

Protección para dispositivos móviles

HP Touchpoint Manager



La reciente expansión de negocios con dispositivos móviles mejora la productividad de tus empleados. Ellos pueden ser productivos en la oficina y en cualquier otro lugar: en el aeropuerto mientras esperan una conexión aérea, en una cena con un cliente, mientras asisten a una conferencia o desde la casa. Pero una mayor flexibilidad incrementa la vulnerabilidad. Cada empleado con un dispositivo móvil (teléfono, tableta, notebook) se convierte en un riesgo para la información de tu organización, que puede ser robada o destruida.

En unos pocos pasos, HP Touchpoint Manager puede proveer protección y tranquilidad para ti y tus empleados.¹ Es una solución necesaria para las compañías que apoyen el programa “Traiga su propio equipo” o “Bring Your Own Device” BYOD. Usando la tecnología de HP Touchpoint Manager un administrador de TI puede disponer de seguridad, configuración rápida, suministro de Wi-Fi y el ajuste de políticas para grupos de usuarios de los dispositivos.

La configuración de la seguridad incluye:

- Detectar, monitorear e instalar el software antivirus (Windows®)
Si no se detecta la protección antivirus, HP Touchpoint Manager automáticamente desplegará y/o activará el Defensor Windows Microsoft® (Windows 8.0 o superior) o el programa de Microsoft® Security Essentials (Windows 7).
- Detectar, monitorear, y utilizar el Windows Firewall (Windows)
Si no se detecta un software de firewall activo, se activará el software de Windows Firewall.
- Borrar un dispositivo después de un número definido de intentos de inicio de sesión fallidos (Android™ / iPhone® y iPad®)
- Desencadenar un dispositivo de bloqueo automático después de un tiempo específico de inactividad (Android/iPhone y iPad)
- Forzar la utilización de la longitud mínima de contraseña/PIN del dispositivo (Android/iPhone y iPad)
- Activar/desactivar la cámara del dispositivo (Android/iPhone y iPad)

HP Touchpoint Manager incluye las plantillas predefinidas de seguridad que incorporan las mejores prácticas de seguridad según las necesidades de los clientes y te permite crear tu propio perfil de seguridad.

Perfiles de seguridad HP Touchpoint Manager

Nivel de suscripción	Configuraciones de seguridad	Perfiles de seguridad		
		Estándar	Mejorado	Máximo
Basic	Monitoreo antivirus	Apagado	Encendido	Encendido
Basic	Monitoreo de firewall	Apagado	Apagado	Encendido
Pro	Bloqueo de dispositivo después de X minutos de inactividad	30	15	5
Pro	Contraseñas deben contener letras	Apagado	Apagado	Encendido
Pro	Contraseñas deben contener números	Apagado	Apagado	Encendido
Pro	Borrar todos los datos en dispositivos después de X ingresos incorrectos de la contraseña	Apagado	Apagado	10
Pro	Longitud mínima de contraseña	0	4	8
Pro	Deshabilitar la cámara	Apagado	Apagado	Apagado
Pro	Habilitar encriptación de dispositivo	Apagado	Apagado	Apagado
Pro	Contraseñas deben tener caracteres especiales	Apagado	Apagado	Encendido
Pro	Contraseña expira después de X días	Apagado	120	90
Pro	Requiere historia de contraseña. Requiere X contraseñas	Apagado	3	5

Debido a que diferentes políticas pueden asignarse a diferentes grupos de dispositivos, es sencillo llevar un registro de qué ajustes se aplican a lo largo de la organización.

Por ejemplo, a los dispositivos de los empleados de un solo departamento, como finanzas o recursos humanos, puede asignarse una política específica de seguridad. Estas también pueden organizarse por tipo (ej. Todas las tabletas). Una vez creado un grupo, podrás aplicarle un perfil de seguridad con un solo clic. Puedes realizar cambios rápidamente. Si identificas riesgos, puedes aplicar un perfil de seguridad más restrictivo, según tu necesidad.

Los beneficios adicionales de seguridad incluyen la función "Encuentra el dispositivo", que protege tu organización contra el robo o pérdida al localizar el dispositivo en un mapa cuando

éste se conecte a Internet.² Esto te permite confirmar que el dispositivo se encuentra donde se tiene que encontrar. Si crees que el dispositivo ha sido robado o perdido, puedes tomar medidas para ubicarlo o proteger sus datos.

Las funciones de protección de dispositivos perdidos incluyen:

- **Sonido de alarma:** Activa un sonido fuerte, que puede ser útil si el dispositivo se ha perdido cerca²
- **Bloqueo del dispositivo:** Provoca un bloqueo de pantalla (Android / iPhone y iPad) o cierre de sesión del sistema operativo (Windows)²
- **Borrar datos del dispositivo:** Provoca un restablecimiento de fábrica (Android / iPhone y iPad) o un borrado seguro de archivos de datos desde el dispositivo (Windows)²

En el caso de que tu organización o las políticas de privacidad del gobierno así lo requieran, la función de búsqueda de dispositivos puede ser desactivada.

Como administrador de TI, HP Touchpoint Manager te permite monitorear fácilmente los dispositivos móviles a administrar, revisar la configuración y estatus de seguridad, tomar medidas para cambiar las políticas de seguridad y decidir sobre los dispositivos perdidos. Las características de seguridad le permiten a tu organización mantener las características de movilidad, garantizando la seguridad y accesibilidad de sus datos, y la productividad de sus empleados.

¹ HP Touchpoint Manager soporta los sistemas operativos Android™, iOS y Windows, y PCs, notebooks, tablets y teléfonos inteligentes de varios fabricantes. No disponible en todos los países. Consultar la información de disponibilidad en hp.com/touchpoint. Touchpoint Manager requiere la compra de una suscripción.

² Sujeto a diversas características ambientales, incluyendo que el producto perdido sea encendido y tenga acceso a internet. El servicio no es una garantía.

Para obtener más información
hp.com/go/getupdated



Compartir con colegas



Calificar este documento

© Copyright 2015 HP Development Company, L.P. La información aquí contenida está sujeta a cambios sin previa notificación. Las únicas garantías para los productos y servicios de HP se especifican en los estatutos de la garantía que acompañan a los productos y servicios. Nada de lo aquí contenido debe interpretarse como una garantía adicional.

Microsoft, Office y Windows son marcas norteamericanas registradas para el grupo de compañías de Microsoft. Intel es una marca de Intel Corporation en los Estados Unidos y en otros países. Android™ es una marca de Google Inc. Apple, iPad y iPhone son marcas de Apple Inc., registradas en los Estados Unidos y en otros países.

4AA6-0367SPL, Noviembre 2015

