Datasheet

# HP Client Security Manager

keep reinventing

HP Client Security Manager Gen4 ofrece una amplia selección de poderosas soluciones de seguridad para empresas de cualquier tamaño y está diseñado para superar a las amenazas cibernéticas actuales, así como proteger tus dispositivos, identidad e información.[1]

## Seguridad efectiva para proteger tu negocio

Las amenazas de seguridad actuales atacan a las empresas desde todos los ángulos. La seguridad de múltiples niveles que necesitas viene integrada en los computadores empresariales HP, y HP Client Security Manager Gen4 facilita la protección personalizada al contar con una sola consola que permite que los usuarios finales o los encargados del departamento de informática administren una poderosa suite de herramientas de seguridad.

## Protégete de accesos no autorizados

Una contraseña ya no es suficiente para proteger la identidad de un usuario, de hecho, la mayoría de los robos de información ocurre por contraseñas débiles, predeterminadas o robadas.[2]

HP Client Security Manager Gen4 facilita el fortalecimiento de la seguridad de acceso gracias a la autenticación multifactor, la cual requiere que los usuarios comprueben su identidad de al menos dos formas.

De esta manera, los usuarios pueden combinar factores de autenticación múltiple, incluyendo:

- Factores basados en software como Bluetooth®, NIP, tarjeta de proximidad o contraseña
- Factores fortalecidos para seguridad avanzada como Smart Card o Contactless Card
- Factores biométricos avanzados como sensor de huellas digitales fortalecido (opcional) o reconocimiento facial (con cámara IR opcional)

## Reduce el periodo de inactividad por contraseñas perdidas

Recuperar contraseñas perdidas puede ser una pérdida de tiempo tanto para los usuarios como para el departamento de informática.

**HP SpareKey** permite que los usuarios restauren su contraseña de Windows y restablezcan el acceso a un computador bloqueado con solo contestar una serie de preguntas de seguridad predeterminadas y personalizadas de manera rápida, fácil y sin tener que hacer llamadas de soporte innecesarias o sin tener periodos de inactividad.[3]

## Defiende tu información

La información es el núcleo de tu negocio y puede convertirse en una pesadilla costosa si cae en las manos equivocadas. HP Device Access Manager te ayuda a controlar los puertos de acceso y los dispositivos de almacenamiento al configurar los permisos del dispositivo para que no se pueda copiar la información confidencial del computador.

HP Device Access Manager:

- Protege el acceso a los puertos USB, unidades de CD y DVD, conexiones Bluetooth® y más
- Te permite definir qué usuarios tienen acceso a los dispositivos y puertos y cómo los pueden usar (por ejemplo, solo en modo de lectura)
- Requiere que los usuarios verifiquen sus credenciales inmediatamente después de que accedan a un puerto o un dispositivo y les permite acceso solo por un determinado tiempo (por ejemplo,10 minutos)

Restringir el acceso a los puertos USB también puede ayudar a proteger contra cualquier malware que entre a través de las unidades USB infectadas.

## Gestionabilidad

Desde una sola consola, HP Client Security Manager también facilita la instalación y administración de funciones avanzadas que se encuentran en las máquinas HP Elite, como **HP Sure Run** y **HP Sure Recover**.[4,5]

Para los usuarios empresariales, **HP Manageability Integration Kit Gen2** también habilitan la gestionabilidad remota de HP Client Security Manager a través de Microsoft System Center Configuration Manager.[6]

## Preguntas frecuentes:

### P: ¿Qué plataformas tienen HP Client Security Manager?

R: HP Client Security Manager Gen4 viene integrado en los PCs HP Pro y HP Elite. Se recomienda revisar las especificaciones del producto para más información.

### P: Tengo un negocio en crecimiento, pero no cuento con un departamento de informática. ¿De todos modos puedo usar HP Client Security Manager?

R: Sí. HP Client Security Manager está diseñado para simplificar la configuración de seguridad y además proporciona una sola consola con opciones que pueden ser instaladas por cada usuario en su propio dispositivo. A medida que tu negocio crece, el departamento de informática puede administrar la configuración de HP Client Security Manager de manera remota.

### P: ¿Puedo elegir cualquier combinación de factores al instalar la autenticación multifactor?

R: Existen algunas restricciones para garantizar una mayor seguridad. Si eliges la tarjeta de proximidad, Bluetooth® o un NIP como factor, se deben combinar con otro factor que no sea la tarjeta de proximidad, Bluetooth® o NIP. La única excepción es que el Bluetooth® y el NIP se permitan como combinación. Por ejemplo, la tarjeta de proximidad y un NIP no serían una combinación permitida, pero la tarjeta de proximidad y la huella digital sí.

### P: ¿Qué quiere decir que un factor de autenticación está "fortalecido"?

R: Fortalecer un factor de autenticación proporciona una protección extra a las credenciales del usuario, lo que hace más difícil que el malware basado en software pueda atacar.

Por ejemplo, HP ofrece sensores de huellas digitales fortalecidos, los cuales verifican la huella digital en el mismo hardware del sensor, que está aislado del resto del sistema y además, está cifrado.

### P: ¿Qué pasa si quiero fortalecer mis políticas de autenticación y factores individuales?

R: Para los usuarios empresariales, HP Multi-Factor Authenticate cuenta con requisitos de autenticación más estrictos.[7] Con HP Multi-Factor Authenticate, las políticas de acceso están fortalecidas al máximo y el departamento de informática podría necesitar hasta tres factores de autenticación. También habilita el acceso multifactor para la VPN.

## Funciones adicionales

HP Client Security Manager facilita la administración local de:

- Autenticación multifactor
- HP Device Access Manager
- HP SpareKey
- HP Password Manager[8]
- Unidades que se cifran automáticamente[9]
- HP Secure Erase[10]
- Inicio de un solo paso
- HP Sure Run
- HP Sure Recover

## Conoce más en hp.com/lar/pcsecure

Comparte con colegas

1. HP Client Security Manager Gen4 requiere Windows y procesadores Intel® o AMD de 8va generación.
2. Verizon, informe sobre investigaciones de robo de información, 2017.
3. HP SpareKey requiere una instalación inicial del usuario.
4. HP Sure Run está disponible en productos HP Elite equipados con procesadores Intel® o AMD de 8va generación.
5. HP Sure Recover está disponible en computadores HP Elite con procesadores Intel® o AMD de 8va generación y requiere una conexión abierta y alámbrica. No está disponible en plataformas con unidades de almacenamiento interno múltiples o Intel® Optane™. Es necesario que respaldes tus archivos, información, fotos y videos importantes antes de usar para evitar la pérdida de información.
6. HP Manageability Integration Kit se puede descargar de hp.com/go/clientmanagement.
7. HP Multi-Factor Authenticate Gen2 requiere Windows, un procesador Intel® Core™ de 7a u 8va generación, gráficas integradas Intel® y WLAN Intel®. Se necesita Microsoft System Center Configuration Manager para la instalación. Los tres factores de autenticación requieren Intel® vPro™. Los factores de autenticación podrían requerir hardware opcional. HP Manageability Integration Kit se puede descargar de hp.com/go/clientmanagement.
8. HP Password Manager requiere Microsoft Internet Explorer. Es probable que no sea compatible con algunos sitios web y algunas aplicaciones. Se soporta en modo computador de escritorio con Windows 8.
9. Las unidades de cifrado automático están disponibles de manera opcional en algunos computadores de HP.
10. HP Secure Erase: Para los métodos descritos en el Instituto Nacional de Normas y Tecnología, publicación especial 800-88 sobre el método de reparación "claro".



4AA7-3204SPL, septiembre de 2018