



Step-by-Step Guide to Deploying Microsoft Exchange Server 2003 SP2 Mobile Messaging with Windows Mobile 5.0-based Devices

March, 2006

Applies to: Exchange Server 2003 SP2
and Windows 5.0-based Devices
with the Messaging and Security Feature Pack

Direct Push Technology requires Windows Mobile 5.0 with the Messaging and Security Feature Pack (MSFP) connected with Exchange Server 2003 Service Pack 2.

Connectivity and synchronization may require separately purchased equipment and/or wireless products (e.g., WiFi card, network software, server hardware, and/or redirector software). Service plans are required for Internet, WiFi and phone access. Features and performance may vary by service provider and are subject to network limitations. See device manufacturer, service provider and/or corporate IT department for details.

Available programs, features and functionality vary by device and Windows Mobile operating system version. PowerPoint Mobile available with Windows Mobile 5.0.

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 OR IMPLIED, 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.

© 2006 Microsoft Corporation. All rights reserved.

The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted 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.

Microsoft, Active Directory, ActiveSync, BizTalk, Hotmail, JScript, MS-DOS, MSDN, MSN, Outlook, SharePoint, Visio, Visual Basic, Visual Studio, Windows, Windows Media, Windows Mobile, Windows NT, Windows Server, and Windows Server System 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.

Deploying Microsoft Exchange Server 2003 SP2 Mobile Messaging with Windows Mobile 5.0-based Devices	5
Introduction	5
Overview: Messaging and Security Feature Pack.....	8
Deployment Configuration and Best Practices.....	12
Deploying Exchange Server 2003 SP2 Mobile Messaging	17
Deployment Process	17
Step 1 - Upgrade to Exchange Server 2003 SP2.....	18
Step 2 - Update All Servers with Security Patches	18
Step 3 - Protect Communications Between the Mobile Devices and Your Exchange Server.....	19
Deploying SSL to Encrypt Messaging Traffic	19
Backing up Server Certificates	24
Single Server Configuration (Optional).....	27
Configuring Basic Authentication	27
Require SSL Connection to the Exchange ActiveSync Web Site Directories	27
Required UrlScan Settings	29
Step 4 - Protect Communications Between the Exchange Server 2003 SP2 Server and Other Servers	32
Step 5 - Install and Configure an ISA Server 2004 Environment or Other Firewall	33
Configuring the Host File Entry	38
Testing OWA and Exchange ActiveSync	39
Testing OWA (If installed).....	39
Step 6 - Configure and Manage Mobile Device Access on the Exchange Server.....	41
Enabling Mobile Access	41
Enable Exchange ActiveSync for All Users	41
Enable User-Initiated Synchronization.....	42
Enable Up-to-date Notifications (Optional)	43
Monitoring Mobile Performance on Exchange Server	45
Step 7 – Install the Exchange ActiveSync Mobile Administration Web Tool	47
Step 8 - Manage and Configure Mobile Devices.....	48
Appendix A. Deploying Exchange ActiveSync with Certificate-Based Authentication.....	53
Introduction	53
Configuring Certificate-Based Authentication for Exchange ActiveSync	53
Exchange ActiveSync Requirements.....	53
Kerberos Basics	55
Alternative Deployment Steps for Certificate-based Authentication	55
Setting up SSL for Exchange ActiveSync Virtual Directory	55
Creating the Exchange ActiveSync publishing rule using tunneling	56
Using Active Directory Users and Computers to Configure Kerberos-Constrained Delegation and Protocol Transitioning.....	57
Overview of Certificate Enrollment Configuration.....	58
Configuring the XML.....	60
Uploading the XML to Active Directory	63
Appendix B. Adding a Certificate to the Root Store of a Windows Mobile-based Device.....	67
Create the Provisioning XML to Install a Certificate to the Root Store.....	67
Create a CAB file containing the provisioning XML	68
Distributing the CAB Provisioning File	68

Deploying Microsoft Exchange Server 2003 SP2 Mobile Messaging with Windows Mobile 5.0-based Devices

Introduction

This document is designed primarily for Information Technology (IT) professionals who are responsible for planning and deploying mobile messaging systems that use Microsoft® Exchange Server 2003 with Service Pack 2 (SP2) and Microsoft® Windows® Mobile™-based devices that have the Messaging and Security Feature Pack.

This document is divided into two main sections that describe the following:

- The essential elements of a mobile messaging system, including requirements; a summary of deployment procedures; an overview of the features of the Messaging and Security Feature Pack; and best practices for networking, security, and device management.
- The guidelines and resources for the deployment of a mobile messaging system, including updating Exchange Server 2003 SP2, setting up Microsoft® Exchange ActiveSync® for mobile access, creating a protected communications environment, and procedures for setting up and managing mobile devices.

For current information on deploying mobile messaging solutions and managing Windows Mobile-based devices, visit the Windows Mobile Center Web site at:
<http://go.microsoft.com/fwlink/?LinkId=62636>

Assumptions

This document assumes that you have an understanding of Microsoft Office Outlook® Web Access, Exchange ActiveSync, Hypertext Transfer Protocol (HTTP), basic Exchange Server 2003 concepts, and basic Microsoft Windows® Internet Information Services (IIS) concepts.

Requirements

The following operating systems and applications are required for successful deployment.

- Microsoft® Windows® 2000 Server with Service Pack 4 (SP4) or Microsoft® Windows Server™ 2003 with Service Pack 1 (SP1) (recommended)
- Microsoft® Exchange Server 2003 SP2 (includes Exchange ActiveSync)
- Microsoft® Exchange ActiveSync® Mobile Administration Web tool
- Microsoft Windows Mobile 5.0-based devices that have the Messaging and Security Feature Pack
- Active Directory® directory service
- Internet Information Services (IIS) 6.0

Note Windows Mobile 5.0-based devices that have a version number of 148xx.2.x.x or higher include the Messaging and Security Feature Pack. To find the operating system version on the device, click **Start**, choose **Settings**, and then click **About**.

Optional Items

You can implement the following components for security and device management tools. See the Best Practices section.

- The most recent version of Microsoft® Desktop ActiveSync®, which is available as a download from the Microsoft download Web site at <http://go.microsoft.com/fwlink/?LinkId=62652>.
- Microsoft® Internet Security and Acceleration (ISA) Server 2004
- Windows certification authority (CA)

-
- RSA® Authentication Manager (6.0)
 - RSA® Authentication Agent for Microsoft Windows
 - RSA SecurID® Authenticator

Deployment Process Summary

Because corporate network configurations and security policies vary, the deployment process will vary for each mobile messaging system installation. This deployment process includes the required steps and the recommended steps for deploying a mobile messaging solution that uses Exchange Server 2003 SP2 and Windows Mobile 5.0-based devices.

The process can be accomplished in the following eight steps:

- **Step 1** – Upgrade Front-End Server to Exchange Server 2003 SP2
- **Step 2** – Update All Servers with Security Patches
- **Step 3** – Protect Communications with Mobile Devices
- **Step 4** – Protect Communications between the Exchange Server and Other Servers
- **Step 5** – Install and Configure an ISA Server 2004 Environment or Other Firewall
- **Step 6** – Configure Mobile Device Access on the Exchange server
- **Step 7** – Install the Exchange ActiveSync Mobile Administration Web tool
- **Step 8** – Manage and Configure Mobile Devices

Planning Resources

The following Microsoft Web sites and technical articles provide background information that is important for the planning and deployment of your mobile messaging solution.

Exchange Server 2003

- Planning an Exchange Server 2003 Messaging System
<http://go.microsoft.com/fwlink/?LinkId=62626>
- Exchange Server 2003 Client Access Guide
<http://go.microsoft.com/fwlink/?LinkId=62628>
- Exchange Server 2003 Deployment Guide
<http://go.microsoft.com/fwlink/?LinkId=62629>
- Windows Server 2003 Deployment Guide
<http://go.microsoft.com/fwlink/?LinkId=62630>
- Using ISA Server 2004 with Exchange Server 2003
<http://go.microsoft.com/fwlink/?LinkId=42243>
- Windows Server 2003 Technical Reference
<http://go.microsoft.com/fwlink/?LinkId=62631>
- IIS 6.0 Deployment Guide (IIS 6.0)
<http://go.microsoft.com/fwlink/?LinkId=62632>
- Microsoft Exchange Server TechCenter
<http://go.microsoft.com/fwlink/?LinkId=62633>
- Exchange Server 2003 Technical Documentation Library
<http://go.microsoft.com/fwlink/?LinkId=62634>

Windows Mobile

- Supporting Windows Mobile-Based Devices within the Enterprise: Corporate Guidelines for Each Stage of the Device's Lifecycle (paper)
<http://go.microsoft.com/fwlink/?LinkId=62635>

-
- TechNet Windows Mobile Center
<http://go.microsoft.com/fwlink/?LinkId=62636>

Security

- Windows Mobile-based Devices and Security (paper)
<http://go.microsoft.com/fwlink/?LinkId=62640>
- Windows Mobile Security <http://go.microsoft.com/fwlink/?LinkId=62641>
- TechNet Security Center
<http://go.microsoft.com/fwlink/?LinkId=62642>

Overview: Messaging and Security Feature Pack

The Messaging and Security Feature Pack for Windows Mobile 5.0 enables Windows Mobile 5.0-based devices to be managed by Microsoft Exchange Server 2003 SP2. The result is a mobile messaging solution that uses the management benefits of Exchange ActiveSync and the new security policy functions on the Windows Mobile 5.0-based devices, which helps you to better manage and control the devices.

Using Windows Mobile 5.0-based devices with the Messaging and Security Feature Pack will give you the following capabilities:

- With Direct Push technology, you can provide your users with immediate delivery of data from the Exchange mailbox to their device. This includes e-mail, calendar, contact, and task information.
- You can define the security policies on your Exchange server and they will be enforced on Windows Mobile 5.0-based devices that are directly synchronized with your Exchange server.
- You can monitor and test Exchange ActiveSync performance and reliability by using the Exchange Server Management Pack.
- You can manage the process of remotely erasing or wiping lost, stolen, or otherwise compromised mobile devices that are directly synchronized with your Exchange server by using the Microsoft Exchange ActiveSync Mobile Administration Web tool.

Features

Direct Push Technology

The Direct Push technology included in Exchange Server 2003 SP2 provides a new approach to the immediate delivery of data from the Exchange mailbox to the user's mobile device. Direct Push works for mailbox data, including Inbox, Calendar, Contacts, and Tasks. The Direct Push technology uses an established HTTPS connection between the device and the Exchange server; previous solutions required the use of Short Message Service (SMS), which is no longer required. No special configuration is required on the mobile device, and you can keep your standard data plan since the service is world-capable and requires no additional software or server installations other than Exchange Server 2003 SP2.

Exchange ActiveSync

Exchange ActiveSync is an Exchange synchronization protocol that is designed for keeping your Exchange mailbox synchronized with a Windows Mobile 5.0-based device. Exchange ActiveSync is optimized to deal with high-latency/low-bandwidth networks, and also with low-capacity clients that have limited amounts of memory, storage, and processing power. Under the covers, the Exchange ActiveSync protocol is based on HTTP, SSL, and XML and is a part of Exchange Server 2003. In addition, Exchange ActiveSync provides the following benefits:

- The consistency of the familiar Outlook experience for users
- No extra software is required to install or configure devices
- Global functionality that is achieved via standard data access phone service

Global Address List Access

Support for over-the-air lookup of global address list (GAL) information stored on Exchange Server. With the Messaging and Security Service Pack, mobile device users will be able to receive contact properties for individuals in the GAL. These properties can be used to search remotely for a person quickly based on name, company, and/or other property. Users will get all of the information they need to reach their contacts without having the data store on their device.

Security Features

Remotely Enforced Device Security Policies

Exchange Server 2003 SP2 helps you to configure and manage a central policy that requires all mobile device users to protect their device with a password in order to access the Exchange server. Not only that, but you can specify the length of the password, require usage of a character or symbol, and designate how long the device has to be inactive before prompting the user for the password again.

An additional setting, wipe device after failed attempts, allows you to delete all data on the device after the user enters the wrong password a specified number of times. The user will see alert dialog boxes warning of the possible wipe and providing the number of attempts left before it happens.

Another setting allows you to specify whether non-compliant devices can synchronize. Devices are considered non-compliant if they do not support the security policy you have specified. In most cases, these are devices not configured with the Messaging and Security Feature Pack.

The device security policies are managed from Exchange System Manager's Mobile Services Properties interface.

Remote Device Wipe

The remote wipe feature helps you to manage the process of remotely erasing lost, stolen, or otherwise compromised mobile devices. If the device was connected using Direct Push technology, the wipe process will be initiated immediately and should take place in seconds. If you have used the enforced lock security policy, the device is protected by a password and local wipe, so the device will not be able to perform any operation other than to receive the remote wipe notification and report that it has been wiped.

The new Microsoft Exchange ActiveSync Mobile Administration Web tool enables you to perform the following actions:

- View a list of all devices that are being used by any user.
- Select or de-select devices to be remotely erased.
- View the status of pending remote erase requests for each device.
- View a transaction log that indicates which administrators have issued remote erase commands, in addition to the devices those commands pertained to.

Advanced Security Features

Certificate-Based Authentication

If SSL basic authentication does not meet your security requirements and you have an existing Public Key Infrastructure (PKI) using Microsoft Certificate Server, you may wish to use the certificate-based authentication feature in Exchange ActiveSync. If you use this feature in conjunction with the other features described in this document, such as local device wipe and the enforced use of a power-on password, you can transform the mobile device itself into a smartcard. The private key and certificate for client authentication is stored in memory on the device. However, if an unauthorized user attempts to brute force attack the power-on password for the device, all user data is purged including the certificate and private key.

For more information, see Appendix A. Deploying Exchange ActiveSync Certificate-based Authentication.

Microsoft has created a tool for deploying Exchange ActiveSync certificate-based authentication. Download the tool and documentation from the Microsoft Download center Web site:

<http://go.microsoft.com/fwlink/?LinkId=63271>

Support for S/MIME Encrypted Messaging

The Messaging and Security Feature Pack for Windows Mobile 5.0 provides native support for digitally signed, encrypted messaging. When encryption with the Secure/Multipurpose/Internet Mail Extension (S/MIME) is deployed, users can view and send S/MIME-encrypted messages from their mobile device.

The S/MIME control:

- Is a standard for security enhanced e-mail messages that use a Public Key Infrastructure (PKI) to share keys
- Offers sender authentication by using digital signatures
- Can be encrypted to protect privacy
- Works well with any standard-compliant e-mail client

For guidance on how to implement the S/MIME control with Microsoft® Exchange Server 2003 SP2, see the Exchange Server Message Security Guide at the following Microsoft Web site: <http://go.microsoft.com/fwlink/?LinkId=63272>.

Administering the Messaging and Security Feature Pack

Safeguards like password policies and remote wipe capabilities provide you with the security features to help you protect your organization's data. With the combination of the management capabilities built into Exchange Server 2003 SP2 and the security and configuration protocols included in the Windows Mobile 5.0-based devices that have the Messaging and Security Feature pack, your control over mobile devices has been streamlined. You will see that most of the administration of the security features for the mobile device happens on the Exchange Server or on the Exchange ActiveSync Mobile Administration Web tool.

The following table summarizes the features and the settings required on the Exchange Server or on the mobile device.

Feature	Exchange Server Settings	Mobile Device Settings
Exchange Direct Push technology	Enabled by default with Exchange Server 2003 SP2 <ul style="list-style-type: none">• Protected configuration with firewall or ISA Server• Set session timeout time to 30 minutes	No device setup required; user steps thru ActiveSync wizard upon login to Exchange server.
Exchange ActiveSync	Enabled by default with Exchange Server 2003 SP2 Set parameters by using Exchange System Manager's Mobile Services Properties	No device setup required; user steps thru ActiveSync wizard upon login to Exchange server.
Wireless access to global address list (GAL)	Default Exchange Server setup Requires Outlook Web Access published on Exchange Server	No device setup required Trusted devices have automatic access to GAL
Remotely enforced IT policy	Enable Direct Push technology in Exchange ActiveSync Use Exchange System Manager's Mobile Services Properties to apply policies	No device setup required; user steps thru ActiveSync wizard upon login to Exchange server.

Remote Wipe	<p>Enable Direct Push technology in Exchange ActiveSync</p> <p>Use Mobile Administration Web tool to initiate, track, and cancel the remote wipe</p>	<p>No device setup required; user steps thru ActiveSync wizard upon login to Exchange server.</p>
Certificate-based authentication	<ul style="list-style-type: none"> • Install certificate on Exchange Servers • Deploy ActiveSync 4.1 to desktops • Use the Certificate Enrollment tool to configure the devices via ActiveSync 	<p>Initial certificate enrollment using Desktop ActiveSync is required</p>
S/MIME mobile device support	<p>Deploy an Exchange Server 2003 messaging system with PKI security</p>	<p>Install certificate enrollment protocol and key on the device</p>

Deployment Configuration and Best Practices

Best practices for deploying a mobile messaging solution on your corporate network are recommendations to help you smooth operation of, and provide a high level of security in, your mobile messaging solution. You can determine what the best practices are for your network configuration and mobile device use.

Network Planning and Design

To design a successful Exchange Server 2003 SP2 messaging system, you must first understand the capabilities and limitations of the software and hardware upon which you will build your messaging system. Whether you are developing a new Exchange Server messaging system or upgrading from a previous Exchange implementation, you need to balance the limitations of your network infrastructure with the capabilities of your messaging system, operating system, and user software.

For more information about how to plan your messaging system, see Planning an Exchange Server 2003 Messaging System at <http://go.microsoft.com/fwlink/?LinkId=62643>

Best Practice: Use Front-end and Back-end Configuration for Exchange Servers

A front-end and back-end configuration is recommended for multiple-server organizations that use Exchange ActiveSync, Outlook Web Access, POP, or IMAP and want to provide HTTP, POP, or IMAP access to their employees. In this architecture, a front-end server accepts requests from clients and proxies those requests to the appropriate back-end server for processing. The front-end and back-end architecture allows the front-end server to handle the Secure Sockets Layer (SSL) encryption, thus enabling the back-end servers to increase overall e-mail performance.

Securing the messaging environment also involves disabling those features and settings for the front-end server that are not necessary in a front-end and back-end server architecture.

For more information about front-end and back-end server architecture, see Exchange Server 2003 and Exchange 2000 Server Front-End and Back-End Topology at <http://go.microsoft.com/fwlink/?LinkId=62643>

Considerations for Deployment on a Single Server

If you are deploying a mobile messaging solution that uses a single Exchange server, you may have to establish some special configurations to avoid conflicts on the virtual directory.

SSL Requirements and Forms-based authentication

In a single-server configuration, Exchange Server ActiveSync accesses the Exchange virtual directory via port 80 by using Kerberos authentication. Exchange ActiveSync cannot access the Exchange virtual directory if either of the following conditions are true:

- The Exchange virtual directory is configured to require SSL.
- Forms-based authentication is configured.

For more information about, and workarounds for, these configurations, see the following article in the Microsoft Knowledge Base:

Exchange ActiveSync and Outlook Mobile Access errors occur when SSL or forms-based authentication is required for Exchange Server 2003

<http://go.microsoft.com/fwlink/?LinkId=62660>

Exchange ActiveSync Mobile Administration Web Tool

When deployed in a single-server configuration, the Exchange ActiveSync Mobile Administration Web tool requires the default configuration on the ExAdmin virtual directory. By default, SSL is not turned on and the vdir has Windows Integrated authentication.

In a single-server configuration, we recommend that you do the following:

- Turn off SSL Required on the ExAdmin virtual directory
 - Use Windows Integrated authentication on the ExAdmin virtual directory
- Note** the Exchange ActiveSync Mobile Administration Web tool should run in the ExchangeAppPool.

This is a known issue. A Knowledge Base article about this issue will be published soon.

RSA SecurID Compatibility

RSA SecurID provides token-based authentication that requires user input and was not compatible with the Direct Push technology, in which the device synchronizes automatically. RSA has updated the RSA Authentication Agent for Windows so that Direct Push technology and scheduled synchronization features function smoothly.

If you are using the RSA SecurID product, be sure to get the latest RSA SecurID software from the RSA Security Web site: <http://go.microsoft.com/fwlink/?LinkId=63273>.

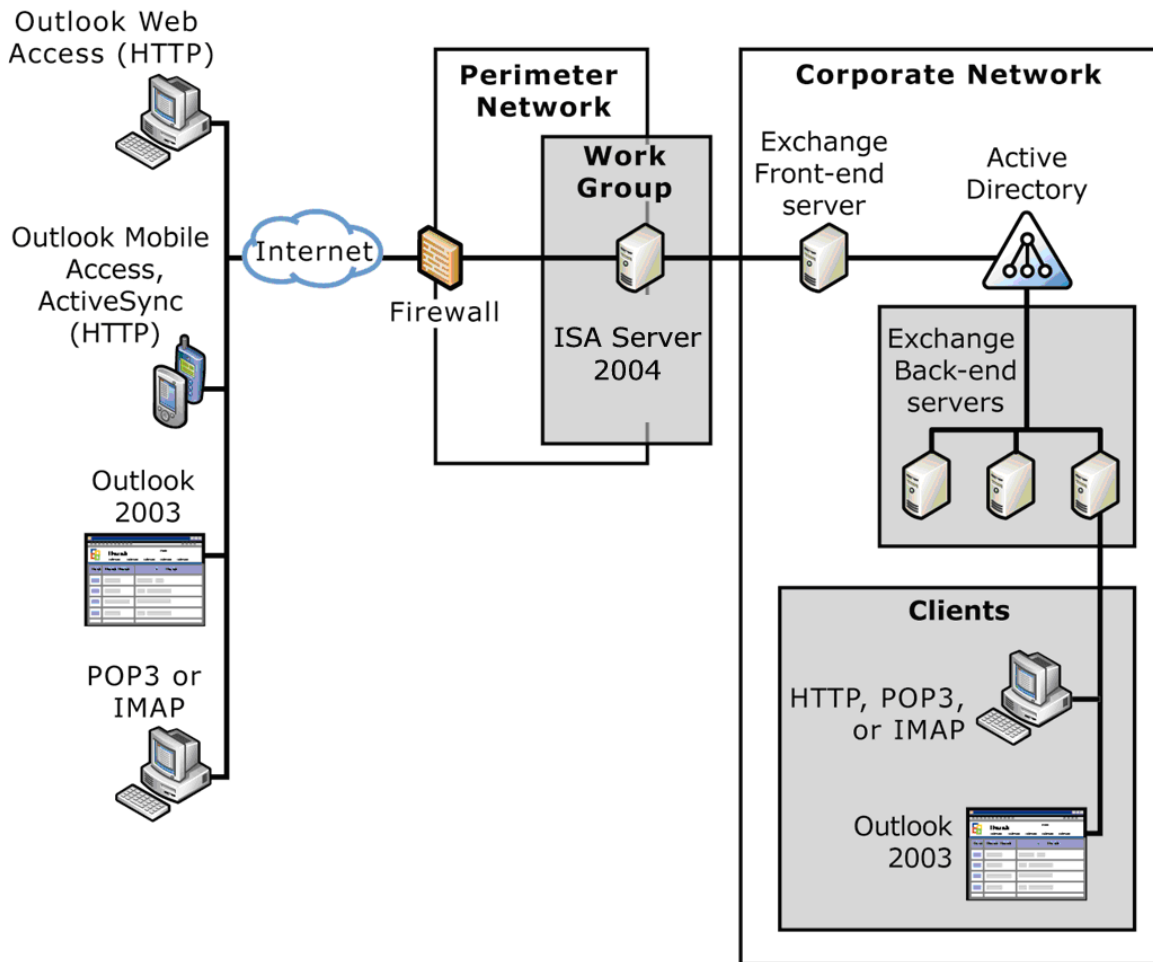
Best Practice: Deploy ISA Server 2004 as an Advanced Firewall

As a best practice alternative to locating your front-end Exchange servers in the perimeter network, you can deploy ISA Server 2004 as an advanced firewall. In this configuration, all of the Exchange servers are within the corporate network and the ISA server acts as the advanced firewall in the perimeter network that is exposed to Internet traffic. This adds an additional layer of security to your network.

All incoming Internet traffic bound to your Exchange servers – for example, Microsoft Office Outlook Web Access and RPC over HTTP communication from Outlook 2003 clients – is processed by the ISA server. When the ISA server receives a request from an Exchange server, the ISA server terminates the connection and then proxies the request to the appropriate Exchange servers on your internal network. The Exchange servers on your network then return the requested data to the ISA server, and then ISA server, which sends the information to the client through the Internet.

During installation of the ISA server, we recommend that you enable SSL encryption, and designate 443 as the SSL port. This leaves the 443 port open as the “Web Listener” to receive Internet traffic. We also recommend that you set up basic authentication for Exchange ActiveSync, and that you require all clients to successfully negotiate an SSL link before connecting to the Exchange ActiveSync site directories. If you follow these recommendations, the Internet traffic that flows into and out of the 443 port will be more protected.

When configured in Web-publishing mode, ISA Server 2004 will provide protocol filtering and hygiene, denial of service (DoS) and distributed denial of service (DDoS) protection, and pre-authentication.



The figure above is an example of a recommended Exchange Server 2003 deployment for mobile messaging with ISA Server 2004.

Best Practice: Configuring your firewall for optimal Direct Push performance

Direct Push technology requires an established connection between the server and the client. No data is sent over this connection unless there is e-mail or data to be transmitted or the device needs to reestablish its connection with the server. This means that the maximum length of the connection is determined by the lowest network timeout in the path between the device and the server.

With good network coverage, the maximum timeout will be determined by the connection timeout that is enforced by the firewalls that deal with Internet traffic to your Exchange front-end servers. If you keep the timeout very low, then you will force the device to reconnect several times, which will quickly drain its battery.

As a best practice, you should adjust the connection timeout of your firewall to ensure that Direct Push functionality works efficiently. In order to optimize battery life, we recommend a timeout period of between 15 and 30 minutes.

Security: Authentication and Certification

Security for communication between the Exchange server and client mobile devices can be increased by using Secure Sockets Layer (SSL) for encryption and server authentication and by using web publishing to protect incoming traffic.

The following best practices will help you build a more secure mobile messaging solution.

Best Practice: Use SSL for Encryption and Server Authentication

To protect outgoing and incoming data, deploy SSL to encrypt all traffic. You can configure SSL security features on an Exchange server to verify the integrity of your content and the identity of users, and to encrypt network transmissions. The Exchange server, just like any Web server, requires a valid server certificate to establish SSL communications.

Windows Mobile 5.0-based devices are shipped with trusted root certificates. Check with your device manufacturer for a current list of the certificate authorities that shipped with your device. If you obtain a root certificate from one of the trusted services, your client mobile devices should be ready to establish SSL communications with no further configuration.

Note Some server certificates are issued with intermediate authorities in the certification chain. If IIS is not configured to send all certificates in the chain to the mobile device during the SSL handshake, the device will not trust the certificate because the device does not support dynamically retrieving the other certificates.

For more information about obtaining server certificates, see “Obtaining and Installing Server Certificates” in the Exchange Server 2003 Client Access Guide at <http://go.microsoft.com/fwlink/?LinkId=62628>

For more information about root certificates for mobile devices, see Appendix B. Adding Root Certificates to Windows Mobile Devices in this document.

Best Practice: Use Web Publishing with Basic Authentication

As a best practice, Web publishing is easier to implement and provides a higher level of security than server publishing, although larger companies that are planning to use client certificate-based authentication must implement the latter.

Server publishing, also known as tunneling, refers to network/transport-layer protection, whereas Web publishing, also known as bridging, refers to application-layer protection. Web publishing is only possible when SSL is terminated on ISA Server 2004. Because ISA Server 2004 only sees encrypted traffic, it cannot perform tasks such as protocol hygiene that require it to analyze the contents; thus ISA Server 2004 only offers protection based on the network/transport layers.

The following table compares the security features of server publishing and Web publishing.

Security Features	Server Publishing	Web Publishing
Synchronous idle character (SYN) flood attack protection	X	X
Flood/network resiliency – mechanisms that are activated when various system and network quotas are reached. These can include blocking traffic, increasing delays, or releasing memory.	X	X
Access control based on source address, source port, destination address, destination port, and protocol.	X	X
Detection and prevention of port scanning, fragment attacks, various TCP/IP attacks, and IP and TCP header validation.	X	X
HTTP protocol hygiene.		X

HTTP session quota.		X
HTTP filtering – this allows the detection of signatures in HTTP requests, which is often used to protect against “zero-day” attacks, for example, when the Web servers are not all fully patched. HTTP filtering reduces the attack surface of the Web server by allowing only certain HTTP verbs, actions or URLs.		X
Pre-authentication and authorization – the Web server only receives traffic from authenticated and authorized users. This means that even if there is vulnerability in IIS, only company employees can actually exploit the vulnerability. Without pre-authentication, the Exchange front-end server is the first line of defense, so it must be in the DMZ.		X
Single sign-on in ISA 2006 provides increased usability.		X
Link translation provides increased usability.		X

Best Practice: Use Server Publishing with Certificate-based Authentication

For certificate-based authentication to work correctly with Exchange ActiveSync, the enterprise firewall must be configured to allow the Exchange front-end server to terminate the SSL connection. Web publishing will not work with certificate-based authentication.

Microsoft has provided several tools to help an Exchange administrator configure and validate client certificate authentication.

For more information, see Appendix A. Deploying Exchange ActiveSync Certificate-Based Authentication.

The Exchange ActiveSync Certificate-based Authentication tool can be downloaded from the Tools for Exchange Server 2003 Web site at <http://go.microsoft.com/fwlink/?LinkId=62656>.

Best Practice: Determine and Deploy a Device Password Policy

For the first time, Exchange Server SP2 and Windows Mobile 5.0-based devices that have the Messaging and Security Feature Pack help you to configure a central security policy that requires all mobile device users to protect their device with a password in order to access the Exchange server.

Within this central security policy, there are several attributes you can configure, including the length of the password (the default is four characters), the use of characters or symbols in the password, and how long the device can be inactive before it prompts the user for the password again.

Once you have determined your device security policies, you can apply them by using Exchange System Manager’s **Mobile Services Properties**. When your users connect to the Exchange server and sign in, the policies will be sent to the device. You can set the interval at which the security policies will automatically be refreshed on the devices.

For more information on setting security policies, see Configuring Security Settings for Mobile Devices in this document.

Deploying Exchange Server 2003 SP2 Mobile Messaging

For simplicity, we have documented the recommended deployment with references to alternative or optional steps. Your production environment may vary—for example, you may use another firewall—but if you read through the process for installing and configuring the ISA server, you should be able to configure your firewall to work with this deployment.

Deployment Process

The following steps summarize the process for deploying an Exchange Server 2003 SP2 mobile messaging solution.

Step 1 – Upgrade Front-End Server to Exchange Server 2003 SP2

Step 2 – Update All Servers with Security Patches

Step 3 – Protect Communications Between the Mobile Devices and your Exchange Server

- Encrypt Messaging Traffic with Secure Sockets Layer (SSL)
- Enable SSL on the Default Web Site
- Configure Authentication
 - Basic Authentication (Recommended)
 - RSA SecurID (Optional)
 - Configure Certification Authentication (Optional)

- Protect IIS by Using UrlScan and IIS Lockdown Wizard

Step 4 – Protect Communications Between the Exchange Server and Other Servers

- Use IPSec to Encrypt IP Traffic (Recommended)

Step 5 – Install and Configure an ISA Server 2004 Environment or Other Firewall

- Create the Exchange ActiveSync Publishing Rule by Using Bridging
- Create the Exchange ActiveSync Publishing Rule by Using Tunneling (with Certificate-Based Authentication)
- Configure the Host File Entry
- Modify the Firewall Idle Session Time-out Settings to 30 Minutes

Step 6 – Configure Mobile Device Access on the Exchange server

- Enable Exchange ActiveSync for All Users
- Enable User Initiated Synchronization
- Enable Direct Push
- Set Security Policy Settings for Mobile Devices
- Monitor Mobile Performance on Exchange Server

Step 7 – Install the Exchange ActiveSync Mobile Administration Web Tool

Step 8 – Manage and Configure Mobile Devices

- Set up Mobile Connection to Exchange Server
- Initiate and Track Remote Wipe on Mobile Devices
- Provision or Configure Mobile Devices
- Initiate and Track Remote Wipe on Mobile Devices

Step 1 - Upgrade to Exchange Server 2003 SP2

Exchange Server 2003 SP2 includes Exchange ActiveSync, the synchronization protocol that keeps the Exchange mailbox synchronized on client mobile devices. By default, Exchange ActiveSync is enabled.

Exchange Server 2003 SP2 contains new features that work with the Windows Mobile 5.0 Messaging and Security Feature Pack to help you to improve the deployment, security, and management of mobile devices.

Note To use the Windows Mobile 5.0 Messaging and Security Feature pack, you must upgrade your front-end Exchange server to Exchange Server 2003 SP2. Back-end Mailbox servers can remain at Exchange 2003 RTM or SP1. However, we recommend that you upgrade both front-end and back-end servers to take advantage of the updates in SP2.

How to Upgrade to Exchange Server 2003 SP2

Download the Service Pack 2 for Exchange Server 2003 file from the following Microsoft Web site: <http://go.microsoft.com/fwlink/?LinkId=62644>

Follow the directions provided to upgrade your Exchange servers to SP2.

Step 2 - Update All Servers with Security Patches

To help you ensure that your mobile messaging network is strong from end to end, take this opportunity to update all of your servers.

After you install Exchange Server 2003 SP2 on your front-end server, update the server software on your other Exchange servers and on any other server that Exchange communicates with, such as your global catalog servers and your domain controllers.

For more information about updating your software with the latest security patches, see the Exchange Server Security Center Web site: <http://go.microsoft.com/fwlink/?LinkId=62646>

For more information about Microsoft security, see the Microsoft Security Web site: <http://go.microsoft.com/fwlink/?LinkId=62649>

Step 3 - Protect Communications Between the Mobile Devices and Your Exchange Server

To help protect the communications between Windows Mobile devices and your Exchange front-end server, follow these steps:

- Deploy SSL to encrypt messaging traffic
- Enable SSL on the default Web site
- Configure basic authentication for the Exchange ActiveSync virtual directory
 - Note** If you plan to use Certificate Authentication instead of basic configuration, you must deploy SSL following the instructions in Appendix A. Deploying Exchange ActiveSync Certificate-Based Authentication.
 - Note** If you are using RSA SecurID, you must update the RSA Authentication Agent.
- Protect IIS by using UrlScan and IIS Lockdown Wizard

See the Best Practices section of this document for more information on authentication and certification.

Deploying SSL to Encrypt Messaging Traffic

To protect incoming and outgoing mail, deploy SSL to encrypt messaging traffic. You can configure SSL security features on an Exchange server to verify the integrity of your content, verify the identity of users, and encrypt network transmissions.

The steps involved in configuring SSL for Exchange ActiveSync are:

1. Obtaining and Installing a Server Certificate
2. Validating Installation
3. Backing up the Server Certificate
4. Enabling SSL for the Exchange ActiveSync virtual directory

Important To perform the following procedure, you must be a member of the Administrators group on the local computer, or you must have been delegated the appropriate authority. As a security best practice, log on to your computer by using an account that is not in the Administrators group, and then use the **Run as** command to run IIS Manager as an administrator. From the command prompt, type the following command:

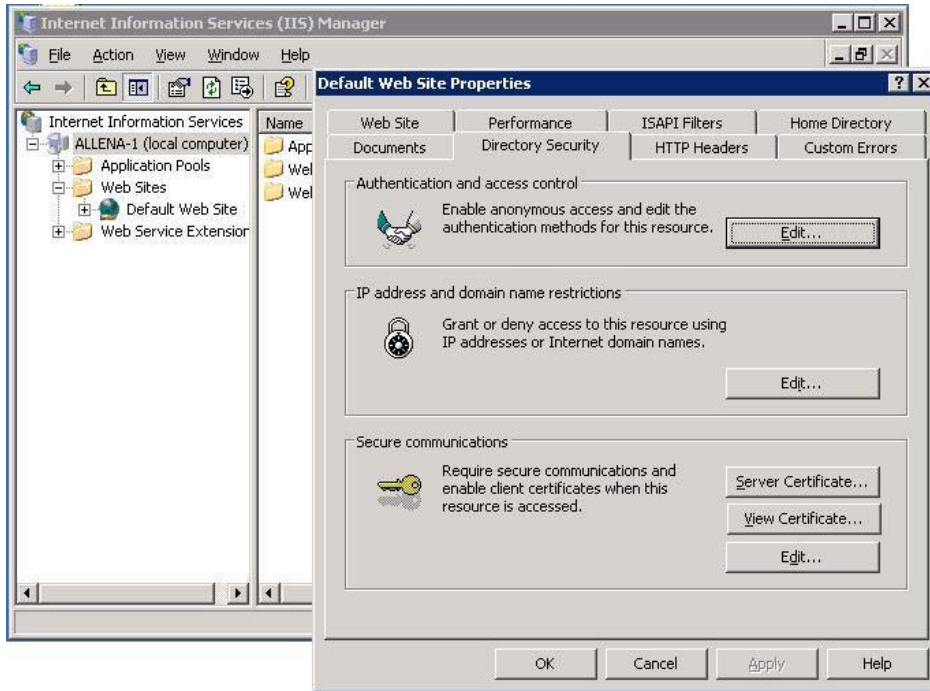
```
runas /user:administrative_accountname "mmc%systemroot%\system32\inetsrv\iis.msc"
```

Obtaining and Installing Server Certificates

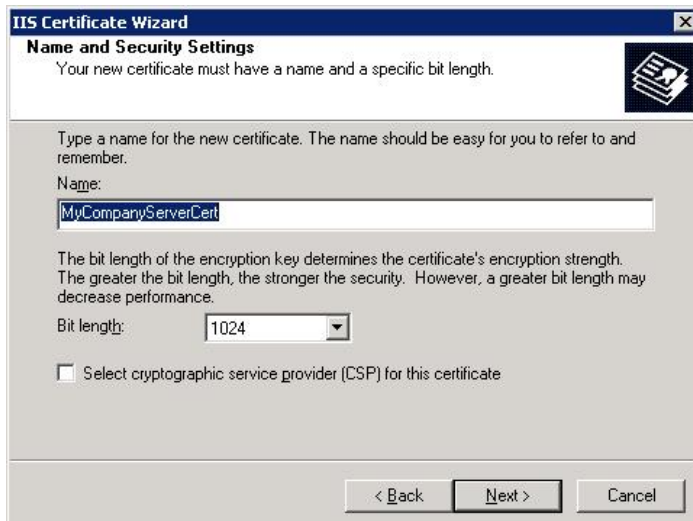
After you obtain a server certificate, you will install the server certificate, verify the installation of the server certificate, and back it up. When you use the Web Server Certificate Wizard to obtain and install a server certificate, the process is referred to as creating and assigning a server certificate.

To Obtain a Server Certificate From a CA

1. Log on to the Exchange server using an Administrator account.
2. Click **Start**, click **Programs**, click **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.



3. Double-click the *ServerName* to view the Web sites. Right-click **Default Web Site** and then click **Properties**.
4. Click to select the **Directory Security** tab. Under **Secure Communications**, click **Server Certificate**.
5. In the **Welcome Web Server Certificate Wizard** dialog box, click **Next**, click **Create a new certificate**, and then click **Next**.
6. Click **Prepare the request now, but send it later**, and then click **Next**.



7. In the **Name and Security Settings** dialog box, type a name for your server certificate (for example, type <Exchange_Server_Name>), click **Bit length of 1024**, and then click **Next**.

Note Ensure that **Select cryptographic service provider** is not selected.

8. In the **Organization Information** dialog box, type a name in the **Organization** text box (for example, type <Company_Name>) and in the **Organizational unit** text box (for example, type <IT Department>), and then click **Next**.
9. In the **Your Site's Common Name** dialog box, type the fully qualified domain name (FQDN) of your server or cluster for **Common name** (for example, type <domain.com>), and then click **Next**. This will be the domain name that your client mobile devices will access.
10. In the **Geographical Information** dialog box, click **Country/region** (for example, US), **State/province** (for example, <State>) and **City/locality** (for example, <City>), and then click **Next**.
11. In the **Certificate Request Filename** dialog box, keep the default of **C:\NewKeyRq.txt** (where C: is the location your OS is installed), and then click **Next**.
12. In the **Request File Summary** dialog box, review the information and then click **Next**. You should receive a success message when the certificate request is complete.



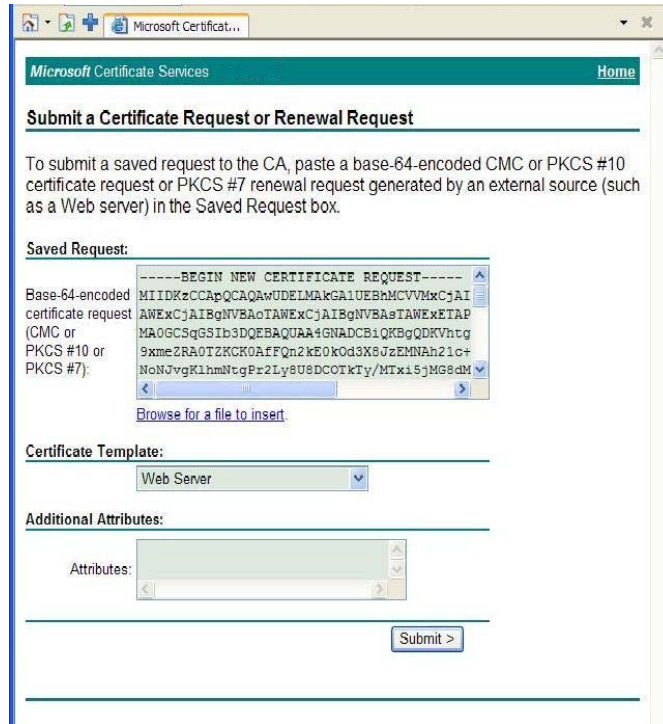
13. Click **Finish**.

Next, you must request a server certificate from a valid CA. To do this, you must access the Internet or an intranet, depending on the CA you choose, by using a properly configured Web browser.

The steps detailed here are for accessing your CA Web site. For a production environment, you will probably request a server certificate from a public trusted CA over the Internet.

To Submit the Certificate Request

1. Start **Microsoft® Internet Explorer**. Type the Uniform Resource Locator (URL) for the Microsoft CA Web site, http://<server_name>/certsrv/. When the Microsoft CA Web site page displays, click **Request a Certificate**, and then click **Advanced Certificate Request**.



2. On the **Advanced Certificate Request** page, click **Submit a certificate request by using a base-64 encoded PKCS#10 file, or submit a renewal request by using a base-64 encoded PKCS #7 file**.
3. On your local server, navigate to the location of the **C:\NewKeyRq.txt** file that you saved previously.
4. Double-click to open the **C:\NewKeyRq.txt** file in Notepad. Select and copy the entire contents of the file.
5. On the CA Web site, navigate to the **Submit a Certificate Request** page. If you are prompted to pick the type of certificate, select **Web Server**.
6. Click inside the **Saved Request** box, paste the contents of the file into the box, and then click **Submit**. The contents in the **Saved Request** box should look similar to the following example:

-----BEGIN NEW CERTIFICATE REQUEST-----

```
MIIDXzCCAsGCAQAwYmVLDLAgBGNVBAAMTI2toYXpZHM0LnJlZG1vbmQuY29ycC5taWNyb3NvZnQuY29tMR
EwDwYDVQQLewhNb2JpbG10eTEEMMAoGA1UEChMDTVRQRmAwDgYDVQQHEwdSZWRtb25kMRMwEwYDVQKI
EwpX
YXNoaW5ndG9uMQswCQYDVQQGEWJVVUzCBnZANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAs0sV2UZ1WAX2ou
+F5S34+6M3A32tJ5qp+c7z1iu4SMkcgebhnt2IMMeF5ZMD2IqfhWu49nu1vLtGHK5wWgHYTC3rTFabLZJ1
bNtXKB/BWwOsmSDYg/A7+oCZB4rHJmpc0Yh4Oj bQKkr64KM67r8jGEPYGMazf2DnUg3xUt9pbBECAwEAAa
CCAZkwGgYKKwYBBAGCNw0CAzEMFgo1LjAuMjE5NS4yMHsGCisGAQQBgjcCAQ4xbTBrMA4GA1UdDwEB/wQE
AwIE8DBEBgkqhkiG9w0BCQ8ENzA1MA4GCCqGSIb3DQMCAGIAgDAOBggqhkiG9w0DBAICAIAwBwYFKw4DAg
cwCgYIKoZiIhvcNAwCwEwYDVROlBAwCgYIKwYBBQUHAWewgf0GcisGAQQBgjcNAgIxge4wgesCAQEewgBN
AGkAYwByAG8AcwBvAGYAdAAgAFIAUwBBACAAUwBDAGgAYQBuAG4AZQBzACAAQwByAHkAcAB0AG8AZwByAG
EACABoAGkAYwAgAFAAacgBvAHYAaQBkAGUAcgoBiQCO5g/Nk+lsuAJZideg15faBLqe4jiiytYeVBAPxLrt
UlyWEQuWdPeEfVr0GWvsjQGwn+WC5m9kVNmcLVsx41QtGDxtuETFOD6dsi/M9wmEy8bsbcNHXs+sntX56Ac
CxBXh1ALaE4YaE6e/zwmE/0/Cmyje3a2o1E5r1k1FFI1KTDwAAAAAAAAAAMA0GCSqGSIb3DQEBBQUAA4GB
AAr7zjg2ykZoFUyt1+EgK106jRsLxJcoqj0oEg575eAlUgbN1e2i/L2RWju7cgo9W7uwppBIAeqd6LJ6s1
```

BRpZz0yeJTDzGIXByG5O6kouk+0H+WHCj2yI30zik8aSyCQ3rQbNvHoURDmWqv9Rp1BDC1SNQLEzDgZjKP
rsGZAVLb

-----END NEW CERTIFICATE REQUEST-----

7. On the **Certificate Issued** page, click **DER encoded**, and then click **Download** certificate.
8. In the **File Download** dialog box, click **Save** this file to disk, and then click **OK**. Keep the default setting to save the file to the desktop, and click **Save**.
9. Close Internet Explorer.

At this point, a server certificate exists on your desktop that can be imported into the Exchange server certificate store.

Next, you must install the certificate.

To Install the Certificate

1. Start **Internet Information Service (IIS) Manager** and expand *<DomainName>*
2. Right-click **Default Web Site**, and then click **Properties**. In the **Properties** dialog box, select the **Directory Security** tab. Under **Secure Communication**, click **Server Certificate**.
3. In the **Certificate Wizard** dialog box, click **Next**.
4. Select **Process the Pending Request and install the certificate**. Click **Next**.
5. Navigate to, or type the location and file name for the file containing the server certificate, certnew.txt, that is located on the desktop, and then click **Next**.
6. Choose the **SSL port** that you wish to use. **Port 443** is the default and is recommended.
7. In the **Certificate Summary Information** dialog box, click **Next**, and then click **Finish**.

Validating Installation

To verify the installation, you can view the server certificate.

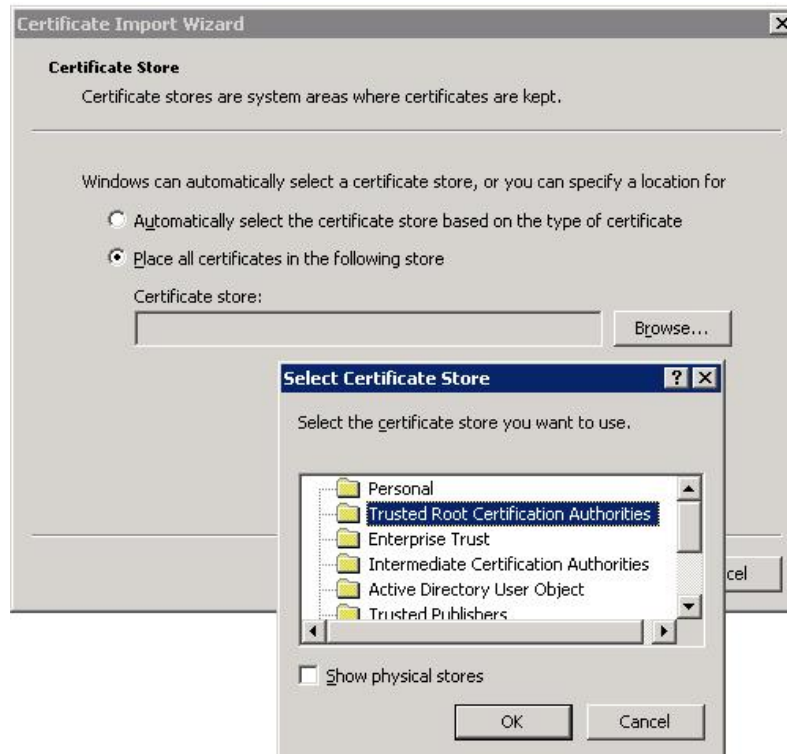
In the **Properties** dialog box, click **Directory Security**, and under **Secure Communication**, click **View Certificate**. At the bottom of the **Certification** dialog box, a message displays indicating that a private key is installed, if a certificate is available.



In order for the authentication to function, you must add the CA to the Trusted Root CA list.

To Add a CA to the Trusted Root CA List

1. Start **Internet Explorer** and type the URL for your **Certificate Authority**. For example, if you received your server certificate from the CA that you configured earlier, type `http://<server_name>/certsrv`.
2. Click **Download a CA certificate, certificate chain, or CRL**, and then click **Download CA certificate** on the next page as well. In the **File download** dialog box, click **Save this file to disk**, and then click **OK**.



3. Type a server certificate **Name**, for example, `<certnewca.cer>` and save the file to the desktop.
4. Navigate to the desktop. Right-click the file that you created in step 3, and then click **Install Certificate**. In the **Certificate Import Wizard** dialog box, click **Next**.
5. Click **Place all certificates in the following store**, and then click **Browse**. Select the **Trusted Root Certification Authorities** folder, and then click **OK**.
6. Click **Next**. A dialog box that says that the certificate is being added to the trusted certificate store appears; click **Yes** to this dialog box. Click **Finish**, and the message "import successful" displays.

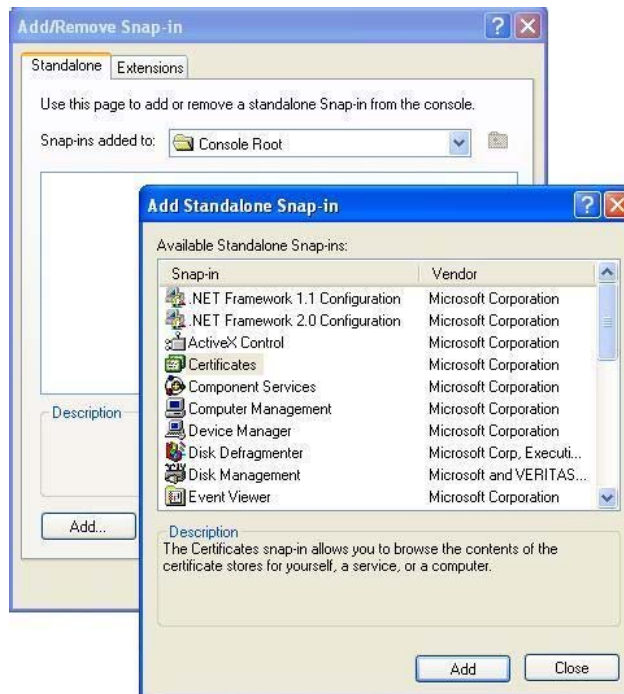
Backing up Server Certificates

You can use the Web Server Certificate Wizard to back up server certificates. Because IIS works closely with Windows, you can use Certificate Manager, which is called **Certificates** in Microsoft Management Console (MMC), to export and to back up your server certificates.

If you do not have Certificate Manager installed in MMC, you must add Certificate Manager to MMC.

To add Certificate Manager to MMC

1. From the **Start** menu, click **Run**.
2. In the **Open** box, type **mmc**, and then click **OK**.
3. On the **File** menu, click **Add/Remove Snap-in**.
4. In the **Add/Remove Snap-in** dialog box, click **Add**.
5. In the **Available Standalone Snap-ins** list, click **Certificates**, and then click **Add**.



6. Click **Computer Account**, and then click **Next**.
7. Click the **Local computer** (the computer that this console is running on) option, and then click **Finish**.
8. Click **Close**, and then click **OK**.

With Certificate Manager installed, you can back up your server certificate.

To Back Up Your Server Certificate

1. Locate the correct certificate store. This store is typically the **Local Computer** store in **Certificate Manager**.
Note When you have **Certificate Manager** installed, it points to the correct **Local Computer** certificate store.
2. In the **Personal store**, click the server certificate that you want to back up.
3. On the **Action** menu, point to **All tasks**, and then click **Export**.
4. In the **Certificate Manager Export Wizard**, click **Yes, export the private key**.
5. Follow the wizard default settings, and type a password for the server certificate backup file when prompted.

Note Do not select **Delete the private key if export is successful**, because this option disables your current server certificate.

6. Complete the wizard to export a backup copy of your server certificate.

After you configure your network to issue server certificates, you must protect your Exchange front-end server and the services for your Exchange server by requiring SSL communication to the Exchange front-end server. The following section describes how to enable SSL for your default Web site.

Enabling SSL for the Default Web Site

After you obtain an SSL certificate to use either with your Exchange front-end server on the default Web site or on the Web site where you host the \RPC, \OMA, \Microsoft-Server-ActiveSync, \Exchange, \Exchweb, and \Public virtual directories, you can enable the default Web site to require SSL.

Note The \Exchange, \Exchweb, \Public, \OMA, and \Microsoft-Server-ActiveSync virtual directories are installed by default on any Exchange Server 2003 SP2 installation. The \RPC virtual directory for RPC over HTTP communication is installed manually when you configure Exchange Server 2003 SP2 to support RPC over HTTP.

For information about how to set up Exchange Server 2003 to use RPC over HTTP, see Exchange Server 2003 RPC over HTTP Deployment Scenarios at <http://go.microsoft.com/fwlink/?LinkId=62656>.

To Require SSL

1. In the **Internet Information Services (IIS) Manager**, select the **Default Web site** or the Web site where you are hosting your Exchange Server 2003 services, and then click **Properties**.
2. On the **Directory Security** tab, in **Secure Communications**, click **Edit**.



3. In **Secure Communications**, click the **Require Secure Channel (SSL)** check box. Click **OK**.

-
4. Depending upon your installation, the **Inheritance Overrides** dialog box may appear. Select the virtual directories that should inherit the new setting, and then click **OK**.
 5. On the **Directory Security** tab, click **OK**.

After you complete this procedure, all virtual directories on the Exchange front-end server on the default Web site are configured to use SSL.

Single Server Configuration (Optional)

If you have forms-based authentication set up on an Exchange organization for Exchange ActiveSync on an Exchange Server with no back-end, additional configurations may be required. For more information about these configurations, see the following article in the Microsoft Knowledge Base:

Exchange ActiveSync and Outlook Mobile Access errors occur when SSL or forms-based authentication is required for Exchange Server 2003

<http://go.microsoft.com/fwlink/?LinkId=62660>

Important Exchange Server 2003 SP2 forms-based authentication does not allow you to set the default domain setting in IIS to anything other than the default domain setting of \. This restriction is in place in order to support user logons that use the User Principle Name format. If the default domain setting in IIS is changed, Exchange System Manager resets the default domain setting to "\" on the server. You can change this behavior by customizing the Logon.asp page in the OWA virtual directory in IIS to specify your domain or to include a list of domain names.

Note If you customize the Logon.asp page in the OWA virtual directory in IIS, your changes may be overwritten if you upgrade or re-install Exchange Server 2003 SP2.

Configuring Basic Authentication

The Exchange ActiveSync Web site supports SSL connections as soon as the server certificate is bound to the Web site. However, users still have the option to connect to the Web site by using a non-secure connection. You can require all client mobile devices to successfully negotiate an SSL link before connecting to the Exchange ActiveSync Web site directories.

We also recommend that you enforce basic authentication on all HTTP directories that the ISA Server makes accessible to external users. In this way, you can take advantage of the ISA Server feature that enables the relay of basic authentication credentials from the firewall to the Exchange ActiveSync Web site.

Require SSL Connection to the Exchange ActiveSync Web Site Directories

This prevents all non-authenticated communications from reaching the Exchange ActiveSync Web site and significantly improves the level of security.

Note If you plan to use Certificate Authentication instead of basic configuration, you must deploy SSL by following the instructions for configuring SSL for Exchange ActiveSync in Appendix A. Deploying Exchange ActiveSync Certificate-Based Authentication.

You can repeat these steps with the /Exchange, /Exchweb, /Public, and /OMA directories found in the left pane of the **IIS MMC** console. This can be done to require SSL on the five Web site directories that you can make accessible to remote users:

/Exchange

/ExchWeb

/Public

/OMA

/Microsoft-Server-ActiveSync

To Require an SSL Connection to the Exchange ActiveSync Web Site Directories

1. Click **Start**, point to **Administrative Tools** and then click **Internet Information Service (IIS) Manager**. In **Internet Information Services (IIS) Manager**, expand your server name and then expand the **Default Web Site** node in the left pane of the console.
2. Right-click on the **Microsoft-Server-ActiveSync** directory so that it is highlighted, and then click **Properties**.
3. Click **Directory Security**. In the **Authentication and access control** frame, click **Edit**.
4. In the **Authentication Methods** dialog box, click to clear all check boxes except for the **Basic authentication** (password is sent in clear text) check box. Place a check mark in the **Basic authentication** check box.



Note On the back-end (mailbox) server, you must enable **Integrated Windows Authentication** in order for Exchange ActiveSync to work. Only disable it on the front-end Exchange server.

5. Click **Yes** in the dialog box that warns you that the credentials should be protected by SSL. In the **Default domain** text box, type in your domain name.
6. Click **OK**.
7. In the **Exchange Properties** dialog box, click **Apply**, and then click **OK**.
8. After you have required basic authentication on the directories that you have chosen, close the **Internet Information Services (IIS) Manager** console.

Configure or Update RSA SecurID Agent (Optional)

If you have chosen to deploy RSA SecurID as an additional security layer, you should set up your Exchange server as an Agent Host within the RSA ACE/Server's database at this point.

Note There have been limitations between IIS 6.0 and the RSA/ACE Agent. Be sure to update your RSA/ACE Agent for better compatibility. For more information, see the RSA Security Web site at <http://go.microsoft.com/fwlink/?LinkId=63273>.

Protecting IIS by Using UrlScan and IIS Lockdown Wizard

Before you expose servers to the Internet, we recommend that you protect IIS by turning off all features and services except those that are required. In Windows 2003 Server, many IIS features are already disabled unless they are required by the server. On Microsoft Windows 2000 Server, you can protect IIS by downloading and running the IIS Lockdown Wizard.

For more information about how to install and use IIS Lockdown Wizard, see the following Microsoft Knowledge Base article:

How to install and use the IIS Lockdown Wizard <http://go.microsoft.com/fwlink/?LinkId=62662>.

The IIS Lockdown Tool (version 2.1) is available at the following Microsoft Web site:

IIS Lockdown Tool (version 2.1) <http://go.microsoft.com/fwlink/?LinkId=62663>

Note To help maximize the security of your Exchange servers, apply all the required updates both before and after you apply the IIS Lockdown Wizard. The updates help the servers remain protected against known security vulnerabilities.

The IIS Lockdown Wizard helps you disable those IIS features and services that are unnecessary to the server software that you are running. To provide multiple layers of protection against attackers, the IIS Lockdown Wizard also contains UrlScan, which analyzes HTTP requests as IIS receives them and rejects any suspicious requests.

The IIS Lockdown Wizard also contains a configuration template for Exchange that turns off unwanted features and services. To use this configuration template, run the IIS Lockdown Wizard, select the Exchange template, and then change or accept the default configuration options.

Download UrlScan separately if you want to run it on Windows Server 2003 SP2. A list of UrlScan features and functionality beyond those provided by IIS 6.0 is available at <http://go.microsoft.com/fwlink/?LinkId=62665>

The UrlScan application is installed in the folder **<drive:>\<Windows directory>\system32\inetsrv\urlscan**.

UrlScan must be correctly configured for use with Exchange Server 2003 SP2. For full details about how to configure UrlScan for use with Exchange Server 2003 SP2, see the following Microsoft Knowledge Base article:

Fine-tuning and known issues when you use the UrlScan tool in an Exchange Server 2003 SP2 environment

<http://go.microsoft.com/fwlink/?LinkId=62666>

Required UrlScan Settings

The following section contains further information about why certain UrlScan settings are required. Unless you configure the following settings in the **Urlscan.ini** file immediately after you run the IIS Lockdown Wizard, you may experience problems with OWA functionality. Exchange ActiveSync and OWA work in similar ways. If OWA is functioning correctly, then the basic infrastructure for Exchange ActiveSync should function correctly as well.

-
- **Allow Dot In Path** Ensure that this setting is set to "1" so that OWA attachments can be accessed and that earlier-version browsers can use OWA.
 - **File Extensions** By default, .htr files are disabled. If this file type is disabled, the OWA Change Password feature does not function.
 - **Deny Uri Sequences** In the [DenyUriSequences] section, sequences that are explicitly blocked can potentially affect access to OWA. Any mail item subject or mail folder name that contains any of the following character sequences is denied access:
 - Period (.)
 - Double period (..)
 - Period and forward slash (./)
 - Backslash (\)
 - Percent sign (%)
 - Ampersand (&)

If you have additional problems when you attempt OWA requests with UrlScan enabled, check the Urlscan.log file for the list of requests that are being rejected.

To Configure Urlscan.ini

1. In the Windows\System32\Inetsrv\Urlscan folder, edit the file Urlscan.ini by using Notepad.
2. Remove the following characters from the **[DenyUriSequences]** section:
 - ..
 - ./
 - \
 - %
 - &
 - :
3. Review the **[AllowVerbs]** section and make sure that it contains the following Verbs:
 - GET
 - POST
 - PROPFIND
 - PROPPATCH
 - BPROPPATCH
 - MKCOL
 - DELETE
 - BDELETE
 - BCOPY
 - MOVE
 - SUBSCRIBE
 - BMOVE
 - POLL
 - SEARCH
 - HEAD
 - PUT
 - COPY
 - OPTIONS

-
- RPC_OUT_DATA
 - RPC_IN_DATA
 - X-MS-ENUMATTS
 - LOCK
 - UNLOCK
4. **Save** and close the file.

Step 4 - Protect Communications Between the Exchange Server 2003 SP2 Server and Other Servers

After you enable the security features to help secure the communications between your client mobile devices and the Exchange front-end server, you also must protect the communications between the Exchange front-end server and the back-end servers. We recommend that you use IPSec to encrypt IP traffic.

HTTP, POP, and IMAP communications between the front-end server and any server with which the front-end server communicates (such as back-end servers, domain controllers, and global catalog servers) is not encrypted. When the front-end and back-end servers are in a trusted physical or switched network, the absence of encryption is not a concern. However, if front-end and back-end servers are kept in separate subnets, network traffic may pass over unsecured areas of the network. The security risk increases when there is greater physical distance between the front-end and back-end servers. In such cases, we recommend that this traffic be encrypted to protect passwords and data.

Using IPSec to Encrypt IP Traffic

Windows 2000 and Windows Server 2003 both support Internet Protocol security (IPSec), which is an Internet standard that allows a server to encrypt all IP traffic except IP traffic that uses broadcast or multicast IP addresses. Generally, IPSec is used to encrypt HTTP traffic; however, you can also use IPSec to encrypt Lightweight Directory Access Protocol (LDAP), RPC, POP, and IMAP traffic. With IPSec, you can:

- Configure two servers that are running Windows 2000 or Windows Server 2003 to require trusted network access.
- Use a cryptographic checksum on every packet to transfer data that is protected from modification.
- Encrypt any traffic between the two servers at the IP layer.

In a front-end and back-end topology, you can use IPSec to encrypt traffic between the front-end and back-end servers that would otherwise not be encrypted.

For more information about configuring IPSec with firewalls, see the following Microsoft Knowledge Base article:

How to Enable IPSec Traffic Through a Firewall <http://go.microsoft.com/fwlink/?LinkId=62667>

For more information about using IPSec to protect communications, consult the IPSec Information Center at <http://go.microsoft.com/fwlink/?LinkId=62668>

Step 5 - Install and Configure an ISA Server 2004 Environment or Other Firewall

Internet Security and Acceleration (ISA) Server 2004 is the advanced application-layer firewall, virtual private network (VPN), and Web cache solution that improves network security and performance.

This section discusses steps for deployment of Exchange Server 2003 SP2 mobile messaging in an ISA environment. You can also use this information to determine what is needed if you are using another firewall service. During this process, you will:

- Install ISA Server 2004
- Create the Exchange ActiveSync publishing rule using Web publishing
Open Port 443 as a Web Listener
- Configure the host file entry
- Set the ISA Server 2004 idle session timeout to 1800 seconds (30 minutes)
Note Increasing the timeout values maximizes performance of the Direct Push technology and optimizes device battery life.
- Test OWA and Exchange ActiveSync
Note If you plan to use Certificate Authentication, you must use Server Publishing or tunneling to create your Exchange ActiveSync publishing rule. See the instructions in Appendix A. Deploying Exchange ActiveSync Certificate-Based Authentication.

Refer to the Best Practices section, Architecture of a Standard ISA Network for background on network architecture and SSL setup.

If you have ISA Server 2000, see Using ISA Server 2000 with Exchange Server 2003 at <http://go.microsoft.com/fwlink/?LinkId=62670>.

Installing ISA Server 2004

Install ISA Server 2004 as a stand-alone firewall on your server. Do not install ISA Server 2004 as part of an ISA Server array, because this requires domain membership. Your ISA server should not be a member server in your Microsoft Windows forest because, if the ISA server is compromised by attacks from the Internet, the attackers can gain access to domain resources if those resources are in the same domain. Additionally, minimize the number of ports that are open to your internal network. Member servers require additional ports for activities, such as talking to domain controllers.

Note We recommend that you set up both Exchange ActiveSync and OWA on the ISA Server. Having OWA published as well as Exchange ActiveSync will give you greater troubleshooting capabilities.

To Install ISA Server 2004

- Install and configure Windows Server 2003 on the firewall computer.
After you install and configure Windows Server 2003 on the firewall computer, go to Windows Update and install all critical security hot fixes and service packs for Windows Server 2003.
- Move the server to a workgroup.
Remove the server from any domains that it is a member of, and place it in a workgroup.
- Install ISA Server 2004.
Export the OWA SSL Cert from the Exchange front-end OWA server to a file.

Creating the Exchange ActiveSync Publishing Rule Using Bridging

Web publishing rules determine how ISA Server 2004 intercepts incoming requests for Hypertext Transfer Protocol (HTTP) objects on an internal Web server, and how ISA Server 2004 responds on behalf of the internal Web server.

During this process, you will be required to provide names for the publishing rule itself, the internal and external Web servers, and the Web Listener. Read through these instructions and determine appropriate names before you begin.

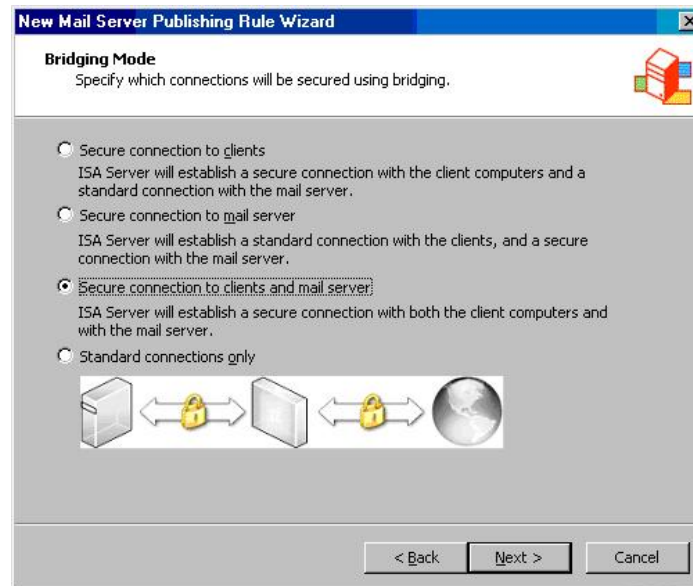
For more information, see Publishing Web Servers Using ISA Server 2004 at <http://go.microsoft.com/fwlink/?LinkId=62672>.

Note If you plan to use Certificate Authentication, you must use Server Publishing or tunneling to create your Exchange ActiveSync publishing rule. Skip the next step and follow the instructions in Appendix A. Deploying Exchange ActiveSync Certificate-Based Authentication.

After you create the Web publishing rule, you will create and configure the Web Listener, complete the Web site rule, and update the firewall policy.

To Create and Name the Exchange ActiveSync Web Publishing Rule

1. In the **Microsoft Internet Security and Acceleration Server 2004** management console, expand the server name and click the **Firewall Policy** node.
2. Right-click the **Firewall Policy** node, point to **New** and then click **Mail Server Publishing Rule**.
3. On the **Welcome to the New Mail Server Publishing Rule Wizard** page, type a name for the rule in the **Mail Server Publishing Rule name** text box. Click **Next**.
4. On the **Select Access Type** page, select the **Web client access: Outlook Web Access (OWA), Outlook Mobile Access, Exchange Server ActiveSync** option and then click **Next**.
5. On the **Select Services** page, click to select the **Exchange ActiveSync** check box. Confirm that there is a check mark in the **Enable high bit characters used by non-English character sets** check box. (If you expect users to read only English-based character sets, you can disable this option by clicking to clear the check box.) For troubleshooting purposes, we recommend that you click to select the **Outlook Web Access** check box. Click **Next**.



6. On the **Bridging Mode** page, click the **Secure connection to clients and mail server** option, and then click **Next**.
7. The **Secure connection to clients and mail server** option creates a Web publishing rule that provides the SSL connection from the client mobile device to the Exchange Web site. This prevents the traffic from moving in the clear, where an intruder can sniff the traffic and intercept valuable information.
8. On the **Specify the Web Mail Server** page, type the name for the **Internal Web site** in the mail server text box, and then click **Next**.
9. This is the name used for the Exchange Server 2003 Web site on the internal network. The name in the request that the ISA Server 2004 firewall sends to the Exchange server on the internal network should be the same as the name on the certificate that is installed on the Exchange ActiveSync Web site.
10. On the **Public Name Details** page, click the **This domain name (type below):** option in the **Accept requests for** list. In the **Public name** box, type the name that external users will use to access the Exchange ActiveSync Web site, and then click **Next**.

All incoming Web requests must be received by a Web Listener. A Web Listener may be used in multiple Web publishing rules.

To Create the Web Listener

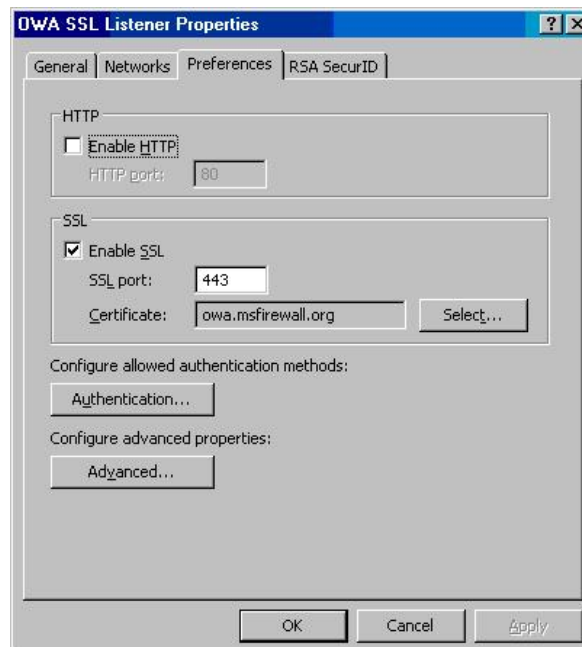
1. On the **Select Web Listener** page, click **New**.
With the ISA Server 2004 Web Listener, you have several options:
 - You can create a separate Web listener for SSL and non-SSL connections on the same IP address.
 - Based on the number of addresses that are bound to the external interface of the ISA Server 2004 firewall, you can configure separate settings for each listener. The Web Listener settings are not global.
2. On the **Welcome to the New Web Listener Wizard** page, type a name for the Web Listener in the **Web listener name** text box, and then click **Next**.
3. On the **IP Addresses** page, select the **External** check box, and then click **Address**.
4. In the **External Network Listener IP Selection** dialog box, select the **Specified IP addresses on the ISA Server computer in the select network** option. In the

-
- Available IP Addresses** list, click on the external IP address that are on the ISA Server 2004 firewall and that you want to listen for incoming requests to the OWA Web site, and then click **Add**. The external IP addresses that you selected now appear in the **Selected IP Addresses** list. Click **OK**.
5. On the **IP Addresses** page, click **Next**.
 6. On the **Port Specification** page, click to clear the **Enable HTTP** check box, select the **Enable SSL** check box, and leave the SSL port number at **443**.
Note By configuring this Web listener to use only SSL, you can configure a second Web listener that is dedicated for non-SSL connections with different settings.
 7. Click **Select**. In the **Select Certificate** dialog box, click the Exchange ActiveSync Web site certificate that you imported into the ISA Server 2004 firewall computer's certificate store, and click **OK**.
Note This certificate will appear in the **Select Certificate** dialog box only after you have installed the Web site certificate into the ISA Server 2004 firewall computer's certificate store. In addition, the certificate must contain the private key. If the private key was not included, it will not appear in this list.
 8. On the **Port Specification** page, click **Next**.
 9. On the **Completing the New Web Listener** page, click **Finish**.

The next step is to configure the Web Listener so that no authentications are configured.

To Configure the Web Listener

1. The details of the Web Listener now appear on the **Select Web Listener** page. Click **Edit**.
2. In the **SSL Listener Properties** dialog box, click the **Preferences** tab.
3. On the **Preferences** tab, click **Authentication**.



4. In the **Authentication** dialog box, click to clear the **Integrated** check box. In the **Microsoft Internet Security and Acceleration Server 2004** dialog box warning that no authentication methods are currently configured, click **OK**. Do not select the **OWA-Forms Based Authentication** check box.
5. In the **SSL Listener Properties** dialog box, click **Apply**, and then click **OK**.
6. On the **Select Web Listener** page, click **Next**.
7. On the **User Sets** page, accept the default entry **All Users**, and then click **Next**.

Note Accepting the **All Users** default entry does not enable all users to access the Exchange Web site. Only users who can authenticate successfully will be able to access the Exchange Web site. The actual authentication is done by the Exchange Web site, which uses the credentials that the ISA Server 2004 firewall has forwarded to it. The ISA Server 2004 firewall and the Exchange Web site cannot both authenticate the user. This means that you must allow **All Users** access to the rule. An exception to this rule is when users authenticate to the ISA Server 2004 firewall itself by using client certificate authentication.
8. On the **Completing the New Mail Server Publishing Rule Wizard** page, click **Finish**.

As a final step, you will allow the Exchange Web site to receive the actual IP address of the mobile device.

To Complete the Web Site Rule and Update the Firewall Policy



1. Right-click the **EAS Web site rule** in the **Details** pane of the ISA Server Management console, and then click **Properties**.
2. In the **Web site Properties** dialog box, click the **To** tab. On the **To** tab, click **Requests appear to come from the original client** option. This option allows the Exchange Web site to receive the actual IP address of the external client mobile device. This feature enables Web logging add-ons installed on the OWA Web site to use this information when creating reports.

3. Click **Apply**, and then click **OK**.
4. Click **Apply** to save the changes and update the firewall policy.
5. In the **Apply New Configuration** dialog box, click **OK**.

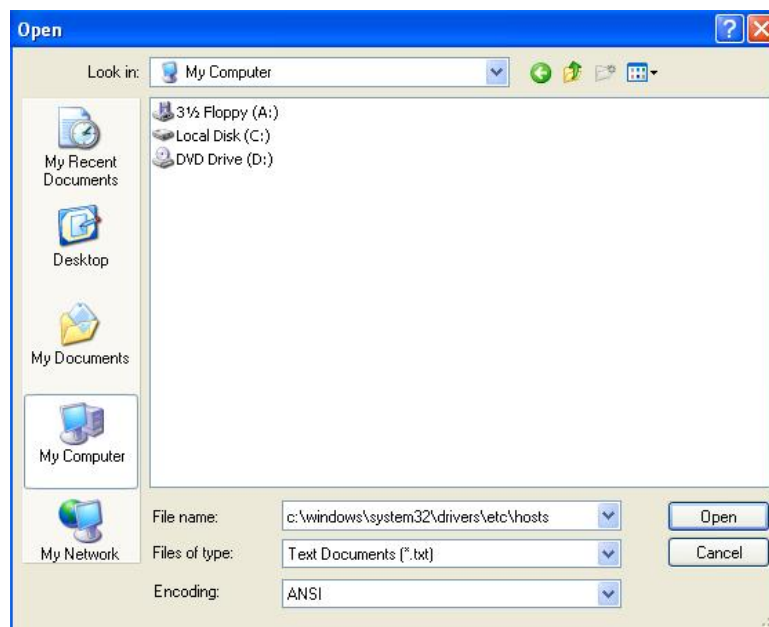
The SSL Web site is now available on the external IP address of the ISA server. You may have to make host record changes on your externally-accessible DNS server to map the IP address of the ISA server's external interface to the host record of the SSL Web site.

Configuring the Host File Entry

The next step is to create a HOSTS file entry on the ISA Server 2004 firewall computer so that it resolves the name that you specified for your internal Web mail server to the IP address of the Exchange server that is on the Internal network.

Note You could also use a split DNS infrastructure for this purpose. However a HOSTS file entry is easier to create. On a production network, you would create a split DNS infrastructure so that the ISA Server 2004 firewall would resolve the FQDN of the OWA Web site to the IP address that the Exchange Server uses on the internal network.

To Configure the Host File Entry



1. Click **Start**, and then click **Run**. In the **Run** dialog box, type **Notepad** in the **Open** text box, and then click **OK**.
2. Click the **File** menu, and then click **Open**. In the **Open** dialog box, type **c:\windows\system32\drivers\etc\hosts** in the **File name** text box, and then click **Open**.
3. Add the following line to the **HOSTS** file: **10.0.0.2 <your firewall name>**
4. Navigate your cursor to the end of the line so that the insertion point sits on the next line, and then press **Enter**.
5. Click **File**, and then click **Exit**.
6. In **Notepad**, save the changes to the file, and then close **Notepad**.

Modifying the ISA Server 2004 idle session timeout

In this step, you will modify the idle session timeout time to accommodate the time required for successful function of the Direct Push technology.

For more information about modifying the idle session timeout time, see the Configuring your firewall for optimal Direct Push performance section in the Best Practices section of this document.

To Set the ISA Server 2004 Idle Session Timeout to 1800 Seconds

1. In the console tree of **ISA Server Management**, click **Firewall Policy**.
2. On the **Toolbox** tab, click **Network Objects**.
3. From the list of folders, expand the **Web Listeners** node, and view the **Properties** of appropriate Web Listener.
4. Select the **Preferences** tab and then click the **Advanced...** button.
5. Modify the **Connection Timeout** from the default 120 seconds (2 minutes) to 1800 seconds (30 minutes).
6. Click **OK** twice to accept the change.
7. Click **Apply** to make these changes.

Testing OWA and Exchange ActiveSync

After you complete the configuration, you should test the following features that you configured:

- Test OWA (Optional)
- Test Exchange ActiveSync

An external client mobile device can access the OWA server as long as it can resolve an FQDN to the external IP address of the ISA server. This is usually achieved by registering a public Internet domain name with a public DNS server that maps the Web site name to the external IP address of the ISA Server.

If you have set up OWA according to the instructions in the Exchange Server 2003 Client Access Guide at <http://go.microsoft.com/fwlink/?LinkId=62628>, you can test it by using the following process.

Testing OWA (if installed)

To test the deployment in a lab environment, specify the Web site host name resolution information by using Notepad, in the client mobile device **hosts** file located under the following path: **system32\drivers\etc\hosts** in the **Windows installation** directory.

To Test OWA (if installed)

1. To connect to the OWA Web site from the external client mobile device, type the Web address as that you specified during setup. Be certain to specify **https** in the URL.
2. When you connect, you should see a logon page requesting credentials and the session type (public or private). You must provide this information before you can access your mailbox.
3. If you have set time-outs or blocked attachments, you can test those features by leaving the browser inactive for a period of time and then trying to access mail, and by trying to open or save attachments.

Testing Exchange ActiveSync

You can configure a mobile device to connect to your Exchange server by using Exchange ActiveSync, and to make sure that ISA Server 2004 and Exchange ActiveSync are working properly.

As an alternative, you can test Exchange ActiveSync by using Internet Explorer.

To test Exchange ActiveSync by Using Internet Explorer

1. Open **Internet Explorer**. In the **Address** bar, type **https://published_server_name/Microsoft-Server-Activesync**, where *published_server_name* is the published name of your OWA server (the name your end users will type).
2. Type the user name and information that you want to authenticate.
3. If you receive an **Error 501/505 "Not implemented" or "Not supported"** error message, ISA Server 2004 and Exchange ActiveSync are working together properly.

Step 6 - Configure and Manage Mobile Device Access on the Exchange Server

The Messaging and Security Feature Pack for Windows Mobile 5.0 enables Windows Mobile 5.0-based devices to be managed by Microsoft Exchange Server 2003 SP2. With the combination of the management capabilities and the security and configuration protocols, most of the administration of the mobile devices happens on the Exchange Server or on the Mobile Administration Web tool.

You can do the following on your Exchange Server:

- Enable mobile access
- Configure security settings
- Monitor mobile performance on your Exchange server

Enabling Mobile Access

With your network configured, you can use the Exchange Server System Manager to do the following:

1. Enable Exchange ActiveSync for All Users
2. Enable User Initiated Synchronization
3. Enable Direct Push for All Users
4. Enable Up-to-date Notifications (Optional)

Enable Exchange ActiveSync for All Users

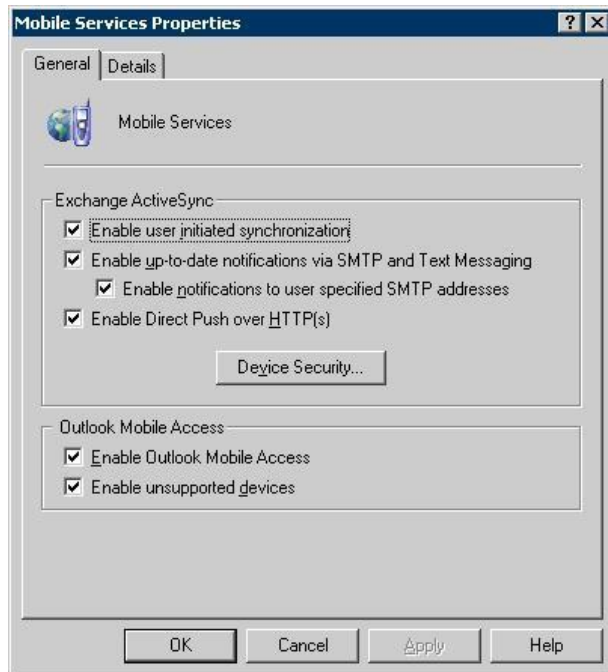
To enable and disable Exchange ActiveSync for your organization, use Exchange System Manager. With the Exchange Server 2003 SP2 installation, Exchange ActiveSync is enabled for all client mobile devices.

However, whenever you add new users to your organization and you want to enable them to use Exchange ActiveSync to access Exchange, use Active Directory Users and Computers to modify the settings for a user or group of users.

The Exchange ActiveSync feature allows users to synchronize their Exchange information with a mobile device.

To Enable Exchange ActiveSync for All Users

1. On the **Start** menu, point to **Programs**, point to **Microsoft Exchange**, and then click **System Manager**.
2. In the console tree, double-click **Global Settings**, right-click **Mobile Services** and then click **Properties**.



3. In **Mobile Services Properties**, under **Exchange ActiveSync**, select from the following:
 - Select the **Enable user initiated synchronization** check box to enable your users to synchronize their Exchange information with their mobile device.
 - Select the **Enable up-to-date notifications via SMTP and Text Messaging** check box to allow users to receive notifications through SMTP in order to keep their device up to date with information on their Exchange server. To allow users to use their own wireless service provider, select the **Enable notifications to user-specified SMTP addresses** check box.
 - Select the **Enable Direct Push over HTTP(s)** check box to allow users to receive notifications through HTTP to keep their device up to date with information on their Exchange server.
4. Click **OK** to save these settings.

Enable User-Initiated Synchronization

Enabling user-initiated synchronization for your mailbox-enabled recipients enables those recipients to synchronize their mailbox using wireless devices. Use the Exchange Features tab to enable this functionality for each user.

To Enable User-Initiated Synchronization

1. On the **Start** menu, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. In the console tree, expand the domain. Double-click **Users**, or double-click the node that contains the recipient information you want to modify.
3. In the details pane, double-click the user for whom you want to enable user initiated synchronization.
4. On the **Exchange Features** tab, under **Mobile Services**, select **User Initiated Synchronization**, and then click **Enable**.

Enable Up-to-date Notifications (Optional)

If you have an existing mobile messaging setup that includes devices that do not support Direct Push technology, you may want to enable this function.

Enabling up-to-date notifications for your mailbox-enabled recipients allows them to keep the data on their wireless devices up to date. Use the Exchange Features tab to enable this functionality for each user.

Note To use up-to-date notifications, you must also enable user initiated synchronization.

To Enable Up-to-date Notifications

1. On the **Start** menu, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. In the console tree, expand the domain. Double-click **Users**, or double-click the node that contains the recipient information you want to modify.
3. In the details pane, double-click the user for whom you want to enable up-to-date notifications.
4. On the **Exchange Features** tab, under **Mobile Services**, ensure that **User Initiated Synchronization** is enabled.
5. Under **Mobile Services**, select Up-to-date **Notifications**, and then click **Enable**.

Configuring Security Settings for Mobile Devices

You can specify security options for your users who connect to Exchange Server using mobile devices. With the Exchange System Manager, you can set the password length and strength as well as controlling the inactivity time and number of failed attempts before the device is wiped.

For more information about setting security policies, see Best Practice: Determine and Deploy a Device Password Policy in this document.

Note The term password referenced in this topic refers to the password a user enters to unlock his or her mobile device. It is not the same as a network user password.

The following are the options you can use to set your security policies:

- **Minimum password length (characters)** Use this option to specify the required length of the user's device password. The default setting is 4 characters. You can specify a password length of 4 to 18 characters.
- **Require both numbers and letters** Use this option if you want to require that users choose a password with both numbers and letters. This option is not selected by default.
- **Inactivity time (minutes)** Use this option to specify if you want your users to log on to their devices after a specified number of minutes of inactivity. This option is not selected by default. If selected, the default setting is 5 minutes.
- **Wipe device after failed (attempts)** Use this option to specify if you want the device memory wiped after multiple failed logon attempts. This option is not selected by default. If selected, the default setting is 8 attempts.
- **Refresh settings on the device (hours)** Use this option to specify how often you want to send a provision request to devices. This option is not selected by default. If selected, the default setting is every 24 hours.
- **Allow access to devices that do not fully support password settings** Select this option if you want to allow devices that do not fully support the device security settings to be able to synchronize with Exchange Server. This option is not selected by default.

Note If this option is not selected, devices that do not fully support device security settings (for example, devices that do not support provisioning) will receive a 403 error message when they attempt to synchronize with Exchange Server.

To Configure Security Settings for Mobile Devices

1. On the **Start** menu, point to **Programs**, point to **Microsoft Exchange**, and then click **System Manager**.
2. In the console tree, double-click **Global Settings**, right-click **Mobile Services**, and then click **Properties**.
3. In **Mobile Services Properties**, click **Device Security**.
4. To specify the device security options, select **Enforce password on device**, and then configure the options according to the policies you have set.



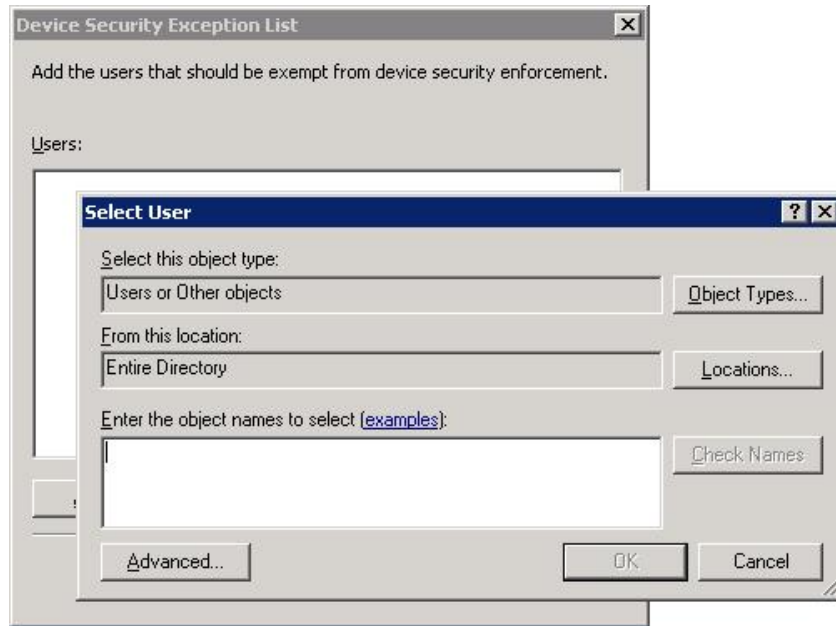
5. Click **OK**.

You can specify the users who you want to be exempt from the settings that you have configured in the **Device Security Settings** dialog box. This exceptions list is useful if you have specific, trusted users of whom you do not need to require device security settings.

To Specify the Users Who are Exempt from Device Security Settings

1. On the **Start** menu, point to **Programs**, point to **Microsoft Exchange**, and then click **System Manager**.
2. In the console tree, double-click **Global Settings**, right-click **Mobile Services**, and then click **Properties**.
3. In **Mobile Services Properties**, click **Device Security**.
4. In **Device Security Settings**, click **Exceptions**.
5. Use the options in the **Device Security Exception List** dialog box to select the user or group of users who you want to be exempt from settings that you have configured in the **Device Security Settings** dialog box.
6. To specify that a user be exempt from device security settings, click **Add**. In **Select User**, specify a user or group of users, and then click **OK**. For information about how to specify users, in the **Select Users** dialog box, click ? in the title bar, and then click the option you want to learn more about.

7. To remove a user from the list of users who are exempt from device security settings, in **Users** list box, select the user you want to remove, and then click **Remove**.
8. Click **OK**.



Monitoring Mobile Performance on Exchange Server

To track performance, availability, and reliability of Exchange ActiveSync and other mobile messaging components, you can use the Exchange Server Management Pack. The Exchange Server Management pack includes rules and scripts components that validate the availability of communication services, send test e-mails to verify operations, and measure actual delivery times.

With Exchange Server 2003 SP2, the following new rules were added:

- Exchange database sizes limits
- Exchange ActiveSync configuration settings
- Exchange ActiveSync Up-to-Date Notifications performance
- Exchange ActiveSync errors
- Monitor intelligent message filtering performance
- Intelligent message filtering for errors
- Sender ID configuration errors
- Sender ID errors
- Disk read/write performance
- DSAccess settings
- Public folder replication

The Exchange Management Pack Configuration Wizard provides a graphical user interface to configure Exchange 2000 and Exchange 2003 Management Packs, including test mailboxes, message tracking, and monitoring services.

You can download the Exchange Management Pack from the Microsoft Web site:
<http://go.microsoft.com/fwlink/?LinkId=55885>.

The Exchange Server Management Pack Guide for MOM 2005 explains how to use the Exchange Management Pack to monitor and maintain messaging resources.

You can download the management pack guide from the Microsoft Web site:
<http://go.microsoft.com/fwlink/?LinkId=58794>.

Step 7 – Install the Exchange ActiveSync Mobile Administration Web Tool

The Microsoft Exchange ActiveSync Mobile Administration Web tool enables administrators to manage the process of remotely erasing lost, stolen, or otherwise compromised mobile devices.

By using the Exchange ActiveSync Mobile Administration Web tool, administrators can perform the following actions:

- View a list of all devices that are being used by any enterprise user.
- Select or cancel the selection of devices to be remotely erased.
- View the status of pending remote erase requests for each device.
- View a transaction log that indicates which administrators have issued remote erase commands, in addition to the devices that those commands pertained to.

Download the Tool

The Exchange ActiveSync Mobile Administration Web tool is available for download from the following Tools for Exchange Server 2003 Web site:

<http://go.microsoft.com/fwlink/?LinkId=54738>.

Installing the Mobile Administration Web tool

To install the Exchange ActiveSync Mobile Administration Web tool on a front-end server that runs Exchange Server 2003 SP2, run the .msi package. The installation package creates the MobileAdmin virtual directory, through which the tool can be accessed.

When installed correctly, the Exchange ActiveSync Mobile Administration Web tool is available from any remote computer that has an Internet browser that can access the virtual directory associated with the tool. However, to access the Exchange ActiveSync Mobile Administration Web tool from the same computer upon which it is installed, you must use one of the following approaches:

- Add the server name to the Local intranet list for Internet Explorer: In Internet Explorer, click Tools, click Internet Options, click Security, click Local intranet, and then click Sites.
- Use localhost as the server name when specifying the mobileAdmin URL in the browser (for example, <https://localhost/mobileAdmin>).

Adding Administrators

By default, access to the Exchange ActiveSync Mobile Administration Web tool is restricted to Exchange administrators and to local administrators. A user from either of these groups can enable additional users to access the tool by modifying the security settings on the MobileAdmin folder in the installation directory. You make this change by right-clicking the folder, and then selecting sharing & security, which displays the **Insert Folder Security** properties dialog box.

By using this user interface, an administrator can add a user or group by clicking **Add** and then entering the name of the user or group to which the administrator wants to grant access.

Similarly, a user or group can be removed by selecting that user or group and then clicking **Remove**.

Step 8 - Manage and Configure Mobile Devices

As a Systems Administrator using Exchange Server 2003 SP2, you now have tools with which to set and enforce your mobile device security policies. You can also control some features on the mobile devices by using provisioning tools.

This section provides instructions and pointers for doing the following administrative tasks:

- Set Up a Connection to Exchange Server
- Initiate and Tracking Remote Wipe on Mobile Devices
- Provision or Configure Mobile Devices

Setting Up a Connection to Exchange Server

Your users can use ActiveSync to partner their Windows Mobile 5.0-based device with an Exchange server by using a USB cable from a desktop computer that is connected to your network. Or they can connect directly to the Exchange server by using their device directly if they have phone or Wi-Fi capability.

Note You may want to point your users to the step-by-step instructions for using ActiveSync and other features on Smartphones and Pocket PCs available at <http://go.microsoft.com/fwlink/?LinkId=37728>.

Connecting to Exchange Server Using a Desktop Computer

The ActiveSync Wizard will walk your users through the synchronization process.

Important Before a USB sync connection can be made, ActiveSync must be installed on the user's desktop computer. An ActiveSync setup disk may accompany the device or it can be downloaded.

As the ActiveSync Wizard is run from a desktop computer that is connected to the corporate network, the user will have the option to connect directly to the Exchange Server.

To connect directly to the Exchange Server, your users will need the following information:

- The path and domain name of the Exchange server.
- Their Exchange username and password.

Note Direct Push technology and security policy enforcement will be effective only when the devices are synchronized directly with the Exchange server. We do not recommend that you synchronize your mobile device only with the desktop computer.

Also in the ActiveSync Wizard, the user can choose which types of data, such as contacts, calendar, tasks, e-mail, to synchronize with the device. You may advise your users to uncheck any data types that should not be stored on their mobile devices.

Connecting Directly to Exchange Server

The user can use a Windows Mobile 5.0-based device to synchronize directly with Exchange Server.

- If Exchange server access was previously set by using ActiveSync on the desktop computer, the information should already be available when direct synchronization is tried.
On the mobile device, the user can click **ActiveSync**, choose **Menu** and select **Add Server Source**. After adding the server path, domain name, user name and password, the user connects directly to the Exchange Server.

Initiating and Tracking Remote Wipe on Mobile Devices

The remote wipe feature of the Messaging and Security Feature Pack is managed by using the Microsoft Exchange ActiveSync Mobile Administrative Web tool. This tool enables you to manage

the process of remotely erasing or wiping lost, stolen, or otherwise compromised mobile devices that are connected to the Exchange server wirelessly.

Using the Mobile Administration Web tool

The Welcome Screen presents the Administrator with a list of available administrative options. Select one of these options to start the associated Web page. The following options are displayed on the Welcome page.

- **Remote Wipe** Run a remote wipe command for a lost or stolen mobile device
- **Transaction Log** View a log of administrative actions, noting time/action/user

Running and Monitoring a Remote Device Wipe

The Remote Device Wipe administrator console provides the following functions:

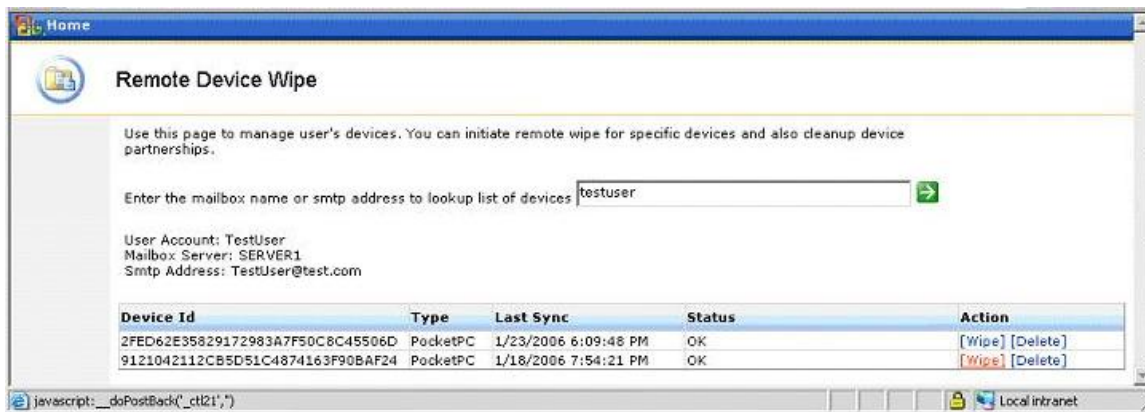
- Issue a remote wipe command for a lost or stolen mobile device.

To issue a remote wipe command, search for a user's mobile devices by specifying the user's name. The tool displays the device ID, device type, and the time the device last synchronized with the server for each of the user's devices. Locate the desired device, and then click Wipe. The tool then displays the up-to-date status for the device, displaying when or if the device has been successfully wiped.

- View the status on a pending remote wipe command.

When a Wipe action is specified for a device, it stays active until the administrator specifies otherwise. This means that, after the initial remote wipe has been completed, the server continues to send a remote wipe directive if the same device ever tries to reconnect.

- Undo (cancel) a remote wipe command if a lost or stolen device is recovered.



If a lost device is recovered, the administrator can cancel this directive to enable the device to successfully connect again. You cancel the wipe by locating the mobile device that has the remote wipe action set, and then clicking Cancel Wipe.

- Delete a device partnership.

The administrator can use the remote wipe console to delete a device partnership from the server. This action has the effect of cleaning up all state associated with a specified device on the server and is primarily useful for housekeeping purposes. If a device tries to connect after its partnership has been deleted, it will be forced to re-establish that partnership with the server through a recovery process that is transparent to both the IT administrator and the device user. This action is carried out by locating the mobile device, and then clicking Delete.

Viewing a Log of Remote Wipe Transactions

The transaction log displays the following information for all critical administrative actions performed with the Exchange ActiveSync Mobile Administration Web tool:

- **Date Time** Date and time when the action was executed
- **User** The user who executed the action
- **Mailbox** The mailbox that the action pertained to
- **Device ID** The device that the action pertained to
- **Type** The type of device that the action pertained to
- **Action** The action taken by the administrator

Configuring the Windows Mobile 5.0-based Device

If you are working with a mobile operator or mobile device manufacturer to deploy your Windows Mobile 5.0-based devices, you may be able to acquire devices that have been pre-configured with the features and settings to fit your needs.

You can use the device provisioning tools that are available in the Windows Mobile 5.0 Software Development Kit (SDK) to configure settings on the devices; to add, update, and remove software; or to change functionality.

Note You must have either manager access to the Windows Mobile 5.0-based devices or the ability to run trusted code on them in order to use the provisioning tools. Check with your mobile operator or device manufacturer for more information on the application security settings on your devices.

See the “Managing Devices” section of the SDK for detailed information. The SDK documentation is included in the MSDN Library at <http://go.microsoft.com/fwlink/?LinkId=63274>. The SDK documentation and tools are available at no charge from the Microsoft Download Center <http://go.microsoft.com/fwlink/?LinkId=63275>.

Note Be aware that there are two versions of Windows Mobile 5.0 software: Microsoft® Windows Mobile Version 5.0 software for Pocket PCs and Microsoft® Windows Mobile Version 5.0 software for Smartphones. While working in the SDK, follow references and directions for the version on your devices, as some procedures are different for the two versions.

Overview of Provisioning

Provisioning a Windows Mobile 5.0-based device involves creating a provisioning XML file that contains configuration information, and then sending the file to the device. Configuration Manager and Configuration Service Providers configure the device based on the contents of the provisioning XML file.

The Configuration Manager is the central authority that processes the provisioning XML file. Configuration Service Providers carry out all configuration queries and changes. After the data is passed to the Configuration Service Providers, they are responsible for carrying out the changes and reporting the success or failure of the transaction.

Note You must have either manager access to the Windows Mobile 5.0-based devices or the ability to run trusted code on them in order to use the provisioning tools.

There are several ways to deliver the provisioning XML file to the device. They include, but are not limited to, the following:

- A device that is connected to a desktop by a USB connection
- Storage cards

-
- Over the air (OTA)
 - Download from a Web site
 - Placement in device ROM or persistent storage

The Provisioning Process

The following is an overview of a sample XML file that you may be able to use to configure your Windows Mobile-5.0based devices with the path and the domain name of your Exchange Server. This provisioning process should enable your users to synchronize their devices without having to enter this information. During this sample provisioning process, you will:

1. Create the XML file.
2. Prepare the XML file for delivery.
3. Deliver the XML File.

In this process, you will use the makecab.exe utility to create a .cab file for delivery to the device. Makecab.exe is included with the Microsoft Windows Operating System, and is available from the Command line.

Provisioning Sample: Configuring Synchronization Settings

Create a valid provisioning XML file named _setup.xml. This file should contain the XML that addresses the Configuration Manager and its associated Configuration Service Providers.

To Create the XML File

1. In Notepad or other text editor, copy the following provisioning code for the Sync Configuration Service Provider and paste it below the first sample code.

```
<wap-provisioningdoc>
    <characteristic type="Sync">
        <characteristic type="Connection">
            <parm name="AllowSSLOption" value="1" />
            <parm name="Server" value="\\testserver"/>
            <parm name="Domain" value="testcompany.com" />
        </characteristic>
    </characteristic>
</wap-provisioningdoc>
```

2. Change **\\testserver** to your server name and **testcompany** to your Exchange server domain name.
3. Save the file as _setup.xml.

The _setup.xml file must be processed as a .cab file before it is transferred and installed on the client mobile device.

To Prepare the XML file for Delivery

1. To create a .cab file from the _setup.xml file, run the Makecab.exe utility, using the following syntax:
2. makecab _setup.xml myFile.cab
3. You may want to have your mobile operator sign the .cab file. This is an optional step that will remove the possibility of your users seeing the **Unknown Publisher** dialog box during installation.

The provisioning .cab file can be distributed to a device cradled to a desktop PC or on a variety of storage cards including MultiMedia Card (MMC), SDIO, and CompactFlash (CF) that are inserted into the device.

Note If the ActiveSync wizard appears when you connect the device to a desktop computer, click **Cancel**. It is recommended that you use Windows Explorer and File explorer to transfer the .cab file to the device.

To Distribute the .Cab File

1. Move or copy the .cab file <myfile.cab> to the device.
2. On the device, locate the file with **File Explorer** and click the .cab icon to initiate the installation.
3. **The Unknown Publisher** dialog box may appear if you did not sign the file. Click **Yes** to continue with the installation. Notification of a successful installation will appear.
4. Select the .cab file and from the **Menu**, choose **Delete** to remove the .cab file from the device.

You can check the device to see if your device provisioning was successful.

To Verify the Changes

1. Uncradle the device or remove the storage card.
2. Click **Start**, click **Programs**, and then click **ActiveSync**.
3. Click **Menu** and select **Configure Server...** The server path will appear in the **Server Address** box.
4. Click **Next**. On the **Edit Server Settings** page, the domain name of your company should appear in the **Domain** box. The **User name** and **Password** boxes will be empty.
5. Click **Back** and then click **Cancel**.

Appendix A. Deploying Exchange ActiveSync with Certificate-Based Authentication

Introduction

This appendix is divided into three main sections that describe the following:

- Alternative installation steps for deploying Certificate-based Authentication
- Configuring certificate enrollment for Windows Mobile 5.0-based devices using the Microsoft Exchange ActiveSync Certificate-based Authentication tool.
- Configuring certificate-based authentication for Exchange ActiveSync.

Note This is a version of the guide that is included with the Exchange ActiveSync Certificate-based Authentication tool. To get the most recent version, you can download it from the Tools for Exchange Server 2003 Web site at <http://go.microsoft.com/fwlink/?LinkId=54738>

System Requirements

The following operating system and applications are required for the correct operation of the tool.

- Windows® 2000 Server SP4 or Windows Server™ 2003 SP1 (recommended)
- Microsoft Exchange Server 2003 SP2
- Windows Mobile 5.0 Messaging and Security Feature Pack
- Active Directory® directory service
- Internet Information Services (IIS)
- Microsoft Desktop ActiveSync® 4.1. Download from Windows Mobile Downloads and Programs: <http://go.microsoft.com/fwlink/?LinkId=62652>
- Windows certification authority (CA)

Configuring Certificate-Based Authentication for Exchange ActiveSync

Key concepts involved in certificate-based authentication include the following:

- Kerberos authentication, including constrained delegation and protocol transitioning. For more information, see Kerberos Authentication in Windows Server 2003 at <http://go.microsoft.com/fwlink/?linkid=51993>.
- Making the following configuration changes in IIS and Active Directory Users and Computers:
 - Setting up SSL for the Exchange ActiveSync Virtual Directory (if it is not already set up).
 - Using IIS Manager 6.0 to configure client certificate-based authentication.
 - Using the **Active Directory Users and Computers MMC** snap-in to configure Kerberos constrained delegation and protocol transitioning.

Note These configuration changes may require changes to the Enterprise firewall configuration.

Exchange ActiveSync Requirements

You need the following requirements to authenticate over Exchange ActiveSync.

- Microsoft Desktop ActiveSync 4.1
- IIS Manager (6.0)

-
- Windows Mobile 5.0 Messaging and Security Feature Pack
 - Windows Server 2003 in native mode
 - Exchange Server 2003 SP2 on front-end servers
 - Active Directory
 - Exchange front-end servers and Active Directory domain controllers that are running Windows Server 2003

Kerberos Basics

Kerberos is a network authentication protocol that authenticates the identity of users who are trying to log on to a network, and encrypts their communications through secret-key cryptography.

Exchange ActiveSync certificate-based authentication utilizes Kerberos transition on the Exchange front-end server. That is, the client certificate is mapped to a user account and the Exchange front-end server must have Kerberos Constrained Delegation (KCD) enabled in order to perform Kerberos impersonation based on the user's certificate.

Note In a domain that is mixed Windows Server 2000 and Windows Server 2003 domain controllers, KCD will be global, allowing the client to access any server or desktop in the domain. In order to limit KCD access to specific servers, for example, the Exchange back-end servers, the domain must use Windows Server 2003 domain controllers exclusively.

For extensive information about Kerberos, see Kerberos Authentication in Windows Server 2003 at <http://go.microsoft.com/fwlink/?linkid=51993>.

Alternative Deployment Steps for Certificate-based Authentication

The next two processes should be substituted for similar steps in the deployment process provided in the main body of this document.

Setting up SSL for Exchange ActiveSync Virtual Directory

In Step 3, do the following to configure Secure Sockets Layer (SSL) for Exchange ActiveSync.

To configure SSL for Exchange ActiveSync

1. When the certificate is installed in **Internet Services Manager**, for the default Exchange HTTP virtual server, right-click **Default Web Site**, and then click **Properties**.
2. Click the **Directory Security** tab, and then select **Edit** under **Secure Communications**.
3. Select the **Require secure channel (SSL)** box. Select the box to **Require 128-bit encryption**.
4. Click **OK** two times.
5. Click **OK** to override any virtual directory inheritance.
6. Repeat the procedure to force an SSL connection on the Microsoft-Server-ActiveSync virtual directory. This can also be done to other Exchange service directories to force SSL authenticate to them also. These directories include the following:
 - Exchange
 - Exchweb
 - Public
 - OMA

Using IIS Manager 6.0 to Configure Certificate-Based Authentication for Clients

IIS Manager is a graphical user interface (GUI) for configuring your application pools or your Web, FTP, Simple Mail Transfer Protocol (SMTP), or Network News Transfer Protocol (NNTP) sites. You can use IIS Manager to configure IIS security, performance, and reliability features. Do the following to use IIS Manager to configure certificate-based authentication:

To use IIS Manager to configure certificate-based authentication

1. In **IIS Manager**, double-click the local computer, right-click the file that you want to configure, and then click **Properties**.
2. Click the **Directory Security** tab.
3. Under the **Secure communications** section, click **Edit**.
4. In the **Secure Communications** check box, do the following:
 - Under **Client certificates**, select **Require client certificates** or **Accept client certificates**. The server requests a client certificate before connecting the user to the resource. Users who do not have a valid client certificate are denied access.
 - Select the **Enable client certificate mapping** check box, and then click **Edit**.
5. Click **OK** two times.
6. Right-click the **Web Sites** directory and then click **Properties**.
7. Click the **Directory Security** tab, and select the **Enable the Windows directory service mapper** check box.
8. Click **OK**.

Creating the Exchange ActiveSync publishing rule using tunneling

The following instructions are for publishing an SSL-protected Web server on ISA Server 2004. Instructions for installing an ISA Server 2004 are included in the section *Install and Configure an ISA Server 2004 Environment or Other Firewall*.

To Publish a Web Server with SSL Tunneling

1. In the **Microsoft Internet Security and Acceleration Server 2004** management console, expand the server name and click the **Firewall Policy** node.
2. Click the **Tasks** tab, and then click **Publish a Secure Web Server**.
3. In the **SSL Web publishing rule name** box, type a descriptive name for this rule, and then click **Next**.
4. Click **SSL Tunneling**, and then click **Next**.
5. In the **Server IP address** box, type the IP address of the Web server where you want to publish the Web site, and then click **Next**.
6. Click to select the check box that corresponds to the network that you want ISA Server to listen to for Hypertext Transfer Protocol Secure (HTTPS) requests. For example, to cause ISA Server to listen on the external network, click to select the **External** check box.
7. Click **Next**, and then click **Finish**.
8. Click **Apply** to update the firewall policy, and then click **OK**.

The SSL Web site is now available on the external IP address of the ISA Server-based computer. You may have to make host record changes on your externally-accessible DNS server to map the IP address of the ISA Server-based computer's external interface to the host record of the SSL Web site.

Using Active Directory Users and Computers to Configure Kerberos-Constrained Delegation and Protocol Transitioning

You must configure Kerberos-constrained delegation and protocol transitioning to enable Exchange ActiveSync to impersonate the user when you access the user's e-mail, calendar, contact, and task information in the Exchange store. For more information, see Kerberos Authentication in Windows Server 2003 at <http://go.microsoft.com/fwlink/?linkid=51993>.

Active Directory Users and Computers is an MMC snap-in that is a standard part of Microsoft Windows Server operating systems. However, when you install Exchange Server 2003, the Setup wizard automatically extends the functionality of Active Directory Users and Computers to include Exchange-specific tasks.

You start Active Directory Users and Computers from either an Exchange server or from a workstation that has the Exchange System Management tools installed.

Note If the Active Directory Users and Computers snap-in is installed on a computer that does not have Exchange Server or the Exchange Server management tools installed, you cannot perform Exchange Server tasks from that computer.

The **Delegation** tab that is referenced in the following procedure lets you configure delegation in three ways:

- **Not allowed** Select the **Do not trust this computer for delegation** option.
- **Allowed for all services** Select the **Trust this computer for delegation to any service (Kerberos only)** option. Refers to the Windows 2000 Server delegation method.
- **Allowed for only a limited set of services** Select the **Trust this computer for delegation to specified services only** option. Refers to the constrained delegation method available with Windows Server 2003.

To use Active Directory Users and Computers to configure constrained delegation and protocol transitioning, follow these steps from the front-end server.

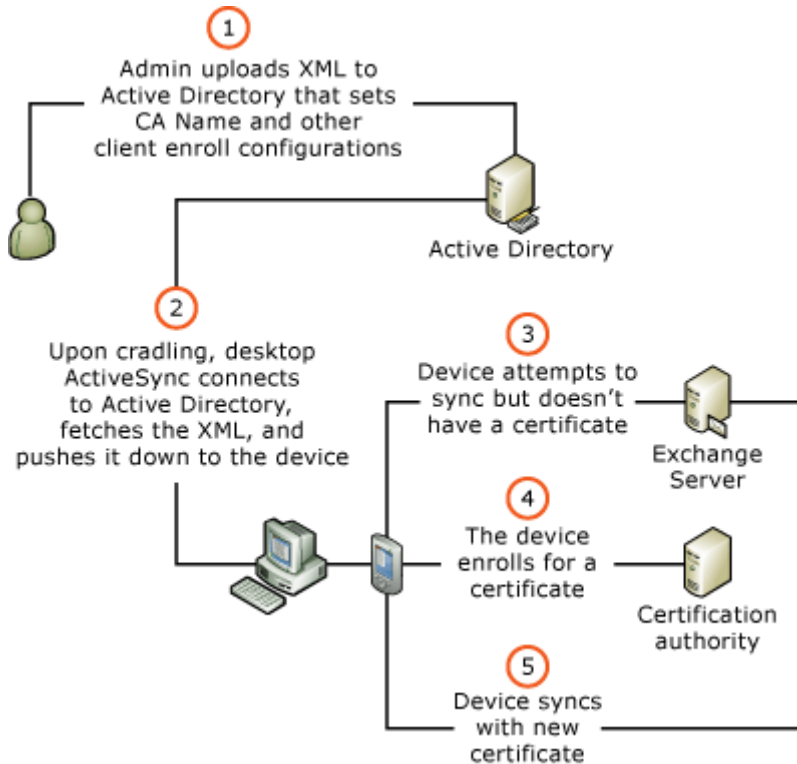
To use Active Directory Users and Computers to configure constrained delegation and protocol transitioning

1. Click Start, point to Program Files, point to Administrative Tools, and then click Active Directory Users and Computers.
 - Important** The change in steps 2, 3, and 4 are permanent. You cannot undo these actions.
2. Expand **Domain Controllers**, right-click the domain, and then select **Raise Domain Functional Level**.
3. In the **Raise Domain Functional Level** box, select **Windows Server 2003** from the list, and then click **Raise**.
4. Click **OK**.
5. In the console tree, click your Domain and expand the tree view.
6. Click **Computers** and expand the tree view. From the list of computers, right-click the **Front-end Exchange Server**, click **Properties**, and then click the **Delegation** tab.
7. On the **Delegation** tab, select **Trust the computer for designation of specified services only**, and then click **Add**.
8. Select **Use any authentication protocol to enable protocol transitioning**, and then click **Add**.
9. Click **Users or Computers**, type the name of the Back-end Exchange Server, and then click **OK**.
10. Select **HTTP** and **W3SRV** and then click **OK** two times.

11. Right-click the back-end Exchange computer, click Properties, and then click **Delegation**.
12. On the **Delegation** tab, select **Trust the computer for designation of specified services only**. If the back-end server is a domain controller, it is already configured to trust the computer for designation of specified services only.

Overview of Certificate Enrollment Configuration

The following workflow drawing shows the end-to-end operation for getting a certificate enrolled and ready for authentication.



There is no interactive user interface (UI) for entering information or configuration. The administrator relies on error messages and progress indicators as part of the device server synchronization certificate enrollment process.

In summary, the IT configuration steps and application actions involved in certificate enrollment are as described in the following table.

Task or activity	What occurs	Outcome
Use the certificate enrollment tool.	The administrator creates the device certificate enrollment configuration XML from the sample XML that is provided with the tool download. Then, the sample XML is uploaded to Active Directory using the Microsoft Visual Basic® Scripting Edition (VBScript) file that was provided with the tool download.	The device certificate enrollment XML that is customized for the users' IT environment is available in the correct Active Directory location. See "Uploading the XML to Active Directory," for more information.

<p>Deploy Desktop ActiveSync 4.1 to user desktops.</p>	<p>Desktop ActiveSync is installed on the user's corporate computer.</p>	<p>The user can cradle the device, thereby connecting it to the corporate network and enabling it to perform the certificate enrollment steps noted below.</p>
<p>Configure device.</p>	<p>The device is connected through Desktop ActiveSync4.1 to the users' corporate desktop, to enroll.</p> <p>The Desktop ActiveSync application downloads the configuration XML from Active Directory.</p> <p>Desktop ActiveSync "pushes" the XML to the Windows-based mobile device over the USB Remote API (RAPI) connection.</p> <p>During the setup of the device and desktop partnership, the user is prompted to enter his or her corporate username, password, and domain. To add these credentials to the device to enable enrollment, the <i>Save the password</i> check box must be selected.</p> <p>Note After the enrollment has been attempted one time, the username, password, and domain information are purged from the memory of the device. These items are used only for one attempted enrollment.</p>	<p>The XML is processed into registry settings that you can use for the certificate enrollment operation.</p>
<p>Attempt at initial synchronization.</p>	<p>The device tries an initial server synchronization.</p>	<p>Synchronization fails.</p> <p>This step occurs by design because the client tries to use Basic authentication password authentication. However, the server requires certificate authentication so it returns an HTTP 403 error to the device. The error indicates that a certificate is required for authentication.</p>
<p>Enroll certification.</p>	<p>The device initiates certificate enrollment using the saved</p>	<p>A connection is made to the Windows Certificate Services</p>

	Exchange ActiveSync username, password, and domain, combined with the certificate enrollment configuration.	<p>Web server that is specified in the enrollment configuration.</p> <p>Enrollment is processed using a Windows 2000 Server or a Windows Server 2003 certification authority (CA) that is running the Web-based enrollment feature.</p> <p>Note If authentication fails because the password is incorrect, the user can retry, but he or she must enter the password on the device. If authentication fails because a bad username or domain was entered, the Exchange server settings on the mobile device must be deleted and then re-created.</p>
Attempt at subsequent synchronization.	Receives the certification context from the Certificate Enrollment API. ActiveSync tries to re-authenticate to the Exchange front-end server that uses the returned certificate.	<p>Certificate-based authentication continues to work after the certificate enrollment step has been processed.</p> <p>The same process is used to enroll for a new certificate if the certificate is deleted or it expires.</p>

Downloading the Certificate Enrollment Tool

The Exchange ActiveSync Certificate-based Authentication tool can be downloaded from the Tools for Exchange Server 2003 Web site at <http://go.microsoft.com/fwlink/?linkid=55032>. The download consists of a folder that contains five items:

- EASAuthUploadXMLtoAD.vbs The VBScript file that uploads the XML configuration file to Active Directory
- EASCertAuthSampleXML.xml The sample XML configuration file.
- EASCertAuthEULA.txt Microsoft Software License Terms.
- EASCertAuthAdminDeployment.doc The user documentation (this file) for the tool.
- RapiConfig.exe A desktop configuration tool that enables the execution of provisioning XML on a Windows Mobile-based device or an emulator that is connected by using Exchange ActiveSync.
- QryCertReg.xml The XML file that is used as a parameter in RapiConfig.exe that indicates whether the mobile device is getting the configuration from Active Directory.

Configuring the XML

For certificate enrollment deployment to continue, pre-configuration must be completed. The administrator must create the device certificate enrollment configuration XML, make changes as required, and upload it to Active Directory. The configuration XML includes:

- Certification authority (CA) server name

- Certificate template that will be used
- Other settings, such as custom Web enrollment URLs

Following is a commented sample of the XML that is changed and then uploaded using the Active Directory VBScript. Sample XML is included in the tool download to help with making changes.

```
<wap-provisioningdoc>
  <characteristic type="Registry">
    <characteristic type="HKCU\Software\Microsoft\CertEnroll\ServerDef">
      <parm name="PrimaryServer" value="http://priserverdef"
datatype="string"/>
      <parm name="SecondaryServer" value="http://secserverdef"
datatype="string"/>
    </characteristic>
  <!-- COMMENT: In the above settings, edit only the name of the primary Windows 2000 Server or
Windows Server 2003 certificate server, http://PrimaryDefaultCAServerName, and the name of
the backup or secondary server, http://SecondaryDefaultCAServerName. The Windows Mobile-
based device tries to enroll against the primary, and it falls back to the secondary server if it fails.
The primary server name is required, and the secondary server name is optional. -->
  <characteristic
type="HKCU\Software\Microsoft\CertEnroll\DomainMapping\<domain name
here">
  <parm name="PrimaryServer" value="http://priserver" datatype="string"
/>
  <parm name="SecondaryServer" value="http://secserver" datatype="string"
/>
</characteristic>
  <!-- COMMENT: You will use the above settings only if your environment has more than one PKI
that it can be enrolled against. If not, delete this whole characteristic. In the above settings, edit
only the name of a domain (MappedDomainName) and the associated primary/secondary servers
(http://MappedDomainPrimary/CAServerName) for that domain. This configuration is optional.
However, if used, both the domain name and the primary CA server name are required, and the
secondary CA server name is optional. When configured, certificate enrollment will try to match
the domain name used for authentication of the certificate enrollment to any domain mapped in
this configuration section. If the domain is found, the certificate enroller uses the configured CA
server name for the connection. This is useful when there is more than one forest or PKI that a
user may have to enroll against. -->
  <characteristic type="HKCU\Software\Microsoft\CertEnroll">
    <parm name="Template" value="user" datatype="string" />
  <!--COMMENT: The template parameter is a required setting. Change the name of the template
to one that is available on Windows 2000 Server and Windows Server 2003 certification authority
(CA). In this sample XML, it is set to user. It is recommended that you use the "user" template
because it is the default template that is available on Windows Certificate Services. -->
  <parm name="CertPickupPage" value="/certsrv/certnew.cer"
datatype="string" />
```

<!--COMMENT: Do not change the CertPickupPage parameters unless you have decided to change the default path of the Windows Certificate Services Web-based enrollment pages on the Web server. These are the default settings-->

```
<parm name="CertReqPage" value="/certsrv/certifnsh.asp"
datatype="string" />
```

<!--COMMENT: Do not change the CertReqPage parameters unless you have decided to change the default path of the Windows Certificate Services Web-based enrollment pages on the Web server. These are the default settings.-->

```
</characteristic>
</characteristic>
</wap-provisioningdoc>
```

Changing the XML

Information about what should be considered for change is included in the following table. Note that each domain has a primary server and a secondary server for fallback. Every deployment must configure the primary and secondary servers for the `serverdef` characteristic.

Use	Characteristic or Parameter	Comments
Required	PrimaryServer	This setting is the name of the default primary certification authority server, including the https schema that will be used.
Optional	SecondaryServer	This setting is the name of the default backup certification authority server that will be used.
Optional	Template	Name of the certificate template that is targeted for enrollment, and the Windows certification authority setting that specifies attributes for a specific certificate type. Select a template from your created templates that suits your requirements for certificate enrollment. The default is ClientAuth.
Optional	DomainMapping	Used only when domain mapping is used. Domain mapping allows the CA name to be mapped to a domain name used during user authentication. You can have 0 or more domain mappings. If you are using domain mapping, put your domain name here and make sure that you include a primary server and a secondary server for each domain name that is mapped. You can have multiple domain names entered here. If the domain used in the logon is not listed as a mapped domain, the code reverts to the PrimaryServer and SecondaryServer entries.
Optional	CertPickupPage and	Used only when the path/name for the Web-based enrollment pages has been changed. The default for CertPickupPage is /certsrv/certnew.cer.
Optional	CertReqPage	Used only when the path/name for the Web-based enrollment pages has been changed. The default for CertReqPage is /certsrv/certifnsh.asp.

Uploading the XML to Active Directory

The VBScript file performs several actions on a computer that is physically connected to the network that hosts the target Active Directory forest, and has a domain administrator logged on. Also, the following procedure works only with Windows Server 2003 Active Directory. The script to upload the completed XML to Active Directory is run from a command line.

To upload the XML to Active Directory

1. Click **Start**, click **Run**, type **cmd** to open a command prompt, and then click **OK**.
2. Type the following command, where file.xml is the name of your customized XML file:
EASAuthUploadXMLtoAD.vbs file.xml

When the XML has been applied, changes are made in the registry by the device configuration manager.

The XML is stored in Active Directory within the [URL](#) property in the [msExchOmaConfigurationContainer](#), in the following path, and available through Active Directory Service Interfaces (ADSI).

CN=WWW-Page-Other

CN=Outlook Mobile Access,

CN=Global Settings,

CN=First Organization, This value can vary across deployments. To discover which value is [First Organization](#), enumerate all the children of the Microsoft Exchange object and look for the child that has the [msExchOrganizationContainer](#) in the [objectClass](#) attribute of its properties.

CN=Microsoft Exchange,

CN=Services,

CN=Configuration,

DC=DC Name (for example, [DomainController1](#)), ADSIEdit will default to the currently connected domain controller

DC=Domain Name (for example, corp),

DC=Forest (for example, Microsoft),

DC=com

The string is identifiable at the start and end as follows:

```
<CertEnrollXML><wap-provisioningdoc>  
...more XML here...  
</characteristic></characteristic></wap-provisioningdoc>
```

The script sets parameters on this location so that authenticated users in the domain can read and download the string to be able to configure the clients.

Testing Your XML Deployment

After you change the XML and upload it to Active Directory using the VBScript, you need to test to see that the XML works correctly.

To test your XML deployment

1. Log on to an ActiveSync desktop that is logged on to a domain in the forest where the XML was published.
2. Copy RapiConfig.exe to a directory on the desktop.

-
3. Connect the mobile device to a desktop using Desktop ActiveSync.
 4. Step through the **Desktop ActiveSync New Partnership** wizard after you connect the device to the desktop for the first time. The **Desktop ActiveSync New Partnership** wizard is the setup wizard that becomes active on the desktop when a new, unknown device connects for the first time. Enter settings in the wizard as you would if you were using a password to authenticate to the server. Enter the name of the Exchange front-end server, the username, password, and domain. Select the Save password check box, which is enabled so the password can be used one time to enroll for a certificate before it is deleted from the device. If the device fails authentication to the server, follow these steps:
 1. Determine whether the certificate is enrolled successfully.
 - Select **Control Panel**, and then double-click **Certificates**.
 - From the **Certificates** dialog box, verify that the certificate has been enrolled in the **Personal** store. If the certificate is there, the enrollment was successful, and you can continue to server or network troubleshooting. If the enrollment was not successful, continue to the next step.
 2. Determine whether the enrollment settings were successfully added to the registry on the device.
 - Click **Start**, click **Run**, type **cmd** to open a command prompt, and then click **OK**.
 - At the command prompt, type the path of the RapiConfig.exe on the desktop using QryCertReg.xml as the parameter: rapiconfig /P /M QryCertReg.xml

A file named RapiConfigOut.xml is produced in the same directory where RapiConfig.exe is located. When you look at RapiConfigOut.xml, you can see whether Desktop ActiveSync published the certificate enrollment configuration to the mobile device. If it has not, RapiConfigOut will look like this:

```
<wap-provisioningdoc>
  <characteristic type="Registry">
    <nocharacteristic type="HKCU\Software\Microsoft\CertEnroll"/>
  </characteristic>
</wap-provisioningdoc>
```

Possible causes for a failure include the following.

- The desktop does not have access or permissions to the correct object attribute in Active Directory. Try to access the location using ADSIEdit or Lightweight Directory Access Protocol (LDAP) from the same desktop by using the same user logon.
- The desktop did not download the settings from Active Directory before the attempt at mobile device enrollment. If your device did not synchronize because it did not have a certificate, it signals the desktop on the next connection to download the enrollment settings. Therefore, try to synchronize from the device, and then cradle the device again to Desktop ActiveSync.

If the enrollment configuration has been propagated correctly, you will see the custom settings configured in the XML.

Error Codes Returned by the Mobile Device

The following table shows the error messages returned to the mobile device.

Error Message	Error Message	Cause	HResult
E_ACTIVASYNC_GETCERT	The Exchange Server requires certificates to log on. Connect your device to your PC on the corporate network to obtain a certificate.	This error is returned when you try to synchronize against a server that requires certificate authentication and you do not have a client certificate on your device.	(HRESULT)0x85030027
E_ACTIVASYNC_ENROLLER_BAD_CERT	Cannot obtain a valid certificate. To try again, please disconnect and reconnect your device to a PC on the corporate network. If this problem persists, please contact your administrator.	This error is returned when the client certificate you used to authenticate with the server is malformed.	(HRESULT)0x85030028
E_ACTIVASYNC_EXPIRED_CLIENT_CERT	The certificate that is required to sync with Exchange Server has expired. To obtain a new certificate, connect your device to your PC on the corporate network.	This error is returned when the client certificate you used to authenticate with the server has expired.	(HRESULT)0x85030029
E_ACTIVASYNC_CERT_AUTH_FAILURE	Could not authenticate using a valid client certificate. To obtain a new client certificate and retry again, please disconnect and reconnect your device to a PC on the corporate network. If this problem persists, please contact your administrator.	This error is returned when the device cannot authenticate to the server by using a client certificate issued by the certification authority.	(HRESULT)0x8503002A

Deploying Desktop ActiveSync 4.1 to User Desktops

For information about ports and ActiveSync 4.1, see the Microsoft Knowledge Base article, TCP ports required by ActiveSync: <http://go.microsoft.com/fwlink/?linkid=3052&kbid=259369>

Appendix B. Adding a Certificate to the Root Store of a Windows Mobile-based Device

To add a certificate to the Root store, you must have manager permission to the device or have the ability to run trusted code. The application security settings on your devices will determine whether or not you can add a root certificate. However, some devices are configured so that you get a prompt when you attempt install a CAB file. In this case, you can follow the procedure below to add a certificate to the Root store.

The root certificates that are included with the Windows Mobile 5.0 device represent the following certificate authorities:

- Verisign
- GTE Cyber Trust
- Equifax
- Entrust
- GlobalSign
- Thawte

It is highly recommended that you install a certificate issued by one of the trusted certificate authorities or a certificate that chains to one of the trusted certificate authorities.

To find out what certificates are on your Windows Mobile-based device, check the Root certificate stores.

- For a typical Windows Mobile-based Pocket PC, go to **Start>Settings>System>Certificates>Root**.
- For a typical Windows Mobile-based Smartphone, go to **Start>Settings>Security>Certificates>Root**.

Create the Provisioning XML to Install a Certificate to the Root Store

The provisioning code carries the certificate hash and instructions for placing it in the root store.

To create a provisioning XML provisioning file

1. Create an XML file and add the following text.

```
<wap-provisioningdoc>
  <characteristic type="CertificateStore">
    <characteristic type="ROOT">
      <characteristic type="<certhash">">
        <parm name="EncodedCertificate"
value="<base64encodedcert>" />
      </characteristic>
    </characteristic>
  </characteristic>
</wap-provisioningdoc>
```

2. In **Windows Explorer**, double-click the root certificate that you need.
3. Choose the **Details** tab.
4. Choose **Thumbprint** in the **Field** list box.

-
5. Select the text in the box below the list box, and then press **CTRL+C**.
 6. In the XML code, replace `<certhash>` with the copied text.
 7. Delete the white spaces in the thumbprint text in the XML code.
 8. In the **Certificate** dialog box, choose OK to close the dialog box.
 9. In **Windows Explorer**, open the exported root certificate using a text editor.
 10. Delete the lines with BEGIN CERTIFICATE and END CERTIFICATE.
 11. Remove line breaks from the remaining text.
This text is the encoded contents of the root certificate.
 12. Select the text, and then press CTRL+C.
 13. In the XML code, replace `<base64encodedcert>` with the copied text.

The completed provisioning XML document will appear as shown in the following example.

```
<wap-provisioningdoc>
  <characteristic type="CertificateStore">
    <characteristic type="ROOT">
      <characteristic type="{hash of certificate}">
        <parm name="EncodedCertificate" value="{encoded hash
of certificate}"/>
      </characteristic>
    </characteristic>
  </characteristic>
</wap-provisioningdoc>
```

14. Save the XML document as an ASCII file named `_setup.xml`.
You must use the name `_setup.xml`. This is how the loader recognizes the provisioning XML file.

Create a CAB file containing the provisioning XML

The `_setup.xml` file must be processed as a `.cab` file before it is transferred and installed on the client mobile device.

From the Windows command line prompt, run the following text:

```
makecab _setup.xml <filename>.cab
```

Distributing the CAB Provisioning File

The provisioning `.cab` file can be distributed to a device cradled to a desktop PC or on a variety of storage cards including MultiMedia Card (MMC), SDIO, and CompactFlash (CF) that are inserted into the device.

Note If the ActiveSync wizard appears when you connect the device to a desktop computer, click **Cancel**. It is recommended that you use Windows Explorer and File explorer to transfer the `.cab` file to the device.

To copy the CAB file from the desktop to the device using File Explorer

1. Copy the `.cab` file to the device.

-
2. On the device, locate the file with **File Explorer** and click the **.cab** icon to initiate the installation.
 3. Notification of successful installation will appear. If you get a prompt, you must say **yes** to let the process execute.
 4. Check the **Root certificate store** to verify successful installation.