Microsoft Office:mac 2004

Microsoft Office 2004 for Mac Resource Kit

Version 2

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. 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.

Microsoft, MS-DOS, Windows, Windows NT, Windows Server, Entourage, Hotmail, and PowerPoint are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Apple, Mac, and Mac OS are trademarks of Apple Computer, Inc., registered in the U.S. and other countries.

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

Getting Started

Microsoft Office 2004 for Mac license terms....9
Office 2004 system requirements....10
What's new in Office 2004....11
Office shared features....11
Word....13
Excel....15
PowerPoint....17
Entourage....18
Virtual PC for Mac....21
Messenger for Mac....22
Resources on the Web....23
Office 2004 for Mac....23
Messenger for Mac....24
Virtual PC for Mac....24

Planning

Using Office 2004 with related Microsoft products....26
Working in an Exchange Server environment....27
Working with Internet Security and Acceleration (ISA) Server....41
Working with Messenger for Mac and Live Communications Server....42
Working with SharePoint....44
Working with Open Database Connectivity (ODBC) and SQL Server....44
Known issues in Office 2004....44
Choosing a deployment option....45
Run-time load options....45
User computer installation options....45
Deploying preferences....46

Deployment

Configuring servers and the network....49
Configuring Exchange Server 2003 to work with Entourage 2004....50
Summary of port requirements....51
Creating an Office 2004 installation image....52
Preparing the initial installation computer....52
Creating the initial Office 2004 installation....53
Adding custom documents, templates, scripts, and sound sets....55
Controlling font installation....55
Configuring Office 2004 preferences....56

Deploying preferences 59
Deploying preferences by using Workgroup Manager 59
Deploying preferences as part of a .pkg file 60
File locations 61
Deploying the Office 2004 programs 62
Run-time load options 63
User computer installation options 64
First-use setup for each user 68
Configuring Entourage at first use by user 68
Importing information into Entourage 2004 69
Deploying Virtual PC 75
Deploying Microsoft Messenger for Mac 75

Security

Office 2004 security environment 77
Overview of Office 2004 security 77
User information 78
Macro security in Office 2004 81
Scripts embedded in e-mail or documents 83
Helping reduce potential security threats 83
Word security 85
Using password protection 86
Opening documents as read-only 87
Protecting form fields 87
Protecting documents during reviews 87
Excel security 88
Using password protection 88
Limiting access to workbook and worksheet elements 90
Protecting the change history for a shared workbook 91
Removing personal or hidden information from a workbook 91
Entourage security 92
Configuring Entourage security features to help prevent viruses 93
Message security 94
Enabling or disabling Secure Sockets Layer (SSL) 100
Importing a self-signed SSL certificate 101
Enabling or disabling password protection 103
Enabling or disabling SMTP authentication 103
Authentication and security using WebDAV 104
Working with Internet Security and Acceleration (ISA) Server 104
Smart card support 105

Messenger for Mac security 105
Virtual PC for Mac security 106
Windows Services for Macintosh 106
Mac OS X Security 107

Configuration

Configuring Microsoft Word 2004 110
Storing components 111
Using add-ins 112
Setting default storage locations 112
Setting default spelling and grammar options 112
Configuring Word on a computer that has multiple users 112
Configuring Microsoft Excel 2004 113
Setting the default storage location 113
Using add-ins 114
Importing information into Excel 115
Using Web queries in Excel 2004 116
Excel specifications and limits 117
Configuring Microsoft PowerPoint 2004 120
Setting the default storage location 120
Configuring Microsoft Entourage 2004 120
Setting Entourage preference options 120
Synchronizing with handheld devices 121
Using Sync Services 122
Using delegation 122
Using public folders 124
Using sharing 124
Creating an Address Book, Calendar, or Mail folder in an Exchange account 125
Setting up out-of-office messages 125
Using complex HTML 126
Addressing e-mail messages by using the Global Address List 127
Using Project Center 128
Accessing Calendar events on an Exchange server 130
Accessing an Exchange account by using Outlook Web Access 130
Changing the LDAP port for Entourage 131
Setting administrative preferences for LDAP 131

Configuring Microsoft Virtual PC 7 for Mac 132
Configuring Microsoft Messenger for Mac 132
Cross-platform compatibility 132
Checking for compatibility 132
Working with Office for Windows documents 133
Working with Visual Basic 135
Using the Microsoft User Authentication Module (UAM) 135
Sharing printers between Macintosh and Windows clients 136
Long file names 137
Using AppleScript 137
Customizing Office 2004 international language settings 137
Office 2004 shared international features 137
International features of Entourage 2004 139
International features of Word 2004 139
International features of Excel 2004 140
Configuring Office 2004 for multiple languages 143

Maintenance

Managing Office 2004 product updates 145
Using AutoUpdate 145
Allowing users to perform updates independently 146
Downloading and distributing updates 146
Maintaining Office 2004 installations 146
Repairing Office 2004 installations 146
Microsoft Error Reporting Protocol 147
Deploying changes to network configuration and other preferences 148
Maintaining Entourage 2004 148
Verifying the integrity of the Entourage identity database 149
Rebuilding the Entourage identity database 150
Backing up the Entourage identity database 150
Compacting the Entourage identity database 151
Restoring the Entourage identity database 151
Troubleshooting Entourage Exchange e-mail accounts 151

Getting Started

Microsoft Office 2004 for Mac license terms....9
Office 2004 system requirements....10
What's new in Office 2004....11
- Office shared features....11
- Word....13
- Excel....15
- PowerPoint....17
- Entourage....18
- Virtual PC for Mac....21
- Messenger for Mac....22

Resources on the Web....23
- Office 2004 for Mac....23
- Messenger for Mac....24
- Virtual PC for Mac....24

The *Microsoft Office 2004 for Mac Resource Kit* has been updated with the latest information about deployment strategies, administration techniques, and security issues. If you have used an earlier version of the *Office 2004 for Mac Resource Kit*, you will find new and expanded coverage about planning for an Office 2004 deployment and maintaining and supporting Office 2004. The *Office 2004 for Mac Resource Kit* is organized into six sections:

- **Getting Started** Describes important licensing information and system requirements for Office 2004, and tells about new features in Office 2004. You will also find a list of online resources that provides additional information about deploying, administering, and using Office 2004.
- Planning Helps you plan your deployment of Office 2004. This section includes topics about deployment scenarios and using Office 2004 with related Microsoft products, including how to integrate Office 2004 into an Exchange environment.
- Deployment Guides you through the deployment process for Office 2004. These topics cover creating a custom Office 2004 installation, different methods of Office deployment, and managing preferences on user computers.
- Security Covers macro security in Office 2004, scripts embedded in mail or documents, and reducing potential security threats. Includes topics about configuring Entourage 2004 security features to help prevent viruses and improve message security.
- Configuration Provides information about configuring Office 2004 programs, Virtual PC for Mac, and Messenger for Mac. Also includes information about cross-platform compatibility and instructions for installing the User Authentication Module.
- Maintenance Describes the tasks and issues associated with updating and maintaining Office 2004 after deployment. Includes topics about administering the Entourage identity database and troubleshooting Entourage Exchange e-mail accounts.

Microsoft Office 2004 for Mac license terms

As outlined in the Microsoft Software License Terms, users can install and use one copy of Microsoft Office 2004 for Mac on a single computer. If a user is the primary user of that computer, the user can also install a second copy of Office, for his or her exclusive use, on a portable computer, as long as that computer is not connected to the same network as the computer that has the primary copy.

> **Note** If users install the same copy of Office 2004 on more than one computer and exceed the number of installations permitted by your organization's license agreement, the Office programs will automatically close shortly after they are opened. Before the programs close, users will be able to save changes that they have made to any open documents.

To install Office 2004 on additional computers, your organization can purchase additional copies of Office through your Microsoft reseller or purchase a volume license through the Microsoft Volume Licensing program.

- **Retail purchase** If your organization needs fewer than five copies of Office, purchase each copy through your Microsoft reseller.
- **Volume licenses** By participating in the Microsoft Volume Licensing program, you can purchase a volume license for five or more copies of Office. For more information about volume licensing, see Licensing for Businesses on the Microsoft Web site at http://www.microsoft.com/mac.

To determine which licensing option best meets your needs or to purchase a volume license, contact your Microsoft reseller. If you do not yet have a relationship with a Microsoft reseller, the Microsoft office for your location can help you find one. For information about contacting a Microsoft office near you, see the Microsoft Worldwide Web site at http://www.microsoft.com/worldwide.

Office 2004 system requirements

To run Office 2004, computers must meet the following minimum requirements.

Component	Minimum requirement
Processor	PowerPC G3 or later version, Mac OS X-compatible processor or later version
Operating system	Apple Mac OS X version 10.2.8 or later version
Memory	256 MB of RAM
Available hard disk space	570 MB for a recommended installation, 630 MB for a full drag-and-drop installation Case-insensitive HFS+ file format, the default format for Mac OS X, is required for Office 2004 installation and for home folders of Office 2004 users. This format is also referred to as Mac OS Extended or HFS Plus. The Office 2004 programs and user home folders may be located on the user's computer or on a file server that uses Apple Filing Protocol (AFP). To determine the format of a hard disk volume, on the **Apple** menu, click **About This Mac**, and then click **More Info**. Open the **Hardware** category if necessary, and then click the computer's hard disk interface type (for example, Parallel SCSI). To determine the format of the hard disk volume on a Mac running an Apple Mac OS X version earlier than 10.3, click the hard disk volume, and then on the **File** menu, click **Get Info**.
Disk drives	CD drive (or a connection to a local area network if you are installing over a network)
Monitor	1024 x 768 or higher resolution monitor displaying thousands of colors
Pointing device	Mouse or compatible pointing device
Internet Access	To use all the features available in Office 2004, we recommend that users have the following additional items and services: • Modem: 14.4 KB or faster • Internet Access: Dial-up or broadband Internet access (for Microsoft Entourage and certain features in other Office 2004 programs). Internet access might require paying a separate fee to a service provider. Local or long-distance telephone charges, or both, might apply.

What's new in Office 2004

The following paragraphs describe new features and improvements available in Office 2004 for Mac.

Office shared features

The following are features and capabilities of Office 2004 common to all Office 2004 programs.

Project Center

Microsoft Office 2004 introduces the Project Center, which provides users with a consolidated view of all information related to a project. Users create Project Center projects in Microsoft Entourage. Working with the Project Palette, users can also use Project Center projects in Microsoft Word, Microsoft Excel, or Microsoft PowerPoint.

Project Center projects consolidate all the e-mail, contacts, Calendar events, notes, tasks, Office documents (including document property information and attachments), other program documents (local and remote), and Scrapbook clips associated with the project.

The Project Center creates Project Watch Folders for Entourage messages and documents. An item is considered part of a project if it is designated as such in Entourage or if an alias to a program document is located in one of the designated Project Watch Folders. Users can flag any Entourage message, Calendar event, task, note, or contact as a project item. Users can also add to projects Scrapbook clips and documents created by using Office 2004 programs and other programs.

Users can invite other Entourage 2004 users to share project information by using a network server that they can all access or by storing project information in a shared folder on the computer. Each subscriber to a project can change project data and control what is shared with others. Users can back up all or part of the project, and can import the information again later.

After a user creates a project in the Project Center in Entourage, the user can use the Project Palette (available in Word, Excel, and PowerPoint) to schedule and view project events, write notes, and create new tasks. When a user creates a task or schedules an event by using the Project Palette, the information also appears on the Calendar or Tasks list in Entourage.

Shared project access

When a user shares a project, Entourage creates a shared folder on the file server and moves any shared files to the shared folder. Only users who are connected to the file server can access shared files. After you, as the administrator, identify a location for storing shared project data, you should obtain a list of the project subscribers and make sure that only those users who need access to project data are allowed access to the file server.

To prevent unauthorized access to shared projects, user access depends on the permissions set for the folder where the project is stored. Any individual with read access to the project folder can view the contents of the project. This might expose confidential information to those who are not invited to join the project. To maintain the security of project data, make sure that the permissions for the project folder provide access only to members of the project. Any user can forward a project invitation to other users, which notifies the users of the project's location if they use Entourage 2004. However, the project originator might not want the recipient of the invitation to join the project. Appropriately designating the permissions for the project folder helps prevent these kinds of problems.

Compatibility Report

Compatibility Report identifies and helps fix items in a document that might not be displayed or printed correctly in earlier versions of Office for Mac or in versions of Office for Windows. Users who share documents with users of other versions of Office can use Compatibility Report to help make sure that their documents appear the way they want when they are opened.

To access Compatibility Report in Word, Excel, and PowerPoint, on the **Tools,** menu, click **Compatibility Report**.

As an administrator or support professional, you can use Compatibility Report to help prevent or diagnose compatibility issues if your users are using documents created by different versions of Office.

Office Toolbox

The Office Toolbox provides access to the following important tools in Office 2004:

- Scrapbook, for storing text, objects, and images.
- Compatibility Report, for verifying that documents will be displayed correctly.
- Project Palette, for access to project information.
- Reference Tools (Microsoft Word 2004 only), for looking up words and doing research.

To access the Toolbox from PowerPoint, Word, and Excel, on the **View** menu, click **Toolbox**.

File recovery

Office 2004 provides a new file recovery feature that by default saves a copy of a working document every 10 minutes. Therefore, if a user loses power or an Office program stops responding, a previously saved or recovered version of the file is available the next time that the program is opened. You can use this feature to help users recover their files.

Enhanced Unicode support

Office 2004 can use a wider range of languages than earlier versions of Office used. With enhanced Unicode characters, Office 2004 can support Latin and East Asian language characters. Office 2004 displays, prints, and accepts input of various Unicode characters, both from the Basic Multilingual Plane and the Supplementary Unicode Planes. Also, Office now fully supports 255-character long file names, which can also include Unicode characters.

AutoUpdate

AutoUpdate, if enabled, automatically searches Microsoft servers for the latest version of Office 2004. You may want to establish a protocol that specifies whether users install updates automatically or following your approval. You can centrally manage the setting that controls whether AutoUpdate checks for updates automatically on user computers. For more information about managing this and other preferences, see Deploying Preferences in the "Planning" section.

Microsoft Error Reporting Protocol

Office 2004 Error Reporting is a new way to let Microsoft know about potential program problems. If an Office program stops responding, a report is generated that details the circumstances. Users can choose whether to send this report to Microsoft. Also, users have the option to automatically reopen the program. This makes it easier for users to return to their work. You will want to establish a policy for your organization that specifies whether users should send error report data directly to Microsoft. Error report data is used to find and fix problems in the software your organization uses. It is not used for marketing purposes. For more information about Office 2004 Error Reporting, see Microsoft Error Reporting Protocol in the "Maintenance" section.

Improved AppleScript support

Office 2004 supports a full, native AppleScript dictionary. AppleScript developers can write scripts that can control Office programs without the additional use of Visual Basic for Applications (VBA). For more information about AppleScript, see AppleScript Resources for Office 2004 in the Developer Center in the Resources area of the Microsoft Web site at http://www.microsoft.com/mac.

Word

The following paragraphs describe new features and improvements available in Word 2004.

Notebook layout view

Microsoft Word 2004 introduces notebook layout view, a new way for users to capture their thoughts and ideas in the equivalent of an electronic notebook. With notebook layout view, users can do the following:

- Organize and search their notes.
- Flag notes for follow-up.
- Assign tasks.
- Attach audio recordings to their notes by using a computer's built-in microphone or a microphone connected to the computer.

Users can use notebook layout view to take meeting or lecture notes, gather research materials, and more.

To use notebook layout view in Word 2004, on the **File** menu, click **Project Gallery**, and then on the **New** tab, click **Word Notebook**.

Improved change tracking

The Word Track Changes tool greatly reduces screen clutter by positioning comment balloons to the side of the main text. Also, users can instantly accept or reject changes, and with improved MSN Messenger integration, send an instant message to the comment author with questions and comments of their own.

The Track Changes tool is integrated with Entourage 2004 and MSN Messenger 4.0 to provide quick and seamless collaboration for creating, sharing, reviewing, and communicating about documents. Users can create a document in Word, send the document to others by using Entourage, track the changes that were made to the document in Word, and send an instant message about the document by using MSN Messenger—all through Word 2004.

To use Track Changes in Word 2004, on the **View** menu, point to **Toolbars**, and then click **Reviewing**.

Reference Tools

The Office Toolbox in Office 2004 includes Reference Tools for looking up words and researching subjects in Word 2004. Make sure to let your users know that they will need an Internet connection to use some Reference Tools that store information on the Web, such as Encarta encyclopedia and MSN Search. However, they will not need an Internet connection to use other Reference Tools, such as the dictionary and the thesaurus.

To use Reference Tools in Word 2004, click **Reference Tools** on the **Tools** menu.

Smart buttons

Smart buttons are automatic functions designed to help keep users in control of their software. The two new smart buttons in Word 2004 help users control the formatting of the document.

Button name	How it works
AutoCorrect Options	When Word makes an automatic correction, users can move the pointer near the changed word and then click **AutoCorrect Options** for a menu of options.
Paste Options	When users paste content into their documents, they can click **Paste Options** for a menu of formatting options.

Navigation pane

For Word 2004, the Document Map has been redesigned as the navigation pane to simplify navigation through long documents. The navigation pane is now much easier to read, and it includes a new thumbnail section that enables users to move quickly through miniature pages of their documents to find the section they want.

To switch to the navigation pane, on the **View** menu, click **Navigation Pane**.

Style improvements

Styles are collections of formatting options that users can apply to characters and paragraphs in a document. In Word 2004, styles are much easier to use. Users can also create list and table styles, and users can access all styles faster from new options on the **Formatting Palette**.

To use styles, on the **Formatting Palette**, under **Styles**, click the option that you want.

Excel

The following paragraphs describe new features and improvements available in Excel 2004.

Page layout view

Excel 2004 introduces page layout view, the new default view for worksheets. While users work, they can use page layout view to see exactly how their document will look when it is printed. Items such as rows, columns, text, charts, graphics, headers and footers, and text boxes appear in their actual positions on the page. This view gives users instant feedback about page layout. Users can view one page or multiple pages of the worksheet, easily navigate from page to page, and edit and format their data all in one view.

If users switch to a different view, such as normal view or page break preview, they can switch back to page layout view by clicking **Page Layout** on the **View** menu.

Charting improvements

Users can create richer and more professional looking charts faster by using the improved charting features in Excel 2004:

- Add depth to charts by using line or fill transparencies.
- Add interest to chart items by changing line widths.
- Color-coordinate charts by using preset color schemes, and more.

Chart options appear on the **Formatting Palette** after you have clicked any chart.

Smart buttons

Smart buttons are automatic functions designed to help keep users in control of their software. The smart buttons in Excel 2004 help users control the formatting of the worksheet and provide users with improved ways to fix errors.

Button name	How it works
Paste Options	When a user pastes text or data onto a worksheet, a menu appears in the lower-right corner of the cell. On the menu, the user can select the paste options he or she wants.
Error Checking	When a user makes an error on a worksheet in Excel 2004, a menu appears in the upper-left corner of the problem cell. On the menu, the user can choose how to fix the problem or whether to obtain additional help about the error.
Auto Fill	When a user completes an Auto Fill action in Excel 2004, a menu appears in the lower-right corner of the range of cells. On the menu, the user can choose how the series should be completed.
Insert Options	When a user inserts cells, rows, or columns in Excel 2004, a menu appears next to what was inserted. On the menu, the user can choose from a variety of formatting options.

Formula editing enhancements

Excel 2004 includes the following formula editing enhancements:

- When a user edits a formula, Range Finder uses color-coded ranges to display the cells referred to in the formula.
- When a user types formulas that contain functions directly into the formula bar or a cell, a Function ScreenTip appears below where the user is typing. These screen tips show the syntax of the function and help the user complete the function arguments.

Headers and footers

Excel 2004 includes features to improve the appearance of worksheets for printed output. Users can perform the following tasks:

- View and edit headers and footers directly on the worksheet by using page layout view.
- Add images and file path information to headers and footers.

To add a header or footer, on the **View** menu, click **Header and Footer**.

XML support

In Excel 2004, XML files created by using Excel 2000 for Windows or later versions can be opened and saved in XML Spreadsheet schemas.

Statistical function improvements

Excel 2004 includes a variety of improvements to key functions:

- More stable procedures for computing summary statistics
- Discovery of colinearity in multiple regressions
- A precise search method for finding the inverse of a continuous probability distribution function
- Improved discrete probability formula evaluation
- Improved random number generation

Improved preferences

Excel 2004 preferences include helpful descriptions that appear in the **Description of preference** box when a user rests the mouse pointer on a preferences option.

To set options in the **Preferences** dialog box, on the **Excel** menu, click **Preferences**.

PowerPoint

The following paragraphs describe new features and improvements available in PowerPoint 2004.

Presenter tools

The following features of the PowerPoint 2004 presenter tools help users better pace and deliver their slide shows:

- A notes pane where users view their prepared speaker notes or take notes during the slide show.
- An on-screen clock, visible only to the user, for timing presentations.
- A thumbnail column for viewing all the slides in a presentation. A user can click a slide in the thumbnail column to move the presentation to that slide.

To use the PowerPoint presenter tools, on the **View** menu, click **Presenter Tools**.

Improved templates and clip art

In PowerPoint 2004, users can easily experiment with different slide show design templates. At a glance, the new thumbnail images show what a presentation looks like with different design templates applied.

To quickly switch to a different design template, on the **Formatting Palette** under **Change Slides**, click the image of the desired template. Also, users can enhance standard templates by taking advantage of new clip art images. On the **Formatting Palette** under **Add Objects**, click **Insert Clip Art**.

Animations and transitions improvements

Animation effects and slide transitions created by using PowerPoint for Windows appear when a user runs those slide shows on the Macintosh. Also, with PowerPoint 2004, a user can create impressive new animations and transitions that are compatible with PowerPoint 2003 for Windows.

Font improvements

PowerPoint 2004 font improvements give more control over how text looks. Users can now format text as condensed or extended, and can set a transparency option for fonts.

Entourage

The following paragraphs describe new features and improvements available in Entourage 2004.

Smart card support

Entourage 2004 now supports the use of digital IDs stored on some smart-card-based keychains to perform secure messaging operations. These operations include digitally signing, verifying, encrypting, and decrypting e-mail messages.

Spotlight integration

Spotlight is now integrated with Entourage 2004. Users can use Spotlight to search quickly for items on their computers. To search in Spotlight, users must have Mac OS X version 10.4 or a later version and set Spotlight preferences.

Junk E-Mail Protection

Entourage 2004 Junk E-Mail Protection identifies and filters out more unwanted messages than did earlier versions of Entourage. By default, Junk E-Mail Protection is set to low, but users can choose from different levels and options to determine the level of protection that they want. You may want to set a required Junk E-Mail Protection level for all users in your network to contribute to a consistent protection level and a more predictable message volume on the network.

This increased level of Junk E-Mail Protection is available in the Microsoft Entourage 2004 Junk E-mail Filter Update 1 (11.1.0). The Microsoft Office 2004 for Mac Service Pack 2 (11.2.0) also includes the improvements released in Office 2004 Service Pack 1 (11.1.0). See the Downloads page of the Microsoft Web site at http://www.microsoft.com/mac to learn more about these updates.

Archiving

Users can archive mail from folders, tasks, contacts, Calendar events, and notes in a single package that they can save and access later. Users can also archive Project Center information. Users can archive mail in their Exchange Inbox and subfolders, but contacts and Calendar items stored on an Exchange Server cannot be archived. You may want to set up a specific network server for users to store archives.

Messenger for Mac integration

Messenger for Mac is integrated into Office 2004 and provides instant message and contact functionality to programs such as Word and Entourage. You may want to set standard Messenger settings for all network users to make sure that instant message communication follows your organization's privacy practices.

Entourage Setup Assistant

The Entourage Setup Assistant walks users through the account setup process and helps configure e-mail accounts automatically. This process enables users to begin using Entourage without entering much information. Administrators will find that Entourage 2004 mail account setup requires less administration than earlier versions of Entourage. For Exchange mail accounts, you should make sure that client computers can use DNS to resolve the domain name of the Active Directory domain where the user account is stored, and can use LDAP to query an Active Directory domain controller for the domain.

Exchange Server support improvements

Organizations can use Entourage 2004 to access Exchange server information. All Entourage messages are continually and automatically synchronized with the information about the Exchange server. The new Account Setup Assistant makes setting up an e-mail account easier for users than earlier versions and verifies settings on their behalf.

Exchange server feature	Benefits
Delegate access	Entourage users can be granted permission to open another person's folders, create items, and respond to requests for that person. Before an Entourage user can access and manage another person's Exchange information, the person granting delegate permission determines the folders the delegate can access and the changes the delegate can make. Users can set up and manage delegate access by using Entourage 2004.
Public Folders	Users can subscribe to and create their own Exchange server public folders.
Sharing	Users can share Exchange Address Book, Calendar, and Mail folders.
Multiple address books, calendars, and Mail folders	Users can create multiple address books, calendars, and Mail folders on the Exchange server by using Entourage.
SyncServices support	Users can synchronize Entourage items with other programs running on the Mac OS X operating system, such as Address Book and iCal.

Message security

Users can use encryption to help protect the contents of the messages they send. They can also use digital ID signatures to help assure message recipients that the message is probably from the identified sender and to help verify the identity of the sender of the signed messages they receive.

Support for World Wide Web Distributed Authoring and Versioning

Entourage 2004 uses the World Wide Web Distributed Authoring and Versioning (WebDAV) standard as the connection protocol for Exchange mail accounts. Microsoft Exchange Server began supporting WebDAV in Exchange 2000 Server when Outlook Web Access and the IIS Web service were integrated. Exchange Server 2003 supports WebDAV.

Entourage 2004 is designed to meet the most important customer feature requirements. It does this by using established protocols with reliable security. Entourage 2004 has improved support for e-mail over the WebDAV protocol. This support provides additional functionality and better performance in a low-bandwidth environment. Also, this support provides for basic delegate access to Exchange calendars, contacts, and e-mail. Additionally, Entourage 2004 uses WebDAV for calendar and contact synchronization.

WebDAV provides the following benefits to users and Exchange administrators:

- Eliminates the need for IMAP and SMTP access to Exchange Server for Entourage clients.
- Provides basic support to allow for delegate access and mail public folders.
- Allows users to access mail on a server behind the firewall without the need to use a virtual private network (VPN). This access is made possible through the front-end server, which publicly exposes HTTP Exchange access to the Internet.

If an Exchange Server administrator has configured Exchange Server to support Outlook Web Access, then, by default, this configuration also supports Entourage 2004 Exchange mail accounts, and no additional Exchange administration is required.

For Global Address List directory lookups, Entourage 2004 uses LDAP. Exchange Server 2003 uses virtual list view (VLV). A VLV is a feature in Active Directory. With VLV, a client application such as Entourage can browse, like the address book, through a large result set without having to transfer the entire set from the server. The Exchange 2000 Server implementation of LDAP does not support VLV.

For more information about administering Exchange Server to support the WebDAV access by Entourage 2004 clients, see the Exchange Server 2003 Technical Documentation Library at http://www.microsoft.com/technet.

Account setup improvements

The Entourage Account Setup Assistant has been improved in the following ways:

- Improvements to the Assistant reduce the amount of information that users are required to enter from earlier versions of Entourage.
- Entourage 2004 supports scenarios where the user ID (Active Directory user account) specified by the user does not match the e-mail address specified by the user.
- Entourage 2004 supports virtual server scenarios where the path of the user's data is not http://*server*/exchange/*user*. Users can enter the full path of their data in the Exchange server field of the account dialog box (for example, http://*server*/*virtualdirectory*/*different_name*).

Forms-based authentication

User accounts are authenticated by using the Exchange Server before Entourage 2004 synchronizes the data. This authentication is performed by using the forms-based authentication feature of Exchange Server. Other transactions between Entourage and the Exchange Server, including synchronization, are authenticated by passing a cookie from Entourage to the Exchange Server. The support for WebDAV in Entourage 2004 enables forms-based authentication.

As soon as both Exchange server and Entourage 2004 are configured for forms-based authentication, Exchange users can log on to their Exchange accounts by using Entourage 2004.

Virtual PC for Mac

Office 2004 for Mac Professional Edition includes Virtual PC for Mac 7.0. If you support cross-platform computer users, you may want to deploy Virtual PC for Mac in your network. Virtual PC for Mac can run Windows XP Professional, Windows XP Home Edition, and Windows 2000 Professional.

Improved performance

Virtual PC 7 is optimized for Mac OS X and features improved graphics and visual display. Programs start quickly, update easily, and are more responsive than in earlier versions of Virtual PC for Mac.

G5 support and Intel-based Macs

Virtual PC 7 is redesigned to take advantage of the speed and capabilities of the new Mac G5 processor. Office 2004 for Mac and Messenger for Mac run on the new Intel-based Macs. For more information about using Microsoft for Mac products with Intel-based Macs, see the Microsoft Web site at http://www.microsoft.com/mac.

Easy printing

For Panther and Tiger users (Mac OS X version 10.3 and 10.4), Virtual PC 7 eliminates the requirement to download special printer drivers. Users can click **Print** and access the same printing functionality and drivers used by the Mac OS.

Fast Save

Users can shut down and save the state of a virtual machine in one easy step. With the Fast Save feature, all Windows-based programs that are running on the virtual machine when it is shut down will be running when the user restarts the virtual machine.

Expanded preferences and settings

You or your users can customize the virtual machine by using new program preferences and virtual machine settings. Sounds, toolbars, shortcuts, memory, and even dock inclusion are found in the new Virtual PC 7 preferences and settings. For more information about managing this and other preferences, see Deploying Preferences in the "Planning" section.

Messenger for Mac

Users can now create corporate accounts and have instant conversations with other corporate users as well as with external users.

Corporate security for corporate messaging

Users can now create corporate accounts and have conversations with other employees behind the corporate firewall. Corporate accounts, which use Microsoft Office Live Communications Server 2005, help you maximize communication and maintain control of critical organization information.

New design

The brushed steel skin, new icons, and new **Personal** and **Corporate** tabs make this dual-purpose program stylish and intuitive.

Public IM support

With the federation features enabled on Live Communications Server, users can have instant message conversations with users who have other instant messaging services in other organizations. If you purchase the instant messaging (IM) connectivity licenses that are required, your Messenger for Mac users can chat with users of AOL Instant Messenger (AIM), Yahoo Messenger, and iChat.

Global address list look-up

Users can add contacts from their organization's global address list to their contacts list if they are on a corporate network that uses Live Communications Server 2005.

Customizable display pictures

Users can change their display name and picture depending on the account they are using.

Encrypted file transfer

Messenger for Mac users can drag more than one file at a time directly into the chat window.

Resources on the Web

Microsoft provides several Web sites that feature information and tools designed to meet the needs of administrators and information technology (IT) professionals. The following Web sites might be of interest to you if you deploy and support Office 2004.

Office 2004 for Mac

The Office 2004 page of the Microsoft Web site at http://www.microsoft.com/mac features guided tours of the Office 2004 programs, a free Office 2004 test drive that you download, and articles and tips about using Office 2004.

The Microsoft for Mac Support page of the Microsoft Web site includes information about the most common issues and solutions for Microsoft for Mac products. You can also search the Support Knowledge Base for Office 2004 support articles from this page of the Microsoft Web site.

The Resources page of the Microsoft Web site provides professionally designed templates for Word, PowerPoint, and Excel that you can download; information about training from third-party resources; resource kits for Microsoft for Mac products; and information for developing custom solutions for Microsoft for Mac programs. You can find more developer resources for the Macintosh at the Apple Developer Connection at http://developer.apple.com.

The Downloads page of the Microsoft Web site includes free updates, converters, and full versions or trial versions of Microsoft for Mac programs. See the Downloads page to learn more about the latest update of Office 2004 for Mac and earlier updates.

See the Microsoft Licensing page to learn about Microsoft Volume Licensing programs for organizations of all sizes.

The Community page of the Microsoft Web site provides information about joining Mac User Groups (MUGs), participating in newsgroups, and connecting with Most Valued Professionals (MVPs). Many Mac MVPs also own or contribute to Office for Mac resource Web sites, which are listed in their profiles.

The Exchange Server 2003 Technical Documentation Library on the Microsoft Web site is a source for information about administering Exchange Server to support the WebDAV access by Entourage 2004 clients.

For more information about administrator resources, see afp548.com, a user community for Mac OS X server administrators.

MacEnterprise at http://macenterprise.org is a Web site for professionals engaged in deploying, managing, and integrating Mac OS X client and server computers in multi-platform computing environments.

Messenger for Mac

You can download Messenger for Mac for free from the Downloads page of the Microsoft Web site at http://www.microsoft.com/mac. You can download the Messenger for Mac Deployment Guide from the Resource Kits page of the Microsoft Web site.

- For information about federation and public IM connectivity, see the Live Communications Server 2005 with Service Pack 1 Planning Guide.
- For information about Live Communications Server Enterprise Edition and enterprise pools, see the Live Communications Server 2005 Technical Overview.
- For information about how to deploy Live Communications Server 2005, see Live Communications Server Deployment Resources.
- For information about the Address Book Service, see the Microsoft Office Live Communications Server 2005 Address Book Service Planning and Deployment Guide.
- For information about Active Directory planning, see the Live Communications Server 2005 Active Directory Preparation Guide.

Virtual PC for Mac

To watch a demo and see how you can use Virtual PC for Mac to access PC-only software, files, networks and devices from Macintosh computers, see the Virtual PC for Mac page of the Microsoft Web site at http://www.microsoft.com/mac.

You can download the Virtual PC version 7 for Mac Deployment Guide from the Resource Kits page of the Microsoft Web site at http://www.microsoft.com/mac.

You can download the latest update to Virtual PC from the Downloads page of the Microsoft Web site at http://www.microsoft.com/mac.

Planning

Using Office 2004 with related Microsoft products 26
Working in an Exchange Server environment 27
Working with Internet Security and Acceleration (ISA) Server 41
Working with Messenger for Mac and Live Communications Server 42
Working with SharePoint 44
Working with Open Database Connectivity (ODBC) and SQL Server 44
Known issues in Office 2004 44
Choosing a deployment option 45
Run-time load options 45
User computer installation options 45
Deploying preferences 46

When you plan to deploy and install Microsoft Office 2004 for Mac and use it with related Microsoft products, you perform the following activities, which are described in detail in this section:

- Deciding how you will set up Office 2004 to use the products in your environment. For more information, see Using Office 2004 with related Microsoft products in this section.
- Deciding whether you will deploy and install the products centrally and what method you will use. For more information, see Choosing a deployment option in this section.

When you deploy Office 2004, you perform the following activities:

1. Configuring servers and the network
2. Creating an Office 2004 installation image
3. Deploying preferences
4. Deploying the Office 2004 programs
5. First-use setup for each user

For more information, see the Deployment section.

Using Office 2004 with related Microsoft products

Your organization can use Office 2004 together with various Microsoft products. This section helps you plan your installation to best use Office 2004 with the following products:

- Microsoft Exchange Server
- Microsoft Internet Security and Acceleration (ISA) Server
- Microsoft Office Live Communications Server and Microsoft Messenger for Mac
- Microsoft Windows SharePoint Services and Microsoft SharePoint Portal Server
- Microsoft Open Database Connectivity (ODBC) and Microsoft SQL Server

Working in an Exchange Server environment

How you integrate Office 2004 into an Exchange Server environment depends on two factors:

- The version of the Mac OS your organization uses
- The functionality requirements of your users

The following topics cover the Exchange integration capabilities of different versions of Office for Mac and the Mac OS and helps you choose which version to deploy according to the needs of your users.

Choosing the appropriate e-mail solution

Macintosh customers now have the following Microsoft e-mail client options for operating within Microsoft Exchange Server environments:

- WebDAV-based products: Microsoft Entourage 2004 or Entourage X version 10.1.4 or a later version
- IMAP-based products such as Microsoft Entourage X
- Microsoft Office Outlook Web Access, which supports browser-based access to an Exchange Server
- Remote Desktop Connection for Mac, which enables a Macintosh client computer to connect to a Windows session established on a server computer
- Microsoft Virtual PC for Mac, which enables Outlook for Windows to run on a PowerPC-based Macintosh computer

These options are not mutually exclusive. You can use any combination of these options in your organization. The following chart compares the features in each option.

Comparing options for Macintosh client computers in Exchange Server environments

Criteria of comparison	Entourage 2004	Entourage X	Outlook Web Access	Remote Desktop Connection for Mac*	Virtual PC for Mac
Client operating system supported	Mac OS X v10.2.8 or a later version	Mac OS X	All Mac OS versions	Mac OS X v10.1 or a later version	Mac OS X v10.2.8 or a later version
Client software required	Entourage 2004	Entourage X	Web browser	Remote Desktop Connection	Virtual PC for Mac, Microsoft Windows, and Outlook for Windows (any version)
Server-side requirements	Microsoft Exchange 2000 Server (with latest Service Pack) or a later Server version. Must enable the following protocols: HTTP, WebDAV, and LDAP. Must also enable Outlook Web Access.	Microsoft Exchange 2000 Server (with latest Service Pack) or a later Server version. Entourage X can connect to an Exchange 5.5 server by using an IMAP account. Entourage X requires Exchange 2000 or a later version to synchronize contacts and events. Must enable Internet Message Access Protocol (IMAP)	Microsoft Exchange Server 5.5 Series or Microsoft Exchange 2000 Server (with latest Service Pack) or a later Server version. Must enable Outlook Web Access	Outlook for Windows (any version) Microsoft Exchange Server version to support chosen Outlook version Operating system software support for Remote Desktop Protocol	Microsoft Exchange Server version to support chosen Outlook version
Support for offline access to data and reminders	Yes	Yes	No	No	Yes

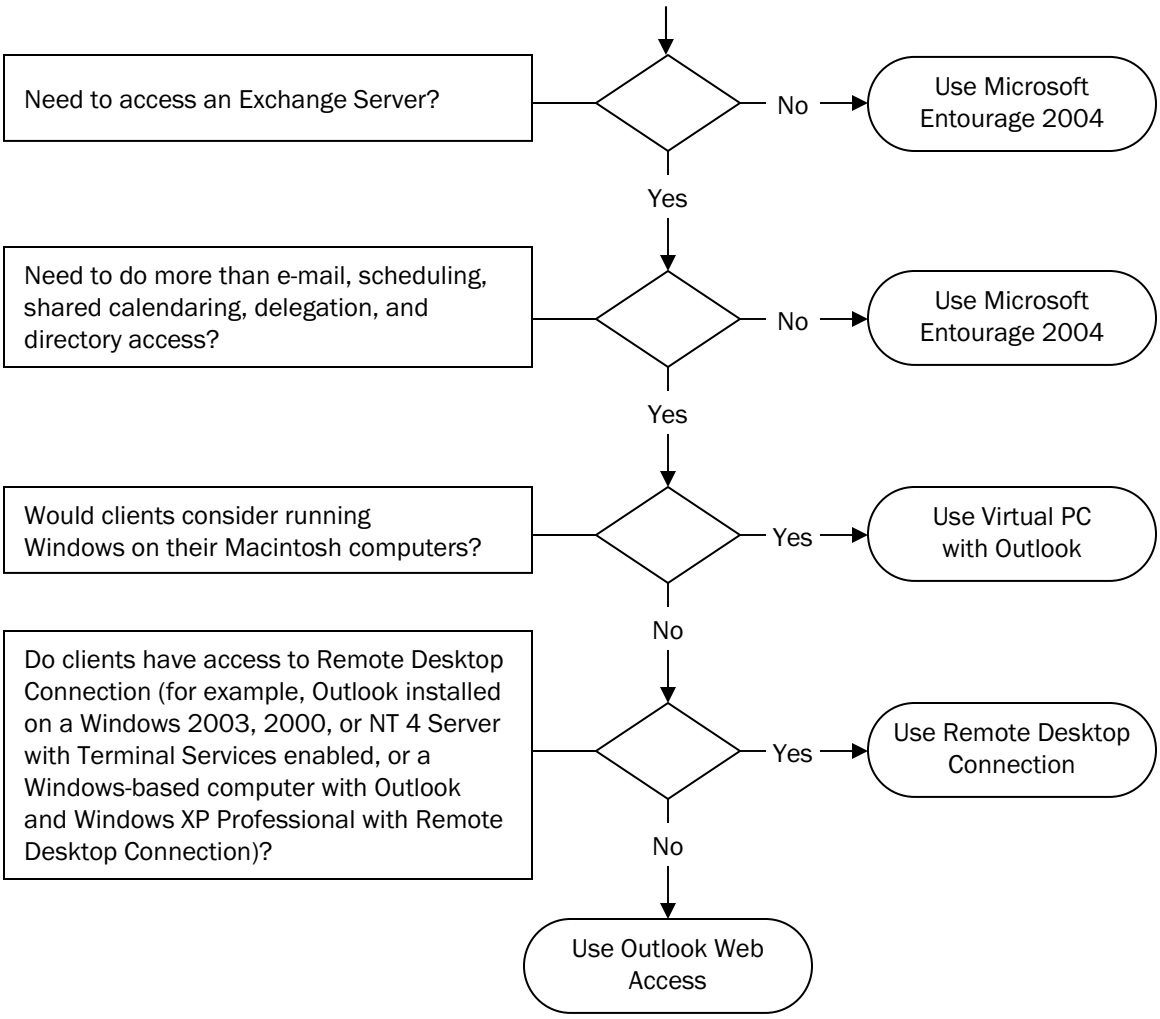
Criteria of comparison	Entourage 2004	Entourage X	Outlook Web Access	Remote Desktop Connection for Mac*	Virtual PC for Mac
100% same experience as using Outlook on a Windows-based computer	No, but similar	No	No	Yes	Yes
Support for handheld synchronization	Yes	Yes	No	No	Yes
Support for scheduling and delegated group calendaring	Yes	No	Yes	Yes	Yes
Support for Exchange-based e-mail	Yes	Yes	Yes	Yes	Yes
Support for HTML mail	Yes	Yes	Yes	Yes	Yes
Support for other e-mail protocols such as POP, IMAP, and Hotmail	Yes	Yes	No	Yes	Yes

Criteria of comparison	Entourage 2004	Entourage X	Outlook Web Access	Remote Desktop Connection for Mac*	Virtual PC for Mac
Support for .pst files	Can import .pst files from Outlook 2001	No	No	Yes	Yes
Support for delegation	Yes	No	Yes	Yes	Yes
Support for Global Address List (GAL) directory search	Yes, includes browse capability when it is used with Exchange on Windows Server 2003	Yes	Yes	Yes	Yes
More Mac-like	Yes	Yes	No	No	No
Requires knowledge of Windows	No	No	No	Yes	Yes
Can be used with the other solutions at the same time	Yes	Yes	Yes	Yes	Yes

* The Remote Desktop Connection features are shown as they work when they are used with Outlook 2000 for Windows or a later version.

The following decision tree can help you determine which solution is right for you in the Mac OS X environment. Remember, you can use more than one solution at the same time in your organization.

E-mail client choices in the Mac OS X environment



Using Entourage 2004

Entourage 2004 provides broad Exchange functionality in a corporate Macintosh environment. This functionality includes robust e-mail, group calendaring, and basic support for delegation and for public folders that contain mail items.

Exchange Server requirements for Entourage 2004

Entourage 2004 uses the World Wide Web Distributed Authoring and Versioning (WebDAV) standard, which uses HTTP, as the connection protocol for Exchange mail accounts. Entourage 2004 has the following requirements:

- Entourage 2004 requires Exchange 2000 Server Service Pack 2 or a later version for WebDAV support.
- Outlook Web Access must be installed and active.
- The following protocols must be enabled:
    - WebDAV (used by Outlook Web Access and Entourage 2004)
    - LDAP (Lightweight Directory Access Protocol).

You cannot use Entourage 2004 with an earlier version of Exchange Server, such as Exchange Server 5.5, because earlier versions of Exchange Server do not support WebDAV. If your organization uses Exchange Server 5.5, your users can use Outlook, Remote Desktop Connection Client for Mac, or Virtual PC for Mac for full Exchange functionality, and can use an IMAP account in Entourage 2004 to retrieve mail from the server if the server has IMAP enabled.

For more information about administering Exchange Server to support WebDAV access by Entourage 2004 clients, see the Exchange Server 2003 Technical Documentation Library on the Microsoft Web site at http://www.microsoft.com/technet.

Synchronizing information between Entourage and the Exchange Server

Whenever the Macintosh computer that is running Entourage 2004 is connected to an Exchange Server, e-mail messages, contacts, and Calendar items are synchronized. Other Exchange Server products (for example, Microsoft Outlook on a Windows-based computer) are also synchronized with the Exchange Server. However, because these programs display and use information differently, the user's information might look different depending on which program is being used to view the information. The following list shows some of these differences:

- If there is a conflict between the Entourage 2004 client-side copy of a synchronized item and its server-side copy, the Entourage 2004 client-side copy overwrites the server-side copy.
- Entourage does not synchronize notes, tasks, contact flags, certificates associated with contacts, project assignments and settings, links, and category information to the Exchange server.
- Although message flags are synchronized with the Exchange server, the task associated with a message flagged for follow up is not synchronized.

Events and Contacts When one or more of the following actions occurs, Entourage synchronizes events and contacts:

- An Exchange account is set up.
- Entourage connects to the Exchange server.
- The user makes a change to an event or contact on a computer that is connected to the Exchange server. Entourage waits one minute before it begins synchronization. If the user makes another change, the one-minute countdown starts over. This schedule prevents Entourage from beginning synchronization too frequently when a user edits multiple records.

Note Because Entourage notes, tasks, contact flags, and categories are not synchronized with the Exchange server, any backup plan that relies only on backing up the Exchange database will not back up these kinds of user data, which are stored in the Users/*username*/Microsoft User Data/Office 2004 Identities/*identity*/Database file for each identity. You may want to create an additional backup plan for this data. For more information about this database, see Entourage identity database in the "Security" section.

E-mail messages Users can access all Exchange mail folders, including subfolders, by using Entourage. Messages are synchronized with the Exchange server when the user changes an e-mail message, using the one-minute countdown that was discussed earlier for events and contacts. In addition, depending on the network configuration, Entourage synchronizes messages in the Inbox with the Exchange server in one of two ways:

- If Entourage is connected to a server that is sending out User Datagram Protocol (UDP) broadcasts, messages are synchronized whenever such a broadcast is received.
- If Entourage does not have access to UDP broadcasts (for example, if it is connected to a front-end server that resides outside your corporate network), it scans for new messages on the server once every minute.

Rules The user cannot create or change Exchange server-based rules by using Entourage, although rules stored on Exchange Server are applied. To change a server-based rule from the Macintosh computer, the user must be connected to his or her mail server and must be running Microsoft Outlook 2001, Virtual PC, or Remote Desktop Connection Client.

Out-of-office messages are usually generated by server-based rules. To manage out-of-office messages, Entourage users who connect to a server that is running Microsoft Exchange 2000 or a later version can use Outlook Web Access. For more information about using Outlook Web Access to set up out-of-office messages, see Setting up out-of-office messages in the "Configuration" section.

Contacts Entourage 2004 users can access contacts stored on an Exchange server from their Macintosh computers. Contacts stored on the Exchange server are synchronized with the Entourage Address Book and appear just as they do in Microsoft Outlook on Windows-based computers.

Entourage and Outlook store some kinds of contact information differently.

Contact information	Entourage 2004	Outlook (on a Windows-based computer)	Result of synchronization
Number of e-mail addresses stored in one contact	13	3	The default e-mail address in the Entourage contact is synchronized to the E-mail field in Outlook. The next 2 addresses in Entourage are synchronized with the E-mail 2 and E-mail 3 fields in Outlook.
“Other” mailing address label	No	Yes	Entourage displays an address labeled as "other" as the "work" address. If this address is edited in Entourage, the next time contacts are synchronized, the address label in Outlook changes to "business."
Number of children’s names in a contact	10	Delimited list	If an Outlook contact that lists more than 10 children is edited in Entourage, Entourage alphabetizes the list and retains only the first 10 names.

Calendar Users can access Calendar items stored on an Exchange server from Entourage 2004. Calendar items are synchronized with the Entourage Calendar.

If users specify travel time in a Calendar item created in Entourage, this information does not appear in Outlook. For example, if a user schedules an item for 1:00 P.M. to 2:00 P.M. with a travel time of 15 minutes, the Outlook Calendar blocks out only the one-hour scheduled time and does not include the travel time.

When an Entourage 2004 user creates a meeting request, the free/busy information for other Exchange users in the same organization is displayed.

Entourage does not detect whether an invitation is out of date or whether it conflicts with other events. In addition, if an Entourage user sends a meeting request to an Outlook user and the invitee makes a counterproposal, the counterproposal appears as text in the Entourage message body. The Entourage user must make any meeting time adjustments manually.

To prevent duplicate reminders, avoid running Outlook and Entourage at the same time.

How Entourage 2004 publishes free/busy data

Entourage 2004 relies on a free/busy publishing service named MadFB (also known as MSExchangeFBPublish), which runs as part of the Microsoft Exchange System Attendant service (MSExchangeSA) in Exchange Server. MadFB has two functions:

- Publish free/busy messages for WebDAV clients.
- Delete duplicate free/busy messages.

The MadFB agent is also used in the same way by Outlook Web Access and Outlook Mobile Access.

For more information about how free/busy data is published to Exchange, see Managing Free/Busy Folders on the Microsoft Web site at http://www.microsoft.com/downloads. The document, available for download, is a Windows executable file.

Deployments in an Active Directory infrastructure

When you set up the Entourage 2004 Exchange client and server, the configuration must meet the following Active Directory and network infrastructure requirements. Otherwise, the user must configure the Exchange mail account manually and provide more detailed information.

Requirements	Description
Client-side requirement	Configure the Network System Preferences on the Macintosh computer that is running Entourage 2004 with the IP address of at least one DNS server. We recommend that you configure the Search Domains in Network System Preferences with the domain names of the Active Directory domain to which the user account belongs.
Server-side requirements	For auto-configuring accounts, Entourage relies on the underlying DNS service that supports your Active Directory infrastructure. The DNS server that is used by the Macintosh computer must be able to either: • Return a DNS resource record identifying the Active Directory domain controller for the domain names it hosts. - or - • Resolve the domain name the user enters for his or her Exchange account. In both cases, the DNS server should be able to provide name resolution for any name in the Active Directory namespace it supports. The Entourage Exchange client must be able to locate the global catalog server for the Active Directory and authenticate the user account supplied for the Exchange mail account. To support this, the DNS resource records that identify the Active Directory domain controllers for the Active Directory global catalog server must be registered with at least one DNS server. This fundamental configuration step is performed at the time Active Directory is deployed. Deploying Entourage requires no additional Active Directory planning or deployment. For more information about deploying Active Directory, see Windows Server 2003 Deployment Guide on the Microsoft Web site at http://www.microsoft.com/technet. **Important** In an Active Directory or network infrastructure that is heavily secured, the Account Setup Assistant can experience difficulty in locating the Active Directory global catalog server and authenticating the user account. Environments where the servers are locked down and the required DNS ports are closed will experience problems.

Default ports that are used by Entourage

Entourage uses default ports for standard communication protocols. Your network and account configuration may require some or all of the following ports.

Default port	Used for
80	HTTP (WebDAV uses HTTP for functions such as synchronizing mail, public folders, contacts, and events)
443	HTTPS using Secure Sockets Layer (SSL), if SSL is enabled for WebDAV
53	DNS queries (To locate the Active Directory global catalog server for a user account, Entourage sends DNS queries to DNS servers)
1023 (and higher)	DNS query responses
135	Assigning delegate rights
3268	LDAP global catalog searches (To obtain Global Address List data, Entourage sends LDAP queries to the Active Directory global catalog server)
3269	LDAP global catalog searches with SSL
389	Other LDAP searches
636	Other LDAP searches with SSL
25	SMTP and SMTPS (SSL/TLS)
143	IMAP
993	IMAPS
110	POP
995	POPS
119	NNTP
563	NNTPS

If for some reason your Exchange deployment uses different LDAP ports, you or your users can change the ports in Entourage. The procedure is the same for both Directory Service accounts and Exchange accounts. For more information about specifying a different LDAP port, see Changing the LDAP port for Entourage in the “Configuration” section.

Entourage port preference settings are stored in the Entourage database. For more information about configuring and deploying Entourage preferences, see Configuring Office 2004 preferences and Deploying preferences in the “Deployment” section.

Differences between Entourage 2004 and Outlook 2003

To help you plan your Entourage deployment and diagnose Entourage issues, the following list shows the significant differences between Entourage 2004 and Outlook 2003:

- Entourage uses the WebDAV protocol to communicate with the Exchange server and to manage mail, Calendar, and contacts. Outlook uses a MAPI-based architecture to communicate with the Exchange server.
- Entourage does not provide offline access to the Global Address List. When a user is working offline, recently used addresses appear in the most-recently-used list in the address fields of an Entourage message.
- Entourage does not support mapping from subscribed public folders (favorites) in Entourage to public folder favorites in Outlook. Favorites established in Entourage are not automatically established as favorites in Outlook and vice versa.
- Entourage does not support Outlook forms, voting buttons, RTF message formatting, or receipt tracking.
- Users cannot use Entourage to create or modify server-side rules. For information about creating server-side rules, see Rules.
- Entourage notifies the user when his or her password is about to expire, but the user cannot change the user account password by using Entourage. You can direct users to use your organization's process for changing network passwords. Additionally, you can enable the Change Password feature in Outlook Web Access. For information about this feature, see Using the Change Password feature with Outlook Web Access, Knowledge Base article KB297121, at http://support.microsoft.com.

Common Entourage issues in an Exchange environment

The following notes describe common issues with administering Entourage clients.

- **Managing automatic distribution lists** Users cannot use Entourage to manage automatic distribution lists. However, they can use Automatic Distribution List Management (AutoDL), which provides a Web browser interface for managing groups in the Active Directory service. Users can add or delete new mailing and security groups and centrally manage the membership list of groups they own. In addition, users who are not group owners can request that they be added to or removed from existing group lists. For more information about AutoDL, see AutoDL Version 2.1 on the Microsoft Web site at http://www.microsoft.com/exchange.

  Entourage cannot expand a distribution list from the global catalog within an address field to display details of the included addresses. Users can view and expand a global distribution list by displaying it in the Global Address List.

- **Recovering deleted e-mail items** When an item is deleted from a folder in a mailbox, that item is first transferred to the Deleted Items folder of that mailbox. Users can then remove the item from the Deleted Items folder. This helps provide some protection in case a user deletes an item accidentally. After the items are removed from the Deleted Items folder, users can still recover them. To recover deleted items, an Entourage user would type a URL of the following format in the browser address bar:

  exchangeServerName/exchange/*userID*/*folderPath*/?cmd=showDeleted&close=1
  - or -
  mail.*yourcompany*.com/exchange/*userID*/*folderPath*/?cmd=showDeleted&close=1

  This URL is accessed by using either http:// or https://, depending on your installation. For more information about recovering deleted items, see Understanding Deleted Item Recovery, Knowledge Base article 228934, at http://support.microsoft.com.

- **Compacting or rebuilding a database** When an Exchange account is used from both Entourage and Outlook, compacting or rebuilding an Entourage database could cause mail messages to be duplicated. To avoid this, delete the Exchange account in Entourage before compacting the database, and then re-create the Exchange account. If duplicates have already been created, the following third-party procedures might be useful to remove them:

  - Outlook: See Duplicates Remover for Outlook on the MAPILab Web site at http://www.mapilab.com.
  - Entourage: See the Macscripter at http://scriptbuilders.net. Various scripts are available. Select the Entourage category and search for *duplicate*.

- **Connecting to the Entourage account for the first time** If an Entourage user's localization (the translation of the names of special folders such as Inbox, Sent Items, and Drafts) differs from the Exchange server localization, use Outlook Web Access or Outlook to connect to the account for the first time. This will prevent Exchange folders from being created that use the server's localization instead of the Entourage localization.

For information about troubleshooting Entourage client operations with Exchange Server, see Troubleshooting Entourage Exchange e-mail accounts in the "Maintenance" section.

Using Outlook Web Access

The Outlook Web Access client has the same Active Directory and networking infrastructure requirements as an Entourage 2004 Exchange client. For more information, see Deployments in an Active Directory infrastructure.

Notes are not supported by Outlook Web Access.

Setting up Outlook Web Access

Requirements	Description
Client	• Mac OS 8.1 to 9.x or Mac OS X • Web browser
Server	• Microsoft Exchange Server 2003, Microsoft Exchange 2000 Server or a later version (with Service Pack 2 or a later version) or Microsoft Exchange Server 5.5 Series must be installed. Tasks are supported beginning with Microsoft Exchange Server 2003. • Outlook Web Access must be installed and active.

If the previous requirements are met, no additional setup is necessary for this solution.

You will need to give your users the address for the Outlook Web Access Web site. It typically follows the form:

exchangeServerName/exchange

- or -

mail.*yourcompany*.com/exchange

It will be accessed by using either http:// or https://, depending on your installation.

When the user is ready to access the Exchange server by using Outlook Web Access, he or she will perform the following procedure:

To access the Exchange server by using Outlook Web Access

1. Open the Web browser.
2. In the Address bar, type the address provided by your Exchange server administrator for the Outlook Web Access Web site.
3. Enter your user name, password, and domain name.
   You can use the Outlook Web Access site much like you would use Microsoft Outlook.

For more information about Outlook Web Access, see Outlook Web Access Features in Exchange Server 2003 on the Microsoft Web site at http://www.microsoft.com/exchange.

Using Remote Desktop Connection Client for Mac

With Remote Desktop Connection for Mac, a user on a Macintosh computer can connect to and use an Outlook session on a Windows-based computer.

Setting up Remote Desktop Connection for Mac

Requirements	Description
Client	• Mac OS X v10.1 or a later version • Remote Desktop Connection Client for Mac
Server	• The Windows Server 2003 operating system, Windows 2000 Server operating system, Windows NT Server 4.0 Terminal Server Edition, or Windows XP Professional • Remote Desktop Connection or Terminal Services must be configured and active. • Outlook 2000 or a later version must be installed and configured.
Default port	3389

If the previous requirements are met, you will need to do very little setup before users can begin using Remote Desktop Connection.

When the user is ready to access the Exchange Server by using Remote Desktop Connection, he or she will perform the following procedure:

To access the Exchange Server by using Remote Desktop Connection Client for Mac

1. Open Remote Desktop Connection Client for Mac.
2. In the **Computer** box, type the name of the Windows-based server or personal computer to use remotely.
3. Click **Connect**.
4. To log on, type your user name, password, and domain name.
5. On the remote computer, open Outlook.

Note For more information about Remote Desktop Connection Client for Mac, see Remote Desktop Connection on the Microsoft Web site at http://www.microsoft.com/mac.

Using Virtual PC for Mac

For information about installing, configuring, and using Virtual PC for Mac, download the Virtual PC version 7 for Mac Deployment Guide from the Resource Kits page of the Microsoft Web site at http://www.microsoft.com/mac.

Client software connecting to Exchange Server requires port 135 for MAPI accounts and may require other ports depending on the client and server software and account type(s) involved. For more information, see the following Knowledge Base articles on the Microsoft Web site at http://support.microsoft.com:

- Exchange Server static port mappings, Knowledge Base article 270836
- How to configure RPC dynamic port allocation to work with firewalls, Knowledge Base article 154596

Working with Internet Security and Acceleration (ISA) Server

ISA Server provides enhanced security and performance by authenticating incoming and outgoing Web requests at the perimeter of your corporate network instead of authenticating requests internally on an Active Directory/Global Catalog server. ISA Server can use several different authentication methods:

- Integrated Windows Authentication (NTLM)
- Digest Authentication
- Basic Authentication
- Forms-Based Authentication (SSL)

Note Entourage 2004 does not currently support Forms-Based Authentication (FBA) when Entourage is used with ISA Server. However, you can configure ISA Server so that your Outlook Web Access server performs this authentication. Entourage and Outlook Web Access sessions will then work with FBA but will not have the benefits of ISA. For more information about supporting FBA in an ISA environment, see Knowledge Base article 909268 on the Microsoft Web site at http://support.microsoft.com.

If you must provide secured external access to the Global Address List, you may prefer not to open ports for LDAP searches through ISA. Instead, you can host a copy of the Global Address List on an Active Directory Application Mode (ADAM) server which is exposed to the Internet for SSL access. For more information about ADAM, see Introduction to Windows Server 2003 Active Directory Application Mode on the Microsoft Web site at http://www.microsoft.com.

For information about ISA Server, see the Microsoft Internet Security and Acceleration Server area of the Microsoft Web site at http://www.microsoft.com/isaserver.

For information about third-party support for additional authentication methods for ISA Server, see User Authentication in the Partners section of the ISA Server area at http://www.microsoft.com/isaserver.

Working with Messenger for Mac and Live Communications Server

Microsoft Messenger for Mac v. 5.1 and later versions make enhanced security, real-time communication, and collaboration simple for corporate Mac users. Messenger for Mac is integrated into Office 2004 and provides instant message and contact functionality to programs such as Word and Entourage.

Messenger for Mac provides two types of communication services for instant messaging:

- **Corporate** A corporate account uses the Live Communications Server service. When Messenger for Mac users are connected to a Live Communications Server, they can communicate in real time over a corporate network. Users can add both coworkers and associates from other companies as contacts to their corporate accounts.
- **Personal** A personal account uses the MSN Messenger service. Users can add friends and family members as contacts to their personal accounts.

The following features are new in Messenger for Mac:

- Conversations with other employees occur through Live Communications Server, with enhanced security behind the corporate firewall.
- Through its integration with Live Communications Server, Messenger supports server-side session logging and more secure corporate messaging.
- With the new tabbed interface, users can quickly switch between corporate and personal accounts.

Messenger system requirements

Before you can deploy Messenger for Mac corporate accounts in your organization, you need the following:

- Live Communications Server 2005 with SP1

Each client Macintosh computer must meet the following requirements for corporate or personal accounts:

- A native G3, G4, G5 or Intel-based Macintosh computer, with 20 MB of available hard-disk space and 128 MB of RAM
- Mac OS X v10.3.x or a later version
- Microsoft Messenger for Mac 5.1 or a later version
- Access to the corporate intranet (for corporate accounts) and the Internet (for personal accounts)

Default ports that are used by Messenger

Messenger uses the following default ports:

Function	Port
Presence and Chat for personal accounts	1863
Presence and Chat for corporate accounts	5060 for TCP and 5061 for SSL
File transfer for both personal and corporate accounts	6891 to 6900

With file transfer, a new port is opened for each concurrent transfer. If a user sends five files at the same time, the ports that are used would be ports 6891, 6892, 6893, 6894, and 6895, respectively. After one transfer is finished, the port returns to the queue so that it can be used for any additional transfers. If you do not want all the ports open, you can open one or two ports and instruct your network users to restrict file transfers to one at a time.

> **Note** On a corporate network, you might want to prevent Messenger for Mac users from using a personal account. To disable personal accounts, disable connectivity with the MSN Messenger service by closing port 1863 in your corporate firewall.

Proxy settings for Messenger

Messenger can use SOCKS 4 (or SOCKS 5 with authentication) and HTTP proxies. When Messenger is opened, proxy information is determined by System Preferences in the following order: SOCKS 4, SOCKS 5, and then HTTP.

If Messenger is unable to detect the proxy settings, the settings can be edited in System Preferences. The settings take effect the next time that Messenger is opened.

For more information about deploying Messenger, download the Microsoft Messenger for Mac Deployment Guide from the Resource Kits page of the Microsoft Web site at http://www.microsoft.com/mac.

For more information about deploying Live Communications Server 2005, see Live Communications Server 2005 Deployment Series in the Live Communications Server area on the Deployment Center page at http://www.microsoft.com/office/livecomm.

For more information about the Address Book Service, see the Live Communications Server 2005 Document: Address Book Service Planning and Deployment Guide in the Live Communications Server area on the Deployment Center page at http://www.microsoft.com/office/livecomm.

Working with SharePoint

Some SharePoint functionality works differently with Office 2004 on the Macintosh than with Office 2003 on a Windows-based computer.

In Windows, users can use an Office 2003 program such as Word to check out documents from a SharePoint site. In Office 2004 on the Macintosh, users must check out documents by using a Web browser. The file is downloaded to the desktop, where users can then open, edit, and save the file by using the associated Office program. Users check the file back in to SharePoint by using the browser. This process supports the version control feature if it is enabled for the document library.

For users to view files on a SharePoint site, anonymous logon is sufficient. However, if users want to author or edit files on SharePoint, they must use an authenticated logon. In an Active Directory environment, users are logged on to SharePoint automatically if they are already logged on to a domain. In other environments, the authentication methods that are supported depend on the browser being used.

If your organization uses the Apple Safari browser, you should enable Basic Authentication on your SharePoint Web site so that users can author and edit files that are hosted on the site. For more information about enabling Basic Authentication, see STS: Must Enable Basic Authentication for Browsers Running on Macintosh OS, Knowledge Base article 288354, on the Microsoft Web site at http://support.microsoft.com.

Working with Open Database Connectivity (ODBC) and SQL Server

Microsoft Excel 2004 can retrieve information from SQL Server and other databases by using a variety of third-party ODBC drivers. For the latest information about ODBC support, see Import data into Excel 2004 by using ODBC in the Excel 2004 Articles and Tricks area on the Microsoft Web site at http://www.microsoft.com/mac. For more information about working with database queries, open Microsoft Query (located in the Microsoft Office 2004/Office folder), and then on the **Help** menu, click **Microsoft Query Help**.

Known issues in Office 2004

For information about known issues in products that are part of the Office 2004 suite, see the Read Me document accompanying each product. You may also want to see the Office 2004 for Mac Solutions Center on the Microsoft Web site at http://support.microsoft.com/mac04office.

Choosing a deployment option

To install a retail version of Office 2004 on an individual computer, follow the instructions provided with the retail product.

To deploy Office 2004 centrally, your organization must obtain a volume license. You cannot deploy retail versions of Office 2004 from a central location. For more information about volume licensing, see Microsoft Office 2004 for Mac license terms in the "Getting Started" section.

Several options are available for centralized deployment of Office 2004. Some options load Office 2004 programs at run time from a central location; others install Office 2004 on the user's computer.

Case-insensitive HFS+ file format, the default format for Mac OS X, is required for Office 2004 installation and for home folders of Office 2004 users. The Office 2004 programs and user home folders may be located on the user's computer or on a file server that uses Apple Filing Protocol (AFP).

Run-time load options

- **Running from a net boot image** Under this option, you establish your configuration of Office 2004 as part of the net boot image. Office 2004 is made available to users automatically when they turn on their computers.
- **Running from a file server** Under this option, you install Office 2004 on a file server. Users then load the Office 2004 programs from the server at run time. A variation of this option is to run the installation from a network domain instead of from an individual file server. In this case, the user does not have to connect manually to the file server because the server volume is mounted automatically.

User computer installation options

Under all the following options, you create an Apple Installer package (.pkg) file that contains the installation image. Optionally, the package file can also contain preference files and a script that you write to prepare the user computer before installation. The package file contains instructions for copying each file in the package to a location that you specify.

- **Installation from a file server** Under this option, you make the .pkg file available to users on a file server. Users install the program on their computers by dragging the .pkg file from the file server to their computers and opening it.
- **Installation by using Apple Remote Desktop** Under this option, you use Apple Remote Desktop to distribute the .pkg file onto user computers and open it automatically.
- **Installation by using NetInstall** Under this option, you use the NetInstall feature of Mac OS X to install the package onto user computers.

These options for deploying the Office 2004 programs are described in more detail in Deploying the Office 2004 programs in the "Deployment" section.

Deploying preferences

For all the previously mentioned deployment methods, you have the option of deploying a default installation image taken directly from the Office 2004 distribution media that you receive from your reseller. If you prefer, you can deploy a customized installation image that includes settings that you choose for your organization. For example, you can specify a macro security level in Word or Excel or configure a default Exchange account in Entourage. By managing custom preference settings, you can increase the standardization of the Office 2004 experience across your user community.

Most Office 2004 preferences are set with key/value pairs that are contained in .plist (property list) files, also known as preference files, stored in the *username*/Library/Preferences/Microsoft folder. The first time an Office 2004 program is opened, Office determines whether the corresponding .plist file for the program is present. If the Microsoft folder and the required preference file are not found, the program creates them. If the appropriate settings file is found, the program uses the preference settings stored in the file. Some Office 2004 preferences are not stored in .plist files but in other locations such as the Entourage database.

Depending on which preferences you want to manage, you can use either of the following options or a combination of the two:

- Deploying preferences by using Workgroup Manager
- Deploying preferences as part of a .pkg file

Deploying preferences by using Workgroup Manager

Office 2004 partially supports the Workgroup Manager solution provided by Apple with Mac OS X Server v10.4. With this solution, you can set .plist preferences and define privileges centrally.

With Workgroup Manager, you use the preference files you create when you customize the installation image to establish settings for Office 2004 preferences and for Apple System Preferences. Office 2004 preferences and settings that are not stored in .plist files cannot be managed with Workgroup Manager.

> **Note** Office 2004 does not disable user interface elements for preferences managed by using Workgroup Manager. This means that users can override centrally managed settings. However, you can configure Workgroup Manager to reset preferences to your selected values at time intervals that you choose.

For more information about Workgroup Manager, see Workgroup Management in the Mac OS X Server area of the Apple Web site at http://www.apple.com/server/macosx.

Deploying preferences as part of a .pkg file

If you are installing Office 2004 on user computers, you can deploy custom preference files to user home folders as part of the .pkg file that you deploy to distribute the Office 2004 programs. If you are not installing Office 2004 on user computers, you can deploy a .pkg file to user home folders by using Apple Remote Desktop. A .pkg file can contain .plist files and other Office 2004 settings files, such as the Entourage database.

For more information about Apple Remote Desktop, a desktop management tool that you can use to control and configure user computers remotely, see Apple Remote Desktop 3 on the Apple Web site at http://www.apple.com/remotedesktop.

> **Note** Office 2004 does not disable user interface elements for preferences managed by using deployed preference and settings files. This means that users can override the initial settings in the deployed files. You can configure Apple Remote Desktop to redeploy .plist files, which resets preferences, at intervals that you choose; however, you cannot redeploy an Entourage database after the user begins to use it.

These options are described in more detail in Deploying preferences in the “Deployment” section.

Deployment

Configuring servers and the network 49
Configuring Exchange Server 2003 to work with Entourage 2004 50
Summary of port requirements 51
Creating an Office 2004 installation image 52
Preparing the initial installation computer 52
Creating the initial Office 2004 installation 53
Adding custom documents, templates, scripts, and sound sets 55
Controlling font installation 55
Configuring Office 2004 preferences 56
Deploying preferences 59
Deploying preferences by using Workgroup Manager 59
Deploying preferences as part of a .pkg file 60
File locations 61
Deploying the Office 2004 programs 62
Run-time load options 63
User computer installation options 64
First-use setup for each user 68
Configuring Entourage at first use by user 68
Importing information into Entourage 2004 69
Deploying Virtual PC 75
Deploying Microsoft Messenger for Mac 75

This section presents the recommended procedure for deploying Microsoft Office 2004 for Mac. This procedure consists of the following major phases:

1. Configuring servers and the network
2. Creating an Office 2004 installation image
3. Deploying preferences
4. Deploying the Office 2004 programs
5. First-use setup for each user

Notes

- To install a retail version of Office 2004 on an individual computer, follow the instructions provided with the retail product.
- To deploy Office 2004 centrally, your organization must obtain a volume license. You cannot deploy retail versions of Office 2004 from a central location across an organization. For more information about volume licensing, see Microsoft Office 2004 for Mac license terms in the "Getting Started" section.

Configuring servers and the network

We recommend that you configure the needed features of your Microsoft Exchange, Lightweight Directory Access Protocol (LDAP), Domain Name System (DNS), and other servers before you create a customized Office 2004 installation image. You also must provide appropriate network permissions for your users and make sure that required ports are open. After you make these preparations, you can test your installation image to make sure that it works correctly before you deploy Office 2004 throughout your organization.

Configuring Exchange Server 2003 to work with Entourage 2004

If your organization currently runs Microsoft Exchange Server and Microsoft Outlook, you must do only minimal additional configuration. To configure Exchange to work with Entourage, you must enable the following features of Exchange Server:

- Outlook Web Access
- Web Distributed Authoring and Versioning (WebDAV)
- HTTP

For more information about these requirements, see the Planning section.

Entourage 2004 supports the same cookie-based authentication that is used by Microsoft Office Outlook Web Access clients who connect to their e-mail accounts through a front-end server in a front-end and back-end server environment. You have the option to enable forms-based authentication, which requires Secure Sockets Layer (SSL), on the front-end server.

Notes

- With forms-based authentication, users must enter their credentials either in the universal naming convention (UNC) format (*Domain**Username*) or in the user principal name (UPN) format (*user*@*domain*.com).
- With forms-based authentication in Exchange Server 2003, you can set the default domain setting in Internet Information Server (IIS) only to the default domain setting of "\" (backward slash). This restriction is designed to support user logons that use the UPN format. If the default domain setting is changed, Exchange System Manager resets the default domain setting to \ on the Web server.

For more information about configuring Exchange Server, see Exchange Server 2003 Technical Documentation Library on the Microsoft Web site at http://www.microsoft.com/technet/prodtechnol.

Summary of port requirements

The following table provides a summary of the ports required by Office 2004 and related products discussed in this document.

Office 2004 component or related product	To work with	Default port requirements
Entourage 2004	Exchange Server	
	HTTP (WebDAV)	80
	HTTPS	443
	DNS queries	53
	DNS query responses	1023 (and greater)
	Assigning delegate rights	135
	LDAP global catalog searches	3268
	LDAP global catalog searches with SSL	3269
	Other LDAP searches	389
	Other LDAP searches with SSL	636
	SMTP (Simple Mail Transfer Protocol) and SMTPS (SSL/TLS)	25
	IMAP (Internet Message Access Protocol)	143
	IMAPS	993
	POP (Post Office Protocol)	110
	POPS	995
	NNTP (Network News Transfer Protocol)	119
	NNTPS	563

Office 2004 component or related product	To work with	Default port requirements
Messenger	Microsoft Office Live Communications Server (for corporate accounts)	Presence and Chat: 5060 for TCP (Transmission Control Protocol) and 5061 for SSL File transfer: 6891 up to 6900 or your preferred limit
	MSN Messenger Service (for personal accounts)	Presence and Chat: 1863 File transfer: 6891 up to 6900 or your preferred limit
Web browser	SharePoint	HTTP: 80 HTTPS: 443
Excel	Open Database Connectivity (ODBC) to SQL Server and other databases	Varies by third-party ODBC driver. For more information, see the documentation for your driver.
Remote Desktop Connection	Any Windows-based program, such as Outlook 2003	3389
Virtual PC	E-mail clients connected to Exchange server	135 and possibly other ports. For more information, see Using Virtual PC for Mac in the “Planning” section

Creating an Office 2004 installation image

This section describes how you can create a version of the Office 2004 folder for deployment. This folder is referred to as the installation image. You can deploy a customized installation image that includes your choice of Office components and supporting files, such as templates. However, customization is not required. You can deploy the default Office 2004 installation image as it appears on the installation media that you receive from your reseller.

Preparing the initial installation computer

Use the following procedure to prepare the Macintosh computer before you install Office 2004.

To prepare the initial installation computer

1. Remove previous versions of Office, including Test Drives, if present, by using the procedure in Removing previous versions of Office.
2. If a *username*\Documents\Microsoft User Data\Office 2004 folder is present, drag it to the Trash.

3. If a *username*\Library\Preferences\Microsoft folder is present, drag it to the Trash.
4. Drag any *username*\Library\Preferences\com.microsoft.*programname*.plist files to the Trash.
5. Remove any Dock icons for Office programs by dragging them off the Dock.
6. Turn off virus-protection software, because it might interfere with installation, and quit any programs that are running.
7. If the computer is currently running the Classic environment (Mac OS 9), switch to Mac OS X. To quit the Classic environment, on the **Apple** menu, click **System Preferences**, and then click **Classic**. On the **Start/Stop** tab, click **Stop**.

Creating the initial Office 2004 installation

You can now install Office on the initial installation computer, and set customized preferences if you want.

To install Microsoft Office 2004 for Mac without customization

1. Insert the Office 2004 CD into the CD drive of the local computer.
2. Drag the Office 2004 folder to the install location (generally the Applications folder for the current user) on the local computer.

   The copied Office 2004 folder and its contents on the local computer are referred to as the installation image.
3. Apply all available service and security releases and updates to the installation image. If Microsoft AutoUpdate is installed on your computer (the default location is the Applications folder), you can open it and it will find the relevant updates. If you are logged on as an administrator, you can also install and run AutoUpdate by starting any Office 2004 program, and then clicking **Check for Updates** on the **Help** menu. Otherwise, you can obtain updates to Office 2004 from the Downloads page of the Microsoft Web site at http://www.microsoft.com/mac.

   You may want to establish a protocol that specifies whether users install updates automatically or only following your approval. For information about centrally managing whether AutoUpdate checks for updates automatically on user computers, see Managing the AutoUpdate process.
4. Proceed to Deploying the Office 2004 programs.

To create a customized Microsoft Office 2004 for Mac installation image

1. Insert the Office 2004 CD into the CD drive of the local computer.
2. Double-click **Office Setup Assistant**.
3. Type a generic user name such as “User” and your organization name. The user name and organization appear as the “registered to” identifiers in subsequent installations of Office 2004 from this installation image and cannot be changed after this point. This user name is also the default user name, which should be personalized by each user at first use.
4. On the pop-up menu under **Select the installation location**, click the local volume and folder you want to use. A Microsoft Office 2004 folder is created within the folder you specify.

   The customized installation image consists of this Microsoft Office 2004 folder and its contents.

   > **Important** Installation under a volume license does not require that you enter a product key. If Setup Assistant requests a product key, the installation CD is incorrect. If this happens, do not continue to prepare an installation image. Obtain a correct CD from your reseller and begin again.

5. Select **Custom Install**.
6. Set or clear the check box next to each component that you want to include or not include in the installation.
7. Click **Install**.
8. After the Setup Assistant finishes installing Office 2004, apply all available service and security releases and updates to the installation image. Microsoft AutoUpdate automatically finds the relevant updates if AutoUpdate is enabled on the computer and the computer has a connection to the Internet. If you are logged on as an administrator, you can also install and run AutoUpdate by opening any Office 2004 program, and then clicking **Check for Updates** on the **Help** menu. Otherwise, you can obtain updates to Office 2004 from the Downloads page of the Microsoft Web site at http://www.microsoft.com/mac.

You may want to establish a protocol that specifies whether users install updates automatically or only following your approval. For information about centrally managing the setting that controls whether AutoUpdate checks for updates automatically on user computers, see Managing the AutoUpdate process.

Adding custom documents, templates, scripts, and sound sets

You can additionally customize Office 2004 installations by adding custom documents, templates, add-ins, scripts, and other items to the Office 2004 installation image.

To add	Do this
An Office document that is opened whenever the user starts the corresponding Office 2004 program	Copy your custom Word, Excel, or PowerPoint startup documents to the appropriate folders in the Microsoft Office 2004/Office/Startup folder.
Custom templates to Office 2004	Copy your custom templates for Word, Excel, or PowerPoint to the appropriate folders in the Microsoft Office 2004/Templates folder.
Custom add-ins to Excel	Copy your custom add-ins to the Microsoft Office 2004/Office/Add-ins folder.
Custom AppleScript scripts to Entourage	Copy your custom scripts to the Microsoft Office 2004/Office/Entourage First Run/ Entourage Script Menu Items folder.
Custom sound sets to Entourage	Copy your custom sound set files to the Microsoft Office 2004/Office/Entourage First Run/ Entourage Sound Sets folder.

Controlling font installation

The first time a user opens any Office 2004 program from a user account that has never run an Office 2004 program, Office determines which fonts are installed. First, Office looks for whether the MS Gothic font is installed in either the Library/Fonts folder or the /Users/*username*/Library/Fonts folder and is active on the system. Then, if the MS Gothic font is not found (for example, if you or your users use a font management utility to temporarily enable or disable installed fonts), Office 2004 installs it together with additional fonts found in the Microsoft Office 2004/Office/Fonts folder. This process is referred to as First Run Font Installation.

If the user account being used to run Office 2004 for the first time has Write privileges for the /Users/*username*/Library/Fonts folder, Office 2004 installs the fonts into that folder. If the user does not have Write privileges for the correct folder, the font installation is omitted.

If your organization uses a centralized font management utility, and you want to avoid font conflicts between Office 2004 and specialized font configurations, you might want to prevent Office 2004 from installing any fonts during First Run Font Installation.

To prevent Office 2004 from installing fonts

- Remove the Do Fonts file from the Microsoft Office 2004/Office folder before you deploy Office 2004.

Configuring Office 2004 preferences

You can customize preference settings for Office 2004 and related programs in your deployment. For example, you can specify a macro security level in Word or Excel or configure a default Exchange account in Entourage. By managing custom preference settings, you can increase the standardization of the Office 2004 experience across your user community.

> **Important** You should log on with the same administrator account during each customization session. This causes all preferences to be stored in the same home folder. This is also the account that you will use later if you are managing preferences with Apple Workgroup Manager. Workgroup Manager uses the preferences associated with this account.

Open each Office 2004 program in your installation image and set the preferences to the values that you want to deploy.

For specific procedures that you may want to use to set selected preferences within Office 2004 programs, see the Configuration and Security sections.

There are several ancillary files in the *username*/Library/Preferences/Microsoft folder that you can customize and deploy. These include the following:

- Custom Dictionary
- Microsoft Office AutoCorrect List (ACL)

You may want to add names or specialized terminology to the Custom Dictionary or the ACL. For more information about customizing the ACL, search for “autocorrect” in Word Help.

To add words to the Custom Dictionary

1. Open the Word 2004 program in your installation image.
2. Open any document.
3. Type any words you want to add to the Custom Dictionary.
4. On the **Tools** menu, click **Spelling and Grammar**.
5. Click **Add** for each word.
6. Click **Close**.

Configuring Exchange accounts for deployment

You can configure and deploy a default Exchange account that has the same information for all users (for example, the server addresses, advanced sending and receiving options, and the address of an Exchange and LDAP server). If you configure an account, you must also enter a default user name, e-mail address, account ID, and password, which each user will customize later.

If you want to set up an Exchange account that uses default settings, you can use the Account Setup Assistant. The Assistant uses the account ID, password, and domain that you provide to automatically detect the correct settings for an account. The Account Setup Assistant uses the Domain Name System (DNS) servers configured in the client Network System Preferences to locate the Active Directory global catalog server that is authoritative for the domain. It then sends an LDAP query using the account ID and password to authenticate the user.

How the Account Setup Assistant works When you set up an Exchange mail account, the Account Setup Assistant tries to locate the information it needs from the Exchange server by performing the following processes:

- The Account Setup Assistant queries the DNS server for all DNS resource records for its domain name. It is looking for the global catalog server for the Active Directory domain to which the user account belongs. To perform this query, the Assistant uses the DNS server configured in the Network Preferences TCP/IP (Transmission Control Protocol/Internet Protocol) connection of the Mac OS. This query returns all the resource records for Active Directory domain controllers that are hosted by the DNS server. After the global catalog server is located, the Assistant performs an LDAP query for the homeMDB LDAP attribute of the user account, which lists the Exchange server for the user account.
- If the query to the DNS server is not successful, the Assistant tries to locate the Exchange server by using the name of the domain that the user enters for his or her Exchange account. For example, if the user enters mydomain.microsoft.com as the domain for an Exchange account, the Assistant creates a DNS query for the name mydomain.microsoft.com. The DNS resource records that the query returns in response to this query include records for the domain controllers in the domain mydomain.microsoft.com.
- If the Assistant cannot find the Exchange server information, it provides a simplified user interface for manual configuration, where the user can enter the information that Entourage could not detect. The Account Setup Assistant then offers to verify the settings specified by the user.

To set up an Exchange account

1. Make sure that the local computer is connected to a network that has access to the Exchange server.
2. In Entourage, on the **Tools** menu, click **Accounts**.
3. Click the **Exchange** tab, and then click **New**. If you see the **New Account** dialog box, click **Assist Me**.
4. Follow the instructions in the Account Setup Assistant.
   - or -
   Click **Configure account manually** to set up the account without the Assistant.

Notes

- When you are prompted to enter an e-mail address, enter a temporary placeholder e-mail address that your users will change later.
- If you want to specify synchronization settings when you set up the account, you can configure the account manually. You can also configure the account manually after the Assistant has tried to configure it automatically.

You have the option to use forms-based authentication with a deployed account. Forms-based authentication must be enabled in Exchange Server and requires that you enable SSL for the account in Entourage.

To enable SSL in Entourage

1. In Entourage, on the **Tools** menu, click **Accounts**.
2. Select the Exchange account, and then click **Edit**.
3. Make sure that Entourage is pointing to your front-end server. On the **Account Settings** tab, in **Exchange Server**, the name of the front-end server should be listed.
4. On the **Advanced** tab, make sure that the **This DAV service requires a secure connection (SSL)** check box is selected.

Configuring Messenger accounts for deployment

You can configure and deploy a default Messenger account that has the same information for all users (for example, the Live Communications Server address, or a setting to prevent users from saving Messenger conversations). Users must enter their account name and password when they first open Messenger. You can also save and deploy contact list files for users to import. For information about configuring Messenger, download the Microsoft Messenger for Mac Deployment Guide from the Resource Kits page of the Microsoft Web site at http://www.microsoft.com/mac.

Managing the AutoUpdate process

The installation methods described in this document for Office 2004 installation on user computers do not install AutoUpdate. However, if a user is logged on with an administrator account, the user can install and run AutoUpdate by starting any Office 2004 program, and then clicking **Check for Updates** on the **Help** menu.

Under Mac OS X, software installation, including updates, requires that the user provide an administrator logon name and password. You should keep confidential the administrator user accounts and passwords for run-time load file servers to prevent users from making software updates or other changes on the servers.

You cannot prevent a user who has an account that has administrator privileges from installing and using AutoUpdate or from downloading updates from the Microsoft Web site. You can, however, use Workgroup Manager or Apple Remote Desktop to reset the AutoUpdate preference settings of any user to Manual or Automatic at intervals that you choose.

To turn automatic update checking on or off

1. On the **Help** menu in an Office 2004 program, click **Check for Updates**.
2. Click **Manually** or **Automatically**.
3. If you clicked **Automatically**, on the **Check for Updates** pop-up menu, click the automatic updates schedule you want.

Your chosen settings are stored in the AutoUpdate preference file, com.microsoft.autoupdate.plist in the Preferences folder.

Managing Apple System preferences

You may also want to centrally manage various Apple System Preferences that affect the operation of Office 2004. These preferences can be managed by using Apple Workgroup Manager or the command-line tools of Apple Remote Desktop. The following table gives examples of Network preference settings that may be relevant. To access these settings, in System Preferences, click **Network**, and then on the **Show** pop-up menu, click the interface that is used to connect to the network.

Apple System Preferences: Network (examples)	Description
TCP/IP tab: Search Domains	Domain information for completing URLs entered by the user that are not fully qualified
Proxies tab	Proxy server port settings

Deploying preferences

Depending on which preferences you want to deploy, you can use either of the following approaches or a combination of the two:

- Deploy preferences by using Workgroup Manager
- Deploy preferences as part of an Apple Installer .pkg (package) file

Deploying preferences by using Workgroup Manager

Office 2004 partially supports the Workgroup Manager solution provided by Apple as a component of Mac OS X Server v10.4. You can use Workgroup Manager to set preferences and define privileges by user, group, or computer, and to perform a broad range of other workgroup management functions. Workgroup Manager runs on a Mac OS X server computer.

You can use this approach to deploy preferences stored in .plist files for Office 2004 and other programs, including many Apple System Preferences. Individual preferences in a .plist file can be managed without disrupting other settings in the same file.

> **Note** Workgroup Manager does not distribute other kinds of files to user home folders. Specifically, Workgroup Manager cannot deploy most Entourage preferences, which are stored in the Entourage database for each identity instead of in .plist files.

Under this approach, you use Workgroup Manager to deploy the preferences in the .plist files that were generated when you customized the Office 2004 installation image. These preferences are stored in the home folder that is associated with the username you were logged on with when you customized the deployment. Because Workgroup Manager deploys the preferences of the user who is currently logged on, you must log on with same username when you use Workgroup Manager to deploy preferences.

Workgroup Manager also offers tools that you can use to change these preference settings or create new ones.

For introductory information about Workgroup Manager, see Workgroup Management in the Mac OS X Server section of the Apple Web site at http://www.apple.com/server/macosx.

For detailed information about managing preferences with Workgroup Manager, see the “Managing Preferences” section of User Management on the Apple Web site at http://www.apple.com/server/documentation.

> **Note** Some Workgroup Manager functionality requires .manifest files. This functionality is not supported by Office 2004, which does not provide .manifest files.

Deploying preferences as part of a .pkg file

If you are installing Office 2004 on user computers, you can deploy custom preference files to user home folders as part of the .pkg file that you deploy to distribute the Office 2004 programs. If you are not installing Office 2004 on user computers, you can deploy a .pkg file that contains preference files to user home folders by using Apple Remote Desktop. You create .pkg files by using Apple PackageMaker.

A .pkg file can contain .plist files, the Entourage database, and ancillary files such as the Custom Dictionary. Apple Remote Desktop does not require a Mac OS X Server. When you deploy a file as part of a package or by using Apple Remote Desktop, the file overwrites all settings in any previous copy of the file in the same location.

Under this approach, you include in the .pkg file the .plist files that were generated when you customized the Office 2004 installation image. You can also include other customized files that are stored outside the Office 2004 folder.

For more information about PackageMaker, see A Quick Look at PackageMaker and Installer and Introduction to Software Distribution on the Apple Developer Connection Web site at http://developer.apple.com/documentation.

Apple Remote Desktop is a desktop management tool that you can use to maintain, upgrade, distribute, and configure software on user computers, collect system hardware and software information about your network of Macintosh computers, and provide remote assistance to users. For an introduction to Apple Remote Desktop, see Apple Remote Desktop 3 on the Apple Web site at http://www.apple.com/remotedesktop. For more information, see Apple Remote Desktop Administrator's Guide on the Resources page in the same area of the Apple Web site.

File locations

Office 2004 preference files are stored in the *username*/Library/Preferences/Microsoft folder.

Exceptions:

- Most Entourage preference settings are not stored in the Entourage preference files, but are stored in the Entourage database, located in the *username*/Documents/Microsoft User Data/Office 2004 Identities/*identityname* folder for each identity. Most users have just a single identity. The default identity name is “Main Identity.”
- The preference file for Microsoft AutoUpdate is named com.microsoft.autoupdate.plist and is stored in the *username*/Library/Preferences folder.
- The preference file for Microsoft Error Reporting Protocol is named com.microsoft.error_reporting.plist and is stored in the *username*/Library/Preferences folder.

Note Some preferences for Office 2004 programs (for example, the current default folder in the **Open** dialog box) are created and managed by Mac OS X and are stored in com.microsoft.*programname*.plist files in the Preferences folder. These files should not be deployed.

If you choose to deploy preferences, you should deploy the following:

- The *username*/Library/Preferences/Microsoft folder if it does not exist on the user computer.
- All files in the Preferences/Microsoft folder.
- If you deploy Entourage settings, you should deploy the *username*/Documents/Microsoft User Data/Office 2004 Identities/Main Identity folder and any files it contains.

Special considerations for deploying Entourage preferences and account settings

When you customize Entourage in the installation image, the preferences that you set and other information that you provide (such as server names) are stored in the Entourage database under the default identity name.

> **Important** If you deploy Entourage settings as recommended into the Office 2004 Identities/Main Identity folder, you must also arrange to preserve any local data that users might already have from a previous use of Office 2004 or Office 2004 Test Drive. To do this, you should rename the existing Main Identity folder in each such case before you deploy the new one. You may want to create and deploy a script for this purpose. Local data means information for which a copy is not present on a mail server. This includes, for example, messages downloaded from POP3 mail servers and locally created information such as Entourage tasks and notes that are not synchronized with Exchange. After the Office 2004 programs are deployed, users can import information from their old identities.

Deploying the Office 2004 programs

To install a retail version of Office 2004 on an individual computer, follow the instructions provided with the retail product.

You cannot deploy retail versions of Office 2004 from a central location across an organization. To deploy Office 2004 centrally, your organization must obtain a volume license. For more information about volume licensing, see Microsoft Office 2004 for Mac license terms in the “Getting Started” section.

Several options are available for deploying a default or customized installation image.

Run-time load options:

- Deploying Office 2004 to run from a net boot image
- Deploying Office 2004 to run from a file server

User computer installation options:

- Deploying Office 2004 for installation on user computers from a file server
- Deploying Office 2004 for installation on user computers by using Apple Remote Desktop
- Deploying Office 2004 for installation on user computers by using NetInstall

Case-insensitive HFS+ file format, the default format for Mac OS X, is required for Office 2004 installation and for home folders of Office 2004 users. The Office 2004 programs and user home folders can be located on the user’s computer or on a file server that uses Apple Filing Protocol (AFP).

User home folders can be located on the user's computer or remotely on a file server that uses AFP.

Important An Entourage user cannot be logged on simultaneously to two computers that access the same identity on a single remote home folder.

The file server can be any of the following:

- A server that is running Mac OS X Server or AppleShare IP
- A Windows 2000 Server or later version running Microsoft Services for Macintosh with optional User Authentication Module (UAM)
- A Windows-based server that is running a third-party product such as ExtremeZ-IP File Server that supports AFP. For more information about ExtremeZ-IP File Server, see the GroupLogic Web site at http://www.grouplogic.com.

Notes

- Microsoft Services for Macintosh uses AFP 2.2, an older form of the Apple Filing Protocol that does not support disconnect/reconnect on sleep/wake and has limitations on the length of supported file names.
- The Microsoft User Authentication Module is not currently supported on Intel-based Macintosh computers.

Run-time load options

Two options are available for deploying Office 2004 programs to load from a server at run time.

Deploying Office 2004 to run from a net boot image

Under this option, you include your default or customized Office 2004 installation image as part of the net boot image. Office 2004 is automatically made available to users when they start their computers. For more information about creating a net boot image, see the documentation for your server operating system.

Deploying Office 2004 to run from a file server

Under this option, you install the default or customized Office 2004 installation image on a file server. Users then load the Office 2004 programs from the server at run time. A variation of this option is to run the installation from a network domain instead of from an individual file server. In this case, the user does not have to connect manually to the file server because the server volume is mounted automatically.

User computer installation options

Three options, described in the following paragraphs, are available for deploying Office 2004 programs to be installed on user computers:

- Installing Office 2004 from a file server
- Installing Office 2004 by using Apple Remote Desktop
- Installing Office 2004 by using NetInstall

In all three cases, you first create an Apple Installer .pkg file from the Office 2004 installation image and other elements by using Apple PackageMaker. The .pkg file contains instructions that specify where Apple Installer should copy each file and folder that you include. The .pkg file should include the following:

- A script to prepare the user computer before you install Office 2004
- The installation image (Office 2004 folder)
- Any customized preference files and folders that you want to deploy, as described in File locations

The recommended contents of the preparation script vary slightly depending on the deployment method.

For more information about AppleScript, see AppleScript Resources for Office 2004 in the Developer Center in the Resources area of the Microsoft Web site at http://www.microsoft.com/mac.

You may find it useful to create the package by using a feature of PackageMaker that automatically selects only items that have changed between two snapshots of a folder. For more information about this feature, see Creating Snapshot Packages with packagemaker on the MacEnterprise.org Web site at http://macenterprise.org.

For more information about PackageMaker, see A Quick Look at PackageMaker and Installer or search for “Introduction to Software Distribution” on the Apple Developer Connection Web site at http://developer.apple.com/documentation.

Installing Office 2004 on user computers from a file server

Under this option, you make the .pkg file available to users by copying it to a shared folder (referred to as the deployment folder) on the network. Users install Office 2004 on their computers by dragging the .pkg file from the deployment folder to their desktop and opening it.

> **Note** If you do not choose to deploy a script or preferences, you do not need to create a .pkg file. You can copy the installation image Office 2004 folder directly to the deployment folder. Users can then install Office 2004 by dragging the Office 2004 folder to the Applications folder on their computers.

Preparing user computers for the file server installation method

Each user computer must be prepared before you begin the installation procedure. We recommend that you include in the .pkg file a script to accomplish the following steps. If you do not include a script that accomplishes all the following steps, you should instruct users to perform the steps that are required immediately before they install Office from the file server.

To prepare user computers for the file server installation method

1. If the computer is currently running the Classic environment (Mac OS 9), switch to Mac OS X and quit the Classic environment. To quit the Classic environment, on the **Apple** menu, click **System Preferences**, and then click **Classic**. On the **Start/Stop** tab, click **Stop**.
2. Turn off virus-protection software, because it might interfere with installation, and quit any programs that are running.
3. Back up any existing Entourage 2004 or Entourage X database or Outlook Calendar and contacts information.

   Users can make a backup copy of their Entourage identity by following the procedure in Backing up the Entourage identity database in the “Maintenance” section. Outlook users can drag Calendar and Contacts folders to an archive folder to help protect data.
4. Remove previous versions of Office, including Test Drives, if present, by using the procedure in Removing previous versions of Office.
5. Remove any Dock icons for Office programs.

User procedure for installing Office 2004 from a file server

Each user drags the .pkg file from the deployment folder to the desktop on his or her computer and opens it. The user is required to provide a username and password for an account that has administrator privileges.

Installing Office 2004 on user computers by using Apple Remote Desktop

Under this option, you use Apple Remote Desktop to distribute the .pkg file onto user computers and open it automatically. You may want to instruct users to leave their computers on overnight so that you can schedule the distribution during non-working hours.

For more information about Apple Remote Desktop, see Apple Remote Desktop 3 on the Apple Web site at http://www.apple.com/remotedesktop.

Preparing user computers for the Apple Remote Desktop installation method

Each user computer must be prepared before you begin the installation procedure. Because users do not control the timing of an Apple Remote Desktop deployment, you must include in the .pkg file a script to accomplish at least the first two of the following steps, and preferably the full set. If you do not include a script that accomplishes all the following steps, you should instruct users to perform the steps that are required before you begin the Apple Remote Desktop deployment.

To prepare user computers for the Apple Remote Desktop installation method

1. If the computer is currently running the Classic environment (Mac OS 9), switch to Mac OS X and quit the Classic environment. To quit the Classic environment, on the **Apple** menu, click **System Preferences**, and then click **Classic**. On the **Start/Stop** tab, click **Stop**.
2. Turn off virus-protection software, because it might interfere with installation, and quit any programs that are running.
3. Back up any existing Entourage 2004 or Entourage X database.

   Users can make a backup copy of their Entourage identity by following the procedure in Backing up the Entourage identity database in the "Maintenance" section. Outlook users can drag Calendar and Contacts folders to an archive folder.
4. Remove previous versions of Office, including Test Drives, if present, by using the procedure in Removing previous versions of Office.
5. Remove any Dock icons for Office programs.

For more information about AppleScript, see AppleScript Resources for Office 2004 in the Developer Center in the Resources area of the Microsoft Web site at http://www.microsoft.com/mac.

Installation methods for use with Apple Remote Desktop

You can specify that Apple Remote Desktop should have Apple Installer open the .pkg file and perform the file copy operations without user intervention. Alternatively, you can instruct users to open the .pkg file after they have prepared their computers. When users open the .pkg file, the files it contains are copied automatically to the locations you specified in the package.

Installing Office 2004 on user computers by using NetInstall

Under this option, you use NetInstall to install the .pkg file onto user computers. NetInstall restarts the user computer at a time that the user chooses, takes control of the computer, installs the package, and then restarts the computer, returning control to the user.

Preparing user computers for the NetInstall installation method

You should create and include in the .pkg file a script to perform the following steps at the beginning of the NetInstall process. If you do not include in the package a script that accomplishes all the following steps, you should instruct users to perform the steps that are required immediately before they run NetInstall.

To prepare user computers for the NetInstall installation method

1. Back up any existing Entourage 2004 or Entourage X database.

   For information about how users can make a backup copy of their Entourage identity, see Backing up the Entourage identity database in the "Maintenance" section. Outlook users can drag Calendar and Contacts folders to an archive folder to help protect data.

2. Remove previous versions of Office, including Test Drives, if present, by using the procedure in Removing previous versions of Office.

3. Remove any Dock icons for Office programs.

User procedure for installing Office 2004 by using NetInstall

1. On the **Apple** menu, click **System Preferences**, and then click **Startup Disk**.

2. Click the NetInstall icon for Office 2004, and then click **Restart**.

   NetInstall restarts the user computer, runs any script you provided, installs the files that are contained in the package to the locations you specified, and then restarts the computer.

Removing previous versions of Office

Use the following procedures to remove previous versions of Office, including Test Drives if present.

Notes

- Removing Office v. X or the Office v. X Test Drive is optional. However, because having multiple versions of Office can be confusing for both the user and the administrator, we recommend removing all versions of Office v. X before you install Office 2004.
- Removing the Office 2004 Test Drive is *required*. Removing Office 2004, if a full version was previously installed, is optional.

First quit any Office daemons that are running, and then remove the Office programs.

To quit the Office daemons

1. In the /Applications/Utilities folder, open Activity Monitor.
2. In the **Process Name** list, click any of the following daemon names that are present, and then on the toolbar, click **Quit Process**. Repeat this step until none of these names appear in the **Process Name** list:

   Database Daemon
   Alerts Daemon
   Microsoft Office Notifications
   Microsoft AU Daemon

   Note If a name appears multiple times, quit all occurrences.
3. If an alias for any of the daemons listed in step 2 is in the /Applications/StartupItems folder, drag it to the Trash.

To remove the Office programs

- Look for the following folders and drag them to the Trash:

Folder name	Associated program
/Applications/Microsoft Office X	Office v. X or Office v. X Test Drive
/Applications/Microsoft Office 2004	Office 2004 or downloaded Office 2004 Test Drive
/Applications/Office Test Drive for Mac (This folder name may have been localized to the language specified for the computer when it was configured the first time.)	Office 2004 Test Drive pre-installed by Apple

First-use setup for each user

Installation is incomplete until the user opens one of the Office 2004 programs. When the user opens the first program, Office 2004 installs additional fonts, if they are required, and collects user information. For more information about controlling the installation of Office 2004 fonts, see Controlling font installation.

Configuring Entourage at first use by user

Make sure that users complete the information in the contact that includes their own information (the Me contact, identified in the Address Book by a highlighted individual Contact Type icon).

Note Users who do not complete this information will not be able to use some features of Office 2004, such as obtaining driving directions in Entourage or displaying their own return address in a letter or envelope created in Word.

Personalizing deployed accounts

If you deployed a default e-mail account, users must double-click the account in the **Accounts** window to add the following account information: name, e-mail address, account ID, and password. To open the **Accounts** window, on the **Tools** menu, click **Accounts**.

Creating new accounts

If you did not deploy an identity, when your users open Entourage for the first time the Entourage Setup Assistant helps them enter their personal information and set up an e-mail account. If you deployed an identity that contains no e-mail account, users must set up their e-mail without the help of the Entourage Setup Assistant.

If users send and receive messages by using mail accounts that you administer, make sure that each user has the following required information:

- An e-mail address
- The protocol for the account type on the mail server (IMAP, POP, SMTP, Exchange)
- An account ID, the part of the e-mail address before the at sign (@)

If a user sets up a mail account that you do not administer, the user must obtain the information from his or her Internet service provider (ISP).

Users might also need the following networking information:

TCP/IP settings	To connect to the Internet, users might have to adjust the settings in the **Network** preferences pane in Mac OS X System Preferences.
Proxy server settings	If your organization uses a proxy server to send and receive messages, users can enter the settings in the **Network** preferences pane in Mac OS X System Preferences.
Security settings	Depending on how the mail server is configured, users can specify more than the default level of security by setting some of the advanced sending and receiving options. For more information about Entourage 2004 security options, see the Security section.

Importing information into Entourage 2004

If users are changing to Entourage 2004 from a different e-mail program or personal information manager (PIM), they can import information that was created in the previous program. This information can include messages, contacts, accounts, rules, signatures, preferences, events, tasks, notes, and custom views.

> **Note** You may want to advise users to back up any data before exporting it to a file or importing it from another program.

Importing information during setup

If a user previously used Microsoft Outlook Express 5.0, Microsoft Entourage 2001, or Microsoft Entourage X, and he or she has an identity folder from any of these programs, the user can import data from one of these identities during step 3 of the Entourage Setup Assistant.

If no Office 2004 identity is found when Entourage 2004 is started, a new identity named Main Identity is created by Entourage Setup Assistant. If the user imports data during setup, the data is imported into Main Identity.

For more information about importing from Outlook Express and Entourage, see the list below.

Importing information after setup

If a user does not import information from a previous Office identity during setup, he or she can import it later. To do this, the user can open Entourage, click **Import** on the **File** menu, and then follow the instructions in the Import Assistant. Information is imported into the active identity.

Importing data directly from other programs

Users can import information directly from the following programs:

- Microsoft Office 2004 archive file
- Microsoft Outlook 2001 for Mac
- Microsoft Entourage X
- Microsoft Entourage 2001
- Microsoft Outlook Express 5.0 or a later version
- Qualcomm Eudora (any version)
- Netscape Communicator (versions 4.*x* only)
- Claris Emailer 2.0v3
- Now Contact or Now Up-To-Date 3.8 or a later version

To import data from these programs into Entourage 2004, users can click **Import** on the **File** menu, and then follow the instructions in the Import Assistant. For more information about specific products, see the following entries.

Importing archive files from Microsoft Office 2004

If the user has an archive (.rge) file from a previous installation of Office 2004, the file can be imported into the active identity.

To import an Office 2004 archive file

1. On the Entourage **File** menu, click **Import**.
2. Make sure that **Import information from an Entourage archive** is selected, and then click the right arrow.
3. Click the archive file that you want to import, and then click **Import**.

Importing PST files from Microsoft Outlook 2001 for Mac

Microsoft Outlook 2001 for Mac users can import their Personal File Folder (PST) files into Entourage 2004 by using the PST Import Tool.

To import Outlook 2001 for Mac PST files into Entourage

1. On the Downloads page of the Microsoft Web site at http://www.microsoft.com/mac, download the PST Import Tool for Entourage 2004 for Mac.
2. Make sure that Entourage 2004 is running, and then double-click **PST Import Tool**.
3. Follow the steps in the wizard to select a .pst file and import it into Entourage 2004. Users can specify the types of data, such as e-mail messages or Calendar items, to import.

Important The PST Import Tool imports only PST files that were created in Outlook 2001 for Mac.

If the user switches Entourage identities during the import process, the import process stops responding. If this occurs, the user must double-click **PST Import Tool** again.

To import a PST file by using the PST Import Tool, the user must have read permissions for the PST file.

The PST Import Tool download includes a Help file that can help users diagnose problems.

Importing data from Microsoft Entourage X or Entourage 2001

Custom Views that filter on more than one area are imported into the new Custom Views area of Entourage 2004. Custom Views that filter on only one area (Mail, Address Book, Calendar, and so on) are imported into the Custom Views section of that area. For example, a Custom View that filters on Address Book is imported into the Address Book section of Custom Views. Also, folder synchronization settings for schedules that receive messages from IMAP and Hotmail accounts are not imported. The user must reenter folder synchronization settings for such schedules.

Users who have Exchange mail accounts in Exchange Update for Entourage X, which is part of Office v. X (10.1.4), can import server-side contact, Calendar, and mail items from the old account to the new Entourage 2004 account.

Importing data from Microsoft Outlook Express 5.0 or a later version

If the user selected default fonts for displaying, creating, or printing items in Outlook Express — for example, if he or she selected the default font for messages in HTML format — the user must restart Entourage after the import process is complete to update these settings in Entourage.

If the user selected an AppleScript script to run as part of a rule, schedule, or action by the Junk Mail Filter in Outlook Express, the script must be updated to work with Entourage. This can be as simple as opening the script in the Script Editor and replacing "Outlook Express" with "Microsoft Entourage" in any "tell application" statements in the script. After the script is updated, the user must open the rule, schedule, or Junk Mail Filter in Entourage, and then select the updated script.

Importing data from Microsoft Outlook Express 4.5

Entourage 2004 does not support importing data directly from Outlook Express 4.5 or earlier versions. To import this data, first upgrade to Outlook Express 5, and then import the data from Outlook Express 5 into Entourage.

Importing data from Qualcomm Eudora (any version)

Because Entourage 2004 does not import the status of messages (whether they are read or unread), the status of all imported messages is marked as unread in Entourage. After the messages are imported, the user can quickly mark all the messages as read. To do this, the user clicks the imported folder in the Folders list, and then clicks **Mark All as Read** on the **Message** menu. Additionally, Entourage does not maintain links between imported messages and their attachments; however, the attachments are stored in the user's Documents/Microsoft User Data/Saved Attachments folder.

Importing data from Netscape Communicator 4.X

During the import process, when users are prompted to select the Netscape user's folder that contains the data they want to import, make sure that they select the folder that contains their profile folder (the Netscape user's folder), not the profile folder itself. If the user has stored his or her profile folder in a different location — for example, in the user's Documents folder — select that folder instead.

Importing data from Claris Emailer 2.0v3

When users import data from Claris Emailer, Entourage automatically starts Emailer. Emailer must be running for Entourage to import data from it.

If users have problems importing data from Claris Emailer, try assigning more memory to Emailer by using the **Get Info** dialog box in the Finder. For more information about assigning more memory to a program, see Mac Help in the Classic environment. After you assign more memory to Emailer, open both Emailer and Entourage, and then begin the import process again.

Because account settings, priorities, rules, mail actions, and schedules cannot be imported from Claris Emailer, users must re-create these items in Entourage. Additionally, Entourage does not maintain links between imported messages and their attachments; however, the attachments are stored in the user's Documents/Microsoft User Data/Saved Attachments folder.

Importing data from Now Contact or Now Up-To-Date 3.8 or a later version

When users import data from Now Contact or Now Up-To-Date, Entourage 2004 automatically starts Contact or Up-To-Date and opens the default data file for the program. However, sometimes users should open Contact or Up-To-Date manually and open the data file that contains the data they want to import before they begin the import process in Entourage. Users must open the program manually if they meet one or both of the following conditions:

They have created more than one data file for Contact or Up-To-Date.

They try to import data and the import stalls, or alerts them of an Apple event time-out, or does not import any data.

Similarly, if users are using a trial version of Now Contact or Now Up-To-Date, make sure that they manually open the program and, before they begin the import process in Entourage, dismiss the initial dialog box that prompts them to register the program.

Because categories cannot be imported from Now Contact and Now Up-To-Date, users must re-create their categories in Entourage. To do this, on the **Edit** menu, point to **Categories**, and then click **Edit Categories**. Also, some types of attachments for contacts and events cannot be imported.

Importing data from a text file

Users can import data directly only from the programs listed earlier. However, users can import contacts and messages from other programs by first exporting the contacts or messages from the other program as a text file, and then importing the file into Entourage. For example, users can export contacts from Microsoft Outlook as a tab-delimited text file and then import the file into Entourage. For more information about exporting data from a specific program, see the documentation for the program.

Users can import the following types of data from a text file:

- **Messages** A user can import messages that have been saved as an MBOX-format text file, a format typically used by UNIX-based systems such as Apple Mail. An MBOX-format text file is a single file that can contain many messages. When the user imports an MBOX-format text file into Entourage, the imported messages appear in a new folder in the Folder list. Users can quickly import an MBOX-format text file by dragging the file from the Finder to the Entourage Folder list.
- **Contacts** Users can import contact information from a text file that was exported from any program, including spreadsheet and database programs. The text file must be exported in tab-delimited or comma-delimited format. For more information about exporting contacts to a text file, see the documentation for the source program.

  Before importing the contact information, users can specify how data fields in the source program correspond to fields in Entourage. For example, if the source program contains a field named Business Phone, users can specify that the data in that field is imported to a Work Telephone field in Entourage. This process is referred to as *mapping*.

To import contact information from a text file

1. On the **File** menu, click **Import**. Select **Import information from a text file**, and then follow the instructions in the Import Assistant.
2. After you select the file that you want to import, the **Import Contacts** dialog box appears and displays data from the first contact record in the file. Fields that correspond to Entourage fields appear opposite their counterparts in the **Mapped fields** box. Fields that do not correspond to Entourage fields appear in the **Unmapped fields** box. You can then adjust the mapping before you import the file.
   - To use previously saved mapping settings, click the settings on the **Map fields using** pop-up menu.
   - To correct mapping errors, drag fields from the **Unmapped fields** box to the right side of the **Mapped fields** box or from one location to another in the **Mapped fields** box.
   - To view other contact records and verify that the data is mapped correctly, click **Next** or **Prev**.

   When you replace a data field in the **Mapped fields** box with one from the **Unmapped fields** box, the replaced data moves to the **Unmapped fields** box. You can then assign that data to a different field. Fields that remain in the **Unmapped fields** box after you click **Import** are added to the **Notes** field in the contact.
3. After the data is mapped correctly, click **Import**.

Users can also import contacts from vCard-format text files. To import a contact to Entourage 2004, export the contact from the program where it was created to a vCard format text file, and then drag the file to the Entourage icon.

For more information about importing contacts into Entourage 2004, including troubleshooting topics, see Entourage Help.

Calendar Users can import Calendar events from vCal-format and iCal-format text files. To import an event to Entourage 2004, the user exports the event from the program where it was created to a vCal-format or iCal-format text file, and then drags the file to the Entourage icon.

Tip You can also use the Entourage text importing features to provide standard data to all your users. For example, you can create a tab-delimited or comma-delimited text file that contains contact information for members of your organization and distribute it when you deploy Office 2004.

Deploying Virtual PC

For information about installing, configuring, and using Virtual PC for Mac, download the Virtual PC version 7 for Mac Deployment Guide from the Resource Kits page of the Microsoft Web site at http://www.microsoft.com/mac.

Deploying Microsoft Messenger for Mac

For information about deploying Messenger, download the Microsoft Messenger for Mac Deployment Guide from the Resource Kits page of the Microsoft Web site at http://www.microsoft.com/mac.

Security

Office 2004 security environment 77
Overview of Office 2004 security 77
User information 78
Macro security in Office 2004 81
Scripts embedded in e-mail or documents 83
Helping reduce potential security threats 83
Word security 85
Using password protection 86
Opening documents as read-only 87
Protecting form fields 87
Protecting documents during reviews 87
Excel security 88
Using password protection 88
Limiting access to workbook and worksheet elements 90
Protecting the change history for a shared workbook 91
Removing personal or hidden information from a workbook 91
Entourage security 92
Configuring Entourage security features to help prevent viruses 93
Message security 94
Enabling or disabling Secure Sockets Layer (SSL) 100
Importing a self-signed SSL certificate 101
Enabling or disabling password protection 103
Enabling or disabling SMTP authentication 103
Authentication and security using WebDAV 104
Working with Internet Security and Acceleration (ISA) Server 104
Smart card support 105
Messenger for Mac security 105
Virtual PC for Mac security 106
Windows Services for Macintosh 106
Mac OS X Security 107

This section provides details about the security features available to users and administrators of Microsoft Office 2004 for Mac. Administrators supporting Office 2004 can use their knowledge of these features to perform the following tasks:

- Instruct users about how to help improve the protection of their information.
- Assess the security of networks and systems.

Office 2004 security environment

To establish the most secure computing environment possible, you must limit the vulnerability of programs and data to malicious attacks. Unfortunately, eliminating all the possible vulnerabilities in an organization's security is impossible. However, you can help establish a more secure environment by limiting the number of possible avenues of attack.

The methods discussed in this section of the *Resource Kit* should help you implement procedures to limit direct assaults on your organization's data from external and internal attacks. As part of implementing these methods, you must train users on how to help protect themselves and the organization from attack. This training builds user awareness about the issues of security and ownership of the data they are trying to protect.

Users who understand possible security threats and know how to implement security plans are the first line of defense against unauthorized access to content. Untrained users can unintentionally expose an organization to unauthorized or malicious use of its data. If you establish a corporate policy for how files are distributed and handled, you can help reduce security vulnerabilities caused by untrained users.

Overview of Office 2004 security

Office 2004 provides methods and features for helping you manage program and document security. Understanding how to use and set the following security-related features in Office 2004 can help you establish a more secure environment:

- User information
- Macro security
- Password and encryption protection
- Encryption and digital signatures
- Trusted sources
- Privacy options

Note You can find security updates and software updates for Office 2004 on the Downloads page of the Microsoft Web site at http://www.microsoft.com/mac. To review a description of the changes that are included in an update, click the update or service pack. You can also use Microsoft AutoUpdate to check for updates to your Microsoft software. For more information about security and other updates, see Managing Office 2004 product updates in the "Maintenance" section.

User information

Office 2004 shares the personal information that users enter during setup among all Office 2004 programs that are installed on the computer. Users should be familiar with the user information that accompanies Office 2004 documents so that they can help make sure that a level of privacy is maintained. As an administrator responsible for corporate security, you should understand how the information is stored in Office 2004 programs and which program features might have to be administered to help maintain this privacy.

Office 2004 programs use identity information to personalize the output of certain features. For example, Microsoft Word, Microsoft Excel, and Microsoft PowerPoint add a user name and a company name to the **Summary** tab in the **Properties** dialog box, and add a user name as a label to comments and revision marks. Word uses this information in documents to generate a return address on envelopes and labels and in wizards that are used to help create letters and other kinds of documents. Word also uses this information when a user opens the business templates in the Project Gallery. Excel uses this information to create custom headers and footers that contain a user name or company name.

When a user opens an Office 2004 program, the program recognizes the current user's identity information. This is referred to as the "active identity." In Word, Excel, and PowerPoint, the active identity determines the author of a document. The active identity also determines which contact information appears in documents created by using templates, such as in the return address for a letter created in Word. Because a user can flag and receive a reminder to follow up on any Office 2004 document, identities also help make sure that each person receives reminders for only his or her own documents.

You can choose to recommend the practice of editing or removing the author and contact information that appears in documents created by using templates. This practice will help ensure that a level of privacy is present in all documents sent outside your organization's network.

You can instruct users to update or remove personal contact information in the following locations:

- In Word, on the **Word** menu, click **Preferences**, and then click **User Information**.
- In Excel, on the **Excel** menu, click **Preferences**, and then click **General**.
- In PowerPoint, on the **PowerPoint** menu, click **Preferences**, and then click **Advanced**.
- In Microsoft Entourage, click **Address Book**, double-click the contact that appears with the **Contact is Me** symbol (highlighted individual Contact Type icon) next to it, and then click the tabs that contain the information to change.

Note When users update the information in any Office 2004 program, it is automatically updated in the other programs.

Unless users send their documents to Microsoft, Microsoft does not have access to any information from the documents.

Entourage identity database

An identity stores a person's Entourage preferences, account settings, Project Center information, Address Book and Calendar information, schedules, tasks, messages, and more. An identity can also store personal information, such as a person's e-mail address and street address, after this information has been entered as a contact and the contact has been marked as **Contact is Me**. When an identity is being used, it is referred to as the "active identity."

When Entourage is installed on a computer, the identity that is currently active in Entourage determines whose user information appears in the other Office 2004 programs.

In Entourage, users can create multiple identities, so that they can more easily share one computer with several people. To ensure that Office 2004 programs use the correct information, a user must either:

- Log on to the computer by using his or her own logon information.
- Switch identities in Entourage.

To switch between identities, the user must close all other Office 2004 programs, and then on the **Entourage** menu, click **Switch Identity**. After the Entourage window closes, users can choose a different identity in the dialog box that appears. Users can display this dialog box automatically every time Entourage is opened, so that each person can choose an identity when he or she opens Entourage.

If more than one user shares a Mac OS account and uses Entourage on the same computer, each user can set up a separate identity so that he or she can configure Entourage to reflect individual preferences. This feature ensures that each person can access his or her own messages, Calendar events, and other items, without having to log on to the computer as a separate user. If your organization supports multiple users on a single computer, you might want to show users how to use identities in Entourage to conduct their individual communications.

Identities are associated with a Mac OS user account. If a user who has a Mac OS account allows other users to use Entourage on his or her computer without logging on to the computer as separate users, the user who has the Mac OS account can maintain the security of the account by not sharing the password for his or her Mac OS user account with the other users.

> **Note** Switching between multiple identities of a single user in Entourage is not controlled by a password.

The first time Entourage is opened, the Microsoft User Data folder is created in the user's Documents folder. The database for each identity is stored in its own folder inside the Microsoft User Data/Office 2004 Identities folder. The following information is stored in the database:

- All Entourage data, such as messages, schedules, tasks, contacts (including the Word Address Book), and preferences
- Project Palette data
- Scrapbook clips

You can move the entire Microsoft User Data folder or only the folder for any single identity, to a different location, such as to another hard disk attached to the computer or to a network. However, if the folder is moved, an alias to the folder must be placed in the folder's original location. Otherwise, Entourage will not be able to find the user data.

For more information about customizing and deploying Office 2004, see the Deployment section.

Relationship with Mac OS user account

If multiple users share a Mac OS user account and use Entourage on the same computer, the security of the computer depends on the security features of the Mac OS user account password. Mac OS X uses four main types of passwords:

- **User account password** A user account password allows users to log on to their home folders. This is often referred to as a "logon password." The user account password provides the most security when multiple users are sharing one Mac OS account and using Entourage on the same computer.
- **Administrator password** An administrator password is needed before an administrator can perform many tasks on the computer. These include setting system preferences, installing software, and administering user accounts. An administrator password is an administrator user's logon password.
- **Master password** The master password is a computer-wide password set up by an administrator as a safeguard in case the administrator forgets his or her logon password. The master password is usually used together with FileVault. FileVault is a way of encrypting a user's home folder so that it cannot be seen by anyone but that user. If a FileVault user forgets his or her logon password, even an administrator cannot log on to the user's account by using an administrator password. Only the master password can override a FileVault user's password.
- **Keychain password** The keychain stores passwords for various programs and resources on the computer. The keychain password "unlocks" the keychain so that the passwords inside it can be used. The password for the default keychain is the same as the logon password when the account is first set up.

Users can use the keychain to store passwords that access servers, Web sites that have enhanced security, shared folders, and password-protected documents. Users can create an additional keychain for personal use that is not automatically unlocked when they log on to their personal account. Users can create additional keychains with passwords that differ from the default logon keychain and logon password. If a user forgets the password to these keychains, neither the user nor an administrator can access them.

For more information about Mac OS passwords, see Mac Help.

Microsoft Error Reporting Protocol

Office 2004 includes the Microsoft Error Reporting Protocol (MERP) to enable users to communicate bug data anonymously to Microsoft. Microsoft uses the bug data to quickly locate and fix software problems and help increase the overall stability of Office 2004. By default, Microsoft Error Reporting is enabled in Office 2004.

If an Office 2004 program stops responding, MERP generates a report that details the circumstances. The MERP user interface asks users to send error report data to Microsoft through the Internet. For an explanation of what the data is, why we collect it, and what we do with it, see Microsoft Online Crash Analysis at http://oca.microsoft.com.

You should review the data collection policy for Microsoft Online Crash Analysis and determine whether this policy is compatible with the privacy standards of your organization. You will want to establish a policy for your organization that specifies whether users should send error report data to Microsoft.

To disable Microsoft Error Reporting in Office 2004

1. Open the Microsoft Error Reporting program, located in the Microsoft Office 2004/Office folder.
2. On the **Microsoft Error Reporting** menu, click **Preferences**.
3. Clear the **Enable Microsoft Error Reporting** check box.

Preferences for Microsoft Error Reporting are stored in com.microsoft.error_reporting.plist. This file is located in the Preferences folder in a user's Library, and can be deployed from a central location across your organization.

If you prefer to disable MERP reporting across all the Macintosh computers in your network, you can use one of the options described in Deploying preferences in the “Deployment” section.

Macro security in Office 2004

This section discusses how Office 2004 helps protect your data from macro viruses. By understanding the options available, you can help your Office 2004 users prevent macro virus infections.

Macro viruses

Office 2004 does not scan a floppy disk, hard disk, removable media, or network drive to find and remove macro viruses. For this kind of protection, you must purchase and install antivirus software. However, by default, Office 2004 displays a warning message whenever a user opens a document that contains macros. Users can then decide whether to open the document with the macros enabled or to disable the macros so that the document can be viewed. If a user disables macros, the macros will not be displayed and the document will be read-only. A macro virus can be harmful only if the macro can run. If users disable the macros, they can open the document more safely.

If users expect documents to contain useful macros, they can click **Enable Macros** to open the document with the macros enabled.

If users do not expect the document to contain macros, or do not know or are not sure of the reliability of the document's source, they should click **Disable Macros** to open the document with macros disabled. For example, a user might notify an administrator that he or she received a document as an attachment to an e-mail message from an unfamiliar source or from a network or Internet site that is not secure. In these cases, you can talk to the originator of the document to verify that it is free of viruses, or instruct the user to click **Disable Macros**.

To turn macro virus protection on or off

1. On the **Application** (**Word** or **Excel**) menu, click **Preferences**, and then click **Security**.
2. Select or clear the **Warn before opening a file that contains macros** check box.

   Caution If a user disables macro virus protection, he or she runs the risk of the computer being infected by a virus, which could cause serious damage to data.

Modifying digitally signed macros

Office 2004 does not recognize digital signatures in macros. Therefore, it cannot update the signature if a user modifies a signed Microsoft Visual Basic for Applications (VBA) macro. Therefore, to prevent modifications, users cannot view in Office 2004 the code for macros that have been digitally signed in the Visual Basic Editor in Microsoft Office for Windows. To view or modify a signed VBA macro in Office 2004, the user must ask the owner of the macro to provide an unsigned version of the macro.

Macro security troubleshooting

The following troubleshooting scenarios provide information about how to resolve the most common macro security issues.

- **User cannot use a macro in a document or add-in program that he or she opened** The user might have chosen to disable macros when the user opened the document. To run the macros, instruct the user to close and then reopen the document or unload and reload the add-in program, and then click **Enable Macros**.
- **User cannot view the macros in a document or add-in program** The macros might have been digitally signed from within the Visual Basic Editor in Office for Windows. Office 2004 for Mac does not recognize digital signatures in macros. Therefore, it cannot update the signature if a user modifies a signed Visual Basic for Applications macro. Users cannot view in Office 2004 the code for macros that have been digitally signed in Office for Windows.

- **Users continue to receive a warning about macros** If the user does not expect the document to contain a macro, the document might have become infected by a virus. Check the computer for viruses, and then try to obtain an uninfected copy of the document from the originator of the document.

  The macro might be in a file that the user downloaded as a page from a Web site and opened as a temporary file. If the virus scanner reports that it has removed a virus in this file every time that the user opens it, the scanner is removing the virus from the temporary file only and not from the original file on the Web server. Check the computer for viruses, and then notify the originator of the file about problems with the macros in the file.

  The document might contain legitimate macros; however, Office 2004 cannot distinguish between safe and unsafe macros. Users can turn off macro virus protection if they no longer want to see these messages.

Scripts embedded in e-mail or documents

To make sure that a user's computer and a user's privacy remain safe from malicious software, Entourage does not run scripts or download files that are contained in complex-HTML messages. Complex HTML is most frequently used by organizations to send newsletters, Web pages, and announcements as messages. However, it can be used by anyone to run scripts or download files that might harm a user's computer or pose a risk to your privacy. Entourage also provides a preference setting that enables users to disable complex HTML. When complex HTML is disabled, users continue to receive complex-HTML messages, but Entourage removes all the special formatting when users open or preview the messages.

For more information about working with complex-HTML messages in Entourage, see Using Complex HTML in the "Configuration" section.

Helping reduce potential security threats

Recent enhancements to Office 2004 improve overall security across the Office 2004 programs. Some of these improvements are at the source code level – for example, recent changes reduce exposure to buffer overflow attacks and specify how attachments to e-mail messages are run. These changes in how Office 2004 programs are installed and run help reduce possible security threats.

Even with all these changes, it is still up to you as the administrator to create and test an installation of Office 2004 that meets the security needs of your organization. This may require a full evaluation of all the sections of Office 2004 programs that perform any of the following processes:

- Access the Internet
- Receive or send e-mail messages
- Receive attachments
- Run add-ins or macros

In addition, you must establish a secure process for how passwords are created and maintained.

Ultimately, Office 2004 programs are only as secure as the network, operating system, and passwords used to help secure access to data that was created by the programs. The following offers general guidelines about the security features of Office 2004 and information about how you can augment the built-in security-related features with simple changes in how Office 2004 is deployed and used.

Evaluate security-sensitive features

Several features of Office 2004 have security-sensitive areas. Specifically, any feature that requires that users access the Internet or that allows users to access the network is considered a possible security risk. Your virus-checking software can help ease many problems associated with these entry points; however, you must also be diligent about protecting the network against intrusion from external communication lines. To be as security conscious as possible, you should:

- Keep virus-checking software current with updates available from the virus-checking software manufacturer.
- Install a proxy server to disable access to potentially unsafe Web sites.
- Reduce the access of external TCP/IP to open ports on your local network. Knowing which ports are open can help you assess the security of your system or troubleshoot connection problems. You should close the ports that you do not use.

You might also want to disable access to some features and settings of Office 2004 programs. To do so, you can customize preference settings for each Office 2004 program in your deployment. You can also examine the preferences and settings for the Mac OS to determine whether any of the settings may help provide for a more secure computing environment. For more information about managing preferences for Office 2004 programs, see Deploying preferences in the “Planning” section.

Evaluate all external software

Executable files purchased from software manufacturers should always have a valid digital signature as part of a certificate obtained from a certification authority. If a product does not have a valid certificate of trust, we recommend that you not install it. However, if that is not an option, evaluate the product before you distribute it to users to make sure that it performs only as expected and does not intentionally or unintentionally distribute a virus.

> **Note** When you activate or install any executable file that works with Word 2004 and Excel 2004, you are presented with a certificate of trust that you must accept before you can continue. If such a request is not presented, the certificate of trust might have been accepted previously or the macro virus protection might be turned off.

Reduce access points that pose security threats

You can help reduce the threat of a security attack by minimizing entry points for attack and by installing virus-checking software and keeping it up to date. Here are some of the ways you can reduce security risks:

- Install a firewall.
- Implement password access to the network.
- Enforce password and rights management to servers and shares in the corporate network.

Each of these is a critical step in reducing security risk. In addition, you must train your users to recognize and implement safer security methods. For example, to eliminate several entry points for worms, viruses, and Trojan horse programs, you would instruct users not to open suspicious e-mail messages or run unapproved programs downloaded from the Web or brought from home.

You can also reduce security risk by deploying only the programs that are required for getting the work done in your organization and by turning on only the preferences and options required for business purposes. Use the custom installation option in Setup Assistant to install only the programs you want. Before you deploy Office 2004 in your organization, use a test computer to evaluate the various configurations that you create. Then, create a custom installation image to deploy. For more information about customizing and deploying Office 2004, see the Deployment section.

Word security

The security and protection features Word provides can limit or restrict access to a document. Administrators will want to review these features with users who will be sending sensitive documents outside the organization. The following security and protection features are available:

- Require users to enter a password to open a document. This prevents unauthorized users from opening the document.
- Require users to enter a password to modify a document. This allows only authorized users to make changes to the document. If someone who has not entered the password changes the document, that person can save the document only by giving it a different file name.
- Have Word recommend opening a document as read-only to suggest, but not require, that users open a document as read-only. If a user opens the document as read-only and then changes it, that person can save the document only by giving it a different file name.
- Prevent users from changing a form. For example, you can apply a level of protection to a form to help prevent unauthorized users from typing information anywhere in the form other than in designated areas.
- Check for macros that might contain viruses whenever the user opens a document.
- Instruct users to remove personal information from documents.

Using password protection

In Word, passwords have several uses. A password can contain any combination of letters, numerals, spaces, and symbols, and it can be up to 15 characters long. Passwords are case sensitive.

You should remind users that when they create a password for a Word document, they should write it down and keep it in a secure location. If the password is lost, the user cannot open or gain access to the password-protected document.

To require users to enter a password to open or modify a document

1. Open the document.
2. On the **File** menu, click **Save As**.
3. Click **Options**, and then click **Security**.
4. Do one or more of the following:

To	Do this
Require users to enter a password to open a document	1. In the **Password to open** box, type a password, and then click **OK**. 2. In the **Confirm Password** dialog box, type the password again, and then click **OK**.
Require users to enter a password in order to modify a document	1. In the **Password to modify** box, type a password, and then click **OK**. 2. In the **Confirm Password** dialog box, type the password again, and then click **OK**.
Change a document password	1. In the **Password to open** or **Password to modify** box, select the symbols that represent the existing password. 2. Type the new password, and then click **OK**. 3. In the **Confirm Password** dialog box, type the password again, and then click **OK**.
Delete a document password	1. In the **Password to open** or **Password to modify** box, select the symbols that represent the existing password. 2. Press DELETE, and then click **OK**.

5. Click **Save**.

Opening documents as read-only

You can suggest that users configure documents that they will be sending outside the organization to be opened as read-only documents.

To set a read-only recommendation

1. Open the document.
2. On the **File** menu, click **Save As**.
3. Click **Options**, and then click **Security**.
4. Select the **Read-only recommended** check box, and then click **OK**.
5. Click **Save**.

Protecting form fields

After a user creates a form that other users will view and complete in Word, the creator of the form must protect it so that users can enter information only in the designated areas.

To prevent users from changing a form that contains form fields

1. On the **Tools** menu, click **Protect Document**.
2. Click **Forms**.
3. To assign a password to the form so that users who know the password can remove the protection and change the form, type a password in the **Password (optional)** box. Users who do not know the password can still enter information in the form fields.
4. Do one of the following:
   - To protect the entire form, click **OK**.
   - To protect only parts of a form, those parts must be in separate sections. Click **Sections**, and then clear the check boxes of the sections that you do not want to protect.

Protecting documents during reviews

As part of preparing a document for review, you can specify that others can change the document only by inserting comments or by inserting comments and tracked changes with revision marks. For added security, you can assign a password to ensure that users do not remove this type of protection.

To prepare copies of a document to be reviewed

1. Open the document that you want to prepare for review.
2. Determine whether the document contains multiple versions by clicking **Versions** on the **File** menu.

   If multiple versions exist, save the current version as a separate document that has a different name, and use this copy as the review copy. This prevents reviewers from opening and viewing earlier versions of the document.
3. On the **Tools** menu, click **Protect Document**.
4. Do one of the following:
   - To let others change the document by inserting comments and tracked changes, click **Tracked Changes**.
   - To let others insert only comments, click **Comments**.
5. To let only authorized reviewers insert comments or changes, type a password.

Excel security

Excel provides the following security and protection features:

- Add, change, or remove password protection.
- Limit access to workbook and worksheet elements.
- Protect the change history for a shared workbook.
- Check for macros that might contain viruses whenever the user opens a workbook.
- Remove personal or hidden information from a workbook.

You should encourage the use of these security and protection features with Excel users who are handling sensitive organization data in Excel workbooks.

Using password protection

The features in Excel for hiding data and protecting worksheets and workbooks by using passwords are not intended to be used as ways to help secure data or help protect confidential information. However, you can recommend that these features be used for other reasons —typically, to present information more clearly by hiding data or formulas that might confuse some users, and to help prevent the wrong user from making an accidental change to workbook data. Excel does not encrypt the data that is hidden or locked in a workbook. Given sufficient time and knowledge, any user can obtain and modify any data in any workbook he or she has access to. To help prevent this, and to help protect confidential information, you can limit access to any Excel worksheets and workbooks by storing them in locations available only to authorized users.

Users can protect separate elements in a worksheet, protect an entire worksheet, or protect an entire workbook. They can also use passwords to restrict access to an entire workbook or to restrict users to read-only access of a workbook.

Passwords are case sensitive. Users must type a password exactly as it was created by the workbook owner. When a user creates a password, he or she should write it down and keep it in a secure location. If the password is lost, users will not be able to open or gain access to the data in a password-protected workbook.

To add, change, or remove password protection

1. On the **File** menu, click **Save As**.
2. Click **Options**, and then do one or more of the following:

To	Do this
Require users to enter a password in order to open a workbook	1. In the **Password to open** box, type a password, and then click **OK**. 2. In the **Confirm Password** dialog box, type the password again, and then click **OK**.
Require users to enter a password in order to modify a workbook	1. In the **Password to modify** box, type a password, and then click **OK**. 2. In the **Confirm Password** dialog box, type the password again, and then click **OK**.
Change a workbook password	1. In the **Password to open** or **Password to modify** box, select the symbols that represent the existing password. 2. Type the new password, and then click **OK**. 3. In the **Confirm Password** dialog box, type the password again, and then click **OK**.
Delete a workbook password	1. In the **Password to open** or **Password to modify** box, select the symbols that represent the existing password. 2. Press DELETE, and then click **OK**.

3. Click **Save**.
4. If prompted, click **Replace** to replace the existing workbook with the open workbook.

Note In a workbook that has been password protected from modifications only, a user can save changes without using the password by first opening the workbook as read-only. The user makes the changes he or she wants in the workbook, and then saves it with a different name. The workbook saved with a new name does not require a password and is available for editing.

Limiting access to workbook and worksheet elements

To limit access to workbook and worksheet elements, do one or more of the following:

To	Do this
Prevent users from making changes to cells on worksheets or to data and other items in charts, and from viewing hidden rows, columns, and formulas	1. Before you protect the worksheet, hide any formulas that you do not want to be visible and unlock any cells that you want to be accessible for changes when the worksheet is protected. 2. On the **Tools** menu, point to **Protection**, and then click **Protect Sheet**. 3. Under **Protect worksheet for**, select the **Contents** check box.
Prevent users from making changes to graphic objects on worksheets or in charts	1. Unlock any graphic objects that you want to be able to change after you protect the worksheet. 2. On the **Tools** menu, point to **Protection**, and then click **Protect Sheet**. 3. Under **Protect worksheet for**, select the **Objects** check box.
Prevent users from making changes to the definitions of scenarios on a worksheet	1. On the **Tools** menu, point to **Protection**, and then click **Protect Sheet**. 2. Under **Protect worksheet for**, select the **Scenarios** check box.
Protect the structure of a workbook so that worksheets in the workbook cannot be moved, deleted, hidden, unhidden, or renamed, and new worksheets cannot be inserted	1. On the **Tools** menu, point to **Protection**, and then click **Protect Workbook**. 2. Under **Protect workbook for**, select the **Structure** check box.
Use windows of the same size and position every time that the workbook is opened	1. On the **Tools** menu, point to **Protection**, and then click **Protect Workbook**. 2. Under **Protect workbook for**, select the **Windows** check box.

To prevent other users from removing workbook protection

- In the **Password (optional)** box, type a password, click **OK**, and then retype the password.

  Passwords are case sensitive. When you assign a password, write it down and keep it in a secure location. If you lose the password, you cannot gain access to the protected workbook or worksheet elements.

Protecting the change history for a shared workbook

This procedure sets a password to prevent unauthorized users from returning a shared workbook to exclusive use and from modifying the number of days that change history is recorded.

To password-protect a shared workbook

1. If your workbook is already shared, stop sharing the workbook.
2. On the **Tools** menu, click **Share Workbook**, and then click the **Editing** tab.
3. Select the **Allow changes by more than one user at the same time** check box.
4. Click the **Advanced** tab.
5. Under **Track changes**, select **Keep change history for**, and then in the **days** box, type the number of days you want to maintain the change history.
6. Click the **Editing** tab, and then clear the **Allow changes by more than one user at the same time** check box.
7. Click **OK**.
8. On the **Tools** menu, point to **Protection**, and then click **Protect Shared Workbook**.
9. Select the **Sharing with track changes** check box.
10. Type the password in the **Password** box, and then when you are prompted, reenter the password.
11. When prompted, save the workbook.

Removing personal or hidden information from a workbook

If your users will share copies of a workbook, it is a good idea to have them review personal and hidden information and decide whether it is appropriate to include. Here are some ways users can help protect their privacy.

Use password protection

If you save a workbook in a file format that can be read by a great number of programs besides Excel — for example, .txt, .htm, and .xml formats — any personal information is easily viewed by anyone who has permission to open the file. By saving a workbook in an Excel file format (.xls), even people who have permission to open the file cannot necessarily find personal information easily. For example, if changes to content are password-protected, only users who know the password can see who has been granted permission to edit certain parts of the workbook.

Remove personal information from file properties

Users can delete the following personal information from the properties for a file: Author, Manager, Company, and Last Saved By. However, some Excel features use this information, so if this information is removed, these features will not work correctly. Removing personal information affects the following features:

- Send to Mail Recipient (for Review)
- Tracked changes
- Comments (names are removed)
- Metadata-based search engines, such as FindFast, and Microsoft SharePoint Portal Server search engines (documents can be indexed by limited data only, such as content and title)

Check for other hidden information

If a user entered personal information, such as his or her name or e-mail address, when the user registered the software, some Office 2004 documents store that information as part of the workbook. Information that is contained in custom fields that users add to the document, such as an "author" or "owner" field, is not automatically removed. Users must edit or remove the custom field to remove that information.

Entourage security

Entourage 2004 provides many security features to help keep sent and received messages safe. As an administrator, you can recommend and support these features to help ensure that sensitive information is more secure. You will also want to be familiar with the following security features if you are evaluating the overall security at your organization.

- **Secure message contents** Users can encrypt e-mail to protect the contents of the messages they send.
- **Verified senders** Users can use digital ID signatures to verify to the recipient of a message that it is really from the sender.
- **Virus protection** Message attachments are a common way for computer viruses to be spread. Entourage can alert users when an attachment is included in a message and give them the opportunity not to open the attachment.
- **Internet connection security** Internet service providers and internal networks offer different levels of protection based on a variety of protocols, such as Secure Sockets Layer (SSL), SMTP authentication, and password protection. The security features available in Entourage can vary depending on the type of Internet connection that you use for a computer.

Configuring Entourage security features to help prevent viruses

Opening an attachment that contains a virus could cause data loss. To help users avoid potential virus activity before it can damage their computers or spread to other computers, Entourage can alert users that a message includes an attachment.

To configure Entourage to help prevent viruses, on the **Entourage** menu, click **Preferences**. Under **General Preferences**, click **Security**. You might want to evaluate the virus protection and notification options in the following table and recommend a standard configuration to all Entourage users to prevent the spread of viruses on the network.

Option	Description
Warn before opening an attachment	Displays a warning before a user opens any attachment. Attachments are a common way for computer viruses to be spread. Opening an attachment that contains a virus could cause data loss.
Warn before allowing an external application to send mail	Displays a warning before allowing an external program to use Entourage to send mail on its behalf. Some computer viruses not only cause problems on the infected computer, but use the e-mail program on the infected computer to send the virus to others. The message and attached virus will look like it came from the owner of the infected computer.
Warn before allowing an external application to access the address book	Displays a warning before allowing an external program to access the information stored in the Entourage Address Book. Some computer viruses will try to find e-mail addresses stored on the infected computer and use these addresses to spread the virus.

Message security

Entourage provides two ways to protect the privacy of messages:

- **Encryption**, which makes the message unreadable to anyone other than the intended recipient.

  When users send messages that are encrypted, each message must be encrypted by using a certificate (public key) for each recipient. The recipient is able to read encrypted messages because the messages contain information that matches the private key stored on the recipient's computer. Entourage also uses a certificate to encrypt messages that a user saves in the Drafts or Sent Items folders, which allows users to review encrypted messages that they have sent.

- **Digital signatures**, which help the message recipient verify the sender's identity.

  When a digitally signed message is sent, the message signature contains the issuer name and a serial number that uniquely identifies the digital identity used to sign the message. The message also includes the certificate (public key) and the validation chain (chain of trust). The recipient uses this certificate to verify which private key was used to sign the message. The recipient can also store the certificate in a contact list so that he or she will always be able to verify digitally signed messages from the user.

You can choose to deploy either method or both methods for any message. Encryption and digital signing are typically used by corporations or government agencies that have a high security standard.

Obtaining a certificate

A user can obtain other people's certificates by receiving digitally signed messages from others and storing their certificates in the Entourage Address Book or keychain. Office supports smart-card-based keychains beginning with Office 2004 for Mac version 11.2.3.

When a user encrypts a message, Entourage searches the Address Book and keychain for the recipient's certificate. If the certificate is not found, Entourage searches the Global Address List or default directory service. When a user searches the Global Address List for the sender's contact information and adds the contact to the Address Book, the contact's certificate is saved to the Address Book together with the contact information.

Obtaining a digital ID

Before users can digitally sign or encrypt a message, they must obtain a digital ID. Users can store and use more than one digital ID on their computers. These digital IDs a user obtains then become the user's certificates.

To deploy digital signatures, you can either set up the computers on your network to have a digital ID, or you can provide instructions to users on how to configure the digital ID themselves. To acquire an Internet digital ID, users must obtain one from a certification authority (CA). Most companies charge a small fee for their certificate services. Some organizations act as a CA for their employees.

To view a list of certification authorities, see Where to Get Your Digital ID at http://office.microsoft.com/assistance. For information about storing a digital ID in your Mac OS keychain, see Importing your new digital ID into your personal keychain at http://www.entourage.mvps.org.

Default secure message settings

You might want to review the default secure message settings for Entourage and, if appropriate, change these settings for your network clients. To ensure a consistent security infrastructure, you can deploy the same security settings across all network clients.

For information about deploying the same security settings for Entourage to all the users on your network, you can use one of the approaches described in Deploying preferences in the "Planning" section.

To change the default secure message settings

1. On the **Tools** menu, click **Accounts**.
2. Select the mail account you want to change, and then click **Edit**.
3. Click the **Security** tab.
4. Select the options that you want:

Option	Description
Signing certificate	Click **Select**, and then select a certificate to use for digitally signing messages from this account. If no certificates are available, you must obtain one from a certification authority. To view a list of certification authorities, see Where to Get Your Digital ID on the Microsoft Web site at http://www.microsoft.com.
Digitally sign all outgoing messages by default	Select to digitally sign all outgoing messages by using the specified certificate by default. This option can be turned on or off for individual messages.
Include my certificate when sending signed messages	Select to include your signing certificate when you send signed messages. The validation chain (chain of trust) and encryption certificate are also included. The message recipient uses the information in the certificate to validate the authenticity of the message. If you do not include your certificate, the recipient cannot verify your signature unless he or she already has access to it in the Global Address List or a directory service

Option	Description
Send clear text signed messages when sending signed messages	Select to allow recipients using e-mail programs that do not support secure messages (S/MIME) to read the message. If you clear this check box, the certificate information is embedded in the message and only those with e-mail programs that support secure messages are able to read the message.
Encryption Certificate	Click **Select**, and then click the default certificate others will use to send encrypted messages to this account. This certificate is also used to encrypt messages that are saved in the Drafts or Sent Items folders in Entourage, which allows you to review encrypted messages even after you send them. If no certificates are available, you must obtain one from a certifying authority. To view a list of certification authorities, see Where to Get Your Digital ID on the Microsoft Web site at http://www.microsoft.com.
Encrypt contents and attachments for all outgoing messages by default	Select to encrypt all outgoing messages by default. The message is encrypted with each recipient's encryption certificate as well as your encryption certificate. This option can be turned on or off for individual messages.

Receiving a message that has restricted permission

If a user receives a message that was created in Microsoft Office Outlook 2003 for Windows and the message uses Information Rights Management (IRM) to restrict permission, the user cannot open the document in Entourage 2004. To open and view the document, the user must ask the sender of the message to remove IRM restriction permission and send the message again.

IRM is an information protection technology that is a feature of Microsoft Office for Windows. IRM allows users and administrators to do the following:

- Share and send confidential documents in e-mail messages.
- Create read-only documents.
- Set expiration dates for documents.
- Maintain control over who can view or change the documents.

For more information about IRM, see the Microsoft Web site at http://www.microsoft.com and search for "IRM."

Receiving e-mail messages

When a user opens an encrypted message, Entourage automatically decrypts the message. When a user opens a digitally signed message, Entourage uses the attached certificate (public key) to validate the private key used to digitally sign the message and determine that no forgery or false representation has occurred. A summary of the security information Entourage can determine is displayed in the Info Bar at the top of the message.

The following table describes the security information Entourage displays in the Info Bar.

Item	Description
Message has not been tampered with	No information in the message body has been added, changed, or deleted.
You trust the signing digital ID	The Mac OS includes 50 or more trusted certificates that are used as root certificates for building others, and administrators can install additional root certificates. The signing digital ID for the message uses a certificate that can be traced back to a trusted root certificate installed on your Macintosh.
The digital ID has not expired	The Mac OS system clock must be set to the correct date and time for this information to be valid.
The digital ID's e-mail address matches the sender's e-mail address	The e-mail address in the certificate used to sign or encrypt the message matches the mail account from which the message was sent (and for which it was meant to be used). If the addresses do not match, the message may still be considered to be valid.
The digital ID has not been revoked	Entourage was able to check information provided by the certifying authority and determine that the certificate has not been revoked.
Revocation information for this certificate could not be determined	Entourage could not find any information issued by the certifying authority about the revocation status for this digital ID.

Notes

- A message is digitally signed when the sender has applied his or her private key to the message.
- If a delegate sent the message on behalf of another person, the delegate's name appears as the sender.

Adding a sender's certificate to the Address Book

To improve the certificate verification process, you might want to inform users that they can add a sender's certificate to the Address Book.

To add a sender's certificate to the Address Book

1. Open a message that has been digitally signed.
2. In the Info Bar at the top of the message, click **View Details**.
3. On the **General** tab, click **Add to Contacts**.

The certificate is stored with the contact entry for this sender. The user can now exchange encrypted e-mail messages with this person, and the user can choose whether to encrypt an individual message or all messages.

Tips

- If a user receives a certificate by another method, such as by a message attachment or on a disk, the user can add it to the contact entry by opening the contact in the Address Book, clicking the **Certificates** tab, and then clicking **Import**.
- To view the certificates for a contact, in the Address Book, double-click the person's name, and then click the **Certificates** tab.
- A user can add a sender's certificate to the Address Book from the Global Address List or default directory service. When a user searches the Global Address List for the sender's contact information and adds the contact to the Address Book, the sender's certificate is saved to the Address Book together with the contact information.

Microsoft Cert Manager

Users can use Microsoft Cert Manager to import and export digital IDs and to view all the digital IDs stored on a computer.

To open Microsoft Cert Manager, double-click **Microsoft Cert Manager**, located in the Microsoft Office 2004/Office folder.

Note In Mac OS X version 10.2.8, Microsoft Cert Manager is required for importing certificates into a personal keychain. In Mac OS X v10.3 and Mac OS X v10.4, Microsoft Cert Manager is optional; you can also request a certificate from a CA and import it by using only the Certificate Assistant in Keychain Access. For more information about using Certificate Assistant in Keychain Access, see Mac Help.

Importing or exporting root certificates A root certificate is a self-signed certification authority (CA) that identifies a CA and its public key. It is used to verify other certificates that are issued by the same CA. The root is stored in a secure location on a computer and is used to verify the authenticity of all certificates that derive from it.

Macintosh computers have a default set of standard root certificates that are trusted, but you may have to install additional root certificates to verify certificates that are issued by non-standard CAs, such as corporations or universities.

To install a root certificate on the computer, the certificate must be in base-64 format (for Mac OS 10.2.8 and later versions), and the person installing the root certificate must have administrator account. If the root certificate is not in the correct format, use the Microsoft Cert Manager (located in the Microsoft Office 2004/Office folder) to convert the certificate to the correct format.

You install root certificates in different ways depending on which Mac OS version is running. If the computer is running a version other than the ones listed here, see the OS documentation for information about how to install a root certificate. Always reopen Entourage after you install new root certificates.

To install a root certificate on Mac OS 10.2.8

1. Copy the PEM (base-64) formatted root certificate to the computer's desktop.
2. In **Terminal**, type the following:

```
$ cd ~/Desktop
$ cp /System/Library/Keychains/X509Anchors ~/Library/Keychains
$ certtool i <filename_of_certificate> k=X509Anchors
$ sudo cp ~/Library/Keychains/X509Anchors /System/Library/Keychains/
<Type the root password>
```

To install a root certificate on Mac OS 10.3 or 10.4

1. Open the Applications/Utilities folder on the computer and locate the Keychain Access program. You do not need to open Keychain Access.
2. Drag the root certificate to the Keychain Access program. Root certificates must be installed one at a time.
3. In the **Add Certificates** dialog box, click **X509 Anchors**, and then click **OK**.

To import other certificates or digital IDs

Note This procedure works only for importing certificates that are not root certificates.

1. In the Microsoft Office 2004/Office folder, open Microsoft Cert Manager.
2. Click **Import**.
3. In the **Import Certificate** dialog box, click the certificate or digital ID to import, and then click **Open**.

To export a certificate

1. Do one of the following:
   - To export a contact's certificate, in the Address Book, open the contact, and then click the **Certificates** tab.
   - To export your own certificate, in the Microsoft Office 2004/Office folder, open Microsoft Cert Manager.
2. Select the certificate you want to export, and then click **Export**.
3. In the **Save As** box, type a name for the certificate.
4. On the **Format** pop-up menu, click a format.
5. Do one of the following:
   - If the program you are planning to export this certificate to requires certificates to be in binary format, click **DER**.
   - If the program requires a base-64 encoded format, click **PEM**.
6. In the **Where** box, select a location.
7. To include all of the certificates used to verify the authenticity of the certificate you are exporting, select the **Include all certificates in the certification path** check box.
8. Click **Save**.

Viewing or deleting a certificate

You can view or delete any certificate that you added. You cannot delete Apple Trusted Root Certificate Authorities, because they are part of the Mac OS.

To view or delete a certificate

1. In the Microsoft Office 2004/Office folder, open Microsoft Cert Manager.
2. On the **Look for certificates of type** pop-up menu, click the type of certificate you are looking for.
3. In the list of certificates, click the certificate you want to view or delete, and then click **View** or **Delete**.

Enabling or disabling Secure Sockets Layer (SSL)

If you enable Secure Sockets Layer (SSL) in Entourage for a server associated with an Exchange account, all Entourage communications with the SSL-enabled server are encrypted. Using the SSL protocol to connect to a server helps ensure the security and privacy of messages handled by the server.

As the Exchange account administrator, you will want to provide SSL setup information to users before they set up their mail accounts. However, users can also change their accounts to use SSL after setup.

For the network users who have an SSL connection, you might need to use a different SMTP port for sending messages in addition to a different POP or IMAP port for receiving messages. SSL is not available for Hotmail accounts.

If you plan to deploy SSL for your Entourage users, you must make sure that SSL is enabled on the Exchange Server. Otherwise, users might not be able to send or receive messages. For information about how to enable SSL on an Exchange Server, see the Exchange Server 2003 Technical Documentation Library at http://www.microsoft.com/technet.

To enable the SSL options in Entourage

1. On the **Tools** menu, click **Accounts**.
2. On the **Mail**, **News**, **Directory Service**, or **Exchange** tab, click the account, and then click **Edit**.
3. Do one of the following:
   - For IMAP, POP, and News accounts, on the **Account Settings** tab, click **Click here for advanced receiving options** or **Click here for advanced sending options**, and then select the options that you want.
   - For Exchange accounts, on the **Account Settings** tab, select the **This DAV service requires a secure connection (SSL)** check box. To enable SSL on the public folders server and the LDAP server, on the **Advanced** tab, select the **This DAV service requires a secure connection (SSL)** check box under **Public folders server** and **Directory Settings**.
   - For Directory Service accounts, on the **Account Settings** tab, click **Click here for advanced options**, and then select the **This LDAP server requires a secure connection (SSL)** check box.

     If your organization uses Microsoft Exchange Server, a directory service account is set up automatically when a user creates an Exchange mail account. To enable the SSL option on the Exchange Server directory service, on the **Advanced** tab, under **Directory Settings**, select the **This LDAP server requires a secure connection (SSL)** check box.

Importing a self-signed SSL certificate

Windows Small Business Server 2003 includes Microsoft Exchange Server 2003 for e-mail services. In Windows Small Business Server 2003, Secure Sockets Layer (SSL) is turned on by default in Exchange Server 2003, and the default SSL certificate is a self-signed certificate. This root certificate is used to configure SSL, which helps secure communications between a Web browser and Entourage.

To use Entourage 2004 with the default self-signed certificate, one of two things must happen:

- The Entourage user adds the certificate to his or her X509 Anchors keychain.

  – or –

- The Exchange administrator obtains a certificate from a public certification authority (CA) which has a root certificate in the X509 Anchors included with Mac OS X. In this case, no action by the user is required.

  To obtain a certificate from a CA, use the Web Server Certificate Wizard to create the request. You can then install the request by using the Configure E-mail and Internet Connection Wizard. For more information about obtaining a certificate or using the wizards, see **Help and Support Center** after Setup is complete. To open Help and Support Center, on a computer that is running Windows Small Business Server 2003, click **Start**, click **Help and Support**, and then search for "To change the Web server certificate."

Obtaining a self-signed certificate on Mac OS X v10.4 or a later version

On Macintosh computers that run Mac OS X v10.4 or a later version, users can obtain the self-signed Exchange certificate on their own by performing the following procedure.

To obtain the self-signed certificate (using Mac OS X v10.4 or a later version)

1. On Exchange Server, make sure that Outlook Web Access is turned on.
2. Open Safari, and then in the Address bar, type the address of your Outlook Web Access Web site.
3. When the security warning appears, click **Show Certificate**, and then drag the certificate icon to the desktop or another location on the Macintosh computer. The certificate is saved as a .cer file.
4. Perform the procedure, To import a self-signed certificate into the X509 Anchors keychain.

Obtaining a self-signed certificate on Mac OS versions earlier than version 10.4

For users who run a version of Mac OS X earlier than 10.4, if your Exchange server is using the self-signed certificate, you or the Exchange administrator must take steps to make the server certificate available to users.

To provide users with a server certificate

1. On the server computer, use the Web Server Certificate Wizard to export the Exchange certificate.
2. Distribute or copy the certificate file to the Macintosh computers on the network, or make the certificate file available for users to copy from a network share.

When users have obtained the self-signed Exchange certificate, they must add the certificate to their X509 Anchors keychain. Provide users with these instructions for importing the certificate.

To import a self-signed certificate into the X509 Anchors keychain

1. Double-click the .cer file.
2. In the Applications/Utilities folder, open Keychain Access.
3. In the **Add Certificates** dialog box, click **X509 Anchors** on the pop-up menu, and then click **Add**.
4. If you are prompted to provide a name and password, type the name and password for an administrator account on the Macintosh computer.

For information about adding certificates to a keychain, see Mac Help.

> **Note** In Mac OS X v10.2, Microsoft Cert Manager is required for importing certificates into a keychain. To open Microsoft Cert Manager, open the Microsoft Office 2004/Office folder, and then double-click **Microsoft Cert Manager**.

Enabling or disabling password protection

Password encryption (POP and IMAP mail accounts only) helps ensure that no one can intercept and use a password to send and receive messages from a user's account. Before you deploy password encryption for your Entourage users who have POP or IMAP accounts, you must know whether the POP or IMAP server accepts password encryption. If it does not, and users configure accounts for password encryption, they might not be able to receive messages.

To enable or disable password protection

1. On the **Tools** menu, click **Accounts**.
2. On the **Mail** tab, click the **IMAP** or **POP** account, and then click **Edit**.
3. On the **Account Settings** tab, click **Click here for advanced receiving options**, and then select or clear the **Always use secure password** check box.

Enabling or disabling SMTP authentication

If your POP or IMAP mail server requires SMTP authentication when users send messages, you can provide special logon information to users for that purpose. Users can choose whether to use the same account ID and password that they use for receiving messages or to specify different ones.

To enable or disable SMTP authentication

1. On the **Tools** menu, click **Accounts**.
2. On the **Mail** tab, click the **IMAP** or **POP** account, and then click **Edit**.
3. On the **Account Settings** tab, click **Click here for advanced sending options**, and then select or clear the **SMTP server requires authentication** check box.
4. If you want to specify different account ID and password information, click **Log on using** and enter your information.

Authentication and security using WebDAV

Entourage uses the World Wide Web Distributed Authoring and Versioning (WebDAV) protocol to communicate with the Exchange server and to manage mail, Calendar, and contacts. WebDAV extensions to HTTP are used for synchronizing mail, public folders, contacts, and events. User accounts are authenticated with the Exchange Server before Entourage 2004 synchronizes the data. Entourage supports Forms Based Authentication, Basic Authentication, or NTLM for WebDAV transactions. Enabling forms-based authentication and SSL on a front-end server allows an organization to more securely provide programs such as Outlook Web Access and Entourage 2004 access to Exchange resources from the Internet.

Regardless of the authentication technique being used with WebDAV, the data is transmitted over the wire in plain text in an XML stream. Third parties could discover this data by using network monitoring or packet sniffing tools. If your users exchange critical or sensitive information with the Exchange server, we recommend that you use Secure Sockets Layer (SSL) to encrypt the data.

For a general discussion of WebDAV authentication and security, see Authentication and Security Using WebDAV in the Microsoft MSDN library at http://msdn.microsoft.com/library.

Working with Internet Security and Acceleration (ISA) Server

ISA Server provides enhanced security and performance by authenticating incoming and outgoing Web requests at the perimeter of your organization's network instead of internally on an Active Directory/global catalog server. ISA Server can use several different authentication methods: Basic, Digest, Integrated Windows (Kerberos and NTLM/NTCR) authentication, Forms-Based Authentication, and certificates.

> **Note** Entourage 2004 does not currently support Forms-Based Authentication (FBA) when it is used with ISA Server. However, you can configure ISA Server to enable your Outlook Web Access server to perform this authentication. Entourage and Outlook Web Access sessions will then work with FBA but will not have the benefits of ISA. For more information about how to support FBA in an ISA environment, see Knowledge Base article 909268 on the Microsoft Web site at http://support.microsoft.com.

For information about ISA Server, see Microsoft Internet Security and Acceleration Server on the Microsoft Web site at http://www.microsoft.com/isaserver.

For information about third-party support for additional authentication methods for ISA Server, see User Authentication in the Partners section of the ISA Server area at http://www.microsoft.com/isaserver.

Smart card support

Mac OS X has built-in smart card support for use with the U.S. Federal Government's Smart Cards that complies with U.S. Department of Defense standards. These standards follow one of the approved specifications:

- CAC (Common Access Card)
- GSCIS (Government Smart Card Interoperability Specification
- PIV (Personal ID Verification)

Entourage now supports the use of digital IDs stored on some smart-card-based keychains to perform secure messaging operations. These operations include digitally signing, verifying, encrypting, and decrypting e-mail messages.

For more information about Apple's support for smart cards, see Smart Card Services on the Apple Developer Connection at http://developer.apple.com.

> **Note** Intel-based Macintosh computers that run Mac OS 10.4.5 do not support the use of digital IDs stored on smart card-based keychains. It is likely that a future Mac OS X v10.4 update will make Entourage support of smart cards possible on Intel-based Macintosh computers.

Messenger for Mac security

Messenger offers two types of communication services — personal accounts and corporate accounts. If your users have personal accounts with the Messenger service, there are no security features in Messenger for you to control. However, there are port and proxy settings that must remain open for Messenger to operate. A network attack that disables these settings is a possible threat.

If your users have corporate accounts, your organization uses Microsoft Live Communications Server 2005 or a later version, which lets you chat in real time with other people in your organization without leaving the organization's firewall. Security features of Live Communications Server include end-to-end encryption through the Transport Layer Security (TLS) protocol and full authentication through Active Directory. As the administrator for your organization, you control these security features. For information about planning and deploying Messenger in an organization that runs Live Communications Server, download the Microsoft Messenger for Mac Deployment Guide from the Resource Kits page of the Microsoft Web site at http://www.microsoft.com/mac.

Virtual PC for Mac security

Microsoft Virtual PC for Mac uses the security features of both Mac OS X and Microsoft Windows. To learn more about the security features of Mac OS X, see Mac Help.

Windows running on a virtual machine is less susceptible to viruses than Windows running on a Windows-based computer. It is unlikely that a virus will affect the Mac OS or Mac files; however, in certain circumstances, your virtual machine running Windows exposes you to the same security risks faced by users running Windows on a Windows-based computer. To reduce your risk, make sure that you always install the latest Windows security updates and service releases.

Windows Services for Macintosh

Services for Macintosh is a component of Microsoft Windows 2000 Server and Windows Server 2003. With Services for Macintosh, multiple platforms can communicate over a network by sharing file and printer resources. After Services for Macintosh is set up, the computer on which it is running can function as a file server, a remote access server, and a print server for Macintosh computers.

With Services for Macintosh, Macintosh computers require only the Mac operating system software to function as clients to the Services for Macintosh server.

Additionally, you can set up the optional Microsoft User Authentication Module (UAM). The Microsoft UAM is a method for encrypting the passwords that you use to log on to Windows AFP Servers. The standard Apple UAM provides only minimal encryption, so your password could easily be intercepted on the LAN or Internet. Although the UAM is not required, it does support network passwords longer than 8 characters and provides for encrypted authentication to servers that are running Windows 2000 Server or Windows Server 2003 and that have Services for Macintosh. The most recent version includes support for NTLMv2 128-bit encrypted authentication and a Mac OS X v10.1 compatible release.

For more information about Services for Macintosh and Microsoft UAM, see Using the Microsoft User Authentication Module (UAM) in the “Configuration” section, or see Windows 2000 SFM on the Microsoft Web site at http://www.microsoft.com/mac.

Mac OS X Security

Mac OS X uses open-source, standards-based security technologies that are easy to administer. Administrators who experience any security problem that they suspect is related to the use of Mac OS on their network can contact Apple at the Apple Product Security Web site at http://www.info.apple.com/usen/security.

By default, Mac OS X closes all communication ports and services, such as file sharing, Web sharing, remote logon, FTP access, remote Apple events, and printer sharing. Also by default, the root account is disabled. However, authorized users can turn on these services, because the root account has full access to the system.

If you want to determine the overall security of your network clients, the various security technologies supported in Mac OS X may be of interest to you. For a list of these standards, search for “Security technologies” in Mac Help.

Configuration

Configuring Microsoft Word 2004 110
Storing components 111
Using add-ins 112
Setting default storage locations 112
Setting default spelling and grammar options 112
Configuring Word on a computer that has multiple users 112
Configuring Microsoft Excel 2004 113
Setting the default storage location 113
Using add-ins 114
Importing information into Excel 115
Using Web queries in Excel 2004 116
Excel specifications and limits 117
Configuring Microsoft PowerPoint 2004 120
Setting the default storage location 120
Configuring Microsoft Entourage 2004 120
Setting Entourage preference options 120
Synchronizing with handheld devices 121
Using Sync Services 122
Using delegation 122
Using public folders 124
Using sharing 124
Creating an Address Book, Calendar, or Mail folder in an Exchange account 125
Setting up out-of-office messages 125
Using complex HTML 126
Addressing e-mail messages by using the Global Address List 127
Using Project Center 128
Accessing Calendar events on an Exchange server 130
Accessing an Exchange account by using Outlook Web Access 130
Changing the LDAP port for Entourage 131
Setting administrative preferences for LDAP 131

Configuration continued

Configuring Microsoft Virtual PC 7 for Mac 132
Configuring Microsoft Messenger for Mac 132
Cross-platform compatibility 132
    Checking for compatibility 132
    Working with Office for Windows documents 133
    Working with Visual Basic 135
    Using the Microsoft User Authentication Module (UAM) 135
    Sharing printers between Macintosh and Windows clients 136
Long file names 137
Using AppleScript 137
Customizing Office 2004 international language settings 137
    Office 2004 shared international features 137
    International features of Entourage 2004 139
    International features of Word 2004 139
    International features of Excel 2004 140
    Configuring Office 2004 for multiple languages 143

As the administrator, you can configure many characteristics and settings of Microsoft Office 2004 programs. Before or after you deploy Office 2004 to users, you can modify Office 2004 program preferences and settings to increase the standardization of the Office 2004 experience across your user community. This section of the *Resource Kit* also covers the system and network dependencies of some Office 2004 features, such as Project Center.

The first time a user opens an Office 2004 program, Office determines whether the corresponding .plist files for the program are present in the *username*/Library/Preferences/Microsoft folder. If the Microsoft folder and required preference files are not found, the program creates them. If the Microsoft folder and the appropriate settings files are found, the program uses the preference settings stored in the settings files. For this reason, you can establish a standard set of preferences by setting preferences within each program and then deploying the Microsoft folder and the settings files it contains.

> **Important** If you deploy a preference file to Office 2004 users as part of a .pkg file or by using Apple Remote Desktop, the file overwrites all settings in any previous copy of the file in the same location. To manage individual preferences in a .plist file without disrupting other settings in the same file, use Apple Workgroup Manager.

For more information about Apple Workgroup Manager and customizing and deploying preferences for Office 2004 programs, see Configuring Office 2004 preferences and Deploying preferences in the "Deployment" section.

Configuring Microsoft Word 2004

If you deploy Word 2004 centrally across your organization, you can set the Word 2004 default preferences to make sure that users have the settings they need to perform their work. For example, if your organization uses a set of common templates, you can store them in a shared network folder and then, before deployment, specify that location in Word Preferences.

The following paragraphs provide examples of preferences that you can set for Word. These preference settings are saved in the com.microsoft.Word.prefs.plist and Microsoft Office Settings (11) files in the user's Library/Preferences/Microsoft folder. Word 2004 also adds preferences to Office preference files the first time a user opens Word 2004.

Storing components

The various components of a Word document — such as styles, macros, default page settings, AutoText entries, AutoCorrect entries, and custom command settings — are stored either in the document itself or in an attached template. Some components reside strictly in the document, others reside in a template, and still others can be stored in either the document or a template.

Of those components that reside in a template, some are always stored with the Normal template or the attached template, and others can be stored in a global template. Users can use Organizer to specify where AutoText entries, styles, custom toolbars, menus, keyboard shortcuts, and macros are stored.

To open Organizer, on the **Tools** menu, click **Templates and Add-Ins**, and then click **Organizer.**

The following table shows where components can be stored.

Component	Document	Normal or other template	Global templates
AutoText entries	No	Yes	Yes
Styles	Yes	Yes	No
Custom toolbars, menus, and keyboard shortcuts	Yes	Yes	Yes
Macros	Yes	Yes	Yes
Boilerplate text and graphics	Yes	Yes	No
Default page settings	Yes	Yes	No
Document text and graphics	Yes	No	No

Using add-ins

Add-ins are supplemental programs that you install to extend the capabilities of Word by adding custom commands and specialized features. You can obtain add-ins from independent software vendors, or you can write your own custom add-in programs.

An add-in must be loaded into Word just like a global template. Like a template, the add-in remains available as long as Word is running. To load the add-in automatically every time that Word is opened, you must store the add-in in the Startup folder. To view or change the location of the current Startup folder, on the **Word** menu, click **Preferences**, and then click **File Locations**. By default, this location is the Microsoft Office 2004/Office/Startup/Word folder. For more information about loading and unloading add-ins, see Word Help.

Setting default storage locations

Before you deploy Office 2004, you can set the default storage locations and search paths for documents, templates, and other items that users create or use in Word 2004. To set the default storage locations for Word, on the **Word** menu, click **Preferences**, and then click **File Locations**. If a storage location is not set, the default folder that appears in the **Open and Save As** dialog boxes is a user's Documents folder.

Setting default spelling and grammar options

Before you deploy Office 2004, you can set the default options for the spelling and grammar checkers. On the **Word** menu, click **Preferences**, and then click **Spelling and Grammar**. The default location of custom dictionaries is Library/Preferences/Microsoft in a user's folder. If you want to use a custom dictionary that is stored in any other location, you must add it to the list of dictionaries in the **Custom Dictionaries** box.

Configuring Word on a computer that has multiple users

When you install Office 2004 on a computer that does not already have an earlier version of Office installed on it, a Normal template is created the first time a user opens Word. The Normal template is created in the first user's Documents/Microsoft User Data folder. When you configure a computer that is running Word for multiple users, you must decide whether users should each have separate Normal templates or should share the same Normal template:

- If you want users to share the same Normal template, make sure that all users have read/write permissions to the first user's Documents/Microsoft User Data folder. Each user can then access and change the Normal template in the first user's Documents/Microsoft User Data folder.

- If you want each user to own a Normal template, make sure that non-administrative users do not have write permissions to the first user's Documents/Microsoft User Data folder.

  To change user permissions, in the Finder, open the user's Documents folder, select the Microsoft User Data folder, and then on the **File** menu, click **Get Info**. On the pop-up menu, click **Ownership & Permissions**, and then change the permissions of the Microsoft User Data folder to **You can = Read Only**.

  After you change the user permissions, the location in which Word creates the Normal template depends on whether automatic logon is turned on for a user's account on the Macintosh computer. By default, Mac OS X is not set to log on automatically when you create a user account.

- If automatic logon is disabled, Word automatically saves a separate Normal template in the user's Documents/Microsoft User Data folder for each user account that uses Word.
- If automatic logon is enabled, users who do not have administrative access are prompted to select a new save location for any changes they make to the Normal template. Word then opens the new Normal template automatically the next time that user logs in and opens Word.

If more than one user who has administrative access uses the computer, those users must maintain separate Normal templates. The users must manually change their **User Templates** paths under **File Locations** in **Preferences** to another location, and then copy the Normal template to that location. Otherwise, all administrative accounts, with or without automatic logon, share the Normal template in the first user's Documents/Microsoft User Data folder.

Configuring Microsoft Excel 2004

If you deploy Excel 2004 centrally across your organization, you can set preferences in Excel 2004 so that each user receives the same set of options and settings. For example, if your organization uses shared workbooks, you can specify the default file location in which the workbooks are saved.

> **Note** If the shared workbook preference is set to use a network file server, and the user opens Excel before connecting to that server, Excel does not prompt the user to connect to the file server. Also, if the user tries to view the default file location setting in Excel Preferences when the user is not connected to the network file server, no preference appears.

The preferences that you can set for Excel are saved in the com.microsoft.Excel.prefs.plist and Microsoft Office Settings (11) files in the user's Library/Preferences/Microsoft folder.

Setting the default storage location

Before you deploy Office 2004, you can set the default location and search path for opening and saving Excel documents. You can also specify the folder from which Excel automatically opens files at startup. To set the default file locations for Excel, on the **Excel** menu, click **Preferences**, and then click **General**. If a default file location is not set, the default folder that appears in the **Open** and **Save As** dialog boxes is a user's Documents folder.

Using add-ins

Add-ins are programs that add optional commands and features to Excel. For example, the Analysis ToolPak add-in provides a set of data analysis tools that can help users save steps when they develop complex statistical or engineering analyses.

Some add-ins are installed and loaded automatically; other add-ins are installed but must be loaded into Excel manually. By default, the standard Excel add-ins are installed and loaded in the Microsoft Office 2004/Office/Add-ins folder. Before you deploy a custom installation image, you can install custom add-ins in the Add-ins folder. You can also designate other shared locations on your network for add-in programs. Users can then load the custom add-ins that you and other users install in the shared folder.

To install an add-in manually, on the **Tools** menu, click **Add-Ins**, and then click **Select**. After an add-in is installed, it appears on the **Add-Ins available** list in the **Add-Ins** dialog box.

Next, the add-in must be loaded into Excel. Loading an add-in makes the feature available in Excel and adds any associated commands to the appropriate menus. To load an add-in, select the check box next to the add-in on the **Add-Ins available** list. Users can also load an add-in for the current Excel session only. To load an add-in for the current Excel session only, on the **File** menu, click **Open**, and then on the **Enable** pop-up menu, select **Add-Ins**.

Some add-ins are not loaded in the **Add-ins** dialog box, but are added as regular menu items, such as Conditional Sum Wizard, Lookup Wizard, Report Manager, and Solver.

To conserve memory and improve performance, unload add-ins that your users rarely use. Unloading an add-in removes its features and commands from Excel but does not remove the add-in file from its original location or from the **Add-Ins available** list. To unload an add-in, clear the check box next to the add-in on the **Add-Ins available** list. When you unload an add-in, it remains in memory until you reopen Excel.

You can create add-ins to assemble and distribute custom features that, from the user's point of view, appear as if they are built into Excel. To create an add-in from a workbook, on the **File** menu, click **Save As**, and then on the **Format** pop-up menu, click **Excel Add-In**.

Users can also save workbooks as add-ins. After a workbook is saved as an add-in, the add-in is protected from changes and cannot be edited. Excel 2004 recognizes files that have the file type XLA8 or the file name extension .xla as add-ins compiled from Excel workbooks. Add-ins can also be written in the C programming language. When add-ins are compiled from C, they should have the file type XLL8 or the file name extension .xll.

The following add-ins are included on the Office 2004 CD and are already installed in Excel 2004:

Add-in	Files	Description
Analysis ToolPak	Analysis ToolPak FuncRes ProcDBRes	Adds financial, statistical, and engineering analysis tools and functions.
Analysis ToolPak VBA	Analysis ToolPak - VBA	Includes VBA functions for Analysis ToolPak.
Conditional Sum Wizard	Conditional Sum Wizard	Creates a formula that sums data in a list if the data matches criteria users specify. This add-in must be loaded manually.
Euro Currency Tool	Eurotool.xla EuroConvert Library	Converts Euro currency between ISO member bodies.
Internet Assistant VBA	HTML.xla	Runs macros that use the legacy HTMLConvert function.
Lookup Wizard	Lookup Wizard	Creates a formula to look up data in a list by using another known value in the list. This add-in must be loaded manually.
Report Manager	Report Manager	Creates reports that contain different print areas in a workbook, custom views of a workbook, and scenarios. This add-in must be loaded manually.
Set Language	Set Language	Sets the current proofing language.
Solver	Solver.xla Solver Library	Calculates solutions to what-if scenarios based on adjustable cells and constraint cells. This add-in must be loaded manually.

Notes

- The Microsoft Office 2004/Office Add-Ins folder contains other files in addition to the files for add-ins listed in the previous table. Users do not have to load these additional files manually because they are loaded when Excel is installed.
- If the source workbook for an add-in contains a reference to another add-in, make sure that when the add-in is distributed, the referenced add-in is stored on the user's computer where the calling add-in can find it. The best strategy is always to store a referenced add-in in the folder that contains the calling add-in. When a source workbook is compiled as an add-in, Excel stores the path of the referenced add-in in the calling add-in.

Importing information into Excel

Excel 2004 for Mac offers several features that enable you to manage data and connect to various data sources. The following paragraphs describe some of the features that you and your users can use to maintain and share data in Excel.

Importing data from a FileMaker Pro database

Excel 2004 provides a FileMaker Import Wizard that you can use to import or convert FileMaker Pro databases to Excel. The FileMaker Import Wizard is available only to users who have FileMaker Pro installed.

When users access a FileMaker Pro database in Excel by clicking **Open** on the **File** menu, the FileMaker Import Wizard opens. With the wizard, users can convert their data so that they can maintain it in Excel. For information about limitations on importing data from a FileMaker database into an Excel workbook, see Excel Help.

Users can also use the FileMaker Import Wizard to set up a query to a FileMaker Pro database. By using a query, users can bring data from the database into Excel and do not need to convert the database. On the **Data** menu, point to **Get External Data**, and then click **Import from FileMaker Pro**. Users can maintain the data in FileMaker Pro and update it in the Excel workbook by clicking **Refresh Data** on the **Data** menu.

Importing data by using Open Database Connectivity (ODBC)

Excel 2004 can retrieve information from SQL Server and other databases by using a variety of third-party ODBC drivers. For the latest information about ODBC support, see Import data into Excel 2004 by using ODBC on the Excel 2004 Articles and Tricks page of the Microsoft Web site at http://www.microsoft.com/mac. For more information about working with database queries, open Microsoft Query (located in the Microsoft Office 2004/Office folder), and then on the **Help** menu, click **Microsoft Query Help**.

Importing and refreshing data from a text file

Users can bring data from text files into Excel just like they can create other database queries. Formatting and formulas are retained when the user opens the file as refreshable. To open the Text Import Wizard, on the **Data** menu, point to **Get External Data**, and then click **Import Text File**. After the user opens the Text Import Wizard, the user can create an External Data Range. This query resembles a regular database query and can be used to retrieve and update data from the original text file. For more information about updating external data, see Excel Help.

Using Web queries in Excel 2004

A Web query retrieves data stored on the Internet or an intranet. For example, users can create a Web query that retrieves a current product price from a database on their intranet. Excel 2004 includes sample Web queries that users can modify by changing the text in any text editor. You can find these samples in Microsoft Office 2004/Office/Queries. To retrieve external data from a Web source, users must have access to the Internet or an intranet, depending on the location of the data source. To run a Web query, on the **Data** menu, point to **Get External Data**, click **Run Saved Query**, locate the query to run, and then click **Get Data**.

Excel specifications and limits

The following table shows the workbook and worksheet specifications of Excel 2004.

Feature	Maximum limit
Open workbooks	Limited by available memory and system resources
Worksheet size	65,536 rows by 256 columns
Column width	255 characters
Row height	409 points
Length of cell contents (text)	32,767 characters (only 1,024 can be displayed in a cell; all 32,767 can be displayed in the formula bar)
Sheets in a workbook	Limited by available memory
Colors in a workbook	56
Cell styles in a workbook	4,000
Named views in a workbook	Limited by available memory
Custom number formats	Limited by available memory
Names in a workbook	Limited by available memory
Windows in a workbook	Limited only by system resources
Panes in a window	4
Linked sheets	Limited by available memory
Scenarios	Limited by available memory; a summary report shows only the first 251 scenarios
Changing cells in a scenario	32
Adjustable cells in Solver	200
Custom functions	Limited by available memory
Zoom range	10 percent to 400 percent
Reports	Limited by available memory
Sort references	3 in a single sort; unlimited when users use sequential sorts
Undo levels	16
Fields in a data form	32
Custom toolbars in a workbook	Limited by available memory
Custom toolbar buttons	Limited by available memory

The following table shows the calculation specifications of Excel 2004.

Feature	Maximum limit
Number precision	15 digits
Largest possible positive number	9.99999999999999E307
Largest possible negative number	-1E-307
Smallest possible positive number	1E-307
Smallest possible negative number	-9.99999999999999E307
Iterations	32,767
Worksheet arrays	Limited by available memory
Selected ranges	2,048
Arguments in a function	30
Nested levels of functions	7
Number of available worksheet functions	329
Earliest date possible for calculation	January 1, 1900 (January 1, 1904, if 1904 date system is used)
Latest date possible for calculation	December 31, 9999
Largest period of time that can be entered	9999:99:99

The following table shows the PivotTable report specifications of Excel 2004.

Feature	Maximum limit
PivotTable reports on a sheet	Limited by available memory
Items in a PivotTable report	8,000
Row or column fields in a PivotTable report	Limited by available memory
Page fields in a PivotTable report	256 (may be limited by available memory)
Data fields in a PivotTable report	256
Calculated item formulas in a PivotTable report	Limited by available memory
Pages in a PivotTable report	8,000

The following table shows the charting specifications of Excel 2004.

Feature	Maximum limit
Charts in a workbook	255
Charts linked to a worksheet	Limited by available memory
Worksheets referred to by a chart	255
Data series in one chart	255
Data points in a data series for 2-D charts	32,000
Data points in a data series for 3-D charts	4,000
Data points for all data series in one chart	256,000
Maximum number of fonts in a chart	255
Line styles	8
Area patterns (screen display)	18
Total area pattern and color combinations (color display)	56,448
Pattern and color combinations (color printer)	56,448 (the actual number depends on your printer and its software)

The following table shows the workgroup specifications of Excel 2004.

Feature	Maximum limit
Users who can open and share a shared workbook at the same time	256
Personal views in a shared workbook	Limited by available memory
Days that change history is maintained	32,767 (default is 30 days)
Workbooks that can be merged at the same time	Limited by available memory
Cells that can be highlighted in a shared workbook	32,767
Colors used to identify changes that are made by different users when change highlighting is turned on	32 (each user is identified by a separate color; changes that are made by the current user are highlighted with blue)

Configuring Microsoft PowerPoint 2004

If you deploy PowerPoint 2004 centrally across your organization, you can make sure that the users in your organization have the settings and files they must have to perform their work. For example, you can give users a custom template so that their PowerPoint presentations include design elements specific to your organization. If your organization uses shared presentations, you can specify the default file location in which the presentations are saved.

The first time each user opens PowerPoint 2004, several preference files are created to store default settings, such as the file format and save location. These preference settings are saved in the com.microsoft.PowerPoint.prefs.plist and Microsoft Office Settings (11) files in the user's Library/Preferences/Microsoft folder.

Setting the default storage location

Before you deploy Office 2004, you can set the default location and search path for opening and saving PowerPoint documents. You can also specify the default location for narration files. To set the default file location for PowerPoint, on the **PowerPoint** menu, click **Preferences**, and then click **Advanced**. If a default file location is not set, the default folder that appears in the **Open** and **Save As** dialog boxes is a user's Documents folder.

You might also want to set preferences for checking spelling in PowerPoint presentations before you deploy Office 2004. On the **PowerPoint** menu, click **Preferences**, and then click **Spelling**. When you create a new custom dictionary in Word, it is also available in PowerPoint.

Configuring Microsoft Entourage 2004

The following topics describe how to configure and use some important features in Entourage.

Setting Entourage preference options

To standardize how Entourage 2004 is used across your organization, you can set several preferences for Entourage before you deploy Office 2004. To open the Preferences dialog box, on the **Entourage** menu, click **Preferences.**

Setting default spelling options

You can set preferences for checking spelling in e-mail messages before you deploy Office 2004. On the **Entourage** menu, click **Preferences**, and then click **Spelling**. The default location of custom dictionaries is Library/Preferences/Microsoft in a user's folder. If you want to use a custom dictionary that is stored in any other location, you must add it to the list of dictionaries in the **Custom Dictionaries** box.

Setting Calendar options

Calendar preferences include settings for the first day of the week, the work week Calendar, work hours, and the time zone for new events. To set preferences for the Calendar, on the **Entourage** menu, click **Preferences**, and then click **Calendar**.

Setting junk e-mail options

To set the preference for the level of protection for junk e-mail, on the **Tools** menu, click **Junk E-mail Protection**.

Setting security options

Before you deploy Office 2004, you can apply uniform security settings for all your Entourage users. For example, you can set an option that warns users before they open an attachment, and an option that prevents users from downloading pictures in e-mail from senders who are not listed in either a user's Address Book or Mailing List Manager. To set security preferences for Entourage, on the **Entourage** menu, click **Preferences**, and then click **Security**.

Setting Spotlight options

You can set a preference to include Entourage items in Spotlight search results. On the **Entourage** menu, click **Preferences**, click **Spotlight**, and then select the **Include Entourage items in Spotlight search results** check box. To search in Spotlight, users must have Mac OS X version 10.4 or a later version.

Synchronizing with handheld devices

If users have handheld devices, they can synchronize, or share, items between Entourage and their handheld devices. When synchronizing items, Entourage copies contacts, tasks, notes, and Calendar events to and from the handheld device. After the user enters information, the user can view or change the information by using either the computer or the handheld device.

If users are using Palm Desktop to store information, they can import this information into Entourage by synchronizing the handheld device with Palm Desktop so that it has the latest information.

Palm Desktop 4.0 is required for Handheld Synchronization to work correctly. If the handheld does not support Palm Desktop 4.0, Handheld Synchronization with Entourage will not work. For more information, contact the handheld device manufacturer.

To synchronize a Palm Desktop 4.0 handheld device

1. Install the Handheld Sync Installer (Entourage Conduit). To do this, open the Microsoft Office 2004/Additional Tools folder. Double-click **Handheld Sync Installer**, and then follow the directions on your screen.
2. In HotSync Manager, make sure that the Entourage Conduit is set up to synchronize. For more information, see HotSync Manager Help and the Microsoft Handheld Synchronization for Mac Read Me in the Microsoft Office 2004/Additional Tools/Handheld Synchronization folder.
3. Synchronize the handheld device with Entourage by using HotSync Manager.

Using Sync Services

Entourage now supports Sync Services, which enables Entourage users to synchronize with devices supported by the Apple iSync program. Users must be running Mac OS X v10.4.3 or a later version to use Sync Services. Sync Services enables users to synchronize Entourage Calendar events, contacts, and tasks with other programs that are running Mac OS X, such as Address Book and iCal. Sync Services also synchronizes Entourage data with the Mac OS so that users can share information across computers by using a .Mac account. To do this, users must select their sync options for .Mac in Mac OS X System Preferences.

> **Important** Make sure that users who synchronize Entourage with iCal know that their actions in one program are synchronized with the other. For example, if an iCal calendar named "Entourage" is deleted, these events are then deleted in the synchronized Entourage Calendar. Entourage Calendar events synchronize with iCal only when a user has an iCal calendar named "Entourage." For more information about synchronizing events with iCal and .Mac, see the Microsoft Entourage 2004 for Mac Read Me.

Using delegation

Before a user can access and manage another user's Exchange information by using Entourage 2004, the user must be given delegate access from the owner of the account. Delegate access can be set up and managed by using Entourage 2004. If a user has delegate access to an account owner's Exchange information, the Entourage user, depending on the permissions granted by the owner, can read and respond to messages, accept or decline invitations, and change or create contact items and Calendar events for the owner. The account owner can grant access and various levels of permissions for the following types of items:

Messages	The owner's Inbox and subfolders appear in the user's Folders list in Entourage Mail view. The user can read, respond to, and organize messages just like in the user's own Inbox.
Calendar events and Address Book contacts	Items stored in the owner's Calendar and Address Book appear in the user's Entourage Address Book and Calendar. Any changes the user makes to an item appear in the owner's Address Book or Calendar the next time synchronization occurs. If a delegate creates a new contact or Calendar event in the delegated Calendar or Address Book, it is added to the owner's Address Book or Calendar the next time synchronization occurs.
Invitations	When the user accepts an invitation in the delegated Calendar, that event is added to the owner's Calendar. All Exchange account Calendars and their events are continually synchronized with the Exchange server.

Microsoft Entourage delegate access permissions

The levels of permission that a delegate can be granted are shown in the following table:

Permission level	Description
Reviewer	A delegate can read items. For example, a delegate with Reviewer permission can read messages in another user's Inbox.
Author	A delegate can read and create items, and can modify and delete the items that were created. For example, a delegate can create task requests and meeting requests directly in the owner's Task or Calendar folder, and then send either item on the owner's behalf.
Editor	A delegate can do everything an Author can do, and can modify and delete the items the owner created.

Sent by permissions

A delegate can send e-mail messages on behalf of the user for whom he or she is a delegate. Sent messages contain both the owner's name and the delegate's name. Message recipients see both the owner's name and the delegate's name in the **From** box.

If a user delegates his or her Calendar, the delegate can accept, decline, or tentatively accept meeting requests on the owner’s behalf. The delegate receives copies of meeting-related messages sent to the account owner. After the delegate responds to the meeting on the owner’s behalf, the meeting is automatically added to the account owner’s Calendar if the response to the meeting is Accept or Tentative.

To set up delegate access in Entourage 2004

1. On the **Tools** menu, click **Accounts**.
2. On the **Exchange** tab, click the account that you want to add a delegate to, and then click **Edit**.
3. On the **Delegate** tab, under **My Delegates**, click **Add**.
4. Type the name of the user who will be the delegate, and then click **Find**.
5. Click the name of the user, and then click **OK**.
6. Select or clear the check boxes to customize permissions.
7. To complete the delegation process, ask the delegate to add the owner to his or her **Users I am a delegate for** list.

To become a delegate

1. On the **Tools** menu, click **Accounts**.
2. On the **Exchange** tab, click the account that you will use to access the delegated items, and then click **Edit**.
3. On the **Delegate** tab, under **Users I am a delegate for**, click **Add**.
4. Type the name of the user who has configured you as a delegate, and then click **Find**.
5. Click the name of the user, and then click **OK**.
6. If you have delegate access to the account of someone whose account is not on the same Exchange server as your account, on the **Delegate** tab, under **Users I am a delegate for**, click **Advanced**.

Using public folders

Public folders in Microsoft Exchange Server provide an effective way to collect, organize, and share information with others in an organization. Public folders are synchronized regularly and their contents are preserved when users are not connected to their Exchange accounts. For this reason, public folders are a good choice to use for folders that are accessed frequently by multiple users. Typically, project teams or user groups use public folders to share information about a common area of interest.

When an Entourage user is connected to an Exchange server, folders labeled Public Folders appear in the Entourage Folder List under the Exchange mail account. The public folder server is determined automatically when the Exchange account is created. The user can set or change public folder settings on the **Advanced** tab of the Exchange account.

> **Note** Users can add a public folder to their Favorites folder if they want to synchronize the contents of the folder automatically and view the contents of the folder when they are offline.

Using sharing

Users can share Address Books, Calendars, and Mail folders stored on an Exchange server with others on the same Exchange server. By setting permissions, a user defines which activities are allowed. Users can select from a predefined set of permissions, or they can customize the permissions to handle how they want to share the Address Book, Calendar, or Mail folder.

After permission is set, those with whom the Address Book, Calendar, or Mail folder is shared can open it in Entourage. When someone opens the shared Address Book, Calendar, or Mail folder, it is added to the Mail view and appears as a new account that contains only those Address Books, Calendars, or Mail folders that the user shared. Opened Calendars and Address Books also appear in the Calendar and Address Book views.

To share an Address Book, Calendar, or Mail folder, both the user sharing and the user who is shared with must have an e-mail account on a server in the same organization that is running Exchange Server 2003 or a later version.

To share an Address Book, Calendar, or Mail folder

1. Click the folder that you want to share, and then on the **Edit** menu, click **Folder Properties**.
2. Click **Permissions**, and then click **Add User**.
3. For each user who should have access to the Address Book, Calendar, or Mail folder, type the name of the user, and then click **Find**.

   You can use the advanced search option if you know the domain name, account ID, and account type of the user who should have access.
4. Select the name of the user in the search results, and then click **OK**.
5. For each user, click the user's name in the list, and then do one or both of the following:
   - On the **Permission Level** pop-up menu, click the level you want.
   - Select or clear the check boxes to customize permissions, and then click the **Edit Items** and **Delete Items** levels you want.

Note To view the shared information, the user who is shared with must open the Address Book, Calendar, or Mail folder in Entourage.

Creating an Address Book, Calendar, or Mail folder in an Exchange account

With Entourage 2004, users can create multiple Address Books, Calendars, and Mail folders on the Exchange server.

To create an Address Book, Calendar, or Mail folder

1. Click **Mail**, and then click an Exchange folder.
2. Click the triangle to the right of **New**, and then click **Folder**.
3. Type a name for the new Address Book, Calendar, or Mail folder.
4. On the **Type** pop-up menu, click **Address Book**, **Calendar**, or **Mail Folder**.
5. Click the location in the list where you want the Address Book, Calendar, or Mail Folder to appear.

Setting up out-of-office messages

In Outlook, you can use the Out of Office feature to reply automatically to incoming e-mail messages that you receive when you are unavailable. Entourage 2004 does not support this feature. However, Entourage 2004 users can access their Exchange server account to manage the Out of Office feature by using Outlook Web Access. Outlook Web Access includes an Out of Office Assistant that automatically replies to e-mail messages that a user receives when he or she is away. Every time that a user opens the assistant, Outlook Web Access sends an automatic reply to someone the first time he or she sends the user a message.

Provide your users with the address of your Outlook Web Address Web site and the following instructions for automatically replying to e-mail messages.

To automatically reply to e-mail messages

1. In your Web browser, type the address provided by your Exchange server administrator for the Outlook Web Access Web site.
2. Type your domain, user name, and password, and then click **Log On**.
3. In the navigation pane, click **Options**.
4. To enable the Out of Office Assistant, under **Out of Office Assistant**, click **I'm currently out of the office**.
5. In the text box, type the message that you want people to receive when they send you e-mail messages when you're away.

To disable automatic replies to e-mail messages

1. Repeat steps 1 through 3 of the previous procedure.
2. Under **Out of Office Assistant**, click **I'm currently in the office**.

Note For more information, see Outlook Web Access Features in Exchange 2003 on the Microsoft Web site at http://www.microsoft.com/exchange.

Using complex HTML

In Entourage 2004, users can receive messages that use complex HTML, which adds special formatting, such as tables, navigation menus, or other effects, to a message. Although users can receive complex-HTML messages in Entourage, they cannot create complex-HTML messages. Users can create e-mail messages that include simple HTML text formatting, such as numbering, bullets, alignment, and background color. To compose e-mail messages that include complex HTML, users can create and mail documents by using Word.

To mail a document from Word

1. Open the document you want to mail.
2. On the **File** menu, point to **Send To**, and then click the option that you want.
3. Address and send the mail message to the recipients.

Complex HTML is most frequently used by organizations to send newsletters, Web pages, and announcements as messages. However, it can be used by anyone to run scripts or download files that might harm computers or pose a risk to users' privacy. To help make sure that users have some protection from malicious software, Entourage does not run scripts or download files that are contained in complex-HTML messages. This does not affect users' ability to read complex-HTML messages.

Complex-HTML messages contain special formatting and typically take longer to appear when users open or preview them. Users can disable complex HTML to improve the performance of opening and previewing messages.

To enable or disable complex HTML in incoming messages

1. On the **Entourage** menu, click **Preferences**.
2. Under **General Preferences**, click **Security**.
3. Under **HTML options**, select or clear the **Display complex HTML in messages** check box.

Tip If a user disables complex HTML, all the special formatting that is contained in a complex-HTML message, such as pictures and tables, is removed when the user opens or previews the message.

Addressing e-mail messages by using the Global Address List

The Exchange Global Address List (GAL) contains all user and distribution list e-mail addresses in your organization. Users can access the GAL in Entourage 2004 when addressing their e-mail. Exchange server and directory service users type the alias or name, or part of the name, and then click **Check Names**. Entourage searches the GAL or default directory service for the correct e-mail address. Entourage then displays all the names in the Global Address List that are related to the alias or name specified by the user. This search also occurs automatically when a message is sent.

Users can also search the GAL by using the Address Book list.

Notes

- For browsing functionality in the GAL, the directory service server must be Windows Server 2003.
- The Exchange 2000 Server implementation of LDAP does not support Virtual List View mode.

Tips

- To display additional columns, hold down CONTROL and click the column header
- To quickly find a name in the GAL, type the first name of the person you are searching for. The GAL scrolls to the first entry with that name.
- To search the GAL using more options, select the directory you want to search in the Address Book list, and then click **Find** or COMMAND (⌘) + F. To create a new meeting request, select the person's name from the GAL, and then click **New Invite To**.
- To use AutoComplete, begin typing a name in the **To**, **Cc**, or **Bcc** box of a new e-mail message. AutoComplete displays a pop-up list of names from Contacts and Recent Addresses, the local Address Book, and the default directory service.

To search for an e-mail address

1. Click **Address Book**.
2. In the Address Book list, click the directory that you want to search.
3. On the pop-up menu next to the search box, click the type of search you want.
4. In the search box, begin typing the name of the person or item you want. For example, to find an e-mail address, begin typing the e-mail address.
5. In the list of search results, click an entry to view more information.

Tips

- To send a message to a person you find in a directory service, click the entry in the results list, and then click **New Message To**.
- To add a person you find in a directory service to the Address Book, click the entry in the results list, and then click **Add to Address Book**.

Using Project Center

Microsoft Office 2004 introduces the Project Center, which provides a single, consolidated view of all information related to a project. A project is created by using Entourage 2004, but a user can connect to the Project Center from Word, Excel, or PowerPoint by using the **Project Palette** on the **Tools** menu. For more information about Project Center, see "About the Project Center" in Entourage 2004 Help.

Only two of the features of the Project Center require administrator assistance.

- **Sharing information** The user who creates a project can choose sharing options for the project file and for items in the project. A user can invite other Entourage 2004 users to share project information by using a public folder or a network file server that all users can access. Each subscriber to a project can change project data and control what is shared with others. This differs from sharing or delegation by using an Exchange server. For more information about sharing and delegation by using an Exchange server, see Using sharing and Using delegation.

  Invitations are sent by e-mail and can be accepted only through Entourage 2004. After an invitation is accepted, Entourage prompts the user to log on to the appropriate network file server.

  Note An unshared document is available only on the computer of the person who created the project.

- **Archiving information** With Project Center, users can back up projects and import them again later. Users can save all the information in a project, or they can choose to save only specific types of project information.

Although Entourage automatically prompts users to log on to the necessary file server, you must give users access to the network file server where project information is shared and archived. If users are invited to a project but do not have access to the file server, they will not be able to join the project.

> **Important** Because projects can contain sensitive information, you should require more secure logon access to the network file server that is used to share and archive project information.

Location of project files

Entourage creates two Project Watch Folders for each project – the Entourage Project Watch Folder and the Finder Project Watch Folder. Entourage then keeps track of the items added, changed, or deleted from these folders and automatically associates them with the project. Encourage users to back up their projects periodically to maintain a record of the items associated with a project and their original locations.

The Entourage Project Watch Folder stores e-mail messages. When an e-mail message is moved or copied to the Entourage Project Watch Folder, it is automatically associated with the project. Users can also use rules to flag messages as part of the project without moving or copying the messages. To create rules in Entourage, on the **Tools** menu, click **Rules**.

The Finder Project Watch Folder contains documents and aliases (shortcuts) to documents. These documents and aliases are automatically associated with a project. Any documents that are added to projects in Microsoft Office programs are added to the Finder Project Watch Folder as aliases. They are not moved or copied. The original versions of documents are stored in the Finder Project Watch Folder only if the user manually put the documents there. When a document is manually moved into the Finder Project Watch Folder, it is automatically associated with the project.

Users can further organize project documents by adding subfolders to a Project Watch Folder. The folder hierarchy in the Finder Project Watch Folder is also shown in Entourage in the Project Center on the **Files** tab.

By default, the Finder Project Watch Folder is stored in the Documents/Office Projects/*Project Name* folder. After creating a project, a user can create an alias to the folder on the desktop.

Finder Project Watch Folders can be stored on a network server and shared. If a project is shared and a document in that project is shared, the document is always moved to the shared folder location on the file server. Users can access shared files only when they are connected to the file server. You must recommend and monitor the file servers that are used to store Finder Project Watch Folders. Support professionals who are troubleshooting lost project data will want to verify that the Finder Project Watch Folders on the share have not been deleted or moved. You also should periodically back up the project information that is on the network file server to make sure that no project information is lost.

Accessing Calendar events on an Exchange server

Entourage 2004 can access Calendar items stored on an Exchange server and synchronize the Calendar items with the Entourage Calendar. When an Entourage 2004 user creates a meeting request, the free/busy information for other Exchange users in his or her organization is displayed. For example, users can follow this procedure to invite other Exchange users to an event:

To invite others to an event

1. Create an event.
2. Click **Invite**, and then address the invitation.
3. Click the **Scheduling** tab to determine whether invitees are free or busy. If you do not see the **Scheduling** tab, make sure that your Exchange account is selected in the **From** box at the top of the invitation.
4. To send the invitation that requests responses from attendees, click **Send**.

   To send the invitation without requesting responses from attendees, clear the **Request Responses** check box on the **Event** menu before you click **Send**.

Notes

- Entourage does not detect whether an invitation is out of date or conflicts with other events.
- Entourage does not support invitation counterproposals in Outlook. If an Entourage user sends a meeting request to an Outlook user and the invitee makes a counterproposal, the counterproposal appears as text in the Entourage message body. The Entourage user must make any meeting time adjustments manually.
- To prevent duplicate reminders, avoid running Outlook and Entourage at the same time.

Accessing an Exchange account by using Outlook Web Access

Entourage 2004 uses the World Wide Web Distributed Authoring and Versioning (WebDAV) protocol to communicate with the Exchange server and to manage mail, Calendar, and contacts. WebDAV is also used by Outlook Web Access on Exchange Server. WebDAV allows users to access mail on a server from across the firewall without the need to use a virtual private network (VPN). This access is made possible through the front-end server, which publicly exposes HTTP Exchange access to the Internet.

You will need to provide your users with the address for the Outlook Web Access Web site. To access the Exchange server, users should perform the following procedure.

To access the Exchange server by using Outlook Web Access

1. In the Web browser, type the address of the Outlook Web Access Web site.
2. When prompted, type your user name, password, and domain name.
   You can use the Outlook Web Access site much like you would use Microsoft Outlook.

Notes

- An Outlook Web Access client used with an Active Directory user account has the same Active Directory and networking infrastructure requirements as an Entourage 2004 Exchange client. For more information, see Deployments in an Active Directory infrastructure in the "Planning" section.
- For more information, see Outlook Web Access Features in Exchange Server 2003 on the Microsoft Web site at http://www.microsoft.com/exchange.

Changing the LDAP port for Entourage

If your Exchange deployment uses non-standard LDAP ports, you or your users can change the ports in Entourage. The procedure is the same for both Directory Service accounts and Exchange accounts.

To specify a different LDAP port number on a user computer

1. On the **Tools** menu, click **Accounts**.
2. Select the account you want to change the port for, and then click **Edit**.
3. Click the **Advanced** tab, and then click **Override default LDAP port**.
4. Specify the port you want to use.

Setting administrative preferences for LDAP

In Office 2004 version 11.2.0 or a later version, you can set two administrative preferences for LDAP. You set these preferences by creating new Boolean entries in microsoft.Entourage.plist in the user's Library/Preferences/Microsoft folder. If these preferences are not included in microsoft.Entourage.plist, the settings use "false."

- **LDAP/UseNormalFilterForVLV** Virtual List View (VLV) is a feature in Active Directory that Entourage uses to browse in the Address Book through a large result set in the Global Address List (GAL). By default, Entourage uses a minimal Active Directory filter when a user searches the GAL.

  To use the standard Active Directory filter for searching the GAL, add a Boolean entry to microsoft.Entourage.plist for LDAP/UseNormalFilterForVLV and set its value to "true." Also, in the directory service account options, make sure that the **Use simple search filter** option is not selected. The standard Active Directory filter includes the msExchHideFromAddressLists attribute set, which hides objects in the GAL. The user can then filter the search results in the Address Book to see only users or to see only distribution groups that meet the search criteria.

- **LDAP/AllowSortingOnNonIndexedFieldsInVLV** By default, a user can sort the search results in the Address Book only by an indexed field, which is typically limited to only the Name column. The user can click the label for the Name column to sort the search results alphabetically in ascending or descending order. When you add a Boolean entry to microsoft.Entourage.plist for LDAP/AllowSortingOnNonIndexedFieldsInVLV and set its value to "true," a user can click other column labels to sort the search results.

Note Turning on these LDAP preferences can cause lookups in the GAL to fail if the GAL contains a very large number of objects. If lookups in the GAL fail, turn these preferences off.

Configuring Microsoft Virtual PC 7 for Mac

For information about configuring Virtual PC 7, download the Virtual PC version 7 for Mac Deployment Guide from the Resource Kits page of the Microsoft Web site at http://www.microsoft.com/mac.

Configuring Microsoft Messenger for Mac

For information about configuring Messenger for Mac, download the Messenger for Mac Deployment Guide from the Resource Kits page of the Microsoft Web site at http://www.microsoft.com/mac.

Cross-platform compatibility

Microsoft Office 2004 Compatibility Report identifies and helps users fix items in documents that might not be displayed or print correctly in earlier versions of Office for Mac or in versions of Office for Windows. If your users share their documents with users of other versions of Office, Compatibility Report helps make sure that these documents appear as expected when they are opened. To use Compatibility Report in Word, Excel, and PowerPoint, on the **Tools** menu, click **Compatibility Report**.

Checking for compatibility

When a user opens a document, Compatibility Report automatically checks for compatibility with Office 97 through Office 2004. It also performs automatic checks for compatibility as users are working in a file. If an issue is found, the **Toolbox** button glows. Users can click the **Toolbox** button to open the Compatibility Report window and review the issues. Compatibility Report also alerts users to issues when a document is first saved and when users click **Save As** on the **File** menu.

Users can configure Compatibility Report to scan for issues with specific versions of Office. To do this, on the **Check compatibility with** pop-up menu, click a version of Office.

Sometimes, Compatibility Report cannot scan the entire document for issues. To make sure that all the content in a document is scanned, have users click **Check/Recheck Document**.

Resolving compatibility issues

Users can click an item on the **Results** list to view an explanation of the issue that was found. Additionally, the object or content that is affected by the issue is selected in the document. If more than one item in the document is affected by the same compatibility issue, the issue is listed on the **Results** list for each affected item in the document.

To resolve compatibility issues, select the issue in the **Results** list, and then do one of the following:

To do this	Click this
Fix the selected issue	**Fix**
Fix all instances of the selected issue	The arrow next to **Fix**, and then click **Fix All**
Ignore only this instance of the selected issue	**Ignore**
Ignore all instances of the selected issue	The arrow next to **Ignore**, and then click **Ignore All**
Ignore this issue in all documents	**Never Show Again**

To learn more about compatibility issues, see Help in each Office 2004 program. If no fix is available, Help frequently contains information about how to work around the issue.

Setting Compatibility Report options

Users can turn off automatic checks for compatibility issues. On the **Application** menu in Word, Excel, or PowerPoint, click **Preferences**. Click **Compatibility**, and then clear the **Check documents for compatibility** check box. To reset the list of compatibility issues users chose to ignore, click **Reset Ignored Issues**. To reset the list of ignored issues, including the list of issues users chose never to show again, click **Reset All Issues**.

Working with Office for Windows documents

When Office 2004 users are working with Microsoft Windows users, cross-platform compatibility is critical. The cross-platform capabilities of Office for Mac make creating, opening, formatting, and collectively working on Windows files a straightforward process.

For more information about compatibility between Microsoft Office on Windows-based computers and Macintosh computers, visit the Compatibility Center on the Resources page of the Microsoft Web site at http://www.microsoft.com/mac. The Compatibility Center includes how-to articles that can help users open, edit, and share their work on either operating system.

Opening a Microsoft Office 2003 document that has restricted permission

If you cannot open a document that was created in a Microsoft Office 2003 for Windows-based program, the document may be using Information Rights Management (IRM) to restrict permission. To open the document, ask the author to remove IRM restriction permission from the document and send it to you again.

IRM is an information protection technology that is a feature of Microsoft Office for Windows-based programs. For more information about IRM, see the Microsoft Web site at http://www.microsoft.com and search for "IRM."

Office 2004 document formats

The following tables describe the file formats supported by Office 2004 programs.

Word for Windows documents

Version	Description
Word 97 through Word 2003 for Windows	The default format for Word 2004 for Mac is shared by Word 97 through Word 2003 for Windows. All data and formatting created in these versions of Word for Windows are fully supported in Word 2004 for Mac.
Versions earlier than Word 97	Users can open documents in Word 2004 for Mac that were created in Word for Windows versions earlier than Word 97. All data and formatting created in these versions are fully supported in Word 2004 for Mac.
Versions of Word earlier than Word 2004 and other programs	Users can save a Word document in Rich Text Format (RTF), which can be opened by earlier versions of Word. Some new features in Word are not supported in earlier versions of Word and other programs. If users create documents that use these new features, they might lose data or formatting when they save documents in RTF.

For more information about file formats that you can use to save documents, see Word 2004 Help.

Excel for Windows workbooks

Version	Description
Excel 97 through Excel 2003 for Windows	The default format for Excel 2004 for Mac is shared by Excel 97 through Excel 2003 for Windows. All data and formatting created in these versions of Excel for Windows are fully supported in Excel 2004 for Mac. Workbooks that are saved in this format can be opened without conversion in Excel 2004 for Mac.
Versions earlier than Excel 97	Users can open workbooks in Excel 2004 for Mac that were created in Excel for Windows versions earlier than Excel 97. All data and formatting created in these versions are fully supported in Excel 2004 for Mac.
Dual file format	Users can save a workbook in the Excel 97 through 2004 and 5.0/95 Workbook dual file format. The workbook is saved in a single file that includes the file format shared by Excel 97 through Excel 2003 for Windows, and Excel 98 through 2004 for Mac, and the format shared by Excel 5.0 and Excel 95.

For more information about file formats that you can use to save workbooks, see Excel 2004 Help.

PowerPoint for Windows presentations

Version	Description
PowerPoint Presentation	PowerPoint Presentation is the default format for PowerPoint 2004 for Mac. This format is shared by PowerPoint 97 through PowerPoint 2003 for Windows. All text and formatting created in these versions of PowerPoint for Windows are fully supported in PowerPoint 2004 for Mac.
Outline Rich Text Format (RTF)	Users can also save the text of a presentation by using Outline Rich Text Format (RTF). Many other programs, including compatible Microsoft Windows-based programs, can read and interpret an RTF document. Saving a PowerPoint presentation as an RTF document saves all text in tables, AutoShapes, and other objects that don't appear in the outline pane. It does not save the presentation graphics.

For more information about file formats that you can use to save presentations, see PowerPoint 2004 Help.

Working with Visual Basic

For reference information about the current and previous object models of Word, Excel, and PowerPoint for Microsoft Windows, see the MSDN Developer Centers on the Microsoft Web site at http://www.microsoft.com. Most of this information also applies to the corresponding Office for Mac programs.

> **Note** Some elements of the Office object model for both the Mac and Windows versions of VBA depend on the operating system. If a user has difficulty running VBA code, see Visual Basic Help in Office 2004 for Mac for Mac-specific information.

For information about strategies for developing cross-platform solutions with VBA, see Visual Basic Help in the Office 2004 for Mac programs.

Using the Microsoft User Authentication Module (UAM)

Services for Macintosh is a component of Microsoft Windows 2000 Server and Windows Server 2003 that supports Apple Filing Protocol (AFP). With Services for Macintosh, multiple platforms can communicate over a network by sharing file and printer resources. After Services for Macintosh is set up, the computer on which it is running can function as a file server, a remote access server, and a print server for Macintosh computers.

With Services for Macintosh, Macintosh computers require only the Mac OS to function as workstations; no additional software is required. You can, however, set up the optional Microsoft User Authentication Module (UAM). The Microsoft UAM is a method for encrypting the passwords that you use to log on to Windows AFP Servers. The standard Apple UAM provides only minimal encryption, if any. Therefore, your password could easily be intercepted on the LAN or Internet. Although the UAM is not required, it does provide for network passwords longer than 8 characters and for encrypted authentication to Windows 2000 Servers or Windows Server 2003 servers that are running Services for Macintosh. The most recent version includes support for NTLMv2 128-bit encrypted authentication and a Mac OS X v10.1 compatible release.

The File Server for Macintosh service, which is also referred to as the MacFile service, makes a file server accessible over TCP/IP and AppleTalk networks. With this service, you can also designate a directory as a Mac-accessible volume. A service also makes sure that Mac file names are valid NTFS file system names, and handles permissions. The MacFile service includes AFP over TCP/IP support, which enables Mac clients to access shared resources by using the faster TCP/IP protocol. With this feature, you can remove the AppleTalk protocol from your network, and Mac clients still have access to shared volumes. The MacFile service also includes AFP 2.2 specification support. To take advantage of this support, your Mac program must be using AppleShare Client 3.8 or a later version.

For more information about Services for Macintosh and Microsoft UAM, see Windows 2000 SFM on the Microsoft Web site at http://www.microsoft.com/mac.

Sharing printers between Macintosh and Windows clients

To enable users of client computers that are running Mac operating systems to print, you must have Print Services for Macintosh installed on the Windows print server.

To install Print Services for Macintosh

1. On the Windows Server 2003-based computer, log on as administrator or as a member of the administrator's group.
2. Press and hold down SHIFT as you insert the Windows Server 2003 CD-ROM into the computer's CD drive or DVD drive. This prevents the program from opening automatically.
3. Click **Start**, point to **Control Panel**, and then click **Add or Remove Programs**.
4. Click **Add/Remove Windows Components**.
5. In the **Components** list, click **Other Network File and Print Services**, leave the check box in its current state (do not select or clear the check box), and then click **Details**.
6. On the **Subcomponents of Other Network File and Print Services** list, click **Print Services for Macintosh**.

   This option enables Macintosh users to send print jobs to a print spooler on the server that is running Windows Server 2003. If you have not already installed the AppleTalk protocol, it is installed automatically when you install Print Services for Macintosh.
7. Click **OK**, and then click **Next**.
8. Click **Finish**.

Note The Print Services for Macintosh service is unavailable in Windows Web Server 2003.

Long file names

Office 2004 supports file names that can contain up to 256 characters in the file name and path combined, and can include any character except a colon (:) or a slash mark (/). Excel is an exception; it supports a maximum of 218 characters in file names.

Using AppleScript

You can automate tasks on Macintosh computers by using the AppleScript scripting language. To extend the functionality of Word or automate repetitive tasks, you can create your own AppleScript scripts, programs, or add-ins. Any setting or configuration that you can specify by using Visual Basic, you can specify programmatically by using AppleScript. You can schedule when to run these AppleScript scripts, and you can also use the scripts to integrate control of other programs with Office programs by using cross-program scripting. You can then distribute these scripts to your users, or use a script to automate Office 2004 deployment in your organization. For information about AppleScript, see AppleScript Resources for Office 2004 on the Developer Center page at http://www.microsoft.com/mac. You can find more developer resources for the Macintosh at the Apple Developer Connection at http://developer.apple.com.

Customizing Office 2004 international language settings

Microsoft Office 2004 for Mac programs support editing and viewing documents in many languages. If your users work with documents that contain text in more than one language or if users share documents with people who use Office on systems that run in other languages, you or your users can customize Office 2004 to manage conventions and requirements unique to each language.

Each program in the English version of Office 2004 has features that enable users to create, view, and edit documents in languages other than English.

Office 2004 shared international features

The following topics describe the international features that are available in all Office 2004 programs.

Unicode support

Office 2004 programs support the input, display, and basic editing of Unicode characters associated with the following keyboards:

Australian, Austrian, Belgian, Brazilian, British, Bulgarian, Canadian, Catalan, Cherokee, Chinese (Simplified), Chinese (Traditional), Croatian, Czech, Danish, Dutch, English, Estonian, Faroese, Finnish, French, German, Greek, Korean, Hawaiian, Hungarian, Icelandic, Inuktitut, Irish, Italian, Japanese, Latvian, Lithuanian, Macedonian (FYROM), Norwegian, Northern Sami, Polish, Portuguese, Romanian, Russian, Serbian, Serbian-Latin, Slovak, Slovenian, Spanish, Swedish, Swiss French, Swiss German, Turkish, Ukrainian, Welsh.

Inputs of the previously mentioned languages are also supported through the following system-level Unicode input methods: Unicode Hexadecimal Input, US Extended, and the Character Palette.

> **Note** Installing Office 2004 on a version of the Mac OS for any of the supported languages except Japanese also enables the multiple-language features of Office 2004.

International proofing tools

International proofing tools for each supported language are installed in the Microsoft Office 2004/Shared Applications/Proofing Tools folder. With the proofing tools for European languages, Office 2004 can hyphenate according to the rules of the language and check the spelling of text. The proofing tools also include a thesaurus for each language and a German grammar checker. British, Australian, and U.S. English proofing tools are included in the English version of Office 2004. The Japanese proofing tool component included in the Microsoft Office 2004/Shared Applications/Proofing Tools folder with non-Japanese versions of Office 2004 provides Japanese rules for full grammar and consistency checking.

Multilingual Web pages

Users of Word, Excel, and PowerPoint can specify the default character set encoding when they save documents as Web pages.

To specify the default character set

1. On the **File** menu, click **Save As**.
2. On the **Format** pop-up menu, select **Web Page (HTML)**.
3. Click **Web Options**, and then click the **Encoding** tab.
4. Select an option on the **Save this document as** pop-up menu.

Sorting rules for multiple languages

Office 2004 programs sort data in tables and lists according to the rules of the language currently selected language in Mac OS X on International pane. To select the language from the International pane, on the **Apple** menu, click **System Preferences**, and then under **Personal,** click **International**. This includes Japanese when the program is registered for using Japanese characters. To do this, users must run the Microsoft Language Register.

Correct date, time, and number style

When users enter dates, times, and numbers, Office 2004 programs can format them in the correct style for different languages. Office 2004 supports international date and time formats.

Euro support

All Office 2004 programs offer full support for entering, displaying, and printing euro currency values. Excel 2004 provides support for performing financial calculations involving the euro.

German post-reform spelling rules

Users can set Word, PowerPoint, and Entourage 2004 preferences to use German post-reform spelling rules when they check the spelling of German text.

International features of Entourage 2004

The following topics describe the international features that are available in Entourage 2004.

Japanese contact format

By using Japanese contact format, users can enter furigana, which are characters used to indicate pronunciation, for contact information such as a contact's first, last, and organization names. Users can also keep track of greeting cards they have sent to or received from a contact according to year. Additionally, Japanese contact format changes the order of some name and address fields and removes others, such as the **Postal code** field, so that users can enter and store Japanese addresses correctly.

Lucky days

The Entourage Calendar can display lucky days. Users can choose between displaying specific lucky days or all lucky days.

Support for Japanese text

By using an input method editor (IME), users can type Japanese text in messages, tasks, and other items. This feature is available when users turn on the Japanese keyboard layout and set the Mac OS to Japanese. To do this, on the **Apple** menu, click **System Preferences**, and then click **International**. Users can also enable this feature by registering Entourage with the Microsoft Language Register for use with the Japanese language.

International features of Word 2004

The Microsoft Proofing Tools are installed in the Microsoft Office 2004/Shared Applications/Proofing Tools folder. After enabling Japanese language support, users can perform the following editing tasks:

- Check spelling and grammar according to the rules of another language.
- Look up words in the thesaurus of another language.
- Hyphenate text in another language.
- Automatically correct text typed in another language.

Formatting options for Japanese text

Special commands on the **Format** menu enable users to fit text to a specified width, set phonetic guides and enclose characters, combine characters to mix horizontal and vertical text in one line, and quickly switch between displaying hiragana and katakana characters as well as between half-width and full-width characters. By using the additional AutoFormat options for Japanese text, users can automatically insert closings in memos and other documents. Users can select options in the **Font** dialog box to specify separate fonts for Asian and Latin text and set emphasis marks. To open the **Font** dialog box, on the **Format** menu, click **Font**.

Searching for Japanese text

Japanese find options enable users to find and replace text that sounds similar and to set specific character-matching options. To do this, on the **Word** menu, click **Preferences**, and then click **Japanese Find**. Users can also set options to broaden or narrow the search for text in a document by treating some punctuation characters as identical.

Setting display options for Japanese text

Users can use Japanese Typography settings to set options for kerning and character spacing, prevent certain characters from appearing at the start or end of lines of text, and set options for line breaks. To do this, on the **Word** menu, click **Preferences**.

Setting layout options for Japanese text

The Japanese Document Grid gives users control over whether to use a line grid or line and character grid to control formatting and the measurements for the grid. To use the Japanese Document Grid, on the **Format** menu, click **Document**, and then click the **Document** tab. This feature enables users to enter characters by using fixed-pitch spacing (as in Genko or Gaozhi formatting). Users can also use the Document Grid to set the gutter at the left, the default, or top of the document and to set the document to print two full-scale pages on one sheet of paper to make booklets.

Users can also specify that their documents automatically adjust the right indent to fit the document grid, snap paragraphs to the grid, and set the paragraph alignment to distribute text. To set these options, on the **Format** menu, click **Paragraph**, and then click the **Indents and Spacing** tab.

International features of Excel 2004

The following topics describe the international features that are available in Excel 2004.

Using phonetic guides

Users can add phonetic guides to Japanese data that has been entered in a cell. The phonetic character string that was used to enter the Japanese data is used to apply phonetic guides. To display the phonetic guides on the screen, on the **Format** menu, point to **Phonetic Guide**, and then click **Show Phonetic Fields**.

If the displayed phonetic guides are incorrect, users can revise them. Select the cell that shows the incorrect phonetic guides. To revise phonetic guides, on the **Format** menu, point to **Phonetic Guide**, and then click **Edit**. Users can change the phonetic guides by using the same method they use to enter a character string.

Users can change the type, alignment, and font of phonetic guides. Three types of phonetic guides are available:

- Hiragana
- Full-width katakana
- Half-width katakana

Users can change the alignment as follows:

Alignment	Result
None	All phonetic guides are combined and aligned along the left edge of the cell.
Left (default)	Positioned along the left edge of the kanji to which the phonetic guides apply.
Center	Centered against the kanji to which the guides apply.
Distributed	Set with equal spacing against both edges of the kanji to which the guides apply.

To change the type, alignment, or font of phonetic guides, on the **Format** menu, point to **Phonetic Guide**, and then click **Settings**.

Sorting data by using phonetics

When worksheet data is sorted, by default Japanese data is sorted by its phonetic guides. If the correct phonetic guides have been used on characters that use them, Japanese terms are sorted in the same order as they would occur in a Japanese dictionary.

Automatic currency selection

Currency formats use the yen as the default monetary unit when an Office program is registered with the Microsoft Language Register for use with the Japanese language.

Language-specific custom lists

Excel provides custom lists appropriate to each supported language. For example, lists of the names of the days of the week and of the months are determined by the language settings in Mac OS X System Preferences. To choose a set of custom lists for a particular region, users must select the corresponding date and number formats on the **International** preference pane in the Apple System Preferences.

Euro conversion in Excel 2004

Like all Office 2004 programs, Excel enables users to enter, display, and print the euro symbol ( ). Excel 2004 also provides extensive support for financial calculations involving euro values through the Euro Currency Tool add-in. To load the Euro Currency Tool, on the **Tools** menu, click **Add-ins**. The Excel 2004 **Formatting** toolbar also includes a **Euro Style** button for formatting cells in euro currency style.

The Euro Currency Tool add-in provides the EUROCONVERT function, which can convert a number to euros, convert from euros to a euro member currency, or convert from one member currency to another by using the euro as an intermediary. The currencies available for conversion are those of European Union members that have adopted the euro. The EUROCONVERT function uses fixed conversion rates that are established by the European Union.

The EUROCONVERT function supports the following euro member countries/regions and currencies:

ISO code	Calculation precision	Display precision
BEF	0	0
LUF	0	0
DEM	2	2
ESP	0	0
FRF	2	2
IEP	2	2
ITL	0	0
NLG	2	2
ATS	2	2
PTE	1	2
FIM	2	2
GRD	0	2
EUR	2	2

For more information about euro currency conversion in Excel, see Excel Help.

Configuring Office 2004 for multiple languages

To enable support for international features in the English version of Office 2004, users must configure their computers to recognize the language they want to use and the proofing tools for the language must be installed.

Enabling Japanese-specific formatting and editing features

Japanese language support is available for users of the English language version of Office 2004 when the Microsoft Language Register is used to register the programs for use with the Japanese language.

By using the Microsoft Language Register, users can enable Japanese features in a number of Office 2004 programs. Users can enable Japanese features by dragging a specific Office program file to the Microsoft Language Register file, located in the Microsoft Office 2004/Additional Tools/Register folder. They should then follow the instructions in the dialog box that appears. To enable Japanese features completely, users must register the following Microsoft Office programs: Excel, Word, Entourage, PowerPoint, Graph, Organization Chart, Clip Gallery, Equation Editor, and Office Notifications.

Enabling European language features

European language support is available when one or more keyboard layouts for supported European languages are enabled on the **Keyboard Menu** tab on the **International** pane in Apple System Preferences. To switch between languages, users can select the appropriate keyboard layout. For more information about setting a keyboard layout, see Mac Help.

European language features in the English version of Office 2004 can also be enabled by installing Office 2004 on a version of the Mac OS for a supported language.

International proofing tools

Proofing tools for the supported languages are located in the Microsoft Office 2004/Shared Applications/Proofing Tools folder.

Maintenance

Managing Office 2004 product updates 145
Using AutoUpdate 145
Allowing users to perform updates independently 146
Downloading and distributing updates 146
Maintaining Office 2004 installations 146
Repairing Office 2004 installations 146
Microsoft Error Reporting Protocol 147
Deploying changes to network configuration and other preferences 148
Maintaining Entourage 2004 148
Verifying the integrity of the Entourage identity database 149
Rebuilding the Entourage identity database 150
Backing up the Entourage identity database 150
Compacting the Entourage identity database 151
Restoring the Entourage identity database 151
Troubleshooting Entourage Exchange e-mail accounts 151

After you deploy Office 2004, you will want to update and maintain your deployment. Office 2004 offers various ways to keep your deployed software up-to-date and running smoothly.

Managing Office 2004 product updates

Over time, Microsoft publishes updates to Office 2004. An update is a widely released fix for a specific problem that addresses a critical or non-critical bug or a security consideration. A service pack is a cumulative set of all security updates, critical updates, and fixes for defects found internally since the release of the product. Service packs may also contain a limited number of customer-requested design changes or features.

You can use Microsoft AutoUpdate for Mac to look for updates to your Microsoft software. Alternatively, you can find updates and service packs for Office 2004 and downloads for the different versions of Office for Mac on the Downloads page of the Microsoft Web site at http://www.microsoft.com/mac. To see a description of the changes that are included in an update, click the update.

You will want to establish a policy for your organization that specifies whether users can download and install updates on their own. You may prefer to evaluate updates centrally and then deploy the ones that meet your criteria.

Using AutoUpdate

AutoUpdate looks for new and updated versions of a user's Microsoft software, and then installs any updates that the user approves. You can control whether AutoUpdate looks for updates automatically or whether the user must start the update process manually.

To turn automatic update checking on or off

1. On the **Help** menu in an Office 2004 program, click **Check for Updates**.
2. In the **Microsoft AutoUpdate** dialog box, click **Manually** or **Automatically**.
3. If you have chosen automatic updates, on the **Check for Updates** pop-up menu, click the schedule you want.

Preferences for AutoUpdate are stored in com.microsoft.autoupdate.plist. This file is located in a user's Library/Preferences folder. You can manage these and other preference settings centrally on user computers. For more information about deploying preferences, see Deploying Preferences in the "Deployment" section.

Allowing users to perform updates independently

If you are not deploying Office 2004 updates centrally, you can instruct users in your organization to use Microsoft AutoUpdate. By default, AutoUpdate is set to look for updates automatically once a week.

Downloading and distributing updates

If you prefer to deploy updates centrally, you can instruct your users not to download updates from the Microsoft Web site and not to use Microsoft AutoUpdate. The following steps describe how to download and distribute an update or service pack of Office 2004.

To download and deploy an update or service pack of Office 2004

- Go to the Downloads page of the Microsoft Web site at http://www.microsoft.com/mac, and then follow the instructions for downloading the latest Office 2004 update or service pack.

  Note If the file that you download does not expand, double-click the downloaded file to put the update volume on your desktop.

- Use one of the available methods for deploying the contents of the volume. For information about deployment options, see Deploying the Office 2004 programs in the "Deployment" section.

Maintaining Office 2004 installations

Office 2004 installations typically require no maintenance. However, if an installation of Office 2004 needs repair, you can quickly remove the installation and re-install it. Also, if an Office 2004 program stops responding, a user can send an error report to Microsoft by using the Microsoft Error Reporting Protocol (MERP). If your network configuration changes, you can deploy new settings to user computers.

Repairing Office 2004 installations

If an installation of Office 2004 does not run or does not function correctly, run the Remove Office utility to remove the installation, and then reinstall Office 2004. You can use Remove Office to remove Office 2004 or any one of its components.

When you install Office 2004, the Remove Office program is installed to the hard disk by default. It is located in the Microsoft Office 2004/Additional Tools/Remove Office folder.

Remove Office removes files installed by Microsoft Office 2004. These files include Microsoft shared libraries that might be required by other programs. If a program does not start after you use Remove Office, try reinstalling the program to fix the problem.

For more information about how to remove Office 2004, see the Microsoft Remove Office Read Me in the Remove Office folder.

Microsoft Error Reporting Protocol

Office 2004 includes the Microsoft Error Reporting Protocol (MERP) to enable users to communicate bug data anonymously to Microsoft. Microsoft uses the bug data to quickly locate and fix software problems and help increase the overall stability of Office 2004. By default, Microsoft Error Reporting is enabled in Office 2004.

If an Office program stops responding, MERP generates a report that details the circumstances. The MERP user interface asks users to send error report data to Microsoft through the Internet. For an explanation of what the data is, why it is collected, and what is done with it, see Microsoft Online Crash Analysis at http://oca.microsoft.com.

You should review the data collection policy for Microsoft Online Crash Analysis and determine whether this policy is compatible with the privacy standards of your organization. You will want to establish a policy for your organization that specifies whether users should send error report data to Microsoft.

To disable Microsoft Error Reporting in Office 2004

1. Start the Microsoft Error Reporting program, located in the Microsoft Office 2004/Office folder.
2. On the **Microsoft Error Reporting** menu, click **Preferences**.
3. Clear the **Enable Microsoft Error Reporting** check box.

   Preferences for Microsoft Error Reporting are stored in com.microsoft.error_reporting.plist. This file is located in the Preferences folder in a user's Library.

Deploying changes to network configuration and other preferences

You can use a combination of available tools to deploy network configuration and other preference changes to user computers.

Some network parameters, such as proxy server port settings, are maintained in the Network area of Apple System Preferences. You can deploy changes to Apple System Preferences by using Apple Workgroup Manager.

You can deploy updates to the Office 2004 program preferences that are stored in .plist files by using Apple Workgroup Manager or Apple Remote Desktop.

> **Note** When you deploy a revised .plist file by using Apple Remote Desktop, you override all stored user preferences for the program governed by the file.

Some settings, such as the mail server name, are stored in the Entourage database. To change Entourage database settings for a group of users, you can write a script and deploy it by using Apple Remote Desktop. To see a dictionary of the Entourage settings that you can change by using AppleScript, drag the Entourage icon (located in the Office 2004 folder) onto the Script Editor icon (located in the Applications/AppleScript folder).

> **Important** Many Entourage preferences cannot be changed by using a script. You also cannot change these preferences by deploying a database with new settings to an existing user identity, because the new settings will override the existing local data for each user.

For more information about deploying preferences, see Deploying Preferences in the “Deployment” section.

For more information about AppleScript, see AppleScript Resources for Office 2004 in the Developer Center under Resources on the Microsoft Web site at http://www.microsoft.com/mac.

For more information about Apple Remote Desktop, see Apple Remote Desktop 3 on the Apple Web site at http://www.apple.com/remotedesktop.

For information about managing preferences by using Workgroup Manager, see the “Managing Preferences” section of User Management on the Apple Web site at http://www.apple.com/server/documentation.

Maintaining Entourage 2004

To maintain Entourage 2004 for users in your organization, you might need to work with the Entourage database and import data to Entourage 2004.

To verify, compact, or rebuild the Entourage database, use the Database Utility tool, located in the Microsoft Office 2004/Office folder. The compacting process first creates a backup and then optimizes the database. For more information about the maintenance activities you can perform on the Entourage database, see Database Utility Help.

Verifying the integrity of the Entourage identity database

If you experience one or more of the following problems with your deployment of Office 2004, the Entourage database might be damaged and you might have to rebuild it:

- Entourage does not start or crashes.
- Entourage items do not open, or the item that opens is not the item that was double-clicked.
- Blank lines appear in the Entourage message list or Word Address Book.
- Word Address Book entries are not displayed correctly.
- The clips in the Scrapbook disappear.
- Information that was added, such as a Calendar event or a contact, cannot be found.
- In an Entourage search, the search results do not match the criteria that were set.
- A blank Office Notifications window appears.

If you suspect that the database is damaged, try to determine the source of the problem before you run the Database Utility to verify the integrity of the database and try to fix it. Repairing the database could cause data loss. Therefore, first make sure that you did not accidentally cause the symptom—for example, by moving a message to the wrong folder. Also, make sure that the problem is not the result of general computer problems, such as a damaged or fragmented hard disk. To do this, run a disk diagnostics and repair program, such as Apple Disk Utility. For more information about identifying and repairing hard disk problems, see the documentation for the disk utility program.

To verify the integrity of the Entourage database

1. Quit all Office programs, including Entourage and Office Notifications.
2. In the Office folder, double-click the Database Utility program.

   -or-

   Hold down the OPTION key while starting Entourage.
3. Click the identity of the database you want to verify.
4. Click **Verify database integrity**, and then click **Continue**.
5. Follow the instructions that appear on the screen.

If Entourage detects a problem with the database, it automatically starts the Database Utility.

Rebuilding the Entourage identity database

When you rebuild the database, Entourage does not modify the existing database. Instead, it makes a copy of the database and then rebuilds and compacts the copy. The copy then becomes the active database. After Entourage finishes the rebuild process, it creates two folders in the Identities folder related to the identity that was rebuilt.

Database folder	Example
Newly rebuilt database	Main identity
Backup copy of the database before it was rebuilt	Main identity [*Backed up date and time*]

The backup copy displays the date and time it was created after its name. If the computer does not have enough free disk space to store both your current database and a copy of it, an out-of-memory error occurs. For example, if the current size of the database is 10 megabytes (MB), you need at least 20 MB of free disk space to rebuild the database.

To rebuild the Entourage database

1. Quit all Office programs, including Entourage and Office Notifications.
2. In the Office folder, double-click the Database Utility program.

   -or-

   Hold down the OPTION key while starting Entourage.
3. Click the identity of the database you want to rebuild.
4. Click **Rebuild database**, and then click **Continue**.
5. Follow the instructions that appear on the screen.

Note In situations where an Exchange account is used from both Entourage and Outlook, rebuilding an Entourage database might cause e-mail messages to be duplicated. To avoid this duplication, delete the Exchange account in Entourage before rebuilding the database, then recreate the Exchange account.

Backing up the Entourage identity database

You will want to create, or instruct your users to create, backups of the Microsoft User Data folder or of only the folder for any single identity. If you cannot start Entourage or open data, first try rebuilding the database. If you continue to have problems, restore the data from the backup copy.

To back up an Entourage identity database

1. In the *username*/Documents/Microsoft User Data/Office 2004 Identities folder, locate the *indentityname* folder that you want to back up.
2. Copy the folder to another location.

Compacting the Entourage identity database

Compacting the Entourage identity database also makes a backup copy of the database, as rebuilding the database does.

To compact and back up the Entourage database

1. Quit all Office programs, including Entourage and Office Notifications.
2. Double-click the Database Utility program located in the Office folder.

   -or-

   Hold down the OPTION key while starting Entourage.
3. Click the identity of the database that you want to compact and back up.
4. Click **Compact database**, and then click **Continue**.
5. Follow the instructions that appear on the screen.

Note If an Exchange account is used from both Entourage and Outlook, compacting an Entourage database might cause mail messages to be duplicated. To avoid this duplication, delete the Exchange account in Entourage before compacting the database, then re-create the Exchange account.

Restoring the Entourage identity database

If problems continue, restore the data from the backup copy.

To restore the Entourage database

1. Locate the existing *identityname* folder in *username/*Documents/Microsoft User Data/Office 2004 Identities that you want to replace with a backup copy.
2. Drag the folder to the Trash.
3. Drag the backup copy to the former location of the folder you are replacing.
4. Adjust the folder name by removing the backup date information, if any. The user can then continue working with the familiar identity name.

Troubleshooting Entourage Exchange e-mail accounts

Your users might encounter the following issues if they use Entourage 2004 as an Exchange client. For more information about common issues with administering Entourage clients, see Common Entourage issues in an Exchange environment in the “Planning” section.

Full mail addresses

Always make sure that messages sent by using the Exchange mail account use the full e-mail address for the account — for example, *alias*@microsoft.com, not just “*alias*”.

Global Address List availability

The Global Address List (GAL) is available to Entourage 2004 users only if the Active Directory global catalog server is exposed to LDAP queries.

Exchange Server issues

If Entourage 2004 users are connected to your Exchange Server network, the following issues might be caused by interaction problems between Exchange Server and Entourage:

- Mail folders are displayed in Outlook Web Access or Outlook, but not in Entourage. Make sure that the latest Exchange server updates and service packs have been applied to the Exchange server. Use Outlook Web Access or Outlook to rename the folders that were not displayed, and then rename them back to their original names. For more information, see Some Exchange 2000 Server folders are missing when you view the folders by using Entourage 2004 for Mac, Knowledge Base article 840546 on the Microsoft Web site at http://support.microsoft.com.
- An unexplained failure to synchronize messages in the Entourage error log might be the result of the Exchange server blocking certain WebDAV verbs that Entourage needs. For more information, see Fine-Tuning and Known Issues When You Use the Urlscan Utility in an Exchange 2003 Environment, Knowledge Base article 823175 on the Microsoft Web site at http://support.microsoft.com.
- The read status of public folder mail messages might be lost when the folder is synchronized. There is no workaround for this issue. This issue may occur if you empty the cache for your Exchange account before the changes are synchronized to your Exchange Server computer. To avoid this problem, do not empty the cache for your Exchange account before changes are synchronized to your Exchange Server computer. For more information, see You may lose changes to e-mail messages when you empty the cache for an Exchange account in Entourage 2004, Knowledge Base article 884989 on the Microsoft Web site at http://support.microsoft.com.
- If users are receiving too many reminders, the Calendar preference **Tentatively add events when invitations are received** might be enabled. To eliminate this kind of reminder, disable this preference.

  Note By default, this preference is disabled when an Exchange account is created in Entourage.

  To disable the "Tentatively add events when invitations are received" preference

  1. On the **Entourage** menu, click **Preferences**.
  2. Under **General Preferences**, click **Calendar**, and then clear the **Tentatively add events when invitations are received** check box.

BlackBerry issues

If your organization uses BlackBerry devices and Exchange 2000 Server and events are duplicated in Entourage calendars that are not on Exchange accounts, make sure that Exchange 2000 Server has the update mentioned in XADM: Update Method Results in Duplicate Calendar Entries with Outlook 2002; Post Exchange 2000 SP2 Update, Knowledge Base article 313863 on the Microsoft Web site at http://support.microsoft.com.

Calendar issues

Entourage 2004 cannot read .msg files. If Outlook users drag events from their Outlook Calendar to outgoing e-mail messages, Outlook attaches these events as .msg files, which Entourage 2004 cannot read. If you experience this problem, instruct users to forward events as .ics files, which is a file format used by iCalendar and supported by Entourage 2004.

Error numbering convention for HTTP-related errors

The WebDAV protocol that is used by Entourage 2004 for Exchange mail accounts uses the error numbering convention defined by the HTTP protocol. The convention is -19000 + <*HTTP status code*>. For example, -18600 translates to 400 and is a “Bad Request” message, and -18596 translates to 404 and is a “Not Found” message. For more information about status strings, see Status Code Definitions at http://www.w3.org.

Error numbering convention for LDAP-related result codes

The Lightweight Directory Access Protocol (LDAP) that Entourage 2004 uses to query the Active Directory global catalog server uses the result code numbering convention defined by the LDAP standards. These result codes can help you troubleshoot problems with the global catalog server. The standard is -17800 + <*LDAP result code*>. Entourage uses the result codes as specified in RFC 2251, section 4.1.10, “Result Message,” with the omission of the "success" result code. For example, -17798 translates to 2 and is the “protocolError” result code. For more information about LDAP result codes, see RFC 2251 at http://www.faqs.org/rfcs.

In some cases, the otherwise unused result codes are supplemented by additional Request For Comments (RFCs) or Internet Engineering Task Force (IETF) drafts, including result codes for controls. An important LDAP extension is for the virtual list view (VLV) control described in LDAP Extensions for Scrolling View Browsing of Search Results at http://www.ietf.org. Section 6.2 of this draft, “Response Control,” describes two new results that Entourage uses for the VLV control: sortControlMissing (60) and offsetRangeError (61).