



Deploying Windows Mobile 5.0 with Windows Small Business Server 2003

Version 1.0
Published February, 2006

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 example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, email address, logo, person, place or event is intended or should be inferred.

© 2006 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, ActiveSync, Exchange Server, Office, Outlook Mobile, PowerPoint, Windows, Windows Media, Windows Mobile, Windows Server System, and Windows Small Business Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

INTRODUCTION	1
WINDOWS MOBILE 5.0.....	1
MESSAGING AND SECURITY FEATURE PACK.....	1
DEVICE DEPLOYMENT	3
CHECKLIST OF REQUIREMENTS	3
STEP 1 - INSTALLING ACTIVESYNC 4.1	4
Option A - Manual Installation	5
Option B - Automatic Installation using Group Policy	5
STEP 2 - ENABLING MOBILE SERVICES FOR USERS	11
STEP 3 - CONFIGURING THE FIREWALL AND WEB SERVICES	12
STEP 4 - DEPLOYING AN SSL CERTIFICATE.....	13
Choosing the Type of Certificate.....	13
Configuring the Certificate.....	15
Option A - Configuring Self-Signed Certificates.....	15
Option B - Configuring Third-Party Certificates	16
STEP 5 - CONFIGURING WINDOWS SBS FOR MSFP.....	20
Installing Exchange Server 2003 Service Pack 2.....	21
Installing Exchange Server ActiveSync Web Administration Tool.....	21
Enabling Direct Push.....	21
STEP 6 - CONFIGURING DEVICE SYNCHRONIZATION	22
STEP 7 - TESTING THE DEPLOYMENT.....	24
Testing Over-the-Air Synchronization.....	24
Testing Direct Push.....	24
REMOTE MANAGEMENT	26
PERFORMING REMOTE DEVICE WIPE	26
IMPLEMENTING DEVICE SECURITY POLICY	27
TROUBLESHOOTING	28
INSTALLING ACTIVESYNC ON CLIENT COMPUTERS	28
INSTALLING EXCHANGE SERVER 2003 SP2	28
CONFIGURING ACTIVESYNC	29
SYNCHRONIZING THE MOBILE DEVICE.....	30
Some Users are Not Able to Synchronize	30
No User is Able to Synchronize	31
Check for Certificate-related Problems.....	31
Check the Application Event Log	31
Check the Firewall Configuration.....	32
ACCESSING EXCHANGE SERVER ACTIVESYNC WEB ADMINISTRATION	32
DEPLOYING SSL CERTIFICATES	33
Obtaining a Certificate.....	33
Creating a Certificate Signing Request	34
Installing a Self-Signed Certificate.....	34
CONFIGURING DEVICES.....	35
Direct Push Messages	35
Device Policy.....	35
Synchronizing.....	35

Introduction

This white paper provides step-by-step instructions for deploying Microsoft® Windows Mobile® 5.0 powered devices in an IT infrastructure that is based on the Microsoft® Windows® Small Business Server 2003 (Windows SBS) server software.¹ It is assumed that the readers have a basic understanding of Windows Mobile and experience in deploying and managing Windows SBS. This white paper is ideal for users who already have a Windows SBS-based infrastructure deployed and want to add Windows Mobile devices to that infrastructure.

Windows Mobile 5.0

Windows Mobile 5.0 is the successor to the Windows Mobile® 2003 operating system that provides new features and tools for improved productivity, connectivity, and security. Some of these new features in Windows Mobile 5.0 include:

- Updated versions of Microsoft Office mobile applications, including Microsoft PowerPoint®.
- Enhanced Microsoft Outlook Mobile® messaging, including photo support.
- Improved navigation and speed.
- Better multimedia features such as support for more ringtones, high-resolution pictures, and Microsoft Windows Media® Player 10.
- Easier and faster synchronization.

Messaging and Security Feature Pack

The improved messaging and security features in Windows Mobile 5.0 are available as part of the Messaging and Security Feature Pack (MSFP) add-on. New features introduced through MSFP include:

- **Direct Push technology:** Items received on the Exchange server, such as new e-mail messages, calendar changes, contact changes, or task updates are immediately sent to a device running Windows Mobile 5.0 with MSFP.²
- **Wireless support for contact information:** This feature enables over-the-air lookup of global address list (GAL) information stored on Exchange Server.
- **Remotely enforced security policy:** IT administrators 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.

¹ Information in this document can also be used to deploy Windows Mobile 5.0 powered devices in a Windows Small Business Server 2003 R2 (Windows SBS 2003 R2)-based infrastructure.

² Direct Push technology uses an IP-based Internet connection and does not use SMS (Short Message Service Text Messaging), which is used by the previous AUTD (Always Up To Date) synchronization process.

- **Remote device wipe:** This feature enables administrators to remotely reset a device over the Internet.

To take advantage of the new features available with Windows Mobile 5.0 with MSFP, Exchange Server 2003 Service Pack 2 (SP2) must be installed on the Windows SBS 2003 server.³

Earlier releases of Windows Mobile 5.0 powered devices do not have MSFP preinstalled. Most mobile operators will be providing software upgrades for these devices. For information about the availability of MSFP or whether MSFP is already installed on your device, contact your mobile operator or device manufacturer. You can also confirm the installation of MSFP by checking the Windows Mobile 5.0 OS build number. On the device, select **Start/Settings/About**. If the build number is 14847 or greater, the device has MSFP installed.

³ SBS 2003 R2 will have Exchange Server 2003 Service Pack 2 preinstalled.

Device Deployment

The deployment process outlined in this white paper can be broken down into the following seven steps:

- Step 1 - Installing ActiveSync® 4.1
- Step 2 - Enabling mobile services for users
- Step 3 - Configuring the firewall and Web services
- Step 4 - Deploying an SSL certificate
- Step 5 - Configuring Windows SBS 2003 for MSFP
- Step 6 - Configuring device synchronization
- Step 7 - Testing the deployment

Note: Step 5 needs to be performed only if you are deploying devices with Windows Mobile 5.0 and MSFP. If you are not (or do not plan on) deploying devices with MSFP, you can skip step 5.

Checklist of Requirements

This section lists the hardware and software requirements for implementing the guidance provided in this white paper. The following table lists the requirements that must be present.

Requirement	Description
Windows Mobile 5.0 powered device	Mobile device running Windows Mobile 5.0.
Wireless data connectivity	The mobile device must have wireless data connectivity provided through a mobile operator, such as GPRS, for accessing the Internet.
Server running Windows SBS 2003	A computer running Windows SBS 2003 or Windows SBS 2003 R2. It is assumed that Exchange Server 2003 is configured and running properly on the server.
ActiveSync 4.1	ActiveSync 4.1 can be downloaded from the following URL: http://www.microsoft.com/downloads/details.aspx?FamilyID=4c254e3f-79d5-4012-8793-d2d180a42dfa&DisplayLang=en
Third-party or self-signed SSL certificate	For guidance on choosing between and obtaining a third-party SSL certificate or a self-signed SSL certificate, refer to the “Deploying an SSL certificate” section in this white paper. While installing a self-signed certificate, you may require the utility smartphoneaddcert.exe, which can be downloaded from the following URL: http://support.microsoft.com/?id=841060

Table 1. Requirements for Deploying the Guidance in This White Paper

In addition, if you are planning to deploy devices running Windows Mobile 5.0 with MSFP, the following additional software is required.

Requirement	Description
Exchange Server 2003 SP2	Exchange Server 2003 SP2 can be downloaded from the following URL: http://www.microsoft.com/technet/prodtechnol/exchange/downloads/2003/sp2/download.mspx If your server is running Windows SBS 2003 R2, you do not require this software update because Windows SBS 2003 R2 has Exchange Server 2003 SP2 preinstalled.
Exchange Server ActiveSync Web Administration tool	The Exchange Server ActiveSync Web Administration tool can be downloaded from the following URL: http://www.microsoft.com/downloads/details.aspx?familyid=e6851d23-d145-4dbf-a2cc-e0b4c6301453&displaylang=en

Table 2. Additional Requirements for Deploying Windows Mobile 5.0 with MSFP

Step 1 - Installing ActiveSync 4.1

Mobile devices need to be connected to a client computer for copying files, installing applications, or synchronizing data directly with the computer. Windows Mobile 5.0 powered devices require ActiveSync 4.1 to be installed on the client computer to establish connections with the computer.

There are two methods of installing ActiveSync on the client computers in an environment. These methods are:

- **Manual Installation:** Involves manually copying and installing ActiveSync on the computer.
- **Automatic Installation using Group Policy:** Involves configuring Windows SBS to automatically install ActiveSync on the client computers that are connected to the server.

The following sections provide the steps for implementing both of these methods.

If you have not already downloaded the ActiveSync 4.1 setup, download it from the following URL:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=4c254e3f-79d5-4012-8793-d2d180a42dfa&DisplayLang=en>

Note: Before installing ActiveSync 4.1 on any computer, ensure that computer meets the minimum system requirements for ActiveSync 4.1 at <http://www.microsoft.com/windowsmobile/downloads/as-sysreq41.mspx>.

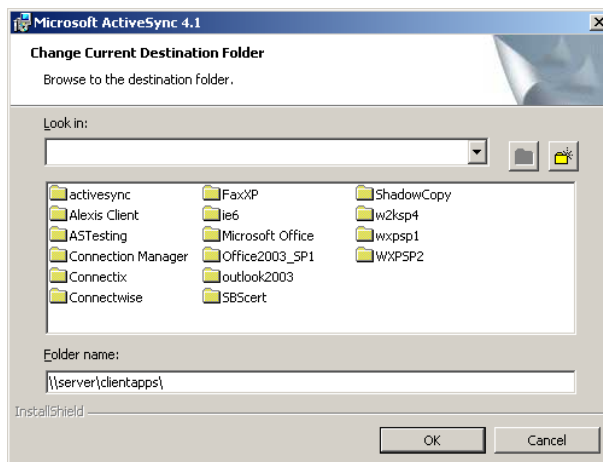
Option A - Manual Installation

To manually install ActiveSync 4.1 on the client computers, copy the downloaded ActiveSync setup file on each computer that will connect to a Windows Mobile-based device. Run and install the ActiveSync 4.1 Setup program.

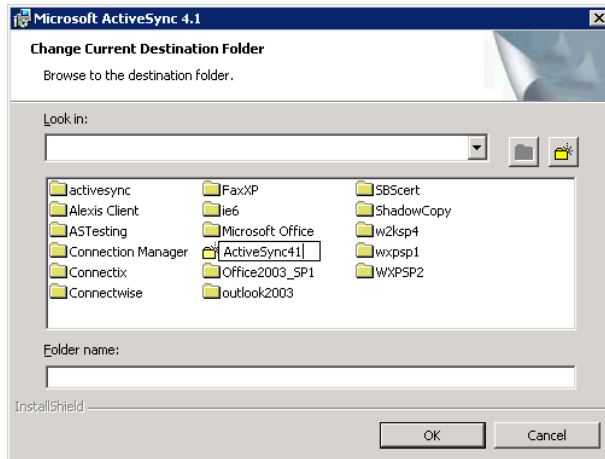
Option B - Automatic Installation using Group Policy

To install ActiveSync automatically using Group Policy, perform the following steps:

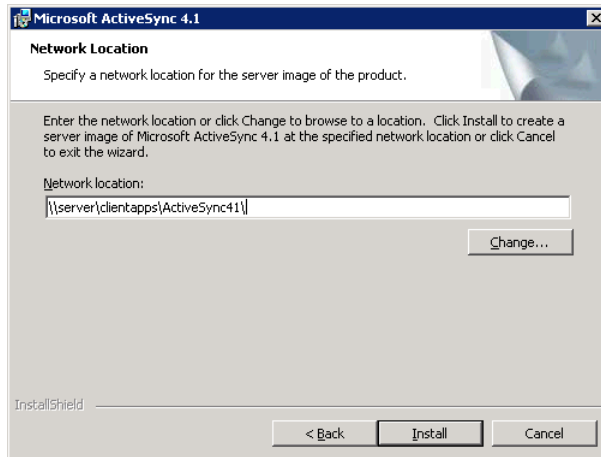
1. Log on to the Windows SBS server.
2. Start the Microsoft ActiveSync 4.1 wizard by performing the following steps:
 - a. Open the command prompt.
 - b. Change the current directory to the folder where the ActiveSync setup is saved.
 - c. Type **setup.exe /V /a**, and press ENTER.
The wizard starts after a short pause.
3. Complete the wizard using the following steps:
 - a. On the **Welcome** page, click **Next**.
 - b. On the **Network Location** page, click **Change**, and perform the following steps:
 - i. Browse to the **ClientApps** share on the Windows SBS server (\localhost\clientapps).



- ii. Create a new folder in the **ClientApps** share by clicking the new folder button and name the new folder "ActiveSync41".



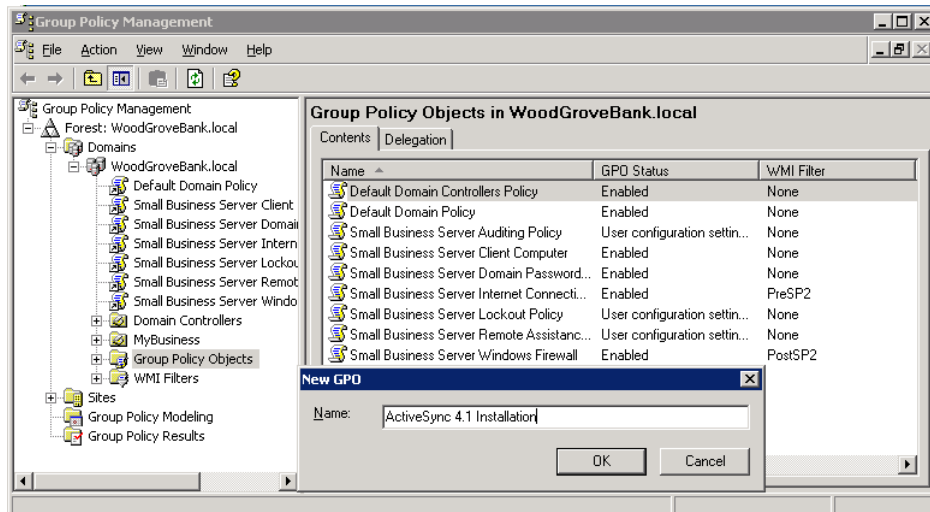
iii. Double click the newly created ActiveSync41 folder and click **OK**.



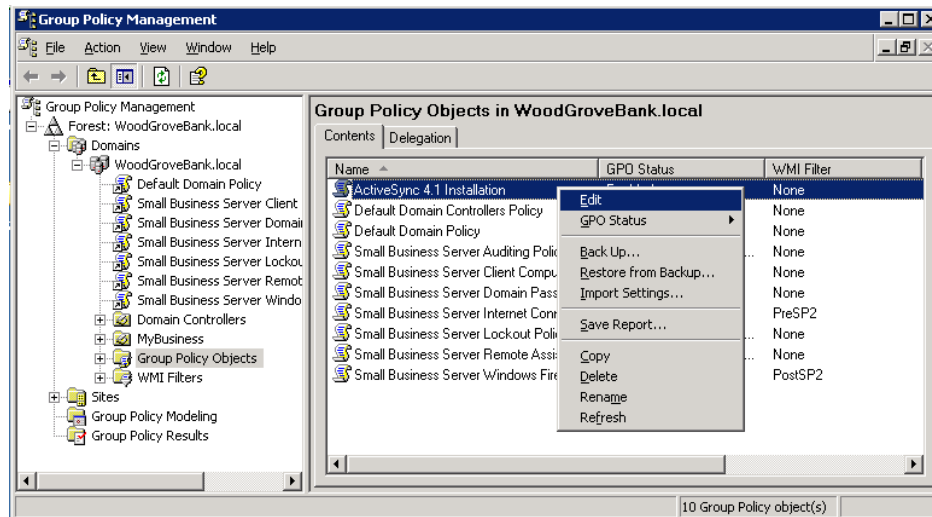
iv. Click the **Install** button.

c. Click the **Finish** button when the installation completes.

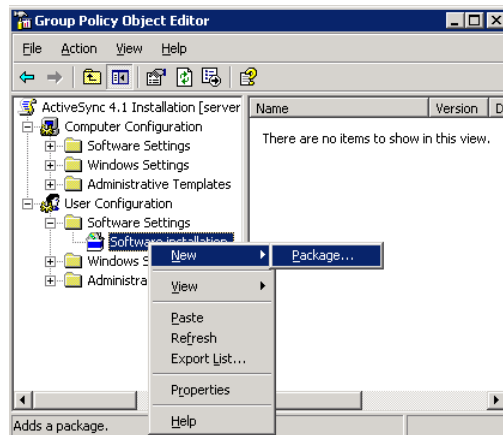
4. Open **Group Policy Management** from **Administrative Tools** and expand *ForestName*, expand **Domains**, and then expand *DomainName*.
5. Right-click **Group Policy Objects** and click **New**.
6. In the **New GPO** dialog box, type **ActiveSync 4.1 Installation** and click **OK**.



7. On the details pane, right-click the newly created Group Policy Object (GPO) (that is, ActiveSync 4.1 Installation) and click **Edit**.

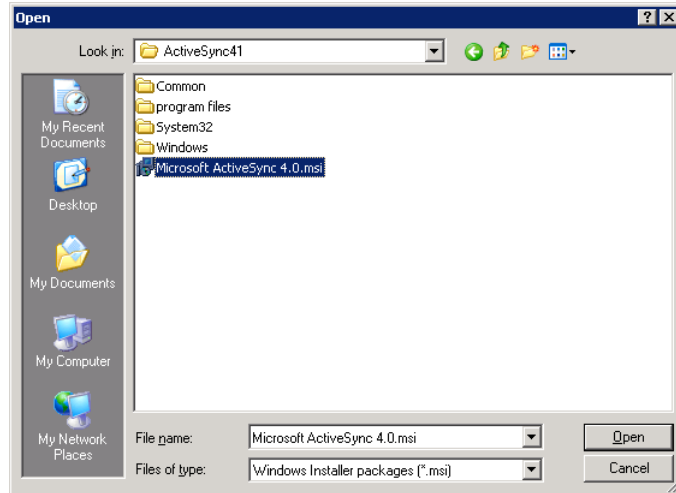


8. In Group Policy Object Editor, expand **User Configuration**, expand **Software Settings**, right-click **Software Installation**, point to **New**, and click **Package**.

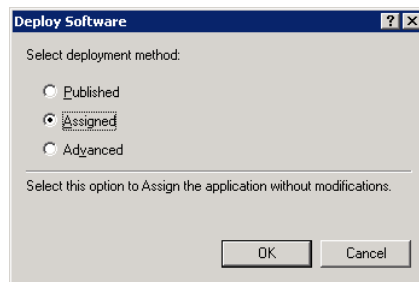


9. In the **Open** dialog box, browse to the ActiveSync41 folder created earlier using a Universal Naming Convention (UNC) path (\\localhost\ClientApps\activesync41\) and double-click the Microsoft ActiveSync 4.0.msi file.

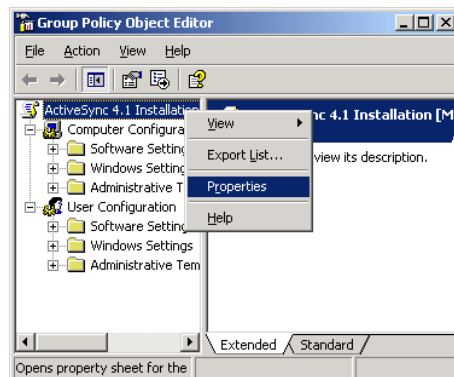
Note: Although the name of the setup file includes “4.0”, the setup installs ActiveSync 4.1.



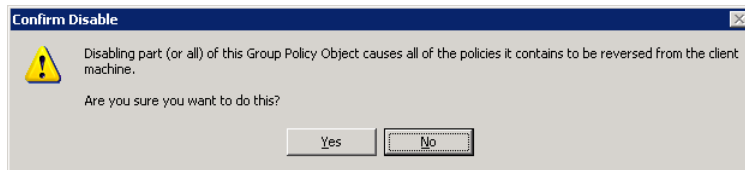
10. On the **Deploy Software** dialog box, click **Assigned** and click **OK**.



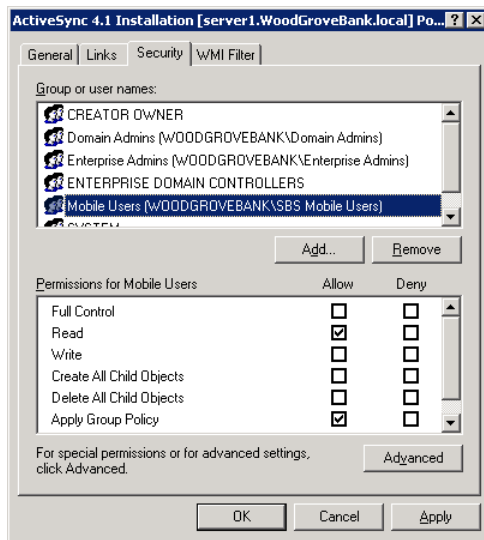
11. In **Group Policy Object Editor**, right-click the newly created GPO name (top node of the console tree) and click **Properties**.



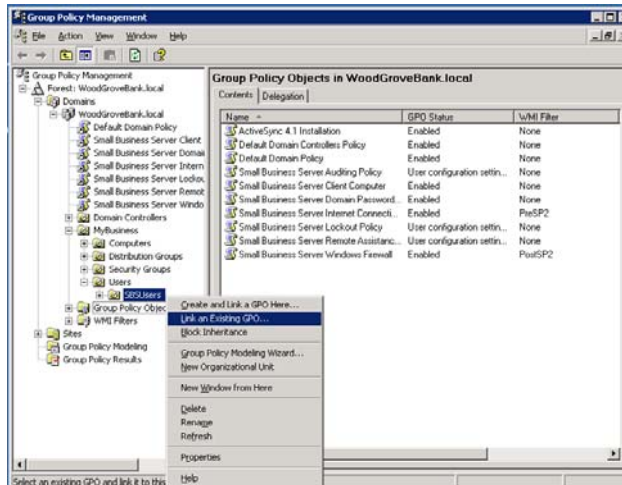
- On the **General** tab, select **Disable computer Configuration settings** and click **Yes** on the **Confirm Disable** dialog box.



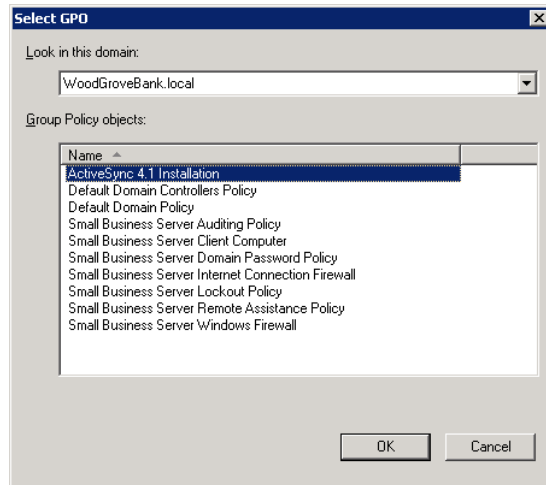
- On the **Security** tab, remove **Authenticated Users** from the list and add **Mobile Users** to the list. Make sure that the **Read** and **Apply Group Policy** permissions are set to **Allow** for **Mobile Users** and then click **OK**.



- Close **Group Policy Object Editor**.
- In **Group Policy Management**, expand **My Business** and then expand **Users**. Right-click **SBS Users** and click **Link an Existing GPO**.



16. In the list of GPOs, click the **ActiveSync 4.1 Installation** GPO and click **OK**.



After these steps are complete, ActiveSync 4.1 will automatically get installed on any computer to which a member of the Mobile Users group logs on. For ActiveSync 4.1 to install successfully, the logged on user must have local administrative rights on the computer.

Note: By default, the Mobile Users group has Virtual Private Network (VPN) access to the Small Business Server. Therefore, if you add any users to this group so that ActiveSync gets installed on their computers, these users will also gain VPN access to the Small Business Server network.

It is important to establish a practice of NOT selecting to install ActiveSync when running the Set Up Computer Wizard. The Set Up Computer Wizard installs an older version of ActiveSync that is bundled with Windows SBS 2003 and does not install version 4.1, which is required for Windows Mobile 5.0 devices.

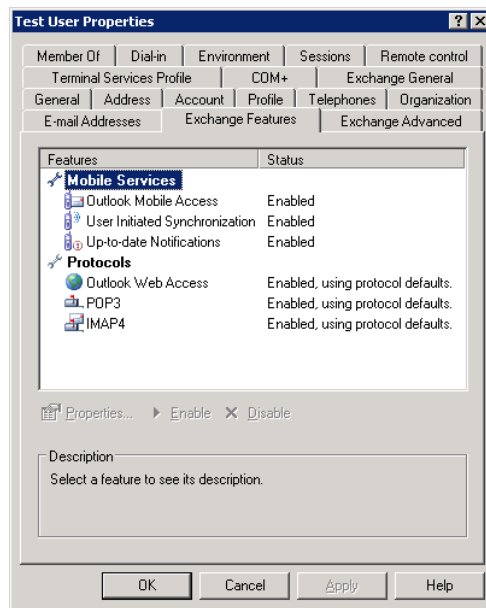
Step 2 - Enabling Mobile Services for Users

Before configuring a mobile device for a user, mobile services must be enabled 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, perform the following steps:

1. Open the **Server Management** console, click the **Users** link, 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 - Configuring the Firewall and Web Services

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

The steps provided in this section automatically configure the following types of firewalls:

- Microsoft Internet Security and Acceleration (ISA) Server included in Windows SBS Premium.
- Built-in Routing and Remote Access firewall in Windows SBS.
- UPnP™ hardware firewall.

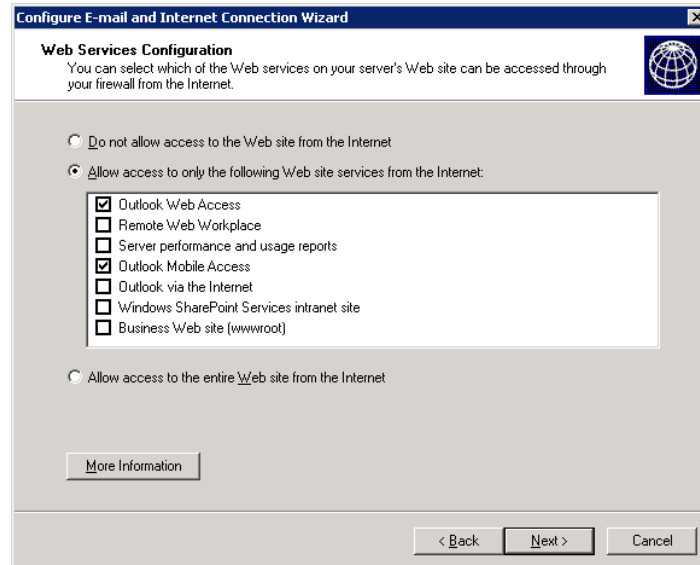
If you are using a firewall other than these, you will need to manually configure your firewall to direct incoming traffic on port 443 to the Windows SBS server.

Perform the following steps to configure the firewall and Web services:

1. Open the **Server Management** console and click the **Internet and E-mail** link.
2. Click the **Connect to the Internet** link 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 click **Next**.
5. On the **Firewall** page, click **Enable Firewall** and click **Next**.
6. On the **Services Configuration** page, select the services that are in use on your network and click **Next**.

7. On the **Web Services Configuration** page, select **Outlook Mobile Access** and any other services that need to be enabled. Click **Next**.

Selecting **Outlook Mobile Access** enables over-the-air sync with Windows Mobile devices. Click **Next**.



8. On the **Web Server Certificate** page, click **Do not change current Web server certificate**, and click **Next**.
9. On the **Internet E-mail** page, click **Do not change Internet e-mail configuration** and 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, you need to ensure that incoming traffic on port 443 is directed to the Windows SBS server.

Step 4 - Deploying an SSL Certificate

This section provides guidance on choosing and configuring a certificate. A certificate is required to securely synchronize data using the Secure Sockets Layer (SSL) protocol. It is important to use SSL to help secure communications between the mobile device and the server.

Choosing the Type of Certificate

The following two options are available for certificate installation for Windows Mobile 5.0 devices:

- **Third-party certificate:** A third-party certificate that has a root certificate store present on the Windows Mobile powered device can be purchased from a trusted root CA and installed on the server.
- **Self-signed certificate:** You can install a self-signed certificate generated by Windows SBS on each device.

Some Windows Mobile 5.0 Smartphone devices may not allow installation of self-signed certificates on the device.⁴ If your Smartphone does not support installation of self-signed certificates, you will need to purchase a third-party certificate to connect to the Exchange server. However, for Pocket PC devices, you can use either type of certificate.

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

Choice	Advantages	Disadvantages
Third-party certificate	<ul style="list-style-type: none"> • No additional configuration is required on the Windows Mobile device. • Can be used with all Smartphone and Pocket PC devices. • Provides additional benefits with other Windows SBS features such as OWA, RWW, and RPC over HTTP. 	<ul style="list-style-type: none"> • Must be purchased and may require a recurring fee for renewals. Can cost around \$100 to \$200 annually. • Requires independent verification of your company information before issuance. Cannot be installed immediately.
Self-signed certificate generated by Windows SBS	<ul style="list-style-type: none"> • Can be easily generated by Windows SBS through CEICW. • No additional cost. • Fewer configurations are required in Windows SBS. 	<ul style="list-style-type: none"> • Requires additional configuration on the device. The certificate must be exported to and installed on each device. • Does not work on many Smartphone devices (check with mobile operator or device manufacturer).

Table 3. Advantages and Disadvantages of Different Types of Certificates

Choose the certificate type that is best suited for your environment. For example, if you are deploying Smartphones that do not support self-signed certificates, choose a third-party certificate. If cost is a concern for you and you are only deploying Pocket PC devices, choose a self-signed certificate.

Keep in mind that a third-party certificate offers additional benefits to users in a Windows SBS-based environment, such as the ability to use Outlook over the Internet from any computer without having to install a certificate and without being prompted with a certificate error when accessing Outlook Web Access, Remote Web Workplace, Windows SharePoint services, or other Web sites hosted on the Windows SBS server.

⁴ Device security policies related to certificate installation are configured by the device manufacturer or the mobile operator. Contact the device manufacturer or your mobile operator to check whether root certificate access is allowed on your Windows Mobile Smartphone devices.

Configuring the Certificate

A certificate must be installed on the Windows SBS server or on the mobile device for Exchange ActiveSync synchronization to work. Based on the type of certificate you select, perform the steps provided in either one of the following two sections.

Option A - Configuring Self-Signed Certificates

This section provides guidance on copying and installing the self-signed certificates created by Windows SBS onto the mobile device. For multiple mobile devices, you will need to install the certificate on each device. Because the certificate would already be installed on the Windows SBS server, no additional configuration needs to be done on the server.

Copying the Certificate File to the Device

Perform the following steps to copy the certificate file to the mobile device:

1. Log on to a client computer that has ActiveSync 4.1 installed.
2. Connect the Windows Mobile device to the computer.
You do not need to establish a partnership; you can simply connect in guest mode.
3. Open **Windows Explorer** and navigate to
\\WindowsSBSServerName\ClientApps\SBScert.
4. Right-click the certificate (.cer) file in the SBScert folder and click **Copy**.

Note: If your Windows SBS Server is running ISA Server, there may be more than one certificate in the folder. Select the one named ISACert.cer.

5. Navigate to **Mobile Device** under **My Computer**.
By default, the contents of the **My Documents** folder on the device are displayed.
6. Right-click the content area and click **Paste** to copy the certificate file to the device.

Installing the Certificate on the Device

Perform the following steps to install the certificate:

1. On the Windows Mobile device, open **File Explorer** (for Pocket PCs) or **File Manager** (for Smartphones).

Note: File Explorer is present at **Start\Programs** on Pocket PCs.
File Manager is present at **Start\More** on Smartphones.

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

If you receive an error and the certificate is not installed, you will need to use an external utility to install the certificate on the device. To install the certificate using this external utility, perform the following steps:

- a. On the client computer, download `smartphoneaddcert.exe` from the following URL:

<http://support.microsoft.com/?id=841060>

If a signed version of `smartphoneaddcert` by your mobile operator is available from this link, download the signed version.

Note: Although the Knowledge Base article, “841060,” at the given link refers to Windows Mobile 2003 and Windows Mobile 2002, the utility will also work with Windows Mobile 5.0. In addition, even though the file is named “`smartphoneaddcert`,” it also works with Pocket PCs.

- b. Run `smartphoneaddcert.exe` and extract `SpAddCert.exe`.
- c. Copy `SpAddCert.exe` to the device.
- d. On the device, create a folder named “Storage” on the root of the device and copy the certificate file into the Storage folder.
- e. On the device, run `SpAddCert.exe`. By default, the certificates in the Storage folder of the device are listed. Select the certificate you just copied and click **OK** on all message boxes that get displayed, to install the certificate.

If you are using a Smartphone and the self-signed certificate still fails to install, the device manufacturer or mobile operator must have disabled access to the root certificates. Check with the device manufacturer or your mobile operator to see if they provide a separate installation utility. Otherwise, you will have to use a trusted third-party certificate by following the instructions provided in the following section.

Option B - Configuring Third-Party Certificates

This section provides guidance on purchasing and installing a third-party certificate on the Windows SBS server.

Note: Some CAs provide their own instructions for installing SSL certificates on the server. Depending on the type of certificate, these instructions may be different than the steps provided in this section. Please follow the installation instructions provided by the CA, if they are available, instead of instructions in this white paper.

Purchasing a Third-Party Certificate

You should only use third-party certificates from a CA that has a root certificate present on the root store of Windows Mobile powered devices. For a listing of CAs offering Windows Mobile-compatible certificates, refer to the following URL:

<http://go.microsoft.com/fwlink/?LinkId=61499>

For purchasing a certificate from a CA, you will need to generate a certificate signing request on the Windows SBS server. To do this, perform the following steps:

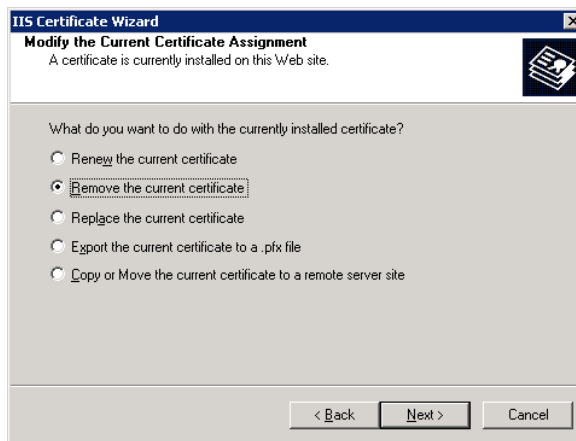
1. Open **Internet Information Services (IIS) Manager** from **Administrative Tools**.
2. Expand *WindowsSBSServerName*, expand **Web Sites**, and right-click **Default Web Site** and click **Properties**.

3. On the **Directory Security** tab, click the **Server Certificate** button to start the IIS Certificate Wizard.
4. On the welcome page, click **Next**.

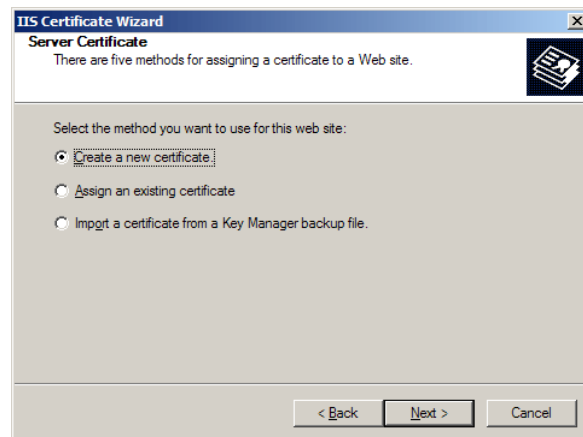
The **Modify the Current Certificate Assignment** page is displayed if you have an existing certificate installed on the server. If the page is displayed, perform the following steps:

- a. Click **Remove the current certificate** and click **Next**.

Note: The existing certificate could have been created while running the Configure E-Mail and Internet Connection Wizard.

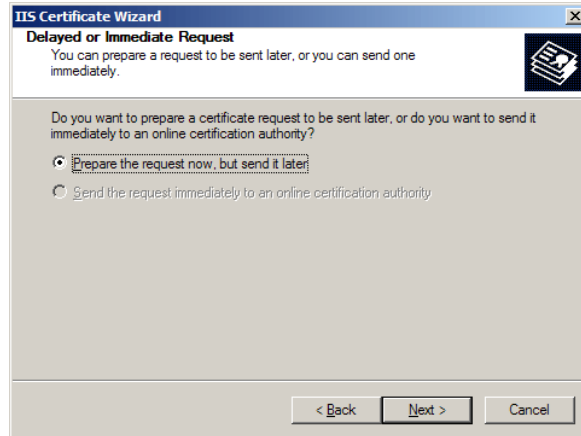


- b. Click **Next** on the next two pages and then click **Finish** to complete the wizard and remove the certificate.
- c. Start the wizard again by clicking the **Server Certificate** button on the **Directory Security** tab. On the welcome page, click **Next**.
5. On the **Server Certificate** page,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

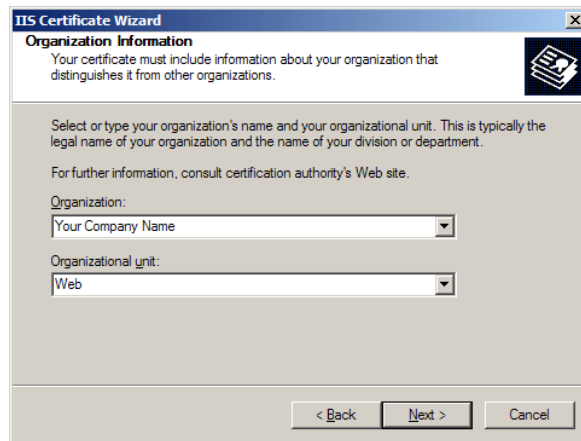


6. On the **Delayed or Immediate Request** page, click **Prepare the request now, but send it later** and click **Next**.

Note: If you have a CA installed on the Windows SBS server, the second option will not be disabled.



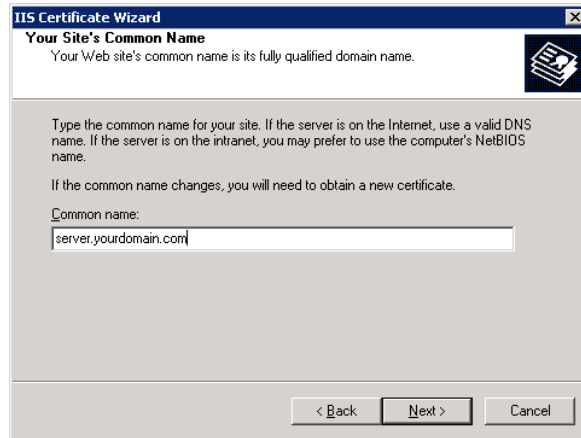
7. On the **Name and Security Settings** page, type the name of the company and click **Next**.
8. On the **Organization Information** page, type the name of the company and the name of the department, which may be the same.



Note: It is important to type the proper company name because the CA will use this name to verify the company information before issuing a certificate. After you submit the request, the CA will verify 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 ensure that your Dun & Bradstreet (D&B) or other commercial directory information is up to date before submitting the certificate signing request because many CAs use that information for verification.

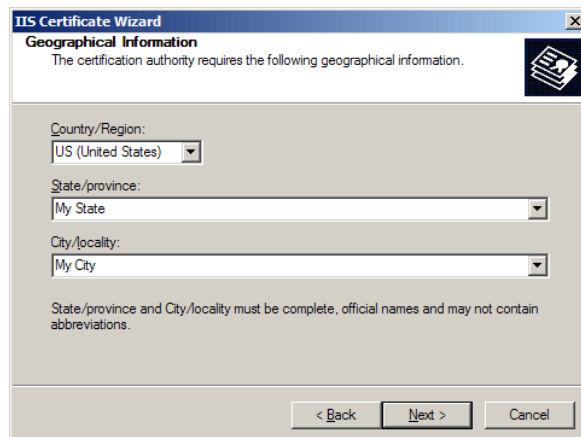
Get the exact verification requirements from the CA you have chosen.

9. 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 provided incorrectly.



The screenshot shows the 'IIS Certificate Wizard' window with the 'Your Site's Common Name' page. The title bar reads 'IIS Certificate Wizard'. Below the title bar, the page title is 'Your Site's Common Name' and the subtitle is 'Your Web site's common name is its fully qualified domain name.' There is a small icon of a certificate on the right. The main text says: '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. If the common name changes, you will need to obtain a new certificate.' Below this is a text box labeled 'Common name:' containing the text 'server.yourdomain.com'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

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



The screenshot shows the 'IIS Certificate Wizard' window with the 'Geographical Information' page. The title bar reads 'IIS Certificate Wizard'. Below the title bar, the page title is 'Geographical Information' and the subtitle is 'The certification authority requires the following geographical information.' There is a small icon of a certificate on the right. The main text says: 'Country/Region: US (United States)'. Below this is a dropdown menu for 'State/province:' containing the text 'My State'. Below that is a dropdown menu for 'City/locality:' containing the text 'My City'. At the bottom, there is a note: 'State/province and City/locality must be complete, official names and may not contain abbreviations.' At the bottom of the window, there are three buttons: '< Back', 'Next >', and 'Cancel'.

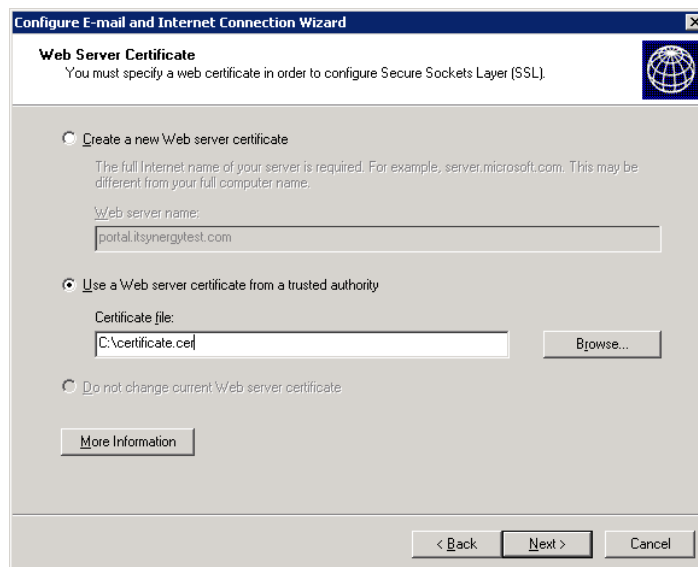
11. Provide a path and file name for saving the request. Click **Next** twice and then click **Finish**.
12. Open the request file you just created using Notepad and copy all of the text in the file, including dashes, into the application form to be sent to the CA.

Note: Be careful not to change or modify any of the certificate settings on the website after creating the certificate request. The steps in the section will not work if the pending request is cancelled for any reason. If you cancel the pending request, you will have to apply with the CA to have the certificate reissued using a new request file.

Installing the Certificate on the Server

After receiving the certificate (.cer) file from the CA, install the certificate on the Windows SBS server. To do this, perform the following steps on the Windows SBS server:

1. Open the **Server Management** console.
2. Click the **Internet and E-mail** link.
3. Click the **Connect to the Internet** link to start the Configure E-mail and Internet Connection Wizard.
4. On the welcome page, click **Next**
5. On the **Connection Type** page, click **Do not change connection type** and click **Next**.
6. On the **Firewall** page, click **Do not change firewall configuration** and 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 finally click **Next**.



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

Step 5 - Configuring Windows SBS for MSFP

The tasks listed in this section need to be performed only if you are deploying Windows Mobile powered devices running Windows Mobile 5.0 with MSFP. For more information on MSFP, refer to the “Messaging and Security Feature Pack” section earlier in this white paper.

Configuring the Windows SBS server for MSFP involves the following tasks:

1. Installing Exchange Server 2003 SP2.

2. Installing Exchange Server ActiveSync Web Administration Tool.
3. Enabling Direct Push.

Installing Exchange Server 2003 Service Pack 2

As discussed earlier, you must have Exchange Server 2003 SP2 already installed on your Windows SBS server⁵ to take advantage of the new features of Windows Mobile 5.0 with MSFP. If it is not already installed, install it by downloading from the following URL:

<http://www.microsoft.com/technet/prodtechnol/exchange/downloads/2003/sp2/download.mspx>

Installing Exchange Server ActiveSync Web Administration Tool

To take advantage of the remote device wipe feature of MSFP, you need to install the Exchange Server ActiveSync Web Administration Tool. Note that before installing the tool, Exchange Server 2003 SP2 must already be installed on the Windows SBS server.

The tool is available for download at the following URL:

<http://www.microsoft.com/downloads/details.aspx?familyid=e6851d23-d145-4dbf-a2cc-e0b4c6301453&displaylang=en>

After installing the Exchange Server ActiveSync Web Administration tool, ensure that the installation was successful by opening Internet Explorer on the server and browsing to <http://localhost/mobileadmin> and logging on to the console by providing domain administrator credentials.

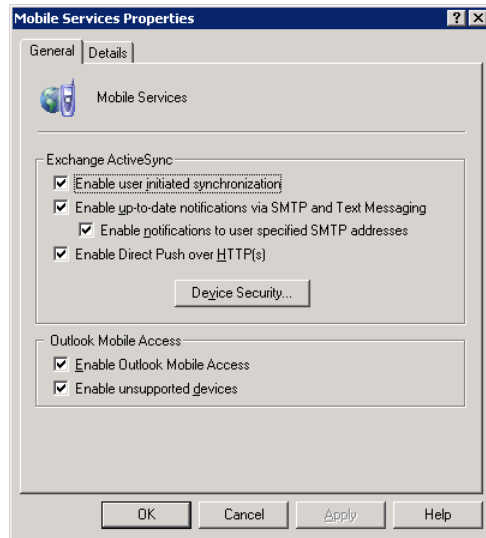
Enabling Direct Push

Direct Push provides users immediate access to new information or changes to information stored on the Exchange server, including E-Mail, Calendar, Contacts, and Tasks.

To enable Direct Push, perform the following steps on the Windows SBS server:

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

⁵ If you are using Windows Small Business Server 2003 R2, Exchange Server 2003 SP2 comes preinstalled.



In addition, enable Direct Push on the device by performing the following steps:

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

Step 6 - Configuring Device Synchronization

This section provides guidance on configuring a Windows Mobile powered device to synchronize with Windows SBS server and client computers that have Microsoft ActiveSync 4.1 installed. For guidance on installing ActiveSync 4.1, refer to the “Step 1 - Installing ActiveSync 4.1” section earlier in this white paper.

To configure a Windows Mobile device to synchronize with the Windows SBS server, perform the following steps:

1. Connect the Windows Mobile device to the client computer. The connection method will depend on the capabilities of the device and the computer and would typically be using a USB, Serial, Bluetooth, or Infrared port.

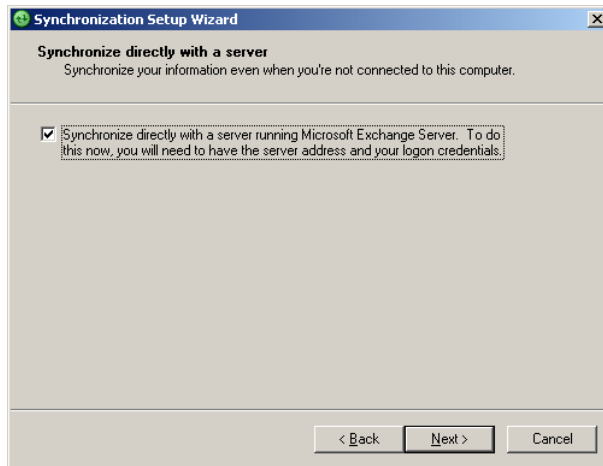
Note: ActiveSync 4.1 must be installed on the client computer.

2. After connecting the device to the client computer, the Synchronization Setup Wizard should open automatically on the client computer.

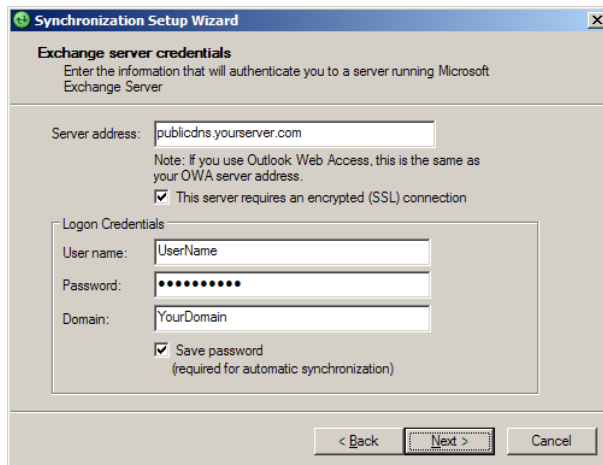
Note: If the device has already been configured once, the screens will be different than those shown here.

3. Click **Next** on the welcome page.

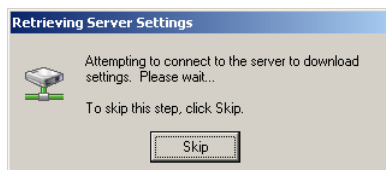
4. On the **Synchronize directly with a server** page, select the **Synchronize directly with a server running Microsoft Exchange Server** check box and click **Next**.



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

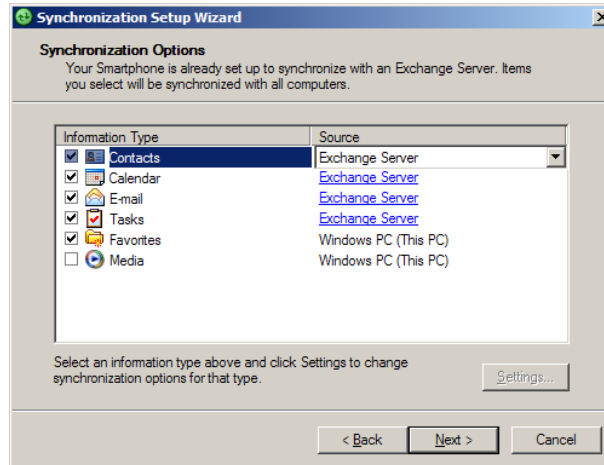


ActiveSync will attempt to connect to the server.



If you receive any errors during the attempt, refer to the "Troubleshooting" section later in this white paper.

6. 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.

Step 7 - Testing the Deployment

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

Testing Over-the-Air Synchronization

To test the configuration of over-the-air ActiveSync on the device, perform the following steps:

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 initiate synchronization.

The device should connect to the Internet, if not already connected, and perform synchronization of the items selected during ActiveSync configuration.

If the sync does not work for any reason, refer to the "Troubleshooting" section later in this white paper for more information.

Testing Direct Push

To test the configuration of Direct Push with any Windows Mobile 5.0 powered devices with MSFP, perform the following steps:

1. Ensure that the 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 will not be used for synchronization when the device is connected to a computer or to a wireless LAN with Internet access.

Remote Management

Windows Mobile 5.0 with MSFP offers several new features that enable better management of mobile devices and better protection of data. This section provides guidance on using some of these features, including:

- Performing remote device wipe.
- Implementing device policies.

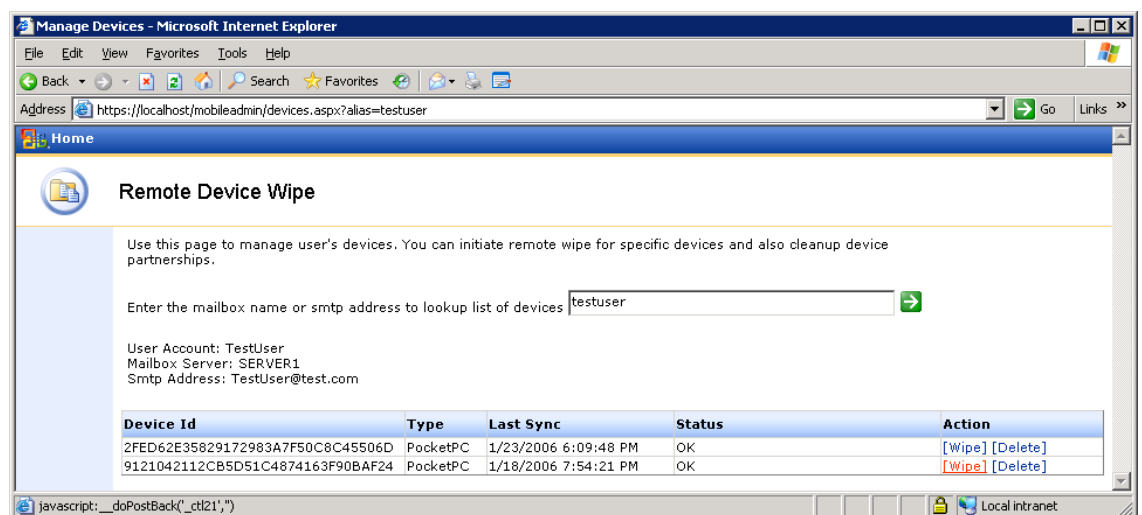
Performing Remote Device Wipe

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

Note: To use the remote device wipe feature, Exchange Server 2003 Service Pack 2 and Exchange Server ActiveSync Web Administration tool must be installed on the Exchange server. For steps on installing this tool, refer to the “Step 5 - Configuring Windows SBS for MSFP” section in this white paper.

To remotely wipe all information on a device, perform the following steps:

1. On any computer in the network, open Internet Explorer, browse to <https://WindowsSBSHostName/mobileadmin>, and log on using domain administrator credentials.
2. Click the **Remote Wipe** link.
3. Enter the mailbox name or the default SMTP address of the user whose device you want to wipe and press ENTER.



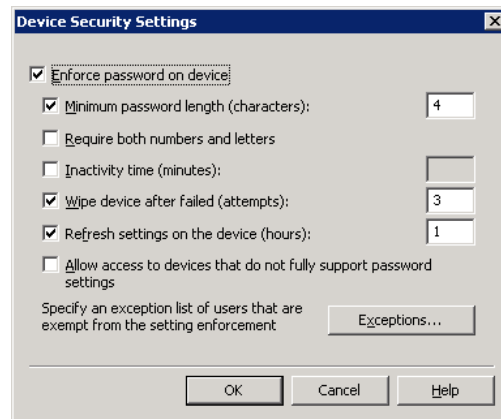
4. Click the **Wipe** link next to the device that you want to remote wipe.

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

Implementing Device Security Policy

You can enforce device security settings on Windows Mobile 5.0 powered devices, such as password requirements. This provides for better protection of information stored on the mobile devices. Device security policy can only be configured on a Windows SBS server with Exchange Server SP2 installed. Perform the following steps to define and enforce the policy:

1. On the Windows SBS server, open **Exchange System Manager**.
2. Expand **Global Settings**.
3. Right-click **Mobile Services** and 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 on some users, click the **Exceptions** button and add the user accounts to the exceptions list.
7. Click **OK**.

Troubleshooting

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

- Installing ActiveSync on Client Computers
- Installing Exchange Server 2003 SP2
- Configuring ActiveSync
- Synchronizing the Mobile Device
- Accessing Exchange Server ActiveSync Web Administration
- Deploying SSL Certificates
- Device Troubleshooting

Installing ActiveSync on Client Computers

If ActiveSync 4.1 fails to get installed on a computer:

- Ensure that you are logged on as a local administrator on the computer. The software will not install 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 that:
 - The access control lists (ACLs) are set properly on the GPO. The Authenticated Users group should be removed from the list, and the Windows SBS Mobile Users group should have Read and Apply Group Policy permissions checked.
 - The GPO is linked to the proper organizational unit (OU). The steps provided in this white paper link the GPO to the Windows SBS Users OU. If you did not use the user setup wizards to create users or if the user accounts are not located in the Windows SBS Users OU for some reason, ActiveSync will not get installed when the users log on.

Installing Exchange Server 2003 SP2

If you are unable to install Exchange Server 2003 SP2 because the Update action is disabled on the **Component Selection** page of the Microsoft Exchange Installation Wizard, ensure that Internet Message Filter (IMF) is not installed on the Exchange server.

Before installing Exchange Server 2003 SP2, you must uninstall the Internet Message Filter (IMF). An updated version of IMF is included as part of Exchange Server 2003 SP2.

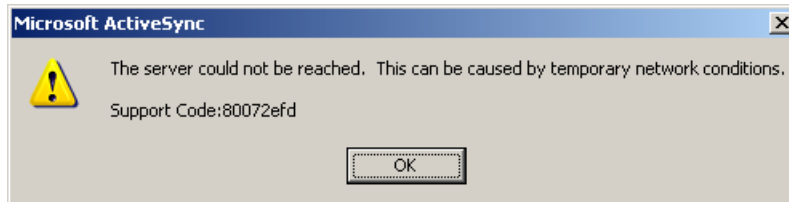
You can uninstall IMF using **Add or Remove Programs** in Control Panel.

For any other issues with the service pack installation, refer to the Exchange Server 2003 SP2 Readme file.

Configuring ActiveSync

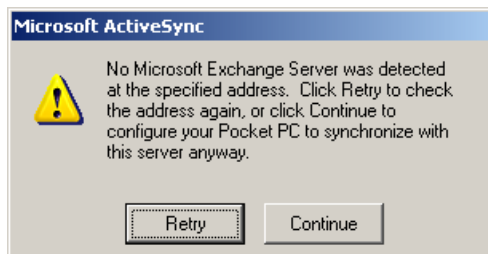
Following are some errors that may occur while configuring ActiveSync:

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



For troubleshooting this problem, refer to the “Check for Certificate-related Problems” section later in this white paper.

- When configuring the server, the following error indicates that the device cannot reach the server. The device would not have reached the point of checking the certificate at the time this error occurs.



Check the firewall configuration and 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.



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

- If you are using a third-party certificate, there is a problem with the server certificate. Try accessing the server from a computer on the Internet using the steps in the “Check for Certificate-related Problems” section later in this white paper.

- If you are redirected to an SSL connection without a prompt for a certificate, ensure that the certificate is from a CA 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. For a list of supported CAs, refer to the following URL:
<http://go.microsoft.com/fwlink/?LinkId=61499>
- If you are not redirected to an SSL connection without a prompt for a certificate, 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 “Option B - Configuring Third- Party Certificates” section. Work with the CA to troubleshoot the issue if none of these steps work.
- If you are using a self-signed certificate, you may have not installed the certificate on the device. You can click **Continue**, and then install the certificate after the wizard completes. You will not be able to 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 “Check for Certificate-related Problems” section to:

- Ensure that the certificate on the server is installed correctly.
- Ensure that the certificate is installed properly on the device.

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. If you receive any other error, follow the instructions provided for using SpAddCert.exe in the “Option A - Configuring Self-Signed Certificates” section.

Synchronizing the Mobile Device

Some Users are Not Able to Synchronize

If some users are not able to synchronize their devices while others can, perform the following checks:

- 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 Windows SBS 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.

- If you are using Smartphones, you may have to use a third-party certificate from a trusted CA. Many Windows Mobile 5.0 powered Smartphone devices cannot use self-signed certificates. However, all Pocket PC devices are capable of adding self-signed certificates, so they can work without third-party certificates.

No User is Able to Synchronize

If no user is able to synchronize devices, you need to perform 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 Windows SBS server. To do this, browse to <http://YourPublicDNS.YourServer.com/exchange> on a computer (not connected to your LAN) with Internet access and ensure you are redirected to an SSL connection without a prompt for a certificate.
- When you synchronize a device, click the **Attention Required** link on the ActiveSync screen. Review the error message to see if there is a reference to a certificate problem.
- If you are using a self-signed certificate, ensure that it has been 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 attempting to install self signed certificates on the device using the instructions in this document. In that case, you may want to manually try exporting the certificate from a workstation connected to the server instead of using the files in the [\\server\clientapps\sbscert](#) directory. The certificate can be exported from the Trusted Root Certificate Authorities\Certificates folder in the Certificates console which can be opened by running certmgr.msc at a command prompt.

Note: Tools such as disablecertchk.exe and addrootcert.exe do not work with Windows Mobile 5.0. These tools were created for earlier versions of Windows Mobile. Follow the instructions in this white paper to add a certificate using the new tools certinst.exe and SpAddCert.exe that are compatible with Windows Mobile 5.0.

Note: certinst.exe is a tool installed on many devices by the device manufactures. It allows you to add a certificate by opening it on the device as described in this white paper.

Check the Application Event Log

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

Check the Firewall Configuration

To check the firewall configuration, perform the following checks:

- Ensure port 443 is open, and that traffic to that port is being directed to the Windows SBS server.
- Ensure that the checks for useragent strings are disabled. Some firewalls have this enabled by default. Exchange ActiveSync does not send useragent strings.
- Ensure that the timeout value is set high enough for SSL connections, typically fifteen minutes.

For more information, refer to the article, "Enterprise firewall configuration for Exchange ActiveSync Direct Push Technology", available at the following URL:

<http://support.microsoft.com/?id=905013>

- If you have not upgraded to Internet Security and Acceleration Server 2004 as part of the installation of SBS Service Pack 1, you need to add a registry key to use direct push with ISA 2000. See <http://support.microsoft.com/?ID=304340> for more information (this article describes a different issue, however the registry change specified in this article applies for direct push on ISA 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, refer to the following URL:
http://www.isaserver.org/tutorials/You_Need_to_Create_a_Split_DNS.html
- If you are using ISA Server 2004 and users can sync over the air, but not from the cradle, you can perform the following steps to resolve some issues with ISA Server 2004:
 - a. Open **ISA Server Management**.
 - b. In the console tree, expand **Configuration** and click **General**.
 - c. In the details pane, click the **Define Firewall Client Settings** link.
 - d. In the **Firewall Client Settings** dialog box, click the **Application Settings** tab and create the following three new application settings.

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

Table 4. New Application Settings to be Created on ISA Server

Accessing Exchange Server ActiveSync Web Administration

If you are not able to access the Exchange Server ActiveSync Web Administration tool Web site, perform the following:

- On the Windows SBS server, open **Internet Information Services (IIS) Manager** and ensure that there is only one default Web site in IIS Manager.

During the installation of the tool, a duplicate default Web site gets created if your original default Web site is bound to a specific IP address. To remove the duplicate default Web site, you have the option of using either one of the following methods:

- Option A:
 - v. Uninstall the tool.
 - vi. Change the IP address settings of the original default Web site to “All Unassigned”.
 - vii. Install the tool again.
 - viii. Revert the IP address settings of the default Web site back to the original values.
- Option B:
 - i. Create a new virtual directory under the original default Web site.
 - ii. Export the settings from the duplicate default Web site.
 - iii. Import the settings to a new virtual directory under the original default Web site.
 - iv. 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 do this, perform the following steps:
 - a. In **Internet Information Services (IIS) Manager**, expand **Default Web Site**, right-click **ExAdmin**, and click **Properties**.
 - b. On the **Directory Security** tab, in the **Secure Communication** section, click **Edit**.
 - c. 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 do this, perform the following steps:
 - a. In **Internet Information Services (IIS) Manager**, expand **Default Web Site** and right-click **MobileAdmin** and click **Properties**.
 - b. On the **Virtual Directory** tab, in **Application Pool**, select **ExchangeApplicationPool**.

Deploying SSL 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 prior to applying for a certificate. You can check your D&B information at the following URL:
<http://www.dnb.com>
- 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:** Prepare to provide Trading License, a copy of a utility bill, a bank statement, or check with the trade name and the company name.
 - **Using a personal name:** Prepare to provide a copy of driver's license or passport. These requirements vary across CAs, but all CAs will verify your identity before issuing 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 certificate will not be issued.

Creating a Certificate Signing Request

Perform the following checks when creating a certificate signing request:

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

Installing a Self-Signed Certificate

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

- Running SpAddCert.exe on the mobile device gives the following error:
`smartphoneaddcert is not a valid Windows CE application`
This error is displayed when the utility is run on a Windows Mobile 5.0 Smartphone that does not accept root certificates. You cannot use a self-signed certificate on such a device. Check with your mobile operator or device manufacturer on whether they provide a separate utility for installing self-signed certificates; if not, you will have to use a third-party certificate.
- Certchk.exe gives an error when run.
Certchk.exe utility is not supported on Windows Mobile 5.0 and will not work.
- AddRootCert.exe cannot be run.
AddRootCert.exe is not supported on Windows Mobile 5.0 and will not work.
- 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, refer to the "Installing the Certificate on the Device" section earlier in this white paper.

Configuring Devices

Direct Push Messages

If messages sent are not being received immediately:

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

Device Policy

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

When the policy is applied to a device, the user is duly 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 will verify server connectivity and ensure 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 Windows SBS server. Look for entries coming from the mobile device and see if there are any error messages that might help in determining the problem.
- Enable logging on the device and check the logs for entries that might give more information on the problem. To enable logging on the device, perform the following steps:
 - a. If you have a Pocket PC:
 - i. Select **Start > Programs > ActiveSync**.
 - ii. Select **Menu > Configure Server**.
 - iii. Select **Next** and then go to **Advanced**.
 - b. If you have a Smartphone:
 - i. Select **Start > ActiveSync**.
 - ii. Select **Menu > Configure Server, Next, Next, Menu > Advanced**.

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