enter*** (Intro). Cuando se le solicite, introduzca el nombre de usuario del administrador y la contraseña.

d. Vaya a ***<Anti-Virus Management Console_server_IP _address>\ofsscan*** y haga doble clic en ***AutoPcc.exe***. Cuando se le solicite, introduzca el nombre de usuario del administrador y la contraseña.

e. Reinicie los sistemas del cliente cuando se complete la instalación.

f. Inicie sesión como **Administrator** (Administrador) o como miembro de ese grupo en todos los equipos cliente y espere a que el icono de Trend Micro OfficeScan de la bandeja del sistema cambie a azul.

g. Omita los pasos restantes de este procedimiento y vaya al procedimiento de configuración de la consola del servidor de Trend Micro OfficeScan.

14. Seleccione los equipos cliente (adquisición, revisión y INW Server) y haga clic en ***Add*** (Agregar).
15. Introduzca el <nombre de dominio>/nombre de usuario y contraseña, y haga clic en ***Log On*** (Iniciar sesión).
16. Seleccione los equipos cliente (adquisición, revisión y INW Server) de uno en uno del panel ***Selected Computers*** (Equipos seleccionados) y haga clic en ***Install*** (Instalar).
17. Haga clic en ***Yes*** (Sí) en la casilla de confirmación.
18. Haga clic en ***OK*** (Aceptar) en el cuadro de mensaje ***Number of clients to which notifications were sent*** (Número de clientes a los que se han enviado notificaciones).
19. Reinicie todos los equipos cliente (adquisición, revisión y INW Server) como administrador o como miembro de ese grupo y espere a que el icono de Trend Micro OfficeScan de la bandeja del sistema cambie a azul y tenga un símbolo de confirmación de color verde.
20. Haga clic en ***Log off*** (Cerrar sesión) para salir de la ***consola de OfficeScan Web***.

Configuración de la consola del servidor de Trend Micro OfficeScan

1. Seleccione ***Start > All Programs > TrendMicro Office Scan server <servername> > Office Scan Web Console*** (Inicio > Todos los programas > servidor de TrendMicro Office Scan <nombre del servidor> > Consola de Office Scan Web). Aparece la pantalla ***Trend Micro OfficeScan Login*** (Inicio de sesión de Trend Micro OfficeScan).
2. Introduzca el nombre de usuario y la contraseña, y haga clic en ***Login*** (Iniciar sesión). Aparece la pantalla ***Summary*** (Resumen).
3. En el panel izquierdo, seleccione el enlace ***Networked Computers > Client Management*** (Equipos en red > Administración del cliente).
4. En el lado derecho, seleccione ***OfficeScan Server*** (Servidor de OfficeScan).
5. En las opciones ***Settings*** (Configuración), seleccione ***Scan Settings > Manual Scan Settings*** (Configuración de escaneo > Configuración de escaneo manual). Aparece la pantalla ***Manual Scan Settings*** (Configuración de escaneo manual).

6. Haga clic en la pestaña ***Target*** (Objetivo) y seleccione solo las siguientes opciones y desmarque el resto de opciones:
   - ***Files to Scan > File types scanned by IntelliScan (Archivos que se van a escanear > Tipos de archivos escaneados mediante IntelliScan).***
   - ***Scan Settings > Scan compressed files (Configuración de escaneo > Escanear archivos comprimidos).***
   - ***Scan Settings > Scan OLE objects (Configuración de escaneo > Escanear objetos OLE).***
   - ***Virus/Malware Scan Settings Only > Scan boot area (Solo configuración de escaneo de virus/malware > Escanear área de reinicio).***
   - ***CPU Usage > Low (Uso de CPU > Bajo).***
   - ***Scan Exclusion > Enable scan exclusion (Exclusión de escaneo > Activar exclusión de escaneo).***
   - ***Scan Exclusion > Apply scan exclusion settings to all scan types (Exclusión de escaneo > Aplicar configuración de exclusión de escaneo a todos los tipos de escaneo).***
   - ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed (Lista de exclusiones de escaneo [directorios] > Excluir directorios en los que estén instalados productos de Trend MicroScan) y seleccione Add path to client Computer Exlusion list (Agregar ruta a la lista de exclusión de equipos del cliente).***
   - Introduzca las carpetas **C:\Program Files (x86)\GE Healthcare\MLCL**, **C:\Program Files\GE Healthcare\MLCL\, D:\GEData\Studies**, **E:** y **G:** una por una. A continuación, haga clic en ***Add*** (Agregar).
7. Haga clic en ***Apply to All Clients*** (Aplicar a todos los clientes).
8. Haga clic en ***OK*** (Aceptar) en el mensaje ***The exclusion list on this screen will replace the exclusion list on the clients or domains you selected in the client tree earlier. Do you want to proceed?*** (La lista de exclusión en esta pantalla sustituirá a la lista de exclusión en los clientes o dominios que ha seleccionado en el árbol del cliente anterior. ¿Desea continuar?).
9. Haga clic en ***Close*** (Cerrar) para salir de la pantalla ***Manual Scan Settings*** (Configuración de escaneo manual).
10. En el panel izquierdo, seleccione el enlace ***Networked Computers > Client Management*** (Equipos en red > Administración del cliente).
11. En el lado derecho, seleccione ***OfficeScan Server*** (Servidor de OfficeScan).
12. En las opciones ***Settings*** (Configuración), seleccione ***Scan Settings > Real time Scan Settings*** (Configuración de escaneo > Configuración de escaneo en tiempo real). Aparece la pantalla ***Real-time Scan Settings*** (Configuración de escaneo en tiempo real).
13. Haga clic en la pestaña ***Target*** (Objetivo) y seleccione solo las siguientes opciones y desmarque el resto de opciones:
   - ***Real-Time Scan Settings > Enable Virus/Malware scan (Configuración de escaneo en tiempo real > Activar escaneo de virus/malware).***
   - ***Real-Time Scan Settings > Enable spyware/grayware scan (Configuración de escaneo en tiempo real > Activar escaneo de spyware/grayware).***
   - ***Files to Scan > File types scanned by IntelliScan (Archivos que se van a escanear > Tipos de archivos escaneados mediante IntelliScan).***

- ***Scan Settings > Scan compressed files (Configuración de escaneo > Escanear archivos comprimidos).***
- ***Scan Settings > Scan OLE objects (Configuración de escaneo > Escanear objetos OLE).***
- ***Virus/Malware Scan Settings Only > Enable IntelliTrap (Sólo configuración de escaneo de virus/malware > Activar IntelliTrap).***
- ***Scan Exclusion > Enable scan exclusion (Exclusión de escaneo > Activar exclusión de escaneo).***
- ***Scan Exclusion > Apply scan exclusion settings to all scan types (Exclusión de escaneo > Aplicar configuración de exclusión de escaneo a todos los tipos de escaneo).***
- ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed (Lista de exclusiones de escaneo [directorios] > Excluir directorios en los que estén instalados productos de Trend Micro).***
- Asegúrese de que las rutas de carpeta ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL, D:\GEData\Studies***, ***E:*** y ***G:*** estén presentes en ***Exclusion List*** (Lista de exclusiones).

14. Haga clic en la pestaña ***Action*** (Acción).
15. Mantenga la configuración predeterminada y desmarque las siguientes opciones:
    - ***Virus/Malware > Display a notification message on the client computer when virus/malware is detected (Virus/Malware > Mostrar notificación en el equipo del cliente al detectar virus/malware).***
    - ***Spyware/Grayware > Display a notification message on the client computer when spyware/grayware is detected (Spyware/Grayware > Mostrar notificación en el equipo del cliente al detectar spyware/grayware).***
16. Haga clic en ***Apply to All Clients*** (Aplicar a todos los clientes).
17. Haga clic en ***Close*** (Cerrar) para salir de la pantalla ***Real-time Scan Settings*** (Configuración de escaneo en tiempo real).
18. En el panel izquierdo, seleccione el enlace ***Networked Computers > Client Management*** (Equipos en red > Administración del cliente).
19. En el lado derecho, seleccione ***OfficeScan Server*** (Servidor de OfficeScan).
20. En las opciones ***Settings*** (Configuración), seleccione ***Scan Settings > Scheduled Scan Settings*** (Configuración de escaneo > Configuración de escaneo programado). Aparece la pantalla ***Schedule Scan Settings*** (Configuración de escaneo programado).
21. Haga clic en la pestaña ***Target*** (Objetivo) y seleccione solo las siguientes opciones y desmarque el resto de opciones:
    - ***Scheduled Scan Settings > Enable virus/malware scan (Configuración de escaneo programado > Activar escaneo de virus/malware).***
    - ***Scheduled Scan Settings > Enable spyware/grayware scan (Configuración de escaneo programado > Activar escaneo de spyware/grayware).***
    - ***Schedule > Weekly, every Sunday, Start time (Programar > Semanal, cada domingo, Hora inicio): 00:00 hh:mm.***
    - ***Files to Scan > File types scanned by IntelliScan (Archivos que se van a escanear > Tipos de archivos escaneados mediante IntelliScan).***

- ***Scan Settings > Scan compressed files (Configuración de escaneo > Escanear archivos comprimidos).***
- ***Scan Settings > Scan OLE objects (Configuración de escaneo > Escanear objetos OLE).***
- ***Virus/Malware Scan Settings Only > Scan boot area (Solo configuración de escaneo de virus/malware > Escanear área de reinicio).***
- ***CPU Usage > Low (Uso de CPU > Bajo).***
- ***Scan Exclusion > Enable scan exclusion (Exclusión de escaneo > Activar exclusión de escaneo).***
- ***Scan Exclusion > Apply scan exclusion settings to all scan types (Exclusión de escaneo > Aplicar configuración de exclusión de escaneo a todos los tipos de escaneo).***
- ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed (Lista de exclusiones de escaneo [directorios] > Excluir directorios en los que estén instalados productos de Trend Micro).***
- Asegúrese de que las rutas de carpeta ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** y ***G:*** estén presentes en Exclusion List (Lista de exclusiones).

22. Haga clic en la pestaña ***Action*** (Acción).
23. Mantenga la configuración predeterminada y desmarque las siguientes opciones:
    - ***Virus/Malware > Display a notification message on the client computer when virus/malware is detected (Virus/Malware > Mostrar notificación en el equipo del cliente al detectar virus/malware).***
    - ***Spyware/Grayware > Display a notification message on the client computer when spyware/grayware is detected (Spyware/Grayware > Mostrar notificación en el equipo del cliente al detectar spyware/grayware).***
24. Haga clic en ***Apply to All Clients*** (Aplicar a todos los clientes).
25. Haga clic en ***Close*** (Cerrar) para salir de la página ***Scheduled Scan Settings*** (Configuración de escaneo programado).
26. En el panel izquierdo, seleccione el enlace ***Networked Computers > Client Management*** (Equipos en red > Administración del cliente).
27. En el lado derecho, seleccione ***OfficeScan Server*** (Servidor de OfficeScan).
28. En las opciones ***Settings*** (Configuración), seleccione ***Scan Settings > Scan Now Settings*** (Configuración de escaneo > Configuración actual de escaneo). Aparece la pantalla ***Scan Now Settings*** (Configuración actual de escaneo).
29. Haga clic en la pestaña ***Target*** (Objetivo) y seleccione solo las siguientes opciones y desmarque el resto de opciones:
    - ***Scan Now Settings > Enable virus/malware scan (Configuración actual de escaneo > Activar escaneo de virus/malware).***
    - ***Scan NowSettings > Enable spyware/grayware scan (Configuración actual de escaneo > Activar escaneo de spyware/grayware).***
    - ***Files to Scan > File types scanned by IntelliScan (Archivos que se van a escanear > Tipos de archivos escaneados mediante IntelliScan).***
    - ***Scan Settings > Scan compressed files (Configuración de escaneo > Escanear archivos comprimidos).***

- ***Scan Settings > Scan OLE objects (Configuración de escaneo > Escanear objetos OLE).***
- ***Virus/Malware Scan Settings Only > Scan boot area (Solo configuración de escaneo de virus/malware > Escanear área de reinicio).***
- ***CPU Usage > Low (Uso de CPU > Bajo).***
- ***Scan Exclusion > Enable scan exclusion (Exclusión de escaneo > Activar exclusión de escaneo).***
- ***Scan Exclusion > Apply scan exclusion settings to all scan types (Exclusión de escaneo > Aplicar configuración de exclusión de escaneo a todos los tipos de escaneo).***
- ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed (Lista de exclusiones de escaneo [directorios] > Excluir directorios en los que estén instalados productos de Trend Micro).***
- Asegúrese de las rutas ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** y ***G:***

30. Haga clic en ***Apply to All Clients*** (Aplicar a todos los clientes).
31. Haga clic en ***Close*** (Cerrar) para salir de la pantalla ***Manual Scan Settings*** (Configuración de escaneo manual).
32. En el panel izquierdo, seleccione el enlace ***Networked Computers > Client Management*** (Equipos en red > Administración del cliente).
33. En el lado derecho, seleccione ***OfficeScan Server*** (Servidor de OfficeScan).
34. En las opciones de ***Settings*** (Configuración), seleccione ***Web Reputation Settings*** (Configuración de reputación web). Aparece la pantalla ***Web Reputation Settings*** (Configuración de reputación web).
35. Haga clic en la pestaña ***External Clients*** (Clientes externos) y desmarque ***Enable Web reputation policy on the following operating systems*** (Activar directiva de reputación web en los siguientes sistemas operativos) si se seleccionó durante la instalación.
36. Haga clic en la pestaña ***Internal Clients*** (Clientes internos) y desactive ***Enable Web reputation policy on the following operating systems*** (Activar directiva de reputación web en los siguientes sistemas operativos) si se seleccionó durante la instalación.
37. Haga clic en ***Apply to All Clients*** (Aplicar a todos los clientes).
38. Haga clic en ***Close*** (Cerrar) para salir de la pantalla ***Web Reputation*** (Reputación web).
39. En el panel izquierdo, seleccione el enlace ***Networked Computers > Client Management*** (Equipos en red > Administración del cliente).
40. En el lado derecho, seleccione ***OfficeScan Server*** (Servidor de OfficeScan).
41. En las opciones de ***Settings*** (Configuración), seleccione ***Behavior Monitoring Settings*** (Configuración de la monitorización del comportamiento). Aparece la pantalla ***Behavior Monitoring Settings*** (Configuración de la monitorización del comportamiento).
42. Desmarque las opciones ***Enable Malware Behavior Blocking*** (Activar bloqueo del comportamiento del malware) y ***Enable Event Monitoring*** (Activar monitorización de sucesos).
43. Haga clic en ***Apply to All Clients*** (Aplicar a todos los clientes).

44. Haga clic en ***Close*** (Cerrar) para salir de la pantalla ***Behavior Monitoring*** (Monitorización del comportamiento).
45. En el panel izquierdo, seleccione el enlace ***Networked Computers > Client Management*** (Equipos en red > Administración del cliente).
46. En el lado derecho, seleccione ***OfficeScan Server*** (Servidor de OfficeScan).
47. En las opciones de ***Settings*** (Configuración), seleccione ***Device Control Settings*** (Configuración del control del dispositivo). Aparece la pantalla ***Device Control Settings*** (Configuración del control del dispositivo).
48. Haga clic en la pestaña ***External Clients*** (Clientes externos) y desmarque las siguientes opciones:
    - ***Notification > Display a notification message on the client computer when OfficeScan detects unauthorized device access (Notificación > Mostrar notificación en el equipo del cliente cuando OfficeScan detecte un acceso no autorizado al dispositivo).***
    - ***Block the AutoRun function on USB storage devices (Bloquear la función de ejecución automática en dispositivos de almacenamiento USB).***
    - ***Enable Device Control (Activar el control del dispositivo).***
49. Haga clic en la pestaña ***Internal Clients*** (Clientes internos) y desmarque las siguientes opciones:
    - ***Notification > Display a notification message on the client computer when OfficeScan detects unauthorized device access (Notificación > Mostrar notificación en el equipo del cliente cuando OfficeScan detecte un acceso no autorizado al dispositivo).***
    - ***Block the AutoRun function on USB storage devices (Bloquear la función de ejecución automática en dispositivos de almacenamiento USB).***
    - ***Enable Device Control (Activar el control del dispositivo).***
50. Haga clic en ***Apply to All Clients*** (Aplicar a todos los clientes).
51. Haga clic en ***Close*** (Cerrar) para salir de la pantalla ***Device Control Settings*** (Configuración del control del dispositivo).
52. En el panel izquierdo, seleccione el enlace ***Networked Computers > Client Management*** (Equipos en red > Administración del cliente).
53. En el lado derecho, seleccione ***OfficeScan Server*** (Servidor de OfficeScan).
54. En las opciones de ***Settings*** (Configuración), seleccione ***Privileges And Other Settings*** (Privilegios y otros ajustes).
55. Haga clic en la pestaña ***Privileges*** (Privilegios), seleccione solo las siguientes opciones y desmarque el resto:
    - ***Scan Privileges > Configure Manual Scan Settings (Privilegios de escaneo > Configuración de escaneo manual).***
    - ***Scan Privileges > Configure Real-time Scan Settings (Privilegios de escaneo > Configuración de escaneo en tiempo real).***
    - ***Scan Privileges > Configure Scheduled Scan Settings (Privilegios de escaneo > Configuración de escaneo programado).***

- ***Proxy Setting Privileges > Allow the client user to configure proxy settings (Privilegios de configuración de proxy > Permitir que el usuario del cliente configure los ajustes de proxy).***
- ***Uninstallation > Require a password for the user to uninstall the OfficeScan Client (Desinstalar > Solicitar una contraseña para que el usuario desinstale el cliente OfficeScan).*** Introduzca la contraseña adecuada y confírmela.
- ***Unloading > Require a password for the user to unload the OfficeScan client (Descargar > Solicitar una contraseña para que el usuario descargue el cliente OfficeScan).*** Introduzca la contraseña adecuada y confírmela.

56. Haga clic en la pestaña ***Other Settings*** (Otros ajustes).
57. Seleccione ***Client Security Settings > Normal*** (Configuración de seguridad del cliente > Normal) y desmarque las demás opciones.

NOTA: Es importante que desactive las siguientes opciones.

- ***Client Self-protection > Protect OfficeScan client services (Protección automática del cliente > Proteger servicios del cliente OfficeScan).***
- ***Client Self-protection > Protect files in the OfficeScan client installation folder (Protección automática del cliente > Proteger archivos de la carpeta de instalación del cliente OfficeScan).***
- ***Client Self-protection > Protect OfficeScan client registry keys. (Protección automática del cliente > Proteger claves de registro del cliente OfficeScan).***
- ***Client Self-protection > Protect OfficeScan client processes (Protección automática del cliente > Proteger procesos del cliente OfficeScan).***

58. Haga clic en ***Apply to All Clients*** (Aplicar a todos los clientes).
59. Haga clic en ***Close*** (Cerrar) para salir de la pantalla ***Privileges And Other Settings*** (Privilegios y otros ajustes).
60. En el panel izquierdo, seleccione el enlace ***Networked Computers > Client Management link*** (Equipos en red > Administración del clientes).
61. En el lado derecho, seleccione ***OfficeScan Server*** (Servidor de OfficeScan).
62. En las opciones de ***Settings*** (Configuración), seleccione ***Additional Service Settings*** (Configuración de servicio adicional).
63. Desmarque la opción ***Enable service on the following operating systems*** (Activar servicio en los siguientes sistemas operativos).
64. Haga clic en ***Apply to All Clients*** (Aplicar a todos los clientes).
65. Haga clic en ***Close*** (Cerrar) para salir de la pantalla ***Additional Service Settings*** (Configuración de servicio adicional).
66. En el panel izquierdo, seleccione ***Networked Computers > Global Client Settings*** (Equipos en red > Configuración general de clientes).
67. Seleccione únicamente las siguientes opciones y desmarque las demás:

- ***Scan Settings > Configure Scan settings for large compressed files (Configuración de escaneo > Configurar ajustes de escaneo para archivos grandes comprimidos).***

- ***Scan Settings > Do not scan files in the compressed file if the size exceeds 2 MB (Configuración de escaneo > No escanear archivos del archivo comprimido si su tamaño es superior a 2 MB).***
- ***Scan Settings > In a compressed file scan only the first 100 files (Configuración de escaneo > Escanear sólo los 100 primeros archivos de un archivo comprimido).***
- ***Scan Settings > Exclude the OfficeScan server database folder from Real-time Scan (Configuración de escaneo > Excluir la carpeta de la base de datos del servidor de OfficeScan del escaneo en tiempo real).***
- ***Scan Settings > Exclude Microsoft Exchange server folders and files from scans (Configuración de escaneo > Excluir las carpetas y archivos del servidor de Microsoft Exchange de los escaneos).***
- ***Reserved Disk Space > Reserve 60 MB of disk space for updates (Espacio de disco reservado > Reservar 60 MB de espacio del disco para actualizaciones).***
- ***Proxy Configuration > Automatically detect settings (Configuración de proxy > Detectar automáticamente los ajustes).***

NOTA: Es importante cancelar la selección de ***Alert Settings > Display a notification message if the client computer needs to restart to load a kernel driver*** (Configuración de alertas > Mostrar notificación si es necesario reiniciar el equipo del cliente para cargar un controlador de kernels).

68. Haga clic en ***Save*** (Guardar).
69. En el panel izquierdo, seleccione el enlace ***Updates > Networked Computers > Manual Updates*** (Actualizaciones > Equipos en red > Actualizaciones manuales).
70. Seleccione ***Manually select client*** (Seleccionar al cliente manualmente) y haga clic en ***Select*** (Seleccionar).
71. Haga clic en el nombre de dominio apropiado en ***OfficeScan Server*** (Servidor de OfficeScan).
72. Seleccione el sistema del cliente uno por uno y haga clic en ***Initiate Component Update*** (Iniciar actualización del componente).
73. Haga clic en ***OK*** (Aceptar) en el cuadro de mensaje.
74. Haga clic en ***Log off*** (Cerrar sesión) y cierre la consola de OfficeScan Web.

Pautas posteriores a la instalación de Trend Micro OfficeScan

1. Lleve a cabo los siguientes pasos para configurar Trend Micro en el sistema/sistemas de adquisición:
    a. Haga clic en ***Start > Control Panel > Network and Sharing Center*** (Inicio > Panel de control > Centro de redes y recursos compartidos).
    b. Haga clic en ***Change adapter settings*** (Cambiar configuración del adaptador).
    c. Haga clic con el botón derecho en ***Local Area Connection*** (Conexión de área local) y seleccione ***Properties*** (Propiedades).
    d. Seleccione ***Internet Protocol Version 4 (TCP/IPv4)*** (Versión del protocolo de Internet 4 [TCP/IPv4]) y haga clic en ***Properties*** (Propiedades).
    e. Anote la dirección IP _____.

f. Cierre todas las ventanas abiertas.

g. Haga clic en ***Start > Run*** (Inicio > Ejecutar) y escriba **regedit**.

h. Vaya a ***HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion***.

i. En el panel de la derecha, haga clic con el botón derecho en un espacio en blanco y seleccione ***New > String value*** (Valor de cadena).

j. Escriba **IP Template** (Plantilla de IP) por nombre y pulse **Enter** (Intro).

k. Haga doble clic en el registro de ***IP Template*** (Plantilla de IP).

l. En el campo de datos ***Value*** (Valor), introduzca la dirección IP de la conexión de área local registrada en el paso e.

m. Haga clic en ***OK*** (Aceptar).

n. Cierre el editor del registro.

2. Active la conexión de bucle invertido. Para obtener más información, consulte Activar la conexión de bucle invertido en la página 6.

3. Configure el servicio del Explorador de equipos. Para obtener más información, consulte Configurar el servicio del Explorador de equipos después de instalar el antivirus en la página 7.

Configuraciones de los ajustes globales de Trend Micro

NOTA: Las siguientes instrucciones solo se deben poner en práctica cuando se utilice la función de CO_2 con PDM en sistemas Mac-Lab/CardioLab. Antes de realizar los pasos descritos a continuación, asegúrese de haberlo consultado con el personal de TI.

1. En el servidor de la consola de administración del antivirus, vaya a la carpeta ***C:\Program Files (x86)\Trend Micro\OfficeScan\PCCSRV***.

2. Abra el archivo ***ofcscan.ini*** en un editor de texto.

3. En la sección ***Global Setting*** (Configuración global), ajuste el valor de la siguiente tecla a "**1**": [Global Setting] ([Configuración global]) ***RmvTmTDI=1***

4. Guarde y cierre el archivo ofcscan.ini.

5. Haga clic en ***Start > All Programs > TrendMicro OfficeScan server - <server name> > Office Scan Web Console*** (Inicio > Todos los programas > servidor de TrendMicro OfficeScan - <nombre de servidor> > Consola de Office Scan Web).

6. Introduzca el nombre de usuario y la contraseña, y haga clic en ***Log On*** (Iniciar sesión). Aparece la pantalla ***Summary*** (Resumen).

7. Haga clic en ***Networked Computers > Global Client Settings*** (Equipos en red > Configuración general de clientes).

8. Haga clic en ***Save*** (Guardar).

9. En el panel izquierdo, seleccione el enlace ***Updates > Networked Computers > Manual Update*** (Actualizaciones > Equipos en red > Actualización manual).

10. Seleccione ***Manually select clients*** (Seleccionar a los clientes manualmente) y haga clic en ***Select*** (Seleccionar).
11. Haga clic en el nombre de dominio apropiado en ***OfficeScan Server*** (Servidor de OfficeScan).
12. Seleccione el sistema del cliente uno por uno y haga clic en ***Initiate Component Update*** (Iniciar actualización del componente).
13. Haga clic en ***OK*** (Aceptar) en el cuadro de mensaje.
14. Haga lo siguiente en cada sistema de adquisición:
    a. Abra el editor del registro.
    b. Vaya a ***HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc***.
    c. Asegúrese de que el valor de registro ***RmvTmTDI*** esté establecido en "**1**".
    d. Vaya a ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services***.
    e. Elimine la clave de registro ***tmtdi*** si existe.
    f. Cierre el editor del registro.
    g. Reinicie los sistemas cliente.
    h. Inicie sesión en los sistemas del cliente como administrador o como miembro de ese grupo.
    i. En cada uno de los sistemas del cliente, abra el símbolo del sistema con privilegios de administrador e introduzca el comando "***sc query tmtdi***".
    j. Asegúrese de que aparece el mensaje ***The specified service does not exist as an installed service*** (El servicio especificado no existe como servicio instalado).
15. En el servidor de la consola de administración del antivirus, haga clic en ***Log off*** (Cerrar sesión) y cierre la consola de OfficeScan Web.

Trend Micro OfficeScan Client/Server Edition 11.0 SP1

Instale Trend Micro OfficeScan Client/Server Edition solo en un entorno de red de Mac-Lab/CardioLab. Trend Micro OfficeScan se debe instalar en el servidor de la consola de administración del antivirus e implementar en el servidor Centricity Cardiology INW y en las estaciones de trabajo de adquisición y revisión como clientes. Utilice las siguientes instrucciones para instalar ***Trend Micro OfficeScan Client/Server Edition 11.0 SP1***.

Las actualizaciones de virus son responsabilidad de la institución. Actualice las definiciones con regularidad para asegurar que el sistema cuente con la protección antivirus más reciente.

Pautas previas a la instalación

1. Se espera que la consola de administración del antivirus Trend Micro se instale de acuerdo con las instrucciones de Trend Micro y que funcione de manera correcta.
2. Durante la instalación de Trend Micro OfficeScan lleve a cabo los siguientes pasos en el servidor de la consola de administración del antivirus:

a. Desmarque ***Enable firewall*** (Activar firewall) en la ventana ***Anti-virus Feature*** (Función de antivirus).

b. Seleccione ***No, Please do not enable assessment mode*** (No activar el modo de evaluación) en la ventana ***Anti-spyware Feature*** (Función de antispyware).

c. Desmarque ***Enable web reputation policy*** (Activar directiva de reputación web) en la ventana ***Web Reputation Feature*** (Función de reputación web).

3. No se recomienda Trend Micro OfficeScan cuando se utiliza la función CO_2 con PDM en sistemas Mac-Lab/CardioLab.

4. Si se requiere Trend Micro OfficeScan:

   a. Se recomienda configurar un servidor de la consola de administración del antivirus Trend Micro para los sistemas Mac-Lab/CardioLab. Es necesario realizar un cambio global en la configuración del antivirus para utilizar la función de CO_2 con PDM en sistemas Mac-Lab/CardioLab.

   b. Si no se puede configurar un servidor de la consola de administración del antivirus de Trend Micro, será necesario un cambio en la configuración global del servidor de la consola de administración del antivirus Trend Micro después de la instalación. Este cambio afectará a todos los sistemas del cliente conectados al servidor de la consola de administración del antivirus Trend Micro y se debe consultar con el personal de TI antes de continuar.

5. Inicie sesión como **Administrator** (Administrador) o como miembro de ese grupo en todos los sistemas del cliente (adquisición, revisión y INW Server) para instalar el software antivirus.

6. Desactive la conexión de bucle invertido. Para obtener más información, consulte Desactivar la conexión de bucle invertido en la página 6.

7. Configure el servicio del Explorador de equipos. Para obtener más información, consulte Configurar el servicio de Explorador de equipos antes de instalar el antivirus en la página 7.

8. Los siguientes certificados raíz e intermedios son necesarios para la instalación en los equipos cliente de adquisición, revisión y INW:

   - AddTrustExternalCARoot.crt
   - COMODOCodeSigningCA2.crt
   - UTNAddTrustObject_CA.crt
   - UTN-USERFirst-Object.crt
   - UTN-USERFirst-Object_kmod.crt

9. Repita los siguientes pasos para instalar los cinco certificados raíz y de nivel intermedio tal y como aparecen en el paso 8.

   a. Vaya a ***C:\Program Files\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Trend Micro***.
   NOTA: En INW, vaya a C:\Program Files (x86)\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Trend Micro.

   b. Si la ruta de la carpeta mencionada anteriormente no está presente, obtenga manualmente los certificados raíz y de nivel intermedio necesarios para la instalación.

   c. Haga doble clic en ***AddTrustExternalCARoot.crt*** para instalarlo en los sistemas MLCL (adquisición, revisión y INW).

d. Abra el certificado y haga clic en ***Install Certificate*** (Instalar certificado).

e. Haga clic en ***Next*** (Siguiente) cuando aparezca el ***Certificate Import Wizard*** (Asistente para la importación de certificados).

f. En la ventana ***Certificate Store*** (Almacén de certificados), seleccione ***Place all certificates in the following store*** (Colocar todos los certificados en el siguiente almacén) y haga clic en ***Browse*** (Buscar).

g. Marque ***Show physical stores > Trusted Root Certification Authorities > Local Computer*** (Mostrar almacenes físicos > Entidades de certificación raíz de confianza > Equipo local) y, a continuación, haga clic en ***OK*** (Aceptar).

h. Haga clic en ***Next*** (Siguiente) en el ***Certificate Import Wizard*** (Asistente para importación de certificados).

i. Haga clic en ***Finish*** (Terminar). Debe aparecer el mensaje ***The import was successful*** (La importación se completó correctamente).

j. Repita el paso 9 para el resto de certificados que aparecen en el paso 8.

NOTA: Todos los certificados tienen una fecha de vencimiento. Una vez que el certificado haya expirado, se deben sustituir y actualizar en los sistemas MLCL para garantizar que el agente OfficeScan funciona como se espera.

Trend Micro OfficeScan: pasos para la implementación de una nueva instalación (método preferido de instalación forzada para 11.0.SP1)

1. Haga clic en ***Start > All Programs > TrendMicro OfficeScan server - <server name> > Office Scan Web Console*** (Inicio > Todos los programas > servidor de TrendMicro OfficeScan - <nombre de servidor> > Consola de Office Scan Web).

NOTA: Para seguir, seleccione ***Continue to this website (not recommended)*** (Continuar en este sitio web [no recomendado]). En la ventana Security Alert (Alerta de seguridad), active ***In the future, do not show this warning*** (No mostrar esta advertencia en el futuro) y haga clic en ***OK*** (Aceptar).

2. Si recibe un error de certificado que indique que el sitio no es de confianza, gestione sus certificados para incluir Trend Micro OfficeScan.

3. Si se le solicita, instale los complementos ***AtxEnc***. Aparece una pantalla de Security Warning (Advertencia de seguridad).

   a. Haga clic en ***Install*** (Instalar).

4. Introduzca el nombre de usuario y contraseña, y haga clic en ***Log On*** (Iniciar sesión).

5. Si se le solicita, haga clic en ***Update Now*** (Actualizar ahora) para instalar nuevos widgets. Espere a que se actualicen los nuevos widgets. Aparecerá una pantalla para indicar que la actualización se ha completado.

   a. Haga clic en ***OK*** (Aceptar).

6. En la barra de menús superior, haga clic en ***Agents > Agent Installation > Remote*** (Agentes > Instalación de agente > Remoto).

7. Si se le solicita, instale los complementos ***AtxConsole***. Aparece una pantalla de Security Warning (Advertencia de seguridad).

   a. Haga clic en ***Install*** (Instalar).

8. Haga doble clic en ***OfficeScan Server*** (Servidor de OfficeScan) en la ventana ***Remote Installation*** (Instalación remota). Todos los dominios se mostrarán en ***OfficeScan Server*** (Servidor de OfficeScan).

9. Haga doble clic en el dominio (por ejemplo: INW). Todos los sistemas conectados al dominio aparecerán.

NOTA: Si hay dominios o sistemas que no aparecen en la ventana ***Domains and Endpoints*** (Dominios y puntos de conexión), vaya a Solución de problemas sobre dominios o sistemas que no aparecen en la ventana de dominios y puntos de conexión en la página 80 para agregarlos de manera manual o ejecutar la instalación directamente desde el equipo cliente.

10. Seleccione los equipos cliente (adquisición, revisión y INW Server) y haga clic en ***Add*** (Agregar).

11. Introduzca el <nombre de dominio>/nombre de usuario y contraseña, y haga clic en ***Log On*** (Iniciar sesión).

12. Seleccione los equipos cliente (adquisición, revisión e INW Server) de uno en uno del panel ***Selected Endpoints*** (Extremos seleccionados) y haga clic en ***Install*** (Instalar).

13. Haga clic en ***OK*** (Aceptar) en la casilla de confirmación.

14. Haga clic en ***OK*** (Aceptar) en el cuadro de mensaje ***Number of clients to which notifications were sent*** (Número de clientes a los que se han enviado notificaciones).

15. Reinicie todos los equipos cliente (adquisición, revisión y INW Server) como administrador o como miembro de ese grupo y espere a que el icono de Trend Micro OfficeScan de la bandeja del sistema cambie a azul y tenga un símbolo de confirmación de color verde.

16. Haga clic en ***Log off*** (Cerrar sesión) para salir de la ***consola de OfficeScan Web***.

Configuración de la consola del servidor Trend Micro OfficeScan para 11.0 SP1

1. Seleccione ***Start > All Programs > TrendMicro Office Scan server <servername> > Office Scan Web Console*** (Inicio > Todos los programas > servidor de TrendMicro Office Scan <nombre del servidor> > Consola de Office Scan Web). Aparece la pantalla ***Trend Micro OfficeScan Login*** (Inicio de sesión de Trend Micro OfficeScan).

2. Introduzca el nombre de usuario y la contraseña, y haga clic en ***Login*** (Iniciar sesión). Aparece la pantalla ***Summary*** (Resumen).

3. En el panel superior, seleccione el enlace ***Agents > Agent Management*** (Agentes > Administración de agentes).

4. En el lado izquierdo, seleccione ***OfficeScan Server*** (Servidor de OfficeScan).

5. En las opciones ***Settings*** (Configuración), seleccione ***Scan Settings > Manual Scan Settings*** (Configuración de escaneo > Configuración de escaneo manual). Aparece la pantalla ***Manual Scan Settings*** (Configuración de escaneo manual).

6. Haga clic en la pestaña ***Target*** (Objetivo) y seleccione solo las siguientes opciones y desmarque el resto de opciones:
   - ***Files to Scan > File types scanned by IntelliScan (Archivos que se van a escanear > Tipos de archivos escaneados mediante IntelliScan).***
   - ***Scan Settings > Scan compressed files (Configuración de escaneo > Escanear archivos comprimidos).***
   - ***Scan Settings > Scan OLE objects (Configuración de escaneo > Escanear objetos OLE).***
   - ***Virus/Malware Scan Settings Only > Scan boot area (Solo configuración de escaneo de virus/malware > Escanear área de reinicio).***
   - ***CPU Usage > Low (Uso de CPU > Bajo).***
7. Haga clic en la pestaña Scan Exclusion (Exclusión de escaneo), seleccione solo las siguientes opciones y desmarque el resto:
   - ***Scan Exclusion > Enable scan exclusion (Exclusión de escaneo > Activar exclusión de escaneo).***
   - ***Scan Exclusion > Apply scan exclusion settings to all scan types (Exclusión de escaneo > Aplicar configuración de exclusión de escaneo a todos los tipos de escaneo).***
   - ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed (Lista de exclusiones de escaneo [directorios] > Excluir directorios en los que estén instalados productos de Trend Micro).***
   - Seleccione ***Adds path*** (Agregar la ruta) de la lista desplegable en ***Saving the officescan agent's exclusion list does the following:*** (Al guardar la lista de exclusiones del agente OfficeScan, sucede lo siguiente:).
   - Introduzca las carpetas **C:\Program Files (x86)\GE Healthcare\MLCL**, **C:\Program Files\GE Healthcare\MLCL\, D:\GEData\Studies**, **E:** y **G:** una por una. A continuación, haga clic en **+**.
8. Haga clic en ***Apply to All Clients*** (Aplicar a todos los clientes).
9. Haga clic en ***OK*** (Aceptar) en el mensaje ***The exclusion list on this screen will replace the exclusion list on the clients or domains you selected in the client tree earlier. Do you want to proceed?*** (La lista de exclusión en esta pantalla sustituirá a la lista de exclusión en los clientes o dominios que ha seleccionado en el árbol del cliente anterior. ¿Desea continuar?).
10. Haga clic en ***Close*** (Cerrar) para salir de la pantalla ***Manual Scan Settings*** (Configuración de escaneo manual).
11. En el panel superior, seleccione el enlace ***Agent > Agent Management*** (Agente > Administración de agentes).
12. En el lado izquierdo, seleccione ***OfficeScan Server*** (Servidor de OfficeScan).
13. En las opciones ***Settings*** (Configuración), seleccione ***Scan Settings > Real time Scan Settings*** (Configuración de escaneo > Configuración de escaneo en tiempo real). Aparece la pantalla ***Real-time Scan Settings*** (Configuración de escaneo en tiempo real).
14. Haga clic en la pestaña ***Target*** (Objetivo) y seleccione solo las siguientes opciones y desmarque el resto de opciones:
   - ***Real-Time Scan Settings > Enable Virus/Malware scan (Configuración de escaneo en tiempo real > Activar escaneo de virus/malware).***

- ***Real-Time Scan Settings > Enable spyware/grayware scan (Configuración de escaneo en tiempo real > Activar escaneo de spyware/grayware).***
- ***Files to Scan > File types scanned by IntelliScan (Archivos que se van a escanear > Tipos de archivos escaneados mediante IntelliScan).***
- ***Scan Settings > Scan compressed files (Configuración de escaneo > Escanear archivos comprimidos).***
- ***Scan Settings > Scan OLE objects (Configuración de escaneo > Escanear objetos OLE).***
- ***Virus/Malware Scan Settings Only > Enable IntelliTrap (Sólo configuración de escaneo de virus/malware > Activar IntelliTrap).***

15. Haga clic en la pestaña Scan Exclusion (Exclusión de escaneo), seleccione solo las siguientes opciones y desmarque el resto:
    - ***Scan Exclusion > Enable scan exclusion (Exclusión de escaneo > Activar exclusión de escaneo).***
    - ***Scan Exclusion > Apply scan exclusion settings to all scan types (Exclusión de escaneo > Aplicar configuración de exclusión de escaneo a todos los tipos de escaneo).***
    - ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed (Lista de exclusiones de escaneo [directorios] > Excluir directorios en los que estén instalados productos de Trend Micro).***
    - Asegúrese de que las rutas de carpeta ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL, D:\GEData\Studies***, ***E:*** y ***G:*** estén presentes en ***Exclusion List*** (Lista de exclusiones).
16. Haga clic en la pestaña ***Action*** (Acción).
17. Mantenga la configuración predeterminada y desmarque las siguientes opciones:
    - ***Virus/Malware > Display a notification message on endpoints when virus/malware is detected (Virus/Malware > Mostrar notificación en los puntos de conexión al detectar virus/malware).***
    - ***Spyware/Grayware > Display a notification message on endpoints when spyware/grayware is detected (Virus/Malware > Mostrar notificación en los puntos de conexión al detectar spyware/grayware).***
18. Haga clic en ***Apply to All Clients*** (Aplicar a todos los clientes).
19. Haga clic en ***Close*** (Cerrar) para salir de la pantalla ***Real-time Scan Settings*** (Configuración de escaneo en tiempo real).
20. En el panel superior, seleccione el enlace ***Agents > Agent Management*** (Agentes > Administración de agentes).
21. En el lado izquierdo, seleccione ***OfficeScan Server*** (Servidor de OfficeScan).
22. En las opciones ***Settings*** (Configuración), seleccione ***Scan Settings > Scheduled Scan Settings*** (Configuración de escaneo > Configuración de escaneo programado). Aparece la pantalla ***Schedule Scan Settings*** (Configuración de escaneo programado).
23. Haga clic en la pestaña ***Target*** (Objetivo) y seleccione solo las siguientes opciones y desmarque el resto de opciones:
    - ***Scheduled Scan Settings > Enable virus/malware scan (Configuración de escaneo programado > Activar escaneo de virus/malware).***

- ***Scheduled Scan Settings > Enable spyware/grayware scan (Configuración de escaneo programado > Activar escaneo de spyware/grayware).***
- ***Schedule > Weekly, every Sunday, Start time (Programar > Semanal, cada domingo, Hora inicio): 00:00 hh:mm.***
- ***Files to Scan > File types scanned by IntelliScan (Archivos que se van a escanear > Tipos de archivos escaneados mediante IntelliScan).***
- ***Scan Settings > Scan compressed files (Configuración de escaneo > Escanear archivos comprimidos).***
- ***Scan Settings > Scan OLE objects (Configuración de escaneo > Escanear objetos OLE).***
- ***Virus/Malware Scan Settings Only > Scan boot area (Solo configuración de escaneo de virus/malware > Escanear área de reinicio).***
- ***CPU Usage > Low (Uso de CPU > Bajo).***

24. Haga clic en la pestaña ***Scan Exclusion*** (Exclusión de escaneo), seleccione solo las siguientes opciones y desmarque el resto:
    - ***Scan Exclusion > Enable scan exclusion (Exclusión de escaneo > Activar exclusión de escaneo).***
    - ***Scan Exclusion > Apply scan exclusion settings to all scan types (Exclusión de escaneo > Aplicar configuración de exclusión de escaneo a todos los tipos de escaneo).***
    - ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed (Lista de exclusiones de escaneo [directorios] > Excluir directorios en los que estén instalados productos de Trend Micro).***
    - Asegúrese de que las rutas de carpeta ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** y ***G:*** estén presentes en Exclusion List (Lista de exclusiones).
25. Haga clic en la pestaña ***Action*** (Acción).
26. Mantenga la configuración predeterminada y desmarque las siguientes opciones:
    - ***Virus/Malware > Display a notification message on the endpoints when virus/malware is detected (Virus/Malware > Mostrar notificación en los puntos de conexión al detectar virus/malware).***
    - ***Spyware/Grayware > Display a notification message on the endpoints when spyware/grayware is detected (Virus/Malware > Mostrar notificación en los puntos de conexión al detectar spyware/grayware).***
27. Haga clic en ***Apply to All Clients*** (Aplicar a todos los clientes).
28. Haga clic en ***Close*** (Cerrar) para salir de la página ***Scheduled Scan Settings*** (Configuración de escaneo programado).
29. En el panel superior, seleccione el enlace ***Agents > Agent Management*** (Agentes > Administración de agentes).
30. En el lado izquierdo, seleccione ***OfficeScan Server*** (Servidor de OfficeScan).
31. En las opciones ***Settings*** (Configuración), seleccione ***Scan Settings > Scan Now Settings*** (Configuración de escaneo > Configuración actual de escaneo). Aparece la pantalla ***Scan Now Settings*** (Configuración actual de escaneo).
32. Haga clic en la pestaña ***Target*** (Objetivo) y seleccione solo las siguientes opciones y desmarque el resto de opciones:

- ***Scan Now Settings > Enable virus/malware scan (Configuración actual de escaneo > Activar escaneo de virus/malware).***
- ***Scan NowSettings > Enable spyware/grayware scan (Configuración actual de escaneo > Activar escaneo de spyware/grayware).***
- ***Files to Scan > File types scanned by IntelliScan (Archivos que se van a escanear > Tipos de archivos escaneados mediante IntelliScan).***
- ***Scan Settings > Scan compressed files (Configuración de escaneo > Escanear archivos comprimidos).***
- ***Scan Settings > Scan OLE objects (Configuración de escaneo > Escanear objetos OLE).***
- ***Virus/Malware Scan Settings Only > Scan boot area (Solo configuración de escaneo de virus/malware > Escanear área de reinicio).***
- ***CPU Usage > Low (Uso de CPU > Bajo).***

33. Haga clic en la pestaña ***Scan Exclusion*** (Exclusión de escaneo), seleccione solo las siguientes opciones y desmarque el resto:
    - ***Scan Exclusion > Enable scan exclusion (Exclusión de escaneo > Activar exclusión de escaneo).***
    - ***Scan Exclusion > Apply scan exclusion settings to all scan types (Exclusión de escaneo > Aplicar configuración de exclusión de escaneo a todos los tipos de escaneo).***
    - ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed (Lista de exclusiones de escaneo [directorios] > Excluir directorios en los que estén instalados productos de Trend Micro).***
    - Asegúrese de que las rutas de carpeta ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** y ***G:*** estén presentes en Exclusion List (Lista de exclusiones).
34. Haga clic en ***Apply to All Clients*** (Aplicar a todos los clientes).
35. Haga clic en ***Close*** (Cerrar) para salir de la pantalla ***Manual Scan Settings*** (Configuración de escaneo manual).
36. En el panel superior, seleccione el enlace ***Agents > Agent Management*** (Agentes > Administración de agentes).
37. En el lado izquierdo, seleccione ***OfficeScan Server*** (Servidor de OfficeScan).
38. En las opciones de ***Settings*** (Configuración), seleccione ***Web Reputation Settings*** (Configuración de reputación web). Aparece la pantalla ***Web Reputation Settings*** (Configuración de reputación web).
39. Haga clic en la pestaña ***External Agents*** (Agentes externos) y desmarque ***Enable Web reputation policy on the following operating systems*** (Activar directiva de reputación web en los siguientes sistemas operativos) si se seleccionó durante la instalación.
40. Haga clic en la pestaña ***Internal Agents*** (Agentes internos) y desmarque ***Enable Web reputation policy on the following operating systems*** (Activar directiva de reputación web en los siguientes sistemas operativos) si se seleccionó durante la instalación.
41. Haga clic en ***Apply to All Clients*** (Aplicar a todos los clientes).
42. Haga clic en ***Close*** (Cerrar) para salir de la pantalla ***Web Reputation*** (Reputación web).

43. En el panel superior, seleccione el enlace ***Agents > Agent Management*** (Agentes > Administración de agentes).
44. En el lado izquierdo, seleccione ***OfficeScan Server*** (Servidor de OfficeScan).
45. En las opciones de ***Settings*** (Configuración), seleccione ***Behavior Monitoring Settings*** (Configuración de la monitorización del comportamiento). Aparece la pantalla ***Behavior Monitoring Settings*** (Configuración de la monitorización del comportamiento).
46. Desmarque las opciones ***Enable Malware Behavior Blocking for known and potential threats*** (Activar bloqueo del comportamiento del malware para amenazas potenciales y conocidas) y ***Enable Event Monitoring*** (Activar monitorización de sucesos).
47. Haga clic en ***Apply to All Clients*** (Aplicar a todos los clientes).
48. Haga clic en ***Close*** (Cerrar) para salir de la pantalla ***Behavior Monitoring*** (Monitorización del comportamiento).
49. En el panel superior, seleccione el enlace ***Agents > Agent Management*** (Agentes > Administración de agentes).
50. En el lado izquierdo, seleccione ***OfficeScan Server*** (Servidor de OfficeScan).
51. En las opciones de ***Settings*** (Configuración), seleccione ***Device Control Settings*** (Configuración del control del dispositivo). Aparece la pantalla ***Device Control Settings*** (Configuración del control del dispositivo).
52. Haga clic en la pestaña ***External Agents*** (Agentes externos) y desmarque las siguientes opciones:
    - ***Notification > Display a notification message on endpoints when OfficeScan detects unauthorized device access (Notificación > Mostrar notificación en los terminales de conexión cuando OfficeScan detecte un acceso no autorizado al dispositivo).***
    - ***Block the AutoRun function on USB storage devices (Bloquear la función de ejecución automática en dispositivos de almacenamiento USB).***
53. Haga clic en la pestaña ***Internal Agents*** (Agentes internos) y desmarque las siguientes opciones:
    - ***Notification > Display a notification message on endpoints when OfficeScan detects unauthorized device access (Notificación > Mostrar notificación en los terminales de conexión cuando OfficeScan detecte un acceso no autorizado al dispositivo).***
    - ***Block the AutoRun function on USB storage devices (Bloquear la función de ejecución automática en dispositivos de almacenamiento USB).***
54. Haga clic en ***Apply to All Clients*** (Aplicar a todos los clientes).
55. Haga clic en ***Close*** (Cerrar) para salir de la pantalla ***Device Control Settings*** (Configuración del control del dispositivo).
56. En las opciones de ***Settings*** (Configuración), seleccione otra vez ***Device Control Settings*** (Configuración del control del dispositivo). Aparece la pantalla ***Device Control Settings*** (Configuración del control del dispositivo).
57. Haga clic en la pestaña ***External Agents*** (Agentes externos) y desmarque ***Enable Device Control*** (Activar el control del dispositivo).

58. Haga clic en la pestaña ***Internal Agents*** (Agentes internos) y desmarque ***Enable Device Control*** (Activar el control del dispositivo).

59. Haga clic en ***Apply to All Clients*** (Aplicar a todos los clientes).

60. Haga clic en ***Close*** (Cerrar) para salir de la pantalla ***Device Control Settings*** (Configuración del control del dispositivo).

61. En el panel superior, seleccione el enlace ***Agents > Agent Management*** (Agentes > Administración de agentes).

62. En el lado izquierdo, seleccione ***OfficeScan Server*** (Servidor de OfficeScan).

63. En las opciones de ***Settings*** (Configuración), seleccione ***Privileges And Other Settings*** (Privilegios y otros ajustes).

64. Haga clic en la pestaña ***Privileges*** (Privilegios), seleccione solo las siguientes opciones y desmarque el resto:

    - ***Scans > Configure Manual Scan Settings (Escaneos > Configuración de escaneo manual).***
    - ***Scans > Configure Real-time Scan Settings (Escaneos > Configuración de escaneo en tiempo real).***
    - ***Scans > Configure Scheduled Scan Settings (Escaneos > Configuración de escaneo programado).***
    - ***Proxy Settings > Allow users to configure proxy settings (Configuración de proxy > Permitir que los usuarios configuren los ajustes de proxy).***
    - ***Uninstallation > Requires a password (Desinstalar > Requiere una contraseña).*** Introduzca la contraseña adecuada y confírmela.
    - ***Unload and Unlock > Requires a password (Descargar y Desbloquear > Requiere una contraseña).*** Introduzca la contraseña adecuada y confírmela.

65. Haga clic en la pestaña ***Other Settings*** (Otros ajustes).

66. Seleccione ***OfficeScan Agent Security Settings > Normal:*** (Configuración de la seguridad del agente OfficeScan > Normal:). ***Allow users to access OfficeScan agent files and registries*** (Permitir que los usuarios accedan a los archivos y registros del agente OfficeScan) y desmarque el resto de opciones.

NOTA: Es importante que desactive las siguientes opciones.

- ***OfficeScan Agent Self-protection > Protect OfficeScan agent services (Protección automática del agente OfficeScan > Proteger los servicios del agente OfficeScan).***
- ***OfficeScan Agent Self-protection > Protect files in the OfficeScan agent installation folder (Protección automática del agente OfficeScan > Proteger archivos de la carpeta de instalación del agente OfficeScan).***
- ***OfficeScan Agent Self-protection > Protect OfficeScan agent registry keys (Protección automática del agente OfficeScan > Proteger claves de registro del agente OfficeScan).***
- ***OfficeScan Agent Self-protection > Protect OfficeScan agent processes (Protección automática del agente OfficeScan > Proteger los procesos del agente OfficeScan).***

67. Haga clic en ***Apply to All Clients*** (Aplicar a todos los clientes).

68. Haga clic en ***Close*** (Cerrar) para salir de la pantalla ***Privileges And Other Settings*** (Privilegios y otros ajustes).

69. En el panel superior, seleccione el enlace ***Agents > Agent Management*** (Agentes > Administración de agentes).

70. En el lado izquierdo, seleccione ***OfficeScan Server*** (Servidor de OfficeScan).

71. En las opciones de ***Settings*** (Configuración), seleccione ***Additional Service Settings*** (Configuración de servicio adicional).

72. Desmarque la opción ***Enable service on the following operating systems*** (Activar servicio en los siguientes sistemas operativos).

73. Haga clic en ***Apply to All Clients*** (Aplicar a todos los clientes).

74. Haga clic en ***Close*** (Cerrar) para salir de la pantalla ***Additional Service Settings*** (Configuración de servicio adicional).

75. En el panel superior, seleccione el enlace ***Agents > Global Agent Settings*** (Agente > Configuración general de agente).

76. Seleccione únicamente las siguientes opciones y desmarque las demás:

    - ***Scan Settings for Large Compressed Files > Configure Scan settings for large compressed files (Configuración de escaneo para grandes archivos comprimidos > Configurar ajustes de escaneo para grandes archivos comprimidos).***
    - ***Scan Settings for Large Compressed Files > Do not scan files in the compressed file if the size exceeds 2 MB*** (Configuración de escaneo para archivos comprimidos grandes > No escanear archivos del archivo comprimido si su tamaño es superior a 2 MB). Realice esto para poder utilizar ***Real-Time Scan*** (Escaneo en tiempo real) y ***Manual Scan/Schedule Scan/Scan Now*** (Escaneo manual/Programar Escaneo/ Escanear ahora).
    - ***Scan Settings for Large Compressed Files > In a compressed file scan only the first 100 files (Configuración de escaneo para archivos comprimidos grandes > Escanear solo los 100 primeros archivos de un archivo comprimido).*** Realice esto para poder utilizar ***Real-Time Scan*** (Escaneo en tiempo real) y ***Manual Scan/Schedule Scan/Scan Now*** (Escaneo manual/Programar Escaneo/Escanear ahora).
    - ***Scan Settings > Exclude the OfficeScan server database folder from Real-time Scan (Configuración de escaneo > Excluir la carpeta de la base de datos del servidor de OfficeScan del escaneo en tiempo real).***
    - ***Scan Settings > Exclude Microsoft Exchange server folders and files from scans (Configuración de escaneo > Excluir las carpetas y archivos del servidor de Microsoft Exchange de los escaneos).***
    - ***Reserved Disk Space > Reserve 60 MB of disk space for updates (Espacio de disco reservado > Reservar 60 MB de espacio del disco para actualizaciones).***
    - ***Proxy Configuration > Automatically detect settings (Configuración de proxy > Detectar automáticamente los ajustes).***

NOTA: Es importante cancelar la selección de ***Alert Settings > Display a notification message*** (Configuración de alertas > Mostrar notificación) si el punto de conexión debe reiniciarse para cargar un modo de controlador de kernels.

77. Haga clic en ***Save*** (Guardar).

78. En el panel superior, seleccione el enlace ***Updates > Agents > Manual Updates*** (Actualizaciones > Agentes > Actualizaciones Manuales).

79. Seleccione ***Manually select agents*** (Seleccionar a los agentes manualmente) y haga clic en ***Select*** (Seleccionar).

80. Haga doble clic en el nombre de dominio apropiado en ***OfficeScan Server*** (Servidor de OfficeScan).
81. Seleccione el sistema del cliente uno por uno y haga clic en ***Initiate Update*** (Iniciar actualización).
82. Haga clic en ***OK*** (Aceptar) en el cuadro de mensaje.
83. Haga clic en ***Log off*** (Cerrar sesión) y cierre la consola de OfficeScan Web.

Configuraciones de los ajustes globales de Trend Micro

NOTA: Las siguientes instrucciones solo se deben poner en práctica cuando se utilice la función de CO_2 con PDM en sistemas Mac-Lab/CardioLab. Antes de realizar los pasos descritos a continuación, asegúrese de haberlo consultado con el personal de TI.

1. En el servidor de la consola de administración del antivirus, vaya a la carpeta ***C:\Program Files (x86)\Trend Micro\OfficeScan\PCCSRV***.
2. Abra el archivo ***ofcscan.ini*** en un editor de texto.
3. En la sección Global Setting (Configuración global) , configure el valor de la siguiente clave a "**1**": [Global Setting] ([Configuración global]) ***RmvTmTDI=1***
4. Guarde y cierre el archivo ofcscan.ini.
5. Haga clic en ***Start > All Programs > TrendMicro OfficeScan server - <server name> > OfficeScan Web Console*** (Inicio > Todos los programas > servidor de TrendMicro OfficeScan - <nombre de servidor> > Consola de OfficeScan Web).
6. Introduzca el nombre de usuario y la contraseña, y haga clic en ***Log On*** (Iniciar sesión). Aparece la pantalla ***Dashboard*** (Panel).
7. Haga clic en ***Agents > Global Agent Settings*** (Agentes > Configuración general de agente).
8. Haga clic en ***Save*** (***Guardar).***
9. En el panel izquierdo, seleccione el enlace ***Updates > Agents > Manual Update*** (Actualizaciones > Agentes > Actualización manual).
10. Seleccione ***Manually select clients*** (Seleccionar a los clientes manualmente) y haga clic en ***Select*** (Seleccionar).
11. Haga clic en el nombre de dominio apropiado en ***OfficeScan Server*** (Servidor de OfficeScan).
12. Seleccione el sistema del cliente uno por uno y haga clic en ***Initiate Update*** (Iniciar actualización).
13. Haga clic en ***OK*** (Aceptar) en el cuadro de mensaje.
14. Haga lo siguiente en cada sistema de adquisición:
    a. Abra el editor del registro.
    b. Vaya a ***HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PCcillinNTCorp\CurrentVersion\Misc.***

c. Asegúrese de que el valor de registro ***RmvTmTDI*** se ha establecido en "***1***".

d. Vaya a ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services***.

e. Elimine la clave de registro ***tmtdi*** si existe.

f. Cierre el editor del registro.

g. Reinicie los sistemas cliente.

h. Inicie sesión en los sistemas del cliente como administrador o como miembro de ese grupo.

i. En cada uno de los sistemas del cliente, abra el símbolo del sistema con privilegios de administrador e introduzca el comando "***sc query tmtdi***".

j. Asegúrese de que aparece el mensaje ***The specified service does not exist as an installed service*** (El servicio especificado no existe como servicio instalado).

15. En el servidor de la consola de administración del antivirus, haga clic en ***Log off*** (Cerrar sesión) y cierre la consola de OfficeScan Web.

Pautas posteriores a la instalación de Trend Micro OfficeScan

1. Active la conexión de bucle invertido. Para obtener más información, consulte Activar la conexión de bucle invertido en la página 6.
2. Configure el servicio del Explorador de equipos. Para obtener más información, consulte Configurar el servicio del Explorador de equipos después de instalar el antivirus en la página 7.

Trend Micro OfficeScan Client/Server Edition XG 12.0

Descripción de la instalación

Instale Trend Micro OfficeScan Client/Server Edition solo en un entorno de red de Mac-Lab/CardioLab. Trend Micro OfficeScan se debe instalar en el servidor de la consola de administración del antivirus e implementar en el servidor Centricity Cardiology INW y en las estaciones de trabajo de adquisición y revisión como clientes. Utilice las siguientes instrucciones para instalar ***Trend Micro OfficeScan Client/Server Edition XG 12.0***.

Las actualizaciones de virus son responsabilidad de la institución. Actualice las definiciones con regularidad para asegurar que el sistema cuente con la protección antivirus más reciente.

Pautas previas a la instalación

NOTA: Internet Explorer 10 es el navegador IE mínimo necesario para ejecutar el gestor OfficeScan.

1. Se espera que la consola de administración del antivirus Trend Micro se instale de acuerdo con las instrucciones de Trend Micro y que funcione de manera correcta.
2. Durante la instalación de Trend Micro OfficeScan lleve a cabo los siguientes pasos en el servidor de la consola de administración del antivirus:

a. Desmarque ***Enable firewall*** (Activar firewall) en la ventana ***Anti-virus Feature*** (Función de antivirus).

b. Seleccione ***No, Please do not enable assessment mode*** (No activar el modo de evaluación) en la ventana ***Anti-spyware Feature*** (Función de antispyware).

c. Desmarque ***Enable web reputation policy*** (Activar directiva de reputación web) en la ventana ***Web Reputation Feature*** (Función de reputación web).

3. Inicie sesión como **Administrator** (Administrador) o como miembro de ese grupo en todos los sistemas del cliente (adquisición, revisión y INW Server) para instalar el software antivirus.

4. Desactive la conexión de bucle invertido. Para obtener más información, consulte Desactivar la conexión de bucle invertido en la página 6.

5. Configure el servicio del Explorador de equipos. Para obtener más información, consulte Configurar el servicio de Explorador de equipos antes de instalar el antivirus en la página 7.

6. Los siguientes certificados raíz e intermedios son necesarios para la instalación en los equipos cliente de adquisición, revisión y INW:

   - AddTrustExternalCARoot.crt
   - COMODOCodeSigningCA2.crt
   - UTNAddTrustObject_CA.crt
   - UTN-USERFirst-Object.crt
   - UTN-USERFirst-Object_kmod.crt

7. Repita los siguientes pasos para instalar los cinco certificados raíz y de nivel intermedio tal y como aparecen en el paso 6.

   a. Vaya a ***C:\Program Files\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Trend Micro***.
   NOTA: En INW, vaya a C:\Program Files (x86)\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Trend Micro.

   b. Si la ruta de la carpeta mencionada anteriormente no está presente, obtenga manualmente los certificados raíz y de nivel intermedio necesarios para la instalación.

   c. Haga doble clic en ***AddTrustExternalCARoot.crt*** para instalarlo en los sistemas MLCL (adquisición, revisión y INW).

   d. Abra el certificado y haga clic en ***Install Certificate*** (Instalar certificado).

   e. Haga clic en ***Next*** (Siguiente) cuando aparezca el ***Certificate Import Wizard*** (Asistente para la importación de certificados).

   f. En la ventana ***Certificate Store*** (Almacén de certificados), seleccione ***Place all certificates in the following store*** (Colocar todos los certificados en el siguiente almacén) y haga clic en ***Browse*** (Buscar).

   g. Marque ***Show physical stores > Trusted Root Certification Authorities > Local Computer*** (Mostrar almacenes físicos > Entidades de certificación raíz de confianza > Equipo local) y, a continuación, haga clic en ***OK*** (Aceptar).

   h. Haga clic en ***Next*** (Siguiente) en el ***Certificate Import Wizard*** (Asistente para importación de certificados).

i. Haga clic en ***Finish*** (Terminar). Debe aparecer el mensaje ***The import was successful*** (La importación se completó correctamente).

j. Repita el paso 7 para el resto de certificados que aparecen en el paso 6.

NOTA: Todos los certificados tienen una fecha de vencimiento. Una vez que el certificado haya expirado, se deben sustituir y actualizar en los sistemas MLCL para garantizar que el agente OfficeScan funciona como se espera.

Trend Micro OfficeScan: pasos para la implementación de una nueva instalación (método preferido de instalación forzada para 12.0)

1. Haga clic en ***Start > All Programs > TrendMicro OfficeScan server - <server name> > Office Scan Web Console*** (Inicio > Todos los programas > servidor de TrendMicro OfficeScan - <nombre de servidor> > Consola de Office Scan Web).

NOTA: Para seguir, seleccione ***Continue to this website (not recommended)*** (Continuar en este sitio web [no recomendado]). En la ventana Security Alert (Alerta de seguridad), active ***In the future, do not show this warning*** (No mostrar esta advertencia en el futuro) y haga clic en ***OK*** (Aceptar).

2. Si recibe un error de certificado que indique que el sitio no es de confianza, gestione sus certificados para incluir Trend Micro OfficeScan.

3. Si se le solicita, instale los complementos ***AtxEnc***. Aparece una pantalla de Security Warning (Advertencia de seguridad).

   a. Haga clic en ***Install*** (Instalar).

4. Introduzca el nombre de usuario y contraseña, y haga clic en ***Log On*** (Iniciar sesión).

5. Si se le solicita, haga clic en ***Update Now*** (Actualizar ahora) para instalar nuevos widgets. Espere a que se actualicen los nuevos widgets. Aparecerá una pantalla para indicar que la actualización se ha completado.

   a. Haga clic en ***OK*** (Aceptar).

6. En la barra de menús superior, haga clic en ***Agents > Agent Installation > Remote*** (Agentes > Instalación de agente > Remoto).

7. Si se le solicita, instale los complementos ***AtxConsole***. Aparece una pantalla de Security Warning (Advertencia de seguridad).

   a. Haga clic en ***Install*** (Instalar).

8. Haga doble clic en ***My Company*** (Mi compañía) en la ventana de ***Remote installation*** (Instalación remota). Todos los dominios se mostrarán en ***OfficeScan Server*** (Servidor de OfficeScan).

9. Haga doble clic en el dominio (por ejemplo: INW). Todos los sistemas conectados al dominio aparecerán.

NOTA: Si hay dominios o sistemas que no aparecen en la ventana ***Domains and Endpoints*** (Dominios y puntos de conexión), vaya a Solución de problemas sobre dominios o sistemas que no aparecen en la ventana de dominios y puntos de conexión en la página 80 para agregarlos de manera manual o ejecutar la instalación directamente desde el equipo cliente.

10. Seleccione los equipos cliente (adquisición, revisión y INW Server) y haga clic en ***Add*** (Agregar).
11. Introduzca el <nombre de dominio>/nombre de usuario y contraseña, y haga clic en ***Log On*** (Iniciar sesión).
12. Seleccione los equipos cliente (adquisición, revisión e INW Server) de uno en uno del panel ***Selected Endpoints*** (Extremos seleccionados) y haga clic en ***Install*** (Instalar).
13. Haga clic en ***Yes*** (Sí) en la casilla de confirmación.
14. Haga clic en ***OK*** (Aceptar) en el cuadro de mensaje ***Number of agents to which notifications were sent*** (Número de agentes a los que se han enviado notificaciones).
15. Reinicie todos los equipos cliente (adquisición, revisión y INW Server) como administrador o como miembro de ese grupo y espere a que el icono de Trend Micro OfficeScan de la bandeja del sistema cambie a azul y tenga un símbolo de confirmación de color verde.
16. Haga clic en ***Log off*** (Cerrar sesión) para salir de la ***consola de OfficeScan Web***.

Configuración de la consola del servidor de Trend Micro OfficeScan para 12.0

1. Seleccione ***Start > All Programs > TrendMicro Office Scan server <servername> > Office Scan Web Console*** (Inicio > Todos los programas > servidor de TrendMicro Office Scan <nombre del servidor> > Consola de Office Scan Web). Aparece la pantalla ***Trend Micro OfficeScan Login*** (Inicio de sesión de Trend Micro OfficeScan).
2. Introduzca el nombre de usuario y la contraseña, y haga clic en ***Login*** (Iniciar sesión). Aparece la pantalla ***Summary*** (Resumen).
3. En el panel superior, seleccione el enlace ***Agents > Agent Management*** (Agentes > Administración de agentes).
4. En el lado izquierdo, seleccione ***OfficeScan Server*** (Servidor de OfficeScan).
5. En las opciones ***Settings*** (Configuración), seleccione ***Scan Settings > Manual Scan Settings*** (Configuración de escaneo > Configuración de escaneo manual). Aparece la pantalla ***Manual Scan Settings*** (Configuración de escaneo manual).
6. Haga clic en la pestaña ***Target*** (Objetivo) y seleccione solo las siguientes opciones y desmarque el resto de opciones:
   - ***Files to Scan > File types scanned by IntelliScan (Archivos que se van a escanear > Tipos de archivos escaneados mediante IntelliScan).***
   - ***Scan Settings > Scan compressed files (Configuración de escaneo > Escanear archivos comprimidos).***
   - ***Scan Settings > Scan OLE objects (Configuración de escaneo > Escanear objetos OLE).***

- ***Virus/Malware Scan Settings Only > Scan boot area (Solo configuración de escaneo de virus/malware > Escanear área de reinicio).***
- ***CPU Usage > Low (Uso de CPU > Bajo).***

7. Haga clic en la pestaña Scan Exclusion (Exclusión de escaneo), seleccione solo las siguientes opciones y desmarque el resto:
   - ***Scan Exclusion > Enable scan exclusion (Exclusión de escaneo > Activar exclusión de escaneo).***
   - ***Scan Exclusion > Apply scan exclusion settings to all scan types (Exclusión de escaneo > Aplicar configuración de exclusión de escaneo a todos los tipos de escaneo).***
   - ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed (Lista de exclusiones de escaneo [directorios] > Excluir directorios en los que estén instalados productos de Trend MicroScan) y seleccione Add path to agent Computer Exlusion list (Agregar ruta a la lista de exclusión de equipos del agente).***
   - Seleccione ***Adds path*** (Agregar la ruta) de la lista desplegable en ***Saving the officescan agent's exclusion list does the following:*** (Al guardar la lista de exclusiones del agente OfficeScan, sucede lo siguiente:).
   - Introduzca las carpetas **C:\Program Files (x86)\GE Healthcare\MLCL**, **C:\Program Files\GE Healthcare\MLCL\, D:\GEData\Studies**, **E:** y **G:** una por una. A continuación, haga clic en ***Add*** (Agregar).
8. Haga clic en ***Apply to All Clients*** (Aplicar a todos los clientes).
9. Haga clic en ***OK*** (Aceptar) en el mensaje ***The exclusion list on this screen will replace the exclusion list on the agents or domains you selected in the client tree earlier. Do you want to proceed?*** (La lista de exclusión en esta pantalla sustituirá a la lista de exclusión en los clientes o dominios que ha seleccionado en el árbol del cliente anterior. ¿Desea continuar?).
10. Haga clic en ***Close*** (Cerrar) para salir de la pantalla ***Manual Scan Settings*** (Configuración de escaneo manual).
11. En el panel superior, seleccione el enlace ***Agent > Agent Management*** (Agente > Administración de agentes).
12. En el lado izquierdo, seleccione ***OfficeScan Server*** (Servidor de OfficeScan).
13. En las opciones ***Settings*** (Configuración), seleccione ***Scan Settings > Real time Scan Settings*** (Configuración de escaneo > Configuración de escaneo en tiempo real). Aparece la pantalla ***Real-time Scan Settings*** (Configuración de escaneo en tiempo real).
14. Haga clic en la pestaña ***Target*** (Objetivo) y seleccione solo las siguientes opciones y desmarque el resto de opciones:
    - ***Real-Time Scan Settings > Enable Virus/Malware scan (Configuración de escaneo en tiempo real > Activar escaneo de virus/malware).***
    - ***Real-Time Scan Settings > Enable spyware/grayware scan (Configuración de escaneo en tiempo real > Activar escaneo de spyware/grayware).***
    - ***Files to Scan > File types scanned by IntelliScan (Archivos que se van a escanear > Tipos de archivos escaneados mediante IntelliScan).***
    - ***Scan Settings > Scan compressed files (Configuración de escaneo > Escanear archivos comprimidos).***

- ***Scan Settings > Scan OLE objects (Configuración de escaneo > Escanear objetos OLE).***
- ***Virus/Malware Scan Settings Only > Enable IntelliTrap (Sólo configuración de escaneo de virus/malware > Activar IntelliTrap).***

15. Haga clic en la pestaña Scan Exclusion (Exclusión de escaneo), seleccione solo las siguientes opciones y desmarque el resto:
    - ***Scan Exclusion > Enable scan exclusion (Exclusión de escaneo > Activar exclusión de escaneo).***
    - ***Scan Exclusion > Apply scan exclusion settings to all scan types (Exclusión de escaneo > Aplicar configuración de exclusión de escaneo a todos los tipos de escaneo).***
    - ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed (Lista de exclusiones de escaneo [directorios] > Excluir directorios en los que estén instalados productos de Trend Micro).***
    - Asegúrese de que las rutas de carpeta ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL, D:\GEData\Studies***, ***E:*** y ***G:*** estén presentes en ***Exclusion List*** (Lista de exclusiones).
16. Haga clic en la pestaña ***Action*** (Acción).
17. Mantenga la configuración predeterminada y desmarque las siguientes opciones:
    - ***Virus/Malware > Display a notification message on endpoints when virus/malware is detected (Virus/Malware > Mostrar notificación en los puntos de conexión al detectar virus/malware).***
    - ***Spyware/Grayware > Display a notification message on endpoints when spyware/grayware is detected (Virus/Malware > Mostrar notificación en los puntos de conexión al detectar spyware/grayware).***
18. Haga clic en ***Apply to All Clients*** (Aplicar a todos los clientes).
19. Haga clic en ***Close*** (Cerrar) para salir de la pantalla ***Real-time Scan Settings*** (Configuración de escaneo en tiempo real).
20. En el panel superior, seleccione el enlace ***Agents > Agent Management*** (Agentes > Administración de agentes).
21. En el lado izquierdo, seleccione ***OfficeScan Server*** (Servidor de OfficeScan).
22. En las opciones ***Settings*** (Configuración), seleccione ***Scan Settings > Scheduled Scan Settings*** (Configuración de escaneo > Configuración de escaneo programado). Aparece la pantalla ***Schedule Scan Settings*** (Configuración de escaneo programado).
23. Haga clic en la pestaña ***Target*** (Objetivo) y seleccione solo las siguientes opciones y desmarque el resto de opciones:
    - ***Scheduled Scan Settings > Enable virus/malware scan (Configuración de escaneo programado > Activar escaneo de virus/malware).***
    - ***Scheduled Scan Settings > Enable spyware/grayware scan (Configuración de escaneo programado > Activar escaneo de spyware/grayware).***
    - ***Schedule > Weekly, every Sunday, Start time (Programar > Semanal, cada domingo, Hora inicio): 00:00 hh:mm.***
    - ***Files to Scan > File types scanned by IntelliScan (Archivos que se van a escanear > Tipos de archivos escaneados mediante IntelliScan).***

- ***Scan Settings > Scan compressed files (Configuración de escaneo > Escanear archivos comprimidos).***
- ***Scan Settings > Scan OLE objects (Configuración de escaneo > Escanear objetos OLE).***
- ***Virus/Malware Scan Settings Only > Scan boot area (Solo configuración de escaneo de virus/malware > Escanear área de reinicio).***
- ***CPU Usage > Low (Uso de CPU > Bajo).***

24. Haga clic en la pestaña Scan Exclusion (Exclusión de escaneo), seleccione solo las siguientes opciones y desmarque el resto:
    - ***Scan Exclusion > Enable scan exclusion (Exclusión de escaneo > Activar exclusión de escaneo).***
    - ***Scan Exclusion > Apply scan exclusion settings to all scan types (Exclusión de escaneo > Aplicar configuración de exclusión de escaneo a todos los tipos de escaneo).***
    - ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed (Lista de exclusiones de escaneo [directorios] > Excluir directorios en los que estén instalados productos de Trend Micro).***
    - Asegúrese de que las rutas de carpeta ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** y ***G:*** estén presentes en Exclusion List (Lista de exclusiones).
25. Haga clic en la pestaña ***Action*** (Acción).
26. Mantenga la configuración predeterminada y desmarque las siguientes opciones:
    - ***Virus/Malware > Display a notification message on the endpoints when virus/malware is detected (Virus/Malware > Mostrar notificación en los puntos de conexión al detectar virus/malware).***
    - ***Spyware/Grayware > Display a notification message on the endpoints when spyware/grayware is detected (Virus/Malware > Mostrar notificación en los puntos de conexión al detectar spyware/grayware).***
27. Haga clic en ***Apply to All Clients*** (Aplicar a todos los clientes).
28. Haga clic en ***Close*** (Cerrar) para salir de la página ***Scheduled Scan Settings*** (Configuración de escaneo programado).
29. En el panel superior, seleccione el enlace ***Agents > Agent Management*** (Agentes > Administración de agentes).
30. En el lado izquierdo, seleccione ***OfficeScan Server*** (Servidor de OfficeScan).
31. En las opciones ***Settings*** (Configuración), seleccione ***Scan Settings > Scan Now Settings*** (Configuración de escaneo > Configuración actual de escaneo). Aparece la pantalla ***Scan Now Settings*** (Configuración actual de escaneo).
32. Haga clic en la pestaña ***Target*** (Objetivo) y seleccione solo las siguientes opciones y desmarque el resto de opciones:
    - ***Scan Now Settings > Enable virus/malware scan (Configuración actual de escaneo > Activar escaneo de virus/malware).***
    - ***Scan NowSettings > Enable spyware/grayware scan (Configuración actual de escaneo > Activar escaneo de spyware/grayware).***
    - ***Files to Scan > File types scanned by IntelliScan (Archivos que se van a escanear > Tipos de archivos escaneados mediante IntelliScan).***

- ***Scan Settings > Scan compressed files (Configuración de escaneo > Escanear archivos comprimidos).***
- ***Scan Settings > Scan OLE objects (Configuración de escaneo > Escanear objetos OLE).***
- ***Virus/Malware Scan Settings Only > Scan boot area (Solo configuración de escaneo de virus/malware > Escanear área de reinicio).***
- ***CPU Usage > Low (Uso de CPU > Bajo).***

33. Haga clic en la pestaña ***Scan Exclusion*** (Exclusión de escaneo), seleccione solo las siguientes opciones y desmarque el resto:
    - ***Scan Exclusion > Enable scan exclusion (Exclusión de escaneo > Activar exclusión de escaneo).***
    - ***Scan Exclusion > Apply scan exclusion settings to all scan types (Exclusión de escaneo > Aplicar configuración de exclusión de escaneo a todos los tipos de escaneo).***
    - ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed (Lista de exclusiones de escaneo [directorios] > Excluir directorios en los que estén instalados productos de Trend Micro).***
    - Asegúrese de las rutas ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** y ***G:***
34. Haga clic en ***Apply to All Clients*** (Aplicar a todos los clientes).
35. Haga clic en ***Close*** (Cerrar) para salir de la pantalla ***Manual Scan Settings*** (Configuración de escaneo manual).
36. En el panel superior, seleccione el enlace ***Agents > Agent Management*** (Agentes > Administración de agentes).
37. En el lado izquierdo, seleccione ***OfficeScan Server*** (Servidor de OfficeScan).
38. En las opciones de ***Settings*** (Configuración), seleccione ***Web Reputation Settings*** (Configuración de reputación web). Aparece la pantalla ***Web Reputation Settings*** (Configuración de reputación web).
39. Haga clic en la pestaña ***External Clients*** (Clientes externos) y desmarque ***Enable Web reputation policy on the following operating systems*** (Activar directiva de reputación web en los siguientes sistemas operativos) si se seleccionó durante la instalación.
40. Haga clic en la pestaña ***Internal Agents*** (Agentes internos) y desmarque ***Enable Web reputation policy on the following operating systems*** (Activar directiva de reputación web en los siguientes sistemas operativos) si se seleccionó durante la instalación.
41. Haga clic en ***Apply to All Clients*** (Aplicar a todos los clientes).
42. Haga clic en ***Close*** (Cerrar) para salir de la pantalla ***Web Reputation*** (Reputación web).
43. En el panel superior, seleccione el enlace ***Agents > Agent Management*** (Agentes > Administración de agentes).
44. En el lado izquierdo, seleccione ***OfficeScan Server*** (Servidor de OfficeScan).
45. En las opciones de ***Settings*** (Configuración), seleccione ***Behavior Monitoring Settings*** (Configuración de la monitorización del comportamiento). Aparece la pantalla ***Behavior Monitoring Settings*** (Configuración de la monitorización del comportamiento).

46. Desmarque las opciones ***Enable Malware Behavior Blocking*** (Activar bloqueo del comportamiento del malware) y ***Enable Event Monitoring*** (Activar monitorización de sucesos).

47. Haga clic en ***Apply to All Clients*** (Aplicar a todos los clientes).

48. Haga clic en ***Close*** (Cerrar) para salir de la pantalla ***Behavior Monitoring*** (Monitorización del comportamiento).

49. En el panel superior, seleccione el enlace ***Agents > Agent Management*** (Agentes > Administración de agentes).

50. En el lado izquierdo, seleccione ***OfficeScan Server*** (Servidor de OfficeScan).

51. En las opciones de ***Settings*** (Configuración), seleccione ***Device Control Settings*** (Configuración del control del dispositivo). Aparece la pantalla ***Device Control Settings*** (Configuración del control del dispositivo).

52. Haga clic en la pestaña ***External Agents*** (Agentes externos) y desmarque las siguientes opciones:

    - ***Notification > Display a notification message on endpoints when OfficeScan detects unauthorized device access (Notificación > Mostrar notificación en los terminales de conexión cuando OfficeScan detecte un acceso no autorizado al dispositivo).***
    - ***Block the AutoRun function on USB storage devices (Bloquear la función de ejecución automática en dispositivos de almacenamiento USB).***
    - ***Enable Device Control (Activar el control del dispositivo).***

53. Haga clic en la pestaña ***Internal Agents*** (Agentes internos) y desmarque las siguientes opciones:

    - ***Notification > Display a notification message on endpoints when OfficeScan detects unauthorized device access (Notificación > Mostrar notificación en los terminales de conexión cuando OfficeScan detecte un acceso no autorizado al dispositivo).***
    - ***Block the AutoRun function on USB storage devices (Bloquear la función de ejecución automática en dispositivos de almacenamiento USB).***
    - ***Enable Device Control (Activar el control del dispositivo).***

54. Haga clic en ***Apply to All Clients*** (Aplicar a todos los clientes).

55. Haga clic en ***Close*** (Cerrar) para salir de la pantalla ***Device Control Settings*** (Configuración del control del dispositivo).

56. En las opciones de ***Settings*** (Configuración), seleccione otra vez ***Device Control Settings*** (Configuración del control del dispositivo). Aparece la pantalla ***Device Control Settings*** (Configuración del control del dispositivo).

57. Haga clic en la pestaña ***External Agents*** (Agentes externos) y desmarque ***Enable Device Control*** (Activar el control del dispositivo).

58. Haga clic en la pestaña ***Internal Agents*** (Agentes internos) y desmarque ***Enable Device Control*** (Activar el control del dispositivo).

59. Haga clic en ***Apply to All Clients*** (Aplicar a todos los clientes).

60. Haga clic en ***Close*** (Cerrar) para salir de la pantalla ***Device Control Settings*** (Configuración del control del dispositivo).

61. En el panel izquierdo, seleccione el enlace ***Agents > Agent Management*** (Administración de agentes).

62. En el lado izquierdo, seleccione ***OfficeScan Server*** (Servidor de OfficeScan).

63. En las opciones de ***Settings*** (Configuración), seleccione ***Privileges And Other Settings*** (Privilegios y otros ajustes).

64. Haga clic en la pestaña ***Privileges*** (Privilegios), seleccione solo las siguientes opciones y desmarque el resto:

    - ***Scan Privileges > Configure Manual Scan Settings (Privilegios de escaneo > Configuración de escaneo manual).***
    - ***Scan Privileges > Configure Real-time Scan Settings (Privilegios de escaneo > Configuración de escaneo en tiempo real).***
    - ***Scan Privileges > Configure Scheduled Scan Settings (Privilegios de escaneo > Configuración de escaneo programado).***
    - ***Proxy Setting Privileges > Allow the agent user to configure proxy settings (Privilegios de configuración de proxy > Permitir que el usuario del agente configure los ajustes de proxy).***
    - ***Uninstallation > Requires a password (Desinstalar > Requiere una contraseña).*** Introduzca la contraseña adecuada y confírmela.
    - ***Unload and Unlock > Requires a password (Descargar y Desbloquear > Requiere una contraseña).*** Introduzca la contraseña adecuada y confírmela.

65. Haga clic en la pestaña ***Other Settings*** (Otros ajustes).

66. Desmarque todas las opciones.

NOTA: Es importante que desactive las siguientes opciones.

- ***OfficeScan Agent Self-protection > Protect OfficeScan agent services (Protección automática del agente OfficeScan > Proteger los servicios del agente OfficeScan).***
- ***OfficeScan Agent Self-protection > Protect files in the OfficeScan agent installation folder (Protección automática del agente OfficeScan > Proteger archivos de la carpeta de instalación del agente OfficeScan).***
- ***OfficeScan Agent Self-protection > Protect OfficeScan agent registry keys (Protección automática del agente OfficeScan > Proteger claves de registro del agente OfficeScan).***
- ***OfficeScan Agent Self-protection > Protect OfficeScan agent processes (Protección automática del agente OfficeScan > Proteger los procesos del agente OfficeScan).***

67. Haga clic en ***Apply to All Clients*** (Aplicar a todos los clientes).

68. Haga clic en ***Close*** (Cerrar) para salir de la pantalla ***Privileges And Other Settings*** (Privilegios y otros ajustes).

69. En el panel superior, seleccione el enlace ***Agents > Agent Management*** (Agentes > Administración de agentes).

70. En el lado izquierdo, seleccione ***OfficeScan Server*** (Servidor de OfficeScan).

71. En las opciones de ***Settings*** (Configuración), seleccione ***Additional Service Settings*** (Configuración de servicio adicional).

72. Desmarque la opción ***Enable service on the following operating systems*** (Activar servicio en los siguientes sistemas operativos).
73. Haga clic en ***Apply to All Clients*** (Aplicar a todos los clientes).
74. Haga clic en ***Close*** (Cerrar) para salir de la pantalla ***Additional Service Settings*** (Configuración de servicio adicional).
75. En el panel superior, seleccione el enlace ***Agents > Global Agent Settings*** (Agente > Configuración general de agente).
76. Seleccione únicamente las siguientes opciones y desmarque las demás:
    - ***Scan Settings for Large Compressed Files > Do not scan files in the compressed file if the size exceeds 2 MB*** (Configuración de escaneo para archivos comprimidos grandes > No escanear archivos del archivo comprimido si su tamaño es superior a 2 MB). Realice esto para poder utilizar ***Real-Time Scan*** (Escaneo en tiempo real) y ***Manual Scan/Schedule Scan/Scan Now*** (Escaneo manual/Programar Escaneo/Escanear ahora).
    - ***Scan Settings for Large Compressed Files > In a compressed file scan only the first 100 files (Configuración de escaneo para archivos comprimidos grandes > Escanear solo los 100 primeros archivos de un archivo comprimido).*** Realice esto para poder utilizar ***Real-Time Scan*** (Escaneo en tiempo real) y ***Manual Scan/Schedule Scan/Scan Now*** (Escaneo manual/Programar Escaneo/Escanear ahora).
    - ***Scan Settings > Exclude the OfficeScan server database folder from Real-time Scan (Configuración de escaneo > Excluir la carpeta de la base de datos del servidor de OfficeScan del escaneo en tiempo real).***
    - ***Scan Settings > Exclude Microsoft Exchange server folders and files from scans (Configuración de escaneo > Excluir las carpetas y archivos del servidor de Microsoft Exchange de los escaneos).***
77. Haga clic en ***Save*** (Guardar).
78. En el panel superior, seleccione el enlace ***Updates > Agents > Manual Updates*** (Actualizaciones > Agentes > Actualizaciones Manuales).
79. Seleccione ***Manually select agents*** (Seleccionar a los agentes manualmente) y haga clic en ***Select*** (Seleccionar).
80. Haga doble clic en el nombre de dominio apropiado en ***OfficeScan Server*** (Servidor de OfficeScan).
81. Seleccione el sistema del cliente uno por uno y haga clic en ***Initiate Update*** (Iniciar actualización).
82. Haga clic en ***OK*** (Aceptar) en el cuadro de mensaje.
83. Haga clic en ***Log off*** (Cerrar sesión) y cierre la consola de OfficeScan Web.

Pautas posteriores a la instalación de Trend Micro OfficeScan

1. Active la conexión de bucle invertido. Para obtener más información, consulte Activar la conexión de bucle invertido en la página 6.
2. Configure el servicio del Explorador de equipos. Para obtener más información, consulte Configurar el servicio del Explorador de equipos después de instalar el antivirus en la página 7.

Solución de problemas sobre dominios o sistemas que no aparecen en la ventana de dominios y puntos de conexión

Cuando se ejecutan los métodos de instalación preferidos tanto para Trend Micro OfficeScan Client/Server Edition 11.0 SP1 como para Trend Micro OfficeScan Client/Server Edition XG 12.0, los dominios y sistemas deben enumerarse para forzar la instalación en el sistema. Estos pasos le ofrecen dos opciones para instalar el software antivirus en los clientes (adquisición, revisión e INW).

Para 11.0 SP1, consulte Trend Micro OfficeScan: pasos para la implementación de una nueva instalación (método preferido de instalación forzada para 11.0.SP1) en la página 59.
Para 12.0, consulte Trend Micro OfficeScan: pasos para la implementación de una nueva instalación (método preferido de instalación forzada para 12.0) en la página 71.

1. Utilice las direcciones IP de los equipos cliente (adquisición, revisión y INW) en la consola de administración, y haga lo siguiente:
    a. Introduzca la dirección IP de cada uno de los sistemas del cliente en el cuadro ***Search for endpoints*** (Buscar puntos de conexión) de uno en uno y pulse ***Enter*** (Intro).
    b. Proporcione el ***<nombre de dominio>/nombre de usuario*** y la contraseña, y haga clic en ***Log On*** (Iniciar sesión).
    c. Escoja uno de los siguientes pasos en base a la versión de su Trend Micro:
        i. Para 11.0 SP1, vuelva al paso 10 en la página 60.
        ii. Para 12.0, vuelva al paso 10 en la página 72.
2. Si no conoce la dirección IP de los sistemas o la opción anterior falla, vaya a cada equipo cliente (adquisición, revisión y INW Server) y haga lo siguiente:
    a. Inicie sesión como **Administrator** (Administrador) o como miembro de ese grupo en todos los equipos cliente.
    b. Haga clic en ***Start > Run*** (Inicio > Ejecutar).
    c. Escriba ***<Anti-Virus Management Console_server_IP_address>*** y pulse ***Enter*** (Intro). Cuando se le solicite, introduzca el nombre de usuario del administrador y la contraseña.
    d. Vaya a ***<Anti-Virus Management Console_server_IP _address>\ofsscan*** y haga doble clic en ***AutoPcc.exe***. Cuando se le solicite, introduzca el nombre de usuario del administrador y la contraseña.
    e. Reinicie los sistemas del cliente cuando se complete la instalación.
    f. Inicie sesión como **Administrator** (Administrador) o como miembro de ese grupo en todos los equipos cliente y espere a que el icono de Trend Micro OfficeScan de la bandeja del sistema cambie a azul.
    g. Escoja uno de los siguientes pasos en base a la versión de su Trend Micro:
        i. Para 11.0 SP1, consulte Configuración de la consola del servidor Trend Micro OfficeScan para 11.0 SP1 en la página 60.
        ii. Para 12.0, consulte Configuración de la consola del servidor de Trend Micro OfficeScan para 12.0 en la página 72.