Manual de producto de GFI

GFI LanGuard™

Guía del evaluador: cómo obtener el máximo beneficio de una prueba de GFI LanGuard

GFI®

Versión del documento: 12.0

Última actualización (mes/día/año): 14/04/2016

Índice

1 Introducción

Gracias por evaluar GFI LanGuard El propósito de esta guía es ayudarlo a obtener el máximo beneficio de su versión de prueba de GFI LanGuard.

En las secciones siguientes, nuestras directrices lo ayudarán a comprobar los beneficios para sí mismo y para cualquier otra persona involucrada en el proceso de decisión.

Tema de esta sección:

1.1 Información general sobre GFI LanGuard

GFI LanGuard es una solución abarcadora de administración de redes. Funciona como un consultor de seguridad virtual y brinda asistencia en las siguientes áreas:

- Administración de revisiones
- Evaluación de vulnerabilidades
- Auditoría de redes y de software
- Inventario de recursos
- Administración de dispositivos móviles
- Análisis de riesgos
- Cumplimiento

GFI LanGuard examina y analiza su red, y permite realizar correcciones en ella.

» Sin importar si la instalación se realiza con o sin agente, GFI LanGuard examina la red en busca de problemas relacionados con la seguridad y recopila información correspondiente a la seguridad. Recopila información acerca de vulnerabilidades de seguridad, revisiones faltantes, Service Pack faltantes, puertos abiertos, recursos compartidos abiertos, usuarios y grupos, aplicaciones instaladas, teléfonos inteligentes y tabletas usados por los empleados e inventarios de hardware. GFI LanGuard se integra en más de 4 000 aplicaciones de seguridad, como antivirus, antispyware o cortafuegos, y realiza informes acerca del estado de estas.

» Con los resultados de los exámenes, usted puede después analizar el estado de su red. GFI LanGuard proporciona un poderoso panel para examinar e investigar los resultados de examen. Se activan sensores de seguridad ante la detección de problemas. Se asigna un nivel de vulnerabilidad a cada equipo examinado según los resultados de auditoría.GFI LanGuard también proporciona informes y comparaciones de resultados.

» Después del examen y el análisis, GFI LanGuard brinda asistencia para corregir los problemas de seguridad y automatiza el proceso cuando es posible.

» Después de crear un examen de línea de base, puede identificar cualquier diferencia o cambio en la seguridad y en las configuraciones de equipos de todos los equipos de la red. Puede, por ejemplo, decidir realizar acciones como implementar actualizaciones de seguridad (y no de seguridad) pertenecientes y no pertenecientes a Microsoft, revertir actualizaciones, implementar software y scripts personalizados, desinstalar aplicaciones no autorizadas y abrir conexiones a escritorios remotos para equipos examinados. Todas estas acciones le permitirán asegurarse de que su red esté actualizada y de que se apliquen las revisiones más recientes.

1.2 ¿Por qué los clientes compran GFI LanGuard?

Según nuestra experiencia, las cinco razones principales por las que los clientes de GFI compran GFI LanGuard son las siguientes:

1. Para minimizar el riesgo de infracciones de seguridad:

» Examinando la red en busca de problemas de seguridad y vulnerabilidad

» Detectando y desinstalando de forma automática cualquier aplicación no autorizada

» Realizando auditorías de software (determinando el software instalado en los equipos en cuestión) y de los dispositivos de hardware de la red

» Recibiendo alertas e informes relacionados con el entorno de seguridad de la red

2. Para automatizar la administración de revisiones; detectar e implementar revisiones faltantes para los sistemas de Microsoft, Mac OS y Linux y otras aplicaciones de terceros.

3. Para realizar auditorías de redes y controlar el estado de estas

4. Para contribuir al cumplimiento de normativas de seguridad que requieran la evaluación regular de vulnerabilidades y la administración de revisiones (por ejemplo, PCI DSS, HIPAA, SOX, GLBA y Coco de la PSN)

5. Para evaluar y administrar la seguridad de los teléfonos inteligentes y las tabletas que usan los empleados para acceder a datos y aplicaciones de la empresa.

En los siguientes temas, se proporcionan escenarios de la vida real con mayor información sobre los usos prácticos de GFI LanGuard:

1.2.1 Utilización de GFI LanGuard paral a evaluación de vulnerabilidades

GFI LanGuard realiza más de 50.000 comprobaciones de vulnerabilidad en su sistema operativo, sus entornos virtuales, sus dispositivos de red y sus aplicaciones instaladas mediante bases de datos de comprobación de vulnerabilidades como OVAL y las 20 directrices principales de SANS.

En esta sección se le proporcionan directrices relacionadas con la manera en que recomendamos abordar las evaluaciones de vulnerabilidades y la corrección de problemas de seguridad para mantener sus equipos seguros y actualizados.

» Mantenga GFI LanGuard actualizado

» Asegúrese de que el equipo en el que GFI LanGuard esté instalado tenga acceso a Internet.GFI LanGuard realiza comprobaciones diarias en busca de información actualizada sobre vulnerabilidades y revisiones.

» Si se utiliza un servidor proxy, se puede configurar en la interfaz de usuario de **GFI LanGuard > Menú principal > Configuration > Proxy Settings...**

» Si no hay disponible acceso a Internet en el equipo en el que GFI LanGuard está instalado, el producto se puede configurar para obtener las actualizaciones de una ubicación alternativa. Se encuentra disponible más información aquí.

» Realice auditorías de seguridad de forma regular

» Cada día se descubren problemas de seguridad nuevos. Para su corrección se requiere planificación anticipada, y es mejor tener conocimiento de los problemas de seguridad lo más temprano posible a fin de poder realizar planificaciones para lograr una corrección eficaz.

» Se recomienda configurar el producto para que realice de forma automática auditorías a diario o semanalmente.

» Implemente primero actualizaciones de seguridad faltantes

» La gran mayoría de los problemas de seguridad se pueden solucionar garantizando que todas las revisiones y todos los Service Pack estén actualizados en cada equipo.

» Los Service Pack incluyen muchas correcciones de seguridad, por lo que se recomienda aplicarlos primero.

» Tras implementar los Service Pack, se recomienda volver a analizar la red, lo que le dará una visión general actualizada del estado de las revisiones de su red.

» Después del examen, implemente las revisiones faltantes

» El producto se puede configurar para implementar actualizaciones de seguridad de forma automática si el administrador lo aprueba previamente.

» Investigue y corrija otros problemas de seguridad

» Los resultados de la evaluación de vulnerabilidades incluyen descripciones detalladas de los problemas de seguridad detectados y referencias a sitios web externos para obtener información adicional.

» GFI LanGuardincluye herramientas para abordar las vulnerabilidades mediante la desinstalación remota de software (no autorizado), habilitar antivirus, antispyware o cortafuegos, desencadenar la actualización de definiciones de antivirus o antispyware, implementar software y scripts personalizados o abrir conexiones a escritorios remotos para los equipos.

» Cómo comprobar el estado de la seguridad de su red

» Utilice **Dashboard > Overview** para obtener información general ejecutiva del estado de seguridad de la red, incluidos los equipos más vulnerables, la distribución de vulnerabilidades y las tendencias de vulnerabilidad

» GFI LanGuard proporciona un nivel de vulnerabilidad de la red que se calcula de acuerdo con los niveles de vulnerabilidad individuales de cada equipo. Cada equipo tiene un nivel de vulnerabilidad según los problemas de seguridad que se detecten en él. Los problemas de seguridad se clasifican con los niveles de gravedad alto, medio o bajo de acuerdo con el sistema de puntuación CVSS, según los cálculos de la NVD.

» Utilice **Dashboard > History** para obtener la lista de problemas de seguridad nuevos detectados junto con una lista de otros cambios de configuración de seguridad en la red.

» Utilice **Dashboard > Vulnerabilities** para obtener una vista detallada de vulnerabilidades detectadas en la red

» Utilice **Dashboard > Patches** para obtener una vista detallada del estado de revisiones de la red

» Utilice el informe **Reports > Network Security Overview** para obtener información general ejecutiva del estado de seguridad de la red

» Utilice el informe **Reports > Vulnerability Status** para obtener información general detallada del estado de seguridad de la red

» Utilice el informe **Reports > Remediation History** para obtener un historial de problemas de seguridad corregidos con GFI LanGuard

»
Utilice el informe **Informes > Auditoría de dispositivo móvil** para obtener información general acerca de qué teléfonos inteligentes y tabletas se conectan a los servidores de Microsoft Exchange de la empresa, y para detectar si tienen sistemas operativos desactualizados, con problemas de seguridad conocidos.

» Los informes se pueden configurar para generarse de forma regular

1.2.2 Utilización de GFI LanGuardGFI LanGuard para la administración de revisiones

GFI LanGuard ofrece la detección, descarga e implementación a petición o automatizada de actualizaciones faltantes, y abarca lo siguiente:

» Sistemas operativos y aplicaciones de Microsoft

» Sistemas operativos y aplicaciones de Mac OS X

» Sistemas operativos y aplicaciones de Linux Se admiten las siguientes distribuciones de Linux: Red Hat Enterprise Linux, Fedora, Ubuntu, Suse, OpenSuse, CentOS y Debian

» Las aplicaciones de terceros más populares y de seguridad que funcionan en plataformas de Windows, incluidos todos los exploradores web principales, los productos Adobe, los tiempos de ejecución Java, etc. Para obtener una lista completa, haga clic aquí.

» Revisiones de seguridad y no de seguridad

» Inversión de revisiones

» Implementación de software y scripts personalizados en la red (cualquier software que se pueda ejecutar de forma silenciosa utilizando GFI LanGuard)

1.2.3 Utilización de GFI LanGuard para el seguimiento de recursos

Los dispositivos no administrados u olvidados representan un riesgo de seguridad. Utiliza GFI LanGuard para hallar dispositivos de los que no haya tenido conocimiento:

» Servidores y estaciones de trabajo

» Equipos virtuales

» Dispositivos basados en IP, como enrutadores, impresoras, puntos de acceso, conmutadores, etc.

» Dispositivos móviles, como iPad, iPhone y teléfonos Android

Para obtener más información, consulte Implementación de software personalizado (page 36).

1.2.4 Utilización de GFI LanGuard para la auditoría de redes y de software

GFI LanGuard proporciona un análisis detallado de lo que sucede en su red; qué aplicaciones o configuraciones predeterminadas plantean un riesgo de seguridad, y toda la información que necesita acerca de su red, como lo que se muestra a continuación:

» Sistemas operativos

» Equipos virtuales

» Hardware y software instalados

» Información sobre la CPU

» Espacio en la HDD

» Dispositivos inalámbricos

» Adaptadores de red

» Servicios

» Políticas de auditoría

» Usuarios y grupos

» Recursos compartidos

» Puertos TCP y UDP abiertos

» Teléfonos inteligentes y tabletas que se conectan a los servicios de la empresa, como Microsoft Exchange, Office 365, Google Apps y Apple Profiles Manager

Utilice **Dashboard > Software** para obtener una vista detallada de todas las aplicaciones instaladas en la red.

Utilice **Dashboard > Hardware** para comprobar el inventario de hardware de la red.

Utilice **Dashboard > System Information** para ver detalles de seguridad acerca de los sistemas presentes en la red.

Utilice **Dashboard > History** para obtener una lista de cambios de seguridad que se produjeron en la red

Utilice **Reports > Software Audit** para generar un informe abarcador acerca de las aplicaciones instaladas en la red.

Utilice el informe Reports > Mobile Device Audit para obtener información general acerca de qué teléfonos inteligentes y tabletas se conectan a los servicios de la empresa, como Microsoft Exchange, Office 365, Google Apps y Apple Profiles Manager, y para detectar si tienen sistemas operativos desactualizados, con problemas de seguridad conocidos.

GFI LanGuard se puede utilizar para marcar, detectar y quitar aplicaciones no autorizadas en la red.

GFI LanGuard se integra en más de 4 000 aplicaciones de seguridad críticas de las siguientes categorías: antivirus, antispyware, cortafuegos, protección contra suplantación de identidad, clientes de copia de seguridad, clientes de VPN, filtrado de URL, administración de revisiones, exploradores web, mensajería instantánea, punto a punto, cifrado de discos, prevención contra pérdida de datos y control de acceso a dispositivos. Proporciona informes sobre el estado de estas y rectifica problemas al permitir operaciones como la habilitación de antivirus o cortafuegos, el desencadenamiento de actualizaciones de definiciones para antivirus o antispyware, o la desinstalación de aplicaciones punto a punto.

1.2.5 Utilización de GFI LanGuardGFI LanGuard para el cumplimiento de la legislación vigente

Cada vez se crean más leyes y normativas que imponen prácticas de seguridad específicas a las empresas. Las instituciones gubernamentales y las empresas que ofrecen servicios financieros y de salud se encuentran entre las entidades más afectadas por estas normativas, pero la tendencia indica que todas las empresas necesitarán tener suficiente seguridad para proteger la privacidad y los datos de sus empleados, clientes y socios. El incumplimiento puede ocasionar la pérdida de oportunidades, la aplicación de sanciones legales y financieras e incluso, en casos extremos, la desaparición.

A continuación se ofrece una lista de elementos de seguridad comunes que estas normativas exigen y los casos en que GFI LanGuard puede ser de ayuda:

- Realización regular de evaluaciones de vulnerabilidades
- Aplicación de las revisiones necesarias en los sistemas
- Verificación de la instalación, del correcto funcionamiento y de la actualización de software antivirus y antispyware en todos los sistemas de la red.
- Verificación de la instalación y activación de un cortafuegos personal en cada sistema de la red
- Verificación de la instalación de software de cifrado en toda la red

GFI LanGuard se puede con otros productos de GFI Software para formar un conjunto de productos dedicados al cumplimiento:

- GFI EventsManager®: solución de administración de registros
- GFI EndPointSecurity™: solución de bloqueo de dispositivos

GFI LanGuard incluye un conjunto de informes predefinidos, dedicados al cumplimiento de PCI DSS, HIPAA, SOX, GLBA y Coco de la PSN, entre otros estándares. Se encuentra disponible más información sobre PCI DSS aquí.

A continuación se ofrece una lista con algunos de los estándares más importantes relacionados con la seguridad de infraestructuras de TI:

- Estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS)
- Ley Healthcare Insurance Portability and Accountability Act (HIPAA)
- Ley Sarbanes–Oxley (SOX)
- Ley Gramm–Leach–Bliley (GLB/GLBA)
- Ley Federal de Administración de Seguridad de la Información (FISMA)
- Ley del Derecho de la Familia a la Confidencialidad de Información Educativa (FERPA)
-

Ley de protección de la infancia en Internet (Children's Internet Protection Act, CIPA)

- Código de conexión de la red del sector público (PSN CoCo)

- Directiva de Protección de Datos de la Unión Europea
- Directiva de Privacidad y Comunicaciones Electrónicas de la Unión Europea

1.2.6 Uso de GFI LanGuard para administración de dispositivos móviles

GFI LanGuard permite detectar teléfonos inteligentes y tabletas que se conectan a los servicios de la empresa, como servidores de Microsoft Exchange, Office 365, Google Apps o Apple Profiles Manager y:

- Clasificar los dispositivos por usuario, fabricante, modelo de dispositivo, sistema operativo, fecha y hora de última conexión
- Realice una evaluación de vulnerabilidades del sistema operativo del dispositivo. Se admiten Android, iOS y Windows Phone.
- Informar acerca de actualizaciones disponibles del sistema operativo
- Envíe notificaciones personalizadas por correo electrónico a los propietarios de dispositivos.

1.3 Obtención de una clave de evaluación

Si aún no descargó GFI LanGuard, antes de iniciar descargue la versión de prueba aquí.

Para iniciar la evaluación de GFI LanGuard, introduzca su clave de evaluación gratuita. La clave de evaluación le proporciona toda la funcionalidad del producto con una limitación de 25 direcciones IP y 25 dispositivos móviles durante 30 días. La clave se envía a la dirección de correo electrónico que usted registró al descargar el producto.

Si no tiene acceso al correo electrónico original con la clave, puede solicitar una nueva clave de evaluación gratuita haciendo clic aquí.

Si necesita realizar la evaluación durante un período más prolongado o con más de 25 direcciones IP y 25 dispositivos móviles, puede enviar su solicitud aquí.

2 Realización de exámenes de seguridad

En los sistemas de Windows, GFI LanGuard permite realizar exámenes de seguridad con y sin agentes. En la actualidad, solo se pueden realizar exámenes sin agentes en los sistemas que no son de Windows (dispositivos de red, teléfonos inteligentes y tabletas de Linux y Mac OS). A continuación se proporcionan algunos elementos que se deben considerar al elegir el método de examen que se utilizará:

Exámenes sin agentes:

- No se realizan instalaciones en equipos clientes
- Todo el procesamiento es realizado por el servidor central; no se requieren recursos de equipos clientes
- Funcionan en sistemas en los que no se admiten agentes

Exámenes basados en agentes:

- Tienen un mejor rendimiento debido a la distribución de la carga en los clientes
- Funcionan mejor en entornos de ancho de banda reducido debido a que la comunicación entre el servidor y los clientes es mucho menos intensiva que en el caso de los exámenes sin agente
- Tienen mayor compatibilidad con los portátiles, ya que los agentes continúan funcionando al estar fuera de línea. Cuando se encuentran en línea, simplemente se sincronizan con el servidor
- Mayor precisión en los resultados debido a que los exámenes locales tienen acceso a más información que los remotos

Tema de esta sección:

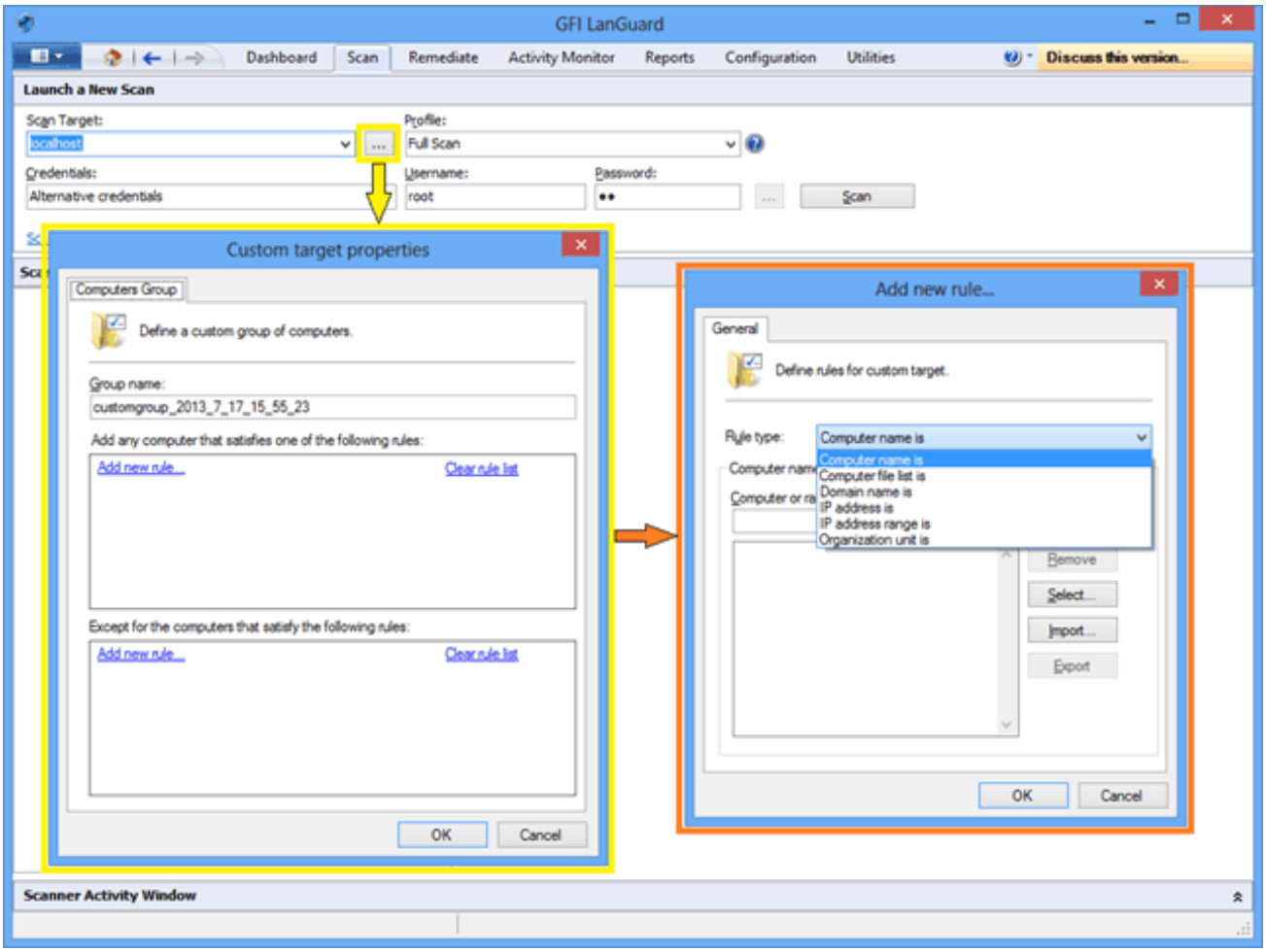
2.1 Exámenes de seguridad sin agentes

2.1.1 Activación de exámenes y seguimiento del progreso en tiempo real

Utilice la ficha Scan para desencadenar exámenes sin agentes de inmediato y realizar el seguimiento del progreso en tiempo real. El destino del examen puede ser cualquier combinación de lo siguiente:

- Nombres de equipos
- Archivos de texto que contengan nombres de equipos
- Una dirección IP individual o un rango de direcciones IP
- Dominios o grupos de trabajos y unidades organizativas

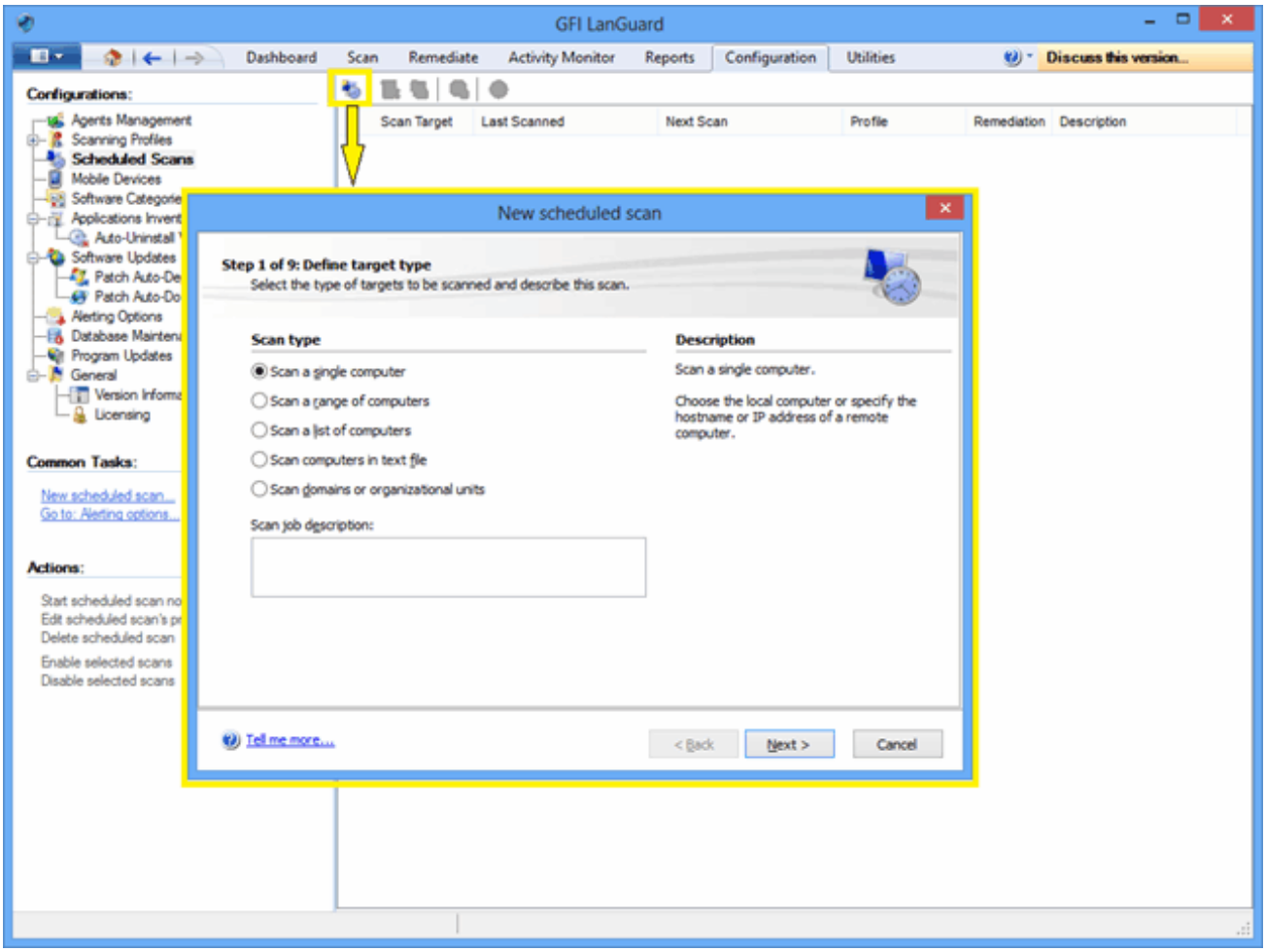
> **Nota:**
> Se requiere acceso administrativo a los equipos remotos para obtener resultados de auditoría de seguridad abarcadores.



Captura de pantalla 1: Exámenes de seguridad sin agentes

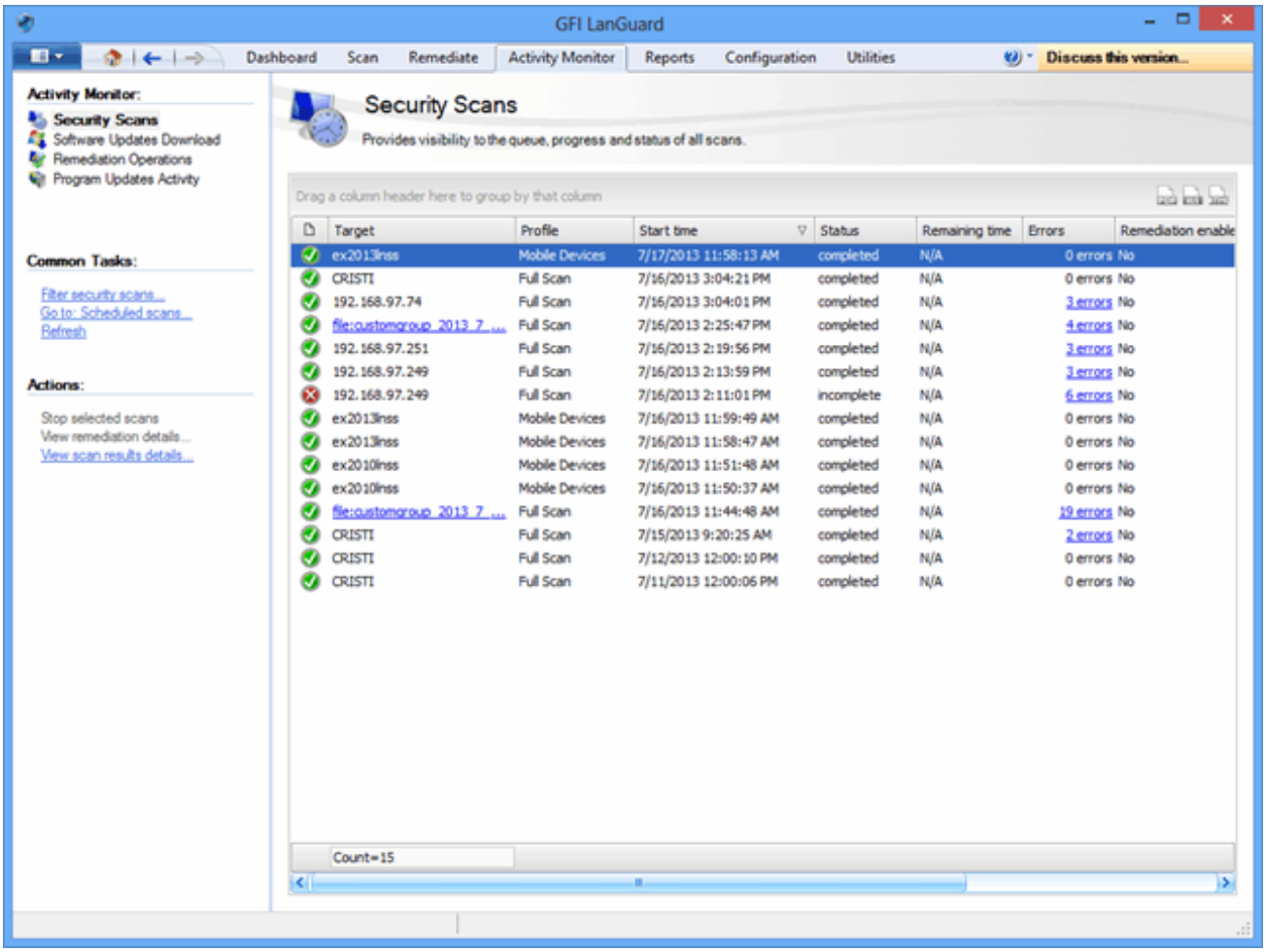
2.1.2 Exámenes programados

1. Para programar la ejecución regular de exámenes sin agentes, haga clic en **Configuration > Scheduled Scans** y seleccione el tipo de destinos que se examinarán.



Captura de pantalla 2: Nuevo examen programado

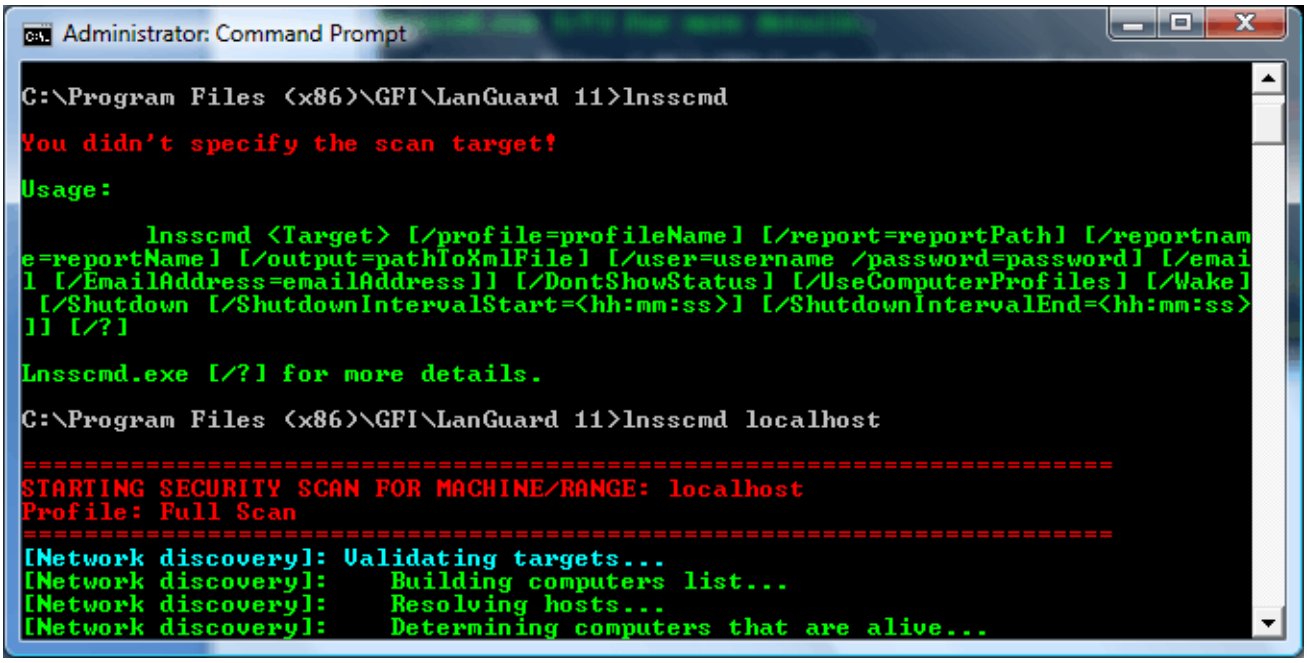
2. Se puede realizar el seguimiento del progreso de los exámenes programados utilizando **Activity Monitor > Security Scans:**



Captura de pantalla 3: Exámenes de seguridad

2.1.3 Exámenes de línea de comandos

1. Para realizar exámenes de línea de comandos, utilice la herramienta lnsscmd.exe



Captura de pantalla 4: Exámenes de línea de comandos

2.2 Auditorías basadas en agentes

El proceso para habilitar agentes es sencillo. Simplemente establezca la lista de equipos, unidades organizativas o dominios en los que los agentes se deban implementar y proporciones credenciales con acceso administrativo a los equipos remotos.

GFI LanGuard se encargará de la operación de implementación.

Qué hacen los agentes:

» GFI LanGuard instala los agentes de forma automática en los equipos seleccionados

» Los agentes solo se instalan en sistemas de Microsoft Windows

» De forma predeterminada, los agentes realizan un examen completo de sus equipos host una vez al día, pero la frecuencia, el tiempo de examen y el perfil de detección se pueden configurar

» Los agentes necesitan aproximadamente 25 MB de RAM y 600 MB de espacio en disco.

» Los agentes consumen energía de la CPU solo cuando el equipo host se somete a auditoría. Esto normalmente se produce durante unos minutos por día y la prioridad del proceso es inferior a normal, de modo que no interferirá con el trabajo realizado en el equipo en cuestión.

» Los agentes se pueden desinstalar desde GFI LanGuard. De forma predeterminada, los agentes se desinstalarán automáticamente si no tienen contacto con su servidor durante 60 días. El número de días se puede configurar.

» Los agentes de GFI LanGuard comunican su estado al servidor de GFI LanGuard utilizando el puerto TCP 1070. El número de puerto se puede configurar.

» GFI LanGuard se puede configurar para realizar, de forma automática, la detección de redes en dominios o unidades organizativas y la instalación agentes en equipos recién detectados.

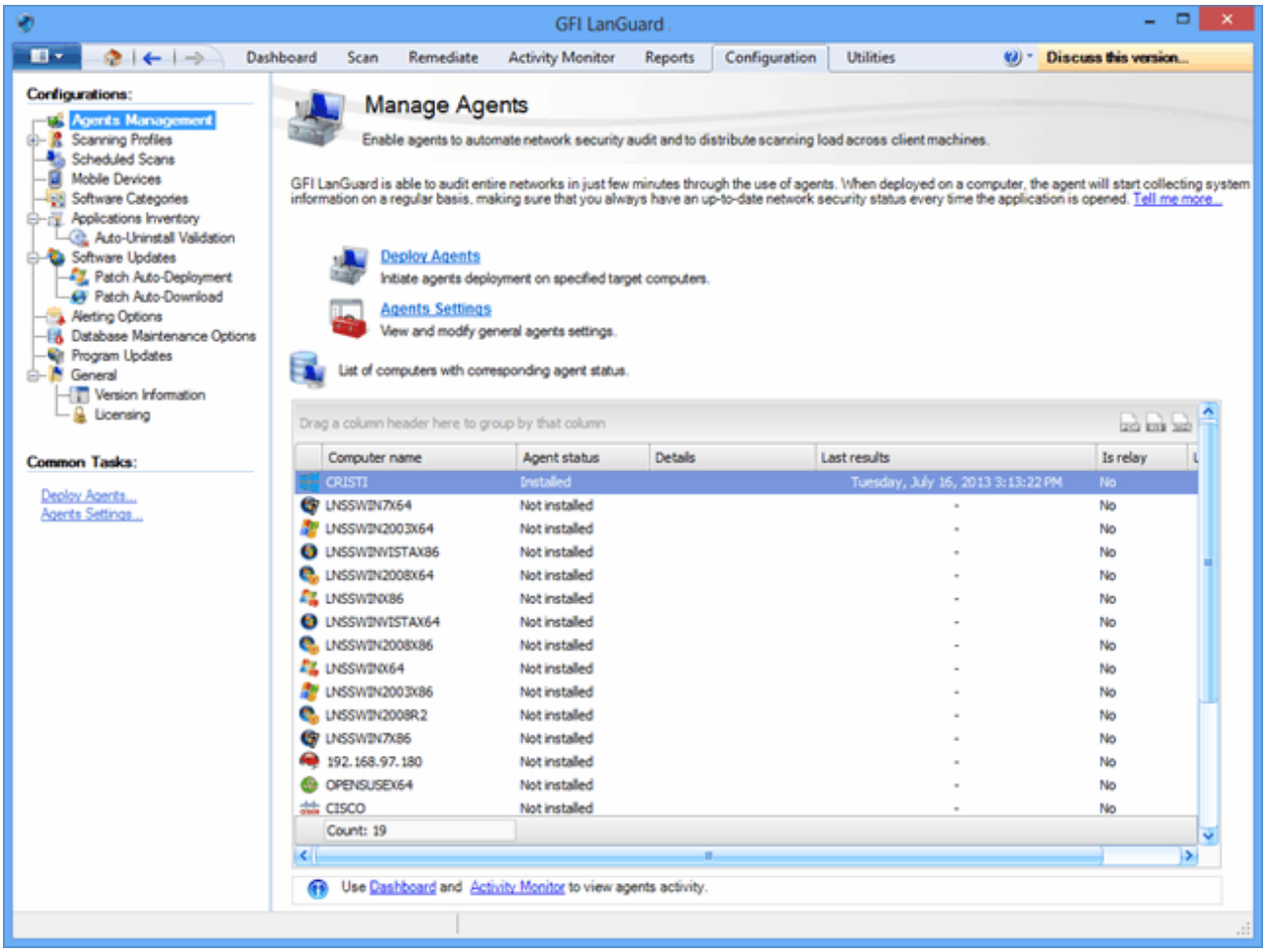
» GFI LanGuard se encarga, de forma automática, de situaciones en las que los agentes se eliminaron por error o se deben actualizar.

> **Importante:**
> Para un agente se puede designar un agente de retransmisión, que permite realizar la corrección con mayor eficiencia y menor consumo de ancho de banda para redes grandes o de sitios múltiples. El agente de retransmisión almacena una copia local de los datos de revisiones (normalmente almacenados en el servidor de GFI LanGuard), y estos se utilizan para corregir equipos cercanos.

> **Nota:**
> Para obtener más información sobre los agentes de retransmisión, consulte Guía del administrador que se puededescargar de aquí.

Para activar agentes:

1. Haga clic en **Configuration > Manage Agents**

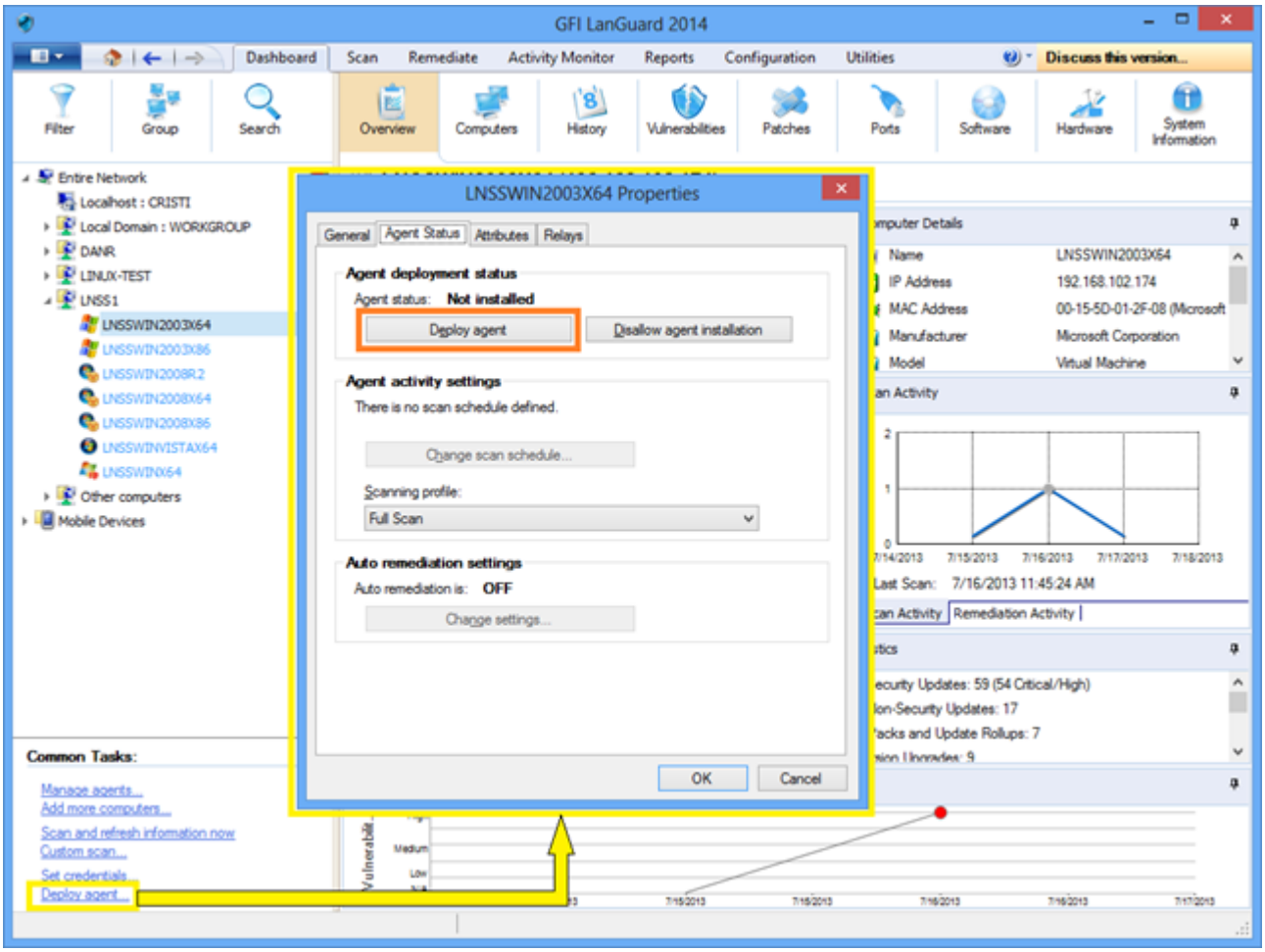


Captura de pantalla 5: Administración de agentes

2.2.1 Solución de problemas de errores de implementación de agentes

Para hallar una lista de posibles causas en caso de que GFI LanGuard no logre implementar agentes en determinadas máquinas, haga clic aquí

Para habilitar y configurar agentes, haga clic en **Dashboard > Overview** y seleccione **Deploy agent…** en la sección **Common Tasks**:



Captura de pantalla 6: Implementación de un agente

2.2.2 Desencadenamiento de exámenes basados en agentes a petición

Los exámenes basados en agentes generalmente se ejecutan de forma automática en segundo plano en equipos remotos según la programación de auditoría establecida (de forma predeterminada, los agentes realizan sus exámenes una vez al día).

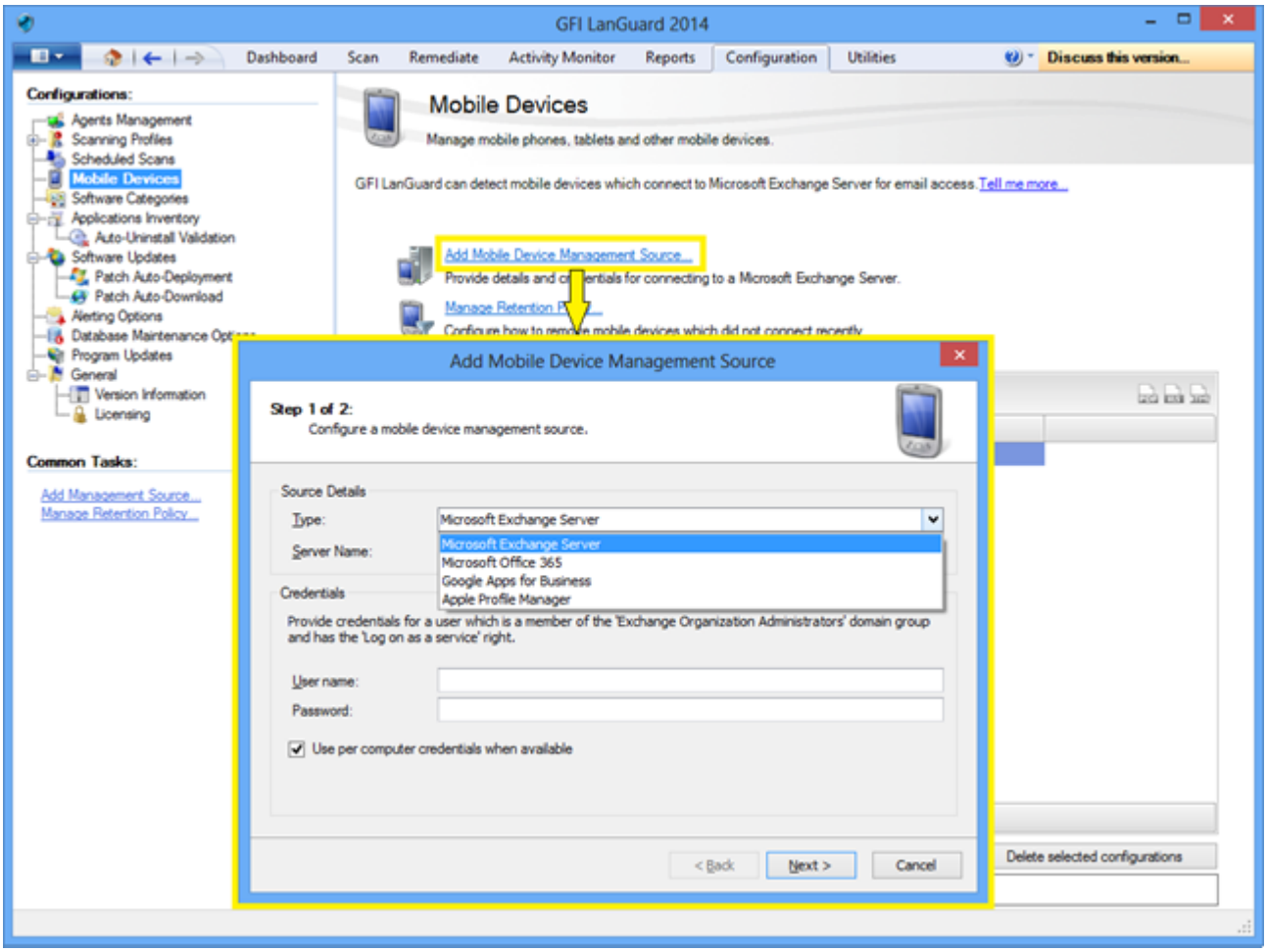
> **Nota:**
> Si se necesita una actualización de la información de seguridad, puede desencadenar exámenes de agentes a petición utilizando la opción**Scan and refresh now** en **Dashboard**.

2.3 Auditoría de teléfonos inteligentes y tabletas

GFI LanGuard permite auditar teléfonos inteligentes y tabletas que se conectan a los servicios de la empresa (como Microsoft Exchange, Office 365, Google Apps y Apple Profiles Manager). Utilice esta característica para enterarse de qué dispositivos móviles usan sus empleados, qué problemas de seguridad tienen y si hay alguna actualización de sistema operativo que corregiría esos problemas de seguridad.

> **Nota:**
> La auditoría de dispositivos móviles se realiza sin agentes. Los sistemas admitidos son: Google Android, Apple iOS y Windows Phone.

Utilice **Configuration > Mobile Devices** para agregar o editar fuentes de administración de dispositivos móviles.



Captura de pantalla 7: Administración de dispositivos móviles

Los exámenes de dispositivos móviles se pueden supervisar utilizando **Monitor de actividad > Exámenes de seguridad**. Los resultados de los exámenes de dispositivos móviles se pueden ver en el panel o al generar informes. El informe de auditoría de dispositivos móviles se centra en los resultados de los exámenes de dispositivos móviles y tabletas.

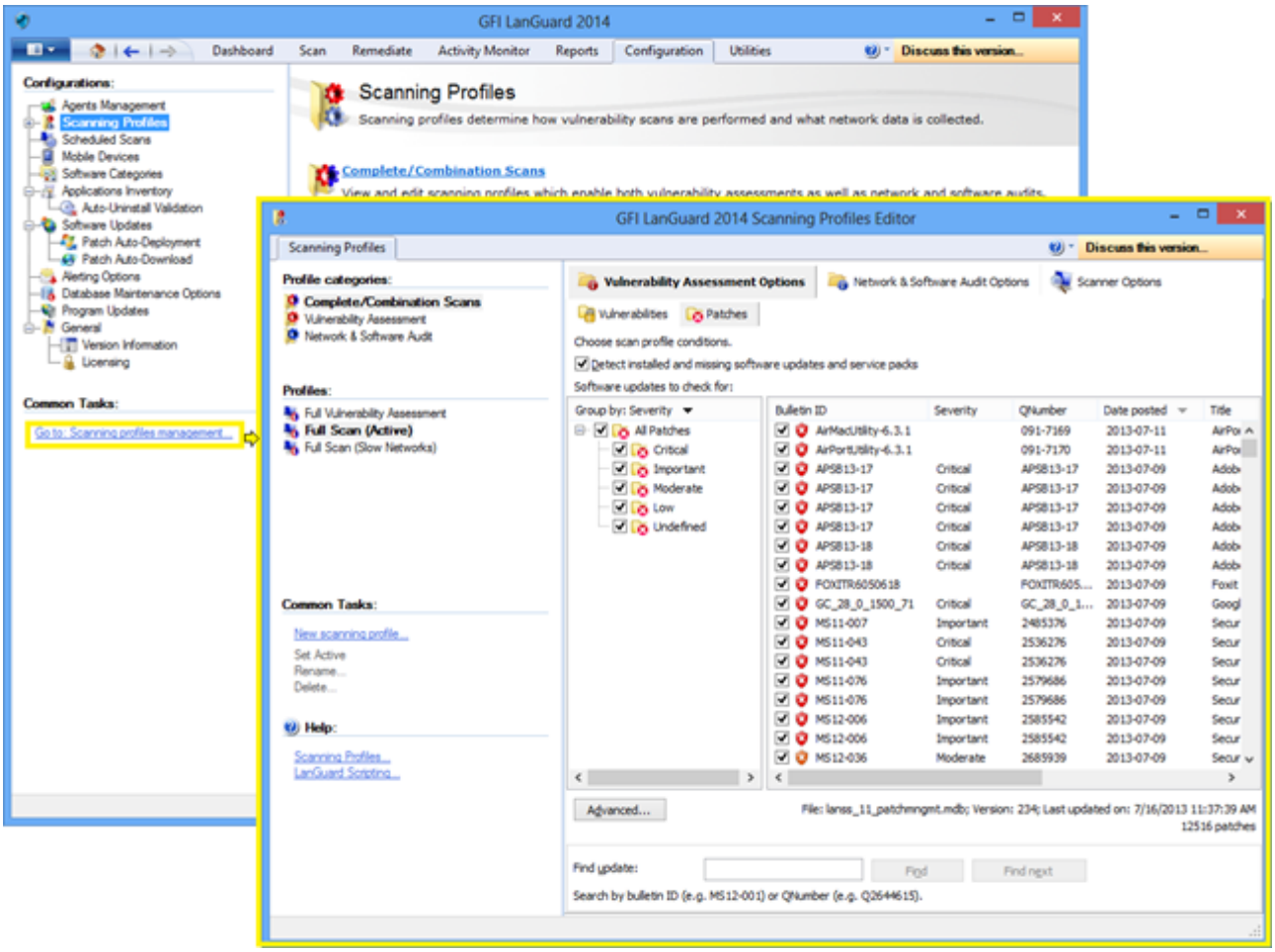
> **Nota:**
> Se pueden enviar notificaciones por correo electrónico a los propietarios de dispositivos móviles para informarles que hay actualizaciones de seguridad del sistema operativo para su dispositivo.

2.4 Perfiles de detección

Los perfiles de detección determinan la manera en que se realizan los exámenes de seguridad: los problemas de seguridad que se deben buscar y los datos de red que se deben recopilar. GFI LanGuard incluye una lista extensa de perfiles de detección predefinidos.

Para ver, modificar o crear perfiles de detección nuevos:

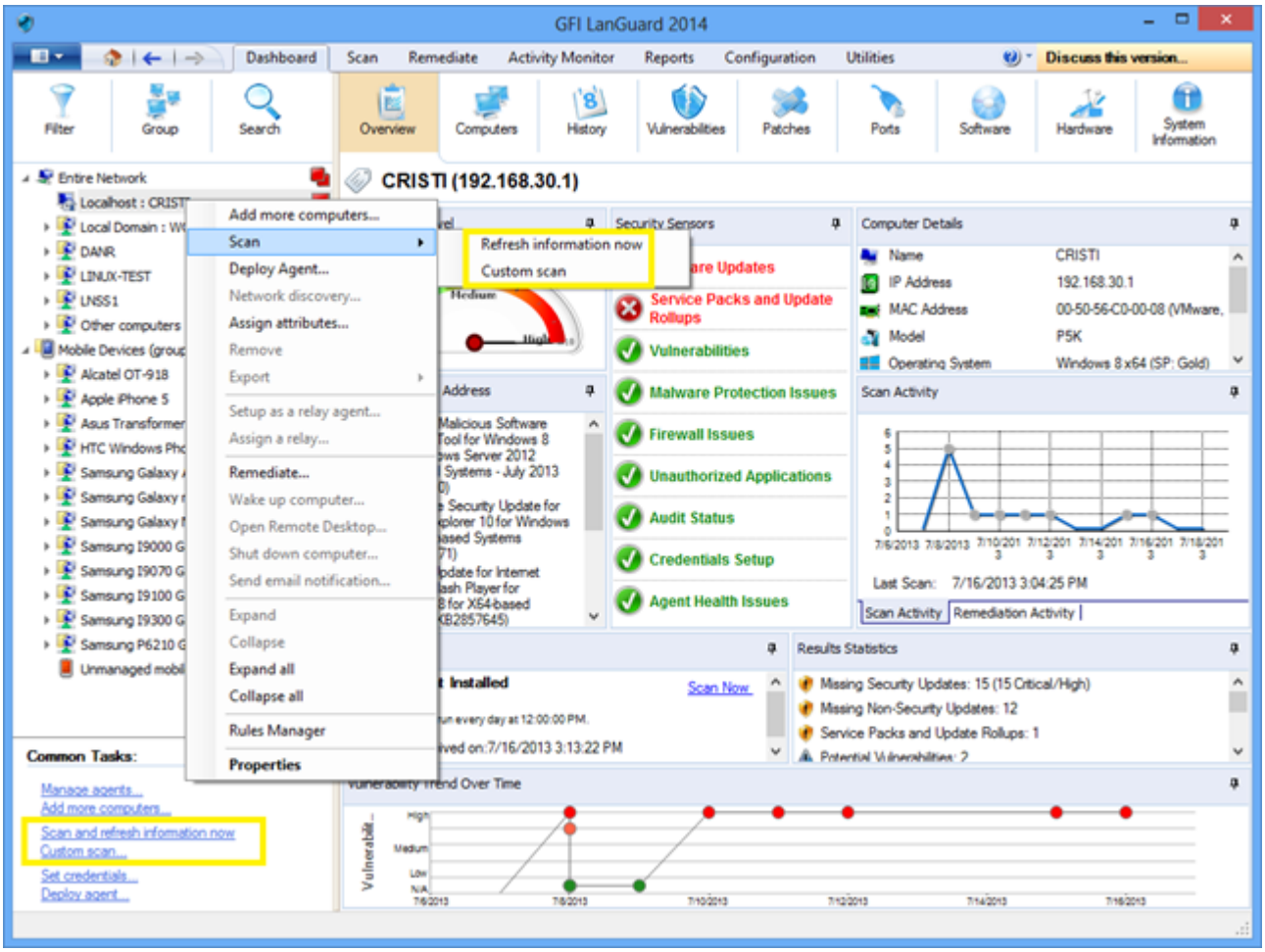
En **Configuration**, seleccione **Scanning Profiles**.



Captura de pantalla 8: Perfiles de detección

2.5 Desencadenamiento de exámenes desde el panel

Una manera sencilla de desencadenar auditorías de seguridad implica utilizar el **panel**. Simplemente seleccione la lista de equipos, dominios o unidades organizativas en el árbol de **Dashboard** y haga clic en las opciones **Scan and refresh information now** o **Custom scan** . Ambas se encuentran disponibles en el área **Common Tasks:** o haciendo clic con el botón secundario en los equipos seleccionados.



Captura de pantalla 9: Desencadenamiento de exámenes desde el panel

Característica	Descripción
Scan and refresh information now	Esta opción desencadena de forma inmediata una auditoría de seguridad que se ejecuta en segundo plano para los equipos seleccionados. En los equipos en los que el agente se instale, el examen será realizado por el agente y de acuerdo con el perfil de detección definido para el agente en cuestión. Para los equipos en los que el agente no esté disponible, se programa la ejecución de un examen sin agente en segundo plano con el perfil **Full Scan**. Utilice **Activity Monitor > Security Scans** para controlar exámenes con agentes y programados sin agentes.
Custom scan...	A través de esta opción se seleccionará la ficha **Scan** con el destino de examen previamente completado y la lista de equipos seleccionados en **Dashboard**.

3 Análisis de resultados de examen

Tema de esta sección:

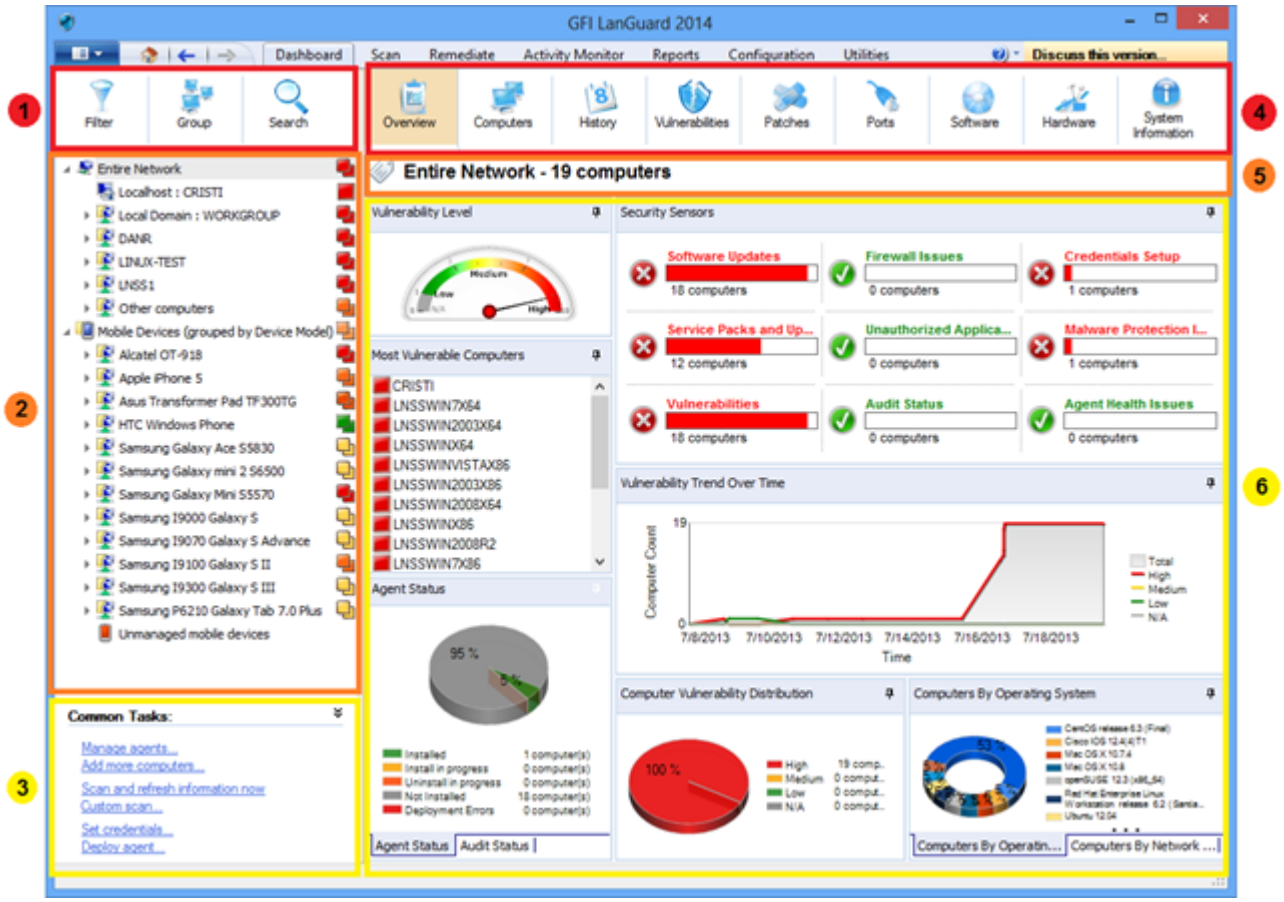
3.1 El panel

El **Panel** agrega resultados de todos los exámenes, sin importar el perfil de detección y si el examen lleva o no agente. El objetivo es mostrar al instante información general completa del estado de seguridad de la red.

En el resumen ejecutivo se muestran, entre otros aspectos, los equipos más vulnerables, los problemas de seguridad más destacados y las tendencias de vulnerabilidad. Los usuarios pueden también desplazarse hasta equipos y problemas específicos.

En el árbol de equipos del lado izquierdo, hay una lista organizada de dominios, unidades organizativas y dispositivos móviles agrupados por usuarios. Del lado derecho, en la sección Dashboard se le proporcionan varias vistas con información exhaustiva sobre según los datos adquiridos durante auditorías. Entre otras posibilidades, el panel le permite determinar el nivel de vulnerabilidad actual de la red, los equipos más vulnerables y el número de equipos de la base de datos.

- Overview,
- Computers, History,
- Vulnerabilities,
- Patches,
- Ports,
- Software y
- Hardware
- System Information.



Captura de pantalla 10: El panel

Sección	Descripción
1	En esta sección se proporciona información sobre: » cómo filtrar equipos del árbol mediante un gran número de criterios, como el sistema operativo, el nivel de vulnerabilidad, la hora del último examen, etc.; » cómo agrupar equipos por dominios y unidades organizativas, sistemas operativos u otros atributos definidos de forma personalizada. Los dispositivos móviles se pueden agrupar por usuario, sistema operativo o modelo de dispositivo. » Búsqueda de dispositivos por nombre o búsqueda de resultados de examen que contengan palabras claves específicas
2	En esta sección se proporciona información acerca de cómo ver y administrar dispositivos examinados y protegidos por GFI LanGuard: » Los servidores y las estaciones de trabajo se detallan en el nodo **Toda la red**, así como los equipos virtuales y los dispositivos de red basados en IP, como enrutadores, conmutadores, impresoras, etc. » Los teléfonos inteligentes y las tabletas que se conectan a los servidores de Microsoft Exchange de la empresa para revisar el correo electrónico de trabajo se detallan en el nodo **Dispositivos móviles**. » El icono del lado derecho del árbol indica el nivel de vulnerabilidad o si hay una auditoría en curso. » Los equipos con texto azul son equipos virtuales. » Utilice **<CTRL> + clic** para seleccionar varios equipos.
3	Esta sección permite que el usuario active acciones para los dispositivos seleccionados en el árbol.
4	Esta sección permite que el usuario seleccione diferentes vistas con estadísticas y resultados de exámenes correspondientes a los dispositivos seleccionados en el árbol.
5	Esta sección permite que el usuario vea la selección actual de dispositivos.

Sección	Descripción
6	Esta sección ofrece información acerca de cómo ver detalles de estadísticas y resultados de exámenes correspondientes a los dispositivos seleccionados en el árbol: » Los sensores de seguridad indican cuántos dispositivos se ven afectados por diferentes problemas de seguridad. » Haga clic en los sensores de seguridad o en las tablas del área Información general del panel para acceder a datos más específicos.

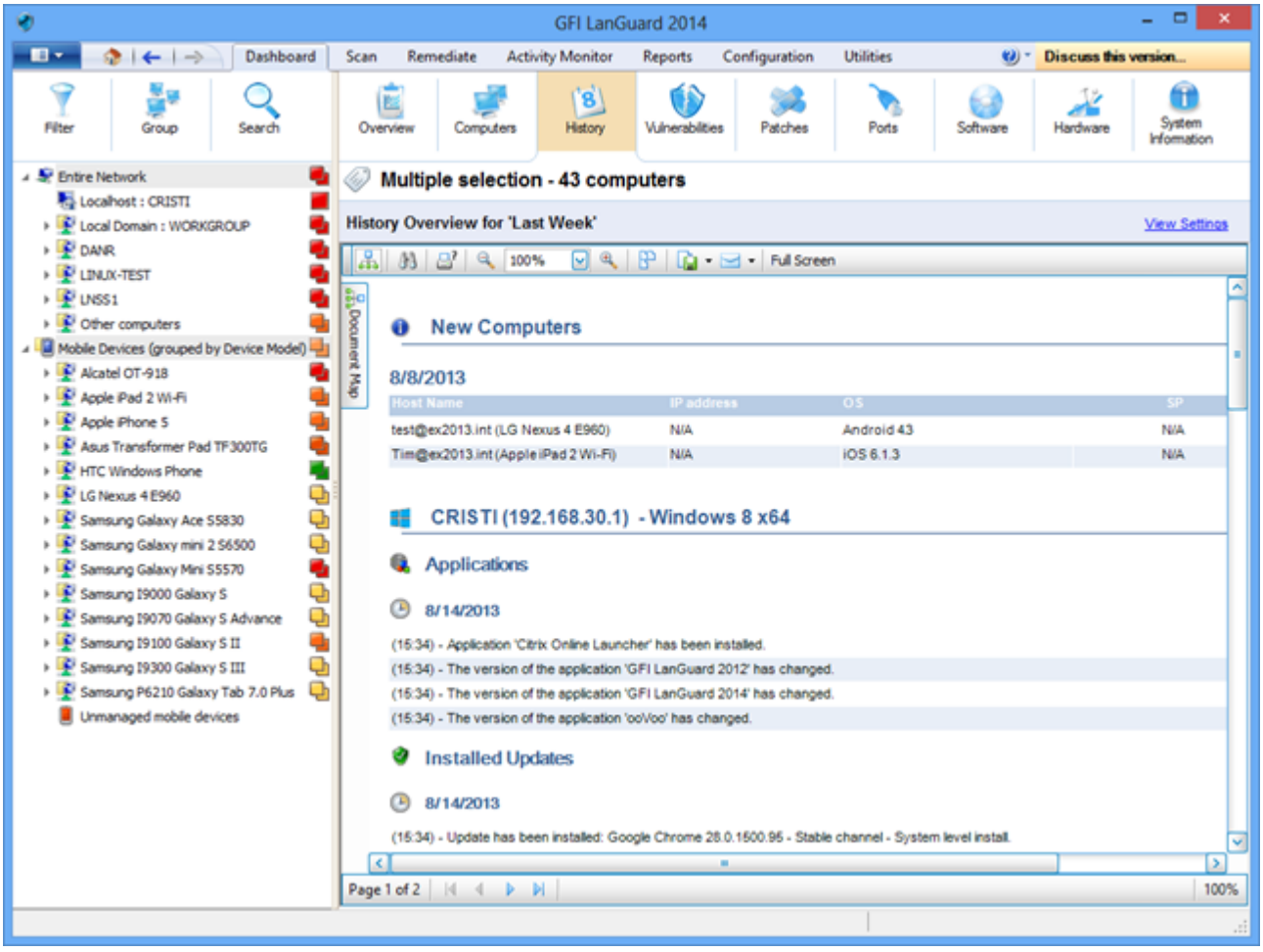
3.2 Cómo ver cambios de seguridad pertinentes en su red

GFI LanGuard notifica al usuario cuando:

- Se detectan dispositivos nuevos
- Se detectan vulnerabilidades de seguridad nuevas
- Se instalan o quitan aplicaciones
- Se inician o detienen servicios
- Se abren puertos nuevos
- Se crean nuevos recursos compartidos
- Se crean nuevos usuarios
- Se detectan cambios de hardware

Para inspeccionar cambios de seguridad pertinentes en su red:

1. Haga clic en **Dashboard > History**.



Captura de pantalla 11: Visualización de cambios de seguridad en su red

> **Nota:**
> Si se configura un destinatario de correo electrónico válido en la configuración de **Alerting options** , GFI LanGuard envía de forma predeterminada un informe de Resumen diario que contiene la vista de historial de toda la red durante las últimas 24 horas.

3.3 Cómo agregar o ver más dispositivos en el panel

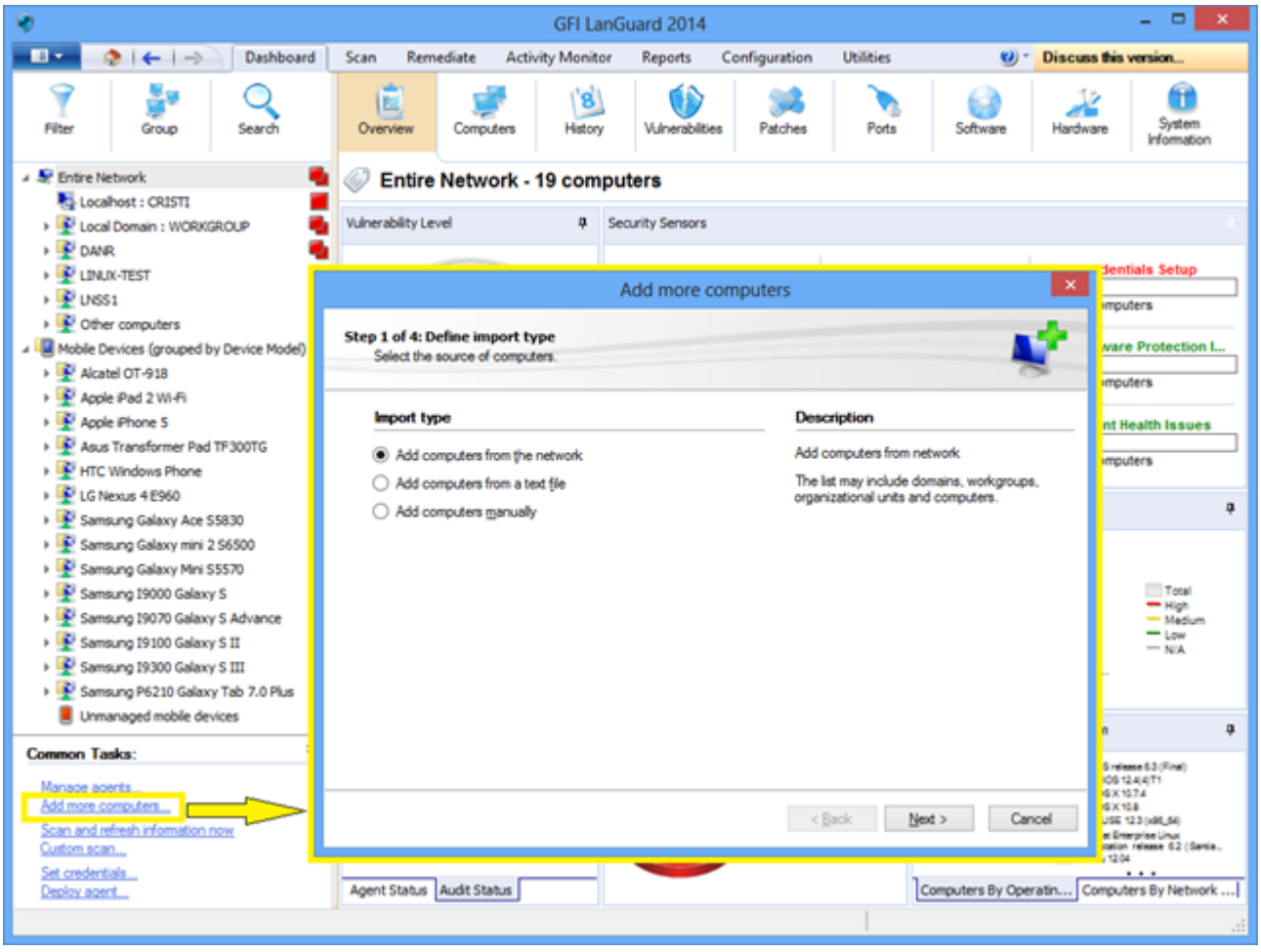
A menos que se aplique un filtro, en el árbol del panel aparecen todos los equipos administrados por GFI LanGuard. Esto significa que todos los dispositivos han sido detectados o examinados por completo por el producto.

Para visualizar los equipos en **Dashboard**, se debe realizar una de las siguientes operaciones:

1. Examine los equipos sin agentes haciendo clic en la ficha **Scan** y después en **Configuration > Scheduled Scans** o en los exámenes de líneas de comandos.

2. Habilite agentes en los equipos haciendo clic en **Configuration > Agents Management**.

3. En **Dashboard**, haga clic en **Add more computers…** en el área **Common Tasks** para agregar dominios o grupos de trabajo y unidades organizativas, o una lista de equipos específicos.

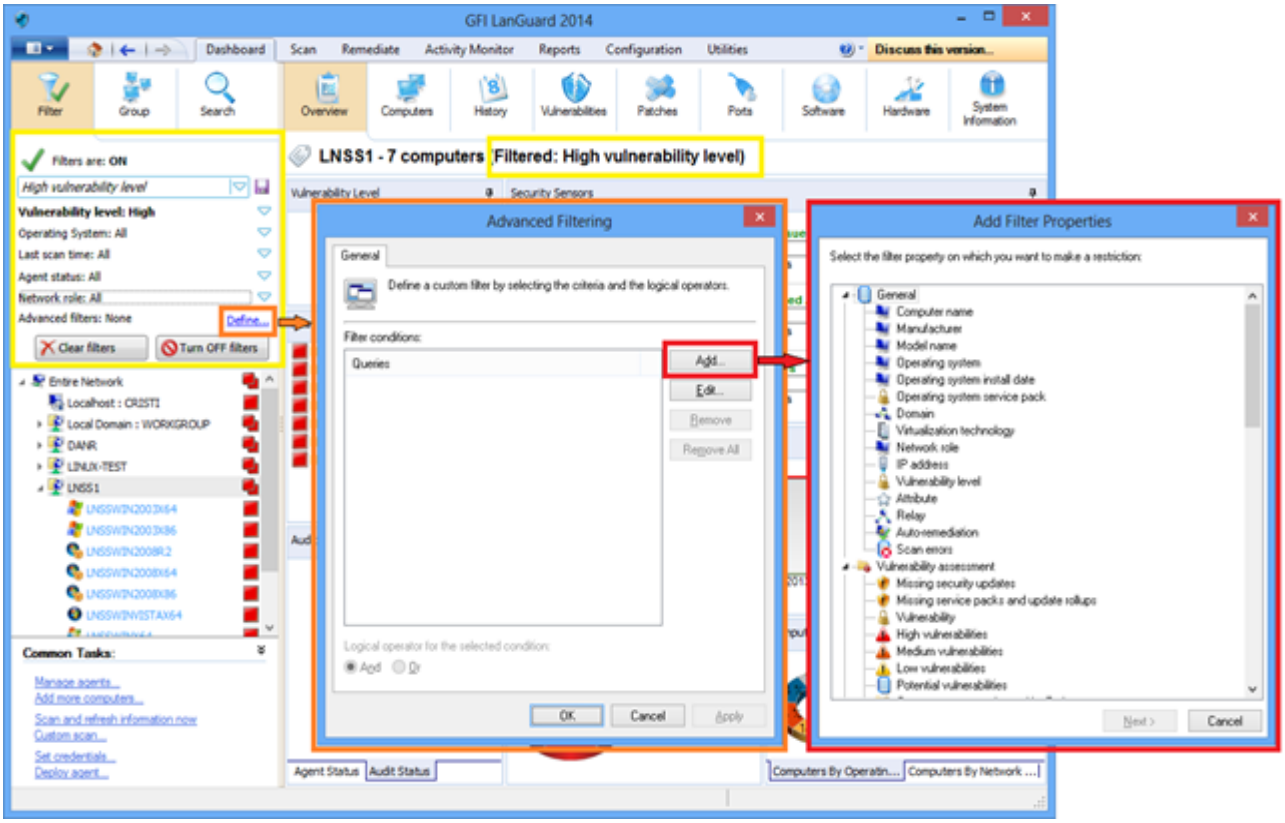


Captura de pantalla 12: Adición y visualización de equipos de equipos desde el panel

Al auditar teléfonos inteligentes y tabletas, utilice **Configuración > Dispositivos móviles** para agregar o editar fuentes de administración de dispositivos móviles (proporcionar detalles sobre los servidores de Microsoft Exchange).

3.4 Cómo filtrar dispositivos

Utilice el área de filtrado, disponible en las vistas **Panel, Corrección** e **Informes**, para filtrar qué dispositivos aparecen en el árbol del lado izquierdo de la pantalla:

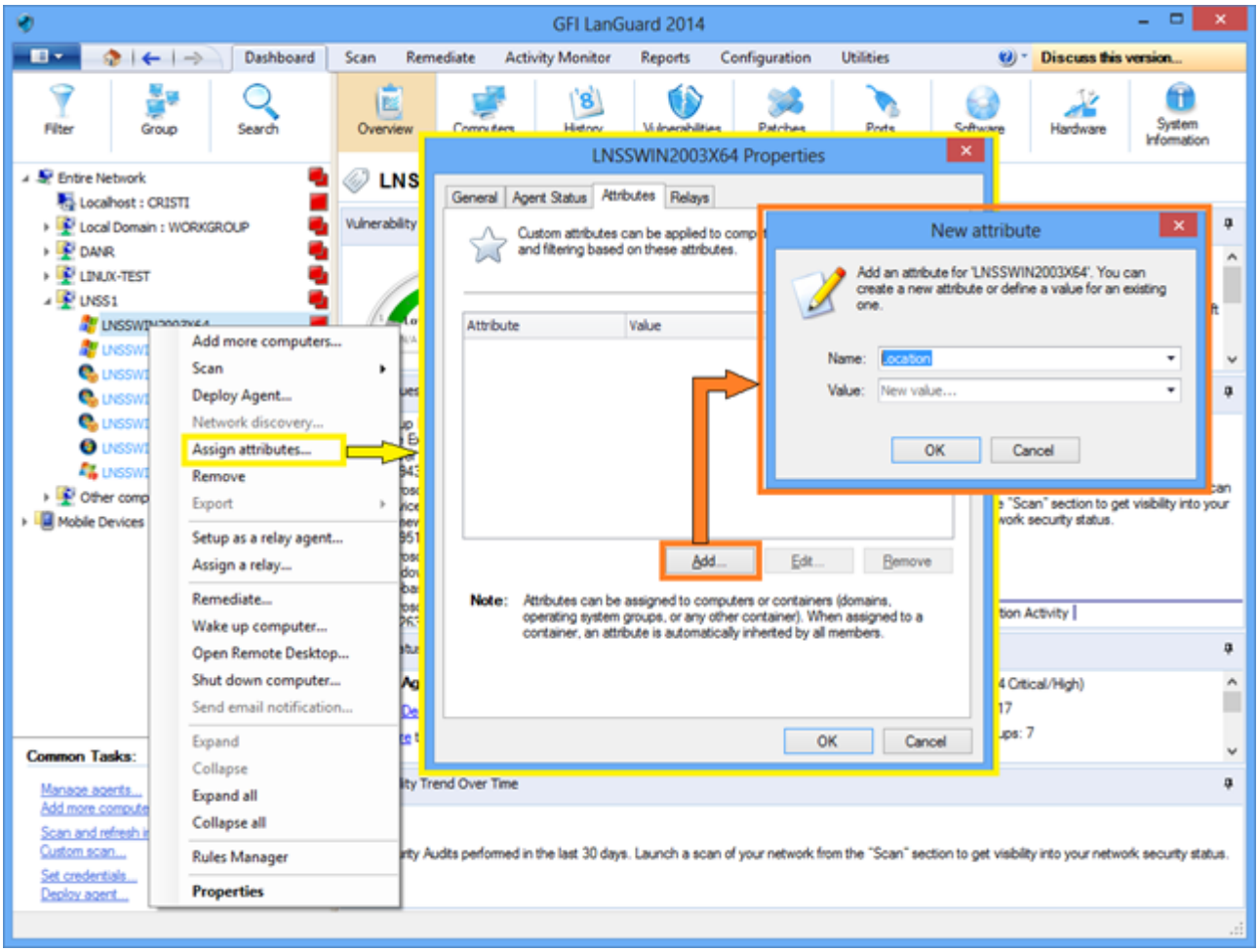


Captura de pantalla 13: Filtrado de equipos

3.5 Cómo agrupar dispositivos

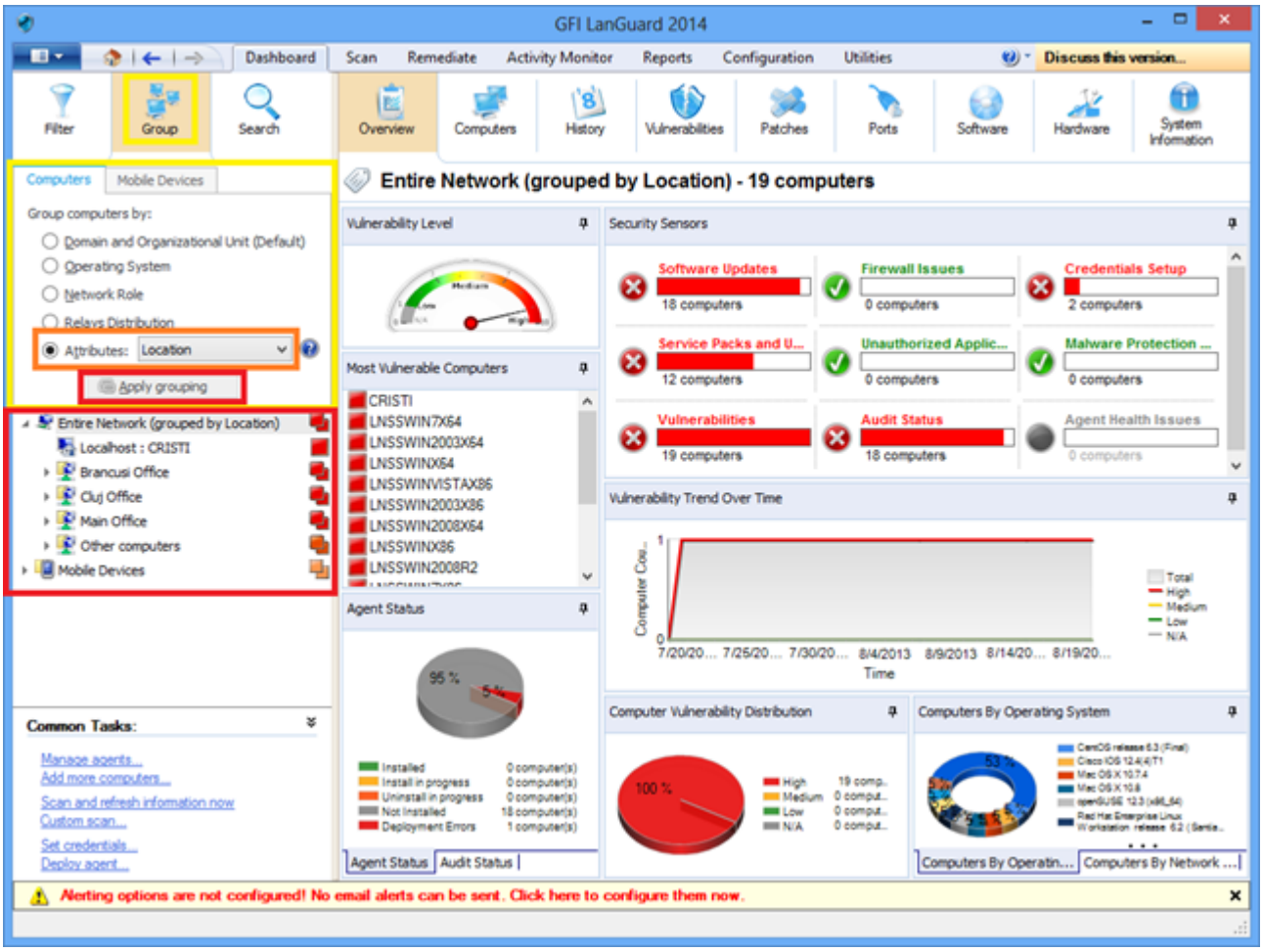
Los equipos del árbol se pueden agrupar por criterios predefinidos, como dominios y unidades organizativas (agrupación predeterminada), sistema operativo, rol de red, distribución de agentes de retransmisión o atributos personalizados definidos por los usuarios. Los dispositivos móviles se pueden agrupar por usuario (agrupación predeterminada), sistema operativo, modelo de dispositivo y atributos personalizados.

3.5.1 Definición de atributos personalizados



Captura de pantalla 14: Definición de atributos personalizados

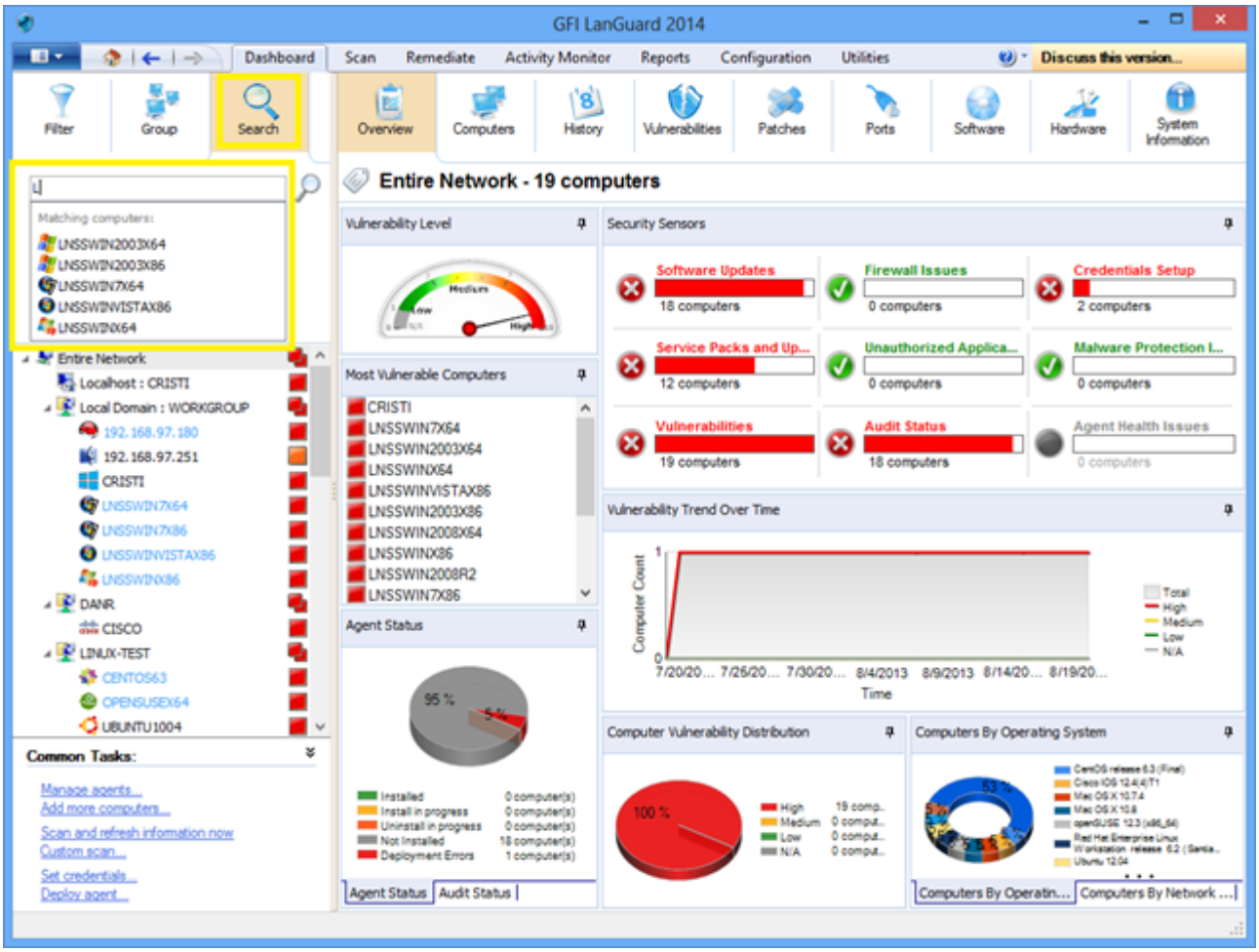
3.5.2 Visualización de equipos por atributos definidos



Captura de pantalla 15: Visualización de equipos por atributos definidos

3.6 Cómo buscar equipos

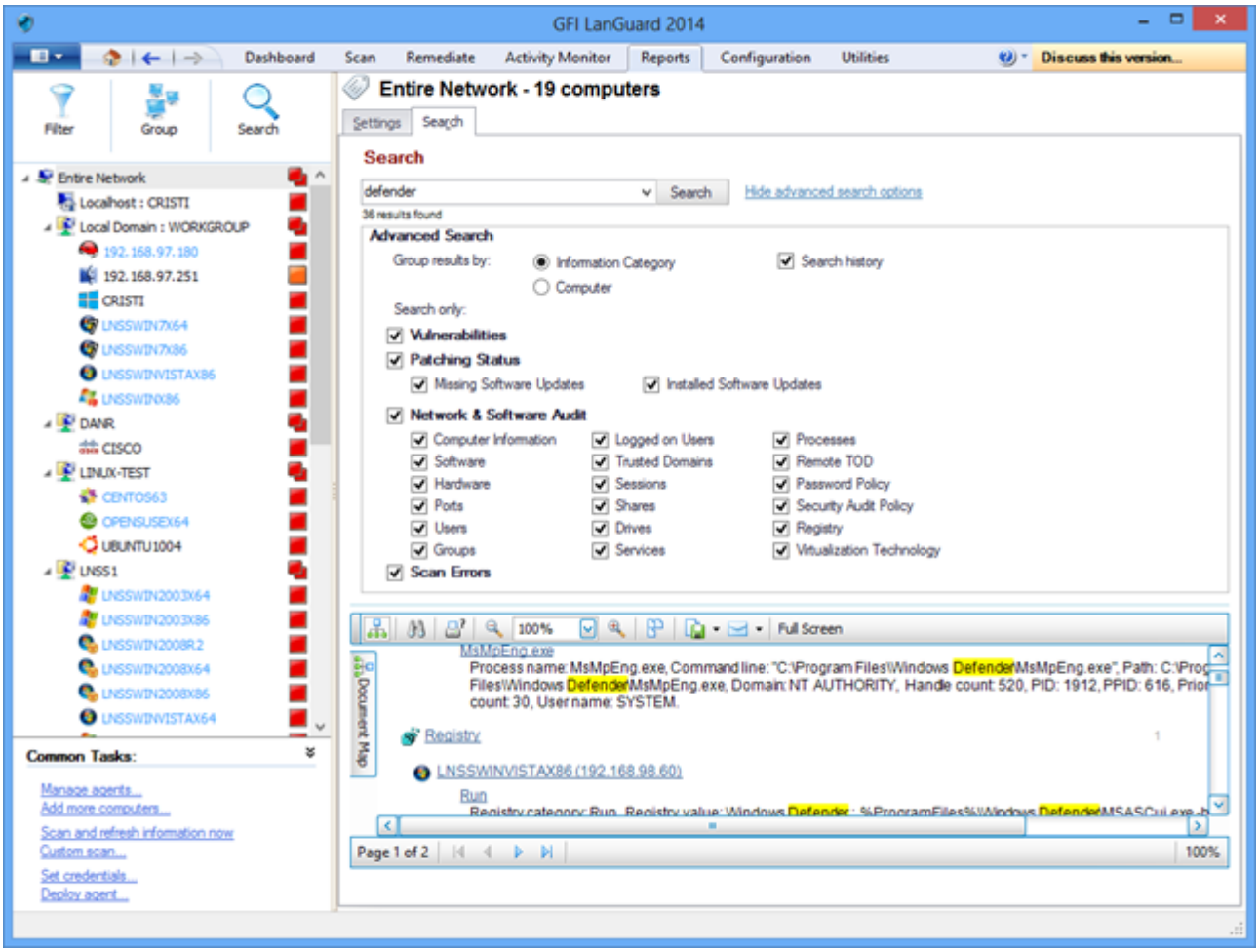
Si se administra una gran cantidad de dispositivos, la localización de estos en el árbol de equipos podría demandar tiempo. Utilice el área de búsqueda disponible en las vistas Panel, Corrección e Informes para localizar los dispositivos al instante.



Captura de pantalla 16: Búsqueda de equipos

3.7 Búsqueda de texto completo

Utilice el área de búsqueda de las vistas **Dashboard**, **Remediate** y **Reports** para ubicar la información al instante en resultados de búsqueda según palabras claves.



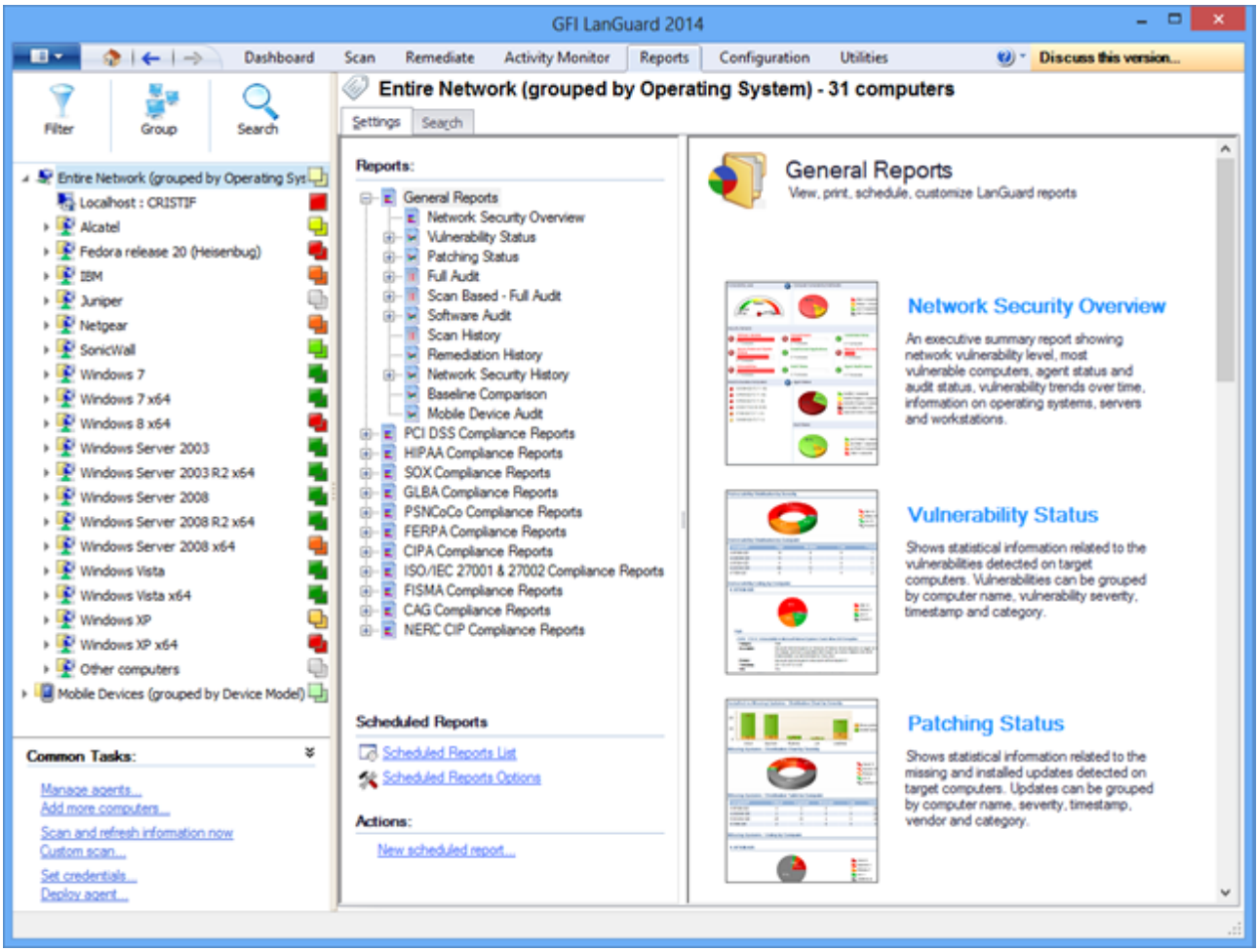
Captura de pantalla 17: Búsqueda de texto completo

Los resultados de búsqueda se pueden agrupar de acuerdo con una categoría en particular. También es posible excluir resultados hallados en otras categorías.

3.8 Generación de informes

GFI LanGuard incluye un conjunto grande de informes ejecutivos, técnicos y estadísticos predefinidos. Todos los informes se pueden personalizar, adaptar, programar para su generación regular y exportar a varios formatos populares entre los que se encuentran el PDF, el HTML, el RTF y el XLS.

A su vez,GFI LanGuard incluye un amplio conjunto de informes dedicados al cumplimiento con varios estándares y varias leyes, entre los que se incluyen PCI DSS, HIPAA, SOX, GLBA y Coco de la PSN.



Captura de pantalla 18: Generación de informes

4 Corrección de problemas de seguridad

Tema de esta sección:

4.1 Implementación de actualizaciones de software faltantes

Para implementar actualizaciones de seguridad y no de seguridad faltantes:

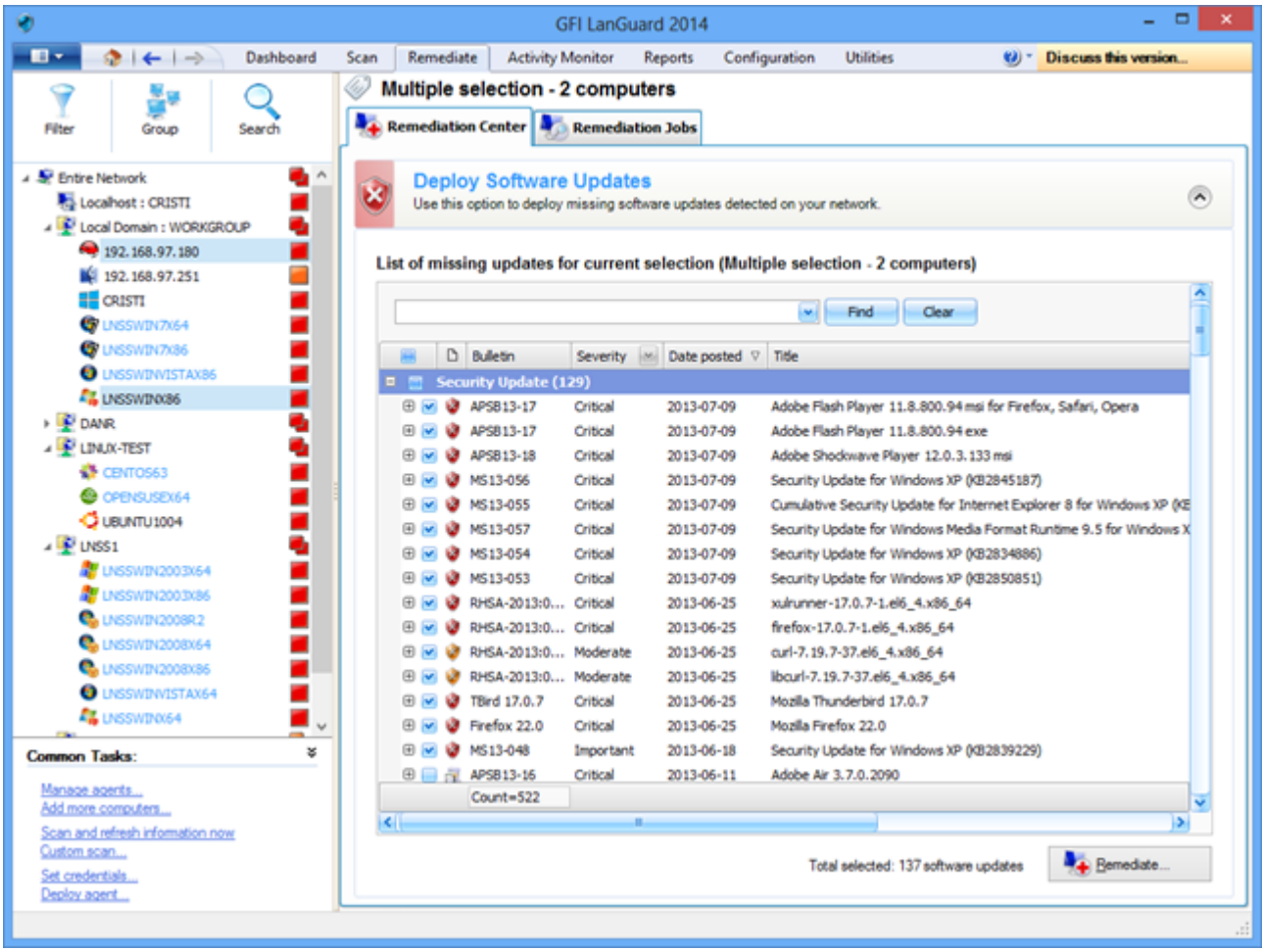
1. Haga clic en **Remediate > Remediation Center > Deploy Software Updates**

2. Seleccione los equipos o grupos de equipos en los que se deben implementar revisiones en el árbol de equipos de la parte izquierda de la pantalla.

Nota:

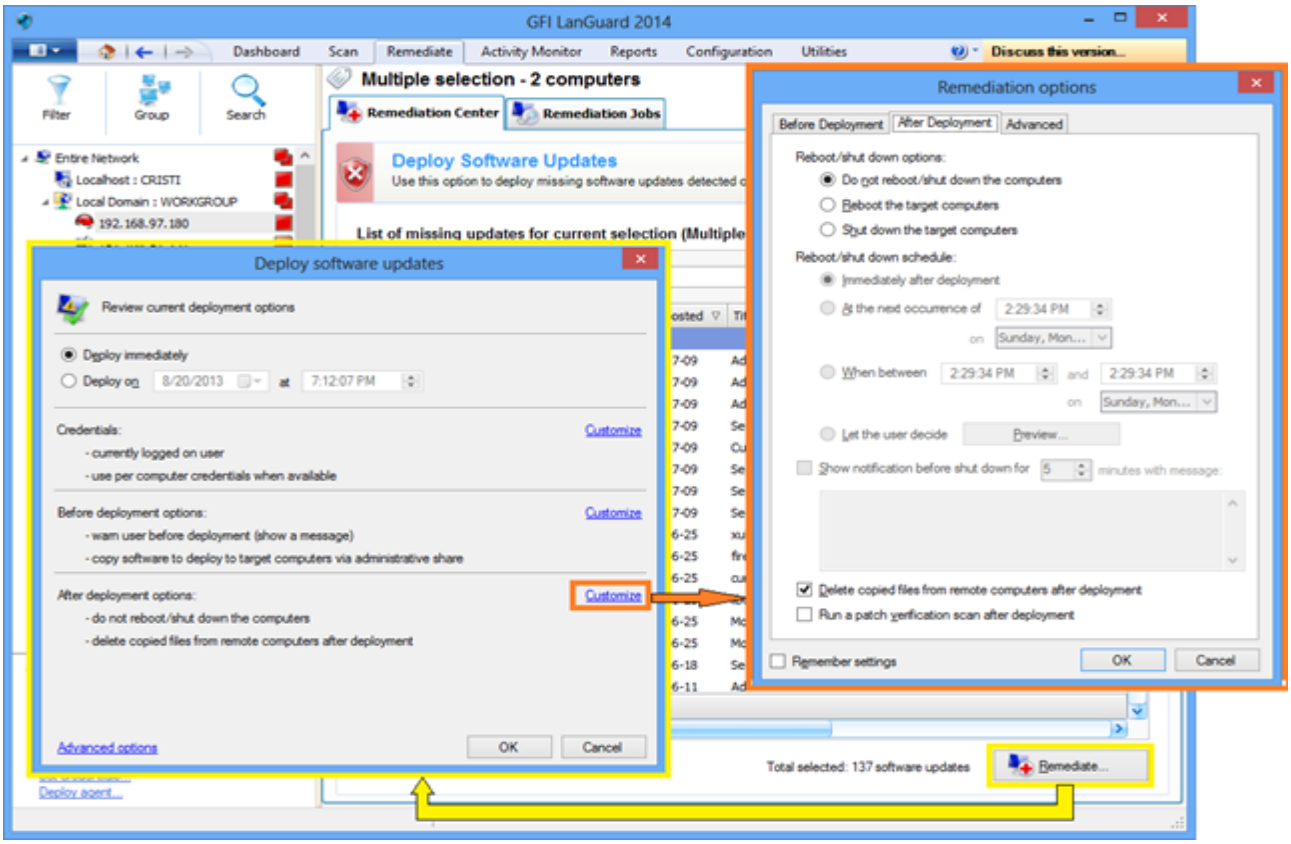
» Se pueden seleccionar varios elementos en el árbol de equipos haciendo **clic en <CTRL>**.

» Para localizar equipos de forma más sencilla en redes grandes, es posible filtrar equipos del árbol aplicando un gran número de criterios. Para obtener más información, consulte Cómo filtrar dispositivos (page 24).



Captura de pantalla 19: Implementación de actualizaciones de software

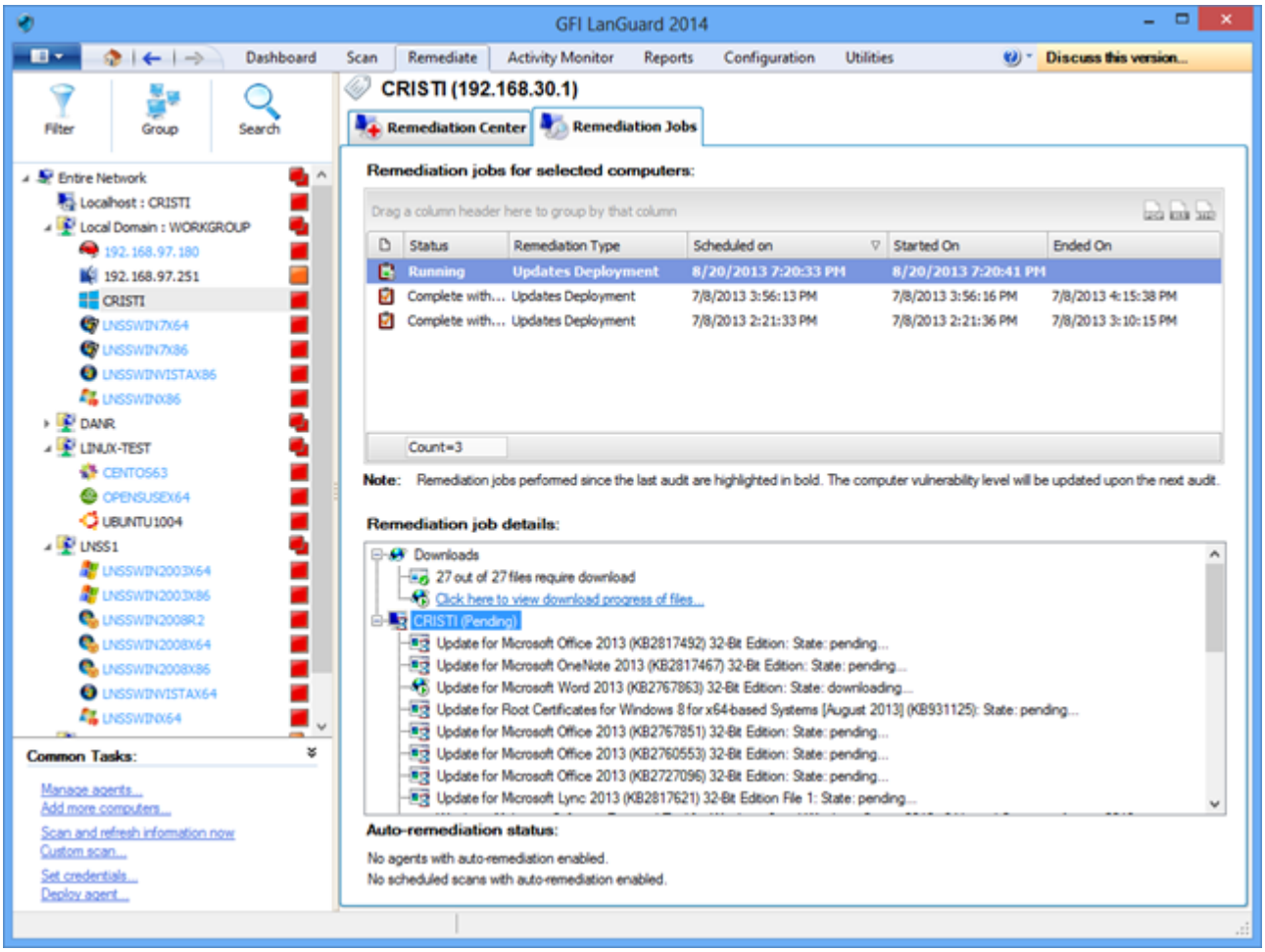
En la pantalla Deploy Software Updates puede ver todas las actualizaciones faltantes para los equipos seleccionados con detalles para cada actualización de la que carece el equipo seleccionado. Es posible ajustar la implementación seleccionando o deseleccionando revisiones o equipos.



Captura de pantalla 20: Opciones de corrección

Para iniciar la operación de implementación:

1. En **Remediate**, seleccione **Remediation Jobs**.
2. En el asistente **Deployment software options**, configure la programación de implementación
3. En el asistente **Remediation options**, seleccione las opciones de reinicio y haga clic en **OK**.



Captura de pantalla 21: Repetición de exámenes de equipos

4. Vuelva a analizar los equipos para acceder al estado de seguridad de estos una vez realizada la implementación.

> **Nota:**
>
> » Para un amplio número de actualizaciones es necesario reiniciar el equipo de destino para que la implementación se complete.
>
> » Si una actualización aún aparece como faltante después de una operación de implementación, asegúrese de que el equipo se haya reiniciado.

> **Nota:**
>
> GFI LanGuard se puede configurar para implementar de forma automática actualizaciones faltantes. Para obtener más información, consulte Automatización de operaciones de corrección (page 44).

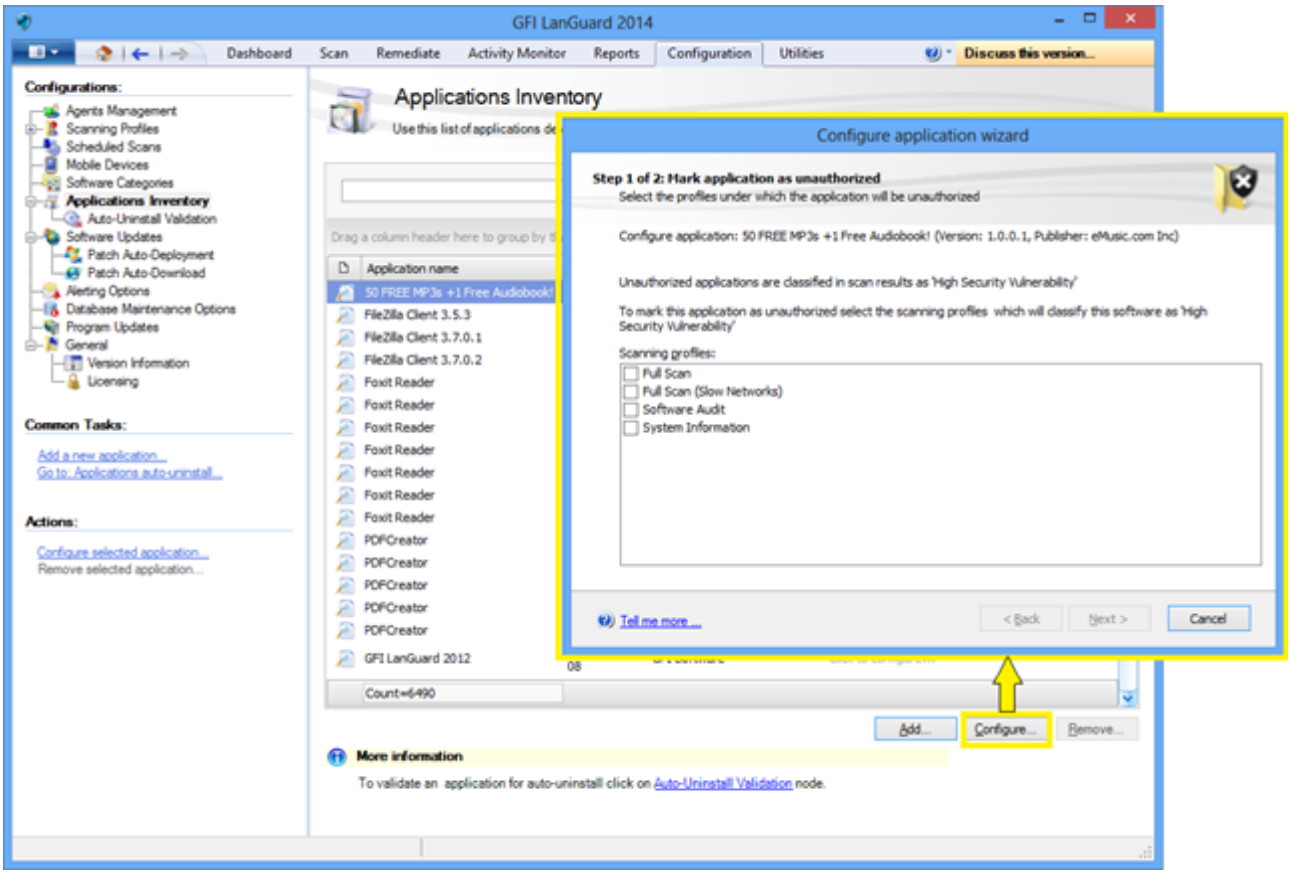
4.2 Desinstalación de aplicaciones no autorizadas

Realice una auditoría completa o una auditoría de software para obtener un inventario de aplicaciones instaladas. Para obtener más información, consulte Realización de exámenes de seguridad (page 10).

> **Nota:**
>
> Es posible agregar aplicaciones no autorizadas, aun cuando no se detectan como instaladas en la red, con el botón "Add...".

Para marcar aplicaciones no autorizadas:

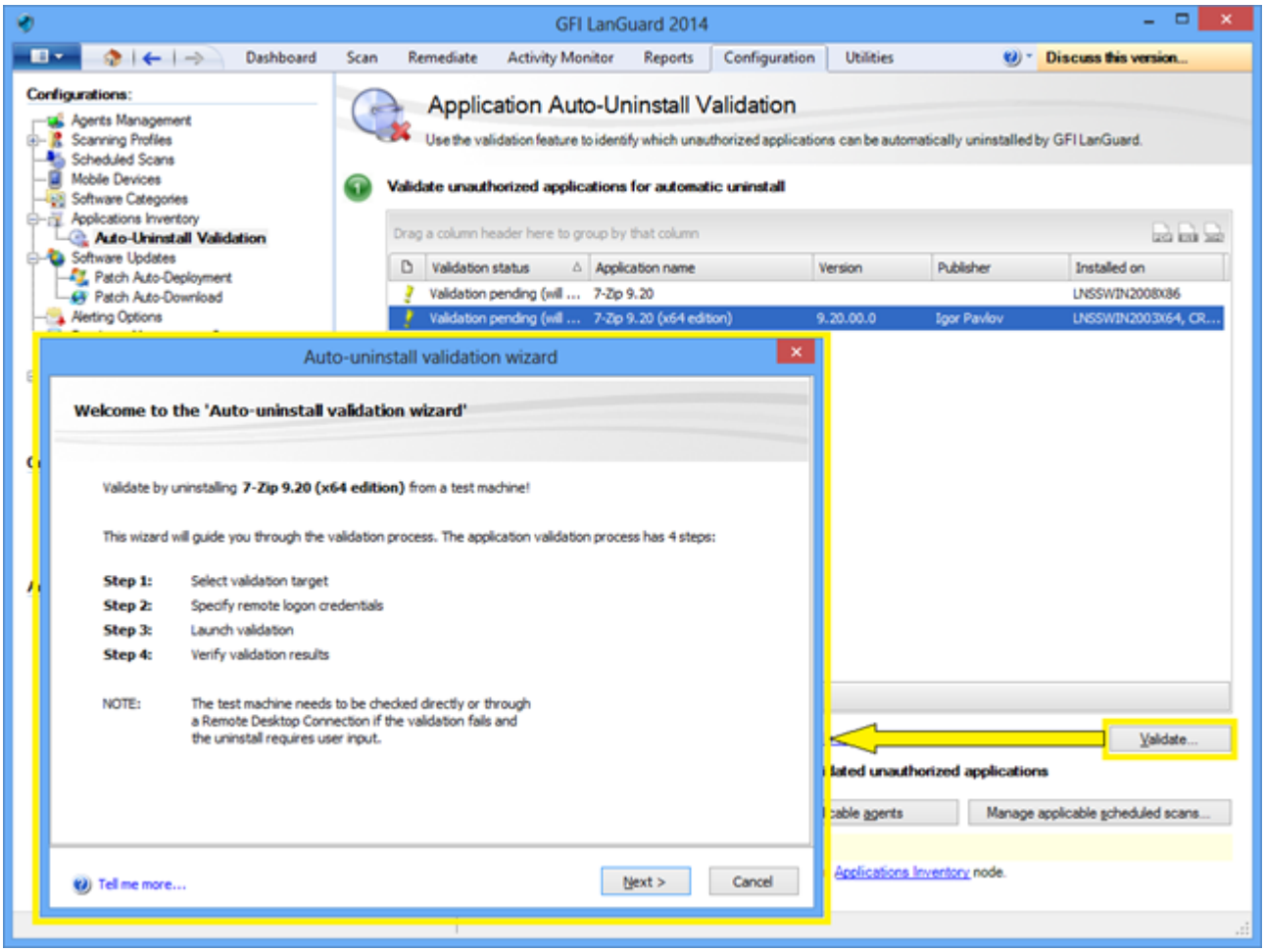
1. Haga clic en **Configuration > Applications Inventory.**



Captura de pantalla 22: Marcado de aplicaciones no autorizadas

2. Utilice **Configuration > Auto-Uninstall Validation** para verificar si GFI LanGuard puede desinstalar con éxito una aplicación no autorizada de forma silenciosa.

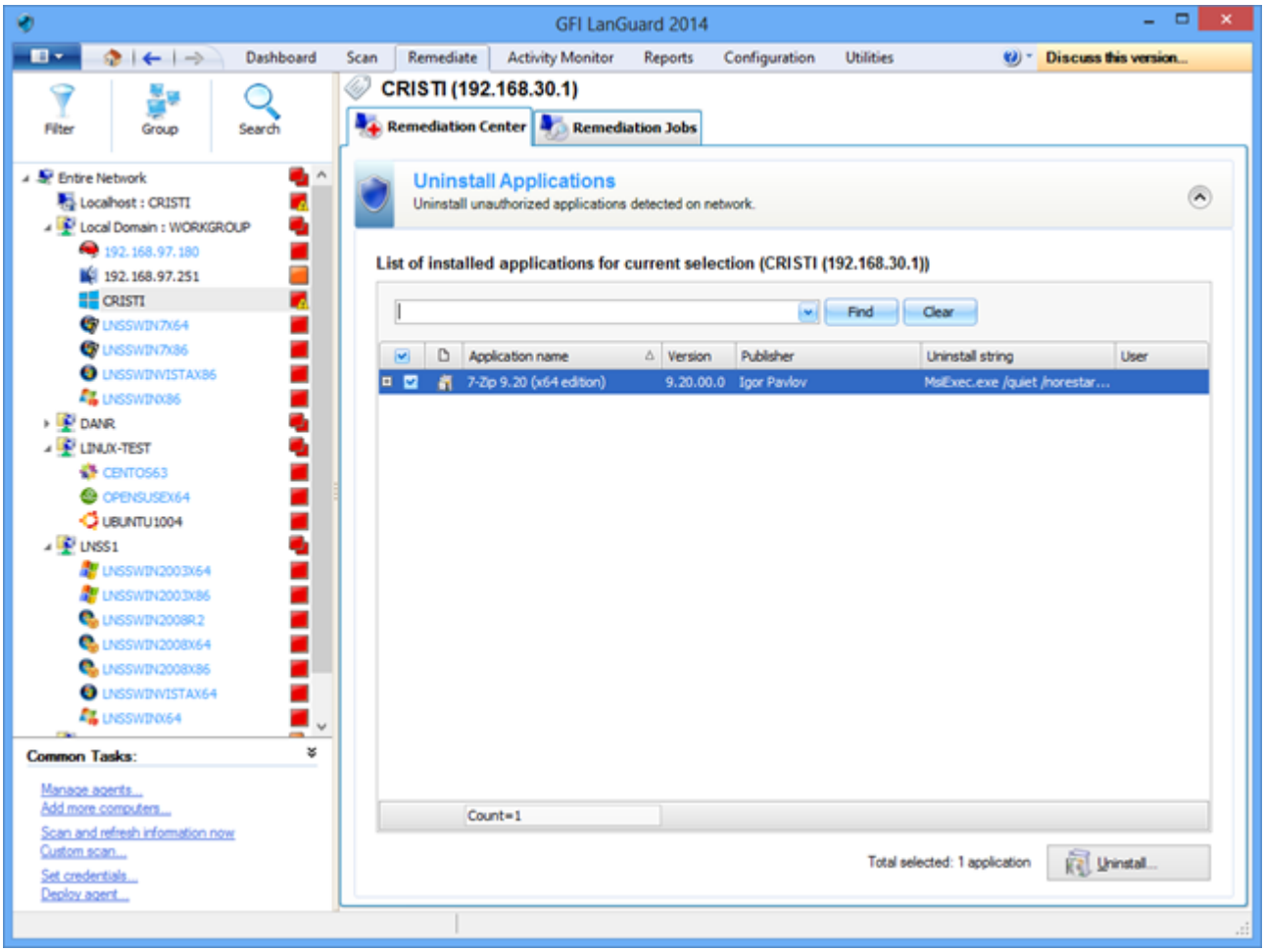
> **Nota:**
> Algunas aplicaciones no admiten la instalación silenciosa y no se pueden quitar a través de GFI LanGuardporque el proceso de desinstalación muestra a los usuarios finales de los equipos de destino cuadros de diálogo que requieren la intervención de estos e interfieren con su trabajo.



Captura de pantalla 23: Validación de la desinstalación automática de aplicaciones

3. Vuelva a examinar su red para detectar todas las aplicaciones no autorizadas.

4. Utilice **Remediate > Remediation Center > Uninstall Applications** para quitar aplicaciones no autorizadas de su red



Captura de pantalla 24: Desinstalación de aplicaciones

5. Vuelva a analizar los equipos para acceder al estado de seguridad de estos una vez realizada la desinstalación.

> **Nota:**
> GFI LanGuard se puede configurar para detectar aplicaciones no autorizadas y quitarlas de su red de forma automática. Para obtener más información, consulte Automatización de operaciones de corrección (page 44).

4.3 Implementación de software personalizado

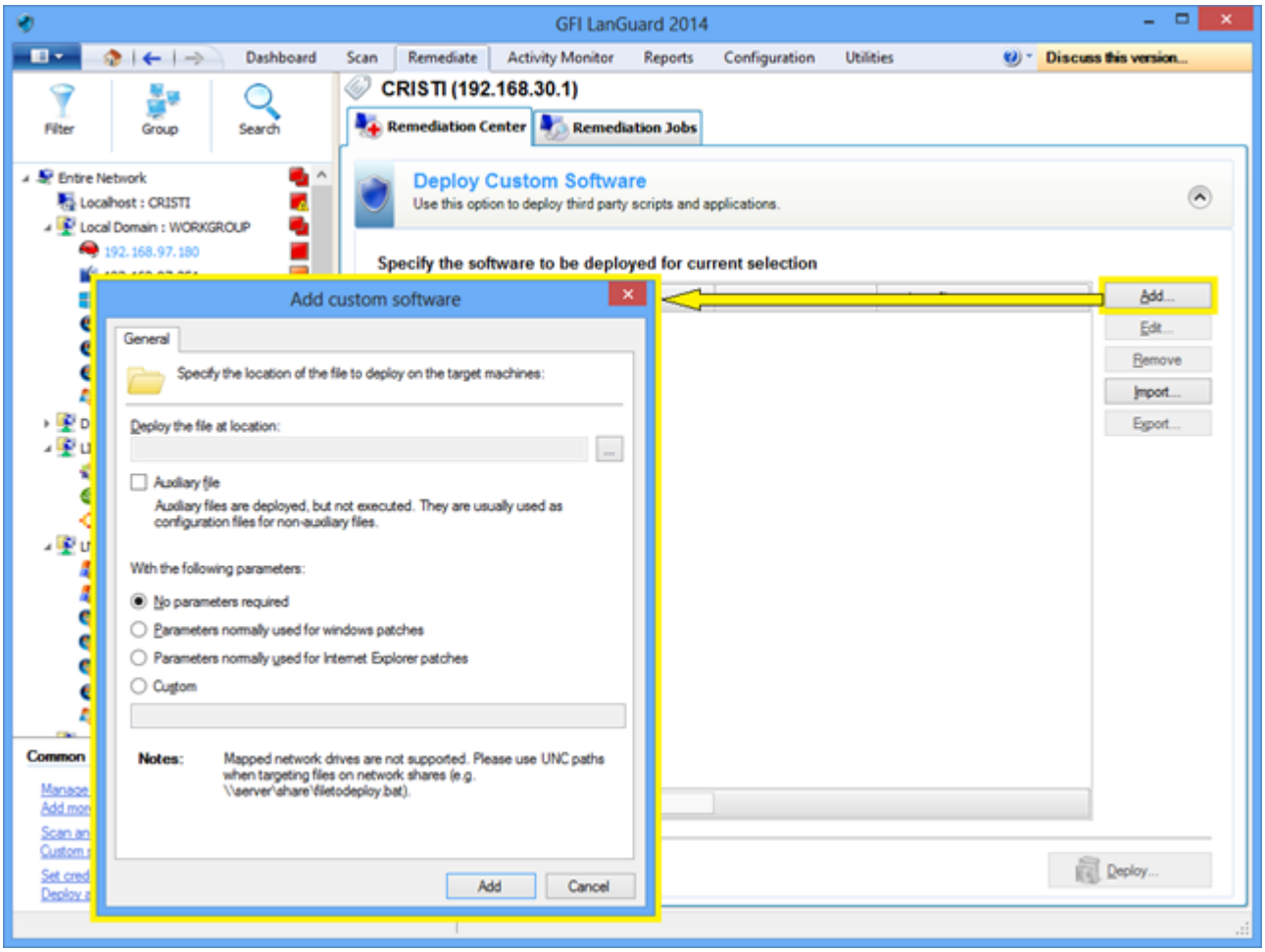
GFI LanGuard puede implementar software y scripts personalizados en toda la red. Prácticamente, cualquier software que pueda funcionar de forma silenciosa se puede implementar utilizando GFI LanGuard.

Para implementar software y scripts personalizados en su red:

1. Haga clic en **Remediate > Remediation Center > Deploy Custom Software**

2. Seleccione los equipos o grupos de equipos en los que se deben implementar revisiones en el árbol de equipos de la parte izquierda de la pantalla.

> **Nota:**
> El software personalizado se debe especificar de forma manual, junto con los parámetros de instalación silenciosa y los archivos de configuración, si es necesario.

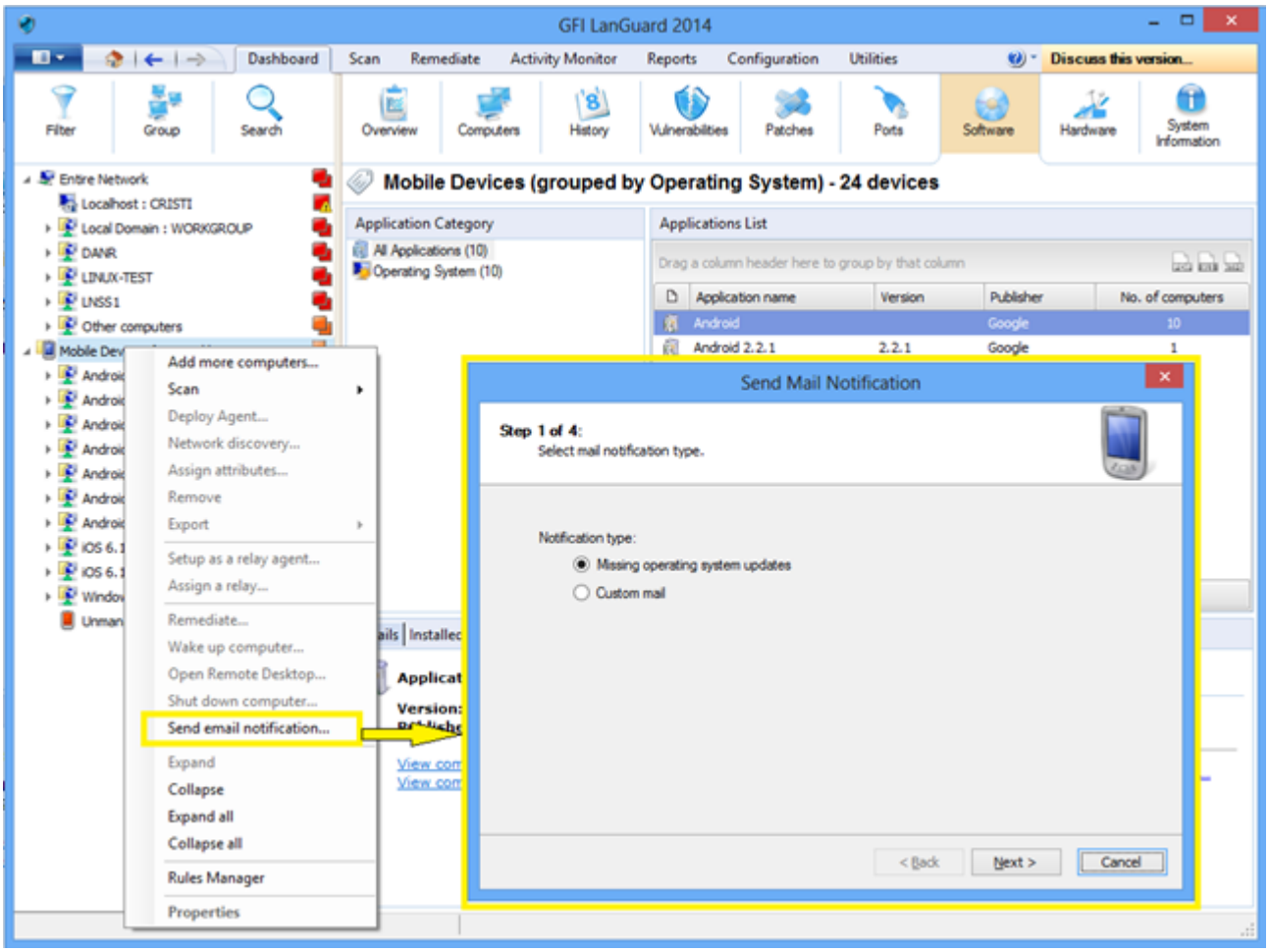


Captura de pantalla 25: Implementación de software personalizado

4.4 Envíe notificaciones por correo electrónico a los propietarios de dispositivos móviles

Los administradores de TI pueden utilizar GFI LanGuard para enviar notificaciones personalizadas por correo electrónico a los propietarios de teléfonos inteligentes y tabletas que se conectan a los servicios de la empresa, como Microsoft Exchange, Office 365, Google Apps y Apple Profiles Manager. Se puede usar una plantilla predefinida de correo electrónico para notificar a los propietarios de dispositivos sobre las actualizaciones más recientes del sistema operativo instalado en sus dispositivos.

Haga clic con el botón secundario en un dispositivo móvil o un grupo de dispositivos móviles en el árbol del panel y seleccione la opción **Enviar notificación por correo electrónico** para enviar mensajes de correo electrónico a los propietarios de dispositivos móviles.



Captura de pantalla 26: Envío de notificaciones por correo electrónico

4.5 Otras operaciones de corrección

Para ver todas las operaciones de corrección disponibles en GFI LanGuard:

1. En **Remediate**, seleccione **Remediation Center**

GFI LanGuard permite operaciones de corrección como las siguientes:

» Rollback patches: esta opción es muy importante cuando se han instalado actualizaciones de seguridad que interfieren con su entorno empresarial

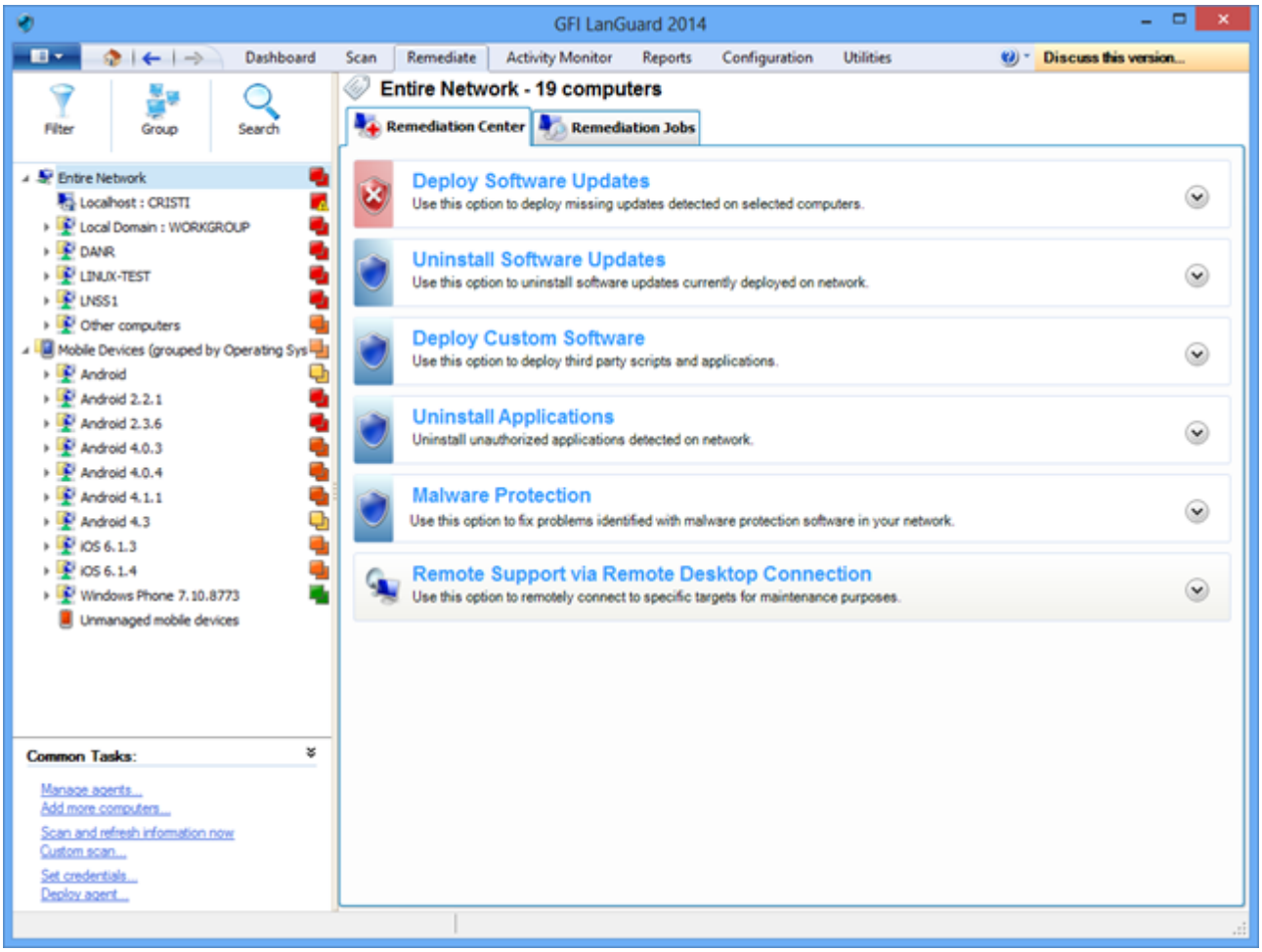
» Desencadenamiento de actualizaciones de definiciones para software antivirus y antispyware

» Desencadenamiento de exámenes de antivirus y antispyware en los equipos remotos

» Habilitación de protección en tiempo real para soluciones antivirus y antispyware

» Activación de cortafuegos

» Apertura de una conexión a escritorio remoto en los equipos de destino para resolver de forma rápida problemas de seguridad que no se pueden solucionar automáticamente



Captura de pantalla 27: Otras operaciones de corrección

5 Automatización de tareas

Tema de esta sección:

5.1 Detección automática de nuevos dispositivos en la red

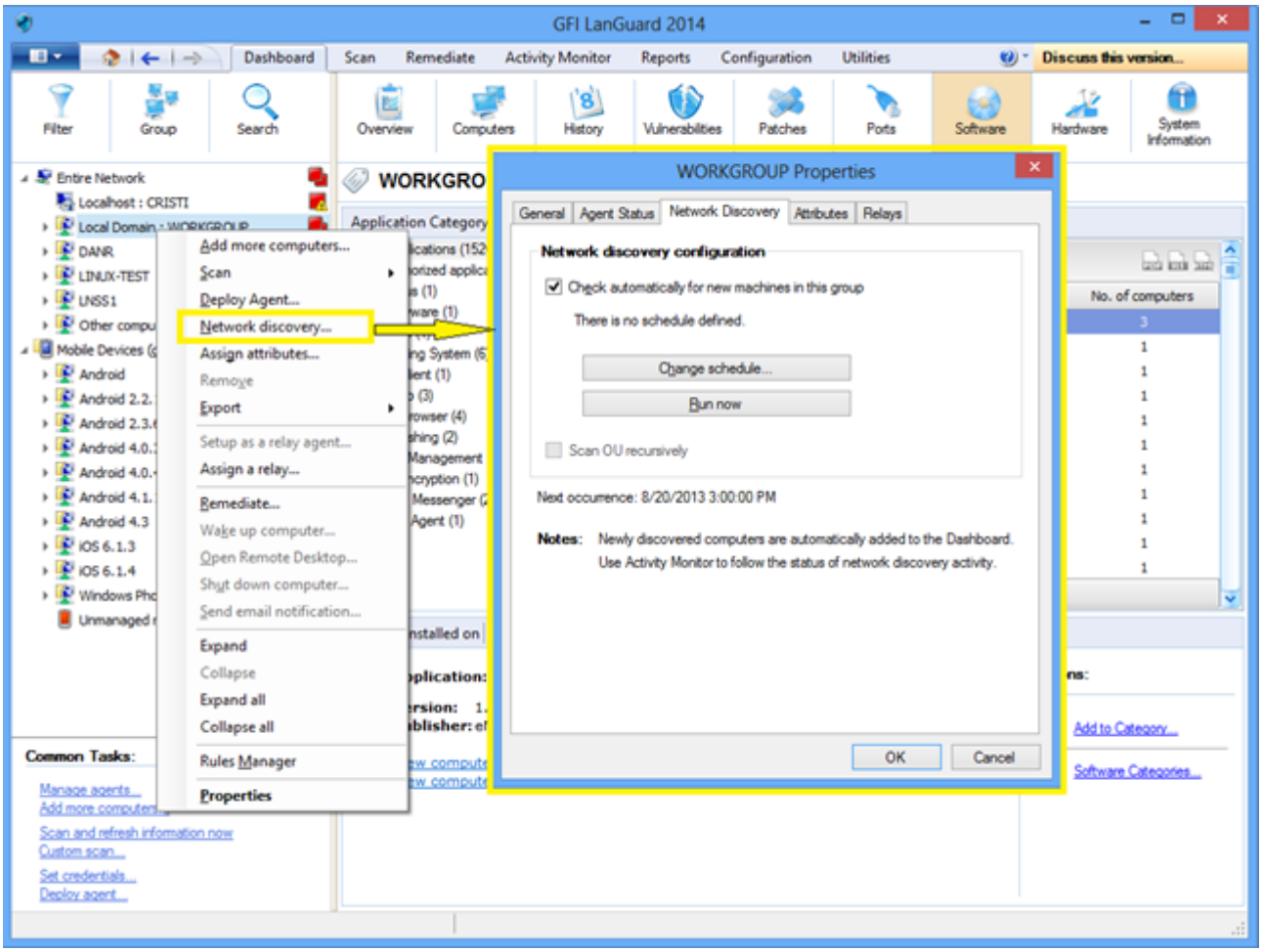
Nota:

» Todas las tareas importantes de GFI LanGuard se pueden configurar para ejecutarse de forma automática con regularidad.

» Para controlar dispositivos nuevos conectados a la red, programe la ejecución regular de un examen en el perfil Network Discovery.

Para detectar de forma automática el momento en que los nuevos equipos se agregan a una unidad organizativa o un dominio determinados:

1. En **Dashboard**, haga clic con el botón secundario en el dominio o la unidad organizativa en el árbol de equipos y seleccione **Network Discovery**…



Captura de pantalla 28: Detección de dispositivos

2. En **Dashboard**, seleccione **History** para determinar qué dispositivos nuevos se detectaron en la red y el momento en que se detectaron por primera vez.

> **Nota:**
> Una vez que se define una fuente de administración de dispositivos móviles, los dispositivos móviles nuevos se detectan automáticamente en forma periódica. Para obtener más información, consulte la sección Auditoría de teléfonos inteligentes y tabletas.

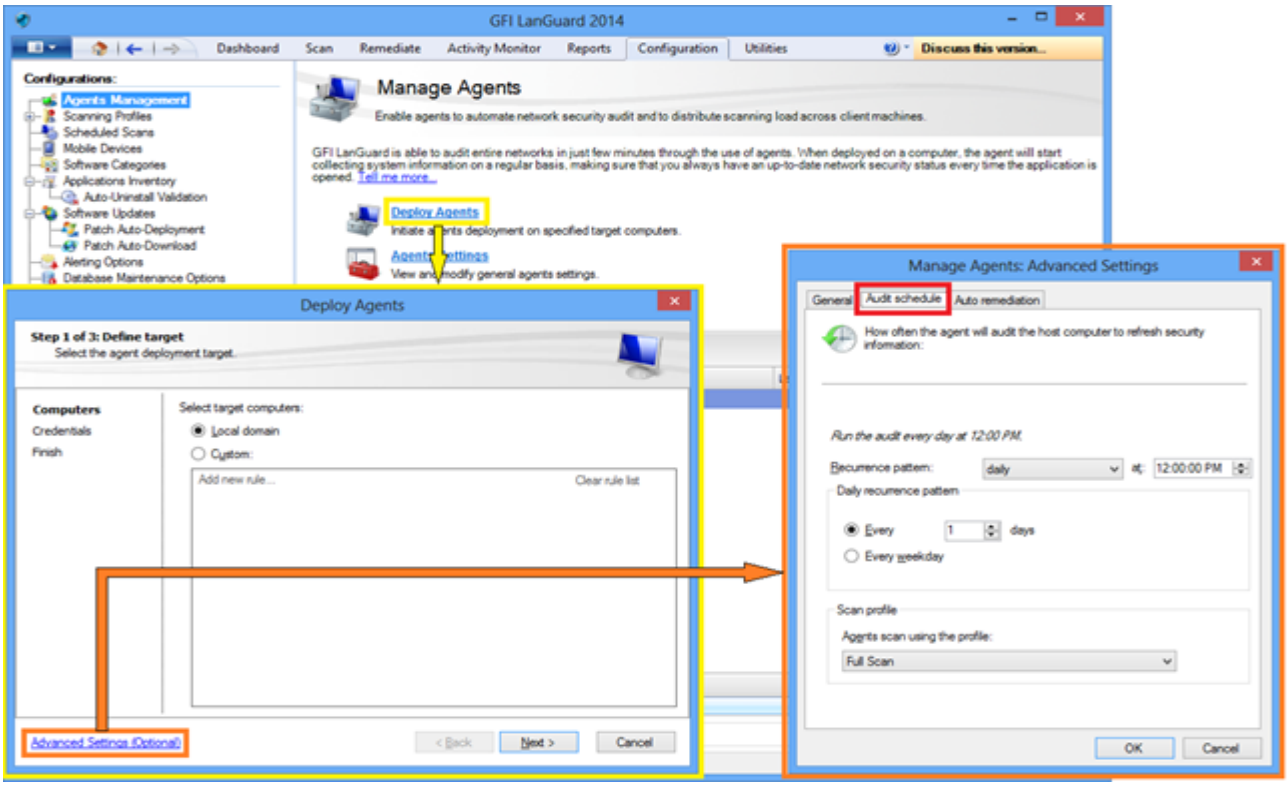
5.2 Automatización de auditorías de seguridad

Las auditorías de seguridad se pueden automatizar de dos maneras:

1. Configurar la ejecución regular en segundo plano de exámenes programados sin agentes

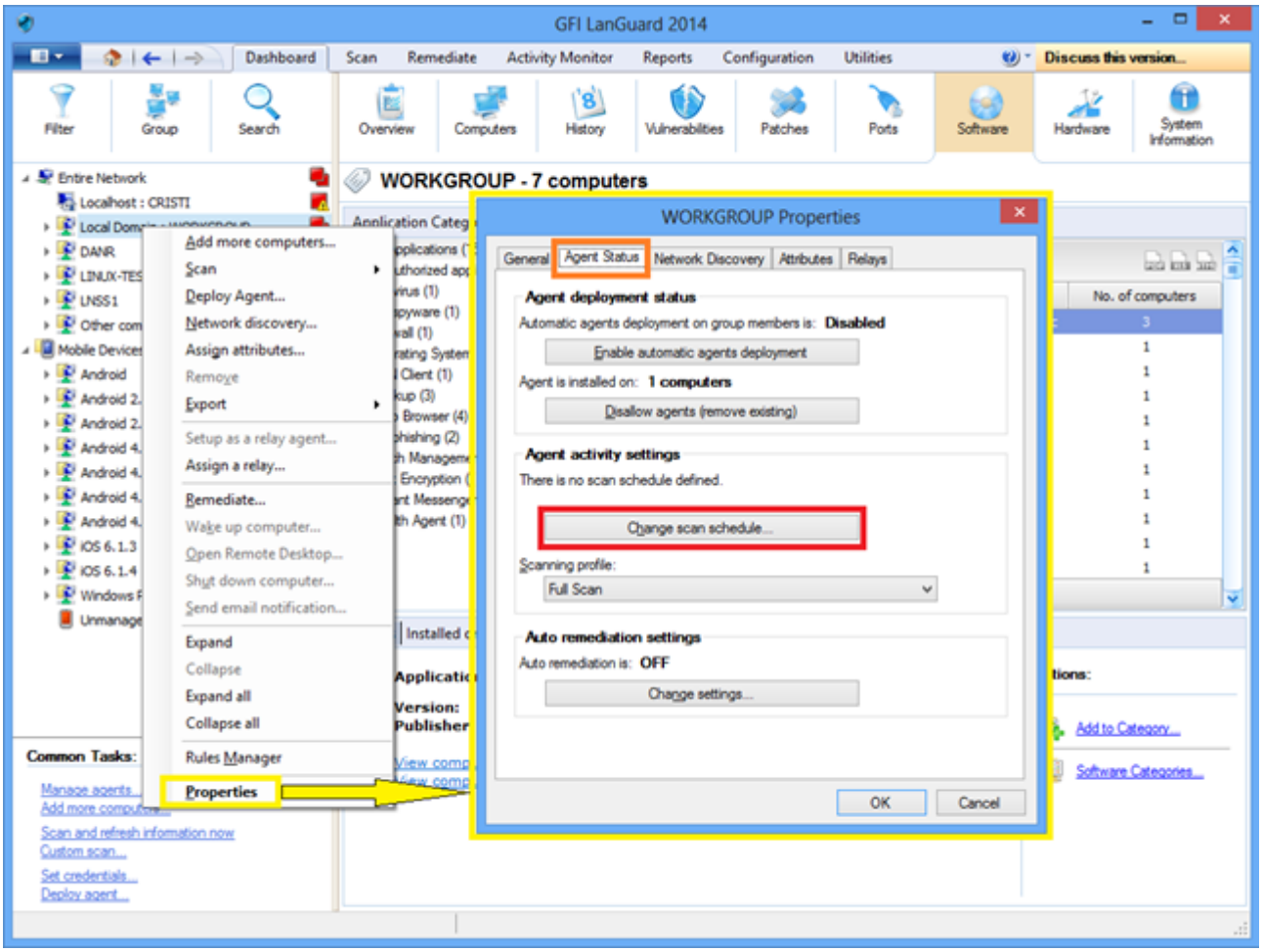
2. Implementar agentes en los equipos de destino. De forma predeterminada, los agentes someten a auditoría el equipo host una vez al día, pero la programación de auditoría se puede personalizar.

5.2.1 Personalización de la programación de auditoría al aplicar agentes



Captura de pantalla 29: Personalización de la programación de auditoría: Implementación de agentes

5.2.2 Personalización de la programación de auditoría para agentes mediante el panel

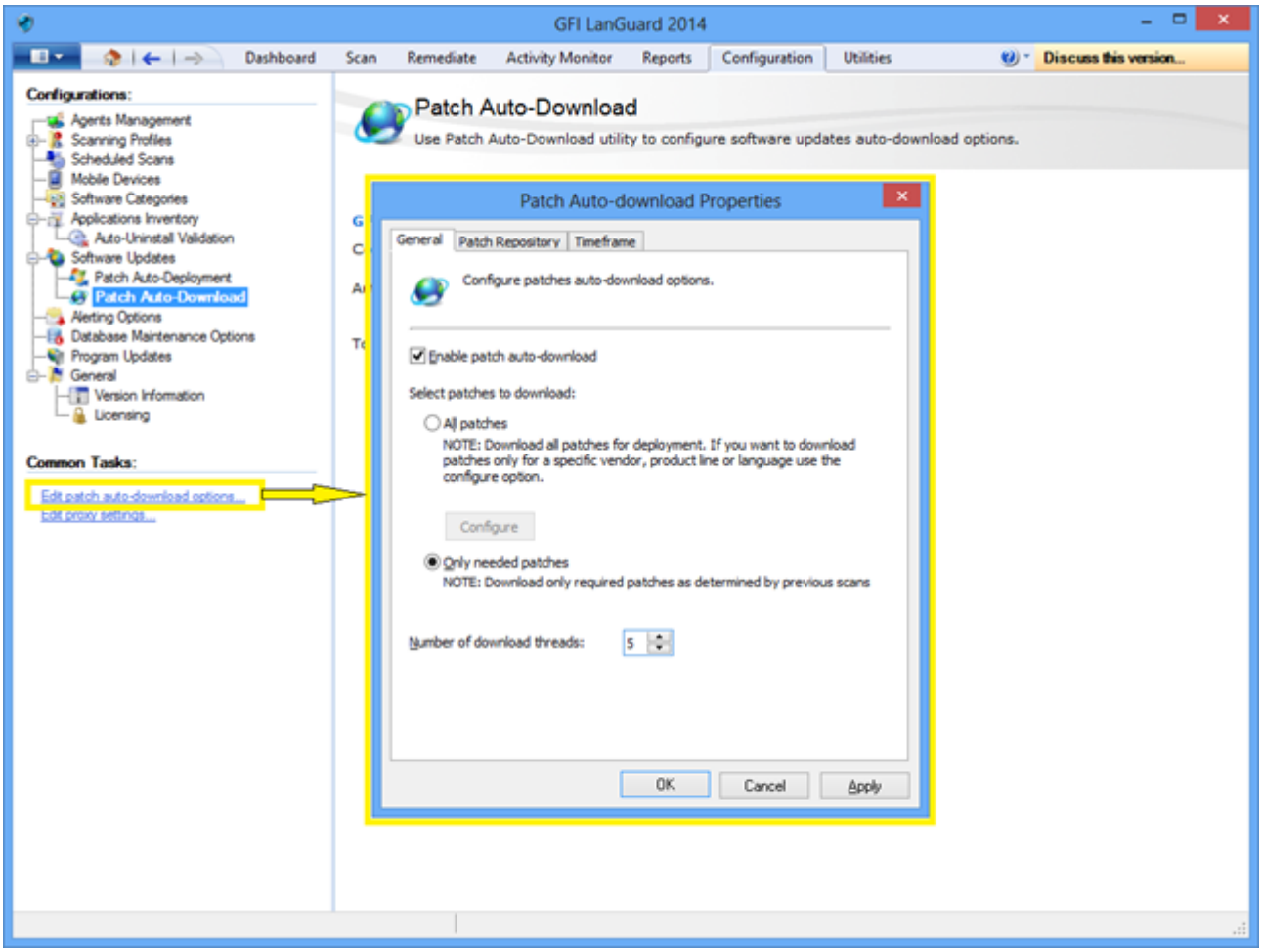


Captura de pantalla 30: Personalización de la programación de auditoría: Utilización del panel

5.3 Automatización de la descarga de revisiones

Utilice Configuration > Patch Auto-Download para configurar el producto de manera tal que descargue actualizaciones automáticamente, a fin de que estas estén disponibles cuando se inicie la implementación. Las opciones disponibles son las siguientes:

- Auto-download all patches
- Auto-download only patches detected as missing by GFI LanGuard
- Auto-download patches for specific vendors, products or languages



Captura de pantalla 31: Automatización de la descarga de revisiones

5.4 Automatización de operaciones de corrección

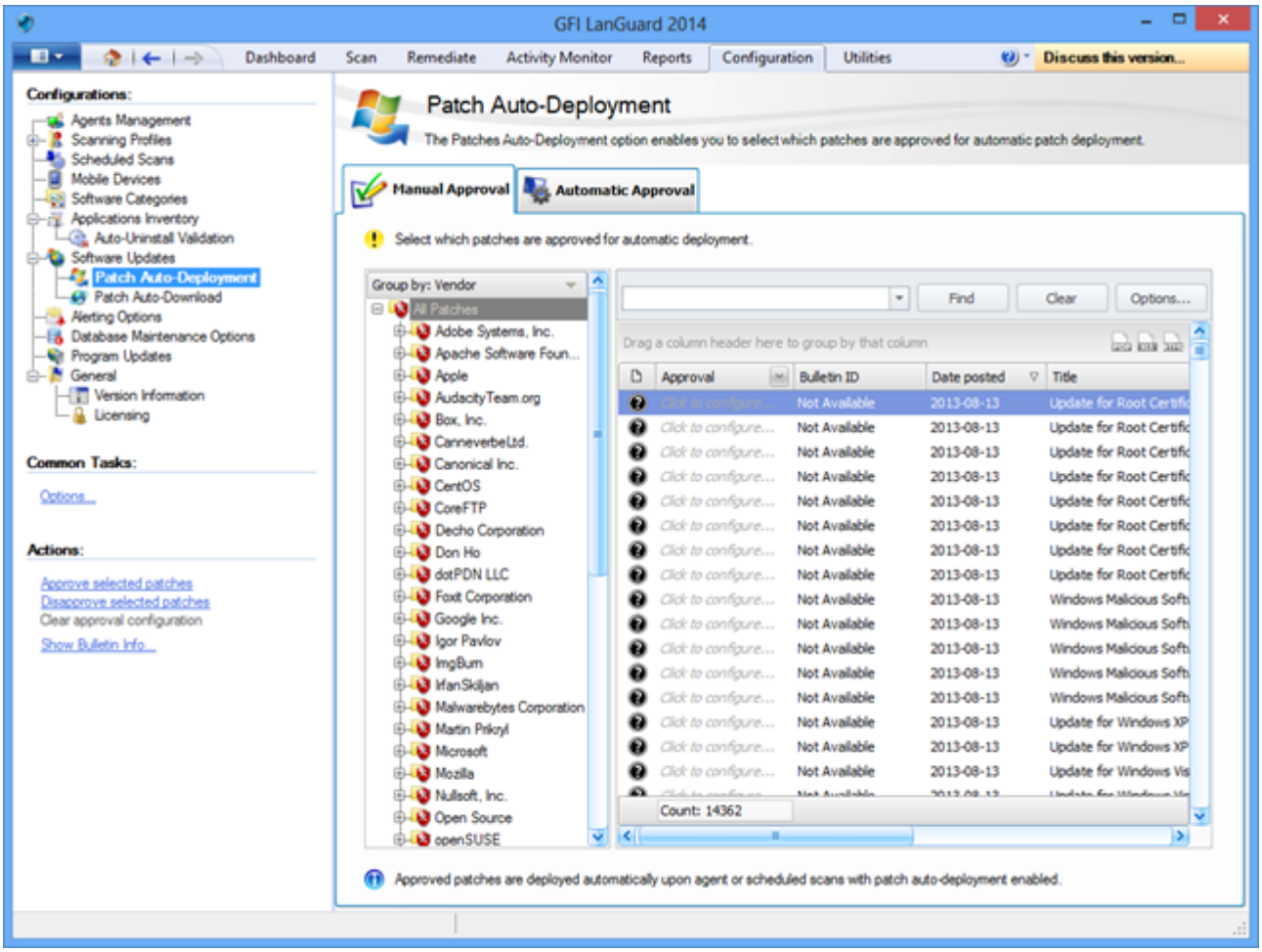
GFI LanGuard se puede configurar para corregir de forma automática determinados aspectos de seguridad, como la implementación de actualizaciones y la desinstalación de aplicaciones no autorizadas a medida que estas se detecten a través de un examen sin agente programado o un examen con agente.

> **Nota:**
> Defina aplicaciones no autorizadas y apruebe actualizaciones de seguridad para la implementación automática antes de continuar.

Para aprobar actualizaciones de seguridad:

1. En **Configuration**, seleccione **Patch Auto-Deployment**.

2. Seleccione la revisiones de la lista.

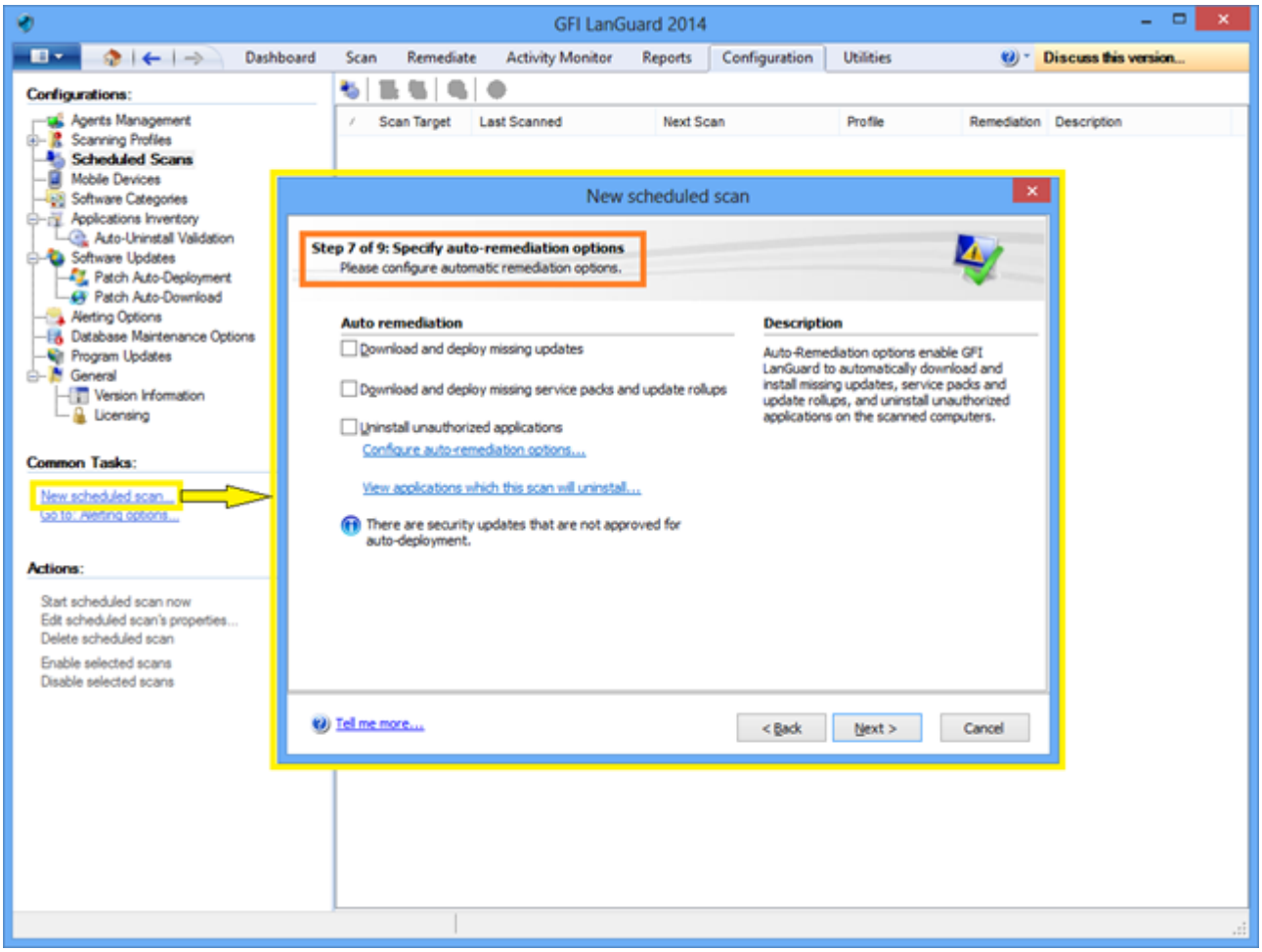


Captura de pantalla 32: Aprobación de actualizaciones de seguridad

Para habilitar la corrección automática para un nuevo examen sin agente:

1. En **Configuration > Scheduled scans > Common tasks**, seleccione **New scheduled scan**.

2. Seleccione las opciones de configuración de corrección automática en el asistente y haga clic en **Finish**.



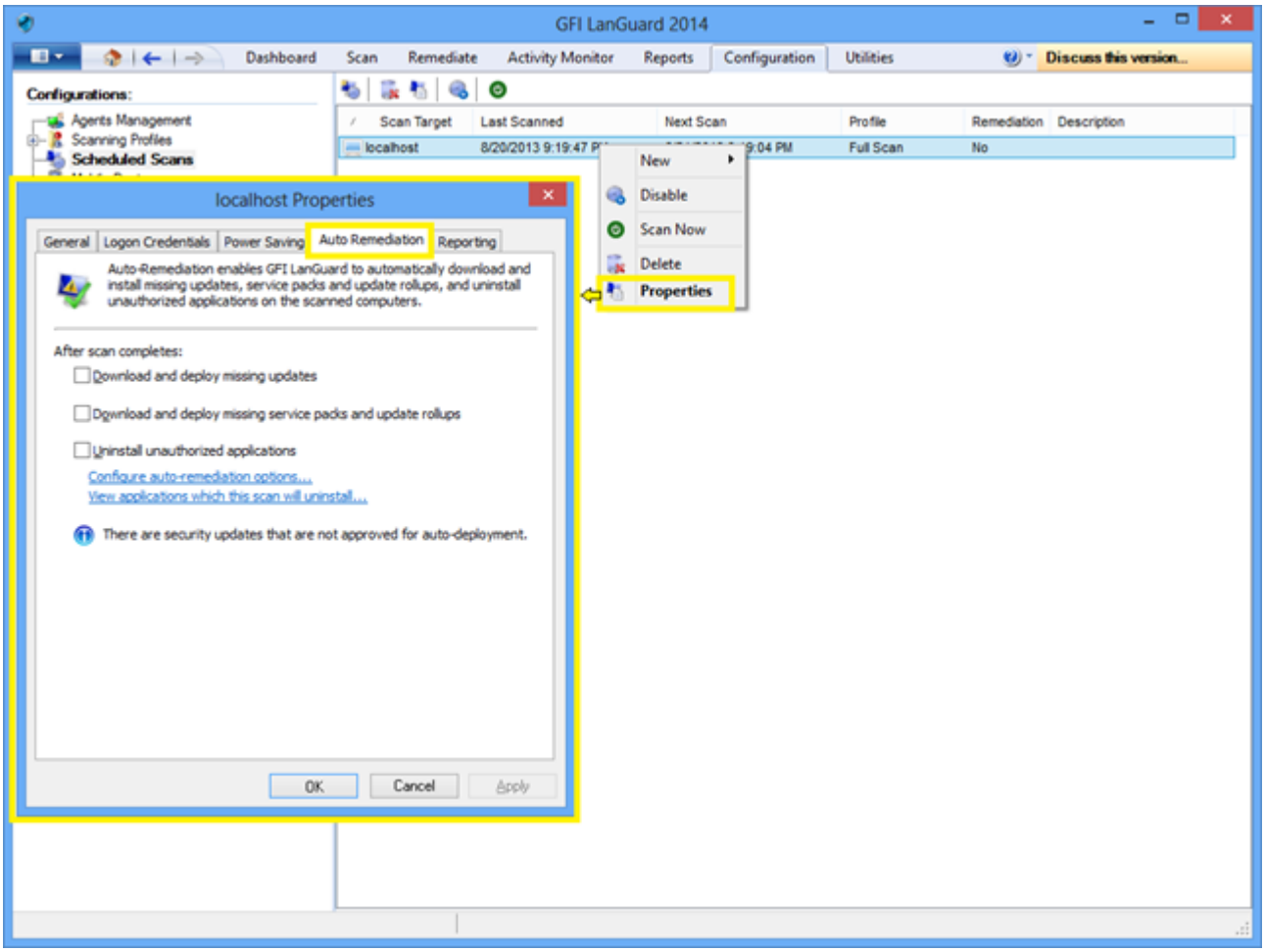
Captura de pantalla 33: Habilitación de la corrección automática para nuevos exámenes de seguridad sin agente

Para habilitar la corrección automática para un examen programado sin agente existente:

1. En **Configuration > Scheduled scans**, seleccione el destino de examen.

2. Haga clic con el botón secundario en el destino seleccionado y haga clic en **Properties**. Esto abrirá el cuadro de diálogo **Properties** de destino.

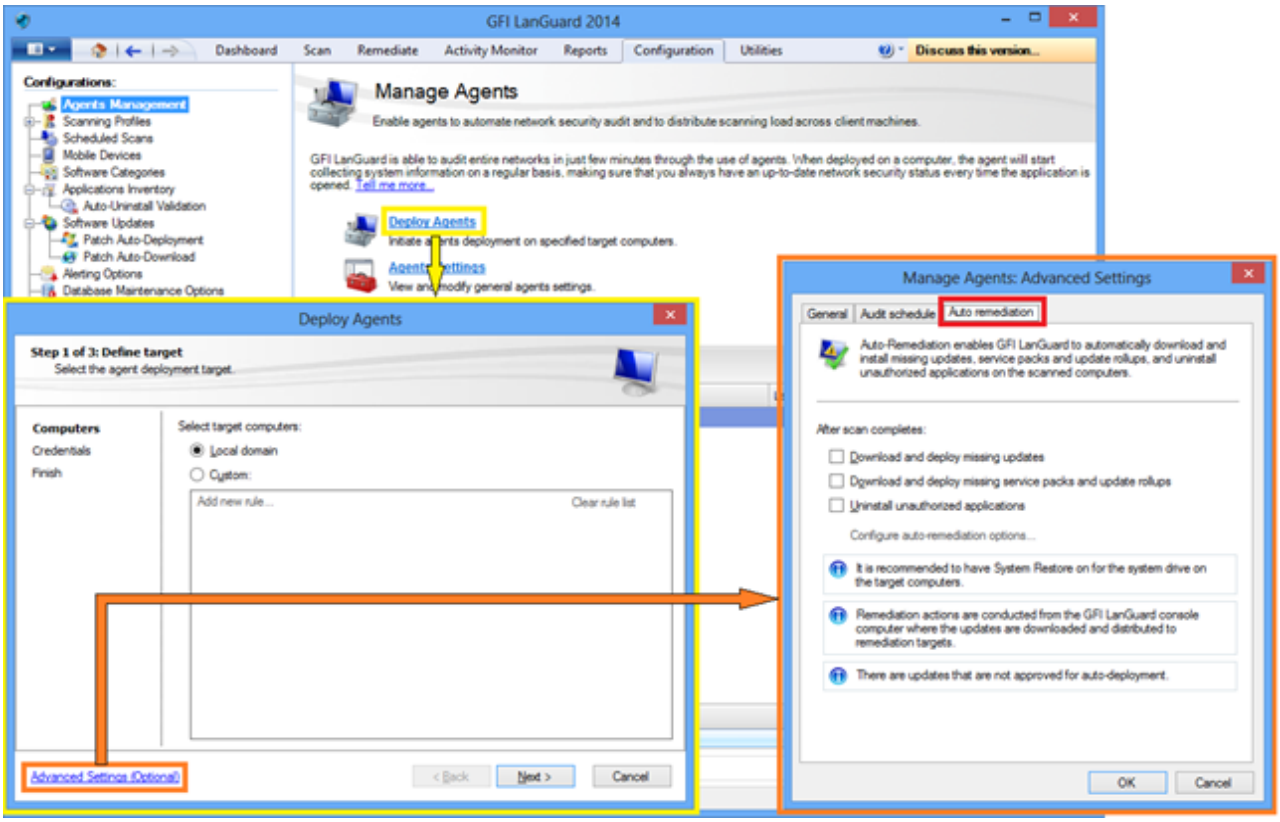
3. En la ficha **Auto Remediation**, seleccione las opciones en el área **After scan completes** y haga clic en **OK**.



Captura de pantalla 34: Habilitación de la corrección automática para exámenes de seguridad sin agente existentes

Para habilitar la corrección automática para agentes en la implementación:

1. En **Configuration > Agents Management**, seleccione **Deploy agents**.
2. En el asistente **Deploy Agents**, seleccione **Advanced Settings**.
3. Haga clic en la ficha **Auto Remediation**, seleccione las opciones en el área **After scan completes** y haga clic en **OK**.



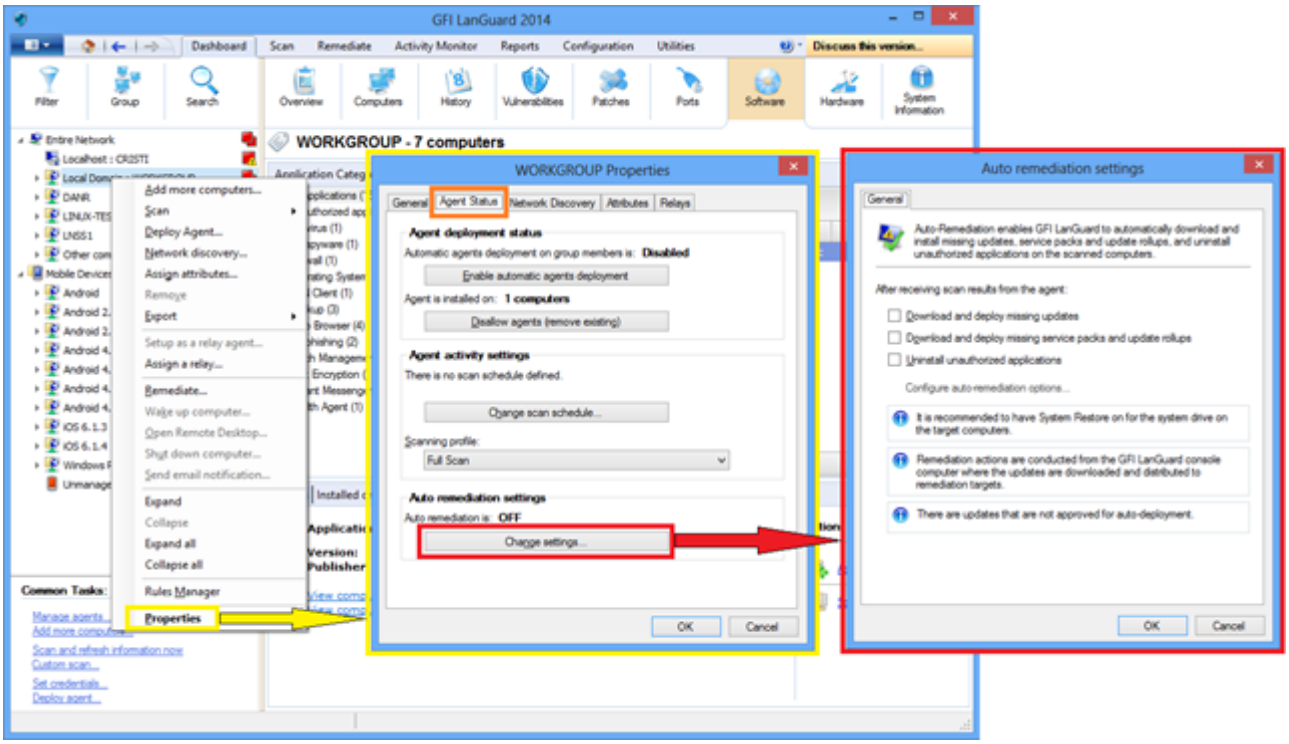
Captura de pantalla 35: Habilitación de la corrección automática para agentes durante la implementación

Para habilitar la corrección automática para auditorías de agentes utilizando el **panel**:

1. En **Dashboard**, haga clic con el botón secundario en un agente y después en **Properties**.

2. En el cuadro de diálogo **Properties**, seleccione la ficha **Agent Status**

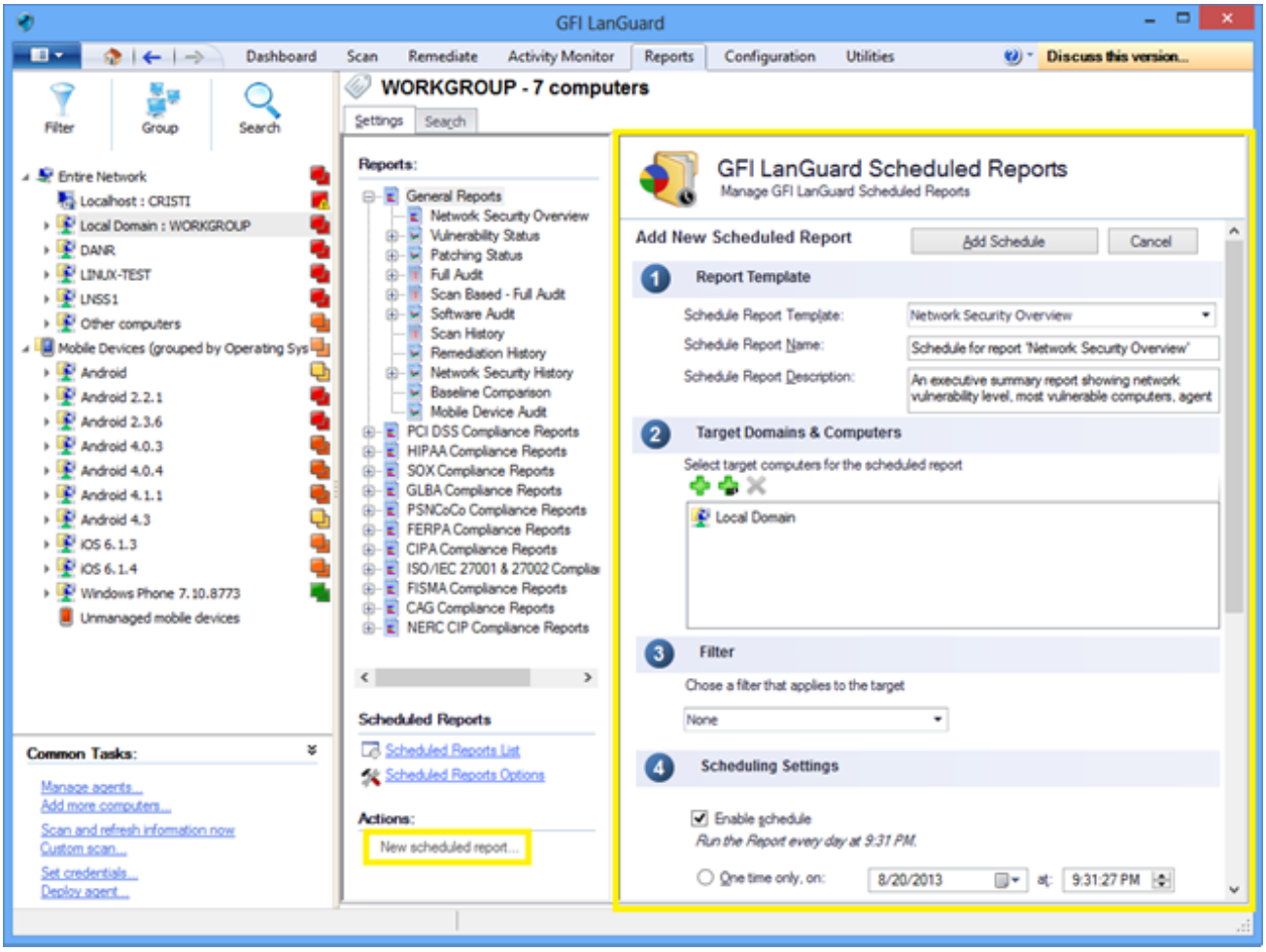
3. Haga clic en **Change settings** y seleccione las opciones en el área **After receiving scan results from the agent**. Después haga clic en **OK**



Captura de pantalla 36: Habilitación de la corrección automática mediante el panel

5.5 Automatización de la generación de informes

Todos los informes se GFI LanGuard se pueden programar para generarse de forma regular y guardarse en el disco, en una ubicación específica, o enviarse a un destinatario de correo electrónico de forma automática.



Captura de pantalla 37: Automatización de la generación de informes

6 Glosario

A

Access™

Sistema de administración de bases de datos relacionales de escritorio de Microsoft® incluido en el paquete de Microsoft® Office. Access™ normalmente se utiliza para bases de datos pequeñas.

Active Directory™ (AD)

Tecnología que proporciona diversos servicios de red, entre los que se incluyen los servicios de directorio similares a LDAP.

Administración de revisiones automática

Tecnología de GFI LanGuard que descarga de forma automática actualizaciones de Microsoft® y las implementa en la red.

Agente de revisión

Servicio de fondo que administra la implementación de revisiones, Service Pack y actualizaciones de software en equipos de destino.

Antispyware

Contramedida de software que detecta spyware que se ha instalado en un equipo sin que el usuario lo sepa.

Antivirus

Contramedida de software que detecta malware que se ha instalado en un equipo sin que el usuario lo sepa.

Archivos de procesamiento por lotes

Archivos de texto que contienen una recopilación de instrucciones que un sistema operativo o una aplicación deben seguir

B

Base de datos de Microsoft® Access™

Sistema de administración de bases de datos relacionales de escritorio de Microsoft® incluido en el paquete de Microsoft® Office. Microsoft® Access™ normalmente se utiliza para bases de datos pequeñas.

Bluetooth

Protocolo inalámbrico abierto de comunicación e interfaz que permite el intercambio de datos entre dispositivos.

Bus serie universal (USB)

Estándar de bus serie ampliamente utilizado para conectar dispositivos a un equipo host.

C

Corrección automática

Tecnología de GFI LanGuard que descarga e implementa de forma automática revisiones faltantes. Si una aplicación se encuentra en la lista negra en GFI LanGuard, la corrección automática la desinstalará del equipo de destino durante las operaciones programadas.

D

deploycmd.exe

Herramienta de línea de comandos de GFI LanGuard que se utiliza para implementar revisiones de Microsoft® y software de terceros en equipos de destino.

Depurador de scripts

Módulo de GFI LanGuard que le permite escribir y depurar scripts personalizados utilizando un lenguaje compatible con VBScript.

Descarga automática

Tecnología de GFI LanGuard que descarga de forma automática revisiones y Service Pack faltantes en los 38 idiomas.

Desinstalación automática de aplicaciones

Acción que permite la desinstalación automática de aplicaciones compatibles con la desinstalación silenciosa de GFI LanGuard.

DMZ

Sección de una red que no es parte de la red interna y que no forma parte de Internet de manera directa. Su objetivo es generalmente actuar como puerta de enlace entre las redes internas e Internet.

DNS

Base de datos que utilizan las redes TCP e IP, que permite la conversión de nombres de host en números IP y el suministro de otra información relacionada con dominios.

F

FTP

Protocolo que se utiliza para transferir archivos entre equipos de redes.

G

GFI EndPointSecurity

Solución de seguridad desarrollada por GFI que permite a las organizaciones conservar la integridad de datos evitando el acceso no autorizado y las transferencias de dispositivos extraíbles.

GPO

Sistema de administración y configuración centralizado de Active Directory que controla lo que los usuarios pueden y no pueden hacer en una red informática.

H

Herramienta de auditoria de SNMP

Herramienta que informa cadenas de comunidad de SNMP vulnerables mediante un ataque por diccionario con los valores almacenados en su archivo de diccionario predeterminado.

Herramienta de auditoría de SQL Server

Herramienta que se utiliza para probar la vulnerabilidad de la contraseña de la cuenta de "sa" (es decir, administrador raíz) y de cualquier otra cuenta de usuarios de SQL configurada en SQL Server.

Herramienta DNS Lookup

Utilidad que convierte nombres de dominio en la dirección IP correspondiente y recupera información en particular del dominio de destino

Herramienta Enumerate Computers

Utilidad que identifica dominios y grupos de trabajo en una red.

Herramienta SNMP Walk

Herramienta que se utiliza para sondear sus nodos de red y recuperar información de SNMP.

Herramienta Traceroute

Herramienta que se utiliza para idenfiticar la ruta de acceso que GFI LanGuard ha empleado para alcanzar un equipo de destino.

Herramienta Whois

Herramienta que le permite buscar información en un dominio o una dirección IP en particular.

Herramientas para enumerar equipos

Herramientas que le permiten recuperar usuarios e información sobre usuarios de su dominio o grupo de trabajo.

I

impex.exe

Herramienta de línea de comandos que se utiliza para importar y exportar perfiles y vulnerabilidades de GFI LanGuard.

Información de boletín.

Contiene una recopilación de información sobre una revisión o actualización de Microsoft®. Se utiliza en GFI LanGuard para proporcionar más información en una revisión o actualización instaladas. La información incluye ID de boletín, título, descripción, URL y tamaño de archivo.

Interfaz de puerta de enlace común (CGI)

Script de comunicación utilizado por servidores web para transferir datos a un explorador de Internet de clientes.

Internet Information Services (IIS)

Conjunto de servicios basados en Internet, creados por Microsoft® Corporation para servidores de Internet.

L

Lenguaje abierto de vulnerabilidad y evaluación (OVAL)

Estándar que promueve contenido de seguridad abierto y públicamente disponible, y estandariza la transferencia de esta información en todo el espectro de herramientas y servicios de seguridad.

Lenguaje de marcado extensible (XML)

Estándar de texto abierto que se utiliza para definir formatos de datos. GFI LanGuard utiliza este estándar para importar o exportar resultados de examen guardados y configuraciones.

Linux

Sistema operativo de código abierto que forma parte de la familia de sistemas operativos Unix.

Lista blanca

Lista de nombres de dispositivos USB o de red no considerados peligrosos. Cuando el nombre de un dispositivo USB o de red contiene una entrada que se halla en la lista blanca durante el examen de una red, GFI LanGuard ignora el dispositivo y lo considera como una fuente segura.

Lista negra

Lista de dispositivos USB o de red considerados peligrosos. Cuando el nombre de un dispositivo USB o de red contiene una entrada que se halla en la lista negra durante el examen de una red, GFI LanGuard presenta el dispositivo como una amenaza de seguridad (vulnerabilidad de seguridad alta).

lnsscmd.exe

Herramienta de línea de comandos de GFI LanGuard que permite la ejecución de comprobaciones de vulnerabilidades en destinos de red.

Localhost

En redes, el localhost es el equipo que se utiliza en el momento. Se puede consultar el localhost utilizando la dirección IP reservada 127.0.0.1. En este manual, el localhost es el equipo en el que GFI LanGuard está instalado.

Localizador uniforme de recursos (URL)

El Localizador uniforme de recursos es la dirección de una página web de la World Wide Web.

M

Malware

Compuesto por "malintencionado" y "software", malware es un término general que se utiliza para citar todo software desarrollado para perjudicar y dañar el sistema de un equipo. Los virus, gusanos y troyanos son todos tipos de malware.

Microsoft® IIS

Conjunto de servicios basados en Internet, creados por Microsoft® Corporation para servidores de Internet.

Microsoft® WSUS

Acrónimo que representa "Microsoft® Windows Server Update Services". Este servicio permite a los administradores gestionar la distribución de actualizaciones de Microsoft® a equipos de red.

Módulo SSH

Módulo que se utiliza para determinar el resultado de las comprobaciones de vulnerabilidades a través de los datos (texto) de la consola producidos por un script ejecutado. Esto significa que puede crear comprobaciones de vulnerabilidades de Linux o UNIX personalizadas utilizando cualquier método de scripting compatible con los SO Linux o UNIX de destino, que envíe resultados a la consola en texto.

N

NETBIOS

Acrónimo que representa "sistema básico de entrada y salida de red". Este sistema proporciona servicios para que las aplicaciones de diferentes equipos de una red se puedan comunicar entre sí.

Netscape

Explorador web desarrollado originalmente por Netscape Communications Corporation.

O

Objeto de directiva de grupo (GPO)

Sistema de administración y configuración centralizado de Active Directory que controla lo que los usuarios pueden y no pueden hacer en una red informática.

OVAL

Estándar que promueve contenido de seguridad abierto y públicamente disponible, y estandariza la transferencia de esta información en todo el espectro de herramientas y servicios de seguridad.

P

Panel

Representación gráfica que indica el estado de varias operaciones que podrían estar actualmente activas, o que están programadas.

Perfiles de examen

Recopilación de comprobaciones de vulnerabilidades que determinan qué vulnerabilidades se identifican y qué información se recuperará de los destinos examinados.

Pings de ICMP

El protocolo de mensajes de control de Internet (ICMP) es uno de los protocolos principales del conjunto de protocolos de Internet. Lo utilizan los sistemas operativos de equipos en red para enviar mensajes de error que indican, por ejemplo, que un servicio solicitado no se encuentra disponible o que un host o enrutador no se han podido alcanzar. El ICMP también se puede utilizar para la retransmisión de mensajes de solicitudes.

Programa de puerta trasera

Método alternativo utilizado para acceder a un equipo o a datos de un equipo a través de una red.

Protocolo de escritorio remoto

Protocolo desarrollado por Microsoft® para permitir que los clientes se conecten con la interfaz de usuario de un equipo remoto.

Protocolo de mensajes de control de Internet (ICMP)

El protocolo de mensajes de control de Internet (ICMP) es uno de los protocolos principales del conjunto de protocolos de Internet. Lo utilizan los sistemas operativos de equipos en red para enviar mensajes de error que indican, por ejemplo, que un servicio solicitado no se encuentra disponible o que un host o enrutador no se han podido alcanzar. El ICMP también se puede utilizar para la retransmisión de mensajes de solicitudes.

Protocolo de transferencia de archivos

Protocolo que se utiliza para transferir archivos entre equipos de redes.

Protocolo simple de administración de redes (SNMP)

El protocolo simple de administración de redes es una tecnología que se utiliza para controlar dispositivos de red como enrutadores, concentradores y connmutadores.

Puertos TCP

Acrónimo que representa "Protocolo de control de transmisión". Este protocolo está desarrollado para permitir que las aplicaciones transmitan y reciban datos a través de Internet utilizando puertos de equipos conocidos.

Puertos UDP

Acrónimo que representa "Protocolo de datagramas de usuario"; se utiliza para transferir datos de UDP entre dispositivos. En este protocolo, los paquetes recibidos no se reconocen.

S

SANS

Acrónimo que significa "Organización investigadora para la administración de sistemas, las redes y la seguridad". Instituto que comparte soluciones relacionadas con alertas de sistema y seguridad.

Scripting Python

Lenguaje de scripting de programación de equipos de alto nivel.

Service Pack de Microsoft® Windows

Recopilación de actualizaciones y correcciones proporcionadas por Microsoft® para mejorar una aplicación o un sistema operativo.

Servicios de terminal

Servicios que permite la conexión con un equipo de destino y la administración de sus aplicaciones instaladas y datos almacenados.

Servidor de correo

Servidor que administra y almacena correos electrónicos clientes.

Servidor web

Servidor que proporicona páginas web a exploradores clientes utilizando el protocolo HTTP.

Servidor web Apache

Projecto de servidor HTTP de código abierto desarrollado y mantenido por la Apache Software Foundation.

Sistema de nombres de dominio

Base de datos que utilizan las redes TCP e IP, que permite la conversión de nombres de host en números IP y el suministro de otra información relacionada con dominios.

SNMP

Acrónimo que representa "Protocolo simple de administración de redes", una tecnología que se utiliza para controlar dispositivos de red como enrutadores, concentradores y connmutadores.

Spyware

Forma de malware pensada para recopilar información de un equipo sin notificar al usuario.

SQL Server®

Sistema de administración de bases de datos relacionales de Microsoft®. Funcionalidad adicional incluida de Microsoft® para SQL Server® (control de transacciones, manipulación de excepciones y seguridad), a fin de que Microsoft SQL Server® pueda admitir organizaciones grandes.

T

Troyanos

Forma de malware que contiene una aplicación oculta que dañará un equipo.

U

URL

El Localizador uniforme de recursos es la dirección de una página web de la World Wide Web.

V

VBScript

Un lenguaje de scripting de Visual Basic es un lenguaje de programación de alto nivel desarrollado por Microsoft®.

Virus

Forma de malware que infecta un equipo. El propósito de este virus es perjudicar un equipo dañando archivos y aplicaciones. Un virus es un programa de duplicación automática y se puede copiar a sí mismo en todo el sistema del equipo.

Vulnerabilidades y exposiciones comunes (CVE)

Lista de nombres estandarizados para vulnerabilidades y otras exposiciones de seguridad de la información. El propósito de CVE es estandarizar los nombres para todas las vulnerabilidades y exposiciones de serguridad de conocimiento público.

W

Wi-Fi/LAN inalámbrica

Tecnología que se utiliza comúnmente en redes de área local. Los nodos de red utilizan datos transmitidos mediante ondas de radio en lugar de cables para comunicarse entre sí.

X

XML

Estándar de texto abierto que se utiliza para definir formatos de datos. GFI LanGuard utiliza este estándar para importar o exportar resultados de examen guardados y configuraciones.

Z

Zona desmilitarizada (DMZ)

Sección de una red que no es parte de la red interna y que no forma parte de Internet de manera directa. Su objetivo es generalmente actuar como puerta de enlace entre las redes internas e Internet.

7 Índice