



## **Deploying Windows Mobile® 6 with Windows® Small Business Server 2003**

---

Microsoft® Corporation

Published: January 2008

Version: 3

### **Abstract**

This document provides step-by-step instructions for deploying devices powered with Windows Mobile® 6 in an IT infrastructure that is based on the Windows® Small Business Server 2003 (Windows SBS) server software.

**Microsoft**

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

© 2006 Microsoft Corporation. All rights reserved.

Microsoft, Outlook, PowerPoint, Windows, Windows Media, and Windows Mobile are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

UPnP is a certification mark of the UPnP Implementers Corporation.

All other trademarks are property of their respective owners.

# Contents

---

Deploying Windows Mobile 6 with Windows Small Business Server 2003 .....	5
Windows Mobile 6.....	5
Messaging and Security Feature Pack .....	5
Before You Begin.....	6
Skill Level.....	6
Windows Mobile Requirements .....	6
Additional requirements .....	7
Process Steps.....	7
Step 1: Install ActiveSync 4.5 or WMDC 6.1 .....	8
Step 2: Enable Mobile Services for Users .....	8
Step 3: Configure the Firewall and Web Services .....	10
Step 4: Install a Certificate.....	11
Choose the Type of Certificate.....	12
Configure the Certificate.....	14
Option A: Configure a Self-Issued Certificate .....	14
Option B: Configure a Third-party Certificate.....	16
Step 5: Configure Windows Small Business Server.....	26
Install the Exchange Server ActiveSync Web Administration Tool .....	26
Enable Direct Push.....	27
Step 6: Configure Device Synchronization .....	28
Device Synchronization Using ActiveSync.....	29
Device Synchronization Using WMDC.....	32
Step 7: Test the Deployment .....	37
Test Over-the-Air Synchronization .....	37
Test Direct Push.....	38
Remote Management .....	38
Remote Device Wipe.....	38
Device Security Policies .....	39
Troubleshooting .....	40
Installing ActiveSync on Client Computers .....	40
Configuring ActiveSync .....	41
Synchronizing the Mobile Device .....	43
Some Users Cannot Synchronize.....	43
No User Can Synchronize .....	43
Accessing the Exchange Server ActiveSync Web Administration Tool .....	45
Deploying Certificates .....	46

Obtaining a Certificate .....	46
Creating a Certificate Signing Request.....	47
Installing a Self-Issued Certificate .....	47
Configuring the Device .....	47
Direct Push Messages .....	47
Device Policy .....	48
Synchronizing .....	48
Related Links .....	49

# Deploying Windows Mobile 6 with Windows Small Business Server 2003

---

Do you want to add Windows Mobile® devices to your network? Is your network based either on the Windows® Small Business Server 2003 (Windows SBS) server software with Service Pack 1 (SP1) or on Windows Small Business Server 2003 R2? If so, you can use the step-by-step instructions in this document to deploy devices that are powered by the Windows Mobile 6 software on a Windows SBS network.

## Note

This is Version 3 of this document. To download the latest updated version, visit the [Microsoft Web site](http://go.microsoft.com/fwlink/?LinkId=75111) (<http://go.microsoft.com/fwlink/?LinkId=75111>). The update might contain critical information that was not available when this document was published.

## Windows Mobile 6

Windows Mobile 6 is the successor to Windows Mobile 5.0. It provides new features and tools to improve productivity, connectivity, and security. Some of the new features in Windows Mobile 6 include:

- The ability to view e-mails in their Rich Text formats, with access to live links to Microsoft® Office SharePoint® or other Web sites.
- Windows Live™ for Mobile, which provides access to a rich set of services like MSN® Messenger with the ability to hold concurrent chats with multiple people, send image or data files, record or send voice notes.
- The newest mobile versions of Microsoft Office, including Microsoft Office Outlook®, Microsoft Office Excel® and Microsoft Office PowerPoint®.
- New and improved user interface that is reminiscent of Windows Vista®.

## Messaging and Security Feature Pack

Windows Mobile 6 now integrates the Messaging and Security Feature Pack (MSFP), which was previously an add-on for Windows Mobile 5.0. This delivers features such as:

- **Direct Push Technology:** Items received on the Microsoft Exchange server, such as new e-mail messages, calendar changes, contact changes, or task updates, are immediately sent to a device that is running Windows Mobile 6. Direct Push Technology uses an IP-based Internet connection and does not use Short Message

Service (SMS), a form of text messaging. SMS is used by the previous Always-up-to-date (AUTD) synchronization process.

- **Wireless support for contact information:** This feature enables over-the-air lookup of global address list (GAL) information that is stored in Microsoft Exchange Server.
- **Remotely enforced security policy:** You can remotely manage and enforce security settings on the mobile devices over-the-air.
- **Local device wipe:** This feature resets the device after a specified number of incorrect logon attempts.
- **Remote device wipe:** This feature allows the administrator to remotely reset a Windows Mobile 6 device.

To take advantage of these new features, you must install Service Pack 2 (SP2) for Microsoft Exchange Server 2003 if your server is running Windows SBS 2003 with SP1. If your server is running Windows SBS 2003 R2, it already has the service pack installed.

## Before You Begin

### Skill Level

The intended audience for this document is Windows SBS administrators. To complete the steps in this document, you should have a basic understanding of Windows Mobile and you should have experience in deploying and managing Windows SBS.

### Windows Mobile Requirements

To complete the steps in this document, make sure your hardware and software meet the requirements in the following table.

**Table 1. Requirements for deploying a mobile device**

Requirement	Description
Windows Mobile 6 device	A mobile device that is running Windows Mobile 6.
Wireless data connectivity	The mobile device must have wireless data connectivity, provided through a mobile operator such as GPRS, to access the Internet, or Wi-Fi network access.
Server running Windows SBS 2003	A server that is running Windows SBS 2003 with SP1 or Windows SBS 2003 R2. It is assumed that Exchange Server 2003 is configured and running properly on the server.

Requirement	Description
Microsoft ActiveSync® 4.5 (for Windows XP)	You can download ActiveSync 4.5 from the <a href="http://go.microsoft.com/?linkid=6257291">Microsoft Web site</a> (http://go.microsoft.com/?linkid=6257291).
Windows Mobile Device Center 6.1 (for Windows Vista)	You can download Windows Mobile Device Center 6.1 (WMDC) from the <a href="http://www.microsoft.com/windowsmobile/devicecenter.msp">Microsoft Web site</a> (http://www.microsoft.com/windowsmobile/devicecenter.msp)

### Additional requirements

In addition to the Windows Mobile requirements above, make sure you have the following server-side software.

**Table 2. Additional Requirements for Deploying Windows Mobile 6**

Requirement	Description
SP2 for Exchange Server 2003	You can download SP2 for Exchange Server 2003 from the <a href="http://go.microsoft.com/fwlink/?LinkId=75114">Microsoft Web site</a> (http://go.microsoft.com/fwlink/?LinkId=75114). If your server is running Windows SBS 2003 R2, this service pack is already preinstalled.
Exchange Server ActiveSync Web Administration tool	You can download the Exchange Server ActiveSync Web Administration tool from the <a href="http://go.microsoft.com/fwlink/?LinkId=75115">Microsoft Web site</a> (http://go.microsoft.com/fwlink/?LinkId=75115).

## Process Steps

To deploy a mobile device on your Windows SBS network, complete the following steps:

- Step 1: Install ActiveSync 4.5 or WMDC 6.1
- Step 2: Enable mobile services for users
- Step 3: Configure the firewall and Web services
- Step 4: Install a certificate
- Step 5: Configure Windows Small Business Server 2003
- Step 6: Configure device synchronization
- Step 7: Test the deployment

## Step 1: Install ActiveSync 4.5 or WMDC 6.1

Mobile devices need to be connected to a client computer to copy files, install applications, and synchronize data directly with the computer. To connect the mobile device, you must install ActiveSync 4.5 on Windows XP client computers, or Windows Mobile Device Centre (WMDC) for Windows Vista client computers.

Manually install ActiveSync 4.5 on the client computers by copying the ActiveSync setup file to each client computer that you want to connect to a Windows Mobile device, and then run the ActiveSync 4.5 Setup program.

Manually install WMDC for client computers running Windows Vista by copying the WMDC setup file to each client computer that you want to connect to a Windows Mobile device, and then run the WMDC setup program.

### Note

If you have not already downloaded the ActiveSync 4.5 setup file, download it now from the [Microsoft Web site](http://go.microsoft.com/?linkid=6257291) (<http://go.microsoft.com/?linkid=6257291>). Before you install ActiveSync 4.5 on any computer, ensure that the computer meets the minimum system requirements for ActiveSync 4.5, which you can find at the [Microsoft Web site](http://www.microsoft.com/windowsmobile/activesync/activesync45.msp) (<http://www.microsoft.com/windowsmobile/activesync/activesync45.msp>).

### Note

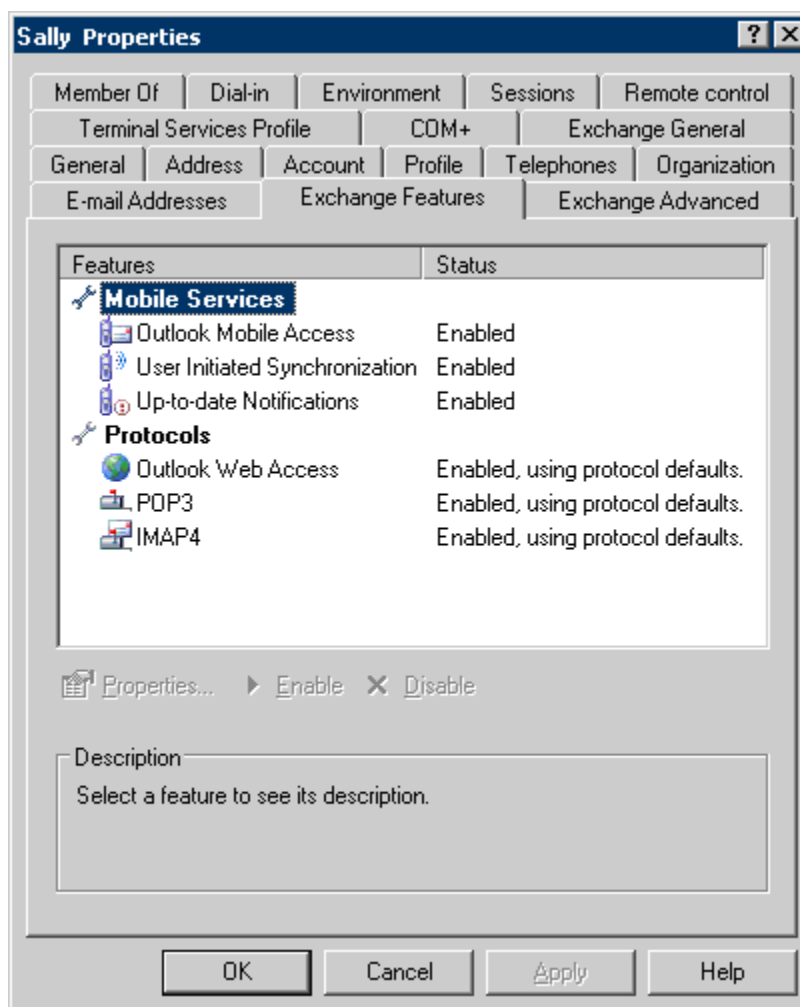
If you have not already downloaded the Windows Mobile Device Centre setup file, download it now from the [Microsoft Web site](http://www.microsoft.com/windowsmobile/devicecenter.msp) (<http://www.microsoft.com/windowsmobile/devicecenter.msp>). Before you install Windows Mobile Device Centre on any computer, ensure that the computer meets the minimum system requirements for WMDC, which you can find at the [Microsoft Web site](http://www.microsoft.com/windowsmobile/devicecenter.msp).

## Step 2: Enable Mobile Services for Users

Before you configure a mobile device for a user, you must enable mobile services for that user's Active Directory® user account. By default, new user accounts that are created in Windows SBS already have mobile services enabled.

► **To ensure that mobile services are enabled for a user:**

1. Open the **Server Management** console, click **Users**, and then double-click the user account.
2. On the **Exchange Features** tab of the **Properties** dialog box, ensure that all mobile services are enabled.



## Step 3: Configure the Firewall and Web Services

To enable mobile devices to access information stored on the Exchange server over the air, ensure that the incoming Exchange ActiveSync traffic is directed to the server that is running Windows SBS.

Complete the steps in this section to automatically configure the following firewalls:

- Microsoft Internet Security and Acceleration (ISA) Server, which is included in Windows Small Business Server Premium Edition
- The built-in Routing and Remote Access firewall in Windows SBS
- The UPnP hardware firewall

If you are using a firewall other than these, you need to manually configure your firewall to direct incoming traffic on port 443 to the server that is running Windows SBS.

To achieve this, you may have to configure the inward policies on your non-UPnP-based firewall, and enable SSL traffic on port 443. Different firewalls process SSL traffic differently, so you may have to either enable SSL traffic within the same policy as the HTTP policy, or you may have to define a new policy for HTTPS (SSL) traffic. Because port 443 is the default port for HTTPS traffic, you will not have to define or re-direct traffic to any specific port. However, make sure that you grant access rights to the correct set of users within the policy, so that only authorized users will be able to access the Internet through the firewall.

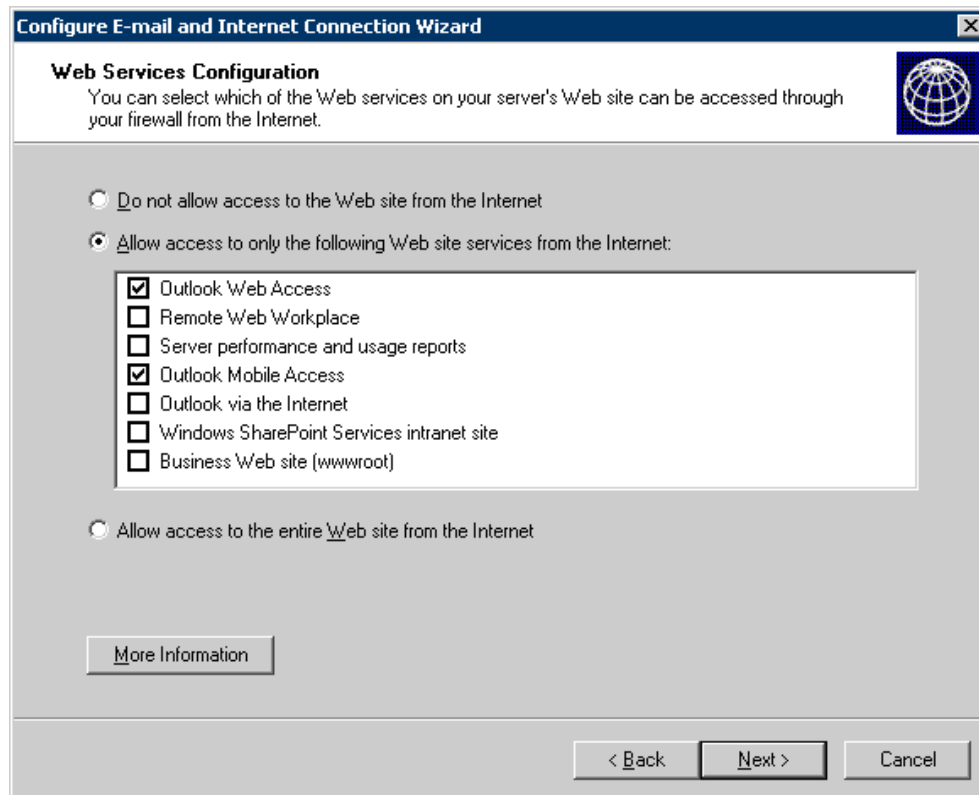
### ▶ To configure the firewall and Web services:

1. Open the **Server Management** console, and then click **Internet and E-mail**.
2. Click **Connect to the Internet** to start the Configure E-mail and Internet Connection Wizard (CEICW).
3. On the **Welcome** page, click **Next**.
4. On the **Connection Type** page, click **Do not change connection type**, and then click **Next**.
5. On the **Firewall** page, click **Enable Firewall**, and then click **Next**.
6. On the **Services Configuration** page, select the services that are in use on your network, and then click **Next**.
7. On the **Web Services Configuration** page, select **Outlook Mobile Access** and any other services that need to be enabled. Click **Next**.

#### **Note**

Selecting Outlook Mobile Access enables over-the-air synchronization

with Windows Mobile devices.



8. On the **Web Server Certificate** page, click **Do not change current Web server certificate**, and then click **Next**.
9. On the **Internet E-mail** page, click **Do not change Internet e-mail configuration**, and then click **Next**.
10. On the **Completing the Configure E-mail and Internet Connection Wizard** page, click **Finish**.

 **Note**

As mentioned earlier, if you are using an external or third-party firewall, ensure that incoming traffic on port 443 is directed to the server that is running Windows SBS.

## Step 4: Install a Certificate

This section provides guidance on choosing and configuring a certificate. A certificate helps securely synchronize data by using the Secure Sockets Layer (SSL) protocol. It is

important to use SSL to help secure communications between the mobile device and the server.

## Choose the Type of Certificate

You can use either of the following two options to install a certificate for Windows Mobile 6.0 devices:

- **Third-party certificate:** You can buy and install a certificate from a trusted root certification authority (CA). The certificate has a root certificate store present on the mobile device. This is the preferred solution. However, you could use a self-issued certificate if it isn't possible to use a third-party certificate.
- **Self-issued certificate:** You can install a self-issued certificate that Windows SBS generates.



### Note

Windows Mobile 6 now contains two certificate stores— the Device Store that contains all the factory-installed Root certificates, and the User Store into which user-issued certificates can be saved. Self-issued certificates generated by Windows SBS will be saved in this User Store. However, with Windows Small Business Server 2003, self-issued certificates can now be manually installed on a Windows Mobile 6 device. This was not the case in many of the Windows Mobile 5 devices.

The following table summarizes the advantages and disadvantages of using these two types of certificates on Windows Mobile devices.

**Table 3. Advantages and Disadvantages of Each Type of Certificate**

Choice	Advantages	Disadvantages
Third-party certificate	<ul style="list-style-type: none"> <li>• No additional configuration is required on the Windows Mobile device.</li> <li>• Can be used with all Windows Mobile Classic, Professional and Standard devices, including Windows Mobile 5 devices.</li> <li>• Provides additional benefits with other Windows SBS features, such as Office Outlook Web Access, Remote Web Workplace, RPC over HTTP, and the ability to suppress warnings on a Web browser.</li> </ul>	<ul style="list-style-type: none"> <li>• Must be purchased, and may require a recurring fee for renewals. Can cost about \$25 to \$1,000 annually.</li> <li>• Cannot be installed immediately, because it requires independent verification of your company information before it is issued. However, there are some third-party certificates that can be immediately installed – but these are exceptional cases.</li> </ul>
Self-issued certificate generated by Windows SBS	<ul style="list-style-type: none"> <li>• Can be automatically generated by Windows SBS through CEICW.</li> <li>• No additional cost.</li> <li>• Fewer configurations are required in Windows SBS.</li> </ul>	<ul style="list-style-type: none"> <li>• Requires additional configuration on the device. The certificate must be exported to and installed on each device.</li> </ul>

Choose the certificate type that is best for your environment.

Keep in mind that a third-party certificate offers additional benefits of convenience to users of a Windows SBS network. For example, they can use Outlook over the Internet from any computer without having to specifically install the certificate on the remote computer, and without being prompted with a certificate error when they access Outlook Web Access, Remote Web Workplace, Microsoft Windows SharePoint Services, or other Web sites that Windows SBS hosts.

## Configure the Certificate

For Exchange ActiveSync synchronization to work correctly, you need to implement either of the following certificate configurations:

1. A trusted certificate that must be installed on the SBS server.
2. The self-issued certificate that must be installed on the mobile device.

Depending on the type of certificate that you select, complete the steps in either of the following two sections.

### Option A: Configure a Self-Issued Certificate

This section tells you how to export and install the self-issued certificate that is created by Windows SBS onto a mobile device. For multiple mobile devices, you need to install the certificate on each device. The certificate is already installed on the server that is running Windows SBS, so you do not need to configure the server.

Perform the following steps to install the certificate on a mobile device:

1. Create a shared folder in which to store the certificate.
2. Export the certificate to the shared folder so the mobile devices can access it.
3. Install the certificate on the Windows Mobile device.

#### ▶ To create a shared folder in which to store the certificate file

1. On the server, open Windows Explorer.
2. Select the root drive or folder in which you want to create the new shared folder.
3. Click **File**, point to **New**, and then click **Folder**.
4. Rename the new folder to something you will remember (for example, **CertShare**).
5. Right-click the renamed folder, and then click **Sharing and Security**.
6. Click the **Sharing** tab, select **Share this folder**, either type a name for the shared folder or accept the default, and then click **OK**.

#### ▶ To export the certificate file to the shared folder so the mobile devices can access it

1. While you are still logged on to the server, open Internet Explorer.
2. Click the **Tools** menu, and then click **Internet Options**. The **Internet Options** dialog box appears.
3. Click the **Content** tab, and then click the **Certificates** button. The **Certificates**

dialog box appears.

4. Click the **Trusted Root Certification Authorities** tab.
5. Scroll through the list of certificates, and then select the certificate that was generated by Windows SBS. You can usually identify the certificate by recognizing the IP address or domain name in the **Issued to** or **Issued by** fields.
6. Click **Export**. The Certificate Export Wizard starts.
7. On the **Welcome** page, click **Next**.
8. On the **Export File Format** page, select **DER encoded binary X.509 (.CER)**, and then click **Next**.
9. On the **File to Export** page, click **Browse**, and then open the shared folder that you created in the previous procedure.
10. Type a file name to identify the certificate that you are exporting, and then click **Save**. The file path appears on the **File to Export** page of the Certificate Export Wizard.
11. Click **Next**.
12. Review the settings for accuracy, and then click **Finish**.
13. Click **OK** to acknowledge that you have successfully exported the certificate.
14. Click **Close** to close the **Certificate** dialog box.
15. Click **OK** to close the **Internet Options** dialog box.

After you successfully export the certificate to the shared folder, complete the following steps to install the certificate on a Windows Mobile device.

#### **To install the certificate on a Windows Mobile device**

1. Connect your mobile device to your client computer, using its cradle or cable.
2. On the client computer, open Windows Explorer, and then open the shared folder that you created on the server.
3. Copy the certificate file from the shared folder, and then paste it into the Mobile Device node in Windows Explorer on the client computer. This places the certificate in the My Documents folder on the Windows Mobile device.
4. On the Windows Mobile device, open **File Explorer**.

#### **Note**

To open **File Explorer**, click **Start**, then click **More**, and click the **File Explorer** icon.

5. Find the certificate file you just copied to the My Documents folder on the device, and then run the file either by tapping the file name or by selecting the file and

pressing **Enter**.

6. Click **Yes** on the confirmation message box to install the certificate. If you receive no error messages, the certificate is installed successfully.

## Option B: Configure a Third-party Certificate

This section tells you how to purchase and install a third-party certificate on the server that is running Windows SBS.

### **Note**

Some certification authorities (CAs) provide their own instructions for installing certificates on the server. Depending on the type of certificate, these instructions may be different than the steps here. You should follow the installation instructions provided by the CA, if they are available, instead of the instructions here.

### **Purchase a Third-party Certificate**

You should use third-party certificates only from a CA that has a root certificate present on the root store of Windows Mobile powered devices.

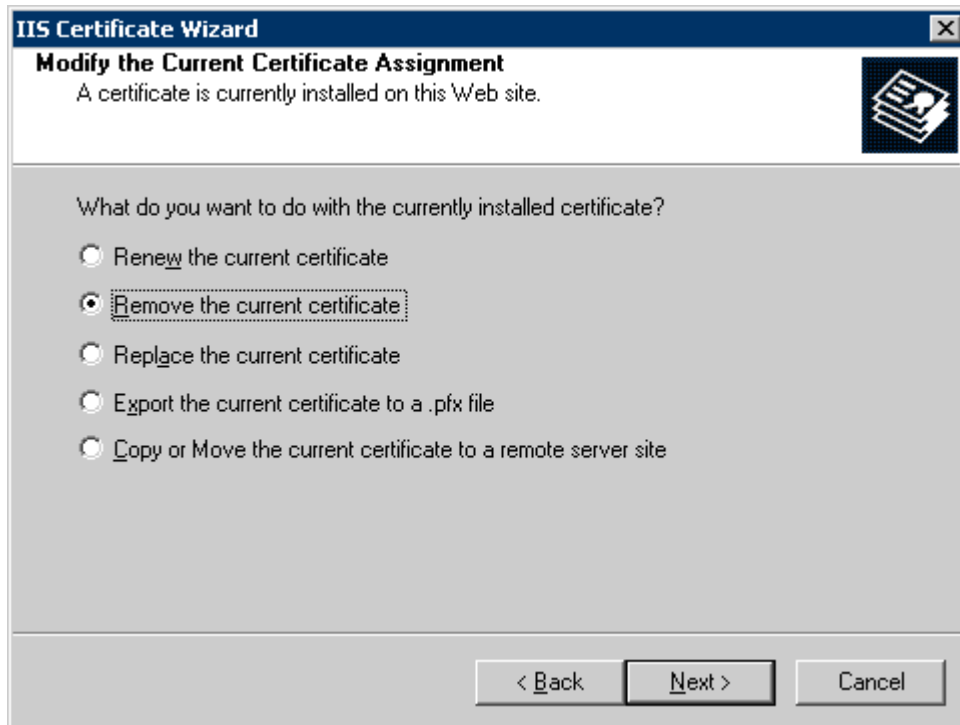
To purchase a certificate from a CA, you need to generate a certificate signing request on the server that is running Windows SBS.

### **To generate a certificate signing request**

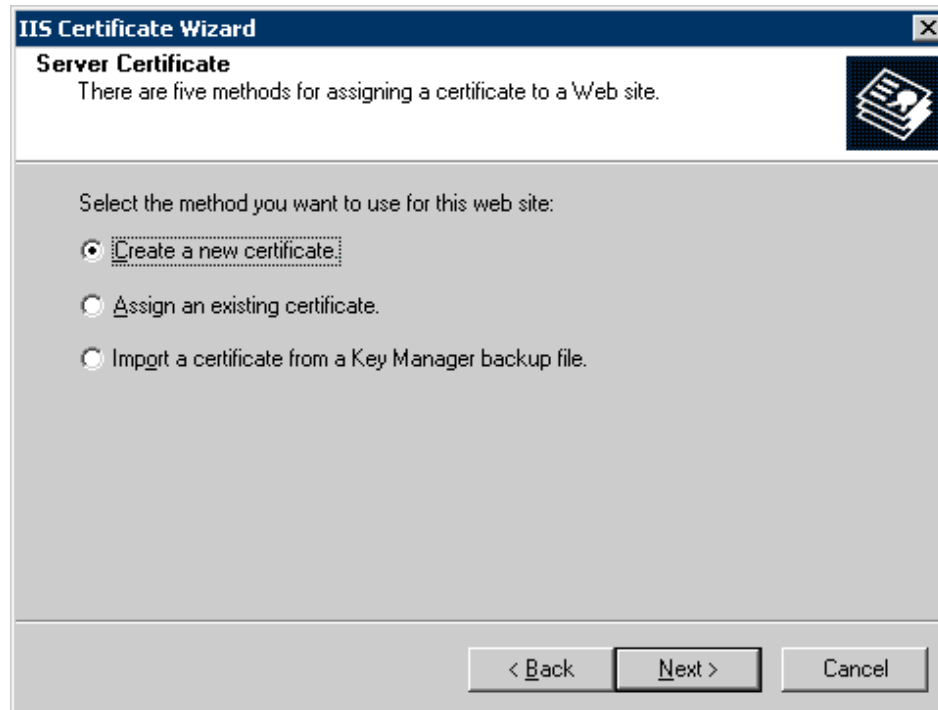
1. Open **Internet Information Services (IIS) Manager** from **Administrative Tools**.
2. Expand **WindowsSBSServerName**, expand **Web Sites**, right-click **Default Web Site**, and then click **Properties**.
3. On the **Directory Security** tab, click the **Server Certificate** button to start the IIS Certificate Wizard.
4. On the **Welcome** page, click **Next**.
5. If you have an existing certificate installed on the server, the **Modify the Current Certificate Assignment** page appears. If the page appears, complete the following steps:
  - a. Click **Remove the current certificate**, and then click **Next**.

### **Note**

The existing certificate may have been created when you ran the Configure E-Mail and Internet Connection Wizard.



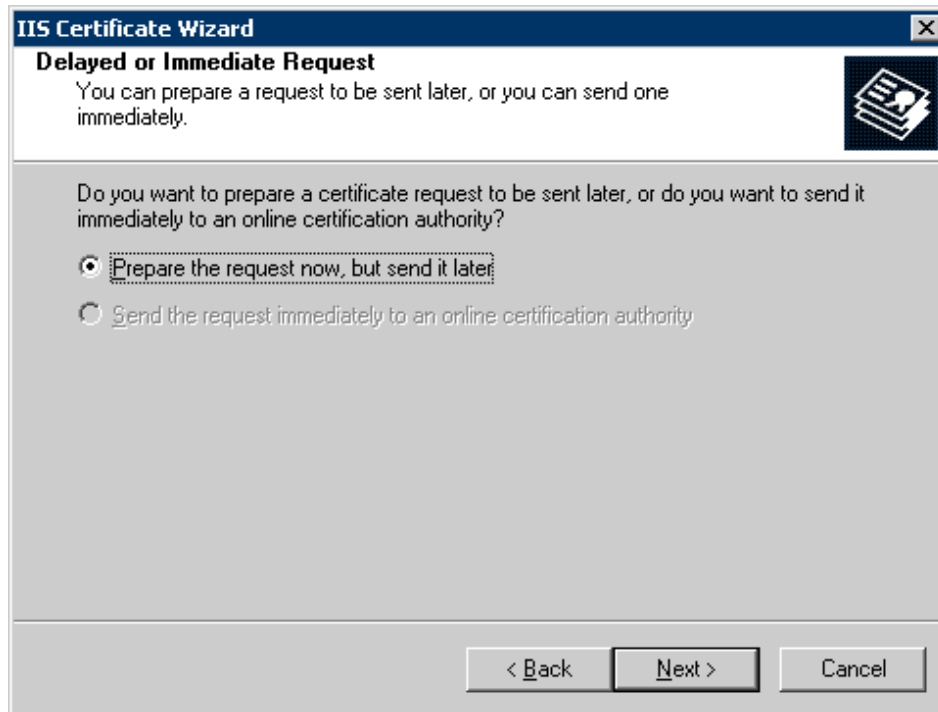
- b. Click **Next** on the next two pages, and then click **Finish** to complete the wizard and to remove the certificate.
  - c. Start the wizard again by clicking the **Server Certificate** button on the **Directory Security** tab.
  - d. On the **Welcome** page, click **Next**.
6. On the **Server Certificate** page, click **Create a new certificate**, and then click **Next**.



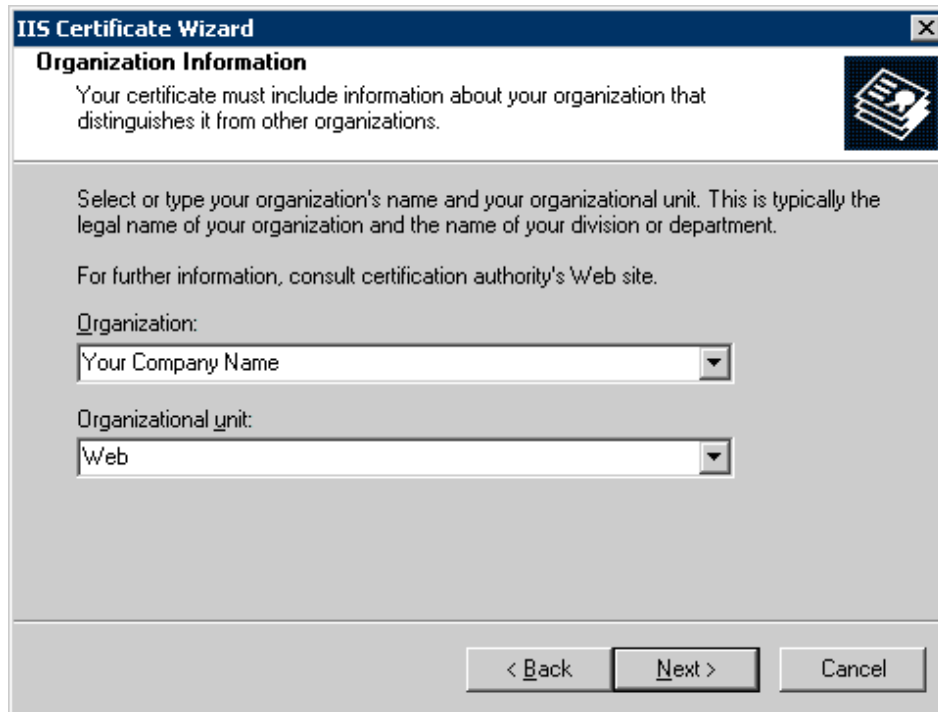
7. On the **Delayed or Immediate Request** page, click **Prepare the request now, but send it later**, and then click **Next**.

 **Note**

If you have a certificate from a CA installed on the server, the second option is not disabled.



8. On the **Name and Security Settings** page, type the name of the company, and then click **Next**.
9. On the **Organization Information** page, type the name of the company and the name of the department, both of which may be the same.

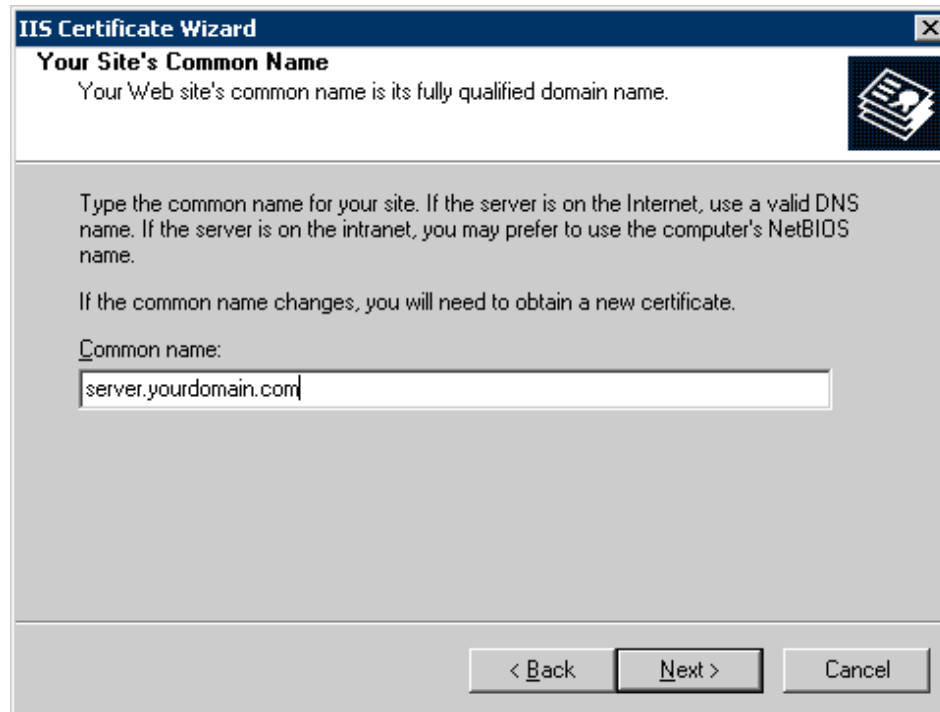


The screenshot shows a Windows dialog box titled "IIS Certificate Wizard" with a close button (X) in the top right corner. The dialog is divided into sections. The top section is titled "Organization Information" and contains the text: "Your certificate must include information about your organization that distinguishes it from other organizations." To the right of this text is a small icon of a document with a keyhole. Below this is a larger text area with the instruction: "Select or type your organization's name and your organizational unit. This is typically the legal name of your organization and the name of your division or department." This is followed by the text: "For further information, consult certification authority's Web site." There are two dropdown menus: the first is labeled "Organization:" and contains the text "Your Company Name"; the second is labeled "Organizational unit:" and contains the text "Web". At the bottom of the dialog are three buttons: "< Back", "Next >", and "Cancel".

 **Note**

It is important to type the proper company name because the CA uses this name to verify the company information before it issues a certificate. After you submit the request, the CA verifies the information that you have submitted, as well as the company information. If you apply for the certificate using a Trade/DBA (Doing Business As) name, be prepared to show documentation of the trade name. Also be sure to update your Dun & Bradstreet (D&B) or other commercial directory information before you submit the certificate signing request, because many CAs use that information for verification. Get the exact verification requirements from the CA that you have chosen.

10. On the **Your Site's Common Name** page, type the public DNS (Domain Name System) name of the server. Take special care to ensure that the information is correct, because the certificate will not work properly if this information is incorrect.



The screenshot shows a Windows-style dialog box titled "IIS Certificate Wizard". The main heading is "Your Site's Common Name". Below the heading, it says "Your Web site's common name is its fully qualified domain name." To the right of this text is a small icon of a document with a keyhole. The main area of the dialog contains the following text: "Type the common name for your site. If the server is on the Internet, use a valid DNS name. If the server is on the intranet, you may prefer to use the computer's NetBIOS name." Below this is another line of text: "If the common name changes, you will need to obtain a new certificate." Underneath is a label "Common name:" followed by a text input field containing the text "server.yourdomain.com". At the bottom of the dialog are three buttons: "< Back", "Next >", and "Cancel".

Important: The URL you enter in this step should be the same one that you entered into the Configure E-mail and Internet Connection Wizard earlier.

11. On the **Geographical Information** page, enter all of the required information. Do not use abbreviations, because some CAs do not accept abbreviations.

**IIS Certificate Wizard**

**Geographical Information**  
The certification authority requires the following geographical information.

Country/Region:  
US (United States)

State/province:  
My State

City/locality:  
My City

State/province and City/locality must be complete, official names and may not contain abbreviations.

< Back    Next >    Cancel

12. Provide a path and a file name for saving the request. Click **Next** twice, and then click **Finish**.
13. Open the request file that you just created by using Notepad, and then copy all of the text that is in the file, including dashes, into the application form that you are sending to the CA.

 **Note**

Be careful not to change or modify any of the certificate settings on the Web site after you create the certificate request. The steps in this procedure do not work if the pending request is cancelled for any reason. If you cancel the pending request, you need to apply to the CA to have the certificate reissued using a new request file.

### Install a Third-party Certificate

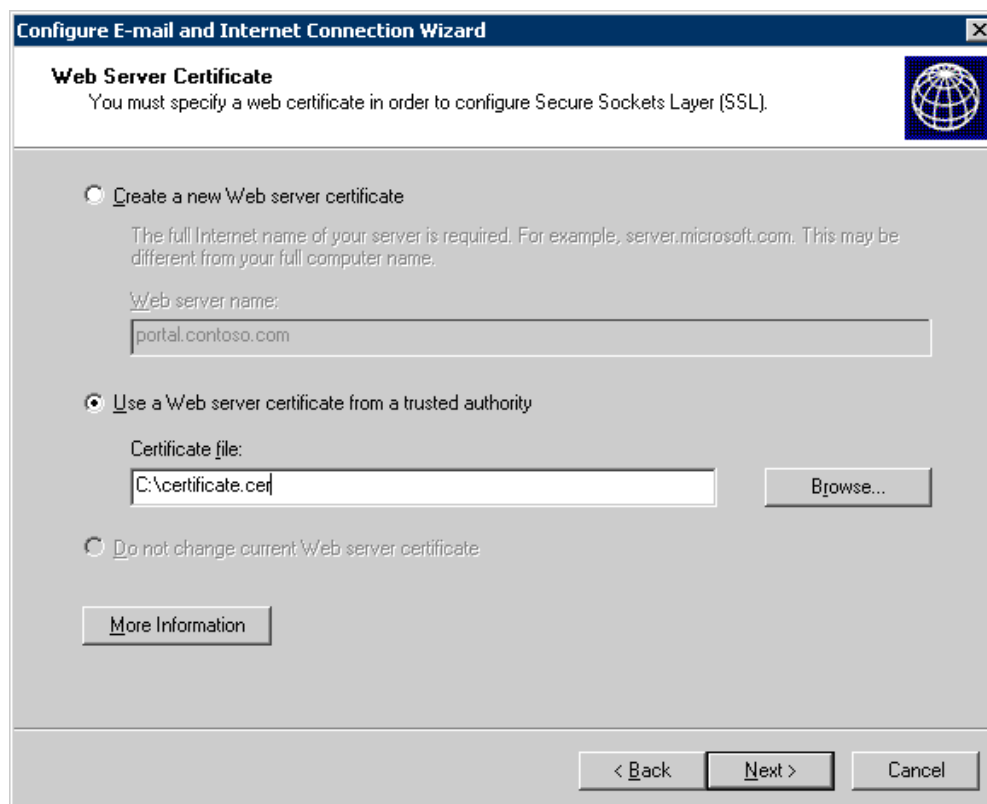
If you purchased or already have a third-party certificate, you may be able to install it by simply cradling the mobile device to the client computer, and then copying the certificate to the **Mobile Device** node of the client computer. However, if this does not work, perform the following steps to configure and install a third-party certificate for use on mobile devices:

1. Install a third-party certificate on the server.

2. Create a shared folder in which to store the certificate.
3. Export the certificate to the shared folder so the mobile devices can access it.
4. Install the certificate on the Windows Mobile device.

▶ **To install a third-party certificate on the server**

1. Open the **Server Management** console.
2. Click **Internet and E-mail**.
3. Click **Connect to the Internet**. The Configure E-mail and Internet Connection Wizard starts.
4. On the **Welcome** page, click **Next**.
5. On the **Connection Type** page, click **Do not change connection type**, and then click **Next**.
6. On the **Firewall** page, click **Do not change firewall configuration**, and then click **Next**.
7. On the **Web Server Certificate** page, click **Use a Web server certificate from a trusted authority**, click **Browse**, navigate to and double-click the certificate file provided by the CA, and then click **Next**.



8. On the **Internet E-mail** page, click **Do not change Internet e-mail configuration**, and then click **Next**.
9. On the **Completing the Configure E-mail and Internet Connection Wizard** page, click **Finish**.

If you are using a trusted certificate, your Windows Mobile device will already have the root of the trusted certificate on it. You can therefore skip the following sequence of configuration tasks, and proceed directly to Step 5.

▶ **To create a shared folder in which to store the certificate**

1. On the server, open Windows Explorer.
2. Select the root drive or folder in which you want to create the new shared folder.
3. Click **File**, point to **New**, and then click **Folder**.
4. Rename the new folder to something you will remember (for example, **CertShare**).
5. Right-click the renamed folder, and then click **Sharing and Security**.

6. Click the **Sharing** tab, select **Share this folder**, either type a name for the shared folder or accept the default, and then click **OK**.

▶ **To export the certificate to the shared folder so the mobile devices can access it**

1. While you are still logged on to the server, open Internet Explorer.
2. Click the **Tools** menu, and then click **Internet Options**. The **Internet Options** dialog box appears.
3. Click the **Content** tab, and then click the **Certificates** button. The **Certificates** dialog box appears.
4. Click the **Other People** tab.

 **Note**

If the certificate that you purchased and installed on the server does not appear in the list on the **Other People** tab, look for it by clicking the other tabs in the **Certificates** dialog box.

5. Select the certificate that you installed on the server, and then click **Export**. The **Certificate Export Wizard** starts.
6. On the Welcome page of the **Certificate Export Wizard**, click **Next**.
7. On the **Export File Format** page, select **DER encoded binary X.509 (.CER)**, and then click **Next**.
8. On the **File to Export** page, click **Browse**, and then open the shared folder that you created in the previous procedure.
9. Type a file name to identify the certificate that you are exporting, and then click **Save**. The file path appears on the **File to Export** page of the **Certificate Export Wizard**.
10. Click **Next**.
11. Review the settings for accuracy, and then click **Finish**.
12. Click **OK** to acknowledge that you have successfully exported the certificate.
13. Click **Close** to close the **Certificate** dialog box.
14. Click **OK** to close the **Internet Options** dialog box.

After you successfully export the third-party certificate to the shared folder, complete the following steps to install the certificate on the Windows Mobile device.

▶ **To install the certificate on the Windows Mobile device**

1. Cradle the mobile device to your client computer.

2. On the client computer, open Windows Explorer, and then open the shared folder that you created on the server.
3. Copy the certificate file from the shared folder, and then paste the copied file into the Mobile Device node in Windows Explorer on the client computer. This places the certificate in the My Documents folder on the device.
4. On the Windows Mobile device, open **File Explorer**.

 **Note**

To open **File Explorer**, click **Start**, then click **More**, and click the **File Explorer** icon.

5. Find the certificate file you just copied to the My Documents folder on the device, and then run the file by either tapping the file name or by selecting the file and then pressing **ENTER**.
6. Click **Yes** on the confirmation message box to install the certificate. If you receive no error messages, the certificate is installed successfully.

## Step 5: Configure Windows Small Business Server

To configure the server, you will need to complete the following tasks:

1. Install SP2 for Exchange Server 2003 (not required if Windows Small Business Server 2003 R2 is used).
2. Install the Exchange Server ActiveSync Web Administration tool.
3. Enable Direct Push.

### Install the Exchange Server ActiveSync Web Administration Tool

To take advantage of the remote-device wipe and the password enforce feature, you need to install the Exchange Server ActiveSync Web Administration tool. Note that before you install the tool, SP2 for Exchange Server 2003 must already be installed on the server running Windows SBS, or the server must be running Windows SBS 2003 R2.

The tool is available for download at the [Microsoft Web site](http://go.microsoft.com/fwlink/?LinkId=75115) (<http://go.microsoft.com/fwlink/?LinkId=75115>).

After you install the Exchange Server ActiveSync Web Administration tool, ensure that the installation was successful. To do this, open Microsoft Internet Explorer® on the

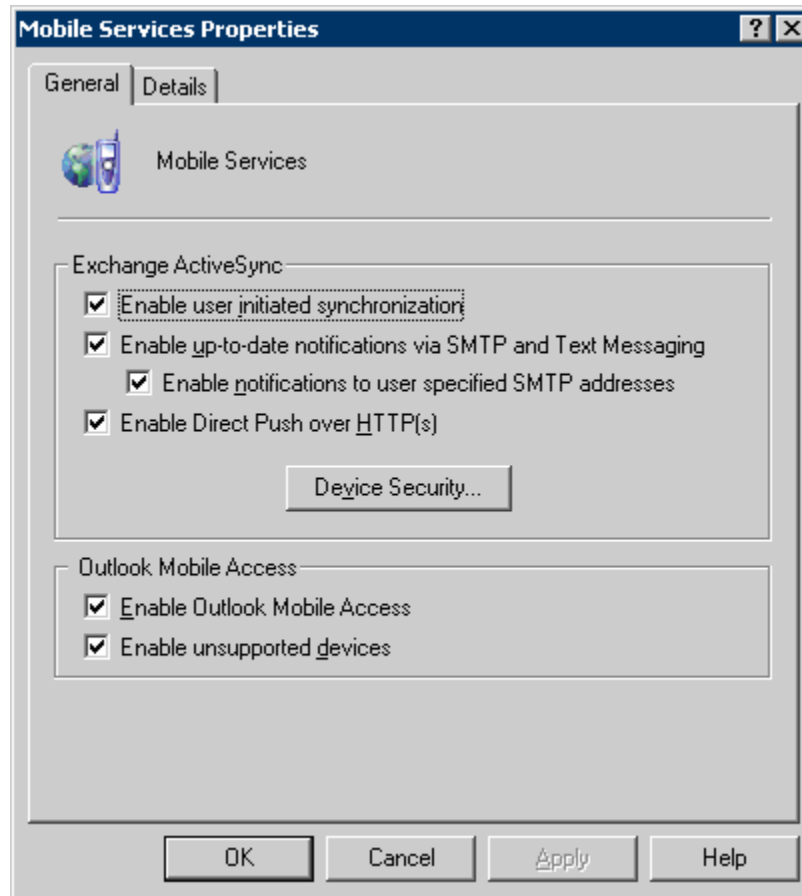
server, browse to <http://localhost/mobileadmin>, and log on to the console by providing domain administrator credentials.

## Enable Direct Push

Direct Push provides users with immediate access to new information or changes to information that is stored on the Exchange server, including e-mail, calendar, contacts, and tasks information.

### ▶ To enable Direct Push on the server

1. Ensure that SP2 for Exchange Server 2003 is installed on the server, or that Windows Server 2003 R2 is being used.
2. Open **Exchange System Manager**.
3. Expand **Global Settings**.
4. Right-click **Mobile Services**, and then click **Properties**.
5. Verify that the **Enable Direct Push over HTTP(s)** check box is selected.



► **To enable Direct Push on the device**

1. Ensure that the device is not connected to a client computer.
2. Run ActiveSync on the device.
3. Navigate to **Menu\Schedule**.
4. Set **Sync during** to **As items arrive**.

## Step 6: Configure Device Synchronization

Depending on the operating system that the client computer is running, device synchronization will happen using either ActiveSync (for Windows XP clients), or WMDC (for Windows Vista clients).

## Device Synchronization Using ActiveSync

This section helps you configure a Windows Mobile device to synchronize with the server and with client computers that have Microsoft ActiveSync 4.5 installed on Windows XP. For guidance on installing ActiveSync 4.5, see “Step 1: Install ActiveSync 4.5”, earlier in this document.

### ▶ To configure a Windows Mobile device to synchronize with Windows SBS

1. Connect the Windows Mobile device to a client computer. The connection method depends on the capabilities of the device and the computer, and it typically uses a USB, serial, Bluetooth, or infrared port.

 **Note**

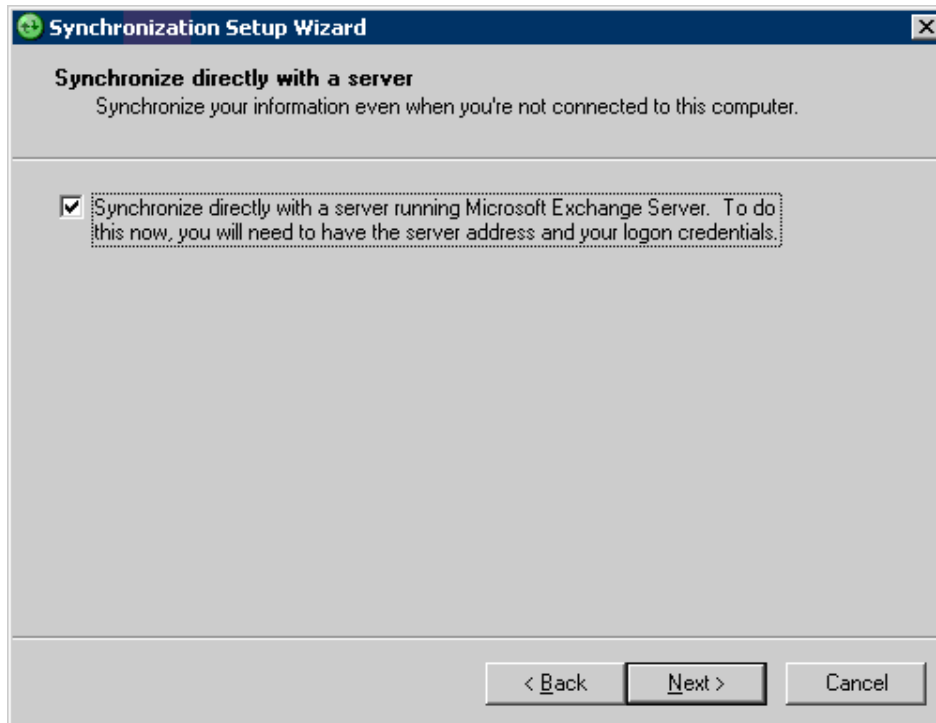
ActiveSync 4.5 must be installed on the Windows XP client computer.

2. After connecting the device to a client computer, the Synchronization Setup Wizard opens automatically on the client computer.

 **Note**

If the device has already been configured once, the screens are different than those shown here.

3. Click **Next** on the **Welcome** page.
4. On the **Synchronize directly with a server** page, select the **Synchronize directly with a server running Microsoft Exchange Server** check box, and then click **Next**.



5. On the **Exchange server credentials** page, type the public DNS name of the server and the logon credentials of the user. Select the **This server requires an encrypted (SSL) connection** and the **Save password** check boxes. Click **Next**.

**Synchronization Setup Wizard**

**Exchange server credentials**  
Enter the information that will authenticate you to a server running Microsoft Exchange Server

Server address:

Note: If you use Outlook Web Access, this is the same as your OWA server address.

This server requires an encrypted (SSL) connection

Logon Credentials

User name:

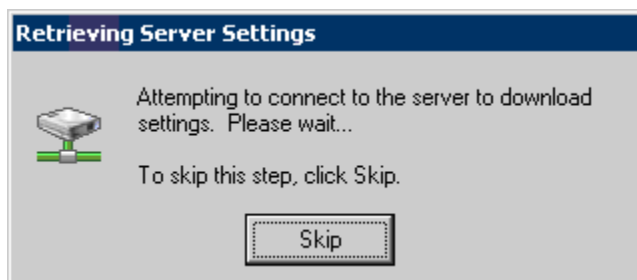
Password:

Domain:

Save password  
(required for automatic synchronization)

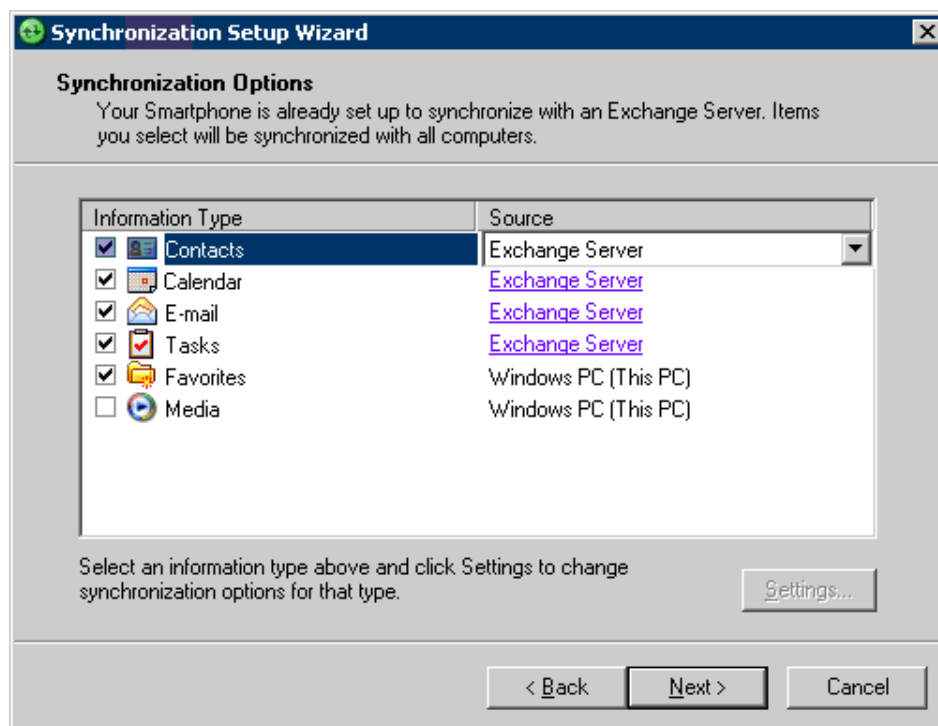
< Back   Next >   Cancel

ActiveSync attempts to connect to the server.



If you receive any errors during the attempt, see “Troubleshooting,” later in this document.

- On the **Synchronization Options** page, select the items that you want the device to synchronize. Select **Exchange Server** as the **Source** for Contacts, Calendar, Tasks, and E-mail. Additional items, such as Media and Favorites, can be synchronized with the client computer only.



7. Click **Next**, and then click **Finish** to complete the wizard.

## Device Synchronization Using WMDC

This section helps you configure a Windows Mobile device to synchronize with the server and with client computers that have Windows Mobile Device Center installed on Windows Vista. For guidance on installing WMDC, see “Step 1: Install ActiveSync 4.5 or WMDC”, earlier in this document.

▶ **To configure a Windows Mobile device to synchronize with Windows SBS**

1. Connect the Windows Mobile device to the client computer. The connection method depends on the capabilities of the device and the computer, and it typically uses a USB, serial, Bluetooth, or infrared port.

📌 **Note**

WMDC must be installed on the Windows Vista client computer.

2. After connecting the device to the client computer, click **Start**, then click **Programs** and click **Windows Mobile Device Center**.

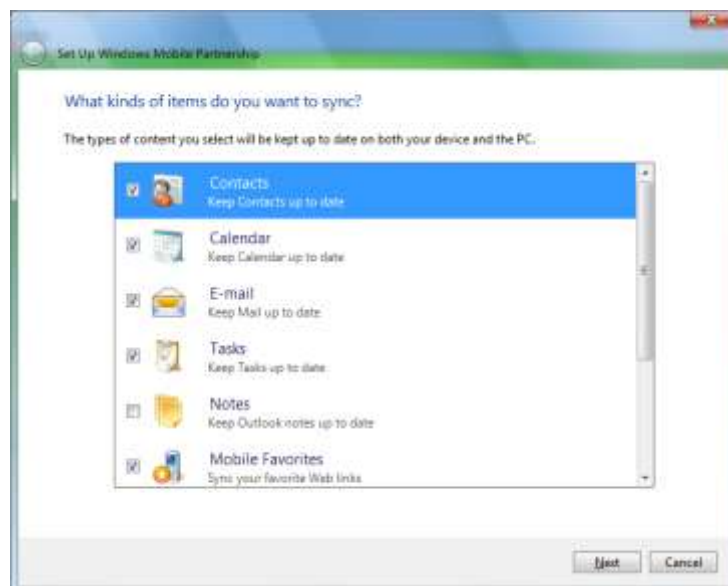
📌 **Note**

If the device has already been configured once, the following screens will be different than those shown here.

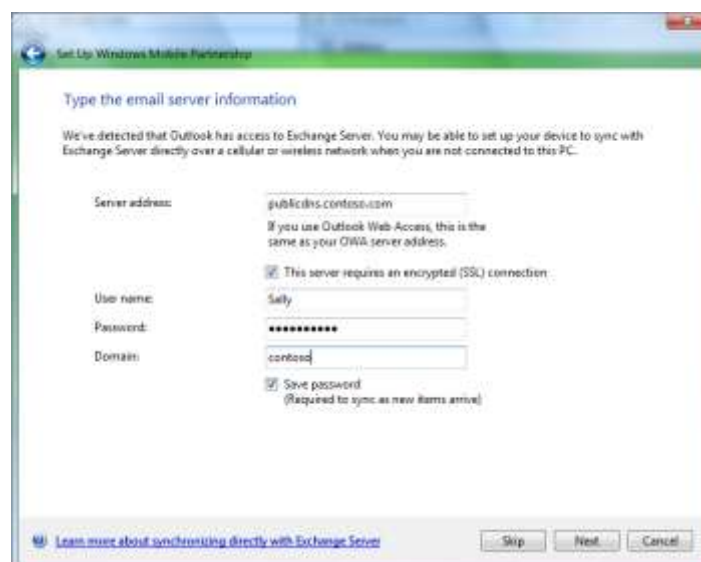
3. Click **Set up your device** on the Home page.



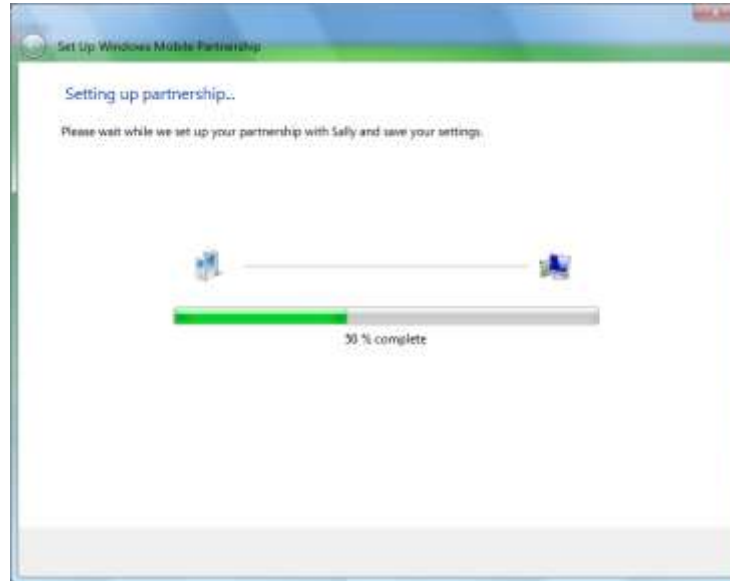
4. The following page will prompt you to check mark the elements that you want to synchronize. On this page, you will see Contacts, Calendar, E-mail, tasks and more. Click **Next** to proceed.



5. This page will prompt you to enter information specific to your Exchange Server. On this page, you will need to enter the **Server address**, the **User name**, the **Password** and the **Domain** for your Exchange Server. If your server requires an encrypted (SSL) connection, you will need to check the relevant box. You can choose to save your password if you wish to. Click **Next** to proceed. WMDC will now attempt to connect to the server.



- You will see a progress bar as WMDC attempts to set up a partnership between your Windows Mobile device and the Exchange Server.



- After the synchronization is complete, the application will return to the home screen, from where you can access Programs and Services, media files, File Management, and Mobile Device Settings.



8. Now click Mobile Device Settings to expand a list of further options. Click **more>>** to proceed.



9. Click **Change content sync settings**.



10. This takes you the screen from which you can select the synchronization settings for your Windows Mobile phone's content.



## Step 7: Test the Deployment

This section provides guidance on testing the deployment of the mobile devices.

### Test Over-the-Air Synchronization

#### ▶ To test the configuration of over-the-air ActiveSync on the device

1. Ensure that the device is not connected to the client computer or to a wireless LAN with Internet access.
2. Ensure that wireless data connectivity to the Internet, such as GPRS, is available on the device.
3. Open ActiveSync on the device and begin to synchronize.

The device connects to the Internet, if it is not already connected, and it synchronizes the items that you selected when you configured ActiveSync.

If the synchronization does not work for any reason, see "Troubleshooting," later

in this document, for more information.

## Test Direct Push

### ▶ To test the configuration of Direct Push

1. Ensure that the mobile device is not connected to a client computer or to a wireless LAN with Internet access.
2. Ensure that wireless data connectivity to the Internet, such as GPRS, is available on the device.
3. Send a message to the user account for which the device is configured.
4. Verify that the device receives the new message immediately.

#### Note

Direct Push is not used for synchronization when the device is connected to a computer or to a wireless LAN with Internet access.

## Remote Management

Windows Mobile 6 offers several new features that help you better manage mobile devices and better protect data. This section provides guidance on using the following two features:

- Remote device wipe
- Device security policies

### Remote Device Wipe

The remote device wipe feature enables you to erase all information on a device remotely. This prevents any compromise of corporate data if a user misplaces a device.

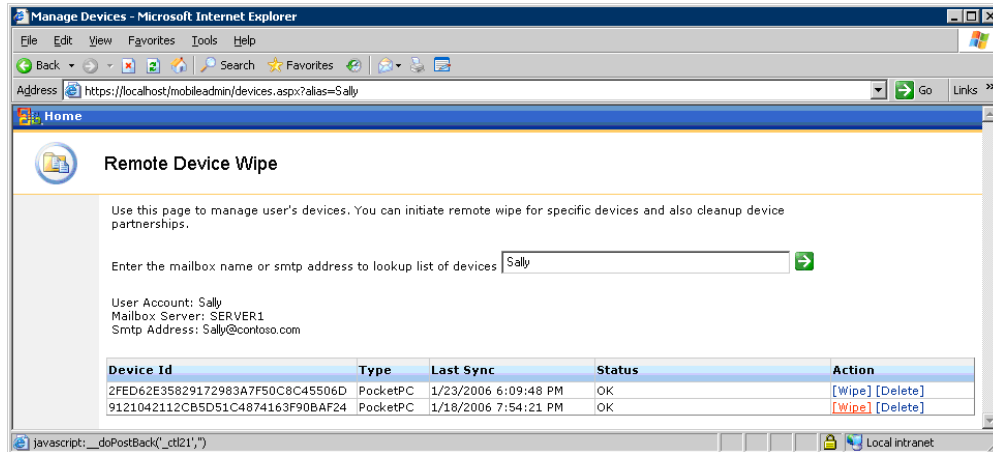
#### Note

Before testing this feature, ensure that any important data is on the Windows Mobile device is correctly backed up.

### ▶ To remotely wipe all information from a device

1. On any computer in the network, open Internet Explorer, browse to <https://ServerName/mobileadmin>, and then log on using domain administrator credentials.
2. Click **Remote Wipe**.

3. Type the mailbox name or the default SMTP address of the user whose device you want to wipe, and then press ENTER.



4. Click the **Wipe** link next to the device name that you want to wipe remotely.

#### Note

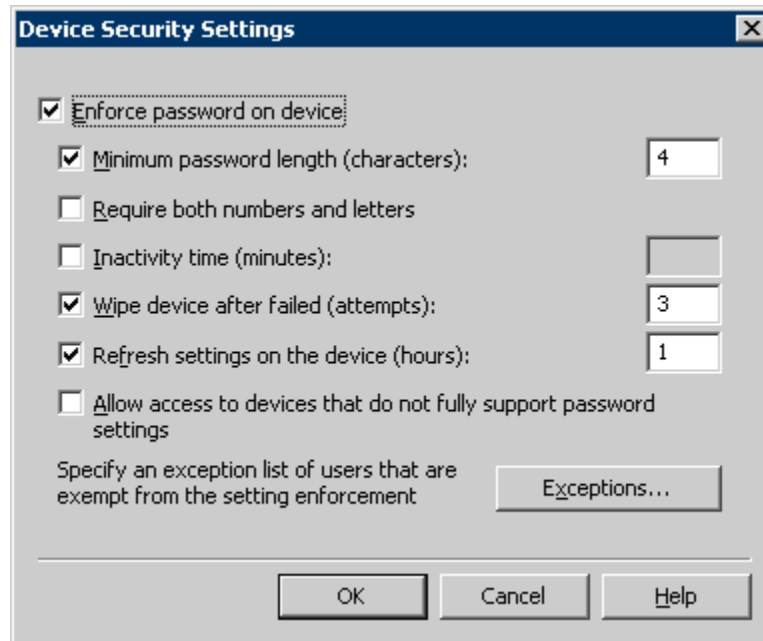
If you plan to ever reuse the same device, go back to the Mobile Admin site and cancel the wipe command after the wipe is successful.

## Device Security Policies

You can enforce device security policies on Windows Mobile 6 devices, such as password requirements. This helps protect information that is stored on the mobile devices. You can configure device security policies only on a server that is running Windows SBS 2003 R2.

### To define and enforce security policies for mobile devices

1. On the server, open **Exchange System Manager**.
2. Expand **Global Settings**.
3. Right-click **Mobile Services**, and then click **Properties**.
4. Click the **Device Security** button.
5. In the **Device Security Settings** dialog box, configure the device security policy for Windows Mobile devices.



6. If you do not want to apply the policy to some user accounts, click the **Exceptions** button, and then add the user accounts to the exceptions list.
7. Click **OK**.

## Troubleshooting

This section provides some troubleshooting steps and tips to resolve a number of issues that may occur while deploying Windows Mobile devices. The troubleshooting steps and tips are categorized into the following sections:

- Installing ActiveSync on client computers
- Configuring ActiveSync
- Synchronizing the mobile device
- Accessing the Exchange Server ActiveSync Web Administration tool
- Deploying certificates
- Configuring the device

### Installing ActiveSync on Client Computers

If ActiveSync 4.5 is not installed successfully on a client computer, try the following:

- Ensure that you are logged on as a local administrator on the computer. The software cannot be installed without local administrative rights.

 **Note**

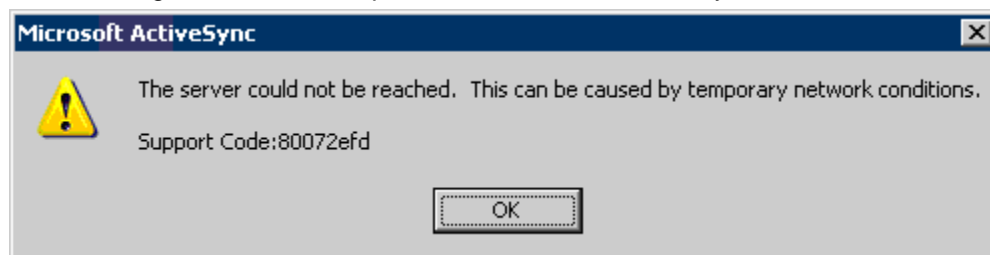
By default, Windows SBS makes a user a local administrator when the user joins the computer to the network using the Connect Computer Wizard.

- If you are using Group Policy to install ActiveSync, ensure the following:
  - The access control lists (ACLs) are set properly on the GPO.
  - The Authenticated Users group must not be on the list, and the Windows SBS Mobile Users group must have Read and Apply Group Policy permissions checked.
  - The GPO is linked to the proper organizational unit (OU). The steps provided in this document link the GPO to the Windows SBS Users OU. If you did not use the User Setup wizards to create user accounts or if the user accounts are not in the Windows SBS Users OU for some reason, ActiveSync will not be installed when the users log on.

## Configuring ActiveSync

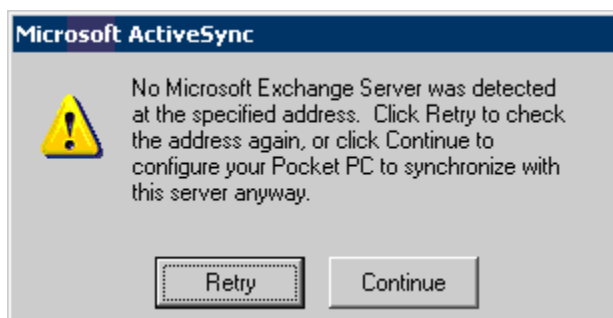
The following are some errors that may occur while configuring ActiveSync:

- The following error indicates a problem with SSL connectivity with the server.



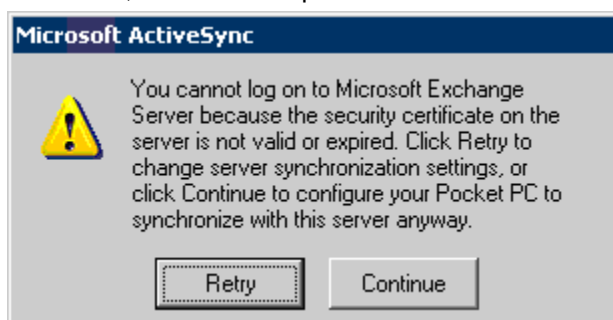
To troubleshoot this problem, see the section “Check for Certificate-Related Problems,” later in this document.

- When configuring the server, the following error indicates that the device cannot reach the server. The device has not reached the point of checking the certificate when this error occurs.



Check the firewall configuration and the IP connectivity.

- When configuring the server, the following error indicates that the device can reach the server, but there is a problem with the certificate.



Depending on the type of certificate you are using, perform one of the following:

- If you are using a third-party certificate, there is a problem with the server certificate. Try to access the server from a computer on the Internet by using the steps in the section "Check for Certificate-Related Problems," later in this document.
- If you are redirected to an SSL connection without a prompt for a certificate, ensure that the certificate is from a CA that is listed in the supported list for Windows Mobile. Windows Mobile devices do not support as many root CAs as Windows-based desktop computers. Your CA may be approved on Windows-based desktop computers but not on Windows Mobile devices.
- If you are prompted for a certificate and are not redirected to an SSL connection, verify that you have the right type of certificate (Web server certificate). You may also try reinstalling the certificate on the server by following the steps provided in the section "Option B: Configure a Third-Party Certificate," earlier in this document. If none of these steps work, work with the CA to troubleshoot the issue.

- If you are using a self-issued certificate, you may have not installed the certificate on the device. Click **Continue**, and then install the certificate after the wizard finishes. You cannot synchronize until the certificate is installed on the device.
- If you have already installed the certificate on the device, there is a problem with the certificate. Use the steps in the section “Check for Certificate-Related Problems,” later in this document, to do the following:
  - Ensure that the certificate on the server is installed correctly.
  - Ensure that the certificate on the device is installed correctly.Try to reinstall the certificate to the device. Make sure that you receive a message on the device that the certificate has been successfully added to the root store.

## Synchronizing the Mobile Device

### Some Users Cannot Synchronize

If some users cannot synchronize their devices, but others can, check the following:

- On the **Exchange Features** tab of the user account properties dialog, ensure that all mobile services are set to Enabled.
- Ensure that the device has Internet access by browsing to a Web site from the device.
- Some carriers require a SIM update to use data service. Check with your mobile operator for any such requirements.
- Ensure that the time and time zone is set properly on the device.
- Some devices cache the IP address of DNS names. If your server uses a dynamic IP address in conjunction with Internet services such as DynDNS.org, you may need to reset the device if your IP address changes.

### No User Can Synchronize

If no user can synchronize devices, do the following:

- Check for certificate-related problems.
- Check the Application event log.
- Check the firewall configuration.

### Check for Certificate-Related Problems

To check for certificate-related problems, perform the following:

- If you are using a third-party certificate, check the certificate on the server. To do this, browse to <http://YourPublicDNS.YourServer.com/exchange> on a computer (not

- connected to your LAN) that has Internet access, and ensure that you are redirected to an SSL connection without a prompt for a certificate.
- When you synchronize a device, click **Attention Required** on the ActiveSync screen. Review the error message to see if it refers to a certificate problem.
  - If you are using a self-issued certificate, ensure that it is installed properly on the device. To do this, browse to <http://YourPublicDNS.YourServer.com/exchange> on the device, and ensure that you are redirected to an SSL connection without a prompt for a certificate.
  - You may receive an error when you try to install a self signed certificate on the device using the instructions in this document. In that case, try to manually export the certificate from a client computer that is connected to the server, rather than use the files in the \\server\clientapps\sbscert directory. You can export the certificate from the Trusted Root Certificate Authorities\Certificates folder in the Certificates console and then open it by running certmgr.msc from the command prompt.

 **Note**

The certinst.exe tool is installed on many devices by the device manufacturers. You can use the tool to add a certificate by opening it on the device, as described in this document.

### **Check the Application Event Log**

Check the application event log on the server for any errors related to ActiveSync.

### **Check the Firewall Configuration**

To check the firewall configuration, check the following:

- Ensure that port 443 is open and that traffic to that port is being directed to the server.
- Ensure that the checks for useragent strings are disabled. Some firewalls have this enabled by default. Exchange ActiveSync does not send user-agent strings.
- Ensure that the timeout value is set high enough for SSL connections, typically 15 minutes.
- For more information, see Knowledge Base article 905013, "Enterprise firewall configuration for Exchange ActiveSync Direct Push Technology", at the [Microsoft Web site](http://go.microsoft.com/fwlink/?LinkId=75116) (<http://go.microsoft.com/fwlink/?LinkId=75116>).
- If you did not upgrade to Internet Security and Acceleration Server 2004 when you installed SP1 for Windows SBS, you need to add a registry key to use Direct Push with ISA Server 2000. For more information, see Knowledge Base article 304340, "The ISA Server response to client options requests is limited to a predefined set," at the [Microsoft Web site](http://go.microsoft.com/fwlink/?LinkId=75117) (<http://go.microsoft.com/fwlink/?LinkId=75117>). (This article

describes a different issue, however the registry change it specifies applies to Direct Push on ISA Server 2000).

If you are using ISA Server, you may need to implement a split DNS configuration to have a uniform experience both inside and outside the LAN. For more information, see "You Need to Create a Split DNS!" at the [ISAServer.org Web site](http://go.microsoft.com/fwlink/?LinkID=75118) (<http://go.microsoft.com/fwlink/?LinkID=75118>).

If you are using ISA Server 2004, and users can synchronize over the air but not from the cradle, you may be able to resolve some issues by configuring settings for ISA Server 2004.

#### ► To configure settings for ISA Server 2004

1. Open **ISA Server Management**.
2. In the console tree, expand **Configuration**, and then click **General**.
3. In the details pane, click **Define Firewall Client Settings**.
4. In the **Firewall Client Settings** dialog box, click the **Application Settings** tab, and then create the following three new application settings.

**Table 4. New Application Settings to Create in ISA Server**

Application	Key	Value
WCESCOMM	Disabled	0
WCESMGR	Disabled	0
REPIMGR	Disabled	0

## Accessing the Exchange Server ActiveSync Web Administration Tool

If you cannot access the Web site for the Exchange Server ActiveSync Web Administration tool, perform the following:

- On the server, open Internet Information Services (IIS) Manager, and then ensure that there is only one default Web site in IIS Manager.  
When the tool is installed, a duplicate default Web site is created if your original default Web site is bound to a specific IP address. To remove the duplicate default Web site, you can use either of the following two methods:
  - **Option A:**
    - a. Uninstall the tool.

- b. Change the IP address settings of the original default Web site to “All Unassigned”.
  - c. Install the tool again.
  - d. Revert the IP address settings of the default Web site back to the original values.
- **Option B:**
    - a. Create a new virtual directory in the original default Web site.
    - b. Export the settings from the duplicate default Web site.
    - c. Import the settings to the new virtual directory in the original default Web site.
    - d. Delete the duplicate default Web site created by the tool.
  - Check the settings of the ExAdmin virtual directory to ensure that SSL is not required.
- ▶ **To check the settings of the ExAdmin virtual directory**
1. In **Internet Information Services (IIS) Manager**, expand **Default Web Site**, right-click **ExAdmin**, and then click **Properties**.
  2. On the **Directory Security** tab, in the **Secure Communication** section, click **Edit**.
  3. Ensure that the **Require secure channel (SSL)** check box is cleared.
- Ensure that the MobileAdmin virtual directory is running in the Exchange Application Pool.
- ▶ **To ensure that the MobileAdmin virtual director is running in the Exchange Application pool**
1. In **Internet Information Services (IIS) Manager**, expand **Default Web Site**, right-click **MobileAdmin**, and then click **Properties**.
  2. On the **Virtual Directory** tab, in **Application Pool**, select **ExchangeApplicationPool**.

## Deploying Certificates

### Obtaining a Certificate

If you are having difficulty in obtaining a third-party certificate, perform the following:

- Ensure that your organization’s Dun & Bradstreet (D&B) or other commercial directory information is up-to-date before you apply for a certificate. You can check your D&B information at the [Dun & Bradstreet Web site](http://go.microsoft.com/fwlink/?LinkId=75119) (<http://go.microsoft.com/fwlink/?LinkId=75119>).

- If you have a trade name, ensure that it is documented with your D&B information. Be prepared to provide proof of the trade name. Examples of items that are commonly accepted by root CAs for issuing a certificate include Articles of Incorporation, Business License, and D&B details.
  - Depending on how you applied for the certificate, prepare as follows:
    - Using a trade or DBA (Doing Business As) name: Provide a trading license, a copy of a utility bill, a bank statement, or else check with the trade name and the company name.
    - Using a personal name: Provide a copy of your driver's license or passport.
- These requirements vary across CAs, but all CAs verify your identity before they issue a certificate. The information provided to the CA must exactly match the information you entered in the original certificate signing request. For example, if your articles of incorporation show an address that is different than the address you provide in the certificate signing request, the CA will not issue the certificate.

### **Creating a Certificate Signing Request**

Perform the following checks when you are creating a certificate signing request:

- Ensure that there is no certificate on the server. If there is, you must remove it before you create the new certificate signing request.
- If you have installed a certificate from a CA on the server, ensure that the certificate signing request is not sent immediately to an online authority. This will not create a third-party certificate.

### **Installing a Self-Issued Certificate**

Following are some problems that may occur while installing a self-issued certificate on a mobile device:

- Running the certificate after copying it to the device does not install the certificate (add to the root store) successfully.

You may need to use SpAddCert.exe to install the certificate to the root store. For instructions, see the section "Option A: Configure a Self-Issued Certificate," earlier in this document.

## **Configuring the Device**

### **Direct Push Messages**

If messages are not being received immediately, do the following:

- Ensure that the device is running Windows Mobile 5.0 with MSFP. Direct Push technology is available only on devices that have MSFP installed. You can check whether MSFP is installed on your device by confirming that the Windows Mobile build number is 14847 or higher.
- Ensure that the device is not cradled to a computer or connected to a wireless LAN. Direct Push works only with over-the-air synchronization.

## Device Policy

If new policies pushed to the device are not applied, ensure that the device has synchronized since the policy was updated. Policies are applied during the ActiveSync cycle, and new policies are not applied until the next synchronization.

When the policy is applied to a device, the user is prompted and is given the opportunity to bring their device into compliance with the new policy—for example, by setting up a password.

## Synchronizing

If a user-initiated synchronization fails on the device:

- Check whether you can access Outlook Web Access (OWA) and Outlook Mobile Access (OMA). This verifies server connectivity, and it ensures that no certificate-related errors exist.
- Check for wireless Internet connectivity from the device. If the device does not have wireless Internet connectivity, contact the mobile operator.
- Check the IIS logs on the server. Look for entries coming from the mobile device, and see if there are any error messages that might help determine the problem.
- Enable logging on the device, and check the logs for entries that give more information about the problem. To enable logging on the device, perform the following steps:
  - **If you have a Windows Mobile Standard device:**
    - a. Click **Start**, click **Programs**, and then click **ActiveSync**.
    - b. Click **Menu**, and then click **Configure Server**.
    - c. Click **Next**, and then click **Advanced**.
  - **If you have a Windows Mobile Classic or Professional device:**
    - a. Click **Start**, and then click **ActiveSync**.
    - b. Click **Menu**, click **Configure Server**, click **Next**, click **Next** again, click **Menu**, and then click **Advanced**.

- c. Change the logging level to **Verbose**. Logs are stored on the device in the **Windows\ActiveSync** folder.
- d. Click **Next**, and then click **Finish**.

## Related Links

- For more information about Windows SBS, see "Windows Small Business Server 2003" at the [Microsoft Web site](http://go.microsoft.com/fwlink/?LinkId=62476) (<http://go.microsoft.com/fwlink/?LinkId=62476>).