CHAPTER 25

Using Outlook Securely

In this chapter

Storing and Sharing Information

Outlook provides many methods for storing and sharing information. You can export information to Personal Folders files for backup and even transfer those Personal Folders files to others to share contacts, emails, tasks, journal entries, notes, and any other type of Outlook item. Using Exchange Server provides additional storage and sharing options, such as public folders and directly accessing another user's folder through folder permissions.

These days, more and more people are living in their email program. You can use email to communicate with coworkers, friends, and family. You can store travel arrangements, financial information, and even important documents right in your Personal Folders file or Exchange mailbox. Because email is used for mission-critical business applications and important personal information, making sure that the information you store in Outlook is secure is very important. Email cannot be used within a vacuum. You cannot use email and not have your computer connected somehow to the outside world, either through a modem or network connection. New viruses that have the capability of wiping your entire hard drive clean with one wrong double-click of a program are introduced every week.

Even if you have an effective antivirus program and always keep it updated, there's always the possibility your computer will fail. I once had a computer literally catch fire in front of me. It was only a year old and hadn't been backed up in a month. I lost a month's worth of digital pictures, files, and emails. It turned out that the power supply was from a bad batch that had a tendency to catch fire after about a year of use. Even though my computer was backed up fairly regularly, I couldn't avoid some loss of data from this minor explosion. Although that scenario was an isolated incident and likely will never happen to you, a computer failure is always possible.

Where is your computer located? If you work in an office, is your computer publicly accessible? Could other employees come in your office on your lunch hour and use your computer without someone stopping them? What sort of information would they be able to access if they did that? Could they send an email from your account without your knowledge? What would you do if that happened? These are all questions you should ask yourself when thinking about the physical security of your computer.

This chapter covers several topics: your computer's physical security, the integrity of your emailed information, and the security of your emailed information. You'll learn about sending and receiving encrypted email, as well as a new feature in Outlook and the other Office 2003 programs, information rights management.

Securing Outlook Items

There are several ways to secure your Outlook items. You can add some basic security to your individual items by marking them private, or you can secure your entire Personal Folders file. Additional steps can be taken when using Outlook as a client for Exchange Server.

You can take security to the next level by using digital certificates and digital signatures. At that point, you should make sure that your computer is physically secure because after you attach a digital signature to your email messages, you want to ensure that you're the only one sending those emails. Otherwise, someone could use the digital certificate to impersonate you when sending messages.

MARK ITEMS AS PRIVATE

When you create certain Outlook items, such as calendar items, journal entries, and tasks, you can mark them as private. This can hide them in several circumstances. If you're sharing a folder with another user, private items are not displayed to the other user. If you give someone delegate access, you can choose whether your delegates can view your private items.

To create a private appointment, check the Private check box on the first page of the Appointment form. After you mark an item as private, you can view the item, but others with access to your folder see only the existence of the item. For example, when viewing the Calendar folder of another user, Figure 25.1 shows a meeting that isn't marked private at 9 a.m. and an appointment that's marked private at 11 a.m.

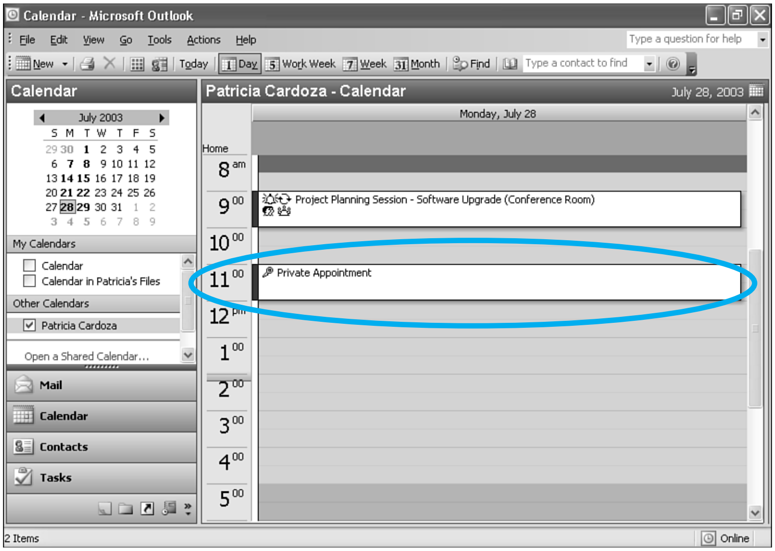
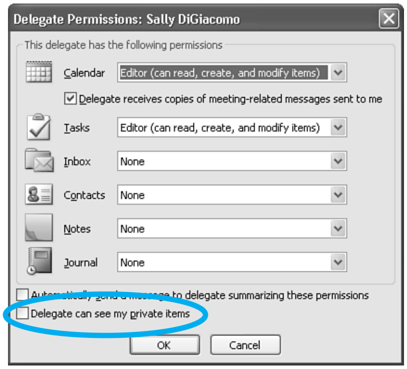

Calendar - Microsoft Outlook
File Edit View Go Tools Actions Help
Type a question for help
New Today Day Work Week Week Month Find Type a contact to find
Calendar
July 2003
My Calendars
Calendar
Calendar in Patricia's Files
Other Calendars
Patricia Cardoza
Open a Shared Calendar...
Mail
Calendar
Contacts
Tasks
Patricia Cardoza - Calendar
July 28, 2003
Monday, July 28
Home
8 am
9 00
10 00
11 00
12 pm
1 00
2 00
3 00
4 00
5 00
Project Planning Session - Software Upgrade (Conference Room)
Private Appointment
2 Items
Online

Figure 25.1
You can mark items private so that their details don't appear to others sharing your folder.

If you've given another Exchange user delegate access to any of your folders, you can choose whether or not to allow that user to view private items. To check this option, select Tools, Options, and click the Delegates tab. Select the delegate and click Permissions to display Figure 25.2. If you want to hide your private items from your delegate, uncheck the box marked Delegate Can See My Private Items.

Figure 25.2
You can prevent your delegates from seeing your private items.



Delegate Permissions: Sally DiGiacomo

This delegate has the following permissions

Calendar	Editor (can read, create, and modify items)
	☑ Delegate receives copies of meeting-related messages sent to me
Tasks	Editor (can read, create, and modify items)
Inbox	None
Contacts	None
Notes	None
Journal	None

□ Automatically send a message to delegate summarizing these permissions

□ Delegate can see my private items

Securing a Personal Folders File

If you're not using Outlook as a client for Exchange Server, or if you aren't storing your Outlook items on the Exchange Server computer, you must be using a Personal Folders file. You can secure your Personal Folders file with a password to make it more difficult for others to open that file without your permission.

NOTE

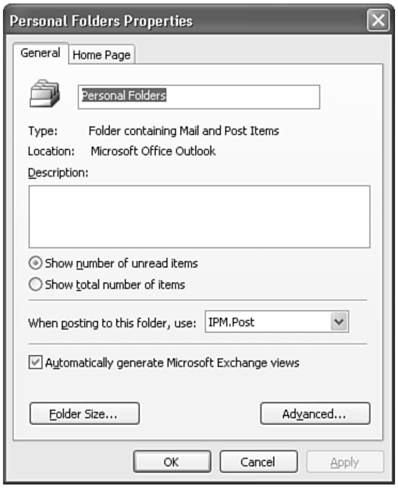
Although you can set a password on your Personal Folders file, doing so doesn't guarantee that no one can open your Personal Folders file. Password-cracking utilities are widely available on the Internet. A good password-cracking utility can be had for under $50. Even though this can be a lifesaver if you ever forget your Personal Folders file password, it also means that an unscrupulous person can crack your password for very little money.

To create a password for your Personal Folders file, use the following steps:

1. Right-click the top-level folder in your Personal Folders file (usually named Personal Folders) and choose Properties.
2. Click the Advanced button to display Figure 25.3.
3. Click the Change Password button to display Figure 25.4.
4. If you previously had a password on the Personal Folders file, enter it in the Old Password text box.
5. Enter your new password in both the New Password and Verify Password text boxes.
6. If you want to save the password so that you don't have to enter it every time you open your file, check the box marked Save This Password in Your Password List.

CAUTION

Be careful when saving your password in your password list. If you do this, anyone with access to your computer can open the Personal Folders file and access the data within it.



Personal Folders Properties

General | Home Page

Personal Folders

Type: Folder containing Mail and Post Items

Location: Microsoft Office Outlook

Description:

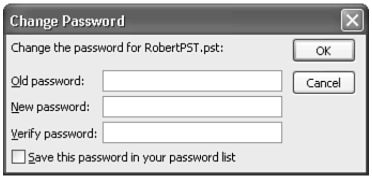
● Show number of unread items

○ Show total number of items

When posting to this folder, use: IPM.Post

☑ Automatically generate Microsoft Exchange views

Figure 25.3
Use this dialog box to assign a password to the Personal Folders file.



Change Password

Change the password for RobertPST.pst:

Old password:

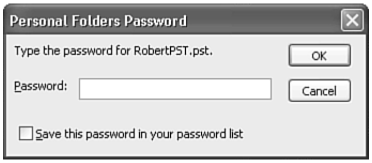
New password:

Verify password:

□ Save this password in your password list

Figure 25.4
You can create a password or change a password from this dialog box.

7. Click OK to save your password andOutlook as a client for Exchange Server, or if you aren't storing your Outlook items on the Exchange Server computer, you must be using a Personal Folders file. You can secure your Personal Folders file with a password to make it more difficult for others to open that file without your permission.To create a click OK again to exit the Personal Folders property dialog box.
8. The next time you start Outlook, you'll be presented with the Personal Folders Password dialog box shown in Figure 25.5. Enter your password and click OK to access your Personal Folders file.



Personal Folders Password

Type the password for RobertPST.pst.

Password:

□ Save this password in your password list

Figure 25.5
Enter your Personal Folders password to access your items.

Exchange Server Security

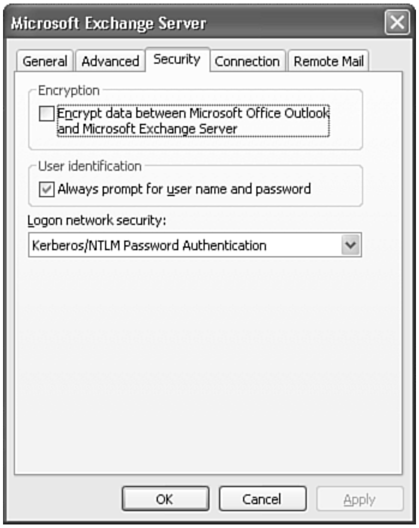
When you use Outlook as a client for Exchange Server, you can take some additional measures to protect your data. First of all, you can require Outlook to ask for a password before it opens. Second, you can control who can access your data and the level of access they have through permissions.

Logon Security

If you use Outlook as an Exchange client, the default configuration is to use NTLM security to access your Exchange mailbox. That means to log on to your Exchange mailbox, you must first be logged on to Windows with the user account associated with your Exchange mailbox. Although this is the easiest method of accessing Outlook as an Exchange client, it doesn't provide any extra security. As long as you've logged on to Windows, anyone can access your Outlook profile.

You can change the authentication method Outlook uses and require that your password be entered every time Outlook is opened. This does nothing for the physical security of your computer or its data, but it prevents anyone who doesn't know your network password from accessing Outlook. To change your authentication method for Outlook, use the following steps:

1. Open Outlook and choose Tools, E-mail Accounts, View or Change Existing E-mail accounts, and click Next.
2. Choose your Microsoft Exchange Server account and click Change.
3. Click the More Settings button to display the General properties for your Exchange account.
4. Click the Security tab to display Figure 25.6.



Microsoft Exchange Server

General | Advanced | Security | Connection | Remote Mail

Encryption

□ Encrypt data between Microsoft Office Outlook and Microsoft Exchange Server

User identification

☑ Always prompt for user name and password

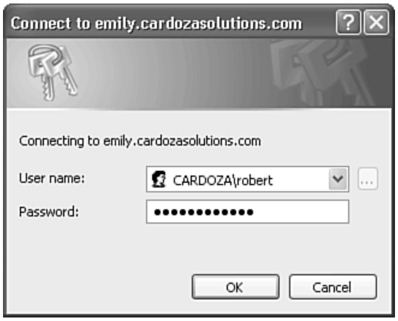
Logon network security:

Kerberos/NTLM Password Authentication

Figure 25.6
Use this dialog box to require Outlook to ask for a password every time it opens.

5. Check the box marked Always Prompt For User Name And Password.
6. Click OK, Next, and Finish to save your changes.

The next time you start Outlook, you'll be required to enter your username, password, and domain to access your Outlook data, as shown in Figure 25.7. You'll have to enter your username and domain in the format *domain\username*. If an incorrect password is entered, Outlook won't open.



Connect to emily.cardozasolutions.com

Connecting to emily.cardozasolutions.com

User name: CARDOZA\robert

Password: ●●●●●●●●●●●●●

Figure 25.7
Enter your username, password, and domain to log on to Outlook.

After you've entered your username, password, and domain, subsequent openings of Outlook will require you to re-enter only your password. The other information is saved unless someone else is also using your computer to access Outlook.

Encryption

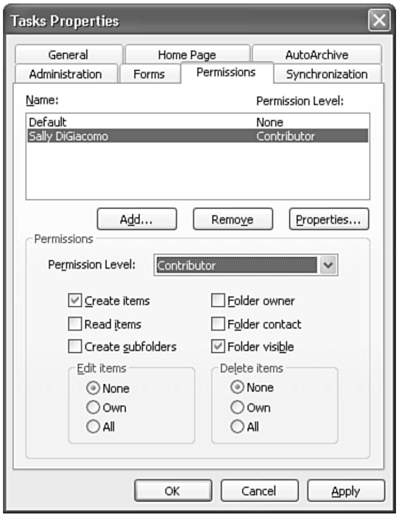
Outlook 2003 offers one additional security feature when connecting to an Exchange Server: encryption. You can choose to encrypt your data as it travels between the client and the server. When the data reaches either the client or the server, it is decrypted. Choosing to encrypt your Outlook data does nothing for the data residing in Personal Folders or Archive files, but it offers an additional layer of security as your messages are transmitted between client and server.

To add encryption to your Exchange email account, use the following steps:

1. Choose Tools, E-mail Accounts, View or Change Existing E-mail Accounts, and click Next.
2. Select your Exchange account and click Change, and then click the More Settings button.
3. Choose the Security tab shown previously in Figure 25.6.
4. Check the box marked Encrypt Information.
5. Click OK twice, click Next, and then click Finish to save your settings.

Using Permissions

If you share your Outlook data with other users through Exchange Server, you can specify the exact permission level they have on all your Outlook items. For example, if you have an assistant, you can give him access to your Calendar folder so that he can schedule meetings for you while you're out of the office. However, you don't want him to be able to change any of your existing meetings. To do this, right-click your Calendar folder and select Properties. Choose the Permissions tab and configure your permissions to match those in Figure 25.8.



Name:	Permission Level:
Default	None
Sally DiGiacomo	Contributor

Permissions

Permission Level: Contributor

☑ Create items
□ Read items
□ Create subfolders
□ Folder owner
□ Folder contact
☑ Folder visible

Edit items
● None
○ Own
○ All

Delete items
● None
○ Own
○ All

Figure 25.8
The permissions shown here allow your assistant to create new items, but not to edit any items.

You can give your assistant Contributor access to your folder. Your assistant can see the folder, but he cannot see any of the items in the folder. He also can't edit any items in the folder, even the items he creates.

➔ For more information on Exchange Server permission levels, **see** "Granting Access to a Public Folder," **p. 705**.

Sending Secure Messages

Now that you know how to secure the individual items within Outlook and secure your computer, you can take security one step further by learning to send secure messages. Sending secure messages is a bit like requiring a driver's license when making a credit card purchase. A digital certificate guarantees that you are who you say you are—much like your driver's license assures a retail store that you're really the same person whose name is on the credit card.

A digital certificate is an electronic driver's license, in a way. Composed of a public and private key, a certificate can accomplish two things. First, it can assure the recipient of your email that it really did come from you. Second, it can guarantee that the email wasn't changed between the sender's machine and the recipient's machine.

Using Certificates

As alluded to previously, a certificate can provide two very valuable services: authentication and encryption. You can use a certificate for authentication to verify that the person sending you email is the same person who owns the email address the email was sent from. In other words, I can't send an email from `john@doe.com` unless my email account actually is `john@doe.com`. I can't spoof an email address and attach a digital certificate to the email at the same time.

Encryption involves taking your plain text email messages and encoding the data so that only the intended recipient can decode the data. Your recipient must have a copy of your public key to decrypt the email message. Anyone else who might try to intercept the email message and open it would see only garbage where the text should be.

NOTE

A certificate works by using the Secure Multipurpose Internet Mail Extensions (S/MIME) protocol that Outlook supports. You can exchange secure messages with anyone who uses an email client that supports S/MIME.

A certificate is made up of two parts: a private key and a public key. The private key is stored on your computer, in the Windows Registry. It isn't known or distributed to anyone. You can use your private key to sign the messages you send.

The public key is a file that you can send to others who want to send you encrypted messages. You can attach the public key to your contact record and share it with others by sending them your contact record. When someone wants to send you an encrypted email, they must use your public key. When you receive the email, you use your private key to decrypt that email. If you want to receive encrypted messages from someone with a digital certificate, you must have a copy of her public key available and attached to her contact record in your Contacts folder.

OBTAINING A CERTIFICATE

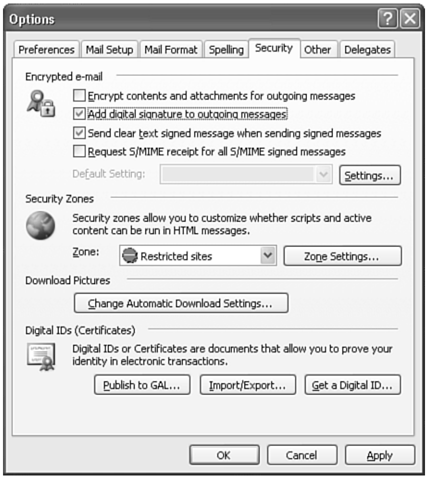
You can obtain a certificate from a certificate authority (CA). Two of the most popular CAs are VeriSign and Thawte. VeriSign offers a free trial digital certificate that's valid for 60 days. If you want to continue using that digital certificate, the price at the time this book was written was $14.95 per year. Thawte offers a free personal digital certificate. To obtain a digital certificate from either of these companies, you need to connect to its Web site and register with a valid email address. You'll receive a confirmation email that requires you to validate your email address before you receive your digital certificate.

After you receive your digital certificate, you can set up Outlook to use that digital certificate to send and receive signed and encrypted email.

SETTING UP CERTIFICATES

When you sign up for a digital certificate from a certificate authority, it will send you a confirmation email, usually with a PIN that you must enter on the CA's Web site to download and install your digital certificate. After you've downloaded the digital certificate, use the following steps to install that certificate in Outlook 2003:

1. From Outlook, choose Tools, Options, and click the Security tab to display Figure 25.9.



Options

Encrypted e-mail

□ Encrypt contents and attachments for outgoing messages

☑ Add digital signature to outgoing messages

☑ Send clear text signed message when sending signed messages

□ Request S/MIME receipt for all S/MIME signed messages

Default Setting:

Security Zones

Security zones allow you to customize whether scripts and active content can be run in HTML messages.

Zone: Restricted sites

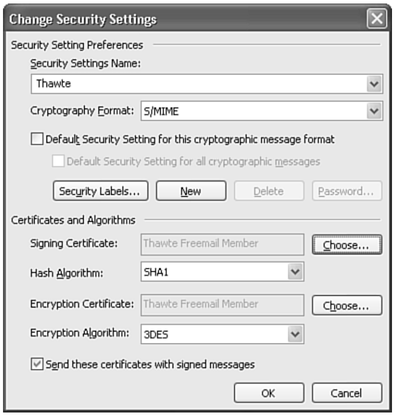
Download Pictures

Digital IDs (Certificates)

Digital IDs or Certificates are documents that allow you to prove your identity in electronic transactions.

Figure 25.9
Use the Security tab to configure digital certificate settings.

2. If you want to send a digital signature with all outgoing messages, check the box marked Add Digital Signature to Outgoing Messages.
3. Click the Settings button to display Figure 25.10 and configure your digital signature.



Change Security Settings

Security Setting Preferences

Security Settings Name: Thawte

Cryptography Format: S/MIME

□ Default Security Setting for this cryptographic message format

□ Default Security Setting for all cryptographic messages

Certificates and Algorithms

Signing Certificate: Thawte Freemail Member

Hash Algorithm: SHA1

Encryption Certificate: Thawte Freemail Member

Encryption Algorithm: 3DES

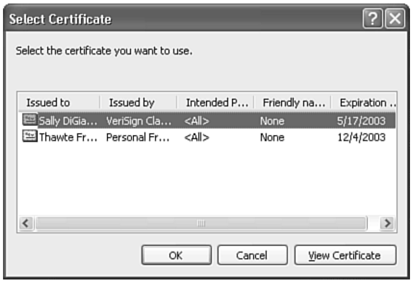
☑ Send these certificates with signed messages

Figure 25.10
Your digital signature might already appear in the drop-down box.

4. You can enter a name in the Security Settings Name box, although it's likely that a name will already be entered in this field when you install the digital certificate.
5. Your next choice depends on whether you want to use your digital certificate for Exchange email or Internet email. Chances are if you're sending mail within your Exchange Server, you don't need a digital certificate. After all, you should be authenticated on the domain if you're using Exchange Server, and very few companies require authenticated email between members of the same Exchange Server. If you're using your digital certificate for Internet email, accept the default choice of S/MIME for the

Cryptographic Message drop-down list. If you need the digital certificate for Exchange email, you can change this drop-down choice to Exchange Server Security.

6. You'll usually want to leave the next two check boxes checked. The first, Default Security Setting for This Cryptographic Message Format, means that for all S/MIME messages you send, you want Outlook to use these security settings. The second check box, Default Security Settings for All Cryptographic Messages means that you want all messages, regardless of format, to use these security settings.
7. In the Certificates and Algorithms section, click the Choose button next to the Signing Certificate text box to display Figure 25.11.



Select Certificate

Select the certificate you want to use.

Issued to	Issued by	Intended P...	Friendly na...	Expiration ..
Sally DiGia...	VeriSign Cla...	<All>	None	5/17/2003
Thawte Fr...	Personal Fr...	<All>	None	12/4/2003

Figure 25.11
Choose the signing and encryption certificates.

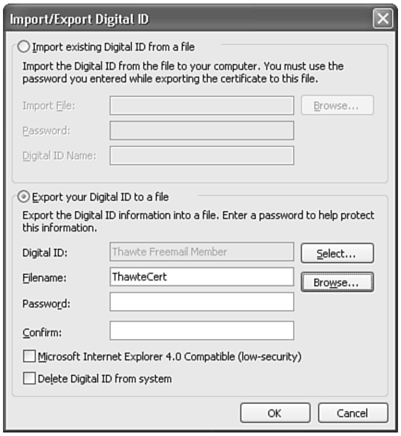
8. If you have multiple certificates installed on this machine, choose the certificate you want to use for this email account. It's possible that you'll have multiple profiles in Outlook with different email addresses. You can install a different certificate for each email address and configure the settings in each Outlook profile. Choose your certificate and click OK to return to the Change Security Settings dialog box. You'll see values in both the Hash Algorithm box and the Encryption Algorithm box. Do not change these values—they're set by the certificate.
9. If you want to send your public key to other users, make sure the check box marked Send These Certificates with Signed Messages is checked. Otherwise, your public key won't be sent with your messages and recipients won't be able to receive encrypted email from you.
10. Click OK twice to save your settings.

You've now completed the setup for your digital certificate and you're ready to send and receive signed messages.

BACKING UP YOUR DIGITAL CERTIFICATE

After you've installed and configured your digital certificate, you can use the following procedure to make a backup copy. A backup copy can be helpful in case of a hard drive failure or if you need to change computers.

1. Within Outlook choose Tools, Options and click the Security tab.
2. In the Digital ID section at the bottom of the dialog, click Import/Export to display Figure 25.12.



Import/Export Digital ID

○ Import existing Digital ID from a file

Import the Digital ID from the file to your computer. You must use the password you entered while exporting the certificate to this file.

Import File:

Password:

Digital ID Name:

● Export your Digital ID to a file

Export the Digital ID information into a file. Enter a password to help protect this information.

Digital ID: Thawte Freemail Member

Filename: ThawteCert

Password:

Confirm:

□ Microsoft Internet Explorer 4.0 Compatible (low-security)

□ Delete Digital ID from system

Figure 25.12
You can export your Digital ID to a file for backup purposes.

25

3. Choose Export Your Digital ID to a File.
4. Click Select to choose your digital ID, click OK when you have selected the proper digital ID.
5. Enter a filename for the exported digital ID or click Browse to choose a location on your hard drive to save the file. Click Save when you've selected a location and entered a filename to return to the Import/Export Digital ID options.
6. Enter a password (and confirm it) for your saved digital ID. This prevents unauthorized users from attempting to import your digital ID. You must enter a password to save your digital ID.
7. Leave the Microsoft Internet Explorer 4.0 Compatible check box unchecked. If you want to remove your digital ID from the system (for example, when trading computers with a colleague), check the box marked Delete Digital ID from system; otherwise, leave this box unchecked.
8. Click OK to export your digital ID.

You should keep the backup copy of your digital ID in a safe place. It's a good idea to back up the file to a CD or disk and keep that copy in a fire safe or somewhere secure.

Importing a Digital ID from a Backup

It is relatively simple to import a digital ID from a backup copy. Use the following steps to import a digital ID:

1. Select Tools, Options, and click the Security tab.
2. Click Import/Export to display the dialog shown previously in Figure 25.12.

3. If it's not selected, select Import Existing Digital ID from a File.
4. Click Browse to select the file you want to import.
5. Enter the password of the saved digital ID.
6. In the Digital ID Name box, enter a name that you want Outlook to use to refer to your digital ID. Any name is acceptable.
7. Click OK to import your digital ID.

NOTE

> After you install your digital ID, Outlook automatically adds two buttons to your email toolbar: Sign and Encrypt. You can use these buttons to sign messages you send to others.

Sending and Receiving Signed Messages

When you've installed and configured your digital ID, you can have Outlook automatically attach your digital ID to all messages you send, or manually attach the digital ID to specific messages you send. There's usually nothing wrong with attaching a digital ID to every message you send, but there are a few circumstances in which you might not want to do so:

- If you routinely send email to recipients who can't decode digitally signed email (such as to a cellular phone or PDA), there's really no benefit to sending an email with a digital ID.
- If the size of an email is ever an issue, consider not including your digital ID unless you absolutely need to. An email with an attached digital ID is at least 6KB larger than an identical email sent without the digital ID. Although this isn't a large amount, the extra KB can add up if you send many emails.

Outlook's default setting is to not automatically attach a digital ID to every outgoing email. To change this, select Tools, Options, and click the Security tab. Check the box marked Add Digital Signature to Outgoing Messages. Doing so automatically adds a digital signature to every outgoing message you send. If you need to send a message without a digital signature, you can always click the Digitally Sign button on the toolbar of the message while composing it to remove the digital signature on a per-message basis. The digitally sign icon looks like an envelope with a red certificate attached.

Sending a Signed Message

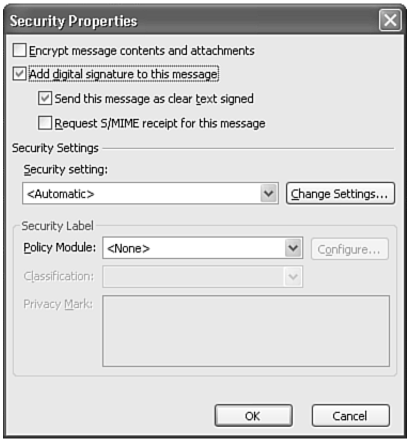
After you've configured your security settings, you can use them to send and receive signed messages. The recipient of your email can examine the digital signature attached to your message to verify that you are who you say you are.

A digitally signed message actually contains two separate copies of the message. The first is an unencrypted copy of the message. The second part is an encrypted version of the same message. When the recipient opens the message, the encrypted version and the unencrypted version are compared. If they match, the certificate is valid and the item is opened normally. If the two versions do not match, the recipient receives a warning that the digital signature is invalid and the message has been changed.

Using the Digitally Sign toolbar button is the easiest way to sign an outgoing message. However, you can also view your security settings through the Message Options dialog box. From this dialog box, you can customize your security settings for the individual message.

To customize the security settings for a message, click the Options button on the message toolbar to display the Message Options dialog box. Click the Security Settings button to display Figure 25.13.

Figure 25.13
You can change the security settings for your individual message using this dialog box.



Security Properties

☐ Encrypt message contents and attachments
☑ Add digital signature to this message
☑ Send this message as clear text signed
☐ Request S/MIME receipt for this message

Security Settings

Security setting: <Automatic>

Security Label

Policy Module: <None>

Classification:

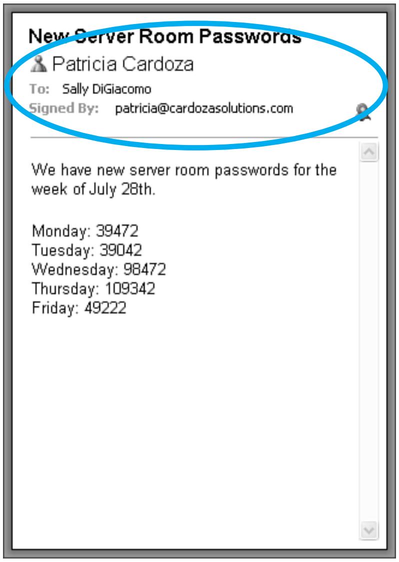
Privacy Mark:

If you've configured Outlook to automatically add a digital signature to all outgoing messages, the Add Digital Signature to This Message box should already be checked. You can choose the default value, Send This Message as Clear Text Signed, if you want recipients who don't have S/MIME security to be able to read your messages. To verify that your digital signature is being validated by recipients and to request confirmation that the message was received unaltered, select the Request S/MIME Receipt for This Message check box. This check box also provides notification telling you who opened the message and when it was opened. If you have multiple certificates installed on your computer, you can use the Security setting drop-down list to choose a specific certificate or you can accept the default automatic setting. This setting uses the values you specified in the Security tab of the Options dialog.

Click OK to save your security settings. Click Close to close the Message Options dialog box and return to your email message. When you send your email message, a digital signature will be attached to the message.

Receiving a Signed Message

Several things happen when you receive a signed message. When you receive the message, the Reading Pane displays an additional line in the message header, as shown in Figure 25.14.



New Server Room Passwords

Patricia Cardoza

To: Sally DiGiacomo

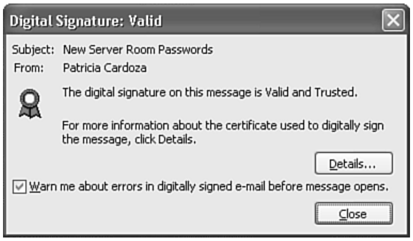
Signed By: patricia@cardozasolutions.com

We have new server room passwords for the week of July 28th.

Monday: 39472
Tuesday: 39042
Wednesday: 98472
Thursday: 109342
Friday: 49222

Figure 25.14
The Reading Pane displays information about who signed the message.

To view a digital signature attached to a message, click the red certificate on the right of the Reading Pane to display Figure 25.15.



Digital Signature: Valid

Subject: New Server Room Passwords

From: Patricia Cardoza

The digital signature on this message is Valid and Trusted.

For more information about the certificate used to digitally sign the message, click Details.

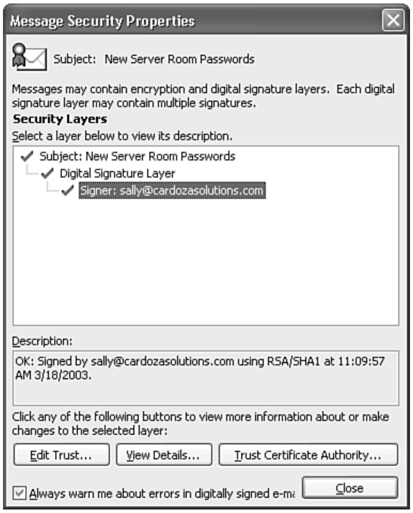
☑ Warn me about errors in digitally signed e-mail before message opens.

Figure 25.15
You can view detailed information about the digital certificate by clicking the certificate icon.

You can view the holder of the digital certificate and the certificate's current status. For more information about the digital certificate, click the Details button to view the Message Security Properties dialog box shown in Figure 25.16.

This dialog box shows extended information about the security layers attached to the message. One message can have multiple signature layers depending on the level of security used to send the message. For each signer, you can view the date and time the message was signed. If you want to edit the level of trust for this certificate, click Edit Trust. You can choose from Inherit Trust from Issuer, Explicitly Trust This Certificate, or Explicitly Don't Trust This Certificate. Use the other tabs in this dialog to view detailed information about the certificate.

Figure 25.16
You can view extended properties of the digital signature from this dialog box.



Subject: New Server Room Passwords

Messages may contain encryption and digital signature layers. Each digital signature layer may contain multiple signatures.

Security Layers

Select a layer below to view its description.

- ✓ Subject: New Server Room Passwords
  - ✓ Digital Signature Layer
    - ✓ Signer: sally@cardozasolutions.com

Description:

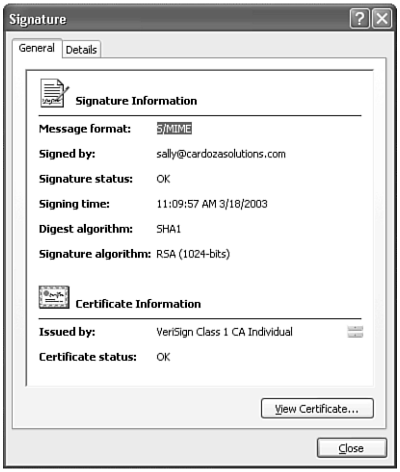
OK: Signed by sally@cardozasolutions.com using RSA/SHA1 at 11:09:57 AM 3/18/2003.

Click any of the following buttons to view more information about or make changes to the selected layer:

☑ Always warn me about errors in digitally signed e-ma

You can also click the View Details button to view additional status information about the digital certificate, as shown in Figure 25.17. You can view the message format, signer, signing time, digest algorithm, signature algorithm, and certificate status.

Figure 25.17
You can view a variety of details about the signer's certificate.



Signature Information

Message format: S/MIME

Signed by: sally@cardozasolutions.com

Signature status: OK

Signing time: 11:09:57 AM 3/18/2003

Digest algorithm: SHA1

Signature algorithm: RSA (1024-bits)

Certificate Information

Issued by: VeriSign Class 1 CA Individual

Certificate status: OK

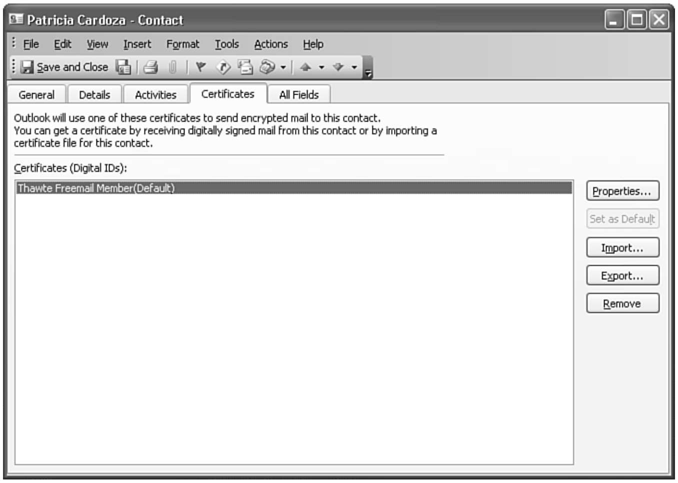
Click Close three times to return to the original email message.

Sending and Receiving Encrypted Messages

Your digital certificate also enables you to send encrypted messages. The difference between sending an encrypted message and sending a signed message is that when sending an encrypted message, the recipient must already have a copy of your public key to be able to decrypt the message. The encryption of the message is based on information stored in the recipient's digital ID. Therefore, encryption can be used to send email only to a recipient who has previously sent you a digitally signed message.

Saving a Sender's Public Key

To exchange encrypted mail with another individual, you must have a copy of that person's public key. The easiest way to obtain a copy of someone's public key is for him to send you an email that's digitally signed. The public key is encoded within the email message. After you receive his message, click the messenger icon next to the sender's name and choose Add to Outlook Contacts. If the sender already exists in your Contacts folder, you can merge the existing data with your new data. This process opens a Contact form with the sender's information displayed. Click on the Certificates tab to display Figure 25.18.



Outlook will use one of these certificates to send encrypted mail to this contact.
You can get a certificate by receiving digitally signed mail from this contact or by importing a certificate file for this contact.

Certificates (Digital IDs):

Thawte Freemail Member(Default)

Figure 25.18
You can view a contact record's certificates in the Contact form.

You'll see the sender's digital certificate listed in the Certificates section of the Contact form. Save and close the contact, and you'll have his certificate available whenever you choose to send him emails.

Sending an Encrypted Email

When you have a copy of a person's public key on your computer, you can use it to send encrypted email to her email. You need her public key because the email is encrypted with the public key and decrypted with the corresponding private key. Because of this, you can be sure that no one other than the intended recipient can ever open your email message.

To encrypt your outgoing message, compose a message as usual. Click the Encrypt Message button on the toolbar to encrypt your email. The Encrypt Message button looks like an envelope with a blue padlock to the right on the icon. Once you click the Encrypt Message button, it will appear depressed. Then just send the email as usual.

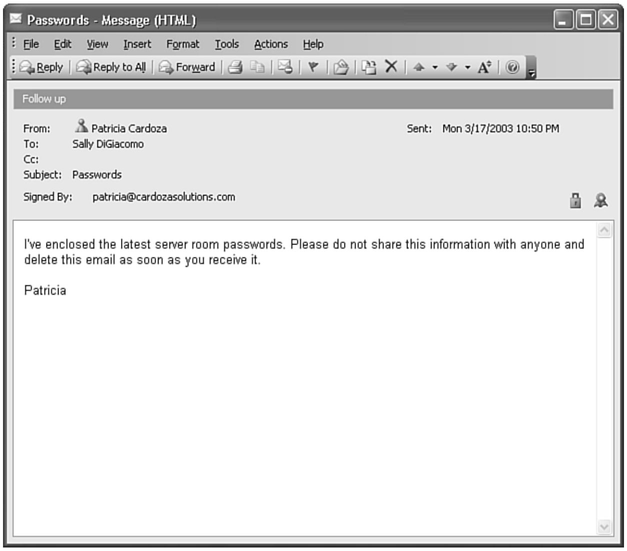
If you encounter an error message while attempting to send an encrypted email, see "Recipient Not Valid for Encrypted Email" in the "Troubleshooting" section at the end of this chapter.

In addition to or instead of clicking the Encrypt Message button on the toolbar, you can click the Options button on the email toolbar to display the Message Options dialog box. Click the Security Settings button and check the box marked Encrypt Message Contents and Attachments. Click OK twice to return to your email message.

Receiving an Encrypted Message

When you receive an encrypted message, you'll notice several things in your Outlook window. First, the message is not visible in the Reading Pane. You can tell the message is encrypted because its icon in your message list has a blue padlock on it. To view the message, you must double-click to open the message. The message will display with both the digital signature icon and the encrypted padlock in the message header, as shown in Figure 25.19.

Figure 25.19
An encrypted and signed message displays both icons in the message header.

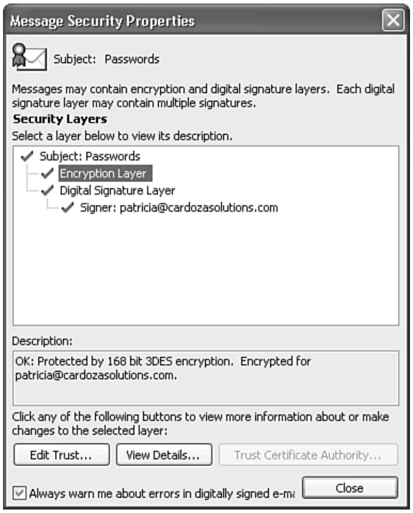


From: Patricia Cardoza
Sent: Mon 3/17/2003 10:50 PM
To: Sally DiGiacomo
Cc:
Subject: Passwords
Signed By: patricia@cardozasolutions.com

I've enclosed the latest server room passwords. Please do not share this information with anyone and delete this email as soon as you receive it.

Patricia

To view information about the encryption, click the blue padlock on the message to display the Message Security Properties dialog box (see Figure 23.20). You'll see an additional security layer for the message. Your message should have both an encryption layer and a digital signature layer. You can click the Encryption Layer line to view information about the encryption.



Message Security Properties

Subject: Passwords

Messages may contain encryption and digital signature layers. Each digital signature layer may contain multiple signatures.

Security Layers

Select a layer below to view its description.

- ✓ Subject: Passwords
  - ✓ Encryption Layer
  - ✓ Digital Signature Layer
    - ✓ Signer: patricia@cardozasolutions.com

Description:

OK: Protected by 168 bit 3DES encryption. Encrypted for patricia@cardozasolutions.com.

Click any of the following buttons to view more information about or make changes to the selected layer:

☑ Always warn me about errors in digitally signed e-ma

Figure 25.20
You can view information about the encryption layer or the digital signature layer.

You can view the type of encryption and the email address of the person who encrypted the message.

Using Security Zones

You can use security zones, an Internet Explorer feature, to view incoming email messages and Web pages that might contain scripts that you want to run on your computer. Although many scripts that come in an email message are useful, some can be very harmful and can contain viruses or otherwise damage your hard drive. You can use security zones to control what happens when you receive an email message that contains a script. You can choose an appropriate security zone for each Web page you access and prevent malicious content from damaging your computer.

There are four security zones, each with its own default security level. The four security zones are

- Local Intranet Zone—This zone is for sites on your local corporate intranet. You likely trust these sites completely. The default security level is set to Medium.
- Trusted Sites Zone—This zone is for sites outside your local intranet that you trust completely. The default security level is Low.
- Internet Zone—This is the zone that most Web sites will use. The default security level for this zone is Medium.
- Restricted Sites Zone—This zone is for sites you don't trust. Its security level is High.

You can manually change the security level for any zone. The different security levels and their effects are listed in Table 25.1.

Table 25.1 Security Level Definitions

Level	Restrictions
High	No potentially damaging content is downloaded or executed on your computer.
Medium	Outlook warns you before running any potentially hazardous content.
Medium-Low	Most content will run without prompts. Unsigned ActiveX controls will not be downloaded.
Low	Outlook accepts all content without warning.

Security zones are usually discussed with respect to Internet Explorer. However, Outlook can render HTML content and even display Web pages as folder home pages. Some of the other content that Outlook can render that might fall under the umbrella of security zones includes

- ActiveX controls
- Downloads
- Java code
- Cookies
- Scripts

Some of this content might be perfectly safe, but if you're not sure, it's best to set your security settings to the most restrictive settings.

In Outlook 2003, all rendered HTML content falls under the Restricted Sites zone. The default security level for this zone is High. That means no potentially damaging content will be downloaded to your computer.

NOTE

A high security level means that you're generally well protected from potentially harmful scripts that attempt to run when you open or view a message. It does not, however, mean that you're completely safe from damaging content. For every security hole that's patched, either in Internet Explorer or Windows, there's a hacker in existence who will try to find another one. If you're planning to use your computer for anything other than playing Solitaire, you should have a good, up-to-date antivirus program installed on your computer.

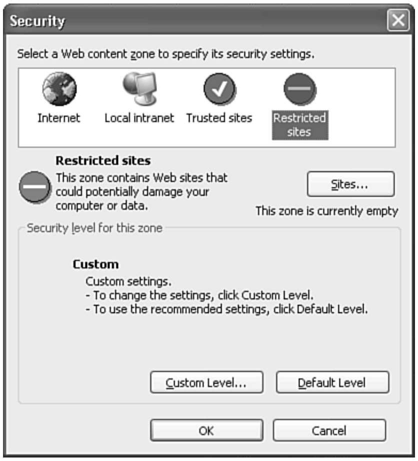
If you have a good antivirus product installed on your computer, you can change the security level for a particular zone or even choose a different security zone for Outlook to use. To change a zone's security level, use the following steps:

1. Select Tools, Options, and click the Security tab.
2. If you want to change the zone Outlook uses, change the Zone drop-down list and choose either Internet zone or the Restricted Sites zone.

CAUTION

> You should really leave Outlook in the Restricted Sites zone. Regardless, you should make sure that you aren't allowing too much potentially dangerous content to run in Outlook and that you have a good antivirus product installed.

3. To change the settings for the selected zone, click the Zone Settings button to display Figure 25.21.



Select a Web content zone to specify its security settings.

Restricted sites
This zone contains Web sites that could potentially damage your computer or data.

This zone is currently empty

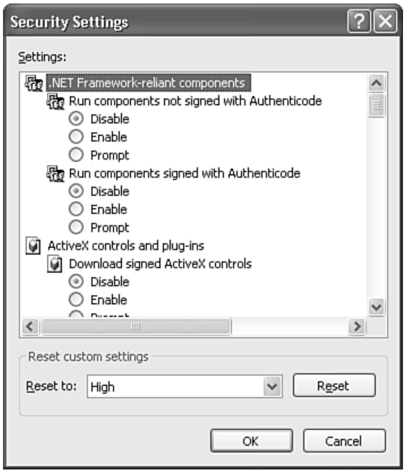
Security level for this zone

Custom
Custom settings.
- To change the settings, click Custom Level.
- To use the recommended settings, click Default Level.

Figure 25.21
You can change the settings for any Web content zone.

4. Click OK to Outlook's warning that you're about to change the way scripts and active content can run.

5. Select the zone you want to edit from the list at the top of the Security dialog box and click Custom Level to display Figure 25.22.



Settings:

.NET Framework-reliant components
Run components not signed with Authenticode
● Disable
○ Enable
○ Prompt
Run components signed with Authenticode
● Disable
○ Enable
○ Prompt
ActiveX controls and plug-ins
Download signed ActiveX controls
● Disable
○ Enable
○ Prompt

Reset custom settings

Reset to: High

Figure 25.22
Use the Security Settings dialog box to choose specific settings for all sorts of potentially dangerous content.

6. For most settings listed in the Security Settings dialog, you can choose Disable, Enable, or Prompt. A few have other options such as High, Medium, and Low, or Disable and Enable. By default, in a high security zone, most of your choices are set to Disable or High. If you need to change any of the selections, it's best to set the option to Prompt rather than enabling the option. Choosing Prompt will at least notify you before a potentially harmful script or ActiveX control is executed on your system.
7. If you want to reset the security zone to a different general security level, choose the level from the Reset To drop-down list and click the Reset button.
8. When you're done editing the security settings, click OK three times to return to Outlook.

Virus Protection

If your computer connects to the outside world in any way, you need to worry about virus protection. If you use email, share disks (even CDs or DVDs burned by others), or browse the Internet, you're vulnerable to a virus attack. Some viruses are relatively innocuous, only copying some files and maybe changing some minor information on your computer, but most viruses are at least somewhat destructive. Some can completely wipe out your computer right after they send a copy of the virus to everyone you've ever corresponded with.

Although Outlook now has significantly higher levels of virus protection than in previous versions, just because you use Outlook with the object model guard and restriction on programmatic sending of email, it doesn't mean you're safe. One of the most rampant viruses of this past year, the Klez virus, used its own SMTP engine. It didn't trigger the security prompts in Outlook at all. In addition, it spoofed addresses so that no one really knew where the original infection started. Klez searched your hard drive and picked two email addresses at random. The first email address would be marked as the From field in the email it sent, and the second address would be inserted in the To field of the email. If anyone you knew was infected with the Klez virus, you probably received emails from other people accusing you of sending them a virus. There's a good chance it wasn't you. It was Klez pretending to be you.

Klez is just one example of the latest group of insidious viruses in the wild today. If you want to protect yourself from viruses, take a few simple precautions:

- Purchase an antivirus program—The best line of defense in the war against viruses is an antivirus program. But it's not good enough to simply install the program; you must make sure that you keep the program current with weekly updates. Most antivirus programs attempt to update their virus definition files once a week, but you can update your virus definitions manually any time you want.
- Be careful with attachments—Despite the advances in virus writing, the majority of viruses are still sent in attached files. If you receive an email from someone you don't know with an attached file, do *not* open that attached file. Instead, send an email to the person asking why he's sending you a file. If he has a legitimate reason for sending you

the attachment, he'll usually be very happy to write back and let you know. Even attached files from people you know can contain viruses. As a general rule, I don't open attached files in an email unless I am expecting them. Even then, I usually save them to disk and manually scan them for viruses before I open the file.

- Look at filenames—A popular trick these days is to send an attached file with two file extensions, such as `joke.jpg.exe`. You might think from the name of the file that it's a harmless image, but really, it's an executable file that can do damage to your computer. If you receive a file with two extensions, always contact the person who sent it to you before opening it.
- Keep up to date on new viruses—Many companies provide detailed information on their Web site or through email when new viruses come out. By signing up for email alerts from one of these companies, you can find out about new viruses right away. Some of the information usually distributed is potential subject lines, potential attached filenames, and detailed information about how to recover from a virus attack.

Even if you follow all these instructions to the letter, it's still possible you could be the victim of a virus attack. As soon as you know you have a virus, disconnect your computer from the Internet. Find another computer you can use, navigate to the Web site of one of the major antivirus companies, and see whether you can find instructions for cleaning the virus off your computer.

Outlook's Built-In Virus Protection

Outlook offers a number of features that help fight against viruses. The first feature you'll probably run into very quickly is the attachment-blocking feature of Outlook.

After the outbreak of the Melissa and I Love You viruses, Microsoft released a patch for Outlook that prevented certain types of attachments from being opened by double-clicking them. This attachment security has been built into Outlook since Outlook 2002 and remains in Outlook 2003.

Outlook classifies attachments into three different levels:

- Level 1—Attachments included in the Level 1 list aren't accessible within Outlook. If you receive a message with a Level 1 attachment, the InfoBar of the message informs you that Outlook has blocked access to a potentially unsafe attachment. The attachment is still stored with the email message, but you cannot access it.
- Level 2—Level 2 attachments cannot be directly opened within an Outlook email message. You must right-click the attachment and save it to disk before you can open it.
- Level 3—Level 3 attachments are unrestricted attachments. You can double-click to open them directly from within Outlook.

➔ For more information about the specific types of attachments blocked in Outlook 2003, **see** "Attachment Security," **p. 471**.

If you're having problems retrieving attachments blocked by Outlook 2003, see "Give Me My Attachments" in the "Troubleshooting" section at the end of this chapter.

Information Rights Management

Outlook 2003 includes one very large new feature: information rights management (IRM). Rights management is a hot topic these days. Ever since the launch of Web sites such as Napster, the recording industry has been very vocal in its support of rights management. The gist of the rights management debate is that if someone wants to restrict access to their own content, they should be able to do so. So, a recording artist can put out a CD and have a reasonable expectation that everyone who wants to play that CD will purchase a copy.

Information rights management is slightly different. It deals with the transfer of confidential or sensitive information between individuals. If you send a private email to your boss informing him of theft of company materials by another employee, you do not want him to forward your email to that employee. You probably don't even want him to print a copy of that email. IRM gives the author control over the content she creates. The author can use IRM to prevent an email from being forwarded, printed, copied, or otherwise distributed.

IRM is present in all Office 2003 applications. For documents and spreadsheets, you can control the access permissions even further. You can allow or disallow users from reading, editing, and printing a document, or even set a document to expire on a certain day and time. When the expiration time passes, the document can no longer be opened by anyone.

IRM works by authenticating the sender as someone who can restrict access to a message or a document. The message is restricted, and then the recipient must authenticate to be able to view the message. For example, if Sally sends a restricted email to `joe@e-mail.com`, Sally must authenticate to a rights management (RM) server to secure the message, and Joe must authenticate to an RM server in order to view the email. That means Joe must be connected to the Internet (or to the Intranet if authenticating to an internal RM server). Joe must then present valid credentials (usually a Passport username and password) to the RM server before he can open the email. If Joe cannot authenticate, or tries to authenticate with invalid credentials, he cannot view the email.

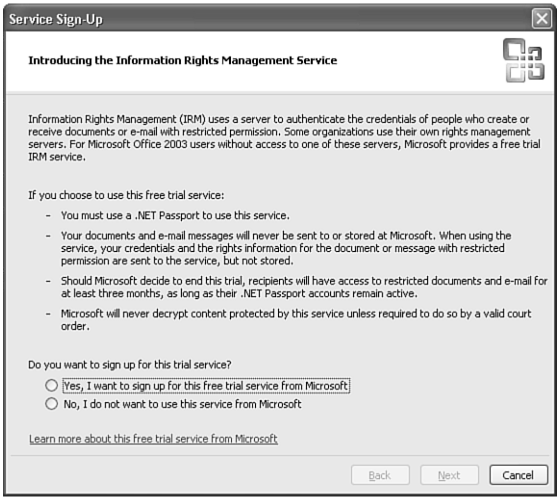
Authentication against a RM server can take two forms. You can use a corporate rights management server or you can use Passport. When Office 2003 is released, Microsoft will also release a server application that enables you to configure a server as a rights management server. You can then authenticate against this server to use IRM. This is probably the most secure way to use IRM. If you leave your current company, you'll no longer be able to authenticate against your corporate RM server and read secured messages.

If your company does not want to invest in a RM server, you can use Microsoft Passport and authenticate against public RM servers Microsoft has set up for this application. The major drawback to using a public RM server is that you must setup a Passport account with the email address you use to read your email. Many people use generic Passport accounts, such as Hotmail accounts, to cut down on spam. To use public RM servers, you must create a new Passport account with the email address you use to read your email. You can, however, choose to opt out of all mailings and not share any of your information with Passport other than your name and email address.

Configure IRM

The first time you use IRM, you must configure it. To configure and use IRM for the first time, use the following steps:

1. Open a new email message.
2. Compose the email as you normally would. Enter a recipient, subject, and message body.
3. Click the Permissions button on the toolbar. The Permissions button is an envelope icon with a red button with a white horizontal line through it.
4. Outlook will inform you that you must download and install the Windows Rights Management client before you can use this feature. Click OK to start the installation process.
5. You can click Open to run the client installation directly from the Web site, or click Save to save the installation file to your hard drive and run it from there.
6. When setup launches, you'll see the Windows Rights Management Client Setup Wizard. Click Next to begin the wizard.
7. Click Next after you've read the privacy statement to display the License Agreement screen. If you want to continue, click I Agree and then click Next.
8. Click Next one last time to begin the installation.
9. When you see the installation confirmation screen, click Close to exit.
10. This returns you to your email message. To continue setup, click the Permissions button on the email message again.
11. You'll now see the Service Signup Screen displayed in Figure 25.23.



Introducing the Information Rights Management Service

Information Rights Management (IRM) uses a server to authenticate the credentials of people who create or receive documents or e-mail with restricted permission. Some organizations use their own rights management servers. For Microsoft Office 2003 users without access to one of these servers, Microsoft provides a free trial IRM service.

If you choose to use this free trial service:

- You must use a .NET Passport to use this service.
- Your documents and e-mail messages will never be sent to or stored at Microsoft. When using the service, your credentials and the rights information for the document or message with restricted permission are sent to the service, but not stored.
- Should Microsoft decide to end this trial, recipients will have access to restricted documents and e-mail for at least three months, as long as their .NET Passport accounts remain active.
- Microsoft will never decrypt content protected by this service unless required to do so by a valid court order.

Do you want to sign up for this trial service?

○ Yes, I want to sign up for this free trial service from Microsoft
○ No, I do not want to use this service from Microsoft

Learn more about this free trial service from Microsoft

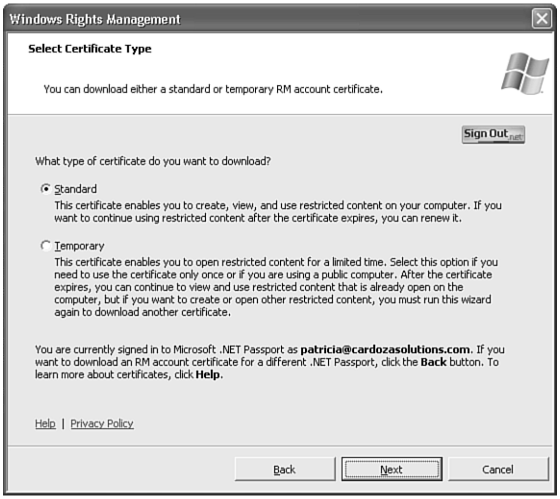
Figure 25.23
After you install the Windows Rights Management Client software, you must register with the service.

12. If you want to use the public RM servers, choose Yes, I want to Sign-Up for This Free Trial Service from Microsoft and click Next.
13. If you already have a .NET Passport for this account, you can click Next through this screen. Otherwise, click No, I Don't Have a .NET Passport and I Want To Get One, and then click Next.
14. If you elected to obtain a .NET Passport, follow the onscreen steps to sign up. Otherwise, continue to step 15.
15. Enter your email address and password when prompted, and click Sign In to display Figure 25.24.

TIP

Although it might be a bit inconvenient, it usually isn't a good idea to choose to have a Passport site sign you in automatically. This can occasionally cause an endless authentication loop.

Figure 25.24
Choose the certificate type you want to install.



Select Certificate Type

You can download either a standard or temporary RM account certificate.

What type of certificate do you want to download?

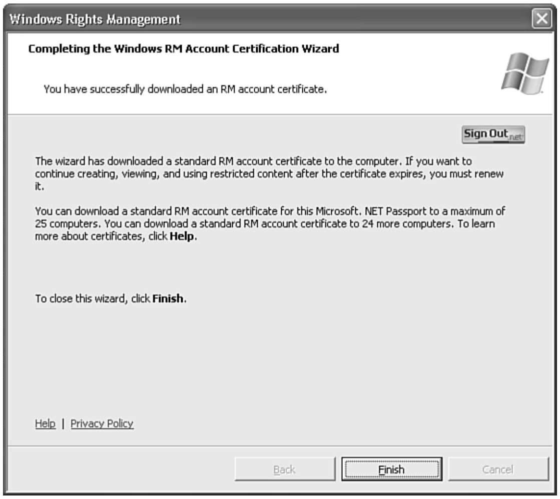
● Standard
This certificate enables you to create, view, and use restricted content on your computer. If you want to continue using restricted content after the certificate expires, you can renew it.

○ Temporary
This certificate enables you to open restricted content for a limited time. Select this option if you need to use the certificate only once or if you are using a public computer. After the certificate expires, you can continue to view and use restricted content that is already open on the computer, but if you want to create or open other restricted content, you must run this wizard again to download another certificate.

You are currently signed in to Microsoft .NET Passport as **patricia@cardozasolutions.com**. If you want to download an RM account certificate for a different .NET Passport, click the **Back** button. To learn more about certificates, click **Help**.

16. If you want to use the certificate repeatedly on this computer, select a standard certificate. If you are using a public computer, you can choose a temporary certificate, which will be valid for only 15 minutes. Click Next.
17. Your certificate will be downloaded and configured on your computer. This process might take several minutes. When it has completed, you'll see the confirmation screen displayed in Figure 25.25. Click Finish to return to your email.

After you complete the initial setup, permissions will be automatically set on your message.



Completing the Windows RM Account Certification Wizard

You have successfully downloaded an RM account certificate.

The wizard has downloaded a standard RM account certificate to the computer. If you want to continue creating, viewing, and using restricted content after the certificate expires, you must renew it.

You can download a standard RM account certificate for this Microsoft. NET Passport to a maximum of 25 computers. You can download a standard RM account certificate to 24 more computers. To learn more about certificates, click **Help**.

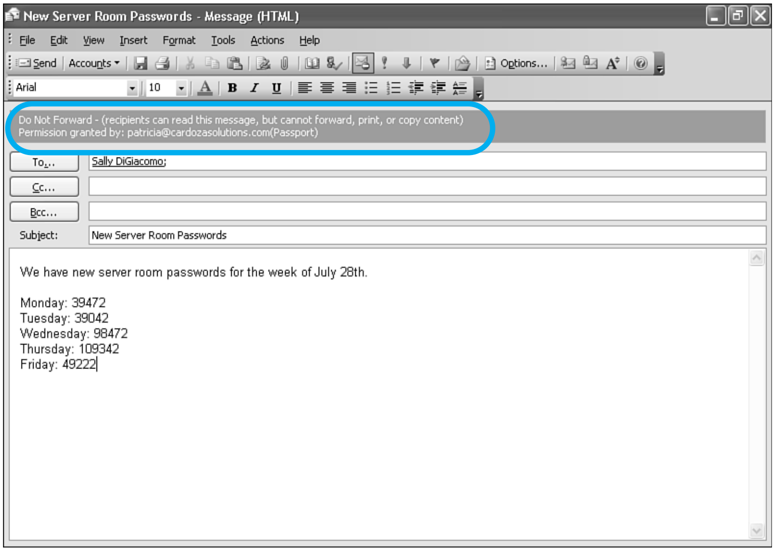
To close this wizard, click **Finish**.

Figure 25.25
The confirmation screen indicates that you've successfully completed setup.

IRM Permissions

In Outlook 2003, IRM is either on or off. You cannot exert the same sort of fine control over an email that you can over a Word document. By restricting access to an email, you're preventing users from forwarding or printing the email. You're also preventing them from editing the email or cutting or copying text. To secure a message using IRM, use the following steps:

1. Compose an email as usual.
2. Click the Permission button on the toolbar.
3. The InfoBar at the top of the message changes as shown in Figure 25.26.
4. Send your email as normal.


New Server Room Passwords - Message (HTML)
File Edit View Insert Format Tools Actions Help
Send Accounts Options...
Arial 10
B I U
To...
Cc...
Bcc...
Subject:

Do Not Forward - (recipients can read this message, but cannot forward, print, or copy content)
Permission granted by: patricia@cardozasolutions.com(Passport)

To...: Sally DiGiacomo;

Subject: New Server Room Passwords

We have new server room passwords for the week of July 28th.

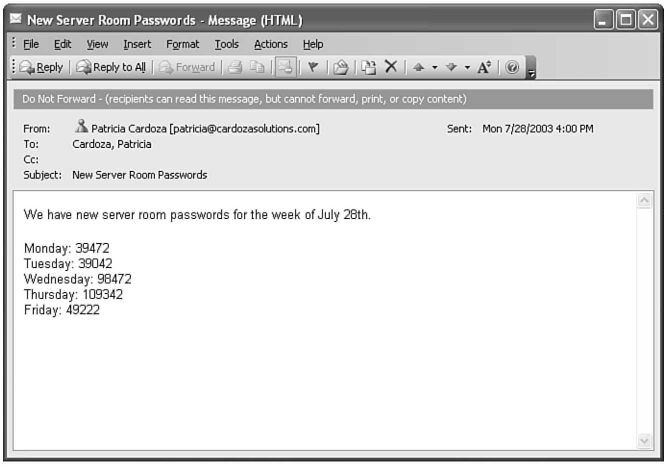
Monday: 39472
Tuesday: 39042
Wednesday: 98472
Thursday: 109342
Friday: 49222

Figure 25.26
The InfoBar indicates that your message will be sent with restricted permissions.

Reading Messages Using IRM

When you receive a message sent with restrictions, it won't be viewable in the Reading Pane. You must open the item to be able to view its contents. The item might take a few minutes to open because it must authenticate to the RM server to verify your identity. If you've received an RM message but haven't yet downloaded and installed the RM client, you'll need to follow the steps previously listed to install the RM client software. When the message opens, it will look similar to Figure 25.27. The Forward button is dimmed, as are the Print button and the Copy button. You cannot forward the message to another user or edit the message for any reason. The Permissions button on the toolbar is selected, but it's also dimmed, so you cannot turn permissions off. If you select the Edit menu, you'll find that the Edit Message option is also dimmed and unavailable. If you try to use Alt+Prt Scrn to make a copy of the message, you won't be able to do so.

Figure 25.27
A message with IRM properties cannot be forwarded, printed, or copied.


New Server Room Passwords - Message (HTML)
File Edit View Insert Format Tools Actions Help
Reply
Reply to All
Forward

Do Not Forward - (recipients can read this message, but cannot forward, print, or copy content)

From: Patricia Cardoza [patricia@cardozasolutions.com]
Sent: Mon 7/28/2003 4:00 PM
To: Cardoza, Patricia
Cc:
Subject: New Server Room Passwords

We have new server room passwords for the week of July 28th.

Monday: 39472
Tuesday: 39042
Wednesday: 98472
Thursday: 109342
Friday: 49222

IRM Limitations

As with any security feature, there are limitations to IRM. For example, you cannot stop someone from using a screen capture program to copy the image of the email. You also can't stop someone from taking a digital picture of the screen and distributing the content that way. You definitely can't stop a recipient from picking up the phone and telling someone else what that content is. IRM only makes it significantly more difficult to distribute private or restricted content.

Even though IRM uses Passport authentication to verify your identity, you can actually use it offline. You must have previously installed the client software and obtained an end user license (EUL). As long as you meet those conditions, you can access content offline or online. Outlook will synchronize the licensing information automatically so that the license is available offline.

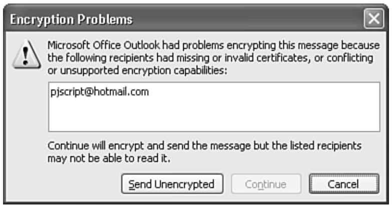
If you're running against a corporate RM server, you can configure additional levels of restrictions. You can prevent reply to a message, prevent reply to all, and enable any of the blocked features such as copying and pasting. If you use Passport authentication against a public RM server, you're limited to one level of restriction on email messages.

IRM isn't designed to completely prevent the spread of unauthorized information. It is, however, designed to make the dissemination of that information extremely difficult.

Troubleshooting

Recipient Not Valid for Encrypted Email

When I try to send an encrypted email to a business colleague I receive the error message shown in Figure 25.28. Why can't I send this person encrypted email?



Microsoft Office Outlook had problems encrypting this message because the following recipients had missing or invalid certificates, or conflicting or unsupported encryption capabilities:

pjscript@hotmail.com

Continue will encrypt and send the message but the listed recipients may not be able to read it.

Figure 25.28
This error is displayed when attempting to send an encrypted email.

This message appears whenever you attempt to send an encrypted email without having a copy of the recipient's public key available and attached to the recipient's contact record. To send an encrypted email, you must have the person in your Contact list and have his public key attached to the Contact record. To obtain a copy of the recipient's public key, have him send you a digitally signed email. You can then click the messenger icon next to his name and choose Add to Contacts. Doing so will add a contact record for him and attach his public key to the contact record.

The reason you need a copy of the recipient's public key is that sending an encrypted message uses his public key to encrypt the message. The recipient can then use his private key to decrypt the message.

Give Me My Attachments

A coworker sent me an Access database that I need to open. But Outlook tells me it blocked access to the unsafe attachment. I know the database is safe; it's from my coworker sitting ten feet from my desk. How can I access this attachment?

If you receive a message with a blocked attachment, you should always check to see what the attachment is before you attempt to retrieve it. Just because it comes from someone you know doesn't mean it's necessarily safe. However, if you know the attachment is safe, you have a few options:

- Have the person zip the attachment and resend it. This is by far the easiest option. Zip files are not restricted by Outlook 2003.
- Edit the Windows Registry to change certain attachment types from Level 1 to Level 2.
- Download the Attachment Options COM add-in to expose a property page within Outlook that edits this Registry key for you. The add-in can be found at `www.slovaktech.com`.
- Export the message to Outlook Express. Outlook Express enables you to turn attachment blocking on or off for the entire program, so you can turn the blocking off, access your file, and then turn the blocking back on.

Be aware that choosing option 2 or 3 puts you at a higher risk for virus attack. However, sometimes you just need to get that attachment.

Improving Your Outlook

This chapter covered a wide variety of security related topics. You learned about digital certificates, signing and encrypting emails, security zones, attachment security, and information rights management. You can use all of these features to make the most of your Outlook 2003 installation. This section shows you how to implement some of the features discussed in this chapter.

When you install Outlook 2003, you can customize some of the features discussed here right away. That way, when you're ready to use them, they'll already be configured for you.

If you think you'll need to send signed or encrypted mail, consider signing up for a digital certificate. You can get a free digital certificate from Thawte or pay $14.95 a year for a certificate from VeriSign. So, which should you choose? Only you can decide. The Thawte certificate is free. The VeriSign certificate has a few advantages, such as the public search feature on the VeriSign Web site. Whatever you choose, you can install your certificate in Outlook and use it to send signed and encrypted mail.

Even though digital certificates are easy to install and configure, that doesn't mean you should sign and encrypt all your email messages. Signing an email message can add to the email's size. In the case of short emails, it can even double their size. With the popularity of cellular phones and Pocket PC Phone devices, you'll probably have a number of recipients who cannot access signed email. For example, a signed email cannot be read as an SMS message on a mobile device.

Attachment security is a hot topic today. Many users install more recent versions of Outlook over older versions that did not have attachment security. If you have attachments stored in a Personal Folders file that you need to access after installing Outlook 2003, you have a couple of options. You can export those messages to Outlook Express, or you can edit the Registry to gain access to those attachments. To edit the Registry, use the following steps:

1. Close Outlook.
2. Launch the Registry Editor by typing **`regedit`** at the Windows Run command (Start, Run) and click OK.
3. Navigate to the following key: `\HKEY_CURRENT_User\Software\Microsoft\Office\11.0\Outlook\Security`.
4. If you haven't previously configured the `Level1Remove` Registry key, you'll have to add a new string value to the key referenced in step 3.
5. After you add the string value, double-click the value to bring up the Edit String dialog box.
6. Enter the list of attachment extensions separated by semicolons. So, to unblock Access databases and batch files, enter **`mdb;bat`**. You don't need to enter the leading period in the extension.
7. Exit the Registry Editor and restart Outlook. You should now be able to view Access databases and batch files attached to email messages.

Information rights management is one of those features that you'll probably have to investigate a little before you decide how to implement it. Some industries will use it heavily, whereas others will probably never bother. Some industries that will probably use IRM heavily include legal firms and any firms that need to exchange sensitive personal information.

I believe that more corporations will utilize IRM internally than externally. When used internally with a rights management server, you can ensure that only authorized users can open secured emails. If a member of your organization leaves the company, all you have to do is revoke her access to the rights management server to prevent her from opening any saved emails. Even if she archives their emails to a Personal Folders file and takes them on a CD when she leaves, she'll be unable to open the emails.

Security is a very serious issue for any company. Be sure to thoroughly investigate all the security features that Outlook 2003 has available.