



Descripción general de las funciones de seguridad de Palm webOS para empresas

Introducción	2
Descripción general de las funciones de seguridad de Palm webOS	3
Comunicación segura	4
Protección de datos en el dispositivo	5
Entorno de aplicaciones	5
Borrado remoto	6
Copia de seguridad y restauración de los datos	6
Conclusión	7



Introducción

Son muchas las ventajas de proporcionar a los profesionales un acceso móvil cómodo al correo electrónico y a los datos críticos de la empresa. Las organizaciones pueden aumentar su productividad, optimizar los procesos de negocio y mejorar la toma de decisiones. El teléfono Palm® Pixi™ Plus con la plataforma Palm webOS™ se ha diseñado para ayudar a los profesionales a aumentar la cantidad de trabajo que realizan en cualquier lugar que se encuentren. Con funciones tan valiosas como el correo electrónico, un completo navegador Web, Wi-Fi con seguridad, desarrollo de aplicaciones basado en Web y la capacidad de utilizar múltiples aplicaciones a la vez, la plataforma webOS se adapta fácilmente al entorno empresarial.

No obstante, la facilidad de acceso conlleva la responsabilidad de proteger los datos de la organización, así como la inversión en dispositivos móviles. Con Palm webOS y su integración en Microsoft® Exchange, los administradores de ST y los responsables de la toma de decisiones de la empresa pueden implementar dispositivos webOS con confianza en su entorno empresarial.

Este documento examina algunos de los temas clave sobre la seguridad móvil y analiza las soluciones de seguridad utilizadas por Palm webOS.

Descripción general de las funciones de seguridad de Palm webOS

Los mismos factores que hacen atractivos los smartphones y los ordenadores de mano para los usuarios móviles, portabilidad y comodidad, también hacen que resulten fáciles de perder. Los dispositivos pueden perderse o ser robados. Es fundamental establecer unas políticas de seguridad adecuadas para el acceso a la red y los dispositivos con el fin de proteger los datos de la empresa. Palm webOS es compatible con este tipo de políticas de seguridad en tres sentidos:

1. Comunicación segura

Los datos que se transmiten entre el dispositivo y la red de la organización deben estar protegidos. La plataforma webOS ofrece tecnologías de eficacia probada para ayudar a garantizar la seguridad de los datos que se transmiten por Wi-Fi, redes de datos móviles y tecnología inalámbrica Bluetooth. La seguridad se integra en aplicaciones críticas como el correo electrónico y el navegador. Además, las terceras partes pueden utilizar protocolos de comunicaciones seguras por Internet como SSL en sus propias aplicaciones webOS.

2. Protección de datos local

La autenticación de inicio mediante contraseña protege el dispositivo frente a usuarios no autorizados. La plataforma webOS incluye una sólida protección integrada mediante contraseña que mantiene el dispositivo bloqueado a menos que se introduzca una contraseña válida. Las contraseñas pueden configurarse en el dispositivo o aplicarse de forma inalámbrica en el entorno empresarial.

3. Entorno de aplicaciones

Las aplicaciones se ejecutan en un entorno “supervisado” en webOS. Este mecanismo ayuda a proteger los datos de una aplicación frente al acceso no autorizado por parte de otra aplicación, rechazando así la efectividad de una aplicación malintencionada.

A pesar de los esfuerzos de los usuarios, los dispositivos pueden perderse. Para minimizar el impacto de un dispositivo perdido, la plataforma webOS proporciona también sólidas medidas de recuperación que permiten a los empleados recuperar su productividad rápidamente:

Borrado remoto

Si un dispositivo webOS se pierde o es robado, el administrador o el propietario pueden borrar de forma remota todos los datos del dispositivo. Los protocolos de eliminación de datos pueden configurarse en el dispositivo (borrado local) o transmitirse inalámbricamente (borrado remoto).

Copia de seguridad de los datos

Cuando un dispositivo se pierde, una copia de seguridad reciente puede minimizar el tiempo de inactividad del usuario y permitir una recuperación rápida de los datos, las aplicaciones y la configuración. De forma predeterminada, los dispositivos webOS están configurados para realizar copias de seguridad diarias. Además, el servicio de copia de seguridad utiliza tecnologías de eficacia probada para autenticar el dispositivo/usuario y garantizar la seguridad de los datos en nube.

Comunicación segura

La plataforma webOS ofrece una amplia variedad de métodos de acceso y transmisión de datos, que incluyen redes de datos móviles, Wi-Fi y tecnología inalámbrica Bluetooth®. La plataforma implementa procedimientos de seguridad como la autenticación y el cifrado de datos para permitir que los usuarios accedan a las redes de la empresa sin preocuparse por los riesgos en la seguridad.

Wi-Fi

La plataforma webOS admite los estándares de seguridad empresariales WPA y WPA2. Los estándares WPA y WPA2 utilizan autenticación 802.1x, comprobaciones de integridad de mensajes y sólidos estándares de cifrado. Mientras WPA utiliza el cifrado TKIP (Temporary Key Integrity Protocol), WPA2 utiliza el estándar AES (Advanced Encryption Standard) para el cifrado de datos. 802.1x utiliza el protocolo EAP (Extensible Authentication Protocol) para la autenticación entre un dispositivo inalámbrico y un punto de acceso antes de proporcionar acceso a la red de la empresa. La plataforma webOS admite los tipos de EAP más populares: EAP-TLS, PEAP v1/v2, EAP-TTLS, EAP-FAST y LEAP. Esta sopa de letras de métodos de autenticación significa que los dispositivos webOS pueden conectarse a redes Wi-Fi de empresa con un alto nivel de confianza en que la comunicación estará protegida y será segura.

Tecnología inalámbrica Bluetooth

La plataforma webOS admite también las funciones de seguridad estipuladas por la especificación Bluetooth 2.1. Debe establecerse una vinculación de confianza con el dispositivo webOS antes de poder enviar o recibir ningún dato. Esto garantiza que el dispositivo conectado sea siempre “conocido” (esté autenticado) porque se ha intercambiado una clave acordada mutuamente. Además, los datos que se transmiten entre los dispositivos están cifrados (nivel de vínculo) mediante los estándares establecidos por las especificaciones Bluetooth.

Certificados digitales

Los certificados digitales son firmas electrónicas que confirman la identidad del servidor. La plataforma webOS utiliza certificados digitales para:

- Establecer conexiones SSL seguras con el servidor desde las aplicaciones de correo electrónico, calendario, contactos y navegador

- Garantizar la seguridad de las conexiones Wi-Fi mediante los protocolos WPA y WPA2
- Firmar digitalmente aplicaciones para evitar las aplicaciones de software malintencionado o no autorizadas

La plataforma webOS incluye certificados raíz para la principal entidad de certificación (CA, Certificate Authority). Además, las empresas pueden instalar sus certificados auto-firmados privados para permitir que los dispositivos webOS se conecten de forma segura a una red. Todos los certificados se almacenan en la biblioteca de certificados de la plataforma y pueden acceder a ellos las aplicaciones de Palm, los servicios de Palm, las redes Wi-Fi y las aplicaciones de terceros desarrolladas con el kit de desarrollo Palm Mojo Software Development Kit (SDK). Para obtener detalles sobre cómo instalar certificados digitales y registrarlos en la biblioteca de certificados de la plataforma, visita kb.palm.com/wps/portal/kb/common/article/40069_en.html

Correo electrónico

La plataforma webOS admite los mecanismos de seguridad ofrecidos por Microsoft Exchange ActiveSync® (EAS) y los protocolos de correo electrónico POP e IMAP.

Cuando se configura un dispositivo webOS para que se sincronice con Microsoft Exchange Server, se utiliza el protocolo de EAS empresarial. La conexión SSL entre el servidor y el dispositivo se protege mediante un certificado de CA o auto-firmado. A menos que los certificados necesarios estén instalados y registrados en la biblioteca de certificados de la plataforma, la sincronización de EAS no podrá continuar. Como se describe en la siguiente sección, la plataforma admite varias políticas de EAS para ayudar a garantizar al administrador de la red que los dispositivos webOS no pondrán en riesgo los datos de la empresa. Con EAS, el usuario puede sincronizar con seguridad el correo electrónico (incluidas las carpetas), los contactos, los calendarios y las tareas, así como buscar direcciones en el directorio de la empresa con la lista global de direcciones (GAL). Este equilibrio entre posibilidades de uso y seguridad aumenta al máximo la productividad de los usuarios.

Navegador

El potente navegador Web de webOS permite a los usuarios navegar e interactuar sin riesgos con sitios Web seguros (https://) mediante SSL. Al interactuar con sitios Web seguros, los usuarios deben prestar atención a los errores y advertencias de los certificados y asegurarse de que la conexión es segura (por ejemplo, la URL empieza por https://). En general, los usuarios deben evitar las actividades confidenciales en redes no seguras como puntos de acceso Wi-Fi públicos no protegidos (que no utilizan seguridad WPA o WPA2).

Protección de datos en el dispositivo

Los usuarios necesitan algo más que una comunicación segura. También necesitan dispositivos seguros. La plataforma webOS ofrece varios métodos para proteger los datos del dispositivo. Los usuarios pueden bloquear los dispositivos webOS mediante una contraseña que evite el acceso no autorizado cuando no se esté utilizando el dispositivo.

Para desbloquear el dispositivo y obtener acceso al mismo, los usuarios deben acreditar su identidad introduciendo la contraseña correcta. Es difícil garantizar la seguridad física de un teléfono, por lo que es muy importante que las personas no autorizadas no puedan acceder al mismo. La autenticación ayuda a proteger el acceso a los datos y la red de la empresa en caso de que el dispositivo se pierda o sea robado.

En un entorno empresarial, los administradores de red pueden garantizar la seguridad de los dispositivos webOS que se conectan a la red mediante la aplicación de políticas de contraseña. Cuando un dispositivo webOS se configura para acceder a Microsoft Exchange, las políticas de Exchange ActiveSync (EAS) se transmiten al dispositivo inalámbricamente, forzando al usuario a proteger el dispositivo mediante una contraseña. Además, un usuario puede configurar varias cuentas de Exchange en un dispositivo webOS y la plataforma impondrá de forma inteligente la intersección de políticas más restrictiva. Ni el usuario ni el administrador deben realizar pasos adicionales. La plataforma webOS simplemente hace lo correcto para que el usuario pueda seguir disponiendo de acceso sin infringir las políticas impuestas por cualquier servidor de Exchange.

La plataforma webOS admite las siguientes políticas de EAS:

- Aplicación de un bloqueo por contraseña en el dispositivo.
- Definición de la longitud mínima de la contraseña. En los teléfonos webOS, las contraseñas alfanuméricas pueden tener entre 2 y 18 caracteres. Las contraseñas numéricas pueden contener hasta 32 números.
- Uso tanto de números como de letras. Los teléfonos Palm webOS admiten una combinación de caracteres numéricos y no numéricos para activar contraseñas más seguras. La seguridad de la contraseña desempeña una función importante en la seguridad del dispositivo.
- Número máximo de intentos fallidos de introducción de la contraseña. Los administradores pueden limitar el número de intentos fallidos de inicio de sesión en un teléfono webOS.

Cuando se supera el límite, se borran los datos del dispositivo (borrado local). Esta es normalmente la mejor y la única forma de enfrentarse a los intentos de “prueba y error” para desbloquear el dispositivo mediante la introducción de varias permutaciones de contraseñas.

- Bloqueo automático tras un periodo de inactividad. La pantalla se bloquea tras 3 minutos de inactividad y los administradores pueden establecer tiempos de espera de la contraseña de hasta 30 minutos.

Para obtener más detalles sobre cómo la plataforma webOS admite las políticas de EAS, visita kb.palm.com/wps/portal/kb/common/article/58353_en.html

Entorno de aplicaciones

En la plataforma webOS, todas las aplicaciones se ejecutan en un entorno “supervisado” para ayudar a limitar el acceso no autorizado a otros datos de aplicaciones y servicios. Las aplicaciones pueden interactuar entre sí sólo mediante las API y los servicios específicos ofrecidos por el sistema operativo dentro del entorno Mojo. Mojo proporciona varios mecanismos para permitir el desarrollo de aplicaciones seguras, e incluso admite criptografía y uso de SSL para conexiones remotas. La validación de certificados se aplica al conectarse mediante SSL a través de Mojo.

Las aplicaciones de Palm webOS que no están precargadas en el dispositivo pueden descargarse sólo desde el servicio App Catalog de Palm. Todas las aplicaciones descargadas desde App Catalog incluyen la firma digital de Palm y se verifican en el momento de la instalación.

El kit Mojo SDK está disponible para descarga en developer.palm.com

Borrado remoto

Si un dispositivo webOS se pierde o es robado, el propietario del dispositivo o el administrador de ST de la empresa pueden borrar los datos que contenga de forma remota. Los siguientes mecanismos minimizan el mal uso de los datos si un dispositivo webOS se pierde o es robado:

- Como se ha comentado anteriormente en este documento, el administrador de ST de la empresa puede limitar el número de intentos fallidos de introducción de la contraseña. Si se supera el límite, se borran todos los datos y la configuración del dispositivo.
- Si el dispositivo webOS se conecta a Microsoft Exchange, el administrador puede iniciar un borrado remoto desde la consola de administración de Exchange. Además, el propietario del dispositivo puede iniciar el borrado remoto iniciando sesión en Outlook Web Access (sólo en Exchange 2007).
- El propietario del dispositivo puede iniciar sesión en la consola de usuario de Palm mediante el ID y la contraseña del perfil de Palm para borrar de forma remota todos los datos del dispositivo perdido o robado. Un usuario puede borrar un dispositivo sólo si éste se ha registrado con un perfil de Palm. Como protección adicional frente a programas malintencionados o borrados accidentales, el usuario debe completar el desafío CAPTCHA antes de iniciar el borrado remoto.

Copia de seguridad y restauración de los datos

Si el dispositivo se pone en riesgo o se pierde, los procedimientos de copia de seguridad y recuperación correctos pueden conseguir que el usuario recupere rápidamente su productividad. Palm ofrece servicios de copia de seguridad y restauración para dispositivos webOS, para que determinados datos de usuario y configuraciones de personalización del dispositivo¹ no se pierdan si se restablece o sustituye el dispositivo. La copia de seguridad de los datos se realiza en servidores gestionados por Palm y se protege mediante políticas y procedimientos de seguridad reconocidos del sector.

La conexión entre el dispositivo y los servidores de copia de seguridad se autentifica mutuamente y se protege mediante SSL, y los datos se cifran durante la transmisión. Si están inactivos, los datos se cifran mediante AES-128 con claves específicas de usuario. Durante el proceso de restauración, sólo puede accederse a los datos si el usuario inicia sesión mediante el correo electrónico y la contraseña del perfil de Palm registrados en el dispositivo. Además, todas las contraseñas almacenadas en el dispositivo se cifran y el dispositivo puede bloquearse mediante un PIN o una contraseña local que active el usuario o el administrador de ST a través de la configuración de Microsoft Exchange.

Los dispositivos Palm webOS están configurados para realizar copias de seguridad de los datos y las preferencias del usuario de forma predeterminada en los servidores gestionados por Palm. El usuario puede desactivar los servicios de copia de seguridad en cualquier momento mediante la aplicación Copia de seguridad incluida. Cuando el usuario desactive la copia de seguridad del dispositivo, los datos de copia de seguridad asociados con el perfil se borrarán de los servidores de Palm.

Para obtener detalles sobre qué datos y configuraciones se incluyen en la copia de seguridad, visita kb.palm.com/wps/portal/kb/common/article/19388_en.html

Conclusión



Entorno de aplicación seguro
Almacenaje de datos protegido
Protección por contraseña / PIN
Contraseñas / credenciales cifradas



Conexión segura
128 bit SSL
Wi-Fi segura (WPA, WPA2)



Almacenamiento cifrado según AES
Autenticación Mutua basada en certificados digitales, empleo de credenciales
Aplicaciones firmadas en el Catálogo
Cumplimiento de la Política EAS, borrado Remoto

La plataforma Palm webOS proporciona protección de datos transmitidos, inactivos o de copia de seguridad mediante el servicio de copia de seguridad de Palm. Admite las políticas de seguridad de empresa más utilizadas y ofrece métodos para recuperarse rápidamente en caso de pérdida o robo de un dispositivo. Palm webOS es una plataforma informática móvil segura que las empresas pueden implementar con confianza.

Al final, parte de la responsabilidad recae en los usuarios, que deben utilizar las funciones de la plataforma para protegerse frente a ataques contra la seguridad. Las empresas deben plantearse ofrecer formación a los empleados sobre las políticas y las prácticas de seguridad de la organización para recordarles hábitos de sentido común como el bloqueo del dispositivo si no se utiliza, la omisión de actividades confidenciales durante la conexión a redes Wi-Fi no protegidas y la consideración de cualquier advertencia de certificados digitales.

Para obtener más información sobre la política de seguridad de Palm, visita palm.com/security

1. La copia de seguridad incluye los contactos, calendarios, notas y tareas, junto con las preferencias y todo el software descargado de App Catalog.

Nota: ST es Servicio Técnico

© 2010 Palm, Inc. Palm, Pre, Pixi, webOS, Mojo, Synergy y Touchstone son marcas comerciales de Palm, Inc. Microsoft, ActiveSync y Outlook son marcas comerciales o marcas registradas del grupo de compañías de Microsoft.

Para obtener información adicional sobre:

Política de seguridad de Palm:

palm.com/security

Palm webOS para empresas:

palm.com/es/es/business/pre-index.html

Palm Pixi Plus:

palm.com/es

Gartner:

gartner.com/DisplayDocument?id=1122312&ref=g_fromdoc

Informe de Philippe Winthrop:

strategyanalytics.com/default.aspx?mod=ReportAbstractViewer&a0=4811

Blog de Philippe Winthrop:

enterprisemobilitymatters.com