



Palm webOS security overview for enterprise

Introduction	2
webOS security overview	3
Secure communication	4
Protecting data on the device	5
Application environment	5
Remote wipe	6
Data backup and restore	6
Conclusion	7



Introduction

The benefits of providing professionals with convenient mobile access to email and critical corporate data are many. Organisations can become more productive, streamline business processes, and enable better decision making. The Palm® Pre™ Plus and Pixi™ Plus phones on the Palm webOS™ platform are designed to help professionals get more work done regardless of where they are. With such valuable features as email, a rich web browser, security-enabled Wi-Fi, web-centric application development, and the ability to use multiple applications at once, the webOS platform fits easily into a corporate environment.

But with ease of access comes the responsibility to protect an organisation's data as well as its investment in mobile devices. With Palm webOS and its integration with Microsoft® Exchange, IT administrators and business decision makers can deploy webOS devices with confidence in their corporate environment.

This paper examines some of the key issues in mobile security and discusses the security solutions utilised by Palm webOS.



Palm webOS security overview

The same factors that make smartphones and handheld devices attractive to mobile users—portability and convenience—also make them easy to lose. A device can be stolen or misplaced. Establishing proper security policies for access to the network and the device is critical to protecting company data. Palm webOS supports proper security policies in three ways:

1. Secure communication

Data in transit between the device and the organisation's network must be protected. The webOS platform provides proven technologies to help secure data in transit over Wi-Fi, cellular data networks, and Bluetooth wireless technology. Security is built in to critical applications such as Email and Browser; moreover, third parties can use secure web communications protocol such as SSL in their own webOS applications.

2. Local data protection

Power-on authentication with a password protects the device from unauthorised users. The webOS platform includes strong built-in password protection that keeps the device locked unless a valid password is entered. Passwords can be configured on the device or enforced over the air in an enterprise environment.

3. Application environment

Applications run in a “sandboxed” environment on webOS. This mechanism helps protect one application's data from unauthorised access by another application, thereby negating the effectiveness of a malicious application.

Despite a user's best efforts, a device can be lost. To minimise the impact of a lost device, the webOS platform also provides robust recovery measures that enable the employee to return to productivity quickly:

Remote wipe

If a webOS device is ever lost or stolen, the administrator or the owner can remotely wipe all data on the device. The protocols of data erasure can be configured on the device (local wipe) or issued over the air (remote wipe).

Data backup

When a device is lost, a recent backup can minimise user downtime and enable quick restoration of data, applications, and configuration. By default, webOS devices are configured for daily backups; in addition, the backup service employs proven technologies to authenticate the device/user and secure the data in the cloud.

Secure communication

The webOS platform offers a variety of ways to access and transmit data, including cellular data networks, Wi-Fi, and Bluetooth® wireless technology. The platform implements security procedures such as authentication and data encryption to enable users to access company networks without the anxiety of security risks.

Wi-Fi

The webOS platform supports the enterprise-grade security standards WPA and WPA2. WPA and WPA2 use 802.1x authentication, message integrity checks, and strong encryption standards. While WPA employs Temporary Key Integrity Protocol (TKIP) encryption, WPA2 employs Advanced Encryption Standard (AES) for data encryption. 802.1x uses Extensible Authentication Protocol (EAP) to authenticate between a wireless device and an access point before the device is granted access to the company network. The webOS platform supports all the popular EAP types: EAP-TLS, PEAP v1/v2, EAP-TTLS, EAP-FAST, and LEAP. This alphabet soup of authentication means that webOS devices can connect to enterprise Wi-Fi networks with a high level of assurance that the communication is protected and secure.

Bluetooth wireless technology

The webOS platform also supports the security features stipulated by Bluetooth specification 2.1. A trusted pair must be formed with the webOS device before any data can be sent or received; this ensures that the connected device is always “known” (authenticated) because a mutually agreed-upon passkey has been exchanged. Further, the data flowing between the devices is encrypted (at link level) with the standards established by the Bluetooth specifications.

Digital certificates

Digital certificates are electronic signatures that confirm the identity of the server. The webOS platform uses digital certificates to:

- Establish secure SSL connections to the server from the email, calendar, contacts, and browser applications

- Secure Wi-Fi connections with WPA and WPA2 protocols
- Digitally sign applications to prevent malware and unauthorised applications

Root certificates for major certificate authority (CA) are included in webOS. In addition, enterprises can install their own private and self-signed certificates to allow webOS devices to securely connect to a network. All certificates are stored in the platform’s certificate library and are accessible by Palm applications, Palm Services, Wi-Fi, and third-party applications developed with the Palm Mojo Software Development Kit (SDK).

For details on how to install digital certificates and register with the platform’s certificate library, go to kb.palm.com/wps/portal/kb/common/article/40069_en.html

E-Mail

The webOS platform supports security mechanisms offered by Microsoft Exchange ActiveSync® (EAS), POP, and IMAP email protocols.

When a webOS device is configured to sync with Microsoft Exchange Server, it employs the enterprise-grade EAS protocol. The SSL connection between the server and the device is secured with a self-signed or CA certificate; unless the required certificates are installed and registered with the platform’s certificate library, the EAS sync cannot proceed. As described in the next section, the platform supports several EAS policies to help assure the network administrator that webOS devices will not compromise company data. With EAS, the user can securely sync email (including folders), contacts, calendars, and tasks as well as look up addresses in the corporate directory with the Global Address List (GAL) feature. This balance between usability and security keeps users at their productive best.

Browser

The powerful web browser in webOS allows users to safely browse and interact with secure websites (https://) using SSL. When interacting with secure websites, users must pay attention to certificate errors/warnings and ensure that the connection is secure (i.e., the URL starts with https://). In general, users should avoid sensitive activities on unsecured networks such as unprotected public Wi-Fi hotspots (that do not employ WPA or WPA2 security).

Protect data on the device

Users need more than just secure communication. They also need secure devices. The webOS platform provides various ways to protect data on the device. Users can lock webOS devices with a password that prevents unauthorised access when the device is not in use.

To unlock the device and gain access, users must authenticate their identity by entering the right password. Because a phone is difficult to secure physically, it's very important that an unauthorised person not be able to access it. Authentication helps protect corporate data and network access in the event of device theft or loss.

In an enterprise environment, network administrators can secure webOS devices connecting to their network by enforcing password policies. When a webOS device is configured to access Microsoft Exchange, the Exchange ActiveSync (EAS) policies are pushed to the device over the air, thereby forcing the user to protect the device with a password. In addition, a user can configure multiple Exchange accounts on a webOS device, and the platform intelligently enforces the most stringent intersection of policies. No additional steps are necessary for the user or the network administrator; the webOS platform simply does the right thing so that the user can continue to get access without violating policies enforced by either Exchange server.

The webOS platform supports the following EAS policies:

- Enforce password lock on the device.
- Define minimum length for the password. For webOS phones, alphanumeric passwords can be between 2 and 18 characters. Numeric passwords can be up to 32 numbers.
- Require both numbers and letters. Palm webOS phones support a combination of numeric and non-numeric characters to enable stronger passwords. Password strength plays an important role in securing a device.
- Maximum failed password attempts. Administrators can limit the number of failed login attempts on a webOS phone. When the limit is exceeded, the device data is wiped (aka local wipe). This is the single usually best way to defeat a trial-and-error attempt to unlock the device by entering various password permutations.

- Auto-lock after a period of inactivity. The screen locks after 3 minutes of inactivity and administrators can set password timeouts up to 30 minutes.

For more details on how webOS supports EAS policies, go to kb.palm.com/wps/portal/kb/common/article/58353_en.html

Application environment

In webOS platform, all applications run in a “sandboxed” environment to help limit the unauthorised access to other applications’ data and services. The applications can interact with each other only using the specific APIs and services offered by the OS within the Mojo environment. Mojo provides a number of mechanisms to allow for development of secure applications, including support for cryptography and the use of SSL for remote connections. Certificate validation is enforced when connecting over SSL through Mojo.

Palm webOS applications beyond those preloaded on the device can be downloaded only from the Palm App Catalog. All applications downloaded from the catalog are digitally signed by Palm and verified at install time.

The Mojo SDK is available for download from developer.palm.com

Remote wipe

If a webOS device is ever lost or stolen, the data on the device can be erased remotely either by the device owner or the enterprise IT administrator. The following mechanisms minimise the abuse of data if a webOS device is lost or stolen:

- As discussed earlier in this document, the enterprise IT administrator can limit the number of failed password attempts. Once the limit is exceeded, all the data and settings on the device are erased.
- If the webOS device connects to Microsoft Exchange, the administrator can initiate a remote wipe from the Exchange Management Console. Alternatively, the device owner can initiate the remote wipe by logging in to Outlook Web Access (Exchange 2007 only).
- The device owner can log in to the Palm User Console with a Palm profile ID and password to remotely erase all data off the lost or stolen device. A user can erase a device only if the device is registered with a Palm profile. As further protection against malicious programs or accidental erasure, the user must complete the CAPTCHA challenge before initiating their remote erase.

Data backup and restore

If the device is lost or compromised, proper backup and recovery procedures can restore users to productivity quickly. Palm offers backup and restore services for webOS devices so that certain user data and device customisation settings¹ aren't lost if a device is reset or replaced. The data is backed up to Palm-operated servers and protected with industry-recognised security policies and procedures.

The connection between the device and backup server is mutually authenticated and secured by SSL, and the data is encrypted in transit. At rest, the data is encrypted using AES-128 with user-specific keys. During a restore operation, data is accessible only after the user logs in with the Palm profile email and password registered to the device. Moreover, all passwords stored locally on the device are encrypted, and the device can be locked by a local PIN or password enabled either by the user or an IT administrator via Microsoft Exchange settings.

Palm webOS devices are configured to back up data and user preferences by default to Palm-operated servers. The user can disable backup services at any time with the included Backup application; once a user disables the device backup, the backup data associated with the profile is erased from Palm's servers.

For details on which data and settings are backed up, go to kb.palm.com/wps/portal/kb/common/article/19388_en.html

Conclusion



Secure application environment
Sandboxed data storage
PIN / password protection
Encrypted passwords / credentials



Secure connection
128-bit SSL
Secure Wi-Fi (WPA, WPA2)



AES-encrypted data store
Mutual authentication based on digital certificates, use of credentials
Signed applications in App Catalog

The Palm webOS platform provides protection of data in transit, at rest, or backed up with the Palm backup service. It supports the most widely used corporate security policies and provides methods to recover quickly from device loss or theft. Palm webOS is a secure mobile computing platform that enterprises can deploy with confidence.

In the end, some onus also rests on users to utilise the platform's capabilities to protect against security attacks. Companies may consider training employees on the organisation's security policies and practices to remind them about common-sense practices such as locking the device when not in use, avoiding sensitive activities when connected to unprotected Wi-Fi networks, and heeding any digital certificate warnings.

To learn more about Palm's security policy, go to palm.com/security

1. Back up includes Contacts, Calendars, Memos, and Tasks along with preferences and any software downloaded from the App Catalog.

© 2010 Palm, Inc. All rights reserved. Palm, Pre, Pixi, webOS, Mojo, Synergy and Touchstone are trademarks of Palm, Inc. Microsoft, ActiveSync and Outlook are either registered trademarks or trademarks of the Microsoft group of companies.

For additional information:

Palm security policy:

palm.com/security

Palm webOS for your business:

palm.com/uk/en/business/pre-index.html

Handset information:

palm.com/uk

Gartner:

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

A Philippe Winthrop report:

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

A Philippe Winthrop blog:

enterprisemobilitymatters.com