



# Palm webOS

## Implementation Guide

First edition, for webOS version 1.4



© Copyright 2010 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

This manual may not be copied, in whole or in part, without written consent.

Every effort has been made to ensure that the information in this manual is accurate. Palm is not responsible for printing or clerical errors.

Palm, Inc., 950 W. Maude Ave., Sunnyvale CA 94085-2801 [palm.com](http://palm.com)

Palm, Mojo, Palm OS, Pixi, Pre, Synergy, and webOS are trademarks of Palm, Inc., a subsidiary of Hewlett Packard Company. Facebook is a registered trademark of Facebook, Inc. Google, Gmail, and Google Talk are trademarks of Google, Inc. LinkedIn and the LinkedIn logo are registered trademarks in the United States and/or other countries. Microsoft, ActiveSync, Excel, Outlook, and PowerPoint are trademarks of the Microsoft group of companies. Yahoo! and Yahoo! Mail are registered trademarks of Yahoo! Inc. Mention of third-party products is for informational purposes only and constitutes neither an endorsement nor a recommendation. Palm assumes no responsibility with regard to the performance or use of these products.



# What's in this guide?

This guide provides best practices for deploying, configuring, and managing Palm® webOS™ phones in enterprise environments.

The guide starts with an overview of Palm webOS benefits for enterprise IT and system administrators.

Subsequent sections provide guidelines for preparing your network, configuring webOS devices, and managing your fleet.

The appendix covers the web-based utility Palm webOS Doctor.

# Contents

|          |   |          |
|----------|---|----------|
| <b>1</b> | <b>What is webOS? .....</b>                     | <b>1</b> |
| 1.1      | Always connected.....                           | 2        |
| 1.2      | Always up to date.....                          | 4        |
| 1.3      | Palm Synergy .....                              | 5        |
| 1.4      | Shortest path to enterprise mobility.....       | 6        |
| <b>2</b> | <b>System requirements.....</b>                 | <b>7</b> |
| 2.1      | Corporate groupware or email server.....        | 7        |
| 2.2      | Palm webOS phones .....                         | 7        |
| 2.3      | Network services .....                          | 7        |
| <b>3</b> | <b>Preparing network access .....</b>           | <b>8</b> |
| 3.1      | Microsoft Exchange ActiveSync (EAS) .....       | 9        |
| 3.1.1    | Microsoft Direct Push services .....            | 9        |
| 3.1.2    | EAS security policies .....                     | 9        |
| 3.1.3    | Global Address List (GAL).....                  | 9        |
| 3.1.4    | Additional supported EAS features.....          | 10       |
| 3.1.5    | Exchange ActiveSync network configuration ..... | 10       |
| 3.1.6    | Exchange account setup .....                    | 11       |
| 3.2      | POP3 and IMAP4 email services .....             | 12       |
| 3.3      | Network security .....                          | 13       |
| 3.3.1    | Supported Wi-Fi security standards.....         | 13       |
| 3.3.2    | Supported authentication methods .....          | 14       |
| 3.3.3    | Determining device password policies.....       | 14       |
| 3.3.4    | WPA/WPA2 enterprise network configuration.....  | 14       |
| 3.4      | Additional resources.....                       | 15       |

|          |  |           |
|----------|--|-----------|
| <b>4</b> | <b>Configuring webOS devices .....</b>                               | <b>16</b> |
| 4.1      | Summary of the configuration process.....                            | 17        |
| 4.2      | How wireless cloud services are coordinated.....                     | 18        |
| 4.2.1    | Palm Services.....   | 19        |
| 4.2.2    | Microsoft Exchange .....   | 19        |
| 4.2.3    | Cloud services .....   | 19        |
| 4.3      | Establishing Palm profile credentials .....                          | 21        |
| 4.4      | Setting up Exchange email accounts .....                             | 22        |
| 4.5      | Setting up POP3, IMAP4, or Yahoo! Mail email accounts .....          | 24        |
| 4.6      | Deleting an email account.....                                       | 26        |
| 4.7      | Configuring Wi-Fi settings .....                                     | 27        |
| 4.8      | Palm mobile hotspot.....   | 29        |
| 4.9      | Installing security certificates .....                               | 31        |
| 4.9.1    | Installing a certificate from an email attachment .....              | 31        |
| 4.9.2    | Installing a certificate by copying it to a device's USB drive ..... | 33        |
| 4.9.3    | Installing a certificate via Outlook Web Access .....                | 35        |
| 4.10     | Deleting security certificates .....                                 | 36        |
| 4.11     | Installing webOS applications.....                                   | 38        |
| 4.11.1   | Installing an application via the Palm App Catalog.....              | 39        |
| 4.11.2   | Installing an application via an unpublished URL .....               | 40        |
| 4.12     | Copying personal files to the USB drive .....                        | 42        |
| 4.13     | Linking to cloud-based services .....                                | 45        |
| 4.13.1   | Adding an account .....  | 46        |
| 4.13.2   | Removing an account .....  | 48        |
| 4.14     | Transferring personal PIM data to webOS.....                         | 50        |
| 4.14.1   | From web-based accounts to webOS .....                               | 50        |
| 4.14.2   | From desktop organizer to webOS .....                                | 51        |
| 4.14.3   | Desktop email and PIM applications to webOS .....                    | 51        |

|          |  |           |
|----------|--|-----------|
| <b>5</b> | <b>Managing webOS devices</b>                | <b>52</b> |
| 5.1      | What's backed up (and what's not)            | 53        |
| 5.2      | Turning backup off                           | 54        |
| 5.3      | Device updates                               | 55        |
| 5.4      | Overview of wiping a device                  | 57        |
| 5.5      | Remote wipe from Exchange Server             | 58        |
| 5.6      | Remote wipe from Outlook Web Access          | 59        |
| 5.7      | Remote wipe from a Palm profile account      | 60        |
| 5.8      | Local wipe                                   | 61        |
| 5.9      | Restoring a device                           | 63        |
| 5.10     | Manually reinstating files on the USB drive  | 64        |
| 5.11     | Reinstating personal data after a wipe       | 65        |
| <br>     |  |           |
|          | <b>Appendix A: Palm webOS Doctor</b>         | <b>66</b> |
| A.1      | Palm webOS Doctor system requirements        | 67        |
| A.2      | How to use Palm webOS Doctor                 | 68        |
| A.3      | Removing the back cover of a Palm Pre phone  | 69        |
| A.4      | Removing the back cover of a Palm Pixi phone | 71        |
| <br>     |  |           |
|          | <b>Index</b>                                 | <b>74</b> |

# 1 What is webOS?

Palm webOS is Palm's next-generation operating system. Designed around an incredibly fast and intuitive user experience and optimized for the multitasking user, webOS integrates the power of a window-based operating system with the simplicity of a browser. Applications are built using standard web technologies but have access to device-based services and data.

Palm webOS is designed to run on a variety of hardware with different screen sizes, resolutions, and orientations, with or without keyboards. It works best with a touch screen (although it doesn't require one). Because the user interface and application model are built around web technology, the range of suitable hardware platforms is quite wide, requiring only a CPU, some memory, a wireless data connection, a display, and a means for interacting with the UI and entering text.

You can think of webOS applications as native applications that are built from the same standard HTML, CSS, and JavaScript used to develop web applications. Palm has extended the standard web development environment through a JavaScript framework called Mojo that provides standardized UI widgets, and access to selected device hardware features and services.

The user experience is optimized for launching and managing multiple applications at once. Palm webOS is designed around multitasking and makes it simple to run background applications, switch between applications in a single step, and easily handle notifications and events without losing context.

Palm webOS applications are built with common web development tools following typical design and implementation practices for Ajax applications. But webOS applications are installed and run directly on the device, similar to native applications on other operating systems.

## 1.1 Always connected

Palm webOS phones are always connected to the data and services that support the phone. Each service manages its own data. Any Personal Information Manager (PIM) data that is not managed by another service is automatically backed up by Palm Services.



### Microsoft Exchange

Palm webOS phones work within Exchange ActiveSync environments without additional servers or middleware. Each phone supports up to 16 EAS accounts, with or without security policies. Each account provides true-IP push email, contacts, calendar, and tasks along with access to Global Address List lookup (GAL). Wireless push services are routed primarily through an available Wi-Fi data connection or secondarily via the phone's wireless data service provided by the carrier.





## Cloud services

Depending upon the carrier, webOS phones can synchronize with email, calendar, contacts, and tasks services from Google™, Facebook, LinkedIn®, and Yahoo!® as well as Microsoft Exchange. Users can upload photos and videos or share them via MMS or email.

## Palm Services

Palm Services provide automated software updates, backup services, and access to the Palm App Catalog. Once per day, each user's account settings (but **never** passwords), pointers to applications downloaded from the Palm App catalog, browser bookmarks, plus PIM data not managed by another service will be automatically backed up to their Palm Profile account.

Note that any data or files on the phone's USB drive will need to be backup separately. For details about what is and what is not backed up, see [Palm Knowledge Base article #19388](#). For a list of third-party synchronization solutions that can back up the phone and the USB drive, see the website [www.palm.com/sync-solutions](http://www.palm.com/sync-solutions).

If a user's phone has been lost, stolen, or wiped, the user can wirelessly restore their phone or reinstate their data and applications onto a replacement phone. For step-by-step instructions, see [topic 5.9 "Restoring a device"](#).

## Non-Exchange services

Although this document primarily covers Microsoft Exchange, webOS phones may be synchronized with Lotus Notes and Groupwise, or may use POP or IMAP-based email servers. Please contact your HP Palm or wireless carrier sales representative for details.

## 1.2 Always up to date

Via automated wireless updates, Palm webOS phones always have the latest system software, current versions of installed applications, and up-to-the-minute Exchange ActiveSync security policies.



### webOS updates

Updates to webOS and other system software add functionality, improve performance, and, of course, fix bugs. System updates are automatically installed over the air, keeping webOS devices always up to date.

### App Catalog updates

Applications downloaded from the Palm App Catalog can be manually updated at any time with the Update application. You can choose to update all applications, individual applications, or selectively refuse updates. You stay in control of your applications.

### EAS security policies

Exchange Server automatically pushes EAS security policy updates to all webOS devices in the fleet. No user action or intervention is required.

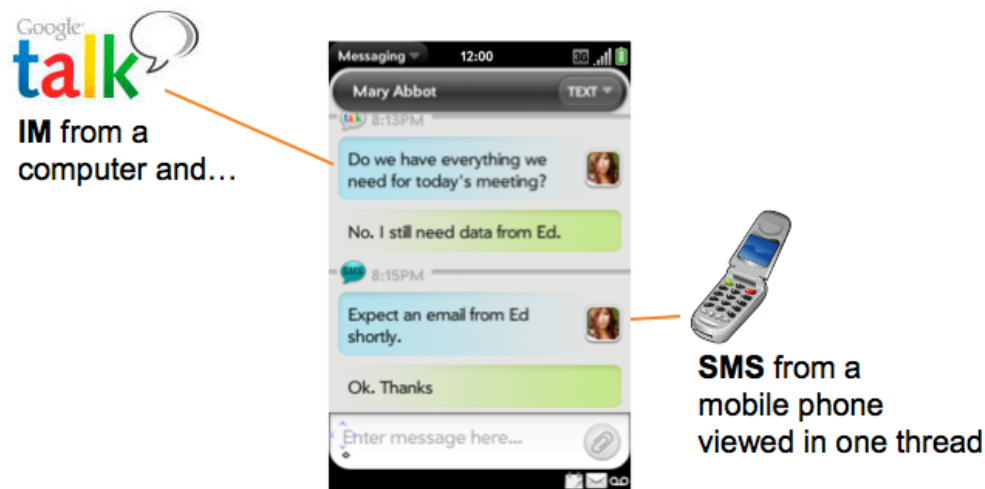
## 1.3 Palm Synergy

An important feature of webOS is Palm Synergy, which displays information from several sources together but synchronizes that information separately.

For example, if a user has a work calendar managed by MS Exchange and a personal work calendar managed by Google, those two calendars may be shown together. The same principle applies to contacts, email, and messaging.



Palm Synergy cleverly works in other places. For example, a text conversation that begins in IM on a computer and continues in SMS can be viewed together in a single thread.



## 1.4 Shortest path to enterprise mobility

The webOS application model combines the ease of development and maintenance of a web application with the deep integration available to native applications, significantly advancing the mobile user experience while keeping application development simple.



You can think of webOS applications as native applications that are built from the same standard HTML, CSS, and JavaScript used to develop web applications.

Palm has extended the standard web development environment through a JavaScript framework called Mojo that provides standardized UI widgets, and access to selected device hardware and services.

In addition, code developers can use the Plug-in Development Kit (PDK) to port C/C++ applications to webOS, including those that use OpenGL ES 1.1 or 2.0. The PDK is used primarily by developers seeking to port existing code libraries or incorporate 3D graphics.

For more details about the ease and speed of developing webOS applications, see the Palm Developer Center at [developer.palm.com](http://developer.palm.com).

## 2 System requirements

In order to deploy webOS devices within your enterprise, you need the following servers, devices, and network services.

### 2.1 Corporate groupware or email server

At least one of the following:

- Exchange ActiveSync for Exchange Server (EAS) 2003 with Service Pack 2
- Exchange ActiveSync for Exchange Server (EAS) 2007 with Service Pack 1
- Exchange ActiveSync for Exchange Server (EAS) 2010
- POP- or IMAP-based email server

### 2.2 Palm webOS phones

Any mix of the following:

- Palm Pre
- Palm Pixi
- Palm Pre Plus
- Palm Pixi Plus

All phones require active data service from a carrier in order to be configured.

All phones require webOS version 1.4 or later.

### 2.3 Network services

In addition, you may need to support:

- WPA/WPA2 Enterprise Wi-Fi security
- Security certificates and root identities

## 3 Preparing network access

This section provides guidelines for preparing your network so that Palm webOS devices may use push services and access network-based corporate resources.

Palm webOS phones support industry-standard IMAP4- and POP3-enabled mail solutions on a range of server platforms including Windows, UNIX, Linux, and Mac OS X. Each phone can access up to 16 email accounts, including multiple push Exchange accounts.

**Important:** *The user's email account information, including Exchange user ID and password, are securely stored on the device but are never backed up to the user's Palm profile.*

### Topics in this section:

[3.1 Microsoft Exchange ActiveSync \(EAS\)](#)

[3.2 POP3 and IMAP4 email services](#)

[3.3 Network security](#)

[3.4 Additional resources](#)

*To go to a topic, click the underlined link.*



## 3.1 Microsoft Exchange ActiveSync (EAS)

Palm webOS phones work within Exchange ActiveSync environments without additional servers or middleware. Devices are managed using standard Microsoft tools.

### 3.1.1 Microsoft Direct Push services

Each webOS phone supports up to 16 EAS accounts, with or without security policies. Each account provides true-IP push email, contacts, calendar, and tasks plus Global Address List (GAL). Wireless push services are routed primarily through an available Wi-Fi data connection or secondarily via the phone's wireless data service provided by the carrier.

### 3.1.2 EAS security policies

Palm webOS supports these Exchange policies:

- Password complexity (numeric or alphanumeric)
- Minimum password length (2-18 for alphanumeric, 4-18 for numeric)
- Maximum number of failed password attempts before local wipe
- Autolock after X minutes of inactivity
- EAS wipe

If a user has multiple EAS accounts, the most stringent combination of security policies is applied to all the EAS accounts. For example, if one account has a 5-minute timeout period and another account requires a 10-digit password, all EAS accounts for that user will require both policies.

For details about these policies and how to set up EAS policies on multiple accounts, see [Palm Knowledge Base article #58353](#)

### 3.1.3 Global Address List (GAL)

Palm webOS phones can access your company's Global Address List to search for a contact's phone number or corporate email address. This feature is supported across multiple EAS accounts.

### 3.1.4 Additional supported EAS features

Palm webOS also supports:

- Access to server folders
- Task synchronization
- Flagging email messages for follow-up

If you are new to Exchange ActiveSync or have recently installed it, you may wish to review the following two topics:

### 3.1.5 Exchange ActiveSync network configuration

Check the following:

- Open port 443 on the firewall. For details on this requirement (opening the HTTPS port — 443) see the following Microsoft TechNet article: [technet.microsoft.com/en-us/library/aa995962%28EXCHG.80%29.aspx](http://technet.microsoft.com/en-us/library/aa995962%28EXCHG.80%29.aspx)
- Install a server certificate on the front-end Exchange server. In the Authentication Method properties, turn on basic authentication only to require an SSL connection to the Microsoft Server ActiveSync directory of your IIS.
- Check that a server certificate is installed on your Microsoft Internet Security and Acceleration (ISA) Server. Update the public DNS so that incoming connections are properly resolved.
- Verify that your network's DNS returns a single, externally routable address to the Exchange ActiveSync server for both intranet and Internet clients.
- Create a web listener on your Microsoft ISA Server. For details, see the Microsoft Exchange documentation at [technet.microsoft.com/en-us/library/bb794914.aspx](http://technet.microsoft.com/en-us/library/bb794914.aspx)
- Also create an Exchange web client access publishing rule. For details, see the Microsoft Exchange documentation at [technet.microsoft.com/en-us/library/aa997148\(EXCHG.80\).aspx](http://technet.microsoft.com/en-us/library/aa997148(EXCHG.80).aspx)
- Set the idle session timeout to 30 minutes on all firewalls and network appliances.



### 3.1.6 Exchange account setup

Check the following:

- For Exchange Server 2003, check the Active Directory to ensure that Exchange ActiveSync is enabled for specific users or groups. For Exchange Server 2007 or Exchange Server 2010, check the Recipient Configuration in the Exchange Management Console.
- Using the Exchange Server 2003 System Manager or the Exchange Server 2007 or later Management Console, configure mobile features, policies, and device security settings.
- For Exchange Server 2003, in order to perform remote wipes from Exchange Server, you need to install the Microsoft Exchange ActiveSync Mobile Administration Web Tool.

Note that for Exchange Server 2007 or later:

- Remote wipes can be issued directly from within Exchange Management Console.
- Each user has the ability to self-serve a remote wipe of their phone via their Outlook Web Access (OWA) client.



## 3.2 POP3 and IMAP4 email services

Palm webOS phones work with POP3 and IMAP4 email servers. Additionally, webOS supports IMAP IDLE (RFC 2177) which is a subset of P-IMAP protocol. For optimum security, these solutions should require user authentication and SSL. The mail servers should be located inside a DMZ sub-network, behind a corporate firewall, or both.

With SSL, Palm webOS phones support 128-bit encryption and X.509 certificates issued by the major certificate authorities. They also support strong authentication methods including industry-standard MD5 Challenge-Response and NTLMv2.

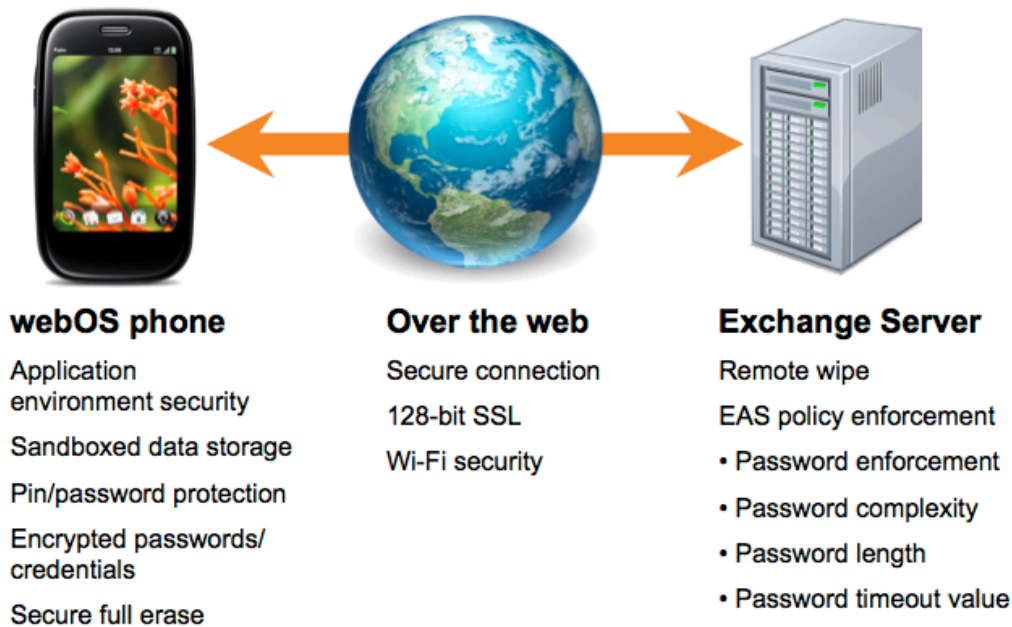
For the full list of pre-installed certificates, see [Palm Knowledge Base article #47857](#).

Check the following:

- For added security, install a digital certificate on the server from a trusted certificate authority (CA).
- Open port 993 in the firewall and make sure that the proxy server is set to IMAP over SSL. This allows Palm webOS phones to retrieve email from your POP or IMAP server.
- Open either port 587, 465, or 25. This allows Palm webOS phones to send email.

## 3.3 Network security

Palm webOS phones support enterprise-grade security standards at all points in the data chain between the device and network servers.



### 3.3.1 Supported Wi-Fi security standards

Palm webOS phones support these 802.1x wireless networking security standards:

- WEP
- WPA Personal (PSK)
- WPA Enterprise with Temporary Key Integrity Protocol (TKIP) encryption
- WPA2 Enterprise with Advanced Encryption Standard (AES) encryption

### 3.3.2 Supported authentication methods

Palm webOS devices support the following 802.1x authentication methods for WEP, WPA Enterprise, and WPA2 Enterprise networks:

- EAP-TLS
- PEAP v1/v2
- EAP-TTLS
- EAP-FAST
- LEAP

### 3.3.3 Determining device password policies

Exchange ActiveSync security policies are wirelessly pushed to Palm webOS phones configured to access Microsoft Exchange accounts. No user intervention is required.

If you're not using Exchange ActiveSync, you should suggest that Palm webOS phone users to set and use a device password with a short timeout period. Data on lost or stolen devices will be inaccessible without the password.

### 3.3.4 WPA/WPA2 enterprise network configuration

Check the following:

- Configure the authentication type for any network appliances so that they are compatible with Palm webOS: EAP-TLS, PEAP v1/v2, EAP-TTLS, EAP-FAST, or LEAP.
- Enable 802.1x on the authentication server. If necessary, install a server certificate and assign network access permissions to users and groups.
- Configure all wireless access points so that they are compatible with Palm webOS 802.1x authentication: EAP-TLS, PEAP v1/v2, EAP-TTLS, EAP-FAST, or LEAP.
- Enter the corresponding RADIUS server information and then test it with a personal computer.
- If you're using certificate-based authentication, configure your public key infrastructure to support device- and user-based certificates with the corresponding key distribution process.
- Check that your certificate formats are compatible with both your authentication server and your fleet of Palm webOS phones.

## 3.4 Additional resources

In addition to this guide, the following may be useful:

- Palm webOS in Enterprise web page at [palm.com/us/business](http://palm.com/us/business)
- Exchange Product Overview at [technet.microsoft.com/en-us/library/bb124558.aspx](http://technet.microsoft.com/en-us/library/bb124558.aspx)
- Deploying Exchange ActiveSync at [technet.microsoft.com/en-us/library/aa995962.aspx](http://technet.microsoft.com/en-us/library/aa995962.aspx)
- Exchange 2003 Technical Documentation Library at [technet.microsoft.com/en-us/library/bb123872\(EXCHG.65\).aspx](http://technet.microsoft.com/en-us/library/bb123872(EXCHG.65).aspx)
- Exchange 2007 Technical Documentation Library at [technet.microsoft.com/en-us/library/bb124558\(EXCHG.80\).aspx](http://technet.microsoft.com/en-us/library/bb124558(EXCHG.80).aspx)
- Exchange 2010 Technical Documentation Library at [technet.microsoft.com/en-us/library/bb124558.aspx](http://technet.microsoft.com/en-us/library/bb124558.aspx)
- Managing Exchange ActiveSync Security at [technet.microsoft.com/en-us/library/bb232020\(EXCHG.80\).aspx](http://technet.microsoft.com/en-us/library/bb232020(EXCHG.80).aspx)
- Wi-Fi for Enterprise web page at [wi-fi.org/enterprise.php](http://wi-fi.org/enterprise.php)
- Palm Pre and Palm Pixi User Guides, available for download at [kb.palm.com/wps/portal/kb/common/article/20198\\_en.html](http://kb.palm.com/wps/portal/kb/common/article/20198_en.html)

To take a tour of webOS, watch the video “Learn how it works” at [palm.com/us/products/software/webos/index.html#video](http://palm.com/us/products/software/webos/index.html#video).

You can also view the same videos on a webOS device by downloading the free Palm Videos application from the Palm App Catalog.

## 4 Configuring webOS devices

This section provides guidelines for configuring webOS devices for use within Exchange ActiveSync environments or with POP3- or IMAP4-based email systems.

### Topics in this section:

- [4.1 Summary of the configuration process](#)
- [4.2 How wireless cloud services are coordinated](#)
- [4.3 Establishing Palm profile credentials](#)
- [4.4 Setting up Exchange email accounts](#)
- [4.5 Setting up POP3, IMAP4, or Yahoo! Mail email accounts](#)
- [4.6 Deleting an email account](#)
- [4.7 Configuring Wi-Fi settings](#)
- [4.8 Palm mobile hotspot](#)
- [4.9 Installing security certificates](#)
- [4.10 Deleting security certificates](#)
- [4.11 Installing webOS applications](#)
- [4.12 Copying personal files to the USB drive](#)
- [4.13 Linking to cloud-based services](#)
- [4.14 Transferring personal PIM data to webOS](#)

*To go to a topic, click the underlined link.*



## 4.1 Summary of the configuration process

The normal process for configuring a webOS device is to:

- Establish Palm profile credentials to enable automated software updates, backup services, and access to the Palm App Catalog
- Set up email accounts (up to 16 accounts, including multiple EAS accounts)

IT or the user may also wish to:

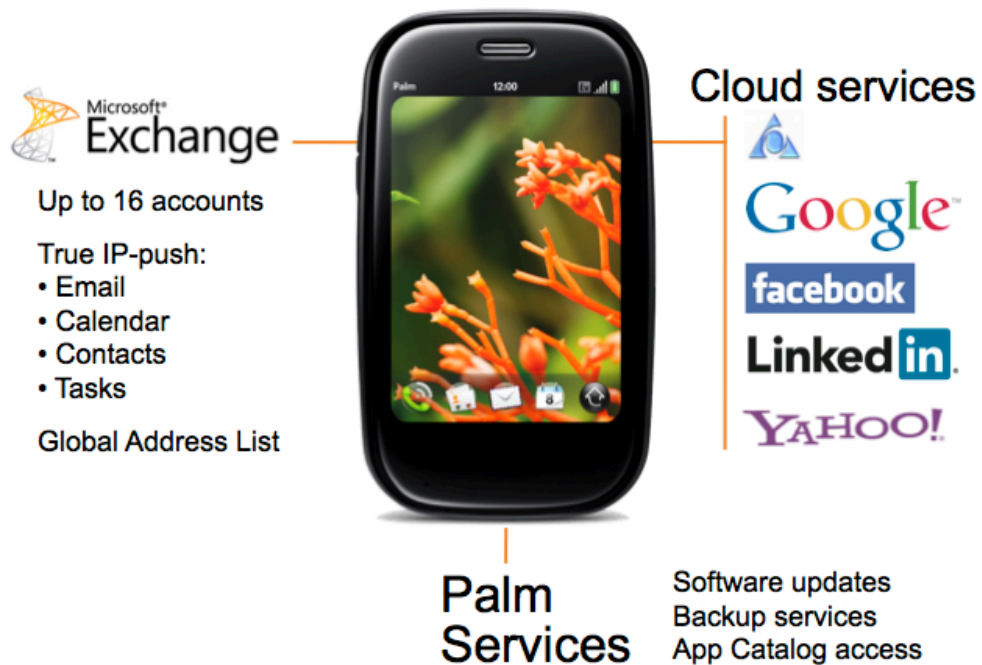
- Configure WPA/WPA 2 Enterprise Wi-Fi settings
- Install security certificates and root identities

Users may wish to:

- Copy media and other personal files to the phone's USB drive
- Link to cloud-based services such as Facebook, Google™, or LinkedIn®
- Transition their personal PIM data from:
  - Palm OS® to Palm webOS
  - Another mobile device to webOS
  - Desktop email and PIM applications to webOS

## 4.2 How wireless cloud services are coordinated

Palm webOS phones rely on over-the-air services for email, backups, updates, data synchronization, and application installation. At a minimum, each webOS phone must have active wireless voice and data service from a carrier and be registered with a Palm profile. Optionally, each phone can be registered with one or more Exchange Servers for push services in addition to being registered with cloud-based services for synchronizing contacts, calendars, and other data.





### 4.2.1 Palm Services

Registering a Palm profile provides secure access to Palm Services:

- Automated device updates whenever webOS is patched or replaced with a new version.
- Access to the Palm App Catalog so that the user may search for and install applications over the air. This access is also essential for installing custom corporate applications via an unpublished URL.
- Automated backup of pointers to installed applications from the Palm App Catalog so that these may be reinstated after a phone has been hard reset or remotely wiped.
- Automated Personal Information Manager (PIM) data backup (contacts, calendar, tasks, memos) for any data that is not being managed by another service.
- Automated backup of web browser bookmarks.

***Important:** Files on the phone's USB drive are not backed up by Palm Services. These files include photos, videos, web downloads, and email attachments plus desktop files copied to the USB drive. Either manually copy those files using USB mode or use third-party synchronization software. For details on using USB mode, see [topic 4.12 "Copying personal files to the USB drive."](#)*

### 4.2.2 Microsoft Exchange

Setting up a push Exchange email account also automatically links the phone to Exchange for push calendar, push contacts, push tasks, and Global Address List (GAL) services. New and updated EAS security policies are automatically pushed to the phone. If a phone has multiple EAS accounts, then the most stringent combination of EAS security policies is applied to all EAS accounts.

### 4.2.3 Cloud services

Optionally, you can link a webOS phone to cloud-based services such as Google , Facebook, or LinkedIn® . Personal data such as contact information or photos from those services are automatically synchronized with the phone. If a cloud-based service offers multiple services, adding an account within one application automatically adds the other services as well. For example, adding a Google email account also adds a Google account to Contacts, Calendar, and Messaging. You can selectively remove services from individual applications with the Preferences & Accounts command. For step-by-step instructions, see [topic 4.13.2 "Removing an account"](#).

#### 4.2.4 Palm Synergy

Through Palm Synergy, similar data from your Palm profile, Exchange, and the various cloud-based services are displayed together in a single view but synchronized separately. In this example, work data from Exchange plus personal data from Google™ are displayed together.



Everything is kept logically separate during synchronization and updates. There's no cross-pollination, even at the field level.

## 4.3 Establishing Palm profile credentials

Once established, a Palm profile connects your phone to Palm Services to get automatic updates, back up device data, and enable access to the Palm App Catalog.

To establish a phone's Palm profile:

1. Hold down the **Power** button until you see a logo on the screen (approximately five seconds).
2. Enter a working email address and a password.

If you're successful, the phone automatically launches an interactive tutorial that teaches basic navigation gestures.

You can manage your Palm profile from your phone, or from the web at [palm.com/profile](http://palm.com/profile).

### Login page

### Device Details

| Device Details |       |                     |            |         |                |
|----------------|-------|---------------------|------------|---------|----------------|
| Phone Number   | Model | Device ID           | OS Version | Primary |                |
| 14085550050    | Pre   | MEID:A10005064756E5 | 1.40.50    | Yes     | Device Options |

## 4.4 Setting up Exchange email accounts

By setting up an Exchange ActiveSync (EAS) push email account, you automatically set up push Calendar, Contacts, and Tasks services as well. You can selectively remove these services from the individual webOS application with that application's Preferences & Accounts command.

Before you begin, you need this information from the system administrator:

- Mail server name for receiving email
- Server domain name
- Username and password

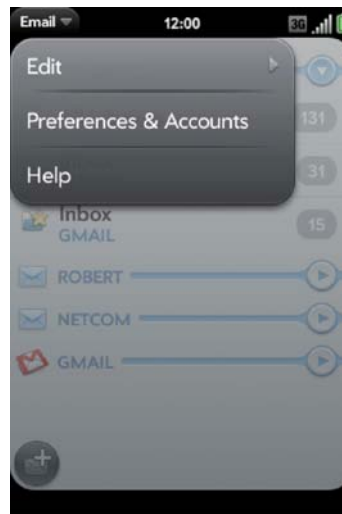
Then follow these steps:

- 1 Open the **Email** application.

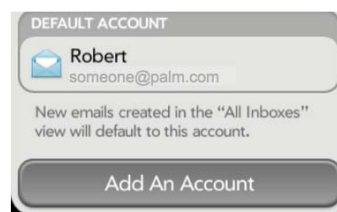


- 2 Tap **Email** in the top-left corner of the screen to open the application menu.

Then tap **Preferences & Accounts**.



- 3 Scroll to the bottom then tap **Add An Account**.

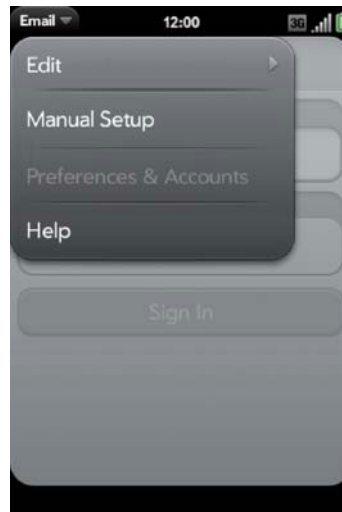


*continued on next page*

- 4 Tap **Email** in the top-left corner of the screen to open the application menu, then tap **Manual Setup**.

**Important:**

*You must select **Manual Setup** in order to enter the incoming server URL and domain name for your Exchange ActiveSync server.*



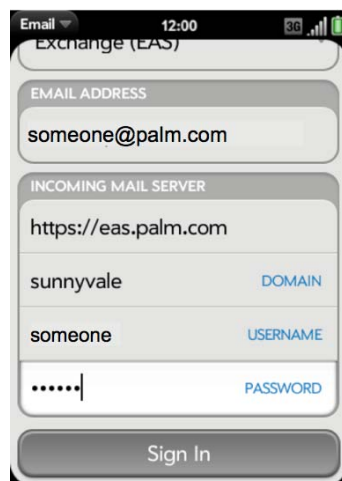
- 5 Change the Mail Type to **Exchange (EAS)**.



- 6 Verify the information in the other fields.

Scroll to the bottom then tap **Sign In**.

**Note:** *To additional EAS accounts, follow steps 2 - 6.*



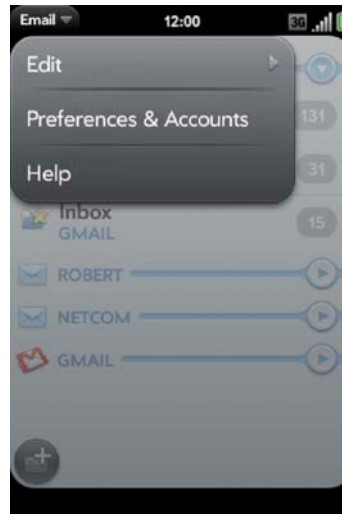
## 4.5 Setting up POP3, IMAP4, or Yahoo! Mail email accounts

To add POP, IMAP, or Yahoo!® Mail email accounts:

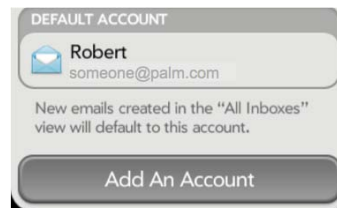
- 1 Open the Email application.



- 2 Tap **Email** in the top-left corner of the screen to open the application menu, then tap **Preferences & Accounts**.



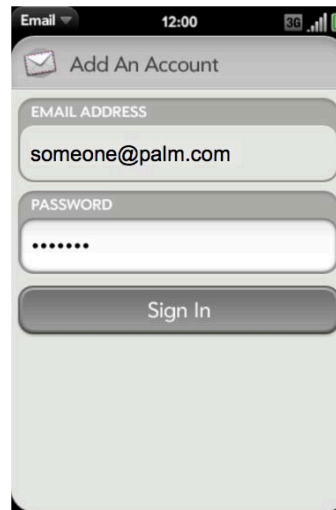
- 3 Scroll to the bottom, then tap **Add An Account**.



- 4 Enter the username and password for this service, then tap **Sign In**.

If successful, webOS will synchronize your email.

If not, you may need to manually enter some settings.



For the major service providers such as Yahoo!™, Google™, or LinkedIn®, you only need your full email address and password. Palm webOS will automatically supply the necessary settings.

For other service providers, after you tap **Sign In**, you may need to manually enter the following settings:

- Account type (POP or IMAP)
- Incoming and outgoing mail server names
- Incoming mail server username and password
- Incoming and outgoing server port numbers
- Any SSL requirements for incoming and/or outgoing mail
- Any authentication (ESMTP) requirements for outgoing mail
- Root folder (IMAP accounts only)

## 4.6 Deleting an email account

To delete an email account and its associated data:

- 1 Open the Email application.



- 2 Tap Email in the top-left corner of the screen to open the application menu, then tap Preferences & Accounts.

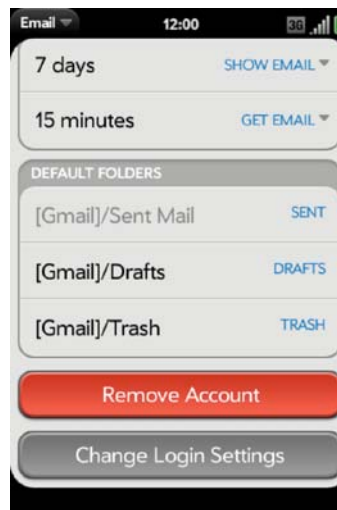


- 3 In the Accounts section, tap the account you wish to delete.

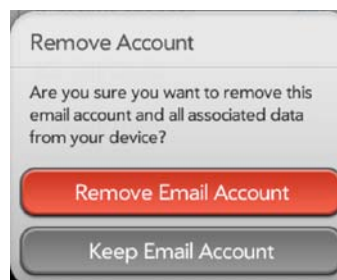
*In this example, Gmail.*



- 4 Scroll to the bottom, then tap Remove Account.



- 5 Confirm by tapping Remove Email Account.





## 4.7 Configuring Wi-Fi settings

Palm webOS phones support 802.1b/g wireless connectivity standards using these authentication standards:

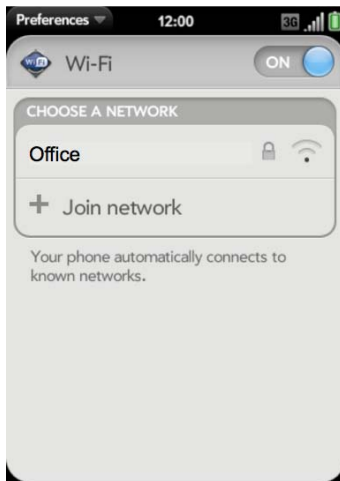
- WEP
- WPA Personal (PSK)
- WPA2 Enterprise with Temporary Key Integrity Protocol (TKIP) encryption
- WPA2 Enterprise with Advanced Encryption Standard (AES) encryption
- 802.1x

To connect to a new Wi-Fi network, do one of the following:

- 1 Launch the **Wi-Fi** application.



- 2 If Wi-Fi is off, tap the slider in the top-right corner to turn it **On**.



- 1 Tap the top-right corner of the screen to open the Connection Menu, then tap **Wi-Fi**.

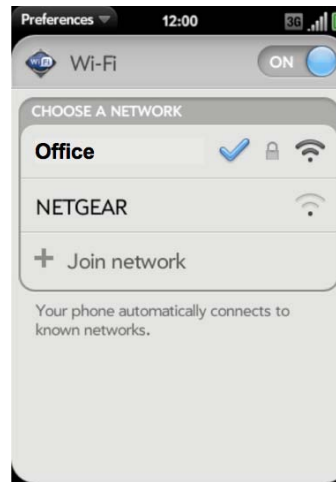


- 2 If Wi-Fi is off, tap **Turn on Wi-Fi**.
- 3 Tap **Wi-Fi Preferences**.

*continued on next page*

The phone will then hunt for visible Wi-Fi networks.

- 1 Once the list of available networks is shown, either:
  - Tap the name of an available network
  - or
  - Tap + Join network

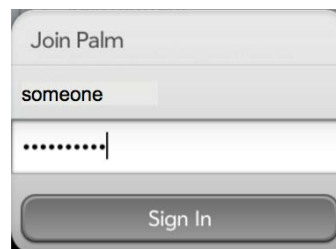


- 2 Enter the necessary credentials:
  - Network name
  - Security:
    - Open, WPA-personal, WEP, Enterprise



Then tap **Connect**.

- 3 If required, enter the Wi-Fi network password, then tap **Sign In**.



Once configured, your phone should be able to automatically rejoin the network whenever it's within range and the phone's Wi-Fi is on.

**Note:** *If your Wi-Fi access method requires certificates, please see [topic 4.9 "Installing security certificates"](#) for details.*

## 4.8 Palm mobile hotspot

Each webOS phone can be configured as a mobile Wi-Fi router that provides service for up to five other devices. Access can be open or limited with a WPA/WPA2 Personal password.



Mobile hotspot service may be bundled with a data plan or may require a monthly surcharge. Also, the carrier may impose monthly upload and download bandwidth limitations.

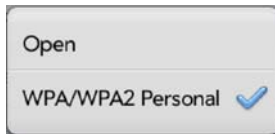
**Note:** As of August 2010, mobile hotspot service is only available from Verizon Wireless.

To enable a phone as a mobile hotspot with WPA/WPA2 Personal security:

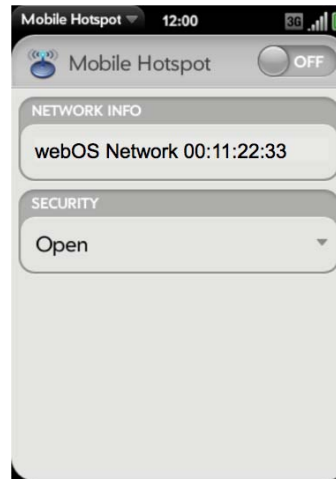
- 1 Open the Mobile Hotspot application.



- 2 Tap **Open** in the Security panel,  
then set it to **WPA/WPA2 Personal**.



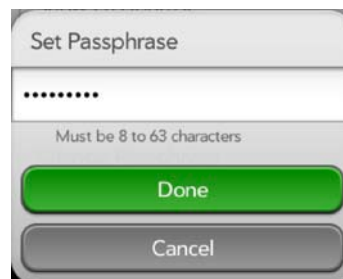
***Note:** You can set the network name to something else by tapping the Network Info field. For example, instead of “webOS Network 00:11:22:33” you could use “ABC”.*



- 3 Tap **Change Passphrase**.

Enter a passphrase  
from 8 to 63 characters.

Tap **Done**.



- 4 Turn on the mobile hotspot by tapping the **On/Off** slider in the top-right corner.

***Note:** When devices connect to your hotspot, you'll be notified with a chime.*

***Note:** You may want to power the phone with a charger while using Mobile Hotspot.*



## 4.9 Installing security certificates

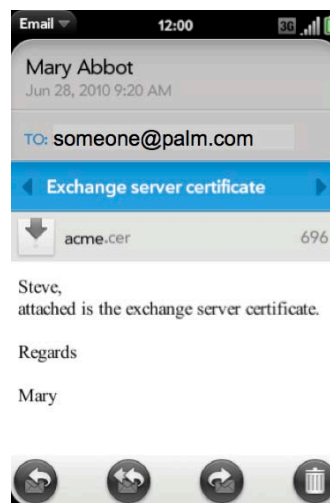
Palm webOS supports SSL CA certificates in X.509 (CER) file format. You can install certificates from an email attachment by copying to the root folder of the device's USB drive or via Outlook Web Access.

*Note:* A number of SSL certificates are preinstalled in webOS that are not visible with Certificate Manager. For the full list of these certificates, see [Palm Knowledge Base article #47857](#).

### 4.9.1 Installing a certificate from an email attachment

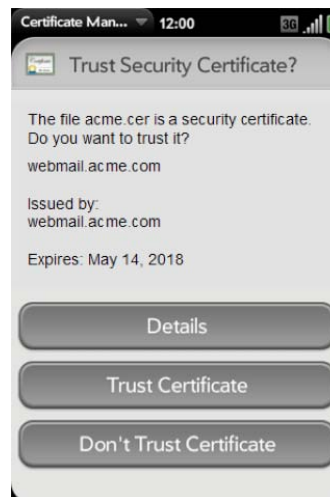
- 1 Open the email with the attached certificate, then tap the attachment.

*In this example, acme.cer*



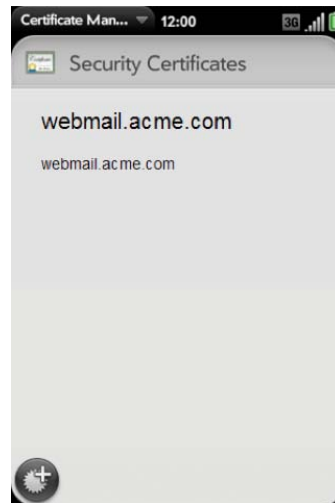
- 2 The Certificate Manager automatically opens.

Tap **Trust Certificate**.



*continued on next page*

- 3 If you're successful, you'll see the certificate in the list of installed certificates.



**Note:** Downloading certificates from the phone's browser works just like installing a certificate from an email—just click on the link containing the certificate and the Certificate Manager will automatically open.

## 4.9.2 Installing a certificate by copying it to a device's USB drive

- 1 Connect your phone to your computer using the Palm USB cable.



- 2 On your phone, tap **USB Drive** (or press **Option + Sym + U**).

On your computer, your phone appears as a removable drive.

On a Windows computer, if the **Found New Hardware** wizard opens, click **Cancel** to close the wizard.



- 3 Open **My Computer** (Windows XP), **Computer** (Windows Vista or Windows 7), or the **Finder** (Mac OS). Double-click the drive representing your phone.

Drag and drop the certificate file to the root folder of your phone's USB drive.

- 4 Repeat step 3 for any intermediate certificates.

*continued on next page*



- 5 To end the connection safely on a Windows computer, right-click the drive representing your phone, and then click **Eject**.

On a Mac computer, drag the drive representing your phone to the **Trash**.

- 6 Wait until the icon representing your phone disappears from view, then disconnect the **Palm USB cable** from the device and the computer.



### 4.9.3 Installing a certificate via Outlook Web Access

- 1 Launch the Web application.

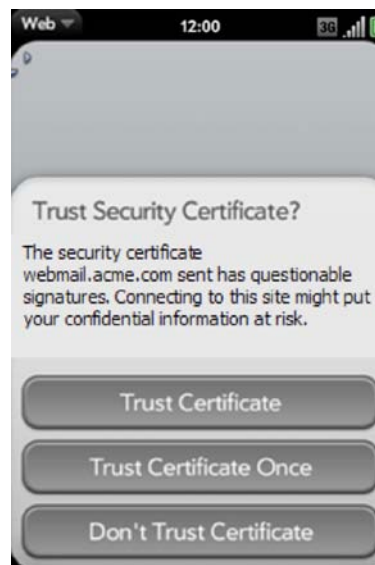


- 2 Open your Outlook Web Access URL.

*In this example, the URL is:  
https://webmail.acme.com*



- 3 Tap Trust Certificate to automatically install the certificate in the library.



## 4.10 Deleting security certificates

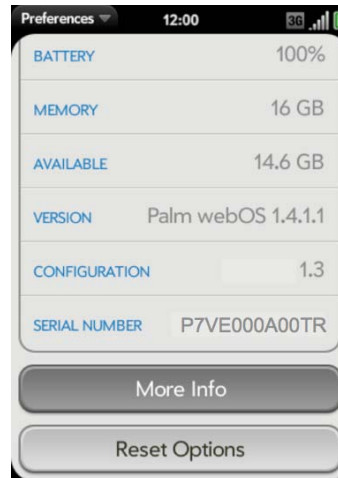
The Certificate Manager is found inside the application menu of the Device Info application.

To delete a certificate:

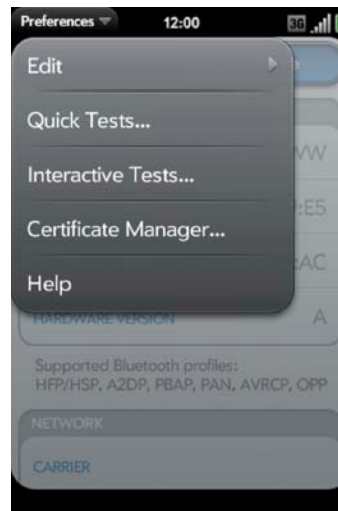
- 1 Open the Device Info application.



- 2 Scroll to the bottom, then tap **More Info**.

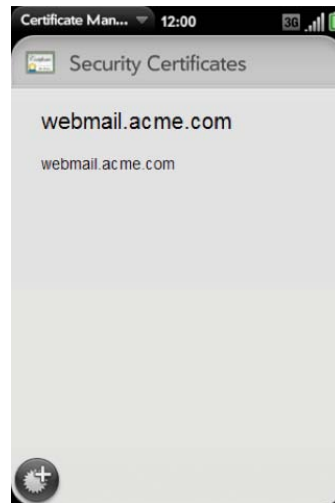


- 3 Tap **Preferences** in the top-left corner to open the application menu, then tap **Certificate Manager...**



*continued on next page*

- 4 Tap the certificate,  
then tap Delete Certificate.



## 4.11 Installing webOS applications

Only phones with registered Palm profiles may install applications wirelessly. Applications are downloadable via the Palm App Catalog, or via an unpublished URL.

The Palm App Catalog contains paid or free applications that have gone through a validation process with Palm's Developer group, plus beta applications available without warranty from Palm or the developer.

Inside the Palm App Catalog, applications are color coded:

Blue for a regular application



Green for a beta application



Gray for a web-distributed application



Applications that are downloadable via an unpublished URL are more secure because they are only visible to those with the proper URL. If that URL becomes compromised, the developer can quickly have the URL changed, or have the application removed from the Palm App Catalog.

### 4.11.1 Installing an application via the Palm App Catalog

Applications in the Palm App Catalog either have been approved by Palm or are available without warranty from the developer via the beta-release program.

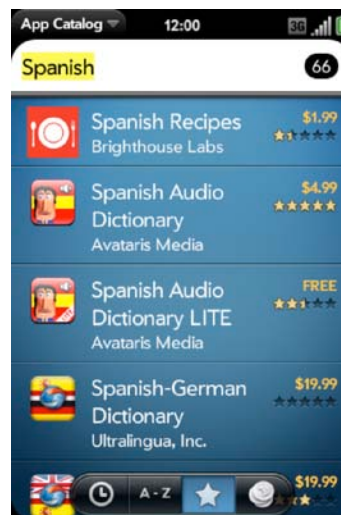
Applications that are free are clearly labeled. Fees for paid applications are charged to the user's credit card number. Use the Preferences & Accounts command in the App Catalog application to set the address to which receipts will be emailed.

To install an application from the Palm App Catalog:

- 1 Open the **App Catalog** application.



- 2 Locate the application either by browsing for it or by:
  - a. Typing the first letters of its name, then pressing the **Return** key.
  - b. Scrolling through the list.



- 3 Tap the application you want to install.
- 4 Tap **Download**.

## 4.11.2 Installing an application via an unpublished URL

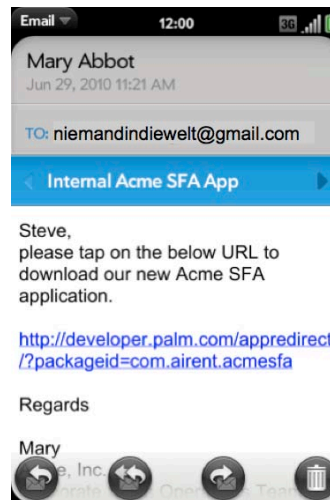
Corporate developers can choose to distribute their applications via either the App Catalog, which is visible to all webOS users, or an unpublished URL.

**Important:** This unpublished URL is *not* password protected. Developers should implement their own authentication methods such as requiring a password to complete installation.

To install an application via an unpublished URL:

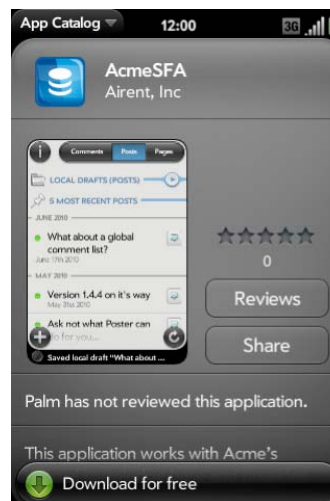
- 1 Open the URL from an email, SMS, or MMS by tapping on it, or manually enter the URL in the Web application.

*In this example, tap the URL in the body of this email.*



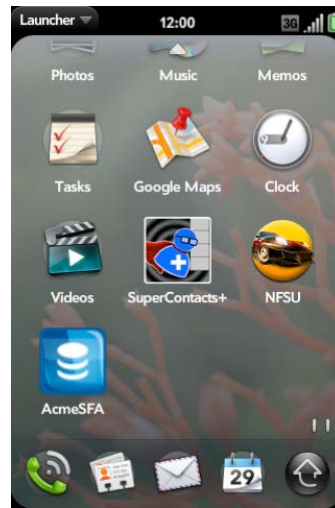
- 2 The App Catalog automatically opens to the application.

Tap Download for free.



- 3 The custom application is now available from the Launcher, just like standard App Catalog applications.

*In this example, the new application AcmeSFA is in the bottom row.*



## 4.12 Copying personal files to the USB drive

You can copy any type of file from a computer to your Palm webOS phone, and from your phone to your computer, by putting your phone in USB Drive mode.

After you copy a file to your phone, you can open the file if your phone has an application that supports that file type:

- Photos (JPEG, BMP, PNG)
- Videos (MPEG4, H.263, H.264, MP4, M4V, 3GP, 3GPP, 3G2, 3GP2)
- Music (MP3, AAC, AAC+, AMR, QCELP, WAV)
- Microsoft Word (DOC, DOCX)
- Microsoft Excel (XLS, XLSX)
- Microsoft PowerPoint (PPT, PPTX)
- Adobe Acrobat (PDF)
- Text files (TXT)

**Important:** All files that you store on the USB drive of your phone are *not* backed up to your Palm profile. Be sure to keep a copy of all such files somewhere other than your phone just in case you lose the phone or must do a full erase of it.

When your phone is in USB Drive mode, you can't make or receive calls or use other wireless features such as email or the web.



To copy files from your computer to the USB drive on the phone:

- 1 Connect your phone to your computer using the **Palm USB Cable**.



- 2 On your phone, tap **USB Drive** (or press **Option + Sym + U**).

On your computer, your phone appears as a removable drive.

On a Windows computer, if the **Found New Hardware** wizard opens, click **Cancel** to close the wizard.



- 3 Open **My Computer** (Windows XP), **Computer** (Windows Vista or Windows 7), or the **Finder** (Mac OS). Double-click the drive representing your phone.

Drag and drop the certificate file to the root folder of your phone's USB drive.

- 4 Repeat step 3 for any additional files or folders.

*continued on next page*



- 5 To end the connection safely on a Windows computer, right-click the drive representing your phone, and then click **Eject**.

On a Mac computer, drag the drive representing your phone to the **Trash**.

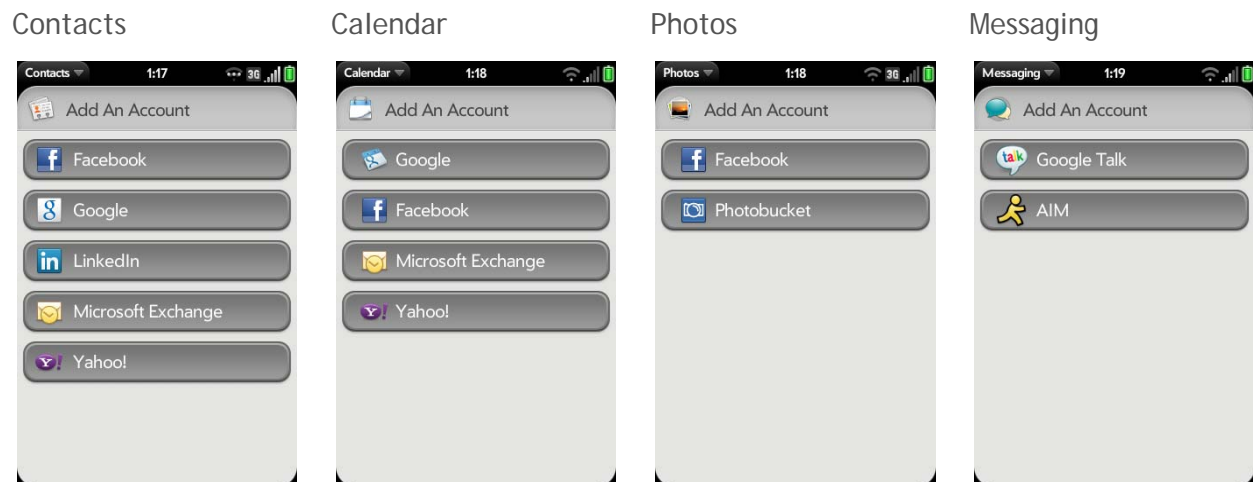
- 6 Wait until the icon representing your phone disappears from view, then disconnect the **Palm USB cable** from the device and the computer.

## 4.13 Linking to cloud-based services

You establish a link to a cloud-based service by adding an account for that service from within a webOS application. Once linked, updates to an item made on either the phone or the service are automatically synchronized with the other.

If a cloud-based account offers multiple services, then adding a cloud based account within one webOS application automatically adds its respective services to other webOS applications. For example, adding a Google email account to a webOS device also adds Google contacts, Google calendar, and Google messaging.

Each application has built-in support for various services:



You can selectively unlink a service. For example, you could remove Google calendar and messaging but keep email and contacts.

**Note:** Some account types such as Yahoo!® may not be available on all wireless carriers.

### 4.13.1 Adding an account

The process for adding an account is the same across webOS applications—launch the application, then use the Preferences & Accounts command.

As an example, here's how to add an account to Contacts:

- 1 Launch the **Contacts** application.

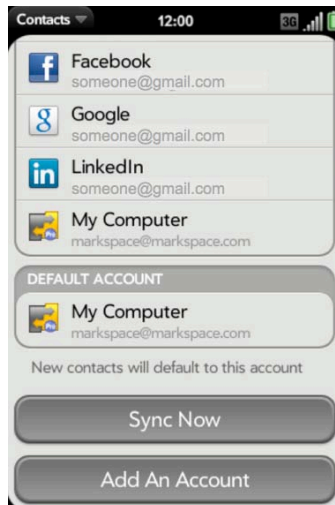


- 2 Tap **Contacts** in the top-left corner to open the application menu.

Tap **Preferences & Accounts**.



- 3 Scroll to the bottom, then tap **Add An Account**.



*continued on next page*

- 4 Tap the name of the account you want to add.



- 5 Sign in with your username and password.

## 4.13.2 Removing an account

The process for removing an account is the same across webOS applications—launch the application, then use the Preferences & Accounts command.

As an example, here's how to remove an account from Contacts:

- 1 Launch the **Contacts** application.

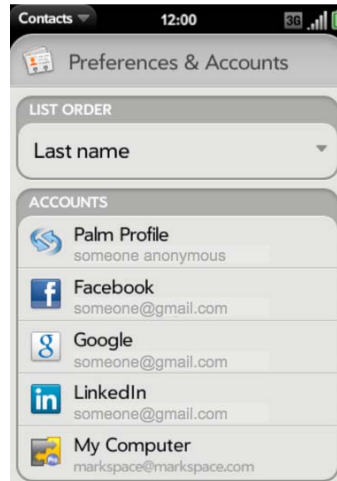


- 2 Tap **Contacts** in the top-left corner to open the application menu.

Tap **Preferences & Accounts**.

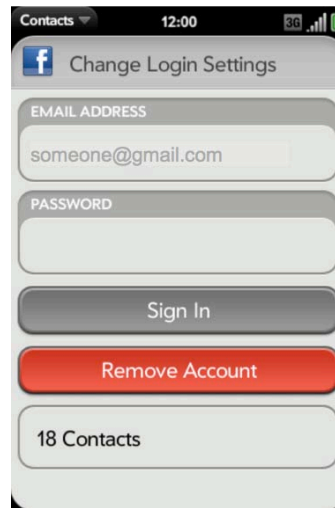


- 3 Tap the name of the account you want to delete.

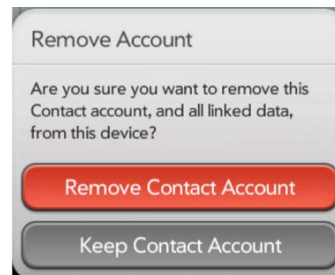


*continued on next page*

- 4 Tap Remove Account.



- 5 Confirm by tapping Remove Contact Account.



## 4.14 Transferring personal PIM data to webOS

You can transfer your personal contacts and calendar from web-based accounts and desktop organizers to webOS.

### 4.14.1 From web-based accounts to webOS

If your information already lives in one of the following web accounts, all you need to do is add the account to your phone.

- Google™
- Outlook/Microsoft Exchange
- Yahoo!
- Facebook
- LinkedIn®

To add an account to your phone:

- 1 On your phone, open **Contacts**.
- 2 Open the application menu and tap **Preferences & Accounts**.
- 3 Tap **Add Another Account** or **Add Account**.
- 4 Enter your username and password for that account.

The info will start showing up shortly. If the new account includes other services, your phone will set them up automatically.

For step-by-step instructions with screen captures, see [topic 4.13.1 "Adding an account."](#)



## 4.14.2 From desktop organizer to webOS

If you manage your contacts and calendar with a desktop organizer, you have two choices. You can move your info to an online service that syncs with your phone over the air. Or you can add third-party software to synchronize directly with your desktop organizer.

Solutions are available for:

- Palm Desktop (Windows)
- Outlook (Windows)
- iCal and Address Book (Mac)

To see the currently available solutions and step-by-step instructions, go to [palm.com/migrate-webos](http://palm.com/migrate-webos).

## 4.14.3 Desktop email and PIM applications to webOS

If you manage your contacts and calendar in some other way, go to [palm.com/migrate-webos](http://palm.com/migrate-webos), then click “Do you have Calendar/Contacts somewhere else?”

### Move Calendar and Contacts to your new webOS™ phone

[Deutsch](#)
[Español](#)
[Français](#)

After you've gotten started with your webOS phone, you're ready to move your existing info to it.


**Bring together what's important to you**

Your phone collects Calendar and Contacts from various sources — work, personal, social — and shows them in one simple view. All of your info remains in its original location. Palm gives you an easy way to bring these items to your phone, even if you used to keep them in a desktop organizer.

**Do you have calendars and contacts in several places?**

We'll connect with them one by one. Pick one below, then come back to [palm.com/migrate-webos](http://palm.com/migrate-webos) (this page) to transfer calendar and contacts from more accounts.

- ▶ [Do you have Calendar/Contacts in a web-based account?](#)
- ▶ [Do you have Calendar/Contacts in a desktop organizer?](#)
- ▶ [Do you have Calendar/Contacts somewhere else?](#)



## 5 Managing webOS devices

This section provides guidelines for managing webOS devices within Exchange ActiveSync environments or with POP- or IMAP-based email systems. Topics include an overview of how cloud services coordinate with each other, the various methods for wiping a device, and how users can restore their device.

### Topics in this section:

[5.1 What's backed up \(and what's not\)](#)

[5.2 Turning backup off](#)

[5.3 Device updates](#)

[5.4 Overview of wiping a device](#)

[5.5 Remote wipe from Exchange Server](#)

[5.6 Remote wipe from Outlook Web Access](#)

[5.7 Remote wipe from a Palm profile account](#)

[5.8 Local wipe](#)

[5.9 Restoring a device](#)

[5.10 Manually reinstating files on the USB drive](#)

[5.11 Reinstating personal data after a wipe](#)

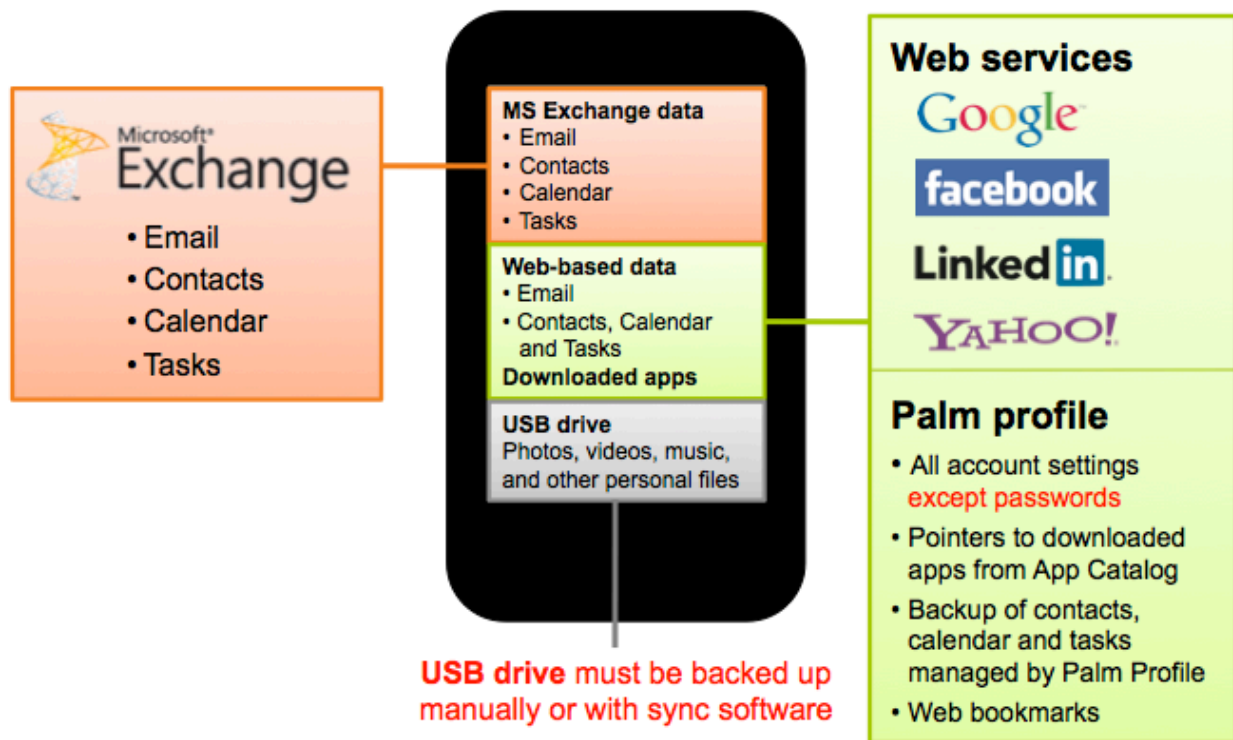
*To go to a topic, click the underlined link.*

## 5.1 What's backed up (and what's not)

User data such as email, contacts, calendar, and tasks are stored and managed in the phone's main memory. Each service synchronizes and manages its own data.

The Palm profile backs up contacts, calendar items, and tasks not handled by another service; account settings for all services (but never passwords); pointers to applications installed from the App Catalog; and web bookmarks.

For a complete description of what's backed up for each application, what's not backed up, and how to use the Backup app, see [Palm Knowledge Base article #19388](#).



**Important:** In addition to main memory, the phone has a USB drive that stores photos, videos, music, email attachments, website downloads, and desktop files transferred from a personal computer. Everything in the USB drive must be backed up manually using USB mode, or with third-party synchronization software.

For details about using USB mode to transfer files onto the USB drive, see [topic 4.12 "Copying personal files to the USB drive."](#)

For a list of third-party synchronization solution, see [www.palm.com/sync-solutions](http://www.palm.com/sync-solutions).

## 5.2 Turning backup off

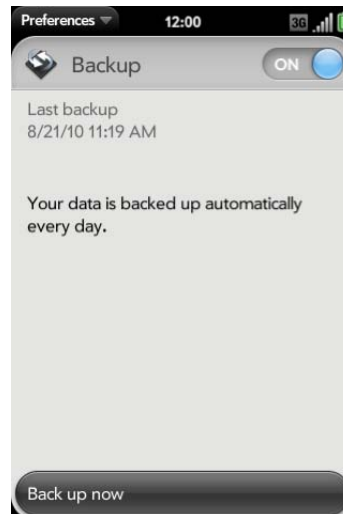
The user has the option to turn automatic backups off. Note that turning off back up also erases any data that was previous backed up to the cloud.

To turn backups off:

- 5 Launch the **Backup** application.



- 6 Tap the **On/Off** button in the upper-right hand corner of the screen.



- 7 Confirm choice by tapping **Turn Off And Erase Backup**.

Automatic backups are now off and the previous backup has been removed from the server.



## 5.3 Device updates

Wireless automated updates keep webOS phones up to date with the latest system software, the latest versions of installed applications, and up-to-the-minute EAS security policies.



Palm webOS devices can be manually updated with the Updates application. You can selectively install updates to applications downloaded from the App Catalog or choose to install all available updates.

You can postpone webOS system software updates, but eventually these will be installed automatically when the phone has sufficient battery charge and is unused (typically at night).

For full details, see “Understanding webOS system updates” at [Palm Knowledge Base article #19181](#).



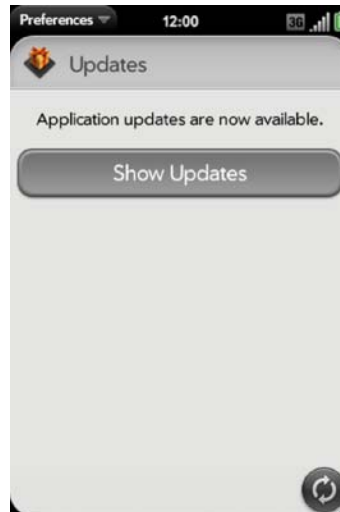
To manually update the phone:

- 1 Launch the **Updates** application.



- 2 The phone then searches for updates to any installed applications from the Palm App Catalog or updates to Palm webOS.

If there are any updates, tap **Show Updates** to continue.



- 3 Either tap the green download arrow next to an available update,



or tap **Install Updates** in the lower-right corner to install all updates.



## 5.4 Overview of wiping a device

A system administrator or a user can remotely wipe the contents of a webOS device to its original, factory settings. The user restores their device by logging into their Palm Profile and reentering passwords and other credentials.

When a webOS device receives a wipe command, it initiates a systematic overwrite of all user data, user installed applications and user settings. The duration of the wipe process depends on the storage capacity of the device. For example, wiping a 16 GB webOS device will take approximately twice as long as an 8 GB webOS device since there is twice the memory that must be overwritten.

System administrators may initiate a remote wipe using:

- Exchange Management Console for Exchange Server 2007 or later
- Exchange ActiveSync Mobile Administration Web Tool for Exchange Server 2003, 2007, 2010

***Note:** Palm webOS phones can be configured via EAS policies to automatically initiate a local wipe after several failed password attempts.*

Users may wipe their device using:

- Palm profile web access found at [palm.com/profile](http://palm.com/profile)
- Outlook Web Access for Exchange Server 2007 or later
- Local wipe with the Device Info application

## 5.5 Remote wipe from Exchange Server

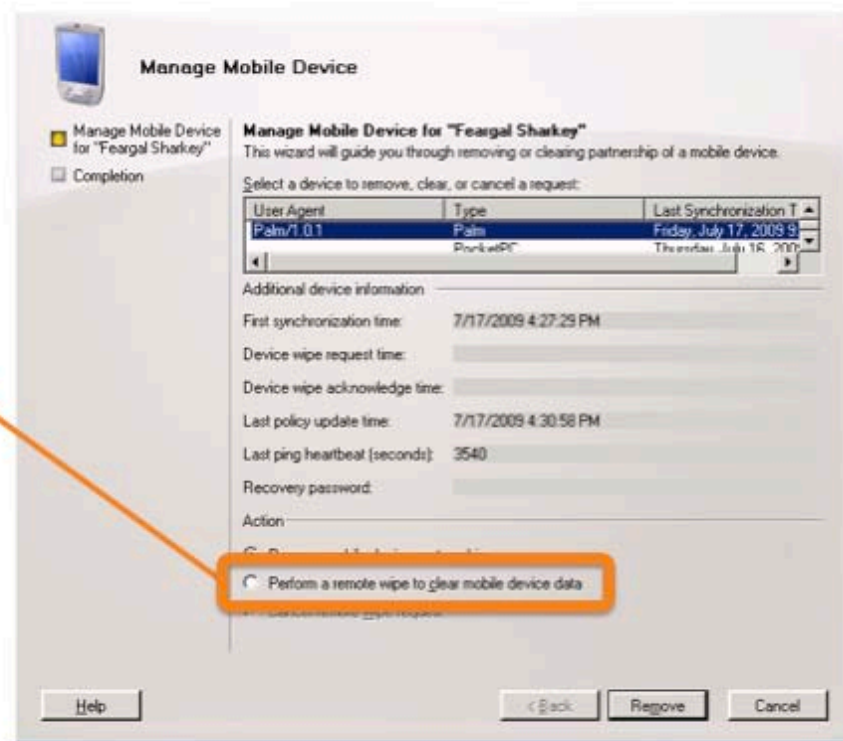
A system administrator can initiate a remote wipe for any webOS phone that is registered with at least one Exchange ActiveSync push services account.

The process is characterized as follows:

IT admin logs in to Exchange server

Selects the user

Issues remote wipe



**Note:** The erase device command must be received by an activated phone within 24 hours. Once started, the wipe process cannot be halted, even if the user removes the battery temporarily. Note that erasing a device does not deactivate the phone from the carrier's network.

Users can restore their own device by powering on the erased device, logging in to their Palm profile, following the on-screen instructions, and then reentering account passwords as needed. For details, see [topic 5.9 "Restoring a device."](#)



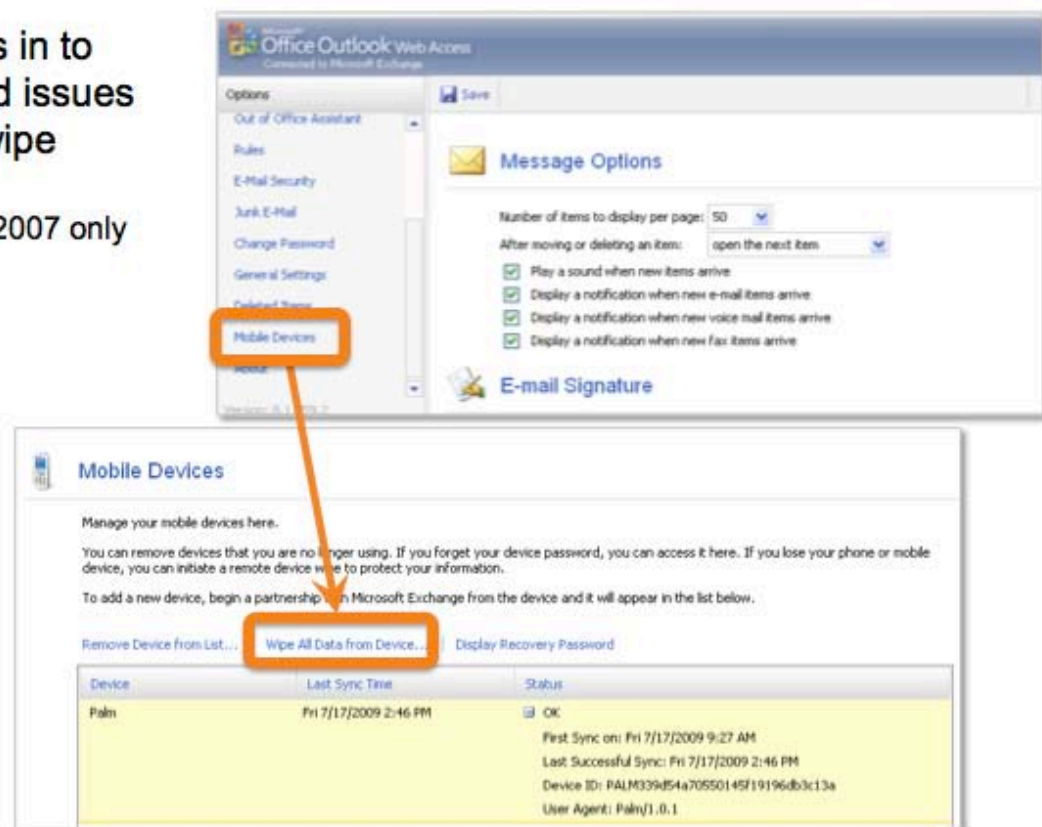
## 5.6 Remote wipe from Outlook Web Access

Exchange Server 2007 and Exchange Server 2010 users can remotely wipe their devices from their Outlook Web Access account.

The process is characterized as follows:

User logs in to OWA and issues remote wipe

Exchange 2007 only



**Note:** The phone must have an active data connection to the network to receive a wipe command. Once started, the erase process cannot be halted, even if the user removes the battery temporarily. Note that erasing a device does not deactivate the phone from the carrier's network.

Users can restore their own device by powering on the erased device, logging in to their Palm profile, following the on-screen instructions, and then reentering account passwords as needed. For details, see [topic 5.9 "Restoring a device."](#)

## 5.7 Remote wipe from a Palm profile account

Users can remotely wipe their device from their online Palm profile.

- 1 Open the web page [palm.com/profile](http://palm.com/profile).
- 2 Log in using the same email and password used when setting up the phone for the first time.
- 3 Click **Device Options** to the right of the phone number.

| Device Details |       |                     |            |         |
|----------------|-------|---------------------|------------|---------|
| Phone Number   | Model | Device ID           | OS Version | Primary |
| 14085550050    | Pre   | MEID:A10005064756E5 | 1.40.50    | Yes     |

Device Options

- 4 Click **Erase Device**.

### I Lost My Phone

If you have lost your phone, use **Erase Device\*** to help keep your data safe.

Erase Device permanently deletes all data on your device.

Erase Device may take up to **2 hours**.

During this time your phone cannot be used.

Erase Device
Cancel

\* The erase device command is sent via SMS and must be received by an activated phone within 24 hours. Erase does not deactivate your phone from your carrier's network. Contact your carrier to deactivate this phone from your carrier's network.

**Note:** The wipe device command is sent via SMS and must be received by an activated phone generally within 24 hours (SMS timeout periods can vary from carrier to carrier and usually don't exceed 72 hours). Once started, the erase process cannot be halted, even if the battery is temporarily removed. Note that erasing a device does not deactivate the phone from the carrier's network.

Users can restore their own device by powering on the erased device, logging in to their Palm profile, following the on-screen instructions, and then reentering account passwords as needed. For details, see [topic 5.9 "Restoring a device."](#)

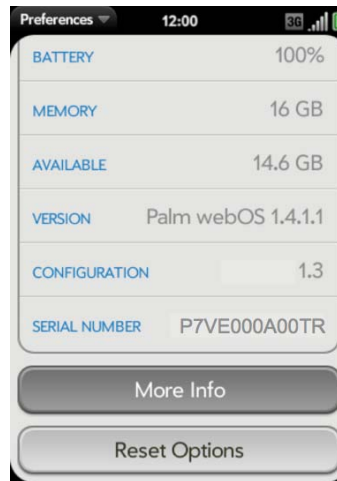
## 5.8 Local wipe

Users can manually wipe their device with the Device Info application:

- 1 Launch the Device Info application.



- 2 Scroll to the bottom, then tap **Reset Options**.



- 3 Scroll to the bottom, then tap **Full Erase**.

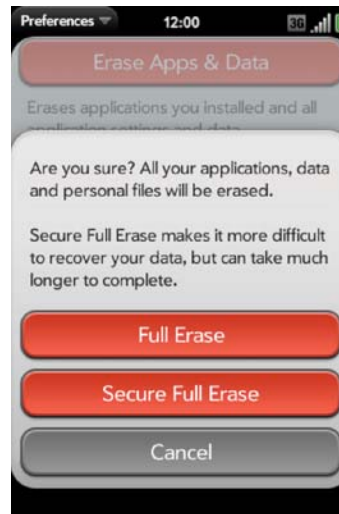


*continued on next page*

- 4 Confirm by tapping Full Erase or Secure Full Erase.

**Important:**

*Once started, this wipe cannot be halted, even if the battery is removed.*



**Tech tip:** You can also perform a Full Erase by holding down the **Option + Sym + Power** buttons for 10 seconds. This is useful for a device with a broken screen.



Users can restore their own device by powering on the erased device, logging in to their Palm profile, following the on-screen instructions, and then reentering account passwords as needed. For details, see [topic 5.9 “Restoring a device”](#) on the next page.

## 5.9 Restoring a device

Users can restore their own device by logging in to their Palm profile. Once logged in, the Palm profile reinstalls PIM data, installed applications, browser bookmarks, and all email and cloud-based service account credentials and settings except for passwords that must be manually reentered.

Any files that were on the USB drive prior to the wipe (security certificates, photos, videos, web downloads, and desktop files) must be either copied to the drive or reinstated from third-party software backup. For details, see the [topic 5.10 "Manually reinstating files on the USB drive"](#).

Start by logging in to your Palm profile:

- 1 Press and hold the **Power** button on the phone until a logo appears on the screen.
- 2 Follow the on-screen instructions.
- 3 Tap your language to select it. The phone will then check for network access.
- 4 When you see the Phone Activated message, tap **Next**.
- 5 Tap **Accept** when asked to confirm terms and conditions for Palm Services.
- 6 Tap **Sign In With My Profile**.
- 7 Enter the email address and password for your Palm profile. Tap **Next**.

Your Palm profile then reinstates:

- All applications acquired through the Palm App Catalog, including custom applications that were distributed via an unpublished URL
- All email account credentials and settings except for passwords
- All cloud-based service credentials and settings except for passwords
- Contacts, Calendar, Memos, and Tasks items backed up by your Palm profile
- Web browser bookmarks

After account settings for all the services have been restored, the device will prompt for all required passwords.

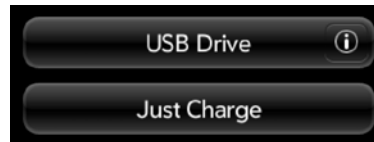
## 5.10 Manually reinstating files on the USB drive

Personal and media files that were on the USB drive prior to the wipe may be reinstated from a desktop copy.

- 1 Connect your phone to your computer using the Palm USB cable.



- 2 On your phone, tap **USB Drive** (or press **Option + Sym + U**).



On your computer, your phone appears as a removable drive.

On a Windows computer, if the **Found New Hardware** wizard opens, click **Cancel** to close the wizard.

- 3 Open **My Computer** (Windows XP), **Computer** (Windows Vista or Windows 7), or the **Finder** (Mac OS). Double-click the drive representing your phone.

Drag and drop the certificate file to the root folder of your phone's USB drive.

- 4 Repeat step 3 for any additional files or folders.
- 5 To end the connection safely on a Windows computer, right-click the drive representing your phone and click **Eject**.

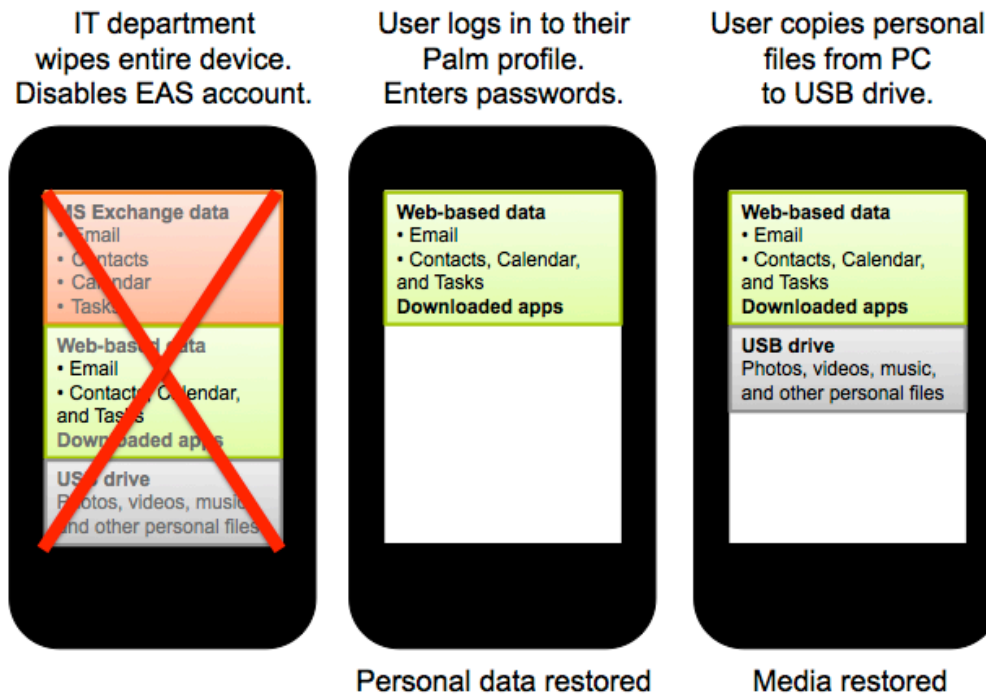
On a Mac computer, drag the drive representing your phone to the **Trash**.

- 6 Wait until the icon representing your phone disappears from view, then disconnect the **Palm USB cable** from the device and the computer.

## 5.11 Reinstating personal data after a wipe

After a wipe that removes all data and applications, users can restore their personal data, files, and Palm App Catalog downloads.

Here's an overview of the process:



To reestablish a phone's Palm profile:

- 1 Hold down the Power button until you see a logo on the screen (approximately five seconds).
- 2 Tap Login to Palm Profile.
- 3 Enter the same email address and password you used when first setting up your Palm profile credentials.

If you have trouble reestablishing your phone's Palm profile credentials because you've forgotten your email or your Palm profile password and did not set up a security question, see [Palm Knowledge Base article #19141](#).

# Appendix A: Palm webOS Doctor

Palm webOS Doctor is a free web-based tool that updates webOS phones to the latest versions of the operating system and other system software. It was designed to restore functionality to webOS phones that have frozen during a wireless system update, most typically because the phone's battery was removed or ran out of power.

Palm webOS Doctor may also be used to preinstall the latest version of webOS before devices are deployed to individual users.

Alternately, users can install the latest version of webOS on their own devices with the Updates application.

## Topics in this section:

[A.1 Palm webOS Doctor system requirements](#)

[A.2 How to use Palm webOS Doctor](#)

[A.3 Removing the back cover of a Palm Pre phone](#)

[A.4 Removing the back cover of a Palm Pixi phone](#)

*To go to a topic, click the underlined link.*





## A.1 Palm webOS Doctor system requirements

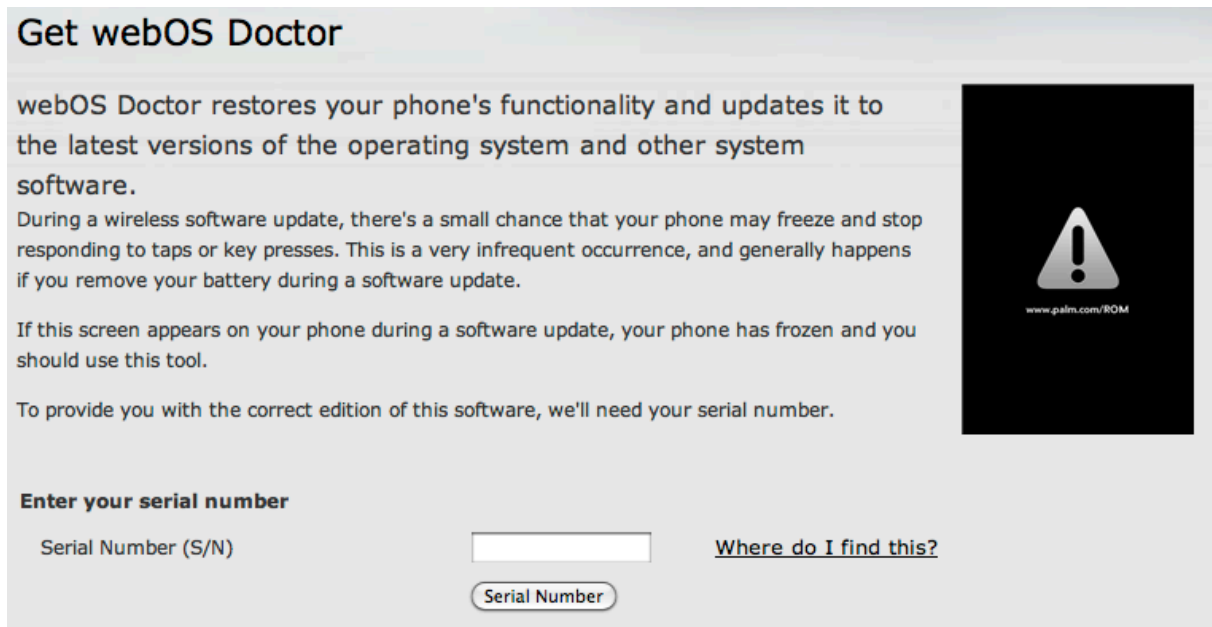
Palm webOS Doctor requires the following:

- Palm AC charger included with the phone
- Palm USB cable
- At least 30% charge on the phone's battery
- Computer with an Internet connection running:
  - Windows XP, Windows Vista, or Windows 7
  - Mac OS X 10.5 (Leopard), or Mac OS X 10.6 (Snow Leopard)  
(*Mac OS X 10.4 is **not** recommended.*)
- Available USB port (not a hub or secondary port)
- Java 1.5 or later installed on the computer  
(Go to [java.com](http://java.com) to install the latest version.)
- 200MB of available storage on the computer

## A.2 How to use Palm webOS Doctor

Connect the phone to an available USB port on your computer (not a hub or a secondary port), then open the Palm webOS Doctor website and follow the instructions.

- 1 Go to [palm.com/ROM](http://palm.com/ROM) in your computer's browser.



**Get webOS Doctor**

webOS Doctor restores your phone's functionality and updates it to the latest versions of the operating system and other system software.

During a wireless software update, there's a small chance that your phone may freeze and stop responding to taps or key presses. This is a very infrequent occurrence, and generally happens if you remove your battery during a software update.

If this screen appears on your phone during a software update, your phone has frozen and you should use this tool.

To provide you with the correct edition of this software, we'll need your serial number.

**Enter your serial number**

Serial Number (S/N)  [Where do I find this?](#)

- 2 Enter the device's serial number located under the battery. For some carriers, the serial number is also listed on the box as the MSN (Manufacturer's Serial Number).

Palm serial numbers have 12 alphanumeric characters, always starting with P. You may need a magnifying glass to properly read the small printed characters.

*For detailed instructions about removing the battery, see ["Removing the back cover of a Palm Pre phone"](#) or ["Removing the back cover of a Palm Pixi phone"](#) later in this appendix.*

**Note:** The entire reset process for each phone can take up to 15 minutes.

If you have difficulty with Palm webOS Doctor, see [Palm Knowledge Base article #44768](#) for step-by-step instructions, or see [webOS Doctor FAQs](#) for troubleshooting tips.

## A.3 Removing the back cover of a Palm Pre phone

**Important:** Before starting, disconnect the USB cable and all accessories.

- a Press and release the back cover release on the bottom of the phone.



- b Insert your thumbnail, a credit card, or a coin into the hairline opening between the cover and the phone.
- c Slide your nail or other item halfway up one side of the phone until you hear the clasp release. Repeat on the other side.



- d Lift off the back.



For further details, see [Palm Knowledge Base article #44919](#).

Replacing the back cover of a Palm Pre phone:

- a Position the cover over the phone and gently press the top two clasps, located at the top corners.
- b Press the two clasps halfway down either side of the phone.
- c Slide out the keyboard, then press the two clasps at the bottom corners.



For further details, see [Palm Knowledge Base article #44919](#).

## A.4 Removing the back cover of a Palm Pixi phone

**Important:** Before starting, disconnect the USB cable and all accessories.

- a Run your thumbnail around the hairline opening to release the upper-left and top clasps. You may hear a sound when each clasp releases.



- b Run your thumbnail around the hairline opening to release the bottom-left and bottom clasps.



*continued on next page*

- c Swing the body of the phone out of the back cover as if the right side were a hinge.



For further details, see [Palm Knowledge Base article #23498](#).

Replacing the back cover of a Palm Pixi phone:

- a Insert the ringer switch into the hole provided for it on the right side of the back cover.



- b Press the back cover and the body of the phone together at each pair of clasps. You can feel the clasps engage.



For further details, see [Palm Knowledge Base article #23498](#)

# Index

- 3D graphics, 6
- ActiveSync, 2, 4, 7, 9, 10, 11, 14, 15, 16, 22, 52, 57, 58
- App Catalog, 3, 4, 15, 17, 19, 21, 39, 40, 41, 53, 55, 56, 63, 65
- authentication, 7, 10, 12, 14, 25, 27, 40
- backup, 3, 17, 19, 53, 54, 63, 64
- C/C++, 6
- CA, 12, 31
- calendar, 2, 3, 5, 9, 19, 45, 50, 51, 53
- certificate authority, 12
- certificates, 7, 12, 14, 16, 17, 31, 32, 33, 36, 43, 64
- cloud-based, 17, 18, 19, 20, 45, 63
- contacts, 2, 3, 5, 9, 18, 19, 45, 50, 51, 53
- CSS, 1, 6
- Device Info, 36, 57, 61, 69, 70, 71
- DNS, 10
- EAS, 2, 4, 7, 9, 10, 17, 19, 22, 23, 55, 57
- email, 2, 3, 5, 7, 8, 9, 10, 12, 16, 17, 18, 19, 21, 22, 24, 25, 26, 31, 40, 42, 45, 51, 52, 53, 60, 63, 65
- Exchange, 2, 3, 5, 7, 8, 9, 10, 11, 14, 15, 16, 18, 19, 20, 22, 23, 50, 52, 57, 58
- Exchange Server, 4, 7, 11, 18, 52, 57, 58, 59
- Exchange Server 2003, 57
- Exchange Server 2007, 57, 58
- Facebook, 3, 17, 19, 50
- firewall, 10, 12
- GAL, 2, 9, 19
- Google, 3, 5, 17, 19, 20, 45, 50
- HTML, 1, 6
- identities, 7, 17
- IMAP, 12, 24, 25
- install, 11, 12, 14, 19, 31, 35, 39, 40, 55, 56, 66, 67
- Internet Security and Acceleration, 10
- ISA, 10
- JavaScript, 1, 6
- LinkedIn, 3, 17, 19, 50
- Mac OS, 8, 33, 43, 64, 67
- middleware, 2, 9
- Mojo, 1, 6
- OpenGL, 6
- Outlook Web Access, 31, 35, 52, 57, 59, 60
- Palm App Catalog, 3, 4, 15, 17, 19, 21, 39, 56, 63, 65
- Palm OS, 17
- Palm Profile, 3, 4, 8, 17, 18, 19, 20, 21, 42, 53, 57, 58, 59, 60, 62, 63, 65
- Palm Services, 2, 3, 19, 21, 63
- password, 8, 9, 14, 21, 22, 25, 28, 29, 40, 47, 50, 57, 60, 63, 65
- PDK, 6
- photos, 3, 19, 53
- Plug-in Development Kit, 6
- POP, 7, 12, 16, 24, 25, 52
- push, 2, 8, 9, 18, 19, 22, 58
- remote wipe, 11, 57, 58
- reset, 19, 68
- root identities, 7, 17
- security certificates, 16, 17, 31, 36
- SMS, 5, 40, 60
- SSL, 10, 12, 25, 31
- synchronization, 10, 18, 19, 20, 53
- tasks, 2, 3, 9, 19, 53
- USB cable, 33, 34, 44, 64, 67, 69, 71
- USB drive, 16, 17, 19, 31, 33, 42, 43, 52, 53, 63, 64
- USB mode, 19, 53
- videos, 3, 15, 19, 53
- webOS, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 14, 15, 16, 17, 18, 19, 22, 25, 27, 29, 31, 38, 40, 42, 45, 46, 48, 50, 51, 52, 55, 56, 57, 58, 66, 67, 68
- webOS applications, 1, 6, 16, 19, 38, 45, 46, 48
- webOS Doctor, 66, 67, 68
- Wi-Fi, 2, 7, 9, 13, 15, 17, 27, 28, 29
- Windows, 8, 33, 34, 43, 44, 51, 64, 67
- X.509, 12, 31
- Yahoo, 3, 24, 50