

Get Mobile!



Omni Mobile Client Installation Quick Start Guide for Windows Mobile Smart Phone Devices

Getting Started

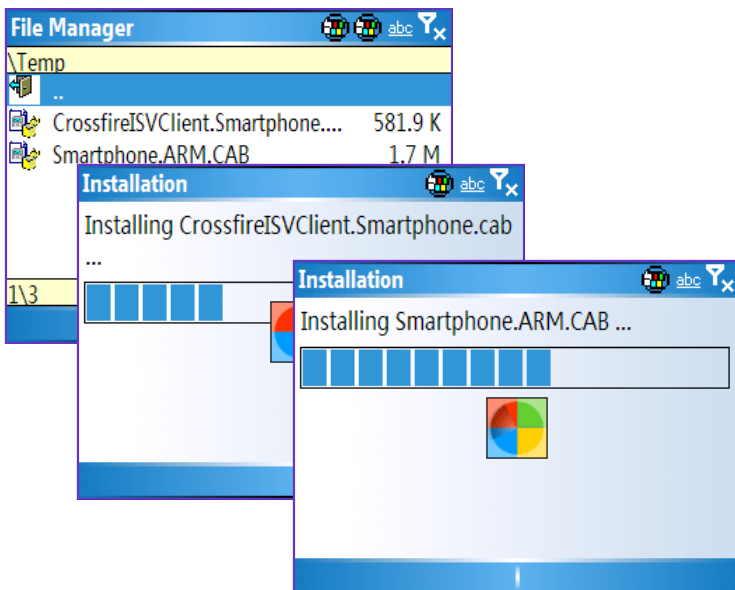
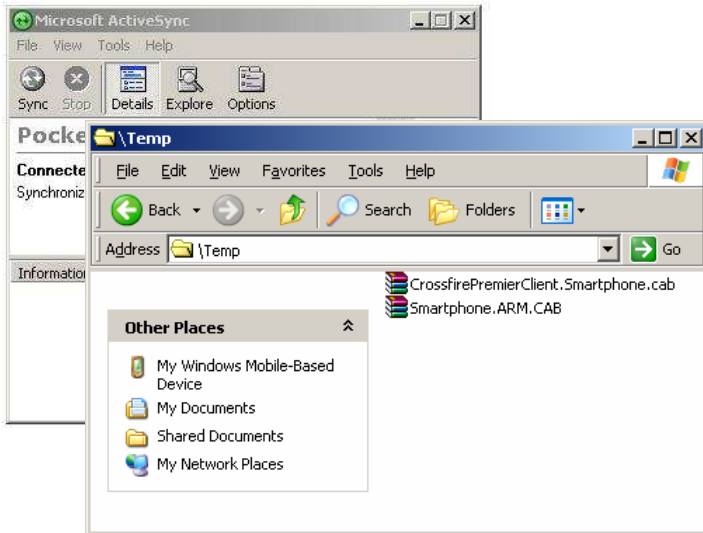
This Quick Start Guide is for Windows Mobile Smart Phones (no touch-screen support) devices. There is a separate Quick Start Guide for Pocket PC and Windows Mobile touch-screen PDA and PDA Phone devices. We recommend your device have a minimum of 3 MB of main memory or storage card space to hold the Omni Mobile client. If you make extensive use of attachments, we recommend an additional 5 MB of main memory space or storage card space. This Guide is for Omni Mobile 2.3 or higher. Refer to the last three pages of this Guide to configure SSL on your device.

Install the Omni Mobile Client

There are two ways to install the Omni Mobile client and provision your account. The **Desktop-based** installation option is used if you can cradle your device to your workstation or have Bluetooth connectivity. This option is recommended for provisioning accounts with large address books or large numbers of calendar entries. Use your workstation to copy the client installation files to your device. **Browser-based** installation is normally used if you cannot cradle your device. Use the Internet browser on your device to copy and install the client files to your device. Installing the client takes two minutes.

Option 1 - Desktop-based Installation

1. Extract the **omnimobile.zip** file to your computer.
2. Cradle your device or use a Bluetooth connection if your device and computer support it and ensure that you are connected using Microsoft ActiveSync.
3. Using a file explorer on your computer, copy the **CrossfirePremierClient.Smartphone.cab** and **Smartphone.ARM.CAB** files to a folder on your device.
5. Using File Manager on your device, select and run the **CrossfirePremierClient.Smartphone.cab** file.



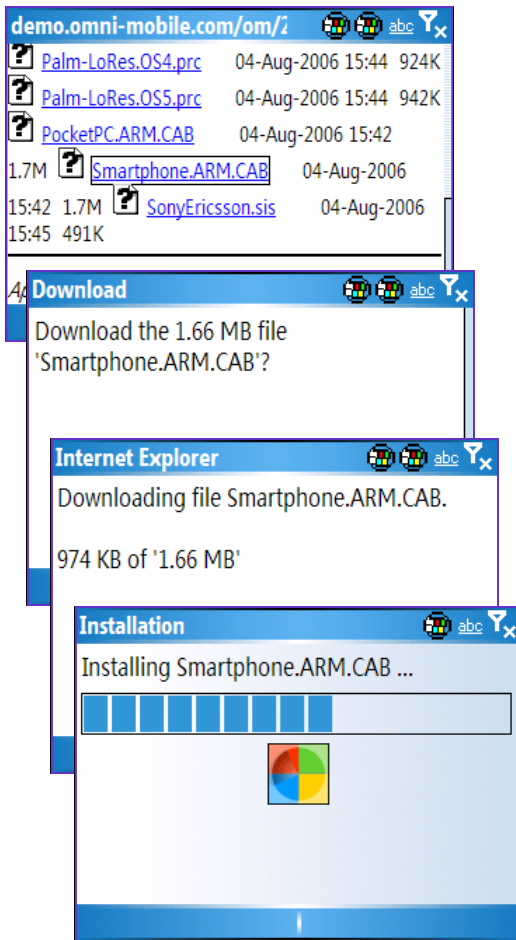
IMPORTANT

CrossfirePremierClient.Smartphone.cab can only be installed into the device's main memory. The Omni Mobile client (**Smartphone.ARM.CAB**) can be installed to the device internal memory or to a SD or CF expansion card. Choose the location with the most available memory.

6. Using File Manager on your device, select and run the **Smartphone.ARM.CAB** file.

Congratulations, you have installed the Omni Mobile client.

Do not start the Omni Mobile client. The next step is to provision your account. Please refer to Page 2: **Provision Your Omni Mobile Account**



Option 2 - Browser-based Installation

For this option, your device must have Internet access and you must be able to browse to web sites using Internet Explorer on your device. Please ask your network administrator for the download **links** for the two required files.

1. On your device, open Internet Explorer and type in the URL to the location hosting the Omni Mobile files (**CrossfirePremierClient.Smartphone.CAB** and **Smartphone.ARM.CAB**).

IMPORTANT

CrossfirePremierClient.Smartphone.cab can only be installed into the device's main memory. The Omni Mobile client (**Smartphone.ARM.CAB**) can be installed to the device internal memory or to a SD or CF expansion card, Choose the location with the most available memory.

2. Five-way toggle to select the **CrossfirePremierClient.Smartphone.cab** file. Select **Yes** to download the file and automatically install after it is downloaded.
3. Five-way toggle to select the **Smartphone.ARM.CAB** file. Select **Yes** to download the file and automatically install after it is downloaded.

Congratulations, you have installed the Omni Mobile client.

Provision Your Omni Mobile Account

There are two options to provision your Omni Mobile account.

Desktop/cradle-based is recommended to provision accounts using your workstation connection. Use this method if you have a large number of emails and calendar entries or large address books you want to configure on your device. **On-Device (cradle or wireless)** is used to copy your policies, folders, email, calendar items and address books directly to your mobile device. Use this option if you have a small amount of data to copy to your device or if you cannot cradle your device.

Option 1 - Desktop-based Account Provisioning

For this option, your computer requires access to the internet and the workstation program **omnimobile-desktop.exe**.

1. On your computer, go to **c:\omnimobile\Account-Creator** and extract the appropriate zip file. For Windows, right-click **omnimobile-desktop.win32-<appropriate version>.zip** and choose **Extract here**. This will create an **omnimobile-desktop** folder that contains **omnimobile-desktop.exe**.





Option 1 - Desktop-based Account Provisioning
(continued)

- 2. Run **omnimobile-desktop.exe** (Windows) or **omnimobile-desktop** (Linux or Mac). Specify the correct URL (http or https) to connect to your GroupWise WebAccess login screen, for example.

```
https://mail.mycompany.com/servlet/webacc
(for GroupWise 6.x)

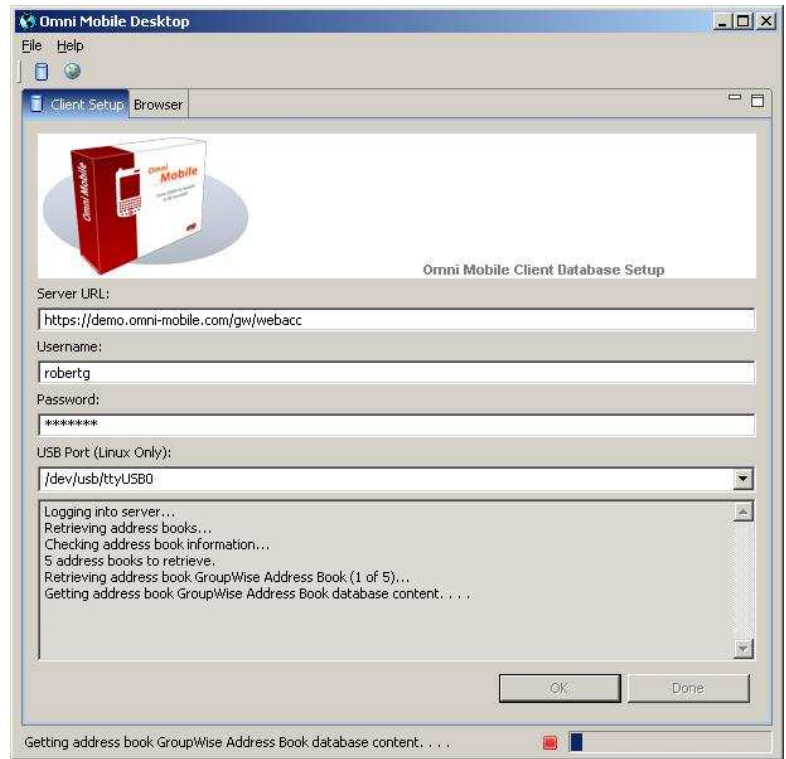
https://mail.mycompany.com/gw/webacc
for GroupWise 7.x)
```

- 3. Provide the user name and password you normally use for GroupWise WebAccess, and click **OK**.

Several minutes may pass while .PDB data files are transferred to your computer into the **UserData** folder in the same directory as the omnimobile-desktop.exe.

- 4. When the data files are finished copying, a message will appear. Click **OK** and **Done**.

- 5. Copy the **UserData** folder from **C:\omnimobile\Account-Creator\omnimobile-desktop** on your computer to the **My Pocket PC\Program Files\Omni Mobile** folder on your device.

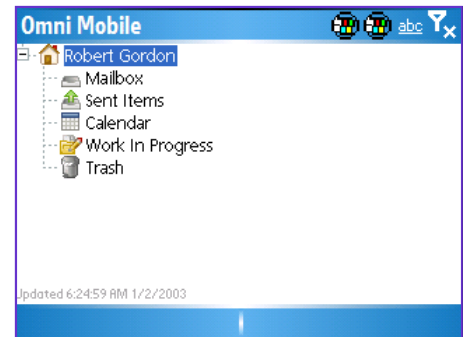


Congratulations

You are now ready to login to Omni Mobile.

You have instant on-line and off-line access to your configured folders, email, appointments, tasks, notes and address books.

If you are using https:// and you get a connection error, you will need to install the SSL certificate (see "Provision your Mobile Device for SSL" on page 5).



Refer to the **Using Omni Mobile Quick Start Guide** for information on how to use the Omni Mobile client.



Option 2 - "On-Device" Account Provisioning

If you start the Omni Mobile client on a device that does not have account "PDB" files provisioned, it will automatically start the "First-run Wizard". For this option, your device must have access to the Internet and you must be able to browse to websites with Internet Explorer on your device.

IMPORTANT

The "First-run Wizard" allows the client software to connect directly to the Omni Mobile server to retrieve the account information based on the User Profile that was configured. Time to complete this process will depend on the amount of mail and calendar entries, the size of address books to copy and the speed of your connection. We recommend you:

- Remain in a single location. Do not do this while moving about.
- Configure your Omni Mobile **Folder** policies to **Copy** a minimum amount of email for each folder (e.g. 1 or 2 days).
- Configure your Omni Mobile **Address Book** policy to synchronize small address books with fewer than 100 contacts. You can add large address books when you are cradle connected.

WHAT IS HAPPENING

When the Omni Mobile client first opens, it displays empty folders that match what you configured in your **Folder** policy. After creating the folder structure, Omni Mobile:

1. Creates the address book structure. You may see notifications looping between **Checking for Changes** and **Folder changes: 1** for a few minutes.
2. Copies all contacts to the Address Books. You will see



3. Copies all calendar items to the Calendar folder.
4. Copies all email items to the Mailbox and other folders specified in the **Folder** policy. You will see



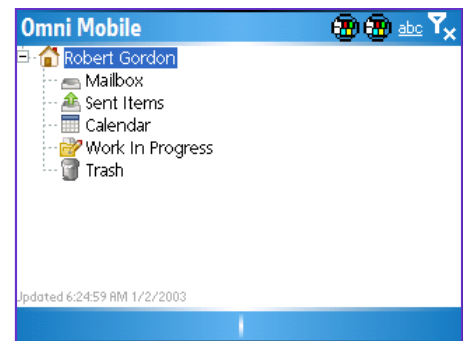
1. On your device, run the Omni Mobile client. This initiates the First-Run Wizard. Provide the URL to your GroupWise WebAccess server, your GroupWise login username and password, and select **Start**.
2. After the folder structure is copied to the device, your Omni Mobile client will start but the folders will not contain any email, calendar items or address book contacts. **If you are using https:// and you get a connection error, you will need to install a SSL certificate (see "Provision your Mobile Device for SSL" on page 5).**
3. You must wait until all of the data gets copied from the Omni Mobile server to your device before you can use your Omni Mobile client (see the "What is Happening" sidebar).

Congratulations

You are now ready to use Omni Mobile.

You have instant on-line and off-line access to your configured folders, email, appointments, tasks, notes and address books.

Refer to the **Using Omni Mobile Quick Start Guide** for information on how to use the Omni Mobile client.





Provision Your Omni Mobile Device for SSL

Omni Mobile uses SSL when you specify **https://** in the **Server:** field in either the **FirstRun** screen or in the client options (from the Tree view go to **Menu > Tools > Options**). By default, Windows Mobile Smartphones will recognize most commercial SSL certificates automatically. If there is an SSL problem you will see a connection error.



In this case you must manually create a certificate file and install it onto the device:

1. Open Internet Explorer and access the URL for the SSL enabled GroupWise WebAccess server e.g. <https://mail.mycompany.com/gw/webacc>
2. If you are prompted with a "Security Warning" window, click **Yes**.



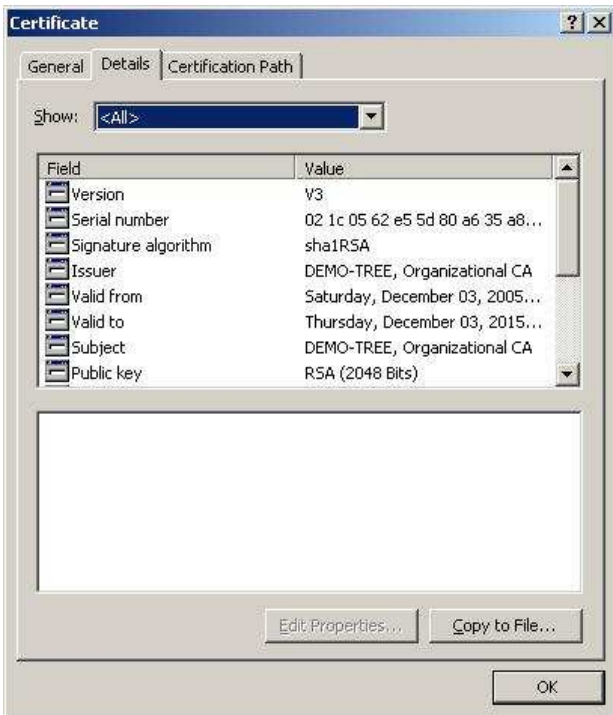
3. In the status bar double-click the lock icon.



4. In the "Certificate:" window select the **Certification Path** tab, highlight **organizational CA** and click **View Certificate**.



5. Click the **Details** tab and ensure that the "Issuer" value contains the correct information.



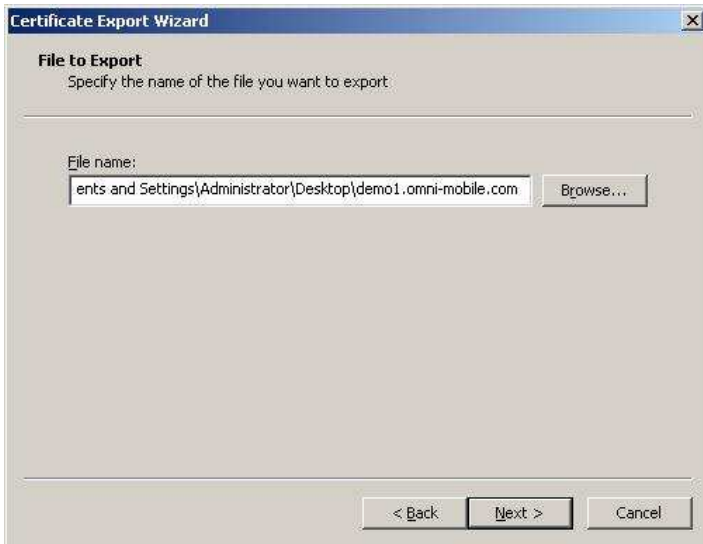
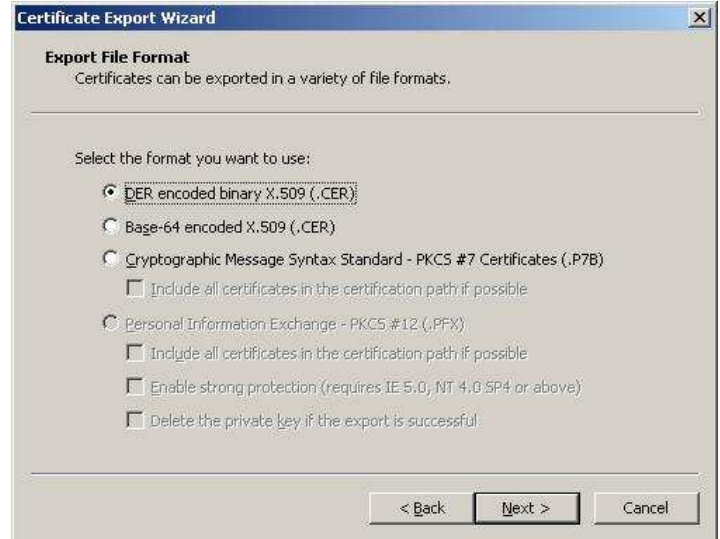
NOTE—It is really important to select the top object in the certification path, e.g. "Organizational CA".

You want to install the "Root Authority" for the SSL certificate that the GroupWise WebAccess server provides to browsers. If the Omni Mobile cannot verify the certificate "Root Authority" against an installed certificate, communications will fail.



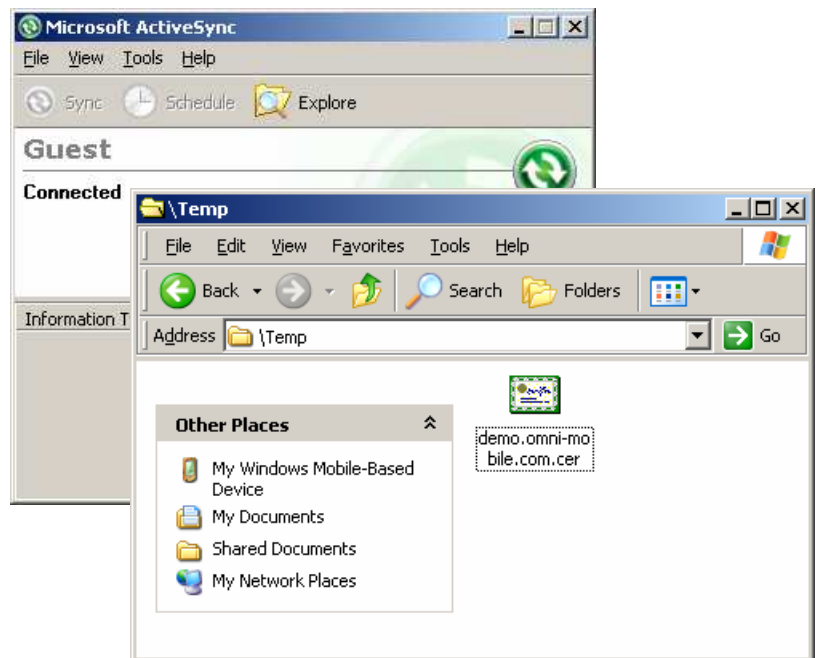
Provision Your Omni Mobile Device for SSL (continued)

- In the "Welcome to the Certificate Export Wizard" window, click **Next >**.
- Select the "DER encoded binary X.509 (CER)" format and click **Next >**.
- Click on "Browse" and navigate to your desktop. Save your certificate. It is best to name it your public name—the name you specified "as should sync with [server name]" e.g. **demo.omni-mobile.com.cer**. The file must have a .CER extension.



- Click **Next >** to proceed.
- Click **Finish** to export the certificate to your desktop.
- In the "The export was successful" window, click **OK** to close the box.
- Click **OK** on the remainder of the boxes to close them and close out of Internet Explorer.

- Connect your Windows Mobile device to your desktop (cradle or sync cable).
- Start ActiveSync and click **Explore** and navigate to the **Mobile Device > Temp** folder.
- Copy the exported root certificate file e.g. **demo.omnimobile.com.cer** from your desktop to the **\Temp** folder





Provision Your Omni Mobile Device for SSL (continued)

- 16. On your device, open "File Explorer" and navigate to **My Device >Temp**, select and click the **.cer** file.
- 17. When prompted if you want to install the certificate, select **Yes**.
- 18. You should now be able to continue with the FirstRun wizard.



If you are running using **http://** before, you can change to using **https://** by changing the **Server:** value in the client options.

1. From the tree view select **Menu > Tools > Options**.
2. Change the **http://** to read **https://** in the **Server:** text box.
3. Select **Save** to save the settings and close the client options window.

The Omni Mobile client will immediately attempt to connect with the Omni Mobile server and confirm that communications are working.

Note: The above process to install SSL certificates will only work on Windows Mobile Smartphone devices that have an Unrestricted Application Security Policy. If your mobile device has been restricted by your service provider to only allow registered certificates to be added, you will receive a warning message similar to:

“This device is currently secured such that certificates cannot be added to the root store. For support, please contact your device administrator.”

In these cases, we recommend you use a Commercial SSL Certificate or you contact your mobile operator for information about how to have your certificate imported. Verizon and Sprint are examples of mobile providers that have restricted application signature requirements.