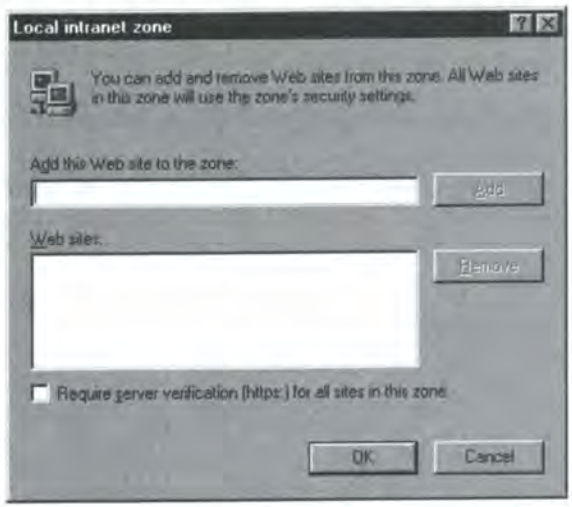
Option	Description
Include all local (intranet) sites not listed in other zones	Includes all sites not included in other zones. Intranet sites have names that do not include periods inside the URL (for example, http://local/). A site name such as http://www.microsoft.com/ is not local, because it contains periods. This site would be assigned to the Internet zone. The intranet site name rule applies to file: as well as http: URLs.
Include all sites that bypass the proxy server	Includes all sites that bypass the proxy server. Typical intranet configurations use a proxy server to access the Internet with a direct connection to intranet servers. This setting uses this kind of configuration information to distinguish intranet from Internet content for purposes of zones. If the proxy server is otherwise configured, this option should be cleared and other options should be used to designate intranet zone membership. In systems without a proxy server, this setting has no effect.
Include all network paths (UNCs)	Includes all network Universal Naming Convention (UNC) paths. Network paths (for example, \\local\file.txt) are typically used for local network content that should be included in the Local Intranet zone. If some network paths should not be in the Local Intranet zone, this option should be cleared, and other options should be used to designate membership. For example, in certain Common Internet File System (CIFS) configurations, a network path can reference Internet content.

3. Click **Advanced**.
4. In the **Local intranet zone** dialog box, enter the addresses of sites to include in this zone, and click **Add** after each site address you enter.



5. If you want to require all sites in this zone to use Hypertext Transfer Protocol Secure (HTTPS) server verification, select **Require server verification (https:) for all sites in this zone**.
6. Click **OK**.

Note If some parts of your intranet are less secure or otherwise not trustworthy, they can be excluded from this zone by assigning them to the Restricted Sites zone.

Once you have checked that the Local Intranet zone is secure, you may want to change the zone's security level to Low to allow a wider range of operations and make the Web pages more functional. You can also adjust individual security settings in the **Custom Settings** dialog box, which is explained in more detail later in this chapter.

Restricted and Trusted Sites Zones

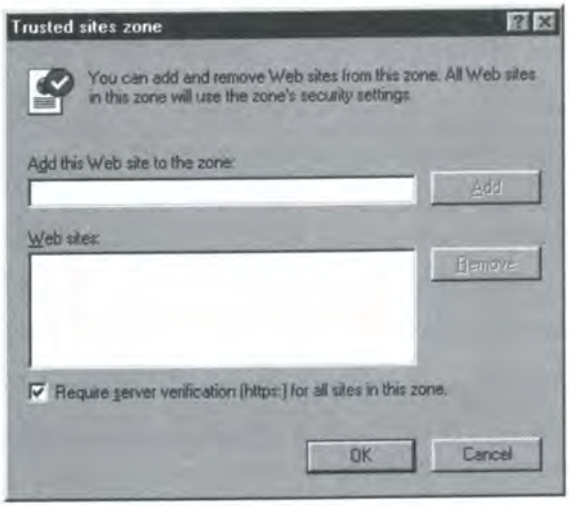
The Restricted Sites and Trusted Sites zones are where you can assign specific Web sites that you trust more or less than those in the Internet zone or the Local Intranet zone.

The Trusted Sites zone is assigned a Low security level setting by default. It is intended for highly trusted sites, such as companies with which you frequently do business, and is sometimes known as an *extranet.* If you assign a site to the Trusted Sites zone, the site will be allowed to perform more powerful operations. Also, Internet Explorer will require the user to make fewer security decisions. Add a site to this zone only if you trust all of its content never to do anything harmful to the user's computer. For the Trusted Sites zone, it is strongly recommended that you use the HTTPS protocol or otherwise ensure that connections to the site are secure.

The Restricted Sites zone is assigned a High security level setting by default. This zone is designed for the rare case of a site you don't trust. If you assign a site to the Restricted Sites zone, the site will be allowed to perform only minimal, very safe operations. Due to the performance restrictions necessary for this extremely high level of security, some Web pages in this zone may not function properly.

▶ **To add sites to the Restricted Sites zone or Trusted Sites zone**

1. On the **Security** tab, in the **Zone** drop-down list, select **Restricted sites zone** or **Trusted sites zone**.
2. Click **Add Sites**.
3. In the **Trusted sites zone** dialog box, type the addresses of sites to include in this zone, and click **Add** after each site address you enter.



Note The **Trusted sites zone** dialog box is shown here, but the **Restricted sites zone** dialog box is identical, except for the title.

Note For the Restricted Sites zone, it is strongly recommended that you use the HTTPS protocol.

4. Click **OK**.

Changing Security Levels

If you choose not to accept the default security levels for the preset zones in Internet Explorer 4, you can easily assign a different level of security—High, Medium, or Low—to any zone.

▶ **To change security levels for a zone**

1. On the **Security** tab, in the **Zone** drop-down list, select a security zone.
2. Select a security level.

Security Level	Description
High (most secure)	Excludes content that could damage users' computers.
Medium (more secure)	Warns users and queries whether they want to run potentially damaging content.
Low	Runs potentially damaging content without notifying users.
Custom (for expert users)	Specifies custom settings for zones.

Note If you want to customize the security level for a zone, select **Custom (for expert users)**, and choose settings that suit your needs. For more information, see the next section.

3. Click **OK**.

Customizing Security Zones

The **Custom** option on the **Security** tab gives advanced users and system administrators additional control over security settings. Again, the options for customizing security zones are the same whether you access them from Internet Explorer 4, the IEAK Configuration Wizard, or the IEAK Profile Manager (with the exception of some Java controls, which will be explained later in this chapter).

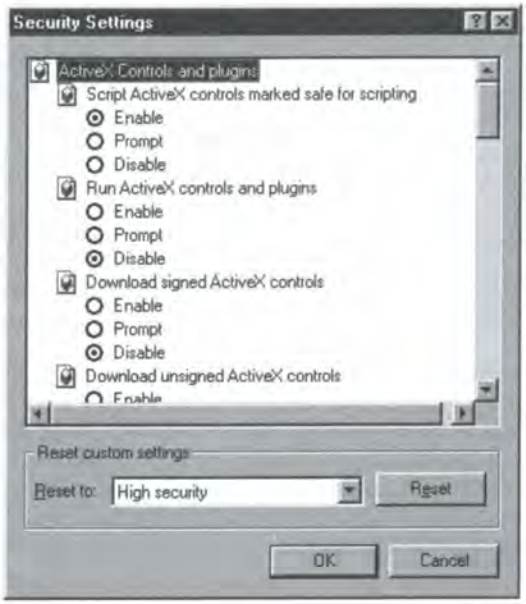
Configuring Custom Settings

The custom security options for Internet Explorer are grouped into the following categories:

- ActiveX Controls and Plug-ins
- Java
- Scripting
- Miscellaneous

▶ **To customize security options**

1. On the **View** menu, click **Internet Options**.
2. Click the **Security** tab.
3. Select a security zone from the **Zone** drop-down list.
4. Select **Custom**, click **Settings**, and then select the options you want.



5. Click **OK**.

The following sections describe the security options for each security category.

ActiveX Controls and Plug-ins

These options dictate how ActiveX controls and plug-ins are downloaded, run, and scripted.

Note If an ActiveX control is downloaded from a site different from the page on which it is used, the more restrictive of the two sites' zone settings will be applied. For example, if a user is accessing a Web page within a zone that is set to enable a download, but the code is downloaded from another zone that is set to prompt a user first, the prompt setting is used.

Script ActiveX controls marked safe for scripting

This option determines whether an ActiveX control marked safe for scripting can interact with a script. The settings for this option are:

- **Enable**, to allow script interaction without user intervention.
- **Prompt**, to query users to choose whether to allow script interaction.
- **Disable**, to prevent script interaction.

Note that safe-for-initialization controls loaded with PARAM tags are unaffected by this option. This option is ignored when **Initialize and script ActiveX controls that are not marked safe** is set to **Enable**, because the setting bypasses all object safety. You cannot script unsafe controls while blocking the scripting of the safe ones.

Run ActiveX controls and plugins

This option determines whether ActiveX controls and plug-ins can be run on pages from the specified zone. The settings for this option are:

- **Enable**, to run controls and plug-ins without user intervention.
- **Prompt**, to query users to choose whether to allow the controls or plug-in to run.
- **Disable**, to prevent controls and plug-ins from running.

Download signed ActiveX controls

This option determines whether users may download signed ActiveX controls from a page in the zone. (For more information about digital signatures, see Chapter 28, "Digital Certificates.") The settings for this option are:

- **Enable**, to download signed controls without user intervention.
- **Prompt**, to query the user whether to download controls signed by publishers who aren't trusted, but still silently download code signed by trusted publishers. (For more information about trusted publishers, see Chapter 29, "Trust-Based Security for Java.")
- **Disable**, to prevent signed controls from downloading.

Download unsigned ActiveX controls

This option determines whether users may download unsigned ActiveX controls from the zone. Such code is potentially harmful, especially when coming from an untrusted zone. The settings for this option are:

- **Enable**, to run unsigned controls without user intervention.
- **Prompt**, to query users to choose whether to allow the unsigned control to run.
- **Disable**, to prevent unsigned controls from running.

Initialize and script ActiveX controls not marked as safe

This option determines whether ActiveX control object safety is enforced for pages in the zone. Object safety should be enforced unless all ActiveX controls and scripts that might interact with pages in the zone can be trusted. The settings for this option are:

- **Enable**, to override object safety. ActiveX controls are run, loaded with parameters, and scripted without setting object safety for untrusted data or scripts. This setting is not recommended, except for secure and administered zones. This setting causes both unsafe and safe controls to be initialized and scripted, ignoring the **Script ActiveX controls marked safe for scripting** option.
- **Prompt**, to attempt to enforce object safety. However, if the ActiveX control cannot be made safe for untrusted data or scripts, then the user is queried whether to allow the control to be loaded with parameters or scripted.
- **Disable**, to enforce object safety for untrusted data or scripts. ActiveX controls that cannot be made safe are not loaded with parameters or scripted.

Java

These options control the permissions that are granted to Java applets when they are downloaded and run in this zone. You can specify:

- The maximum permission level granted to signed applets downloaded from the zone.
- The permissions granted to unsigned applets downloaded from the zone.
- The permissions granted to scripts on pages in the zone that call into applets.

Note If a Java applet is downloaded from a different site than the page on which it is used, the more restrictive of the two sites' zone settings will be applied. For example, if a user is accessing a Web page within a zone that is set to allow a download, but the code is downloaded from another zone that is set to prompt a user first, then the prompt setting is used.

Java permissions

The settings for this option are:

- **Custom**, to control permissions settings individually. To view and change custom Java permissions for each security zone, use the Internet Explorer **Custom Java Security** dialog box. For more information, see "Configuring Custom Java Security" in Chapter 29, "Trust-Based Security for Java." You can also use the IEAK Configuration Wizard and Profile Manager to edit the advanced Java permissions for each security zone. For more information, see Customizing Java Permissions for User Groups" in Chapter 29.
- **Low Safety**, to enable applets to perform all operations.

- **Medium Safety**, to enable applets to run in their *sandbox* (an area in memory outside of which the program cannot make calls), plus capabilities like *scratch space* (a safe and secure storage area on the client computer) and user-controlled file I/O.
- **High Safety**, to enable applets to run in their sandbox.
- **Disable Java**, to prevent any applets from running.

Scripting

These options specify how scripts are handled by Internet Explorer.

Active scripting

This option determines whether script code on pages in the zone is run. The settings for this option are:

- **Enable**, to run scripts without user intervention.
- **Prompt**, to query users to choose whether to allow the scripts to run.
- **Disable**, to prevent scripts from running.

Scripting of Java applets

This option determines whether applets are exposed to scripts within the zone. The settings for this option are:

- **Enable**, to allow scripts to access applets without user intervention.
- **Prompt**, to query users to choose whether to allow scripts to access applets.
- **Disable**, to prevent scripts from accessing applets.

Downloads

These options specify how downloads are handled by Internet Explorer.

File download

This option controls whether file downloads are permitted from the zone. Note that this option is determined by the zone of the page with the link causing the download, not the zone from which the file is delivered. The settings for this option are:

- **Enable**, to allow files to be downloaded from the zone.
- **Disable**, to prevent files from being downloaded from the zone.

Font download

This option determines whether pages of the zone may download HTML fonts. The settings for this option are:

- **Enable**, to download HTML fonts without user intervention.
- **Prompt**, to query users to choose whether to allow HTML fonts to download.
- **Disable**, to prevent HTML fonts from downloading.

User Authentication

This option controls how HTTP user authentication is handled.

Logon

The settings for this option are:

- **Anonymous logon**, to disable HTTP authentication and use the guest account only for CIFS.
- **Prompt for user name and password**, to query users for user IDs and passwords. After a user is queried, these values can be used silently for the remainder of the session.
- **Automatic logon only in Intranet zone**, to query users for user IDs and passwords in other zones. After a user is queried, these values can be used silently for the remainder of the session.
- **Automatic logon with current user name and password**, to attempt logon using Windows NT® Challenge Response (also known as NTLM authentication). If Windows NT Challenge Response is supported by the server, the logon uses the user's network user name and password for logon. If Windows NT Challenge Response is not supported by the server, the user is queried to provide the user name and password.

Miscellaneous

These options control whether users can submit nonencrypted form data, launch applications and files from IFRAMEs, install Active Desktop items, drag files, or copy and paste files from this zone.

Submit non-encrypted form data

This option determines whether data on HTML forms on pages in the zone may be submitted. Forms sent with SSL (Secure Sockets Layer) encryption are always allowed; this setting only affects non-SSL form data submission. The settings for this option are:

- **Enable**, to allow information using HTML forms on pages in this zone to be submitted without user intervention.
- **Prompt**, to query users to choose whether to allow information using HTML forms on pages in this zone to be submitted.
- **Disable**, to prevent information using HTML forms on pages in this zone from being submitted.

Launching applications and files from an IFRAME

This option controls whether applications may be run and files may be downloaded from an IFRAME reference in the HTML of the pages in this zone. The settings for this option are:

- **Enable**, to run applications and download files from IFRAMEs on the pages in this zone without user intervention.
- **Prompt**, to query users to choose whether to run applications and download files from IFRAMEs on the pages in this zone.
- **Disable**, to prevent applications from running and files from downloading from IFRAMEs on the pages in this zone.

Installation of desktop items

This option controls whether users can install Active Desktop items from this zone. The settings for this option are:

- **Enable**, to install desktop items from this zone without user intervention.
- **Prompt**, to query users to choose whether to install desktop items from this zone.
- **Disable,** to prevent desktop items from this zone from being installed.

Drag and drop or copy and paste files

This option controls whether users can drag files or copy and paste files from a source within the zone. The settings for this option are:

- **Enable**, to drag files or copy and paste files from this zone without user intervention.
- **Prompt**, to query users to choose whether to drag or copy files from this zone.
- **Disable**, to prevent dragging files or copying and pasting files from this zone.

Software channel permissions

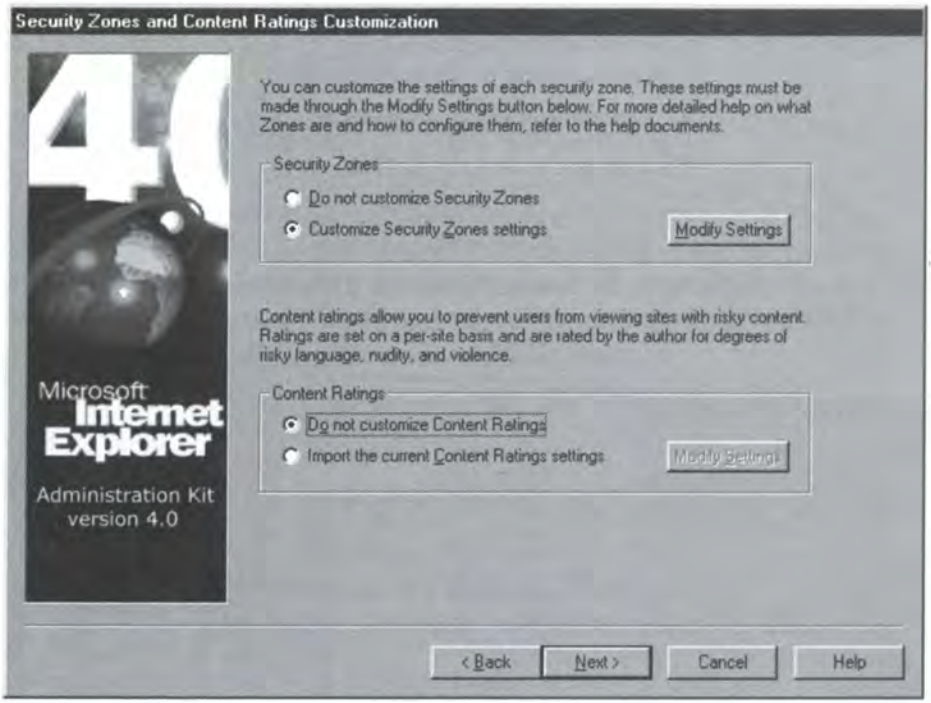
This option controls the permissions given to software distribution channels. The settings for this option are:

- **Low safety**, to allow users to be notified of software updates by e-mail, software packages to be automatically downloaded to users' computers, and software packages to be automatically installed on users' computers.
- **Medium safety**, to allow users to be notified of software updates by e-mail and software packages to be automatically downloaded to (but not installed on) users' computers.
- **High safety**, to prevent users from being notified of software updates by e-mail, software packages from being automatically downloaded to users' computers, and software packages from being automatically installed on users' computers.

Deploying Security Zones in User Groups

System administrators can use the IEAK Configuration Wizard to deploy and lock down security zone settings in their organizations. Using the IEAK, you can also build custom packages with specific security settings for different user groups. (For more information, see "Building Custom Packages" in Chapter 36.) Once custom settings have been deployed, you can use the IEAK Profile Manager to update those settings.

To specify security settings using the IEAK Configuration Wizard, use the **Security Zones and Content Ratings Customization** page. You can either accept the default security settings or customize the settings to meet your needs.



▶ **To customize security settings with the IEAK Configuration Wizard**

1. Select **Customize Security Zones settings**.
2. Click **Modify Settings**.
3. Use the **Security** dialog box and the **Security Settings** dialog box to customize the security settings for each security zone.

The dialog boxes for designating the sites included in security zones, changing security levels, and customizing security options are the same as the dialog boxes presented in Internet Explorer, described in the "Setting Up Security Zones" section earlier in this chapter.

Locking Down Security Options

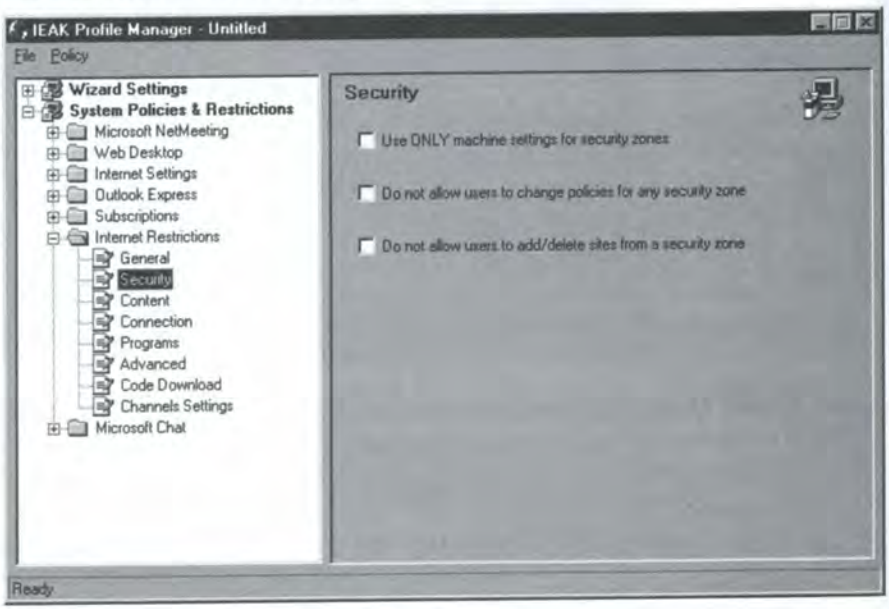
Once you've built your custom security packages, you can also use the IEAK Configuration Wizard to lock down security options and restrict users from changing security configurations. After browsers are deployed, you can use the IEAK Profile Manager to lock down security options for user groups that have the automatic browser configuration implemented. (For more information, see Chapter 37, "Automatic Browser Configuration.") Again, the dialog boxes look the same in both the Configuration Wizard and the Profile Manager.

Using the IEAK, you can specify one or more of the following lock-down options:

- Lock down all security settings so users cannot change them. Security settings can be changed using automatic browser configuration, if implemented.
- Prevent users from changing settings for security zones. Users can still add sites to or remove sites from zones.
- Prevent users from adding sites to or removing sites from zones.

▶ **To lock down security options**

1. In the IEAK Wizard or the IEAK Profile Manager, navigate to the **System Policies & Restrictions** page.
2. In the **System Policies & Restrictions** hierarchy, select **Internet Restrictions**, and then select the **Security** object.



Note The IEAK Profile Manager is shown here, but the **System Policies & Restrictions** page of the IEAK Configuration Wizard works similarly.

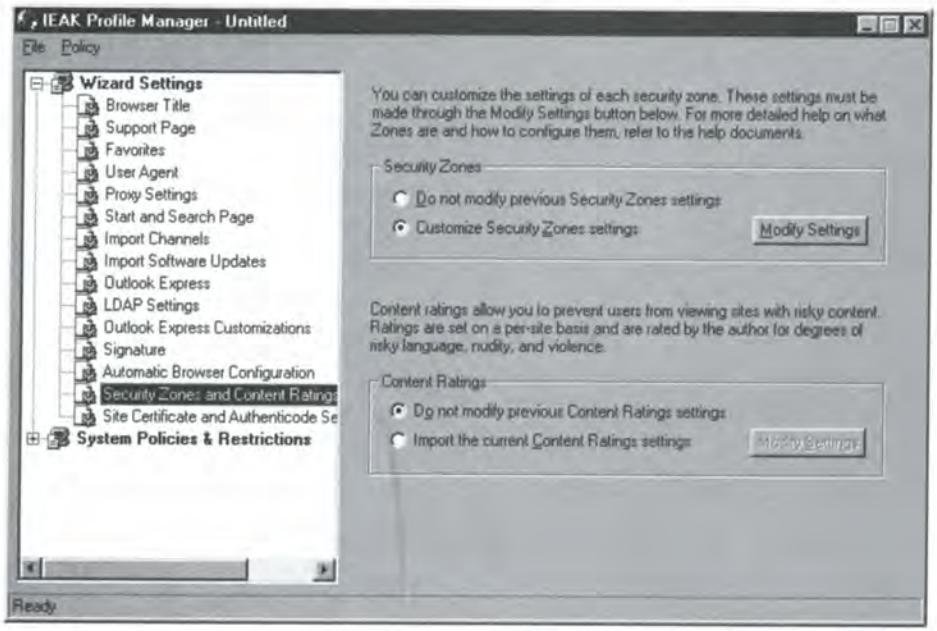
3. In the right pane, select the options you want.

Option	Description
Use ONLY machine settings for security zones	Locks down all security settings. End users cannot change security settings specified for the zones. Settings can be changed using auto-configuration files and automatic browser configuration.
Do not allow users to change policies for any security zone	Prevents users from changing security settings for security zones.
Do not allow users to add/delete sites from security zone	Prevents users from adding sites to or deleting sites from security zones.

4. Save your changes to the auto-configuration (.ins) file or finish building the custom package, as appropriate.

Managing Security Settings for Deployed Browsers

To manage security settings for deployed browsers, you can use the IEAK Profile Manger in conjunction with automatic browser configuration. (For more information, see Chapter 37, "Automatic Browser Configuration.") You can update your security settings by opening the auto-configuration (.ins) file in the IEAK Profile Manager and selecting the **Security Zones and Content Ratings** object in the Wizard Settings hierarchy on the left pane.



▶ **To customize security zones with the IEAK Profile Manager**

1. Select **Customize Security Zones settings**.
2. Click **Modify Settings**.
3. Use the **Security** dialog box and the **Security Settings** dialog box to customize the security settings for each security zone.

   The dialog boxes for designating the sites included in security zones, changing security levels, and customizing security options are the same as the dialog boxes presented in Internet Explorer, described in the "Setting Up Security Zones" section earlier in this chapter.
4. On the **File** menu, click **Save** to save changes to the auto-configuration (.ins) file.

   Changes are made to users' configurations as scheduled by automatic browser configuration.

You can also lock down security zone updates so users cannot modify the zone settings. For more information, see "Locking Down Security Options" earlier in this chapter.

CHAPTER 28

Digital Certificates

In this chapter

Digital Certificates Overview 468
Understanding Commercial Certificate Authorities 469
Understanding Certificate Servers 471
Understanding Authenticode 471
Authenticode 2.0 473
Features 473
After Authenticode 1.0 Expiration 473
Upgrading to Authenticode 2.0 474
Using Secure Client/Server Communications 474
Secure Channels 474
Server Gated Cryptography 475
CryptoAPI 2.0 477
Secure Networks 477
Socks Firewall Support 477
Windows NT Server Challenge Response 477
Configuring Certificates 478
Root Certificate Authorities 479
Client Certificates 480
Trusted Publishers and Certificate Authorities 481
Deploying Customized Certificates in User Groups 483
Locking Down Certificates 485
Managing Certificates for Deployed Browsers 486

Digital Certificates Overview

Digital certificates are electronic credentials that verify an individual's or an organization's identity on the Web. The identity of the digital certificate owner is bound to a pair of electronic keys that can be used to encrypt and sign digital information, assuring that the keys actually belong to the person or organization specified. (For more background information about digital signatures and certificates, see "Overview: Understanding Trust Management" at the beginning of Part 7.)

Digital certificates contain at least the following information:

- Owner's public key
- Owner's name or alias
- Expiration date of the digital certificate
- Serial number of the digital certificate
- Name of the certification authority that issued the digital certificate
- Digital signature of the certification authority that issued the digital certificate

Digital certificates may also contain other user-supplied information, including:

- Postal address
- E-mail address
- Basic registration information (country, postal code, age, and gender)

Digital certificates are authenticated, issued, and managed by a trusted third party called a Certificate Authority (CA). The CA must provide a combination of three essential elements: technology, such as security protocols and standards, secure messaging, and cryptography; infrastructure, including secure facilities, customer support, and redundant systems; and practices, including a defined model of trust and a legally binding framework for subscriber activities and disputes. In short, a CA must be a trusted online service operating 24 hours a day, 7 days a week, on a global basis. In addition to obtaining digital certificates from commercial CAs, you can also implement certificate servers such as Microsoft Certificate Server to provide certificate services for your Web infrastructure. Digital certificates form the basis for secure communication and client and server authentication on the Web. Digital certificates can be used to:

- Encrypt secure communication channels between client machines and the servers on the Web.
- Verify the identity (user authentication) of clients and servers for secure communication channels between clients and servers on the Web.
- Encrypt messages for secure Internet e-mail communications.

- Verify the authorship of Internet e-mail messages.
- Sign executable code to be downloaded on the Web.
- Verify the source and integrity of signed executable code downloaded from the Web.

You can install certificates and configure certificate settings for Internet Explorer to control secure e-mail communications, the downloading of active content, and user authentication for clients and servers. System administrators can use the Internet Explorer Administration Kit (IEAK) Configuration Wizard to specify certificate configurations for the custom packages of Internet Explorer they deploy in user groups. The IEAK Profile Manager can be used to manage certificate configurations for user groups through the automatic browser configuration feature of Internet Explorer.

Understanding Commercial Certificate Authorities

Commercial CAs issue digital certificates verifying the electronic identity of individuals and organizations on the Web. The CAs' primary responsibility is to confirm the identity of those seeking a digital certificate, thus ensuring the validity of the identification information contained in the digital certificate.

CAs do the following types of services:

- Provide, manage, and renew digital certificates.
- Authenticate the identities of individuals and organizations.
- Verify the registrations of individuals and organizations.
- Publish and maintain a Certificate Revocation List (CRL) of all digital certificates that have been revoked by the CA.
- Handle legal and liability issues for broken security.

Many commercial CAs offer certificate services for Microsoft products, as well as a wide range of other certificate services. For a current list of CAs who support Microsoft products, visit **http://www.microsoft.com/security/**.

Commercial CAs issue various types of digital certificates, such as:

- Personal certificates for individuals to digitally sign communications and assure secure transactions over the Internet and intranet.
- Client and server certificates for managing secure transactions between clients and servers.
- Software publisher certificates for individuals who digitally sign their software.
- Software publisher certificates for commercial software publishers who digitally sign their software.

CAs can also issue many other types of certificates. Each CA operates within the aegis of its Certification Practices Statement (CPS). It's a good idea to visit the CA's Web site and read the CPS to understand the certificates issued and the CA's operating procedures.

You should consider the following issues when choosing a Certificate Authority:

- Is the Certificate Authority a trusted entity operating a certification practice that can both meet your needs and operate efficiently in your region? Others should immediately recognize your Certificate Authority as a reputable, trustworthy organization. If you choose an authority with a questionable reputation, you run the risk of having users reject your server certificate.
- Is the Certificate Authority familiar with your organization's business interests? Look for a Certificate Authority from whom you can leverage technical, legal, and business expertise.
- What type of information will the authority require from you in order to verify your identity? Most Certificate Authorities will require detailed information, such as your identity, your organization's identity, and your official authority to administer the Web server for which you are requesting a certificate. Depending on the level of identification assurance required, a Certificate Authority may require additional information, such as professional affiliations or financial information, and the endorsement of this information by a notary.
- Does the authority have a system for receiving online certificate requests, such as requests generated by a key manager server? An online system can speed up processing of your certificate requests.
- With a commercial CA, you have less flexibility in certificate issuance and management. Some CA services and products may not integrate with your existing security model and directory services.
- Substantial costs can be associated with obtaining a server certificate, especially if you need a high degree of identification assurance.

Understanding Certificate Servers

Instead of obtaining all digital certificates from commercial CAs, you can implement a certificate server such as Microsoft Certificate Server to manage the issuance, renewal, and revocation of industry-standard digital certificates for your users. You can use these digital certificates in conjunction with servers that support SSL or PCT to build a secure Web infrastructure for the Internet or intranet. For large organizations with complex Web needs, certificate servers can offer many advantages over commercial CAs, including total control over certificate management policies and lower costs.

Depending on your relationship with your users, you can obtain server certificates from a commercial CA or you can issue your own server certificates. For services on your intranet, user trust is normally not an issue, and you can easily configure Internet Explorer to trust server certificates issued by your organization. For services on the Internet, however, users may not know enough about your organization to trust server certificates issued by you. Therefore, you may need to obtain server certificates issued by a well-known, commercial CA to ensure that users trust secure channels on your Internet sites.

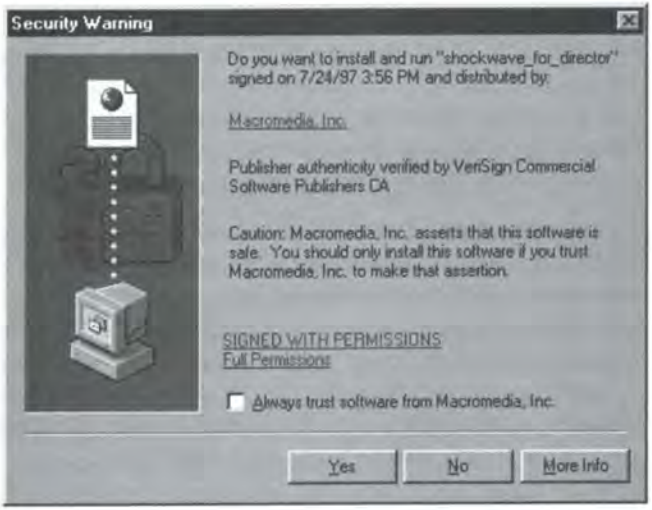
Understanding Authenticode

Microsoft Authenticode 2.0 technology is used to identify the publisher of a piece of software and verify that it hasn't been tampered with. Software publishers who obtain a digital certificate from a CA can use Authenticode signing tools to digitally sign their software packages for distribution over the Web. (For more information, see the *Microsoft Internet Client Software Development Kit.*)

Authenticode is client-side software that watches for the downloading of ActiveX controls, .cab files, Java™ applets, or executable files, and then displays warnings to the user about possible security issues. In addition to these warnings, Authenticode displays certificate information, such as the name included in the digital signature, whether it's a commercial or personal certificate, and the date the certificate expires. This information is presented so that users can make a more informed decision before continuing with the download.

Authenticode works by looking for digital certificates (or the lack thereof) in the files being downloaded. The digital certificate is incorporated in a .cab or .ocx file at the time it is compiled. Part of a certificate is the digital signature—the name of the independent software vendor (ISV). A file containing a digital signature is referred to as *signed.*

If a piece of software has been digitally signed, Internet Explorer 4 can verify that the software originated from the named software publisher and that it has not been tampered with. Internet Explorer will display a verification certificate if the software passes the test.



A valid digital signature, though, does not necessarily mean that the software is without problems. It just means that the software originated from a traceable source that you may choose to trust and that the software has not been tampered with since publication. Likewise, an invalid signature does not prove the software is bad or dangerous, but just alerts users to potential dangers and problems.

When a digital signature fails the verification process, Internet Explorer reports the failure, reports why the signature is invalid, and queries users to choose whether to proceed with the download.

Internet Explorer can be configured to take different actions, depending on the status of digital signatures. A signature can be unsigned, signed using valid certificates, or signed using invalid certificates.

For signed or unsigned software, you can configure Internet Explorer to:

- Prevent downloading or running the software from a zone.
- Download and run the software without user intervention from a zone.
- Query users to make a choice whether to download or run the software from a zone.

How you configure Internet Explorer to respond to certificates will depend on various factors, such as the level of trust you have for the security zone where the content originated. If you are deploying Internet Explorer in an organization, you'll also want to consider the level of trust you have for the intended user group and the level of technical expertise the users have. For example, you might trust unsigned software from your intranet, but not trust unsigned active content from the Internet. In that case, you would configure Internet Explorer to automatically download unsigned active content from the intranet without user intervention and prevent the download of unsigned active content from the Internet. For more information about configuring security settings, see Part 7, "Security and Privacy."

Authenticode 2.0

Internet Explorer 3 browsers include Authenticode 1.0, but the client-side technology expired on June 29, 1997. Authenticode 2.0 not only renews security features for Internet Explorer users, but also brings new improvements.

Features

The new time-stamping feature of Authenticode establishes that a given piece of software was properly signed during the valid lifetime of a publisher's certificate. (The reason certificates have a limited lifetime is to prevent giving counterfeiters enough time to crack the code associated with the certificate.)

With Internet Explorer 4, Authenticode 2.0 delivers another new feature to protect Web surfers. Before downloading any potentially hazardous code, Internet Explorer 4 can automatically check to make sure a publisher's certificate has not been revoked. Publishers can have their certificates revoked if they abuse their code-signing agreement; for example, by creating malicious code that harms users' computers.

Plus, the valid-site-check feature verifies that the certificate is valid on the actual Web site where it resides. Based on security settings within the certificate, a certificate may be valid only on a specific site.

After Authenticode 1.0 Expiration

Users who don't upgrade to Authenticode 2.0 won't face new security risks, and signed code that has already been downloaded will continue to work; but users may start receiving warnings that some of the software found on the Internet is not safe to download—even if it has been properly signed by a reputable software publisher.

- **If security is set to High:** Even if the code has been properly signed and updated, you may be prompted that the code is not safe to download.
- **If security is set to Medium:** Even if the code has been properly signed and updated, you may be prompted that the certificate used to sign the code is out-of-date.

Upgrading to Authenticode 2.0

Microsoft Internet Explorer 4 will be shipping with Authenticode 2.0 support within the box. This upgrade to Authenticode supplies several new features that make running a signed ActiveX control more secure.

This technology can be introduced into Internet Explorer 3 using the Authenticode 2.0 patch made available in June 1997. To install the Authenticode 2.0 patch, users must be running the Windows® 95 or Windows NT® 4.0 operating system and Internet Explorer 3 or later on their computers.

Using Secure Client/Server Communications

Digital certificates can be used for secure communications and user authentication between clients and servers on the Web. With digital certificates, clients can be assured of a server's identity; the server proves its identity by presenting a certificate. A user who connects to a Web site that has a server certificate signed by a trusted authority can be confident that the server is actually operated by the individual or organization identified in the certificate. Similarly, digital certificates enable servers to be confident of a client's identity. When a user connects to a Web site, the server can be assured of the user's identity if the server receives the client certificate.

Secure Channels

The exchange of digital certificates between clients and servers is performed using a secure transmission protocol, such as Secure Sockets Layer (SSL) or Private Communications Technology (PCT). SSL 2.0 supports server authentication only. PCT 1.0 and SSL 3.0 support both client and server authentication. Secure transmission protocols can provide three basic security services:

- **Mutual authentication.** Verifies the identities of both the server and client through exchange and validation of their digital certificates.
- **Communication privacy.** Encrypts information exchanged between secure servers and secure clients using a secure channel.
- **Communication integrity.** Verifies the integrity of the contents of messages exchanged between client and server, which ensures that messages have not been altered en route.

Note Encrypting all traffic between clients and servers using secure channels places a high load on secure clients and servers because all information that is transferred must be encrypted and unencrypted. Therefore, secure channel encryption is normally used only for the transfer of small amounts of sensitive information, such as personal financial data and user authentication information.

Server Gated Cryptography

In situations that require the highest-possible level of security, such as online banking, Server Gated Cryptography (SGC) can be used to provide stronger encryption for the client, but only if the server is authorized to use SGC. A special certificate is required. SGC enables financial institutions with Microsoft Windows NT–based Internet servers to use 128-bit SSL encryption—the industry's toughest-to-crack code.

Some of the key benefits of SGC are:

- Banks and financial institutions can securely conduct financial transactions with their retail customers worldwide without requiring customers to change their standard Web browser or financial software.
- Microsoft's online banking solutions do not require any special client software. Customers can use standard, off-the-shelf, 40-bit exportable versions of Microsoft Internet Explorer to connect to an SGC server and conduct secure transactions with strong, 128-bit cryptography.
- SGC is fully interoperable with Netscape browsers and servers. This means that Internet Explorer users will be able to communicate at 128 bits with Netscape servers.

Enabling SGC

SGC works with standard, off-the-shelf export-version servers and client applications that use an updated Schannel.dll and have an SGC digital certificate. The updated Schannel.dll can be freely downloaded from the Microsoft Web site. End users can enable their Internet Explorer browser for SGC by simply downloading the exportable 128-bit SGC add-on. Banks can enable Internet Information Server (IIS) for SGC if they have the standard, off-the-shelf version of Microsoft IIS 3.0, which is part of Windows NT 4.0. They simply download and apply the patch that will update their Schannel.dll file for IIS 3.0. They can use the KeyManager in IIS 3.0 to generate a request for a certificate, which must then be submitted to an authorized Certificate Authority. Once the certificate has been issued and installed, IIS will be fully SGC enabled and will be able to communicate at 128 bits with SGC-enabled Microsoft and Netscape clients.

Implementing SGC

SGC builds on the standard SSL 3.0 protocol. If the server presents the special SGC certificate, then a 128-bit SSL session is set up; otherwise, a 40-bit session is set up. Just like a normal SSL session, the session keys are destroyed after the session is complete.

Two different implementations of SGC currently exist. Both are described below:

Microsoft's Implementation of Server Gated Cryptography Negotiates the SSL Connection Once.

- The client sends a normal export (40-bit) client hello to the server.
- The server responds with a *server hello,* selecting a 40-bit cipher supported by the client. The server certificate arrives with the *server hello.*
- The client examines the server certificate and determines that it is allowed to do "fast" SGC by checking the key usage extensions for the existence of the Microsoft Fast SGC key usage extension (1.3.6.1.4.1.311.10.3.2) and by verifying that the certificate chain is rooted with the Microsoft SGC Root or the VeriSign Class 3 CA.
- The client ignores the rest of the *server hello* up to the ServerHelloDone message.
- The client resets its handshake hashes and sends another *client hello,* containing all of the ciphers allowed in SGC (that is, 128-bit RC4, and so forth).
- The server receives the *client hello* and starts the handshake over again, completing the handshake with full-strength ciphers.

Netscape's Implementation of Server Gated Cryptography Negotiates the SSL Connection Twice.

- The client and server do a complete SSL handshake.
- The client then examines the server certificate to see if it should do SGC.
- The client then initiates a REDO by sending a *client hello* immediately after the SSL handshake has completed. The *client hello* contains the strong ciphers allowed in SGC (that is, 128-bit RCA, and so forth).
- The second SSL handshake completes with full-strength ciphers.

Details on SGC Certificates

Each server certificate may contain an extension listing key usage. Both Netscape and Microsoft clients look in these extensions to determine whether a server is certified for SGC.

If the certificate chain is rooted with the VeriSign Class 3 CA and it contains the Netscape key usage extension (OID 2.16.840.1.113730.4.1), then the client may do the Netscape method of SGC.

If the certificate chain is rooted with the Microsoft SGC certification authority and it contains the Microsoft SGC key usage extension SGC OID (1.3.6.1.4.1.311.10.3.2), then the client may do the Microsoft method of SGC.

To ensure interoperability, Microsoft will produce a special certificate signed by the Microsoft SGC certificate to chain to the VeriSign class 3 CA. This certificate will be installed in the Microsoft SGC solution (Schannel.dll). This will allow VeriSign to issue SGC certificates for use by Microsoft client and server software. Thus:

- If a Microsoft Internet Explorer client connects to a Netscape server with a VeriSign SGC Certificate, Internet Explorer will do Netscape's method of SGC. If Internet Explorer connects to a Microsoft Internet Information Server with a VeriSign SGC Certificate, it will do Microsoft's method of SGC.
- If a Netscape client connects to a Netscape server with a VeriSign SGC Certificate, or to a Microsoft Internet Information Server with a VeriSign SGC Certificate, it will do Netscape's method of SGC.

CryptoAPI 2.0

CryptoAPI provides the underlying security services for secure channels and code signing. Through CryptoAPI, developers can easily integrate strong cryptography into their applications. Cryptographic Service Provider (CSP) modules interface with CryptoAPI and perform functions including key generation and exchange, data encryption and decryption, hashing, digital signatures, and signature verification. CryptoAPI is included as a core component of the latest versions of Windows. Internet Explorer 4 will automatically provide this support for earlier versions of Windows.

Secure Networks

Socks Firewall Support

Many corporations provide their employees with access to the Internet through firewalls that protect the corporation from unwanted access. Socks is a standard protocol for traversing firewalls in a secure and controlled manner. Internet Explorer 4 is compatible with firewalls that use the socks protocol. Hummingbird Communications, a leading provider of firewalls, provided this support.

Windows NT Server Challenge Response

Corporations can take advantage of the Microsoft Windows NT Challenge Response (NTLM authentication) that might already be in use on their Windows NT Server network. This enables users to have increased password protection and security while remaining interoperable with their existing Internet information servers.

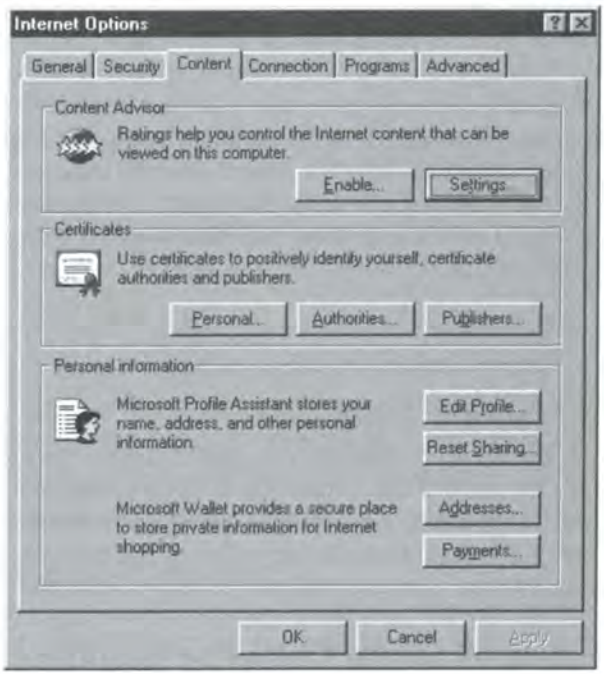
Configuring Certificates

You'll need to consider three areas of trust when installing and configuring certificates in Internet Explorer 4: root certificates for CAs, client certificates, and trusted publishers and CAs. The dialog boxes you'll use for configuration are the same whether you access them from Internet Explorer, the IEAK Configuration Wizard, or the IEAK Profile Manager.

From Internet Explorer, you access the certificates options from the **Content** tab.

▶ **To open the Content tab from Internet Explorer**

1. On the **View** menu, click **Internet Options**.
2. Click the **Content** tab.



3. After you finish configuring certificates, click **OK** or **Apply** on the **Content** tab to save the changes to Internet Explorer.

If you're building custom packages to deploy in user groups, see "Deploying Browsers with Customized Certificates" later in this chapter. If you're using the IEAK Profile Manager to configure certificates, also see "Managing Certificates for Deployed Browsers" later in this chapter.

Root Certificate Authorities

Many CAs have their root certificates already installed in Internet Explorer. You can select any of these installed certificates as trusted CAs for server-user authentication, client-user authentication, secure e-mail, and software publishers.

Some CAs do not have their root certificates in Internet Explorer. If you want to use their services, you'll need to import their root public key into Internet Explorer. Each CA's Web site has instructions on obtaining their root certificate (public key). You can use the IEAK Configuration Wizard and the IEAK Profile Manager to import root certificates. For more information, see "Deploying Browsers with Customized Certificates" and "Managing Certificates for Deployed Browsers" later in this chapter.

To remove certificates or select trusted certificates for Internet Explorer, use the **Certificate Authorities** dialog box.

▶ **To configure root certificates**

1. On the **Content** tab, click **Authorities**.
2. In the **Certificate Authorities** dialog box, select an issuer type from the **Issuer Type** list.



Issuer Type list:

- **Server user authentication**, to trust digital certificates from servers with digital certificates issued by the selected CAs.
- **Client user authentication**, to trust digital certificates from clients with digital certificates issued by the selected CAs.
- **Secure e-mail**, to trust transactions with other computers with digital certificates issued by the selected CAs.
- **Software publisher**, to trust downloads for software digitally signed by publishers with certificates issued by the selected CAs.

3. Select or clear check boxes for the listed CAs.

Note When you select a CA's root certificates as a trusted CA, you are trusting content from sites, people, and publishers with credentials issued by the CA.

4. Click **Close**.

Client Certificates

You may also want to install client certificates, which are used to authenticate users' computers as clients for secure Web communications. You can use the **Client Authentication** dialog box to install or remove client certificates for Internet Explorer.

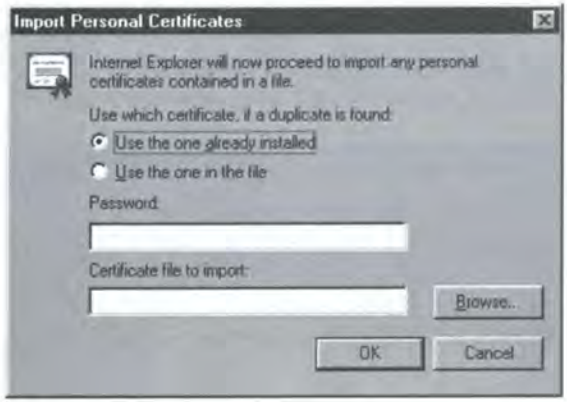
▶ **To import client certificates**

1. In the **Content** tab, click **Personal**.



2. In the **Client Authentication** dialog box, click **Import**.

3. In the **Import Personal Certificates** dialog box, click **Browse**, and open the certificate file to import.



4. In the **Password** box, enter your certificate password.
5. Click **OK**.
6. Click **Close**.

Trusted Publishers and Certificate Authorities

To designate a publisher or CA as a trusted publisher or CA for Internet Explorer, use the **Security Warning** dialog box that appears when you download software from that publisher or CA. Active content that is digitally signed with a valid certificate by trusted publishers or CAs will download without user intervention, unless downloading active content is disabled in the security settings for the security zone. You can also use the **Authenticode Security Technology** dialog box to remove publishers and CAs from the list of trusted publishers and authorities.

▶ **To add a trusted publisher or CA**

1. Use Internet Explorer to download signed active content from the publisher or CA.
2. When the **Security Warning** dialog box appears, select **Always trust software from** *publisher or CA name*.
3. Click **Yes** to add the publisher or CA to the list of trusted publishers and CAs.

▶ **To remove a trusted publisher or CA**

1. On the **View** menu, click **Internet Options.**
2. In the **Content** tab, click **Publishers**.
3. In the **Authenticode Security Technology** dialog box, select a publisher or CA from the list of trusted publishers and CAs.



4. Click **Remove**.
5. Click **OK**.

Deploying Customized Certificates in User Groups

System administrators can use the IEAK Configuration Wizard to deploy certificate configurations in their organizations. Using the IEAK, you can also build custom packages with specific security settings for different user groups. (For more information, see "Building Custom Packages" in Chapter 36.)

To specify certificate settings using the IEAK Configuration Wizard, use the **Site Certificate and Authenticode Settings** page. You can either accept the default certificate settings or customize the settings to meet your needs. The options in the IEAK for configuring root certificates authorities, client certificates, and trusted publishers and CAs are similar to those presented in Internet Explorer 4, described in more detail in the "Configuring Certificates" section earlier in this chapter.



▶ **To accept the default settings in the IEAK**

1. Select **Do not customize Certificate Authorities**.
2. Select **Do not customize Authenticode Security**.
3. Finish building the custom package.

▶ **To add new root certificates**

1. Select **Import current Certificate Authorities**.
2. Click **Add New Root**.
3. From the **Browse** dialog box, select the *file name* of the root certificate file, and click **Open**.

▶ **To customize trusted certificates**

1. Select **Import current Certificate Authorities**.
2. Click **Modify Settings**.
3. Use the **Site Certificates** dialog box to remove certificates or to select trusted certificates for each **Issuer Type**.

▶ **To remove a trusted publisher or CA**

1. Select **Import current Authenticode Security information**.
2. Click **Modify Settings**.
3. Use the **Authenticode Security Technology** dialog box to remove certificates.

▶ **To add a trusted publisher or CA**

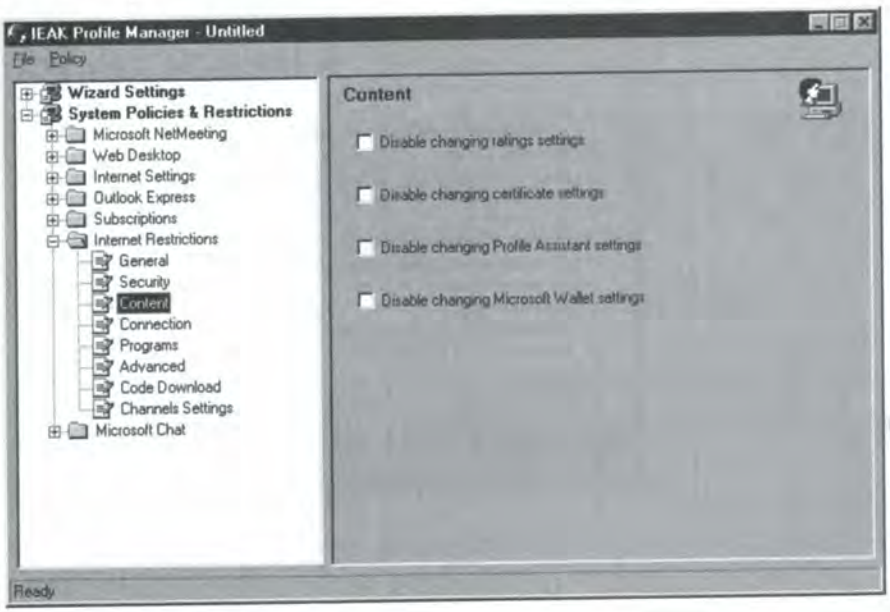
1. Use Internet Explorer to download signed active content from the publisher or CA.
2. When the **Security Warning** dialog box appears, select **Always trust software from** *publisher or CA name*.
3. Click **Yes** to add the publisher or CA to the list of trusted publishers and CAs.

Locking Down Certificates

Once you've built your custom certificate packages, you can also use the IEAK Configuration Wizard to lock down certificate configurations and restrict users from changing certificate settings. After browsers are deployed, you can use the IEAK Profile Manager to lock down certificates for user groups that have automatic browser configuration implemented. (For more information, see "Automatic Browser Configuration" in Chapter 37.)

▶ **To lock down certificates**

1. In the **System Policies & Restrictions** page of the IEAK Configuration Wizard or at the IEAK Profile Manager, in the **System Policies & Restrictions** hierarchy, select **Internet Restrictions,** and then select the **Content** object.



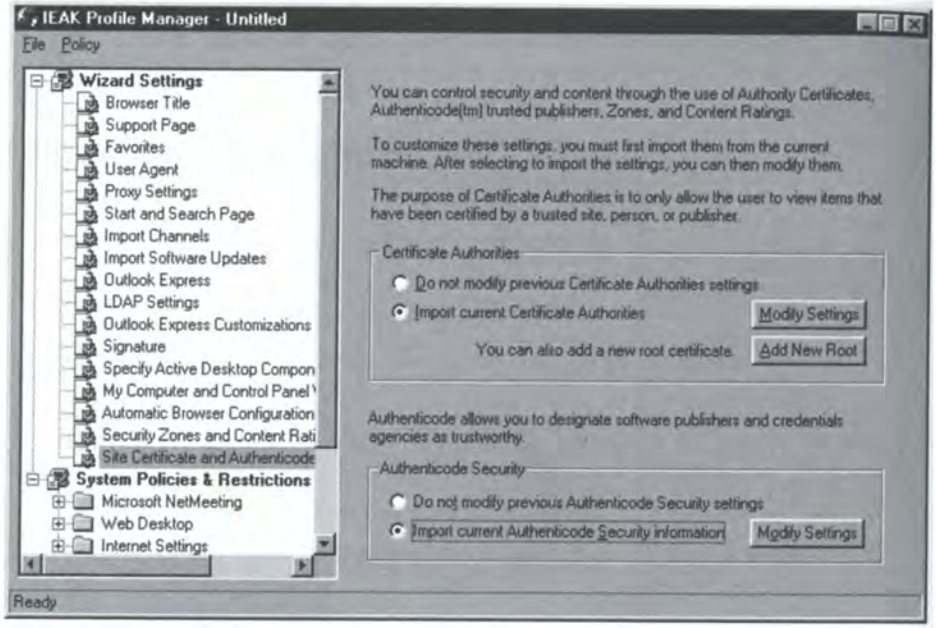
Note The IEAK Profile Manager is shown here, but the **System Policies & Restrictions** page of the IEAK Configuration Wizard works similarly.

2. In the right pane, select **Disable changing certificate settings**.
3. Save your changes to the auto-configuration (.ins) file, or finish building the custom package, as appropriate.

Managing Certificates for Deployed Browsers

To manage certificates for deployed browsers, you can use the IEAK Profile Manager in conjunction with automatic browser configuration. (For more information, see "Automatic Browser Configuration" in Chapter 37.)

You can update certificate settings by opening the auto-configuration (.ins) file in the IEAK Profile Manager and, in the left pane, selecting the Wizard Settings hierarchy, and then selecting the **Site Certificates and Authenticode Settings** object.



▶ **To add new root certificates**

1. Select **Import current Certificate Authorities**.
2. Click **Add New Root**.
3. From the **Browse** dialog box, select the *file name* of the root certificate file, and click **Open**.

▶ **To customize trusted certificates**

1. Select **Import current Certificate Authorities**.
2. Click **Modify Settings**.
3. Use the **Site Certificates** dialog box to remove certificates or to select trusted certificates for each **Issuer Type**.

▶ **To remove a trusted publisher or CA**

1. Select **Import current Authenticode Security information**.
2. Click **Modify Settings**.
3. Use the **Authenticode Security Technology** dialog box to remove certificates.

▶ **To add a trusted publisher or CA**

1. Use Internet Explorer to download signed active content from the publisher or CA.
2. When the **Security Warning** dialog box appears, select **Always trust software from** *publisher or CA name*.
3. Click **Yes** to add the publisher or CA to the list of trusted publishers and CAs.

▶ **To save changes to the auto-configuration (.ins) file**

- From the **File** menu, click **Save**.

Changes are made to users' configurations as scheduled by automatic browser configuration. You can also lock down certificates so users cannot modify the certificate settings.

CHAPTER 29

Trust-Based Security for Java

In this chapter

Trust-Based Security for Java Overview 490
Understanding Trust-Based Security 490
Security Zones 491
Permission Model 491
Permission Signing 492
Permission Scoping 493
Package Manager 495
Trust User Interface 496
Configuring Custom Java Security 496
Customizing Java Permissions for User Groups 502
Specifying Untrusted Signed Permissions 507
Specifying Unsigned and Trusted Signed Permissions 507

Trust-Based Security for Java Overview

Trust-based security for Java is a cross-platform security model for Java that provides fine-grained management of the permissions granted to Java applets and libraries. It uses Java Cabinet (CAB) signing technology to ensure that an applet can only perform actions for which it specifically requests permissions. With trust-based security for Java, developers can precisely limit the section of code where permissions have been granted, and administrators can have flexible control over the permissions granted to local classes. When combined with Internet Explorer security zones, trust-based security can also simplify security decisions for end users. For more background information about trust-based security for Java, see "Trusting Java," in the "Overview: Understanding Trust Management" section, at the beginning of Part 7.

Understanding Trust-Based Security

Trust-based security for Java includes:

- **Security zones.** Administer related sites (such as all sites on a company intranet) as a group.
- **Permission model.** Integrate zones to provide fine-grained, parameter-based control over what Java classes can do.
- **Permission signing.** Specify the permissions used by a set of signed classes as a part of the signature itself, rather than through calls in the Java code.
- **Permission scoping.** Precisely limit the sections of code where a permission that has been granted to a class is actually activated and available for use.
- **Package Manager.** Flexibly control the permissions granted to local classes, unlike competing models, which allow only a few trust levels for local classes.
- **Trust User Interface.** Greatly simplify or eliminate the decisions that end users need to make regarding zones and permissions administration.

Trust-based security for Java comes with default settings that meet many organizations' needs without customization. Or, system administrators can use the Internet Explorer Administration Kit (IEAK) Configuration Wizard to specify custom Java security settings for user groups in their organization.

Security Zones

Security zones provide a new approach to secure browsing with Internet Explorer 4 by dividing the Internet and intranet into four groupings of trusted (safe) and untrusted (unsafe) areas and assigning a specific security level to each area. (For more information, see Chapter 27, "Security Zones.") Security zones interact with the trust-based security for Java permission model (explained in the following section) to create a configurable, extensible mechanism for providing security for users. Network administrators can configure three different sets of permissions for each zone for both signed and unsigned code:

- **Permissions granted without user intervention.** These are permissions available to applets from the zone without user intervention. They can be separately specified for signed and unsigned applets.
- **Permissions granted with user intervention.** Users are queried whether to grant these permissions to applets from the zone.
- **Permissions that are denied.** These are permissions that are considered dangerous and are therefore automatically denied to applets from the zone.

Applets that use only permissions granted without user intervention run automatically. If an applet uses any permissions that are denied, the applet will not run. If an applet uses permissions granted with user intervention, a dialog box will be displayed, listing all the permissions and their associated risk, and users are queried whether to trust the applet. If users choose not to trust the applet, the applet can continue to run with alternate and limited functionality, but is prevented from using the expanded set of permissions.

Permission Model

The permission model for trust-based security supports a rich set of permissions, which can be controlled by parameters such as storage (scratch) space size and network connections allowed. The following sets of permissions correspond to the standard Java sandbox:

- Allow thread access in the current execution context.
- Open network connections to the applet host.
- Create a top-level pop-up window with a warning banner.
- Access reflection to classes from the same loader.
- Read base system properties.

With trust-based security for Java, you can create sets of permissions that greatly expand permissions or restrict the sandbox. To view and change custom Java permissions for each security zone, use the Internet Explorer **Custom Java Security** dialog box. (For more information, see "Configuring Custom Java Security" later in this chapter.) You can also use the IEAK Configuration Wizard and Profile Manager to edit the advanced Java permissions for each security zone. (For more information, see "Customizing Java Permissions for User Groups" later in this chapter.)

Permission Signing

Trust-based permission signing extends the signed .cab file functionality provided by Internet Explorer 3. Under trust-based security, a signed .cab file can securely specify not only the identity of the signer, but also the set of permissions being requested for the signed classes. Because the system can determine all the permissions requested by a Java component by inspecting the signature, the Trust User Interface can present a single dialog box displaying all of the relevant trust questions before any of the code starts to run. Since the set of permissions are fully defined and understood by the Java virtual machine, the Trust User Interface can accurately warn users about the risk of each permission.

Java code may be signed with default capabilities of High, Medium, and Low Safety settings:

- **High Safety** is a restrictive set of capabilities that are the equivalent of "sandboxed" Java code. This setting allows the applet to:
  - Have thread access in the current execution context.
  - Create a top-level pop-up Window with a warning banner.
  - Access Reflection APIs for classes from the same loader.
  - Read system properties.
  - Open network connections to the host machine.
- **Medium Safety** includes the capability of High Safety and adds:
  - Storage (scratch) space.
- **Low Safety** includes the capabilities of High and Medium Safety and additionally allows the applet to:
  - Perform file I/O.
  - Execute other applications on the client.
  - Implement user-interface dialog boxes.
  - Provide thread group access in the current execution context.
  - Open Network Connections to machines other than the host.

- Load libraries on the client.
- Make native method calls.
- Determine whether an applet can make native method calls.
- Create a top-level pop-up window without a warning banner.
- Exit the virtual machine.
- Perform registry operations.
- Perform printing operations.
- Create a ClassLoader.
- Access Reflection APIs.
- Read system properties.

For more information about signing Java code, see the *Microsoft Internet Client Software Development Kit (SDK)* and the *Microsoft SDK for Java.*

Permission Scoping

Trust-based permission scoping prevents permissions granted to a trusted component from being misused (inadvertently or intentionally) by a less trusted component. Permission scoping allows a trusted class to precisely limit the range of code for which a granted permission is enabled for use. This is important because some methods that use enhanced capabilities are designed to be safely called by anyone, while other methods are only designed to be used internally by trusted callers and should not expose their permissions to less trusted callers.

For example, a trusted class might want to expose a **WriteEventLog** method. This method is safely callable by anyone and uses a public helper function called **WriteData** to actually write each log item to a file. The write permissions to the log file for **WriteData** should be enabled only when called from **UpdateEventLog** and other trusted functions, not when called directly by an untrusted caller (otherwise, the untrusted caller could use **WriteData** to store arbitrary data in the log file).

Trust-based security distinguishes between permissions that have been *granted* to a class and permissions that are actually *enabled* (and activated for use) at a particular time. The granted permissions are determined by the administrative options for a class's zone and the permissions with which the class was signed. The enabled permissions are determined by the permissions granted to other callers on the call stack and whether any explicit calls to the **activatePrivilege**, **disablePrivilege**, or **revertPrivilege** APIs have been made. If the call stack has less-trusted callers on it, the enabled capabilities can be more restrictive than the enabled permissions.

The first essential rule in trust-based security permission scoping is that permissions are never inherited from the caller. If a class has not been directly granted a permission, then it can never make use of that permission, regardless of what permissions its callers may have. This makes trust-based security invulnerable to luring attacks, in which an untrusted class "lures" a trusted class into calling it and is incorrectly allowed to make use of the expanded permissions of its caller.

The second essential rule is that even if a class has been granted a permission, its methods must explicitly enable that permission using the **activatePrivilege** method whenever there is a caller on the call stack that has not been granted that permission. The following pseudocode is a more precise description of this version:

```
CheckAccess(Privilege P)
{
Frame F = first_frame();
// start at the active frame

  while
  (F is not beyond the end of the stack)
  {
   if (P has not been granted to F)
    return FALSE;
     if (P has been activated on F)
      return TRUE;
       if (P has been disabled on F)
        return FALSE;

        F = next_frame(F);
    }
 return TRUE;
}
```

This says that a permission P is enabled only if P is granted in all of the stack frames from the active frame up to the earliest frame on the stack, or up to a frame that has called **activatePrivilege** on P, and if no intervening frame has called **revertPrivilege** on P.

In the example described earlier, the trusted class could allow the **WriteEventLog** function to be used from any caller by inserting a call to **activatePrivilege** at the beginning of the function and a call to **revertPrivilege** at the end of the function. (The raised permissions would terminate as soon as the **WriteEventLog** method returned, so the **revertPrivilege** call is not strictly necessary.) This allows the storage (scratch) space functionality to be accessed from untrusted callers only at well-defined places; for example, under the control of the **WriteEventLog** function, but not when an untrusted caller called **WriteData** directly.

Note that under trust-based security, *no* changes to the source code would be called if WriteEventLog did not need to be called from methods that hadn't been granted file write permissions. This would be the case, for example, if the method was part of a class in a stand-alone application.

For more information about permission scoping, see the *Microsoft Internet Client SDK* and the *Microsoft SDK for Java.*

Package Manager

Package Manager allows the installation of local class libraries that are not fully trusted, using permission signing. This is especially important for Java Beans and class libraries. It is desirable to allow these components to reside locally and to have some expanded permissions, but not to give them unlimited power.

System libraries are libraries that are both shared and have all possible security permissions available to them. These are the core of the Java system APIs and are the most privileged Java code. Most packages installed from nonsystem providers do not need this level of privilege, but Java has traditionally treated all local classes on the ClassPath as if they were system libraries.

Under trust-based security, classes from installed packages are not shared between applets or applications that use them. They also carry specific system permission identifiers that are approved by either the user or the system administrator when that package is installed on the user's system. These permission identifiers determine the maximum permissions that can be used by the classes in that package.

For more information about Package Manager, see the *Microsoft Internet Client SDK* and the *Microsoft SDK for Java.*

Trust User Interface

The Trust User Interface defined by trust-based security for Java shields end users from complicated trust decisions and reduces the number of dialog boxes they must answer. The integration of capabilities with security zones means that users only need to make a simple "Yes/No" choice when deciding whether to trust an application. The fine-grained decisions of which capabilities to allow have already been made by an administrator.

In addition, permission signing allows trust-based security to predetermine all the capabilities used by a class. When a package is installed, trust-based security for Java can use the signature to determine exactly the system permissions that it needs to provide, and a single trust dialog box can reliably present all of the capabilities required by an application before running any code. Since the default system permissions are well defined and static, their level of risk can be determined and refined over time, ensuring acceptable risk representation. All non-default system permissions should have a default risk level of Extreme.

For more information, see the *Microsoft Internet Client SDK* and the *Microsoft SDK for Java.*

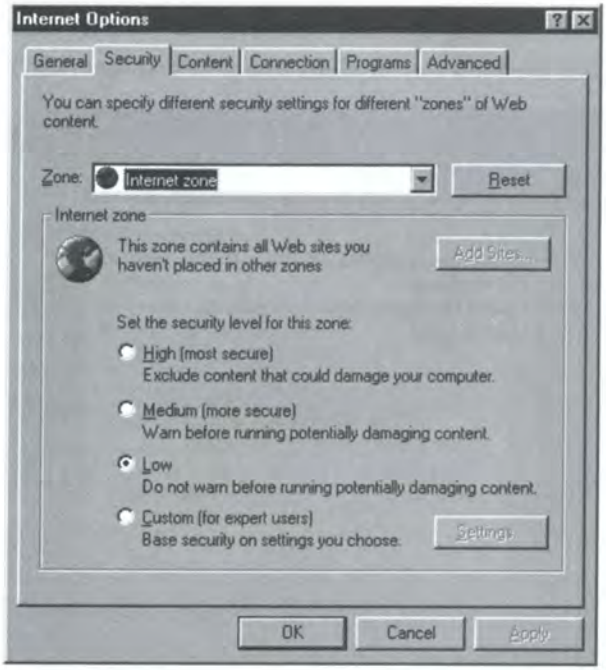
Configuring Custom Java Security

To view and change custom Java permissions for each security zone, use the **Custom Java Security** dialog box. You can specify the way Java applet permission requests are controlled for both signed and unsigned applets.

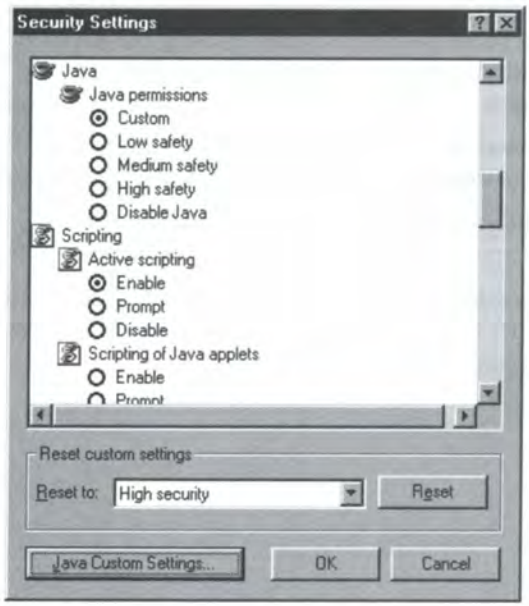
Note This section describes the user interface for customizing Java permissions for Internet Explorer 4.01. The interface for Internet Explorer 4.0 differs, but it is similar to the advanced Java permissions editor dialog boxes described in "Customizing Java Permissions for User Groups," next in this chapter. For more information, see Help for Internet Explorer 4.

▶ **To access the Custom Java Security dialog box**

1. On the **View** menu, click **Internet Options.**
2. Click the **Security** tab.
3. In the **Zone** drop-down list, select a security zone to customize.



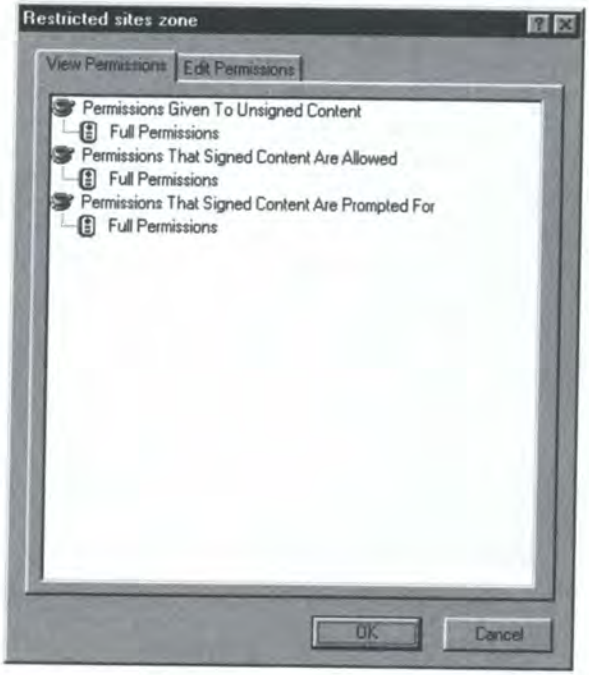
4. Under **Internet zone,** select **Custom (for expert users)**, and click **Settings**.
5. In the **Security Settings** dialog box, in the **Java** hierarchy, select **Java permissions**, and then select **Custom**.



6. Click **Java Custom Settings**.

▶ **To view permissions at the Custom Java Security dialog box**

- Click the **View Permissions** tab.

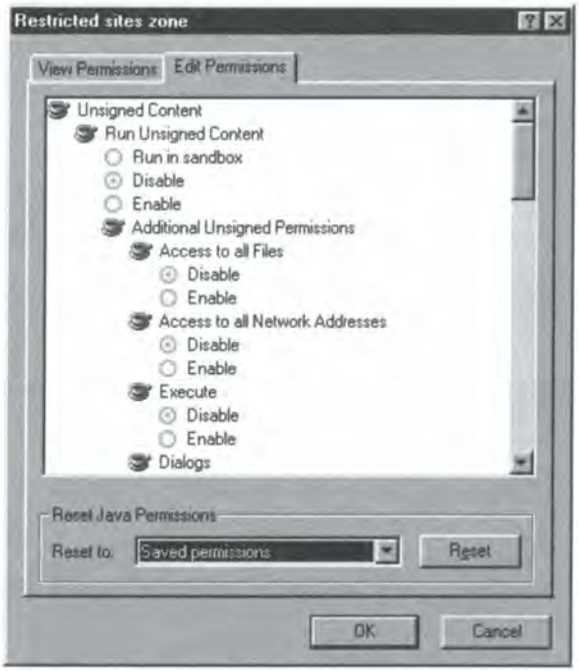


This tab displays permissions in a hierarchical tree, which you can expand and collapse. These permissions are set using the advanced Java permissions editor (see "Customizing Java Permissions for User Groups," next in this chapter). Permissions are organized into the following categories:

- **Permissions Given To Unsigned Content.** Unsigned Java applets that request these permissions can run without user query.
- **Permissions That Signed Content Are Allowed.** Signed Java applets that request these permissions can run without user query.
- **Permissions That Signed Content Are Prompted For.** Users are queried whether to allow signed applets to run when applets request these permissions.

▶ **To change custom Java permissions at the Custom Java Security dialog box**

1. Click the **Edit Permissions** tab.



2. Configure the custom Java permissions options.

Option	Description
Unsigned Content—Run Unsigned Content	
Run in sandbox	Select to run unsigned Java applets for this zone in a Java sandbox that you specify. You can enable or disable individual options in **Additional Unsigned Permissions** by selecting **Disable** to disable and **Enable** to enable options.
Disable	Select to disable running unsigned applets for this zone. All options in **Additional Unsigned Permissions** are disabled and shaded.
Enable	Select to enable running unsigned applets for this zone. All options in **Additional Unsigned Permissions** are enabled.

Option	Description
Unsigned Content—Additional Unsigned Permissions	
Access to all files	Select **Enable** to allow unsigned applets to have read access to all files on your system. Select **Disable** to prevent unsigned applets from having read access to all the files on your system.
Access to all network addresses	Select **Enable** to allow unsigned applets to have access to network addresses. Select **Disable** to prevent unsigned applets from having access to network addresses.
Execute	Select **Enable** to allow unsigned applets to run other applications. Select **Disable** to prevent unsigned applets from running other applications.
Dialogs	Select **Enable** to allow unsigned applets to create file dialog boxes. Select **Disable** to prevent unsigned applets from creating file dialog boxes.
System information	Select **Enable** to allow unsigned applets to read system properties. Select **Disable** to prevent unsigned applets from reading system properties.
Printing	Select **Enable** to allow unsigned applets to access printer resources. Select **Disable** to prevent unsigned applets from accessing printer resources.
Protected scratch space	Select **Enable** to allow unsigned applets to use storage area on your hard disk. Select **Disable** to prevent unsigned applets from using storage area on your hard disk.
User-selected file access	Select **Enable** to query you whether unsigned applets can access selected files. Select **Disable** to prevent unsigned applets from accessing any files and to prevent querying you for permission.
Signed Content—Run Signed Content	
Prompt	Select to set individual options in **Additional Signed Permissions** to **Prompt**. You can select **Disable** to disable and **Enable** to enable each individual option.
Disable	Select to disable running signed applets for this zone. All options in **Additional Signed Permissions** are disabled and shaded.
Enable	Select to enable running unsigned applets for this zone. All options in **Additional Signed Permissions** are enabled.
Signed Content—Additional Signed Permissions	
Access to all files	Select **Prompt** to query you before signed applets can have read access to all the files on your system. Select **Enable** to allow signed applets to have read access to all files on your system. Select **Disable** to prevent signed applets from having read access to all the files on your system.
Access to all network addresses	Select **Prompt** to query you whether signed applets can have access to network addresses. Select **Enable** to allow signed applets to have access to network addresses. Select **Disable** to prevent signed applets from having access to network addresses.

Option	Description
Signed Content—Additional Signed Permissions *(continued)*	
Access to all network addresses	Select **Prompt** to query you whether signed applets can have access to network addresses. Select **Enable** to allow signed applets to have access to network addresses. Select **Disable** to prevent signed applets from having access to network addresses.
Execute	Select **Prompt** to query you whether signed applets can run other applications. Select **Enable** to allow signed applets to run other applications. Select **Disable** to prevent signed applets from running other applications.
Dialogs	Select **Prompt** to query you whether signed applets can create file dialog boxes. Select **Enable** to allow signed applets to create file dialog boxes. Select **Disable** to prevent signed applets from creating file dialog boxes.
System information	Select **Prompt** to query you whether signed applets can read system properties. Select **Enable** to allow signed applets to read system properties. Select **Disable** to prevent signed applets from reading system properties.
Printing	Select **Prompt** to query you whether signed applets can access printer resources. Select **Enable** to allow signed applets to access printer resources. Select **Disable** to prevent signed applets from accessing printer resources.
Protected scratch space	Select **Prompt** to query you whether signed applets can use storage area on your hard disk. Select **Enable** to allow signed applets to use storage area on your hard disk. Select **Disable** to prevent signed applets from using storage area on your hard disk.
User-selected file access	Select **Prompt** or **Enable** to query you whether signed applets can access selected files. Select **Disable** to prevent signed applets from accessing any files and to prevent querying you for permission.
Reset Java Permissions	
Saved permissions	In the **Reset to:** drop-down list, select and click **Reset** to restore all settings to the last saved permission. Initially, these settings are the settings set using the advanced Java permissions editor (see "Customizing Java Permissions" earlier in this chapter). Every time you change settings and click **OK**, a new set of saved permissions is saved.
High security	In the **Reset to:** drop-down list, select and click **Reset** to reset all permissions to High security level (most restrictive; applets run in safe mode).
Medium security	In the **Reset to:** drop-down list, select and click **Reset** to reset all permissions to Medium security level (applets run with some restrictions).
Low security	In the **Reset to:** drop-down list, select and click **Reset** to reset all permissions to Low security level (least restrictive; applets run with all permissions).

Customizing Java Permissions for User Groups

System administrators can use the IEAK Configuration Wizard to deploy custom Java permissions in their organizations. Using the IEAK, you can also build custom packages with specific Java permissions for different user groups. Once a custom browser has been deployed, the IEAK Profile Manager can be used to update Java permissions. (For more information, see "Building Custom Packages" in Chapter 36.)

Note This section describes the user interface for customizing Java permissions for Internet Explorer 4.01. The interface for Internet Explorer 4.0 differs, but it is similar to the advanced Java permissions editor dialog boxes described in this section. For more information, see Help for Internet Explorer 4.

To customize Java permissions for each security zone, use the advanced Java permissions editor dialog boxes. You can access the advanced Java permissions editor using the IEAK Configuration Wizard or the IEAK Profile Manager. Typically, end users cannot access the advanced Java permissions editor from Internet Explorer. However, when the IEAK is installed, and you run the IEAK Configuration Wizard or Profile Manager, access to the advanced Java permissions editor from Internet Explorer is turned on.

You can specify how applet permissions are handled for three classes of permission requests:

- Unsigned permission requests from unsigned applets.
- Trusted signed permission requests from signed applets.
- Untrusted signed permissions from signed applets.

You can specify the way applet permissions are controlled for:

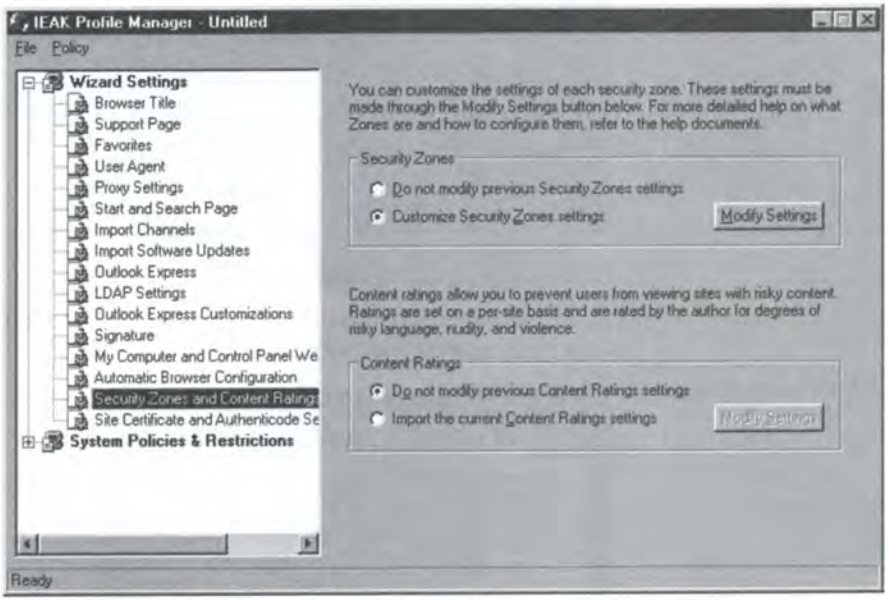
- **Unsigned Permissions.** Grant these permissions to unsigned applets from the zone. Unsigned applets that request these permissions can run without user action. Unsigned applets that request additional permissions cannot run.
- **Trusted Signed Permissions.** Grant these permissions to trusted signed applets from the zone. Signed applets that request these trusted permissions can run without user action.
- **Untrusted Signed Permissions.** Grant these permissions to untrusted signed permissions from the zone. Signed applets that request these permissions are handled in one of the following ways:
  - Users are queried whether to allow the applet to run with these permissions.
  - Applets are prevented from running with no user query.

  You can optionally specify that all signed applet permission requests not specified as trusted or untrusted are treated as untrusted signed permissions.

End users can use the **Custom Java Security** dialog box to view and change custom Java permissions for each security zone. For more information, see "Configuring Custom Java Security" earlier in this chapter.

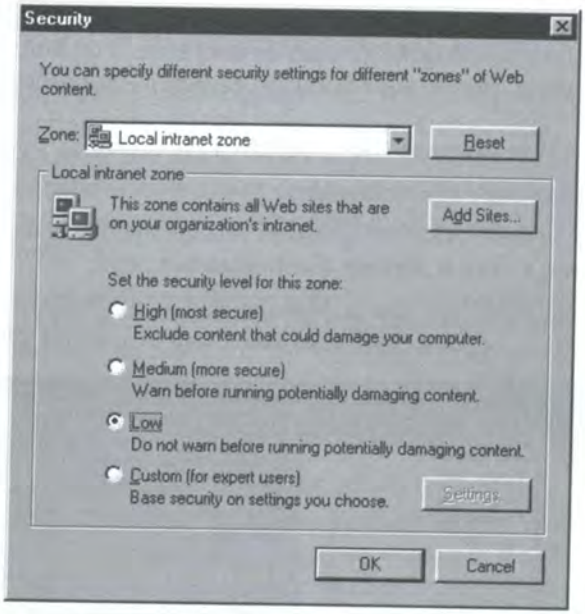
▶ To access the advanced Java permissions editor

1. Perform one of the following:
   - Run the IEAK Configuration Wizard, and navigate to the **Security Zones and Content Ratings Customization** page.
   - Run the IEAK Profile Manager and, in the **Wizard Settings** hierarchy, select the **Security Zones and Content Ratings Customization** object.

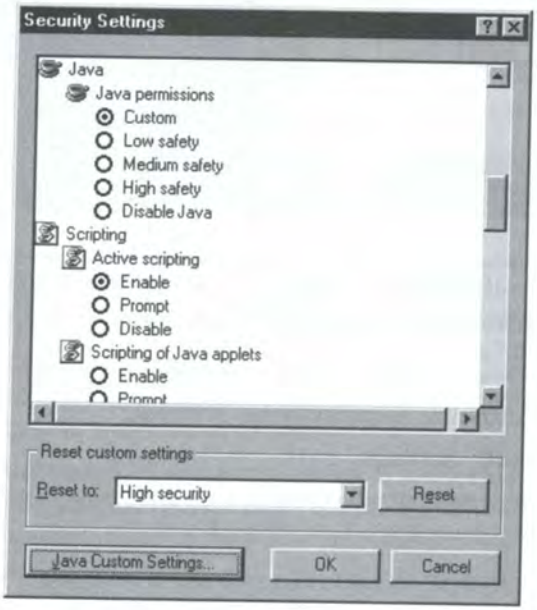


Note The IEAK Profile Manager is shown here, but the **Security Zones and Content Ratings Customization** page of the IEAK Configuration Wizard works similarly.

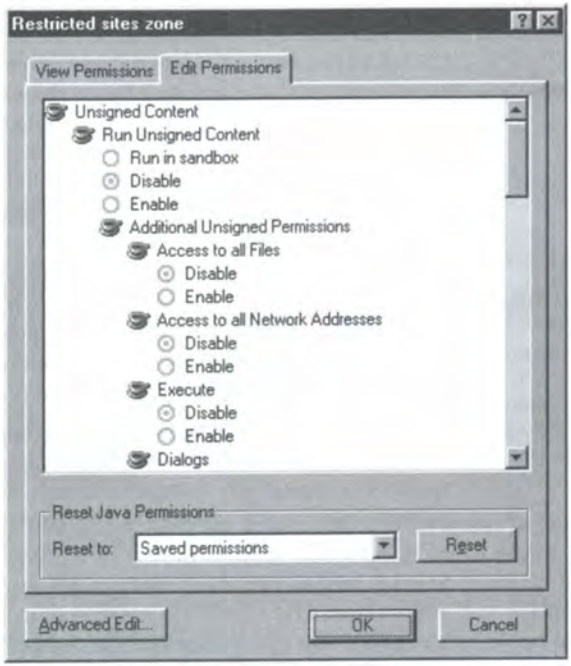
2. Select **Customize Security Zones settings**.
3. Click **Modify Settings**.
4. In the **Security** dialog box, select a security zone to customize from the **Zone** drop-down list.



5. Select **Custom (for expert users)**, and click **Settings**.
6. In the **Security Settings** dialog box, in the **Java** hierarchy, select the Java permissions **Custom** option.

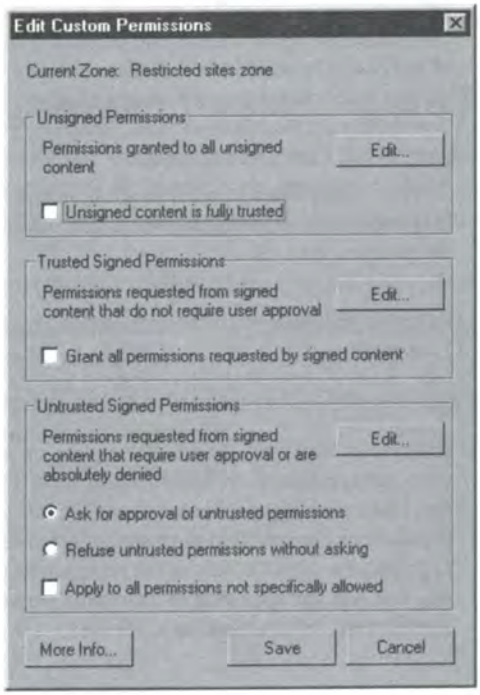


7. Click **Java Custom Settings**.
8. Click **Advanced Edit**.



▶ **To customize advanced Java permissions**

1. Use the **Edit Custom Permissions** dialog box to specify custom permissions.



Option	Description
Unsigned Permissions	Click **Edit** to open the **Unsigned Permissions** dialog box and specify permissions granted to unsigned Java content for this zone. Unsigned Java applets that request permissions can run from this zone without user query, but unsigned applets that request permissions not granted cannot run from this zone. For more information, see "Specifying Unsigned and Trusted Signed Permissions" and "Specifying Untrusted Signed Permissions" later in this chapter.
Unsigned content is fully trusted	Select to trust all unsigned content from this zone. You should exercise caution before selecting this option, because it allows unsigned Java applets to run from this zone without user query and with full access to the user's computer and network resources. This option overrides any changes you make using the **Unsigned Permissions** dialog box.
Trusted Signed Permissions	Click **Edit** to open the **Trusted Signed Permissions** dialog box and specify the permissions granted to signed Java content for this zone. Java applets that request only these permissions can run without user query. For more information, see "Specifying Unsigned and Trusted Signed Permissions" and "Specifying Untrusted Signed Permissions" later in this chapter.
Grant all permissions requested by signed content	Select to trust all signed content from this zone. Selecting this option means signed Java applets can run with all requested permissions, without user query. This option overrides any changes you make using the **Trusted Signed Permissions** dialog box.
Untrusted Signed Permissions	Click **Edit** to open the **Untrusted Signed Permissions** dialog box and specify the permissions you do not want to be trusted for signed Java content for this zone. When signed Java applets request these permissions, either the user is queried to allow the applet to run, or permissions are denied and the applet cannot run, depending on whether **Ask for approval of untrusted permissions** or **Refuse untrusted permissions without asking** is selected. For more information, see "Specifying Unsigned and Trusted Signed Permissions" and "Specifying Untrusted Signed Permissions" later in this chapter.
Ask for approval of untrusted permissions	Select to query users whether to allow signed Java applets that request untrusted permissions to run. The applet can run only if the user approves the permissions.
Refuse untrusted permissions without asking	Select to prevent signed Java applets that request untrusted permission from running.
Apply to all permissions not specifically allowed	Select to control how signed Java applets are handled that request permissions not specified as trusted or untrusted in **Trusted Signed Permissions** and **Untrusted Signed Permissions**. When a signed applet requests permissions not specified as trusted or untrusted, either the user is queried to permit the applet to run, or the permissions are denied, depending on whether **Ask for approval of untrusted permissions** or **Refuse untrusted permissions without asking** is selected.

2. Click **Save** to save the changes as the default custom Java settings for user groups.
3. Save your changes to the auto-configuration (.ins) file, or finish building the custom package, as appropriate.

Specifying Untrusted Signed Permissions

You can use the **Unsigned Permissions** dialog box to specify custom permissions for untrusted signed Java applets. (The dialog boxes for **Unsigned Permissions** and **Untrusted Signed Permissions** are identical except for the title.) The dialog box is grouped into seven tabs, as detailed in the coming sections.

The effect of the permissions you assign here depends on whether you select **Ask for approval of untrusted permissions** or **Refuse untrusted permissions without asking**:

- If you select **Ask for approval of untrusted permissions**, users are queried whether to permit applets that request these permissions to run.
- If you select **Refuse untrusted permissions without asking**, applets that request these permissions cannot run.

▶ **To customize untrusted signed permissions**

1. In the **Edit Custom Permissions** dialog box, under **Untrusted Signed Permissions**, click **Edit**.
2. Click the appropriate tab, and customize the options as necessary.

Specifying Unsigned and Trusted Signed Permissions

You can use the **Unsigned Permissions** and **Trusted Signed Permissions** dialog boxes to specify custom permissions for unsigned and signed Java applets. The dialog boxes are grouped into seven tabs.

▶ **To customize unsigned or trusted signed permissions**

1. In the **Edit Custom Permissions** dialog box, under **Unsigned Permissions** or **Trusted Permissions**, click **Edit**.
2. In the resulting dialog box, click the appropriate tab, and customize the options, as necessary.

The following sections describe all customization options.

Note The tabs shown are for the **Unsigned Permissions** dialog box, but the **Trusted Signed Permissions** dialog box is identical except for the title.

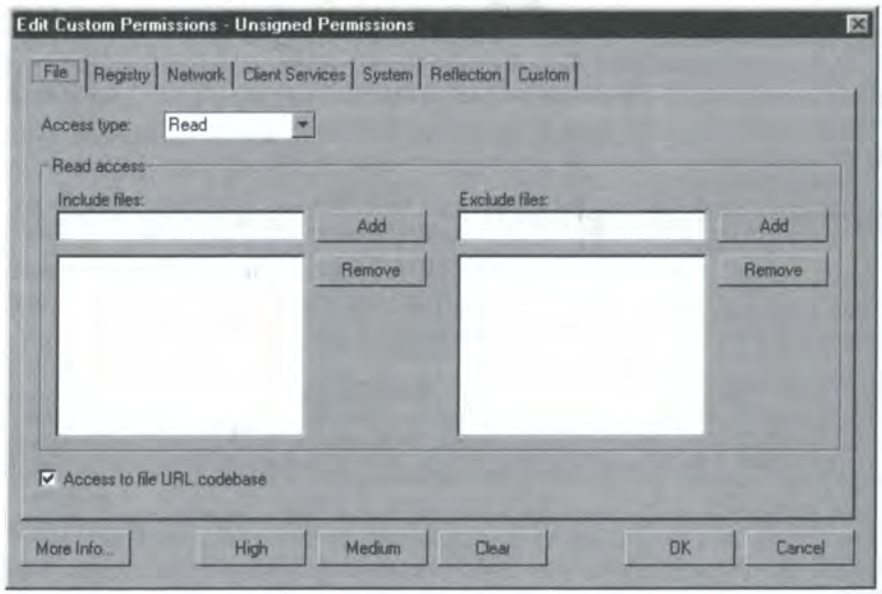
File tab

Use the **File** tab to specify files and file types that you will allow in this permission set for this zone. By default, all files are excluded, so you do not need to specify files to exclude, unless they are a subset of the files you are including. For example, if you include a multimedia file type (*.avi), you can exclude a specific file of that type (huge.avi). You can specify different permissions for Read, Write, and Delete access.

For example, for read access, you could type the following masks:

Include Files: C:\Windows*
Exclude Files: *.exe

These masks would result in read access to everything in the Windows directory, except for the .exe files in the Windows directory.

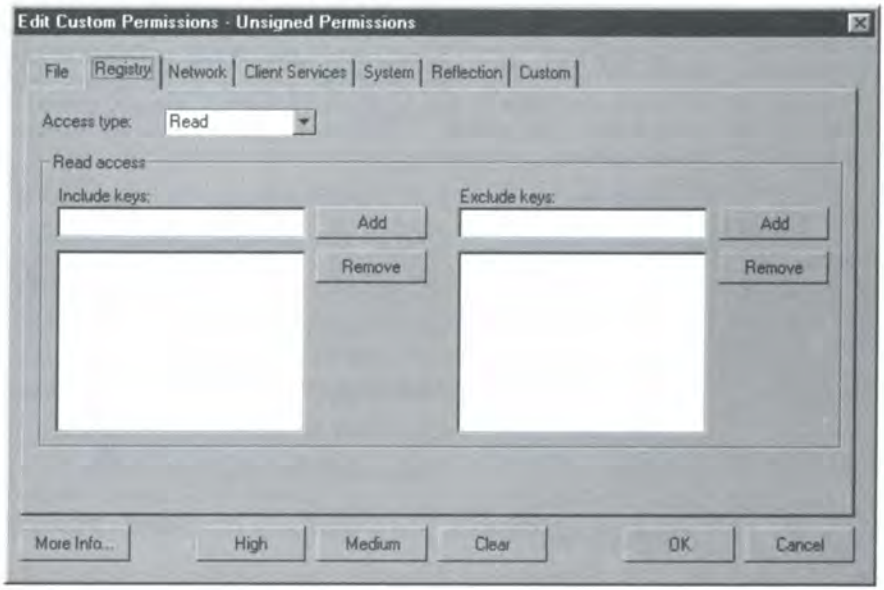


Option	Description
Access type	Select either **Read**, **Write**, or **Delete** to specify that applets can have read, write, or delete access to the included files for this zone.
Read access	
Include files	Enter the files to include for the selected access type.
Exclude files	Enter the files to exclude from the selected access type.
Access to file URL codebase	Select to allow access to the file URL codebase.
Security level	
High	Click to set the security level to High (most secure).
Medium	Click to set the security level to Medium.
Clear	Click to clear all options and settings on this tab.

Registry tab

Use the **Registry** tab to specify registry keys you will allow in this permission set for this zone. By default, all registry keys are excluded, so you do not need specify registry keys to exclude, unless they are a subset of the registry keys you are including. For example, if you include **HKEY_CURRENT_USER**, you can exclude a specific registry category underneath that key (**HKEY_CURRENT_USER\Network**).

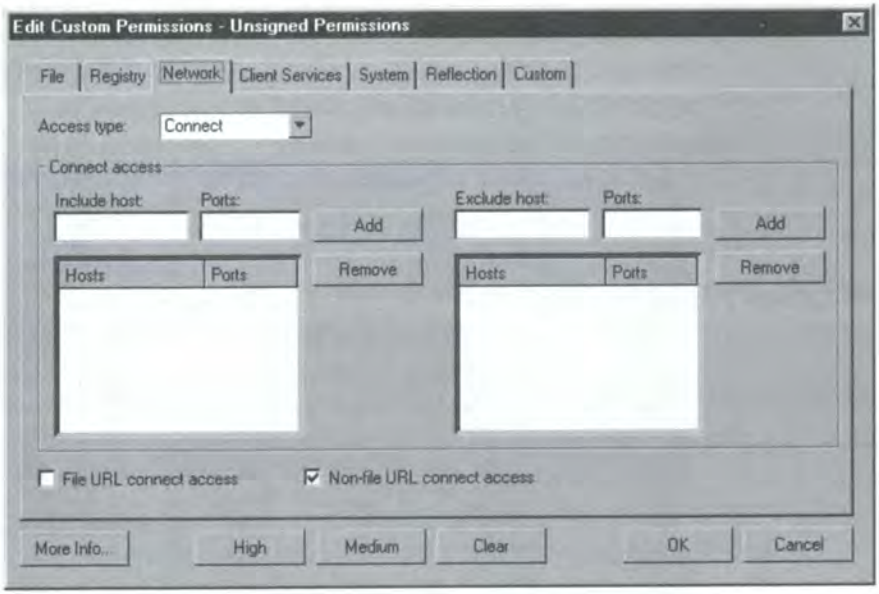
You can specify different permissions for different types of access: read, write, delete, open, and create. Access can be specified either on a global basis or to specific portions of the registry using wildcard masks for either included keys or excluded keys.



Option	Description
Access type	Select either **Read**, **Write**, **Delete**, **Create**, or **Open** to specify that applets can have read, write, delete, create, or open access to the included registry keys.
Read access	
Include keys	Enter the registry keys you want to include for the selected access type.
Exclude keys	Enter the registry keys you want to exclude from the selected access type.
Security level	
High	Click to set the security level to High (most secure).
Medium	Click to set the security level to Medium.
Clear	Click to clear all options and settings on this tab.

Network tab

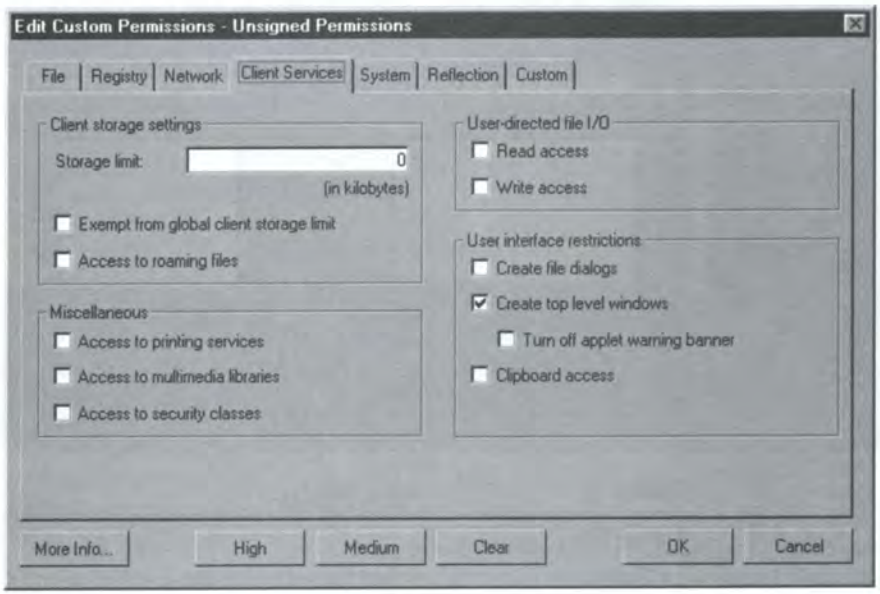
Use the **Network** tab to specify the type of connections you will allow, and to which hosts and ports. By default, all hosts and ports are excluded, so you do not need to specify hosts and ports to exclude, unless they are a subset of the hosts and ports you are including. You can specify different permissions for different types of connections: connect addresses, bind addresses, multicast, and global ports.



Option	Description
Access type	
Connect	Select to enable applets to have general communication to included hosts
Bind	Select to enable applets to connect to included hosts and ports.
Multicast	Select to enable applets to join specific multicast groups.
Global Ports	Select to enable applets to use communication settings that override the rules of the included ports.
Connect access	
Include host/Ports	Enter the hosts and ports that you want to enable applets to communicate with.
Exclude host/Ports	Enter the hosts and ports that you want to exclude from communicating with applets.
File URL connect access	Select to enable applets to connect to file:// URLs.
Non-file URL connect access	Select to enable applets to connect to non-file URLs.
Security level	
High	Click to set the security level to High (most secure).
Medium	Click to set the security level to Medium.
Clear	Click to clear all options and settings on this tab.

Client Services tab

Use the **Client Services** tab to specify which client resources and services Java applets can access for this permission set and zone.

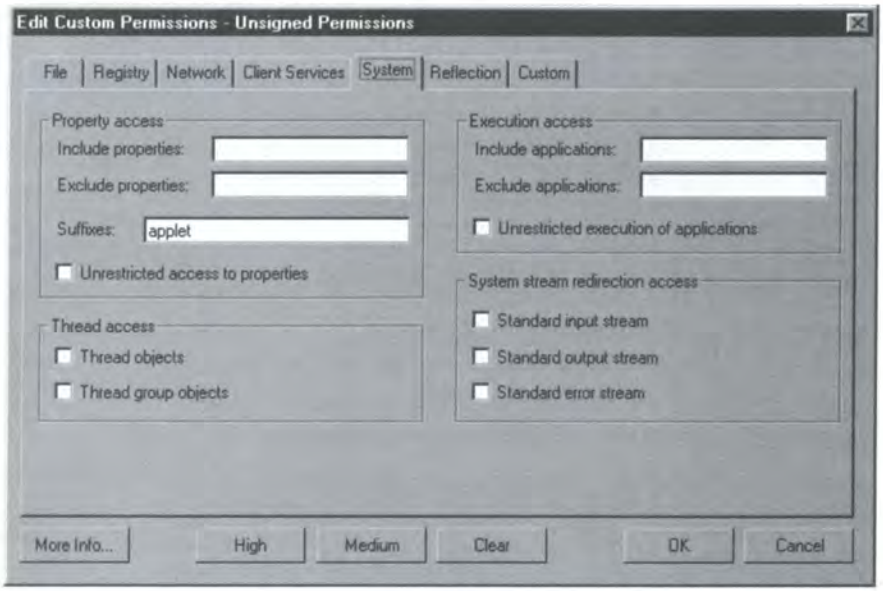


Option	Description
Client storage settings	
Storage limit	Enter the number of kilobytes of storage (scratch) space that applets can use on the client. Applets can access storage space determined by the size of the specified storage space and whether the storage space is private or global. Private storage space is encrypted and only available to the signed class or other classes signed by the same entity. Global storage space can be shared among arbitrary classes.
Exempt from global client storage limit	Select to enable applets to ignore the specified storage limits for all Internet files.
Access to roaming files	Select to enable roaming files to be created. Roaming files are created in the user's profile and are present on any computer the user is logged on to.

Option	Description
User-directed I/O	
Read access	Select to enable applets to read files on the client.
Write access	Select to enable applets to write to files on the client.
Miscellaneous	
Access to printing services	Select to enable applets to use the printing services.
Access to multimedia libraries	Select to enable applets to access the extended aspects of the DirectX™ APIs.
Access to security classes	Select to enable Java applets to access the JDK security classes java.lang.security.
User interface restrictions	
Create file dialogs	Select to enable applets to create file dialog boxes.
Create top level window	Select to enable applets to create a top-level window.
Turn off applet warning banner	Clear to display a warning when an applet requests to create a top-level window.
Clipboard access	Select to enable applets to use the client's clipboard to cut, copy, or paste information.
Security level	
High	Click to set the security level to High (most secure).
Medium	Click to set the security level to Medium.
Clear	Click to clear all options and settings on this tab.

System tab

Use the **System** tab to specify which operating system resources and services Java applets can access for this permission set and zone.



Option	Description
Property access	
Include properties	Enter the names of system properties that applets can access.
Exclude properties	Enter the names of system properties that you want to exclude applets from accessing.
Suffixes	Enter the suffixes of system properties that applets can access.
Unrestricted access to properties	Select to enable applets to have unrestricted access to system properties.
Thread access	
Thread objects	Select to enable unrestricted thread access for applets.
Thread group objects	Select to enable unrestricted thread group access for applets.

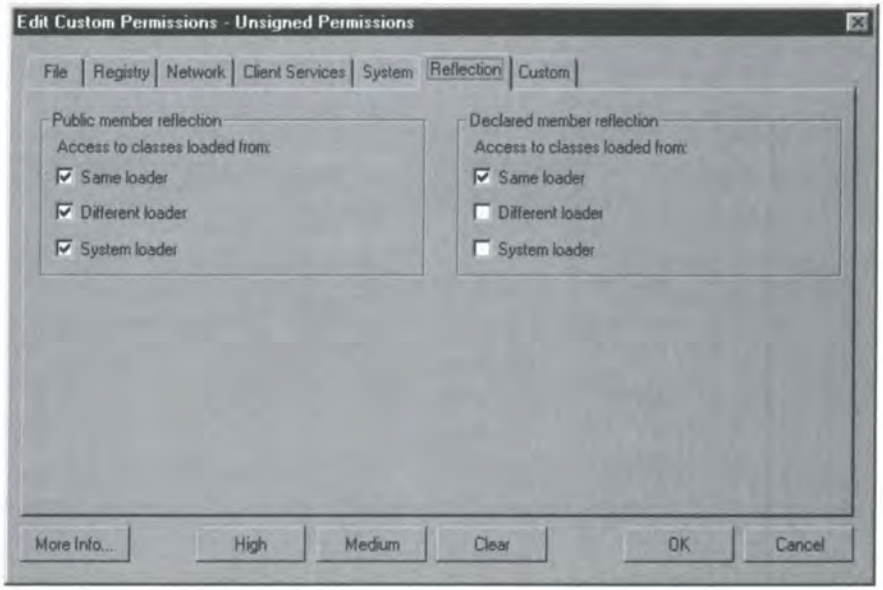
Option	Description
Execution access	
Include applications	Enter the names of applications that applets can run.
Exclude applications	Enter the names of applications that applets cannot run.
Unrestricted execution of applications	Select to enable unrestricted access for applets to run applications.
System stream redirection access	
Standard input stream	Select to enable applets to set the System.in stream.
Standard output stream	Select to enable applets to set the System.out stream.
Standard error stream	Select to enable applets to set the System.err stream.
Security level	
High	Click to set the security level to High (most secure).
Medium	Click to set the security level to Medium.
Clear	Click to clear all options and settings on this tab.

Note Java applets can read the system properties using the **System.getProperty** method. The following table lists the default system properties that can be read by applets.

Permission	Property
Java version	Java.version
Java vendor-specific string	Java.vendor
Java vendor URL	Java.vendor.url
Java class version number	Java.class.version
Operating System name	Os.name
User account name	User.name
User's home directory	User.home
User's current working directory	User.dir

Reflection tab

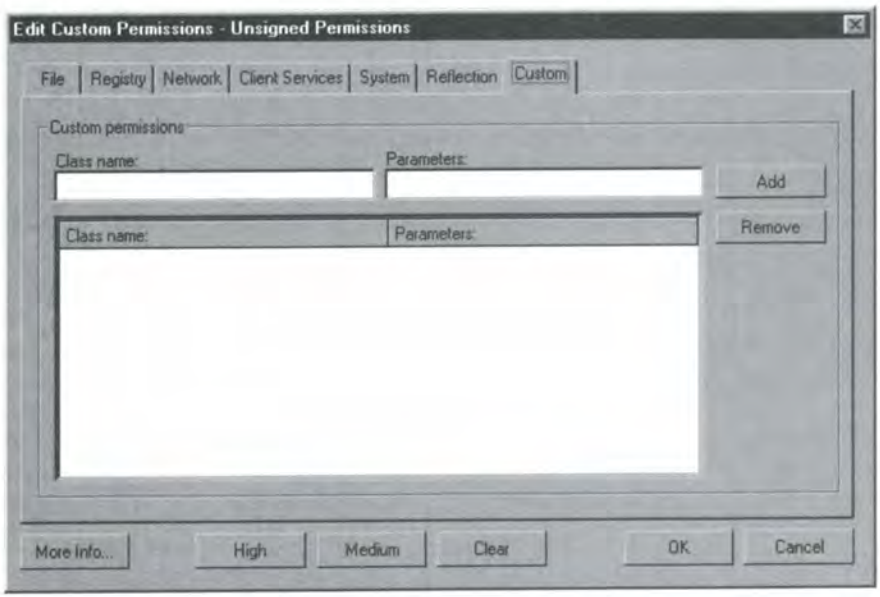
Use the **Reflection** tab to specify which Reflection APIs Java applets can access for this permission set and zone.



Option	Description
Public member reflection	
Same loader	Select to enable public reflective access to the reflection APIs for classes from the same loader.
Different loader	Select to enable public reflective access to the reflection APIs for classes from different loaders.
System loader	Select to enable public reflective access to the reflection APIs for classes from the system loader.
Declared member reflection	
Same loader	Select to enable declared reflective access to the reflection APIs for classes from the same loader.
Different loader	Select to enable declared reflective access to the reflection APIs for classes from different loaders.
System loader	Select to enable declared reflective access to the reflection APIs for classes from the system loader.
Security level	
High	Click to set the security level to High (most secure).
Medium	Click to set the security level to Medium.
Clear	Click to clear all options and settings on this tab.

Custom tab

Use the **Custom** tab to specify custom permission settings by class name and parameters. You can assign permissions to a Java class and specify what parameters are allowed.



Option	Description
Custom permissions	
Class name	Enter the Java classes to include in this permission set.
Parameters	Enter the parameters that are allowed for the included Java classes.
Security level	
High	Click to set the security level to High (most secure).
Medium	Click to set the security level to Medium.
Clear	Click to clear all options and settings on this tab.

CHAPTER 30

Content Advisor

In this chapter

Content Advisor Overview 520
Understanding Content Ratings 520
RSACi Content Ratings 520
Other Rating Systems 521
Supervisor Password 522
Configuring Content Advisor 522
Deploying Content Advisor Settings to User Groups 526
Locking Down Content Advisor Settings 528
Managing Content Advisor Settings for Deployed Browsers 529

Content Advisor Overview

Just as parents want assurances that children cannot visit Web sites that display inappropriate content, businesses often want to block the use of sites that offer no business value to their employees. To help meet these needs, the Content Advisor in Internet Explorer 4 can be used to control the types of content available through the browser. Parents or system administrators can adjust the content rating settings to reflect what they think is appropriate content in four areas: language, nudity, sex, and violence. Users can also subscribe to independent ratings bureaus and use third-party ratings to control access to Web content.

System administrators can use the Internet Explorer Administration Kit (IEAK) 4 Configuration Wizard to build and deploy custom packages with pre-configured Content Advisor settings for their user groups. Settings can also be locked down so they cannot be altered by end users. After browsers are deployed, administrators can use the IEAK Profile Manager to update Content Advisor settings through the automatic browser configuration feature of Internet Explorer.

Understanding Content Ratings

When you enable the Content Advisor, Internet Explorer 4 reads special tags placed in the HTML code of Web pages by content providers to determine whether that page meets your criteria for suitable content.

The most common content ratings are based on the Platform for Internet Content Selection (PICS) standard for defining and rating systems. PICS is an industry-developed technical standard that uses HTML meta tags to block access to Web pages based upon the values of the meta tags. For more information about PICS, visit **http://www.w3.org/PICS/**.

Internet Explorer 4 comes installed with the PICS-based RSACi content rating system. You can also subscribe to independent PICS ratings from other ratings bureaus. Or, you can import other content rating systems that meet your needs.

RSACi Content Ratings

RSACi is an open, objective, content rating system developed by the Recreational Software Advisory Council (RSAC), an independent, nonprofit organization. The RSACi system provides users with information about the level of sex, nudity, violence, offensive language (vulgar or hate-motivated) in software games and Web sites. For more information about RSAC and RASCi, see **http://www.rsac.org/**.

The following table shows the five levels of the RASCi rating system and describes the content *allowed* for each level in the four areas of content: language, nudity, sex, and violence. Level 0 is the most restrictive and level 4 the least restrictive.

Level	Violence Rating	Nudity Rating	Sex Rating	Language Rating
4	Rape or wanton, gratuitous violence	Frontal nudity qualifying as provocative display	Explicit sexual acts or sex crimes	Crude, vulgar language, or extreme hate speech
3	Aggressive violence or death to humans	Frontal nudity	Nonexplicit sexual acts	Strong language or hate speech
2	Destruction of realistic objects	Partial nudity	Clothed sexual touching	Moderate expletives or profanity
1	Injury to a human being	Revealing attire	Passionate kissing	Mild expletives
0	None of the above, or sports related	None of the above	None of the above or innocent kissing; romance	None of the above

You can set content ratings at any level from level 0 to level 4 in each of the four content areas. All content ratings are set at level 0 by default. When the Content Advisor is on and the PICS rating for a Web page exceeds the rating level you specify, users are prevented from accessing the page.

Web site publishers can obtain PICS content ratings from RSAC as well as a number of other nonprofit and fee-based ratings services. PICS ratings can be voluntarily added to Web sites by publishers.

You can also obtain independent PICS ratings from ratings bureaus. Ratings bureaus are typically fee-based and specialize in rating Internet sites. You can specify a ratings bureau for Internet Explorer to use to obtain PICS ratings for Web pages. Since Internet Explorer must contact the ratings bureau to obtain ratings, using ratings bureaus can slow down access to Web pages considerably.

You can configure Internet Explorer to prevent users from accessing Web pages without content ratings, or you can allow users to view unrated pages. For more information, see "Configuring Content Advisor" later in this chapter.

Other Rating Systems

Some Web publishers may rate their sites using rating systems that are not based on PICS. To use rating systems that are not based on PICS, you must subscribe to ratings services that support the non-PICS rating system and then import the rating system so Internet Explorer can use it to rate Web content. For more information, visit the Web sites of the ratings services and see "Configuring Content Advisor" later in this chapter.

Supervisor Password

The first time you turn Content Advisor on, you'll need to specify a supervisor password. The supervisor password allows administrators or supervisors to turn Content Advisor on or off and change Content Advisor settings for users.

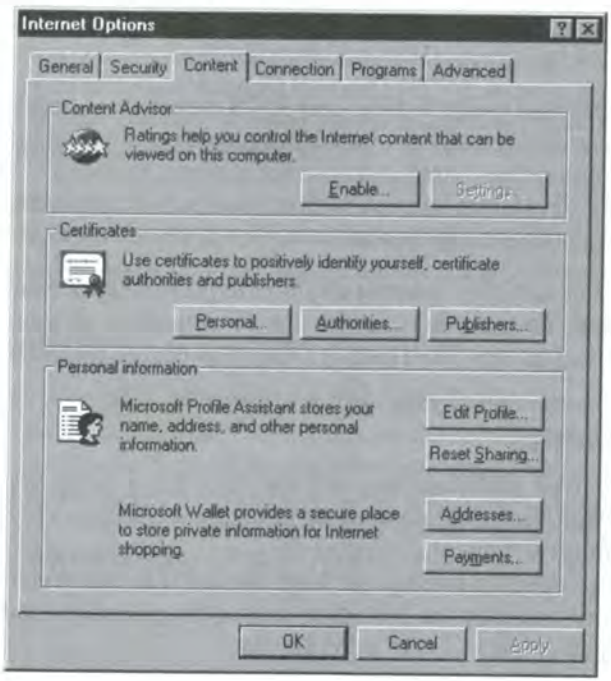
In addition, you can configure Internet Explorer to allow users to display restricted Web pages by typing the supervisor password. When users attempt to access restricted content, the **Content Advisor** dialog box queries users to enter the supervisor password to optionally view restricted content. Or, you can also disable the option to enter the supervisor password to view restricted content. For more information, see "Configuring Content Advisor" later in this chapter.

Configuring Content Advisor

The Content Advisor is turned on and off by using the **Content** tab. You can use the Content Advisor **Ratings**, **General**, and **Advanced** tabs to configure the Content Advisor settings Internet Explorer uses to restrict user access to Web content.

▶ **To access the Content Advisor**

1. From the **View** menu, click **Internet Options**.
2. Click the **Content** tab.



▶ **To turn on Content Advisor**

1. On the **Content** tab, under **Content Advisor**, click **Enable**.
2. Enter the ***supervisor password*** when queried.

   The Content Advisor controls users' access to restricted Web content.

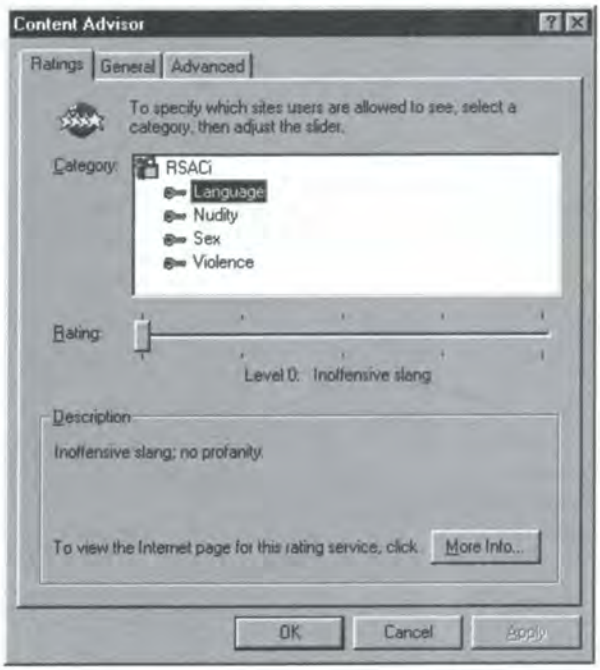
▶ **To turn off Content Advisor**

1. On the **Content** tab, under **Content Advisor**, click **Disable**.
2. Enter the ***supervisor password*** when queried.

   The Content Advisor no longer restricts Web content.

▶ **To configure content ratings**

1. On the **Content** tab, under **Content Advisor**, click **Settings**.
2. In the **Content Advisor** dialog box, on the **Ratings** tab, select the **Language**, **Nudity**, **Sex**, or **Violence** ratings category.

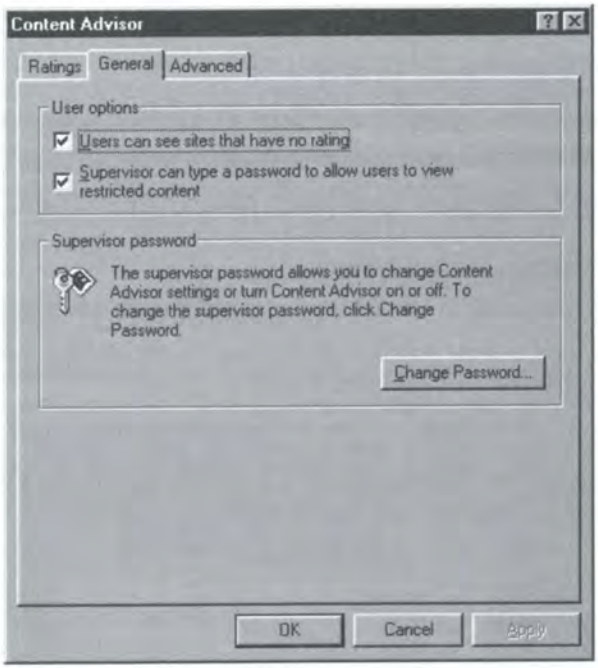


3. Click the **Rating** slider, and move the slider to the content level you want to allow users to access for the ratings category.

   The default settings for each content category is level 0, which is the most restrictive setting. Level 4 is the least restrictive setting. For more information about ratings levels, see "Content Ratings" earlier in this chapter.

▶ **To configure user options**

1. In the **Content Advisor** dialog box, click the **General** tab.
2. Select the **User options** you want.



Option	Description
Users can see sites that have no rating	Clear to restrict access to Web pages that are not rated. Select to allow users to display Web pages that are not rated.
Supervisor can type a password to allow users to view restricted content	Clear to prevent users from optionally viewing restricted content by entering the supervisor password. Select to query users for the supervisor password when they attempt to view restricted content. When selected, users can display restricted content by entering the supervisor password at the **Content Advisor** dialog box.

▶ To change the supervisor password

1. In the **Content Advisor** dialog box, on the **General** tab, click **Change Password**.
2. In the **Old password** box, type the old supervisor password to verify that you are authorized to change Content Advisor settings.



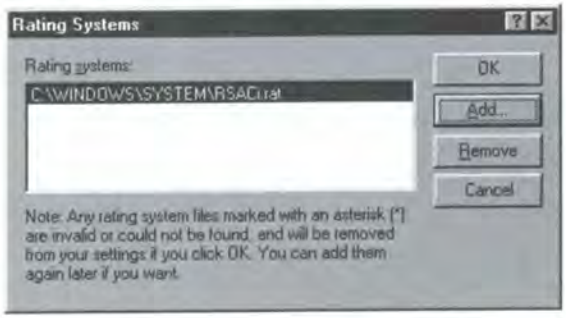
3. In the **New password** box, type the new password.
4. In the **Confirm new password** box, type the new password again.
5. Click **OK**.

▶ To import new rating systems and ratings bureaus

1. If necessary, install rating systems files following the directions provided by the ratings service.
2. In the **Content Advisor** dialog box, click the **Advanced** tab.



3. Click **Rating Systems**.
4. In the **Rating Systems** dialog box, select the rating system's rating (.rat) file from the list, and click **Add**.



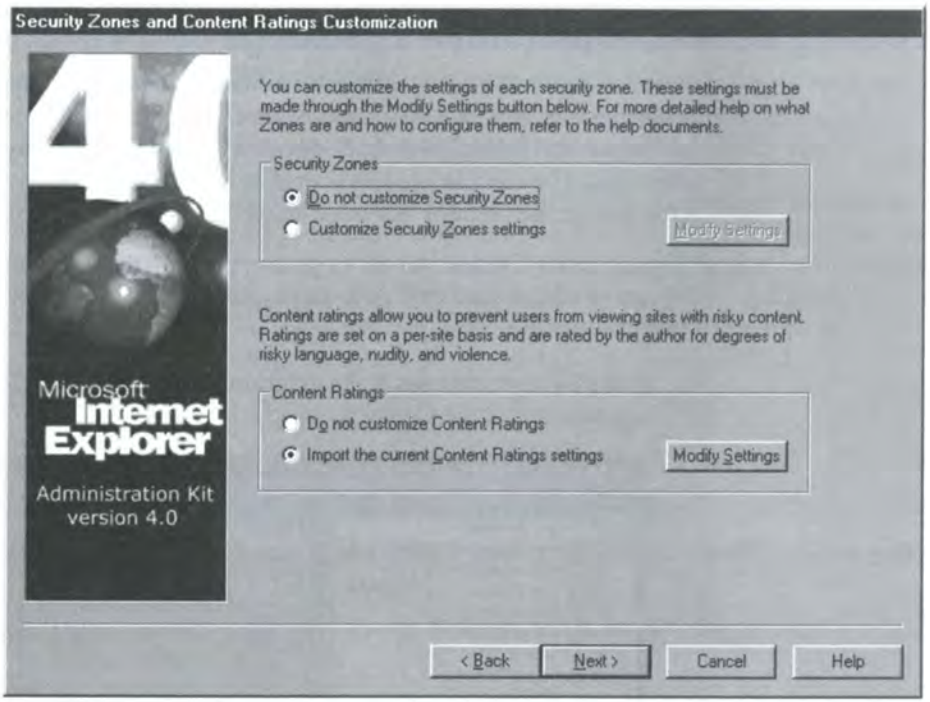
5. If this service uses a ratings bureau, select the ratings bureau from the **Ratings bureau** list.
6. Click **OK**.

You can now use the new rating system to set Web content restrictions following the instructions provided by the ratings service.

Deploying Content Advisor Settings to User Groups

Administrators can use the IEAK Configuration Wizard to build and deploy custom packages with pre-configured Content Advisor settings for user groups. (For more information, see "Building Custom Packages" in Chapter 36.)

You start by configuring the Content Advisor settings on the computer running the IEAK Configuration Wizard and then import the settings using the **Security Zones and Content Ratings Customization** page of the wizard. You can also open the Content Advisor and modify the settings from the **Security Zones and Content Ratings Customization** page.



▶ **To import Content Advisor settings**

1. On the **Security Zones and Content Ratings Customization** page, select **Import the current Content Ratings settings**.
2. To modify the current Content Advisor settings, click **Modify Settings** and use the Content Advisor **Ratings**, **General**, and **Advanced** tabs to configure the Content Advisor settings. (For more information, see the previous section.)
3. Click **Next**.
4. Finish building the custom package.

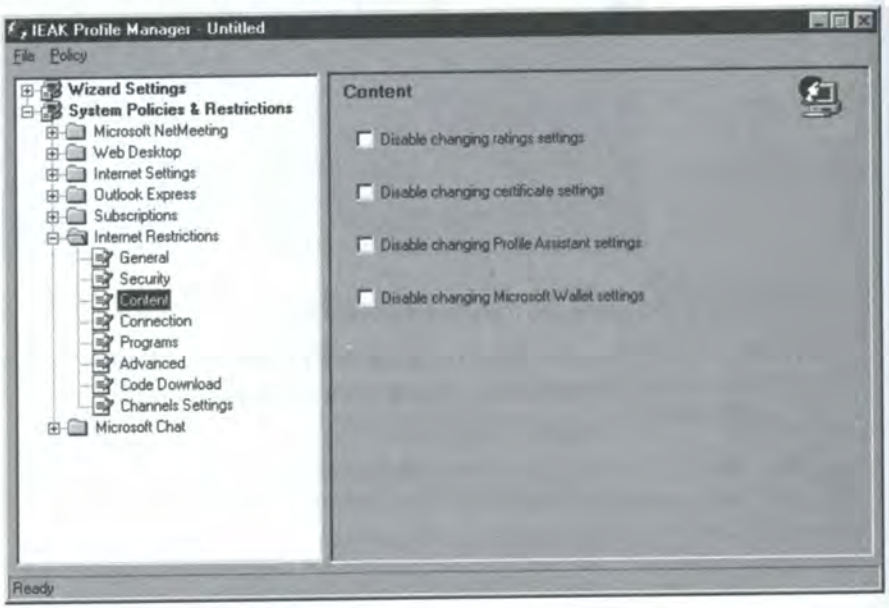
The Content Advisor configuration you import from the current desktop will then be installed on users' desktops when the custom package is deployed. You can also lock down Content Advisor settings so users cannot modify the settings even if they know the supervisor password.

Locking Down Content Advisor Settings

You can use the IEAK Configuration Wizard to build and deploy custom packages and lock down Content Advisor settings so users cannot modify the settings even if they know the supervisor password. After browsers have been deployed, you can use the IEAK Profile Manager to lock down Content Advisor changes for user groups that have automatic browser configuration implemented.

To lock down Content Advisor options, perform the following steps at the **System Policies and Restrictions** page of the IEAK Wizard or at the IEAK Profile Manager:

1. In the **System Policies & Restrictions** hierarchy, select **Internet Restrictions**, and then select the **Content** object.



Note The IEAK Profile Manager is shown here, but the **System Policies and Restrictions** page of the IEAK Configuration Wizard works similarly.

2. In the **Content** pane, select **Disable changing ratings settings** to prevent users from changing Content Advisor settings even if they know the supervisor password.
3. Save your changes to the auto-configuration (.ins) file or finish building the custom package, as appropriate.

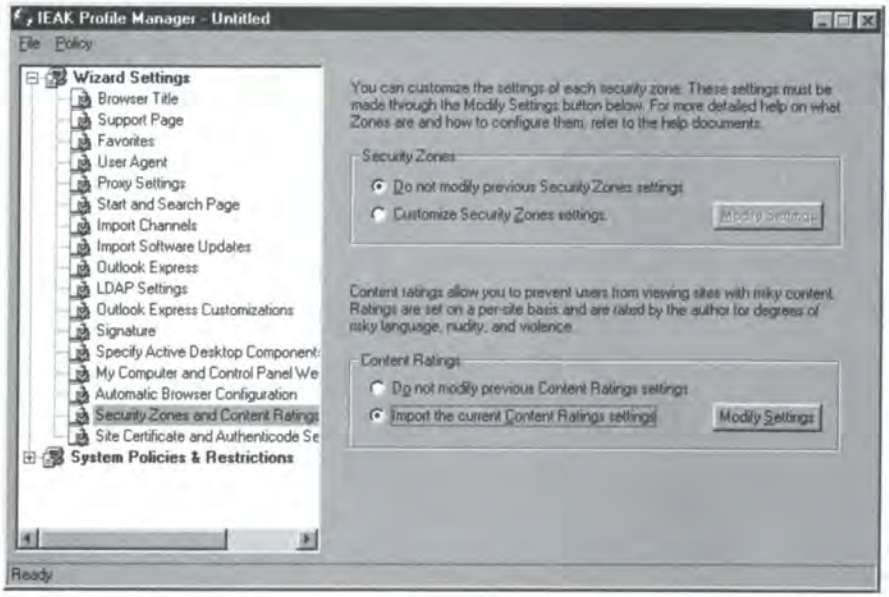
Managing Content Advisor Settings for Deployed Browsers

You can use the IEAK Profile Manager in conjunction with automatic browser configuration to update Content Advisor settings for deployed browsers. (For more information, see "Building Custom Packages" in Chapter 36.)

To change Content Advisor settings for a user group, you configure the Content Advisor settings on the machine running the IEAK Profile Manager and then use the Profile Manager to import the configuration. Then save the new configuration settings to the auto-configuration files for the user group. When automatic browser configuration is refreshed at users' computers, users' desktops are configured with the new Content Advisor settings you have specified.

▶ **To change Content Advisor settings for a user group**

1. Run the IEAK Profile Manager.
2. Open the auto-configuration (.ins) file for the user group.
3. In the left pane, select **Wizard Settings**, and then select **Security Zones and Content Ratings Customization**.
4. In the right pane, under **Content Ratings**, select **Import the current Content Ratings settings**.



5. Click **Modify Settings**, and use the **Content Advisor Ratings**, **General**, and **Advanced** tabs to configure the Content Advisor settings. (For more information, see "Configuring Content Advisor" earlier in this chapter.)
6. On the **File** menu, click **Save** to save changes to the auto-configuration file.

Changes are made to users' configurations as scheduled by automatic browser configuration.

CHAPTER 31

User Privacy

In this chapter

Understanding User Privacy 532
- Secure Communications 532
- Zone-Based Password Security Protection 532
- Control over Cookies 533
- Profile Assistant 533
- Microsoft Wallet 535

Configuring Privacy Options 536
- Configuring Profile Assistant 537
- Configuring Microsoft Wallet 538
- Configuring User Privacy Security Options 541

Understanding User Privacy

Internet Explorer 4 supports a wide range of Internet privacy standards and provides many features and options to help ensure user privacy on the Web. When you communicate over the Web, you want to know that what you send and receive cannot be intercepted or deciphered and that your passwords and other private information cannot be used by others. You also want to be sure that nobody can access information on your computer without your knowledge. Internet Explorer 4 protects your privacy in two key ways: it supports the latest Internet security and privacy standards; and it provides encryption and identification capabilities that ensure the Internet e-mail you send cannot be read or tampered with.

Secure Communications

Internet Explorer 4 supports the latest Internet security standards to block anyone from eavesdropping on your electronic communications. It supports the Secure Sockets Layer (SSL) and Private Communications Technology (PCT) protocols, so you can securely send information over the Internet. SSL and PCT protocols are used to create a secure channel that prevents anyone from eavesdropping on your communications over the Web.

When a Web site you are browsing supports SSL or PCT, Internet Explorer displays a lock icon in the browser's status bar at the bottom of your computer screen. When you see this lock, you know that you can safely send information over the Internet to the site you are browsing. You can configure Internet Explorer to allow SSL and PCT communications. For more information, see "Configuring User Privacy Security Options" later in this chapter.

In addition, Outlook™ Express (the e-mail and newsgroup program in Internet Explorer 4) also lets you encrypt your messages and use a personal digital signature to ensure that your identity is protected over the Internet. For more information on Outlook Express, see Chapter 18.

Zone-Based Password Security Protection

Internet Explorer prompts you before you transmit your user name or password to sites you haven't designated as Trusted in the security zones settings. For sites you do trust, you can configure security zones to send information without prompting you. For more information on security zones, see Chapter 27, "Security Zones."

Control over Cookies

An HTTP cookie is a small file that an individual Web site stores on your computer to provide customization features. For example, when you set custom settings on MSN™, The Microsoft Network, that information is stored in a cookie file on your computer. MSN then reads the cookie each time you visit the site. That's how MSN knows which options to display.

You can configure Internet Explorer to handle cookies in the following ways:

- Prevent cookies from being stored on your computer.
- Query you whether you want to accept cookies from the site.
- Allow cookies to be stored on your computer without notifying you.

For more information, see "Configuring User Privacy Security Options" later in this chapter.

Note Accepting a cookie does not give a Web site access to your computer or any personal information about you other than what you have specified in the customized settings for that site.

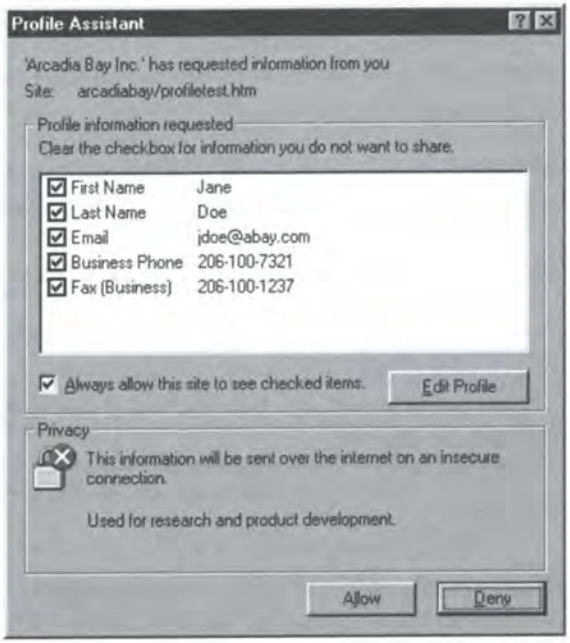
Profile Assistant

The Profile Assistant makes it easy for you to share registration and demographic information with Web sites that request this information, while maintaining your privacy and safety. The Profile Assistant saves you from having to repeatedly enter the same information, such as your name and e-mail address, every time you visit a new Web site. None of this information can be viewed on your computer or shared with others without your permission.

The Profile Assistant supports the Internet privacy model defined by the Platform for Privacy Preferences (P3), a World Wide Web Consortium (W3C) project. Basically, the P3 privacy model enables personal information to be exchanged between users and Web sites, while respecting the user's right to privacy. Users can store personal information in user profiles in secure, encrypted information stores on their computers and can choose whether to share the information upon request. Web sites can request information from users' profiles, but are not allowed to access profile information unless the users consent. Since the Profile Assistant complies with the Internet's P3 privacy standards, it can also work with other Internet programs and servers. (For information about how to write scripts to access Profile Assistant information, see the *Microsoft Internet Client SDK*.)

When a Web site requests information from your user profile, the **Profile Assistant** dialog box opens.

You can use the **Profile Assistant** dialog box to verify who is requesting information, choose which information (if any) to share, and understand how the Web site intends to use the information.



Option	Description
'*Requester name*' has requested information from you	Displays the name of the requester. This can be an individual or an organization.
Site	Displays the URL of the site requesting information from the user profile.
Profile information requested	Displays the list of information items requested. In the example shown: **First Name**, **Last Name**, **Email**, **Business Phone**, and **Fax (Business)**. Clear the check box for any items you don't want to send to the requester.

Option	Description
Always allow this site to see checked items	Select this option to add this site to a list of sites you allow to access your Profile Assistant information without notifying you. You can clear the list from the **Content** tab by clicking the **Reset Sharing** button.
Edit Profile	Click this button to open the **User Profile** dialog box where you can edit the profile information to be sent to this site. For example, you could change your fax number to send a new fax number to the site.
Privacy	Displays a message explaining whether the information you are sharing will be secure when it is sent over the Internet. It also displays a message describing how the requester intends to use this information.

Web sites can request up to 29 different items of information from your user profile. For more information, see "Configuring Profile Assistant" later in this chapter.

Microsoft Wallet

Microsoft Wallet is a software payment program that you can used to conduct secure financial transactions over the Web with sites that support the Wallet. You can use the Wallet to securely store private information, such as credit card account information, for making payments over the Internet. You decide what to put in Microsoft Wallet, who gets to see it, and who gets to use it. Once you've entered information into Microsoft Wallet, you'll never have to retype it.

The Wallet includes a protected storage area where your private information is stored. The information in the Wallet's protected storage area is encrypted and can only be accessed and viewed by you.

The Wallet supports all industry-standard payment methods, including Secure Sockets Layer (SSL) and Secure Electronic Transaction (SET), to enable the secure, electronic use of credit cards. The Wallet also supports add-on payment methods, such as digital cash and electronic checks, as required by merchants and financial institutions. Users obtain the payment method add-on and instructions on how to install and use the add-on from the appropriate merchant or financial institution.

The Wallet provides the **Address Options** dialog box and the **Payment Options** dialog box to store your address and payment information separately. You can use the **Address Options** dialog box to enter, store, and access addresses that can be referenced for shipping and billing during online order entry. Names, e-mail addresses, and telephone numbers of Wallet users can be viewed in the Address Book.

You can use the **Payment Options** dialog box to enter, securely store, and access various types of payment methods for making online purchases. This information is protected with a password you define. When you shop at an Internet store that supports the Wallet, the site may prompt you to select payment methods stored in the Wallet and authorize payment by typing your password.

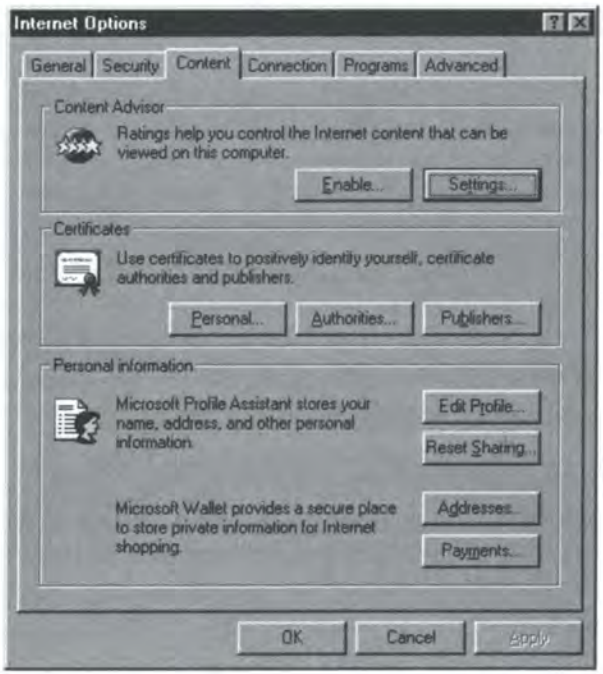
For more information, see "Configuring Microsoft Wallet" later in this chapter.

Configuring Privacy Options

To configure the Internet Explorer privacy options, use the **Content** and **Advanced** tabs.

▶ **To open the Content tab**

1. From the **View** menu, click **Internet Options**.
2. Click the **Content** tab (or, when you're ready, click the **Advanced** tab).

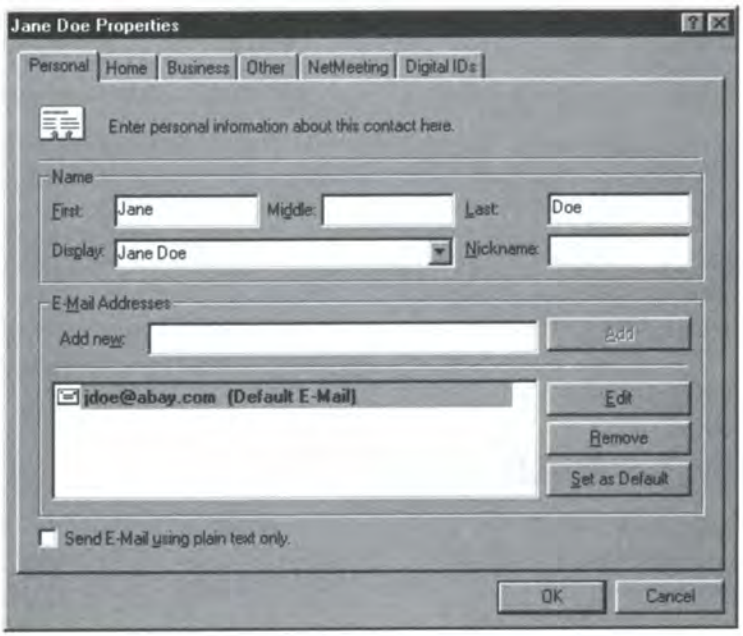


Configuring Profile Assistant

You can use the **User Profile** dialog box to configure your user profile to share with Web sites. The **User Profile** dialog box contains six tabs and is used by other Internet programs, including NetMeeting™ conferencing software and Outlook Express. The Profile Assistant uses information from the **Personal**, **Home**, **Business**, and **Other** tabs to create your user profile. You can access the **User Profile** dialog box from the **Content** tab.

▶ **To create or edit a user profile**

1. On the **Content** tab, click **Edit Profile**.
2. In the appropriate boxes on the **Personal**, **Home**, **Business**, and **Other** tabs, type the information you want to share.



User profiles can include the following information:

Personal Tab	Home Tab	Business Tab	Other Tab
First name	Home street address	Company name	Notes
Middle name	Home city	Business street address	
Last name	Home state/province	Business city	
Display name	Home zip code	Business state/province	
	Home country	Business country	
Default e-mail address	Home phone	Business zip code	
	Home fax	Job title	
	Home cellular phone	Department	
	Gender	Office	
	Personal Web page URL	Business phone	
		Business fax	
		Business pager	
		Business Web page URL	

3. Click **OK**.

   The Profile Assistant creates your user profile using the information you specify and saves the profile in the protected information store.

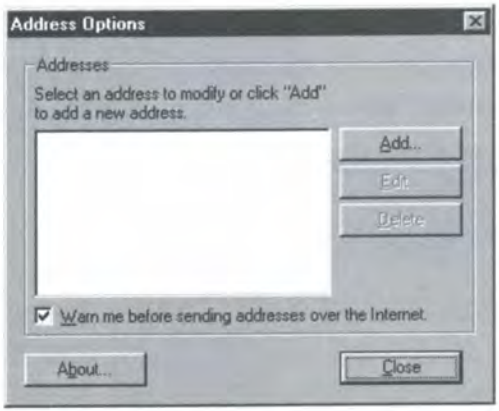
You can use the **Advanced** tab to disable sites from requesting the information in the Profile Assistant. For more information, see "Configuring User Privacy Security Options" later in this chapter.

Configuring Microsoft Wallet

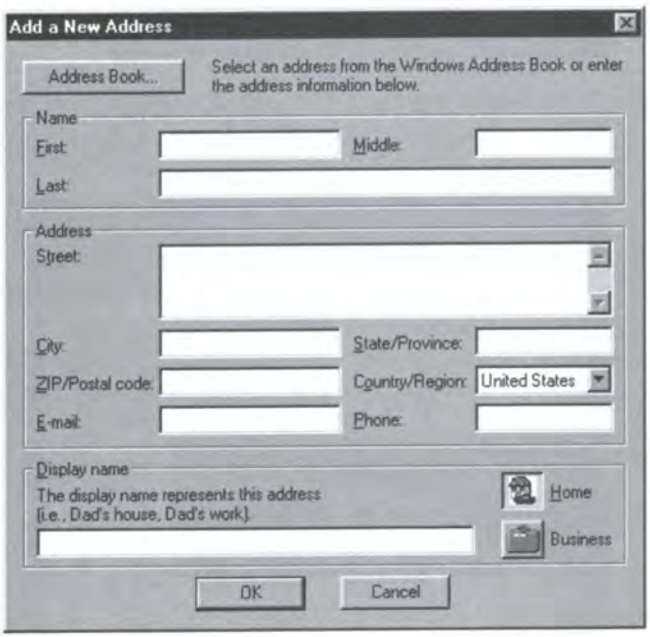
You can use the Microsoft Wallet **Address Options** and **Payment Options** dialog boxes to configure the information you can use for payments over the Internet. You can access the Wallet dialog boxes from the **Content** tab.

▶ **To add or edit addresses used for payments**

1. On the **Content** tab, click **Addresses**.
2. Click **Add** to add a new address or **Edit** to edit an existing address.



3. In the **Add a New Address** dialog box, type the Name and Address information, or click **Address Book** to select an existing address from the Address Book.

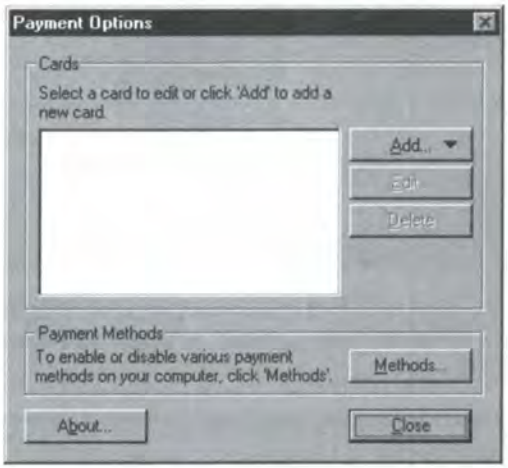


Note The **Add a New Address** dialog box is shown here, but the **Edit a New Address** dialog box is identical except for the title.

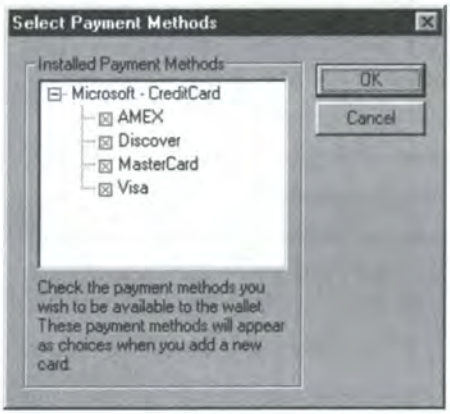
4. In the **Display name** box, type a display name to be used for this address.
5. Click **Home** to indicate a home address, or click **Business** to indicate a business address.
6. Click **OK**.

▶ **To add payment methods to the Wallet**

1. On the **Content** tab, click **Payments**.
2. On the **Payment Options** dialog box, click **Methods**.



3. On the **Select Payment Methods** dialog box, from the **Installed Payment Methods** list, select the credit cards you want to be available to the Wallet.



4. Click **OK**.

   These credit cards become available, so you can now use the **Payment Options** dialog box to add your personal account information to the Wallet.

▶ **To add personal credit card information**

1. In the **Payment Options** dialog box, click **Add** to add a credit card to the list of payment options.
2. On the list of credit cards, click the credit card you want to add and use the Add a New Credit Card Wizard to add the credit card.



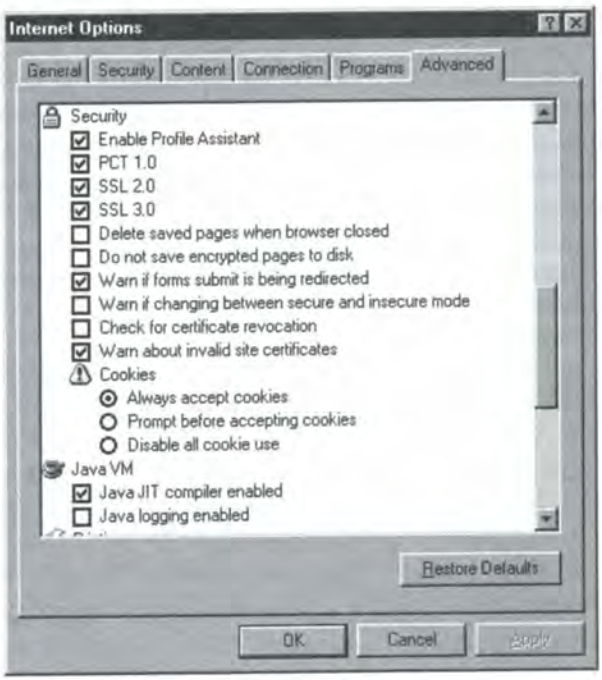
You must provide your credit card account information and a password. You will need to enter this password before you can use the credit card to make a payment or edit the credit card information. This way, another person cannot sit down at your computer to make purchases on the Internet. Internet Explorer encrypts and stores this information in the Wallet's protected storage area.

Configuring User Privacy Security Options

You can configure a variety of user-privacy security options for Internet Explorer. These options appear in the **Advanced** tab, under the **Security** object.

▶ **To configure advanced security options**

1. From the **View** menu, click **Internet Options**.
2. Click the **Advanced** tab.
3. Select or clear options under the **Security** object.



Option	Description
Enable Profile Assistant	Clear to prevent sites from requesting user profile information. When this check box is cleared, you will not be queried to provide information to Web sites.
PCT 1.0	Select if you want to send and receive secured information through PCT, a protocol developed by Microsoft that is significantly more secure than SSL 2. Note that some Web sites might not support this protocol.
SSL 2.0	Select if you want to send and receive secured information through SSL Level 2, the standard protocol for secure transmissions. All secure Web sites support this protocol.
SSL 3.0	Select if you want to send and receive secured information through SSL Level 3, a proprietary protocol that is intended to be more secure than SSL 2. Note that some Web sites might not support this protocol.
Delete saved pages when browser closed	Select to delete all secure Web pages from the Internet Explorer cache whenever you exit Internet Explorer. You cannot browse secure Web sites or Active Channel content offline after secure pages have been deleted from the cache.
Do not save encrypted pages to disk	Select to specify that secured information is not saved to your hard disk. This is useful if you are using Internet Explorer from a shared server and you do not want other people to see your secure information.
Warn if forms submit is being redirected	Select for Internet Explorer to query you whether to submit a Web-based form if the information is sent to a different Web location than the one on which the Web page form resides.
Warn if changing between secure and insecure mode	Select for Internet Explorer to warn you when you are switching between Internet sites that are and are not secure.
Check for certificate revocation	Select for Internet Explorer to check digital certificates from Web sites to see if they have been revoked before accepting certificates as valid.
Cookies	
Warn about invalid site certificates	Select for Internet Explorer to warn you when addresses (URLs) in digital certificates from Web sites are not valid.
Always accept cookies	Select if you want Internet Explorer to accept cookies without prompting you first.
Prompt before accepting cookies	Select for Internet Explorer to query you whether you want to accept a cookie from a Web site.
Disable all cookie use	Select to prevent cookies from being stored on your computer. When selected, Web site requests to store cookies are automatically denied without notifying you.

4. Click **OK**.

PART 8

Internet Explorer 4 Accessibility

Microsoft® Internet Explorer 4 introduces a number of advances that make the Web more accessible to computer users with disabilities. In particular, several features allow users to customize the appearance of Web pages to meet their own needs and preferences. Internet Explorer 4 also includes the best features of Internet Explorer 3, including the ability to navigate the Web using the keyboard. Users without disabilities may also be interested in many of these options as ways to customize colors and fonts to their own tastes or to save time using keyboard shortcuts. Part 8 describes the features in Internet Explorer that support enhanced accessibility and explains how to use them to accommodate different accessibility needs.

Chapter 32: Accessibility Overview

This chapter outlines the accessibility benefits offered by the new features in Internet Explorer 4 and lists some upgrade considerations for users transitioning from Internet Explorer 3. It also offers an outline of accessibility features and functions that are recommended for users with different types of disabilities, including users who are blind, have low vision, are deaf or hard-of-hearing, have physical impairments, have seizure disorders, or have cognitive or language impairments. In addition, this chapter provides an extensive list of other accessibility resources, including telephone numbers, postal addresses, and Web sites.

Chapter 33: Accessibility Features and Functionality

This chapters details procedures and shortcut keys for using keyboard navigation of the Internet Explorer browser, the Windows® Desktop Update, the Internet Explorer Help tool, and Web pages. Plus, it offers shortcut keys for the new AutoComplete feature. It details procedures for customizing the display of fonts, colors, and formatting on Web pages, the Help tool, and on the Windows Desktop Update. It also explains how to configure a wide range of advanced Internet accessibility options, such as disabling or enabling sounds, graphics, and

animations; the use of smooth scrolling; and the treatment of hyperlinks. The last section discusses the accessibility features of NetMeeting™ and offers keyboard shortcuts.

Note Not all accessibility features were completed when Internet Explorer 4.0 first shipped. Internet Explorer 4.01 contains significant accessibility enhancements. The information presented in Part 8 assumes users are working with version 4.01. To find version information about your current copy of Internet Explorer, go to the **Help** menu, and select **About Internet Explorer**. If it says, "Version 4.72.2106.8," or later, then you are using Internet Explorer 4.01. Version 4.01 is available for free download at **http://www.microsoft.com/ie/ie40/download/**. For Active Setup information, to easily download just the updated files you need, see Part 1, Chapter 2, "Phase 1: Active Setup."

CHAPTER 32

Accessibility Overview

In this chapter

Accessibility Benefits 546
Upgrade Considerations 548
Suggested Features for Different Types of Disabilities 549
- Features for Users Who Are Blind 549
- Features for Users with Low Vision 550
- Features for Users Who Are Deaf or Hard-of-Hearing 551
- Features for Users with Physical Impairments 552
- Features for Users with Seizure Disorders 553
- Features for Users with Cognitive and Language Impairments 553

Accessibility Resources 554

Accessibility Benefits

Microsoft is committed to making computers easier to use for everyone, including individuals with disabilities. In recent years, Microsoft has established close relationships with users who have disabilities, organizations representing such individuals, workers in the rehabilitation field, and software developers who create products for this market. Internet Explorer 4 includes many new features that benefit users with disabilities. The most important new features allow users to:

- **Control how Web pages are displayed.** You can customize the colors of background, text, and hyperlinks based on your preference. You can control the size and typeface of fonts for all the Web pages you view by installing your own style sheet. Style sheets can also be used to make headings larger or to highlight italicized text with a different color. Any feature you choose for Web pages can also be used with the Active Desktop™ interface, Windows Explorer, and Internet Explorer Help. Users who like large fonts can also take advantage of the new scrolling menus, which prevent large menus from running off the screen.
- **Work better with screen readers and other accessibility aids.** Internet Explorer uses the new HTML 4 standard, which lets Web-page designers add additional information, such as the name of an image or control, that is useful to blind individuals who use screen readers. You can choose to turn off smooth scrolling and other effects that can confuse screen-reading utilities. The Dynamic HTML Object Model in Internet Explorer 4 makes possible exciting new classes of add-on utilities for Internet Explorer. Some, such as PowerToys, provide important features for users with disabilities. PowerToys offer the ability to zoom in on Web pages, view a framed page in its own frame, and conduct searches more easily. (For more information about PowerToys, visit **http://www.microsoft.com/ie/ie40/powertoys/**.)
- **Reduce the amount of typing required.** Using the AutoComplete feature, Internet Explorer 4 makes it easier for users to enter long or repetitive URLs. AutoComplete finishes typing URLs based on a cached history of sites you've visited before and an automatic domain-searching feature. Explorer bars for Search, History, Favorites, and Active Channels make it easier to find the things you need, things you've seen, or Web pages you use most often. The improved QuickLinks toolbar makes it even easier to return to the sites you visit the most.

- **Customize layout to make it easier to perform the tasks you need.** The Windows Desktop Update, an optional set of features of Internet Explorer 4, allows you to further customize your desktop, **Start** menu, and taskbar. Choose from a range of desktop toolbars, or create your own. Your Web **Favorites** menu can now be accessed from the **Start** menu, for faster access to the sites you choose. The new Address bar allows you to enter URLs directly from your Windows desktop, without having to launch the browser first. Shortcuts to the programs and folders you use the most can be set in a custom, dockable toolbar, for one-click access any time.
- **Have the information you need "pushed" to you.** The Webcasting features in Internet Explorer 4 allow you to spend less time searching and less effort navigating. Now you can subscribe to Web sites and be automatically notified of updates to the site. You can even schedule automatic downloads of updated information for easy, offline viewing. (For more information, see Part 4, "Information Delivery: Webcasting.")
- **Get better feedback.** Two new sound events, Start Navigation and Complete Navigation, have been added to the sounds list in Control Panel to signal when a Web page begins loading and when it finishes loading. These optional sounds can be helpful to users who are blind or have low vision. You can also set the appearance of hyperlinks to show when they are activated or rolled over with a mouse.
- **Use a mouse with greater ease.** With the Windows Desktop Update, you can choose to single-click instead of double-clicking to initiate common computer operations such as opening folders. And you can put the most commonly used commands and shortcuts on desktop toolbars where they are always one click away.
- **Communicate.** Microsoft NetMeeting delivers a complete Internet conferencing solution that can greatly enhance accessibility for users with a wide range of disabilities. NetMeeting users can experience the benefits of real-time, multipoint communication that allows them to collaborate and share information with two or more conference participants at the same time. NetMeeting offers a powerful set of data conferencing features, as well as audio and video conferencing.

In addition, features carried over from Internet Explorer 3 include the ability to:

- **Navigate with the keyboard.** Users can key through pages, panes, hyperlinks, toolbars, and other controls.
- **Replace images with textual descriptions.**
- **Turn off pictures, videos, and sounds.**
- **Use the High Contrast option.** This Windows option allows users to choose a simple color scheme and omit images that make text difficult for them to read.

Upgrade Considerations

Significant changes in architecture between Internet Explorer 4 and Internet Explorer 3 may affect the functionality of certain accessibility aids written for version 3. It is recommended that users test Internet Explorer 4 with their equipment to determine the specific places where its behavior differs from version 3. Also contact the vendor of your adaptive aids to find out how they work with Internet Explorer 4. The modular structure of Internet Explorer 4 makes it easy to customize the feature set by installing or uninstalling components based on the functionality that works best for you. Many features can also be turned on or off, according to your preferences.

Depending on each person's specific needs, different users may find challenges with different aspects of Internet Explorer 4, but the following list details a few general considerations when upgrading to version 4:

- Users who rely on keyboard navigation should be aware that the Help tool in Internet Explorer 4 works differently than in Internet Explorer 3. Most of the functionality is available through the keyboard, although some features, such as hyperlinks, are not accessible from the keyboard. All hyperlinked topics, however, are also listed in the Help Contents and Index, which are completely accessible from the keyboard.
- When navigating to a Web page, Internet Explorer 4 always sets the keyboard focus to the beginning of the page. When returning to a visited page, Internet Explorer 4 resets the keyboard focus to the beginning of the page. Internet Explorer 3 would allow you to continue navigating from the point of your last link—the last place you had visited on the page.
- Internet Explorer 4 allows you to navigate through links using the TAB key, just as you did in version 3. However, version 4 will also allow navigating to objects that are not currently visible on the screen. This may result in the keyboard focus seeming to "disappear" at times. Simply pressing TAB additional times will bring it back into view.
- The Windows Desktop Update in Internet Explorer 4 replaces the traditional **Start** menu with a scrolling **Start** menu that supports dragging, so that menu items can be rearranged. However, this type of menu limits the number of menu commands visible at one time to those that fit in a single column. Although long menu lists won't display all at once, all menu items are navigable by keyboard. Still, users who need to keep as many options as possible on the screen at one time and who currently have many commands on their **Start** menu may want to remove some commands from the **Start** menu and use the new desktop toolbar, the Quick Launch toolbar, or the custom toolbar feature to make those commands available from other places on the desktop. (See Part 3, Chapter 12, "Start Menu and Taskbar" for more information.)

- Users may have some difficulty reading the descriptions of images when the images are not displayed. Internet Explorer 3 allowed you to choose to display the entire description, whereas version 4 may cut off portions of those descriptions. Internet Explorer support for HTML 4, however, now allows you read the full descriptions of images while they are displayed.
- Internet Explorer 4 uses menus and check boxes that may not be described correctly by some blind-access utilities. If you choose the Windows Desktop Update option when installing Internet Explorer, these menus will also be used in Windows Explorer. It is recommended that you test these features with your adaptive aid to see if there any problems. Also contact the vendor of your aid to find out if there are any upgrades that may better support Internet Explorer 4.

Suggested Features for Different Types of Disabilities

The following lists are suggestions of features that may be useful to users with certain types of disabilities. These lists are not complete, as the needs and preferences of individuals vary, and many people have a combination of disabilities or differing abilities.

Features for Users Who Are Blind

Many users who are blind use screen readers—assisting software that provides a spoken or Braille description of windows, controls, menus, images, text, and other information that is typically displayed visually on a screen. Internet Explorer 4 provides improved functionality for screen readers and offers a range of other features and options that can be helpful to blind individuals.

The list below recommends specific settings and features that can benefit users who are blind. To learn about any of these features or for procedures that explain how to configure a certain setting, see the next chapter, "Accessibility Features and Functionality."

- Use keyboard navigation for Internet Explorer, Web pages, the Active Desktop, Internet Explorer Help, and NetMeeting.
- Use the Accessibility options on the **General** tab of the **Internet Options** dialog box to:
  - Ignore colors specified on Web pages.
  - Ignore font styles specified on Web pages.
  - Ignore font sizes specified on Web pages.
  - Format documents using your own style sheet.

- Use the **Advanced** tab on the **Internet Options** dialog box to:
  - Always expand alternate text for images.
  - Move the system caret with focus/selection changes.
  - Disable smooth scrolling.
  - Select not to show pictures in Web pages.
  - Select not to play animations in Web pages.
  - Select not to play videos in Web pages.
  - Disable smart image dithering.
- Use the **Sounds Properties** dialog box from Control Panel to:
  - Assign a sound to the Start Navigation event.
  - Assign a sound to the Complete Navigation event.

Features for Users with Low Vision

Common forms of low vision are color blindness, difficulty in changing focus, and impaired contrast sensitivity. Users with color blindness may have difficulty reading colored text on a colored background. Users who have difficulty changing focus or who experience eye strain with normal use of a video display may have difficulty reading small text, discriminating between different font sizes, or using small on-screen items as targets for the cursor or pointer. Users with impaired contrast sensitivity may have difficulty reading black text on a gray background. Individuals with low vision sometimes use magnification software or hardware, and as a result, may prefer to use keyboard shortcuts to make the selection of on-screen elements easier than it would be using the mouse.

The list below recommends specific settings and features that can benefit users who have low vision. To learn about any of these features or for procedures that explain how to configure a certain setting, see the next chapter, "Accessibility Features and Functionality."

- Use keyboard navigation for Internet Explorer, Web pages, the Active Desktop, Internet Explorer Help, and NetMeeting.
- Use the Accessibility options on the **General** tab of the **Internet Options** dialog box to:
  - Ignore colors specified on Web pages.
  - Ignore font styles specified on Web pages.
  - Ignore font sizes specified on Web pages.
  - Format documents using your own style sheet.

- Use the **Advanced** tab on the **Internet Options** dialog box to:
  - Always expand alternate text for images.
  - Move the system caret with focus/selection changes.
  - Disable printing of background color and images.
  - Select to show the **Font** button in the browser toolbar.
  - Select not to display small icons.
- Use the **Colors** options on the **General** tab on the **Internet Options** dialog box to:
  - Choose text and background colors for Web pages (or create custom colors).
  - Choose the visited and unvisited colors for Web links (or create custom colors).
  - Choose to display Web pages using the Windows High Contrast color scheme, which offers a simple color palette and omits images that make text difficult to read.
- Use the **Sounds Properties** dialog box from Control Panel to:
  - Assign a sound to the Start Navigation event.
  - Assign a sound to the Complete Navigation event.

Features for Users Who Are Deaf or Hard-of-Hearing

Sound cues in programs are not useful to users with hearing impairments or users working in a noisy environment. Users who are deaf may have sign language as their primary language and English as their secondary language, and as a result, they may have difficulty reading pages that use custom fonts, depart from typographical convention—such as mixing uppercase and lowercase letters—or use animated text displays.

The list below recommends specific settings and features that can benefit users who are deaf or hard-of-hearing. To learn about any of these features or for procedures that explain how to configure a certain setting, see the next chapter, "Accessibility Features and Functionality."

Note Users who are deaf and have sign language as their primary language and English as a second language may also be interested in the features recommended for users with cognitive or language impairments.

- Use the **Accessibility Properties** dialog box from Windows Control Panel to select SoundSentry, which generates visual warnings when your system makes a sound.

- Use the **Accessibility Properties** dialog box from Windows Control Panel to select ShowSounds, which displays captions for the speech and sounds the system makes.
- Integrate NetMeeting.
- Use the **Advanced** tab on the **Internet Options** dialog box to disable sounds in Web pages.

Features for Users with Physical Impairments

Some users are unable to perform certain manual tasks, such as using a mouse or typing two keys at the same time. Others may have a tendency to hit multiple keys, "bounce" fingers off keys, or be unable to hold a printed book. Many users need keyboards and mouse functions to be adapted to their requirements. Others rely exclusively on a single input device.

The list below recommends specific settings and features that can benefit users who have physical impairments. To learn about any of these features or for procedures that explain how to configure a certain setting, see the next chapter, "Accessibility Features and Functionality."

- Use keyboard navigation and shortcuts for Internet Explorer, Web pages, the Active Desktop, Internet Explorer Help, and NetMeeting.
- Use Explorer bars.
- Use Webcasting to subscribe to Web sites and Active Channels. (For more information, see Part 4, "Information Delivery: Webcasting.")
- Use the Accessibility options on the **General** tab of the **Internet Options** dialog box to:
  - Ignore font sizes specified on Web pages.
  - Format documents using your own style sheet.
- Use the **Colors** box on the **General** tab of the **Internet Options** dialog box to add hover colors to hyperlinks.
- Use the **Advanced** tab on the **Internet Options** dialog box to:
  - Always expand alternate text for images.
  - Move the system caret with focus/selection changes.
  - Choose to use AutoComplete.
  - Underline hyperlinks when hovering (rolling over them).
  - Select to show the **Font** button in the browser toolbar.
  - Select not to display small icons.

Features for Users with Seizure Disorders

Users with seizure disorders (such as epilepsy) may be sensitive to screen refresh rates, blinking or flashing images, or specific sounds.

The list below recommends specific settings and features that can benefit users who have seizure disorders. To learn about any of these features or for procedures that explain how to configure a certain setting, see the next chapter, "Accessibility Features and Functionality."

- Use the ESC key to immediately turn off animations.
- Use the **Advanced** tab on the **Internet Options** dialog box to:
  - Disable animation.
  - Disable video.
  - Turn off sounds.

Note If RealAudio is installed, or if a movie is playing, sound might play, even if you clear the **Play sound** check box on the **Internet Options** dialog box.

Features for Users with Cognitive and Language Impairments

Cognitive impairments take many forms, including short-term and long-term memory loss, perceptual differences, and developmental disabilities. Language impairments, such as dyslexia or illiteracy, are also quite common. Even people learning the language used by their computer software as a second language can be considered to have a form of language impairment.

The list below recommends specific settings and features that can benefit users who have cognitive or language impairments. To learn about any of these features or for procedures that explain how to configure a certain setting, see the next chapter, "Accessibility Features and Functionality."

- Use keyboard navigation and shortcuts for Internet Explorer, Web pages, the Active Desktop, Internet Explorer Help, and NetMeeting.
- Use Explorer bars.
- Use Webcasting to subscribe to Web sites and Active Channels. (For more information, see Part 4, "Information Delivery: Webcasting.")
- Use the Accessibility options on the **General** tab of the **Internet Options** dialog box to:
  - Ignore colors specified on Web pages.
  - Ignore font styles specified on Web pages.
  - Ignore font sizes specified on Web pages.
  - Format documents using your own style sheet.

- Use the **Colors** options on the **General** tab on the **Internet Options** dialog box to:
  - Choose text and background colors for Web pages (or create custom colors).
  - Choose the visited and unvisited colors for Web links (or create custom colors).
  - Choose to display Web pages using the Windows High Contrast color scheme, which offers a simple color palette and omits images that make text difficult to read.
  - Choose a hover color for hyperlinks.
- Use the **Advanced** tab on the **Internet Options** dialog box to:
  - Always expand alternate text for images.
  - Move the system caret with focus/selection changes.
  - Choose to launch Active Channels and the browser in full screen mode, which removes all toolbars and scrollbars from the screen. This allows users with cognitive disabilities to have more information on the screen at one time or to remove distractions from peripheral controls.
  - Choose to use AutoComplete.
  - Choose to display friendly URLs.
  - Select to show the **Font** button in the browser toolbar.
  - Select not to display small icons.
  - Disable graphics.
  - Disable animation.
  - Disable video.
  - Select not to use smooth scrolling.

Accessibility Resources

For more information about Microsoft products and accessibility, see **http://www.microsoft.com/enable/**. This site also discusses how to design accessible Web pages that take advantage of new features in Internet Explorer 4. Plus, it offers information on new PowerToys, which make Internet Explorer even more accessible.

If you are deaf or hard-of-hearing, complete access to Microsoft product and customer services is available through a text telephone (TTY/TDD) service.

Customer Service

You can contact the Microsoft Sales Information Center on a text telephone by dialing (800) 892-5234 between 6:30 A.M. and 5:30 P.M. Pacific time.

Technical Assistance

For technical assistance in the United States, you can contact Microsoft Technical Support on a text telephone at (425) 635-4948 between 6:00 A.M. and 6:00 P.M. Pacific time, Monday through Friday, excluding holidays. In Canada, dial (905) 568-9641 between 8:00 A.M. and 8:00 P.M. eastern time, Monday through Friday, excluding holidays. Microsoft support services are subject to the prices, terms, and conditions in place at the time the service is used.

Microsoft Documentation in Alternative Formats

In addition to the standard forms of documentation, many Microsoft products are also available in other formats to make them more accessible. Many of the Internet Explorer 4 documents are also available as online Help, online user's guides, or from the Microsoft Web site. You can also download many Microsoft Press® books from the Microsoft Web site at **http://microsoft.com/enable/**.

If you have difficulty reading or handling printed documentation, you can obtain many Microsoft publications from Recording for the Blind & Dyslexic, Inc. Recording for the Blind & Dyslexic distributes these documents to registered, eligible members of their distribution service, either on audio cassettes or on floppy disks. The Recording for the Blind & Dyslexic collection contains more than 80,000 titles, including Microsoft product documentation and books from Microsoft Press. For information about eligibility and availability of Microsoft product documentation and books from Microsoft Press, contact Recording for the Blind & Dyslexic at the following address or phone numbers:

Recording for the Blind & Dyslexic, Inc.
20 Roszel Road
Princeton, NJ 08540

Phone: (609) 452-0606
Fax: (609) 987-8116

World Wide Web: **http://www.rfbd.org/**

Microsoft Products and Services for People with Disabilities

For more information for people with disabilities, contact:

Microsoft Sales Information Center
One Microsoft Way
Redmond, WA 98052-6393

Voice telephone: (800) 426-9400
Text telephone: (800) 892-5234

World Wide Web: **http://microsoft.com/enable/**

Computer Products for People with Disabilities

Microsoft provides a catalog of accessibility aids that can be used with the Windows and Windows NT® operating systems. You can obtain this catalog from the Microsoft Web site or by phone at the Microsoft Sales Information Center.

The Trace R&D Center at the University of Wisconsin-Madison publishes a database of more than 18,000 products and other information for people with disabilities. The database is available on their Web site. The database is also available on a compact disc, titled *CO-NET CD*, which is issued twice a year. The Trace R&D Center also publishes a book, titled *Trace ResourceBook,* which provides descriptions and photographs of about 2,000 products.

To obtain these directories, contact:

Trace R&D Center
University of Wisconsin
S-151 Waisman Center
1500 Highland Avenue
Madison, WI 53705-2280

Fax: (608) 262-8848

World Wide Web: **http://trace.wisc.edu/**

Information and Referrals for People with Disabilities

Computers and other assisting devices can help persons with disabilities to overcome a variety of barriers. For general information and recommendations on how computers can help you with your specific needs, you should consult a trained evaluator. For information about locating programs or services in your area that may be able to help you, contact:

National Information System
University of South Carolina
Columbia, SC 29208

Voice/text telephone: (803) 777-1782

Fax: (803) 777-9557

CHAPTER 33

Accessibility Features and Functionality

In this chapter

Using Keyboard Navigation 558
- Using Internet Explorer Shortcut Keys 558
- Using Keyboard Navigation of Web Pages 559
- Using AutoComplete Shortcut Keys 560
- Using Keyboard Navigation of the Windows Desktop Update 561
- Using Keyboard Navigation of the Help Tool 562

Customizing Display of Fonts, Colors, and Styles 566
- Overriding Web-Page Formatting 567
- Changing Font Size 568
- Creating a Style Sheet 568
- Changing the Default Font 571
- Changing the Color of Text and Backgrounds 571
- Changing the Color of Hyperlinks 572
- Setting Hover Colors 573
- Creating Custom Colors 573
- Selecting the High Contrast Color Scheme 574
- Understanding Font-Size Changes 574

Configuring Advanced Internet Accessibility Options 575

Using Accessibility Features in NetMeeting 579
- Using NetMeeting Keyboard Navigation and Shortcuts 580

Using Keyboard Navigation

One of the most important accessibility features is the ability to navigate with the keyboard, because it is helpful to people with a wide range of disabilities. Keyboard shortcuts are also useful to anyone who wants to save time by combining key commands with mouse control for maximum navigational efficiency. This section discusses:

- Internet Explorer shortcut keys
- Keyboard navigation of Web pages
- AutoComplete shortcut keys
- Keyboard navigation of the Windows Desktop Update
- Keyboard navigation of the Help tool

Using Internet Explorer Shortcut Keys

You can use shortcut keys to move between screen elements, choose commands, and view documents.

To	Press
Move forward between links and the Address, Links, and Explorer bars	TAB
Move back between links and the Explorer, Links, and Address bars	SHIFT+TAB
Activate a selected hyperlink	ENTER
Display a shortcut menu for the page or hyperlink	SHIFT+F10
Go to the previous page	ALT+LEFT ARROW
Go to the next page (after having used ALT+LEFT to go backward)	ALT+RIGHT ARROW
Move forward between frames and the Address, Links, and Explorer bars	CTRL+TAB
Move back between frames and the Explorer, Links, and Address bars	SHIFT+CTRL+TAB
Scroll toward the beginning of a document	UP ARROW
Scroll toward the end of a document	DOWN ARROW
Scroll toward the beginning of a document in larger increments	PAGE UP or SHIFT+SPACEBAR
Scroll toward the end of a document in larger increments	PAGE DOWN or SPACEBAR
Move to the beginning of a document	HOME
Move to the end of a document	END
Refresh the current page	F5
Stop downloading a page and stop animation	ESC
Go to a new location	CTRL+O

To	Press
Open a new window	CTRL+N
Save the current page	CTRL+S
Print the current page or active frame	CTRL+P

For additional information about using Windows with the keyboard, see the *Microsoft Windows Keyboard Guide*, which is available at **http://www.microsoft.com/enable/**.

Using Keyboard Navigation of Web Pages

You can move forward and backward between the browser Address bar and hyperlinks using TAB and SHIFT+TAB. A one-pixel-wide border, or *focus box*, will appear around links, so you can see what is selected. When you press the TAB key, the selection rotates forward through the Web page in this order:

1. The current address (URL) in the Address bar
   - If the Address bar is not displayed, you may not see a focus box on your screen.
   - To display the Address bar, on the **View** menu, point to **Toolbars,** and then select **Address Bar**.
2. The Links bar
   - The Links bar is not displayed by default, so you may not see a focus box on your screen.
   - To display the Links bar, on the **View** menu, point to **Toolbars**, and then select **Links**.
3. The Explorer bar
   - If an Explorer bar is open, you'll see an entry highlighted on the bar.
   - To display an Explorer bar, on the **View** menu, point to **Explorer Bar**, and then select one of the Explorer bars. Or, simply click the **Search**, **Favorites**, **History**, or **Channel** icon on the browser toolbar. (For more information about Explorer bars, see Part 2.)
4. Hyperlinks on the page, moving left to right, then down
   - As links are highlighted, the link's URL appears on the message bar.
   - Press ENTER to activate the link.
   - Press SHIFT+F10 to open a shortcut menu for the link.
5. The Address bar.

Note Web-page designers may specify a different order for their links than the standard left-to-right and top-to-bottom order.

You can use SHIFT+TAB to move between the same areas, but in reverse order. However, the focus stops on the page as a whole before reaching the links on the page. When using SHIFT+TAB, the focus moves in the following order:

1. The current address (URL) in the Address bar
2. The page as a whole
3. Links on the page in right-to-left and then upward order
4. The Explorer bar
5. The Links bar
6. The Address bar

You can quickly skip to the next frame by pressing CTRL+TAB, or go to the previous frame by pressing CTRL+SHIFT+TAB.

Using AutoComplete Shortcut Keys

The Address bar in Internet Explorer 4 automatically completes site addresses and directory paths for you, based on recently visited sites or local files. It also adds prefixes and suffixes to Internet addresses. You can easily override the suggestions by typing over them. AutoComplete makes it easier for you to enter URLs and reduces the opportunity to make mistakes by filling in long URLs automatically. You turn AutoComplete on and off from the **Advanced** tab on the **Internet Options** dialog box. (For more information, see Chapter 9, "Browser Features and Functionality.")

AutoComplete also includes the following shortcuts:

- To add to the string that has been automatically completed, press the RIGHT ARROW key, and then enter the additional characters.
- To skip to break or separate characters in URLs (such as \), press and hold CTRL, and then use the LEFT ARROW or RIGHT ARROW keys.
- To search your history file, enter the beginning of an address, and then press the UP ARROW or DOWN ARROW keys to complete it.
- To add a prefix or suffix to a partial URL, press CTRL+ENTER to add "http://www." before the entry and ".com" after it.

If you install the Windows Desktop Update, AutoComplete will also work when you use the **Run** command from the **Start** menu.

Using Keyboard Navigation of the Windows Desktop Update

When you install Internet Explorer 4, you have the option of installing the Windows Desktop Update, a set of features that integrates the Web into every aspect of personal computing. For more information about the Windows Desktop Update, including descriptions of the new toolbars, see Part 3, "True Web Integration: Windows Desktop Update."

Press TAB and SHIFT+TAB to move forward and backward, respectively, between the **Start** button, the Quick Launch toolbar, the taskbar, desktop icons and items, and the desktop Channel bar. A 1-pixel-wide border appears around items, so you can see what is selected.



The selection rotates forward through the desktop elements in this order:

1. The **Start** button
2. The Quick Launch toolbar
   - One of the Quick Launch icons appears selected.
   - You can use the arrow keys to move among the toolbar icons. Once the focus is on an icon, press ENTER to launch the application, or press SHIFT+F10 to display the shortcut menu for the toolbar. (All the toolbars on the desktop share the same shortcut menu.)
   - The arrow keys wrap, so continuously pressing the RIGHT ARROW key will eventually bring it back to the leftmost icon.
3. The taskbar
   - A selection will not appear on the taskbar, but the focus is in fact there. Press SHIFT+F10 at this point to display the shortcut menu for the toolbar. (All the toolbars on the desktop share the same shortcut menu.).
   - Press the RIGHT ARROW key to select an application. You can press ENTER to display the selected application, or press SHIFT+F10 to display the shortcut menu for that application.
   - Use the arrow keys to move between the applications.

4. The desktop icons
   - An icon on the desktop appears selected.
   - Use the arrow keys to move between the icons on the desktop. You can press ENTER to open the application or document, or press SHIFT+F10 to display the shortcut menu for that icon.
   - Press CTRL+SPACEBAR to select or deselect the current icon. When no icon is selected, you can press SHIFT+F10 to display the shortcut menu for the entire desktop.
5. The Active Desktop items
   - A desktop item appears selected.
   - Use TAB to move forward through the hyperlinks in that item and on to the other items on the desktop. You can press ENTER to activate a hyperlink.
6. The desktop Channel bar
   - The topmost button on the Channel bar appears selected.
   - Use arrow keys to move between the icons on the Channel bar. Press ENTER to display a channel using Internet Explorer.
   - Note that you can only reach the Channel bar by pressing TAB. The Channel bar is skipped when you navigate in reverse order using SHIFT+TAB.
7. The **Start** button.

If you add other bars, such as the Address bar, QuickLinks toolbar, desktop toolbar, or a custom toolbar, you can also use TAB and SHIFT+TAB to navigate to these bars.

Using Keyboard Navigation of the Help Tool

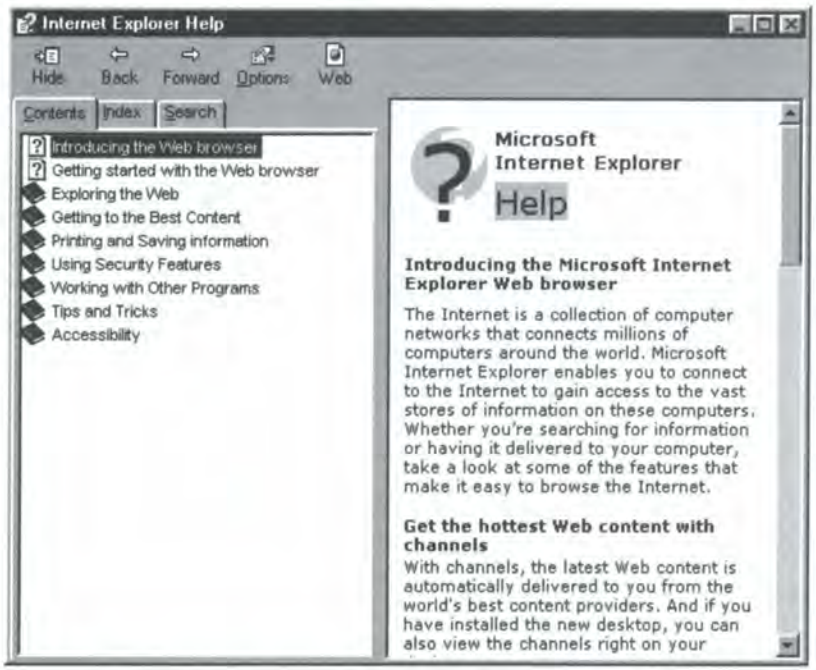
The new Internet Explorer Help is based on a new Help tool called HTML Help, which displays Help information as Web pages. This new tool offers several significant accessibility advantages (explained in detail in the next section), but it also introduces a few changes and possible limitations in terms of keyboard navigation:

- Unlike in previous versions of Help, you cannot use TAB to navigate between buttons, links, or panes of Internet Explorer 4 Help. You can, however, use ALT+C, ALT+I, and ALT+S to navigate to and from the Contents, Index, and Search tabs, respectively, and press ENTER to move to the topic pane.
- The keyboard cannot be used to activate Help topic hyperlinks at this time. However, relatively few Internet Explorer Help topics contain hyperlinks, and all the hyperlink topics can also be accessed using Contents, Index, and Search.

- When you display a topic in the right pane, it continues to be displayed until replaced with another selection—by highlighting a selection and pressing ENTER. This can be confusing in navigation, because the topic name currently selected in the left pane may not match the topic shown on the right.
- The **Hide** button on the Help toolbar hides the left pane (used for Contents, Index, and Search). When the left pane is hidden, there is no way to navigate Help. The keyboard cannot be used to make the left pane visible again.

▶ **To use the Help Contents list**

1. On the **Internet Explorer Help** dialog box, click **Contents**.

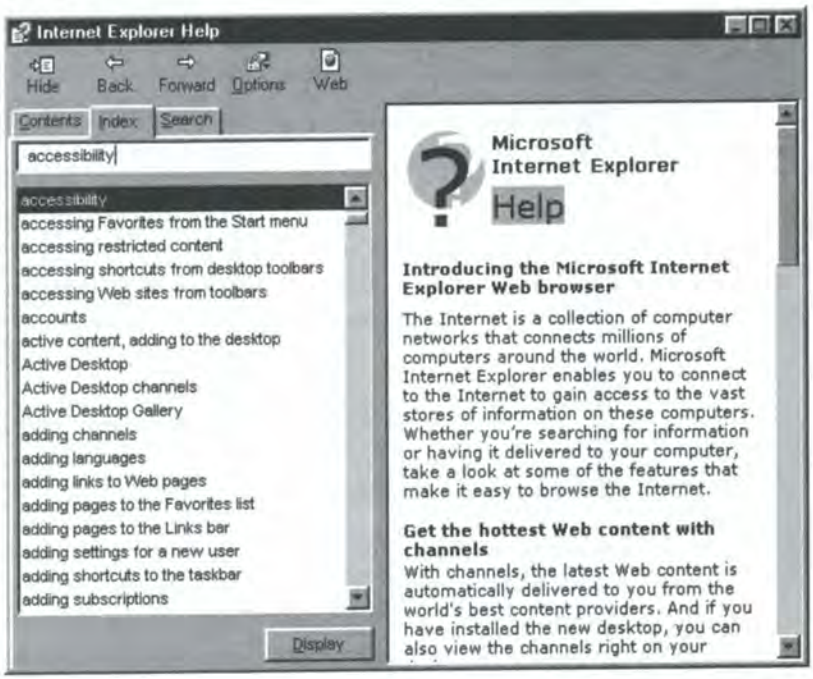


2. When Help is launched, the focus may be on the Help topic. To bring it back to the Contents pane, press ALT+I to toggle to the **Index** tab, and then press ALT+C to toggle to the **Contents** tab.
3. Use the UP ARROW and DOWN ARROW keys to move the selection in the Contents list. As you select parent topics, they will automatically open, indicated by the open-book icon and the expanded list of child topics. As you leave the last child page of an opened topic and move on to the next topic, the opened topic closes, collapsing the list and displaying a closed book icon.
4. Press ENTER to open and close topics indicated by book icons.

5. When you have highlighted the title of an available topic (indicated by a page icon), press ENTER to select the topic and display the information in the right pane. When the information in the right pane is replaced with a new topic, the keyboard focus moves to the Help topic. The string you searched for is highlighted wherever it appears in the topic.
   - Use the arrow keys to scroll up and down or left and right.
   - Press HOME or END to scroll the screen to the beginning or end of the topic.
   - Use CTRL+F10 to display the shortcut menu for the topic.
6. To return to the Contents list, press ALT+C.
7. Press ALT+F4 to exit Help.

▶ To use the Help Index

1. On the **Internet Explorer Help** dialog box, press ALT+I to display the **Index** tab.

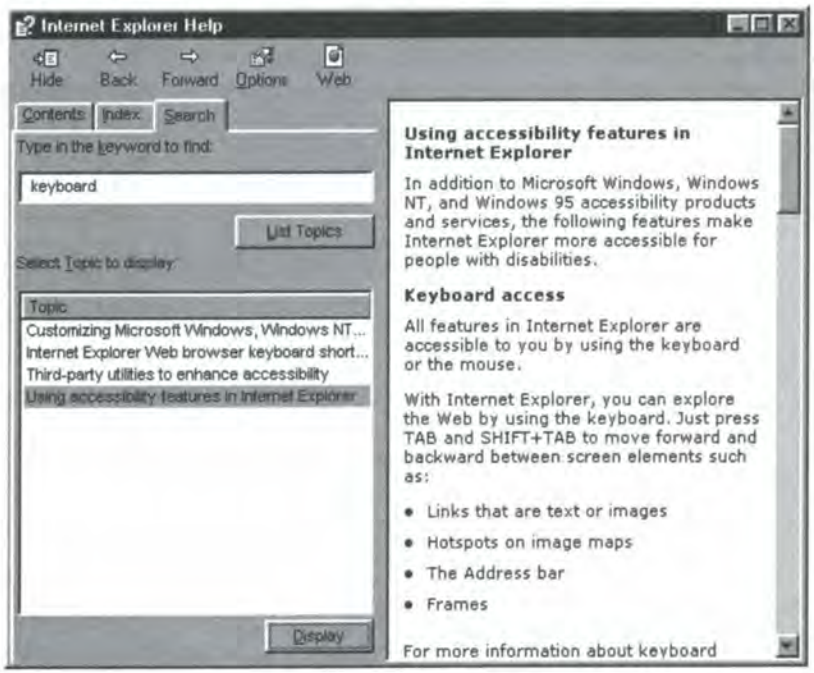


The **Index** tab has a text box where you can enter a term and a list box showing all available index entries. The keyboard focus will be in the text box. The first time you use this page, the text box is empty.

2. Use the arrow keys to scroll up and down the list of all topics. Topics will be highlighted as you scroll, and as they are highlighted they will appear in the text box. You may also enter the topic you want in the text box. The topic list will scroll to highlight matching topics as you type.
3. Press ENTER or ALT+D to display the highlighted topic information. Your topic will be displayed in the pane on the right, and the keyboard focus will move to the Help topic. The string you searched for will be highlighted wherever it appears in the topic.
   - Use the arrow keys to scroll up and down or left and right in the topic pane.
   - Press HOME or END to scroll the screen to the beginning or end of the topic.
   - Use CTRL+F10 to display the shortcut menu for the topic.
4. Use ALT+I to return to the Index to choose other topics, or ALT+F4 to close Help.

▶ To search for a topic by keyword

1. On the **Internet Explorer Help** dialog box, press ALT+S to bring the **Search** tab to the front. The keyboard focus will be in the keyword text box.



2. Enter the keyword you want.
3. Press ENTER or ALT+L. A list of topics pertaining to your keyword will appear in the **Topic** list box.

4. Press ALT+T and then the DOWN ARROW key to move the keyboard focus to the first item in the **Topic** list box. (The keyboard focus will not appear in the list box immediately after pressing ALT+T; it will appear after using the DOWN ARROW key.)
5. Use the UP ARROW and DOWN ARROW keys to highlight a topic.
6. Press ENTER or ALT+D to display the highlighted topic information in the pane on the right. The keyboard focus will move to the Help topic. The string you searched for will be highlighted wherever it appears in the topic.
   - Use the arrow keys to scroll up and down or left and right.
   - Press HOME or END to scroll the screen to the beginning or end of the topic.
   - Use CTRL+F10 to display the shortcut menu for the topic.
7. Use ALT+T to return to the **Search** tab to choose another topic, or ALT+K to begin another search
8. Use ALT+F4 to exit Help.

Customizing Display of Fonts, Colors, and Styles

When Web authors and designers create Web pages, they often specify particular font colors and sizes, typefaces, and background colors. These settings may be specified for each item as it is coded on the Web page, or they may be defined in a *style sheet*, which is a type of template for specifying how different styles should appear throughout a Web site. Internet Explorer 4 lets you override any or all of these settings. You can specify your own font and color preferences for all Web pages. You can also override formatting by using your own style sheet or by selecting the **High Contrast** option from the Windows Control Panel. If you're using the Windows Desktop Update, these font, color, and style options will also affect your Windows desktop and the presentation of your file folders.

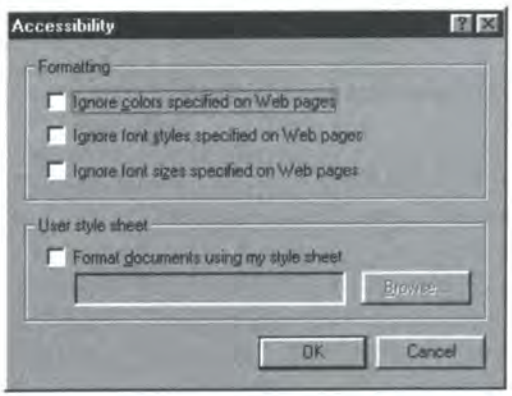
In Internet Explorer 4, Help information is displayed as Web pages, which means that most of the accessibility features in the Internet Explorer browser are now also available for viewing Help topics. The new Internet Explorer Help is based on a new Help tool called HTML Help. HTML Help will be used by many applications in the future and was designed to replace the standard Windows Help. This holds great promise for people with disabilities. You can override and customize formatting and color settings, display text instead of images, disable animation, and even apply your own style sheet in order to have complete control over how Help is presented. When you adjust these and similar options in Internet Explorer and then restart Help, your settings will automatically apply to all Help topics you view.

Overriding Web-Page Formatting

Note Because of the different ways Web pages can be formatted, some pages will not be affected by the procedures to customize options that are explained in this section. To change the appearance of such pages, you'll need to override the page formatting.

▶ **To override page formatting**

1. On the **View** menu, click **Internet Options**.
2. On the **General** tab, click **Accessibility**.



3. Select any of the following options:
   - **Ignore colors specified on Web pages**
   - **Ignore font styles specified on Web pages**
   - **Ignore font sizes specified on Web pages**
   - **Format documents using my style sheet**
4. Click **OK**.

Changing Font Size

When browsing a Web page, you can opt to immediately change the size of the displayed text.

▶ **To immediately display all text in a larger or smaller font size while viewing a page**

1. On the **View** menu, click **Fonts**, or click the **Font** button on the toolbar.
2. Choose the size you want. A check mark will appear next to your choice, and the change will immediately take effect.

If the **Font** button is not displayed on the toolbar, you can add it using the **Internet Options** dialog box.

▶ **To add the Font button to the toolbar**

1. On the **View** menu, click **Internet Options**.
2. Click the **Advanced** tab. A checklist of options appears.
3. Select **Toolbar** and **Show font** button.
4. Click **OK**.

Note The changes created by the **Fonts** menu option or **Font** button procedure will be active only for your current session. (To change the default font size: on the **View** menu, click **Internet Options**, and on the **General** tab, click **Fonts**; select a **Font Size** from the drop-down list.)

For more information about changing font sizes, see "Understanding Font Size Changes" later in this chapter.

Creating a Style Sheet

This section shows a sample style sheet that adjusts the display of Web pages and Help topics to be more easily read by users with certain types of low vision. In particular, it overrides normal formatting of all displayed pages in the following ways:

- Everything appears in high contrast, with a black background and brightly colored text. Body text is white, highlighted text is yellow, and links are brighter versions of their normal blue and purple.
- All text is displayed large and in a plain, sans-serif font. Body text is 24 point, and headings are 32 point.

- All bold, italics, and underlining, which can be difficult to read, are replaced by normal text with a single highlight color.
- The keyboard focus is emphasized by showing the active link in a bright, light green, sometimes called "low vision green."

These settings affect all pages viewed in Internet Explorer, as well as pages displayed by other programs (such as HTML Help) using Mshtml.dll.

▶ **To create a high-visibility style sheet**

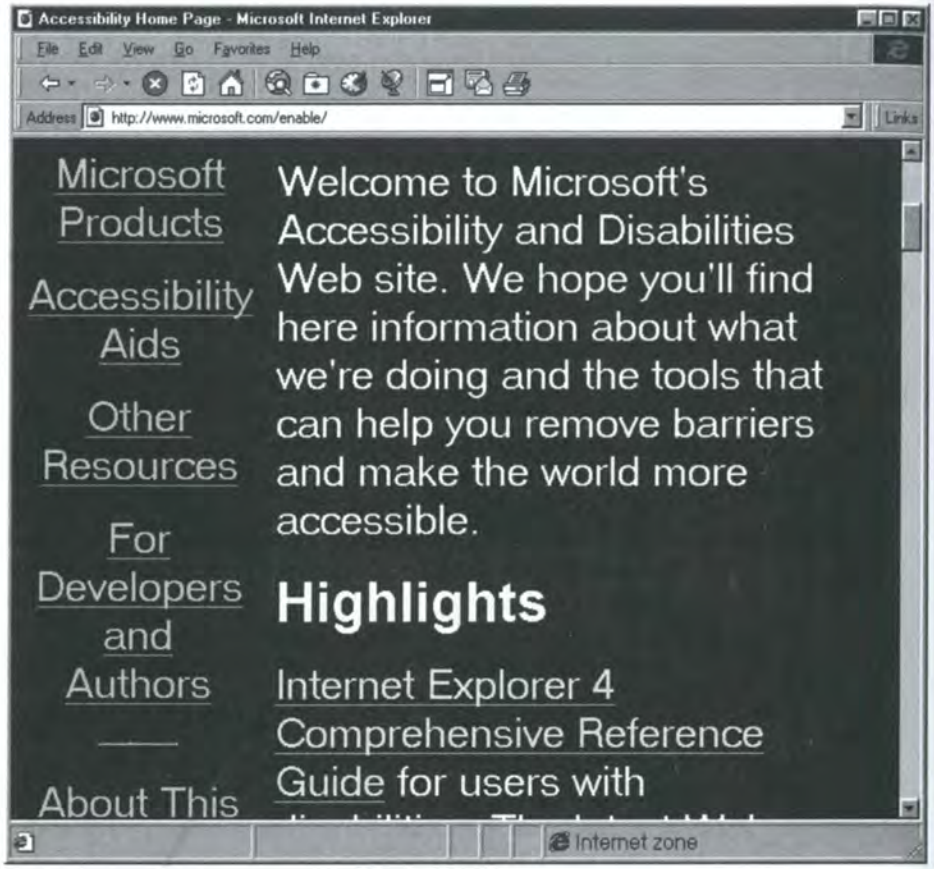
1. Open Notepad.
2. Enter the following text into the new file:

```
<STYLE TYPE="text/css">
<!- -
BODY, TABLE {
    font-size: 24pt;
    font-weight: normal;
    font-family: sans-serif;
    background: black;
    color: white;}

B, I, U {color: yellow; font-weight: normal; font-style: normal;}
H1 {font-size: 32pt;}
H2 {font-size: 32pt;}
H3 {font-size: 32pt;}
H4 {font-size: 32pt;}
H5 {font-size: 32pt;}

a:visited {color: #FF00FF}
a:link {color: #00FFFF}
a:active {color: #B1FB17}
-->
</STYLE>
```

3. Save the file to the folder of your choice with a .css file name extension (for example, mystyle.css).
4. In Internet Explorer, on the **View** menu, click **Internet Options**.
5. On the **General** tab, click **Accessibility**.
6. Click **Format documents using my style sheet**.
7. Enter the path of the style sheet file you just created, or click **Browse** to navigate to the file's location.
8. Click **OK**.



Note The style sheet in the preceding example is just one possible solution for increasing the readability of the Web pages you view. By editing the style sheet, you can change the background color and the size, color, and style of the fonts to whatever works best for you.

Caution Use caution when experimenting with the **Format documents using my style sheet** option. Errors in style sheets can cause serious problems with Internet Explorer. It is best to use style sheets that have been created by professional designers. When trying out new style sheets, keep the style-sheet files on a floppy disk that can be removed in case a problem occurs.

Changing the Default Font

You can select the font you prefer to be used as the Internet Explorer default font.

▶ **To change the default display font**

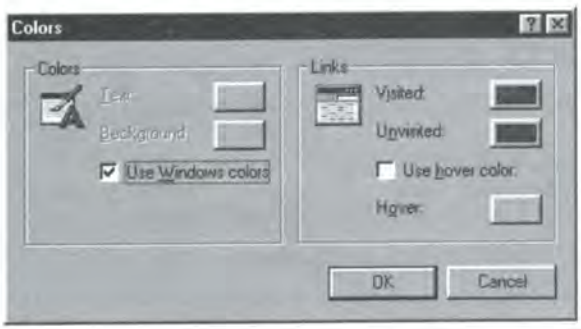
1. On the **View** menu in Internet Explorer, click **Internet Options**.
2. On the **General** tab, click **Fonts**.
3. Select the character set of your choice. Fonts appear in the drop-down list boxes.
4. Select the fonts of your choice.
5. Click **OK**.

Changing the Color of Text and Backgrounds

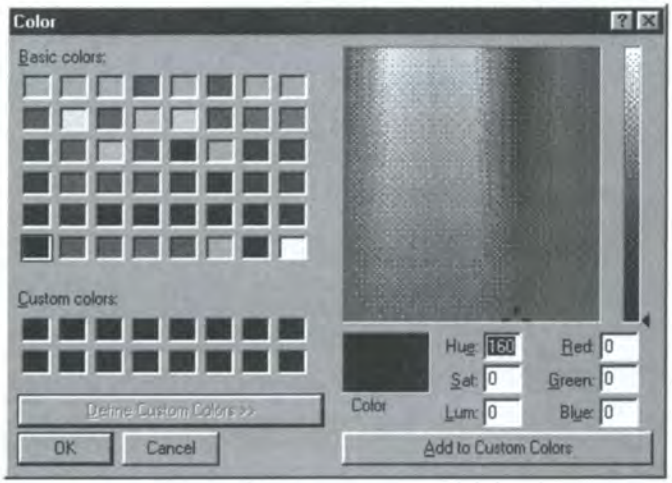
You can select the colors you prefer for text and background on Web pages.

▶ **To change the color of text and backgrounds**

1. On the **View** menu, click **Internet Options**.
2. On the **General** tab, click **Colors**.



3. In the **Colors** box, click the **Use Windows colors** check box to clear it. Then click the **Text** or **Background** button.
4. In the **Color** dialog box, click the color of your choice from the color palettes. (To create custom colors, see "Creating Custom Colors" later in this section.)



5. Click **OK**.

Changing the Color of Hyperlinks

You can select the colors you prefer for hyperlinks on Web pages.

▶ **To change hyperlink colors**

1. On the **View** menu, click **Internet Options**.
2. On the **General** tab, click **Colors**.
3. In the **Links** box, click the **Visited** or **Unvisited** button.
4. In the **Color** dialog box, click the color of your choice from the color palettes. (To create custom colors, see "Creating Custom Colors" later in this section.)
5. Click **OK**.

Setting Hover Colors

You can select the colors you prefer to be displayed when you are hovering on (rolling over) a Web object.

▶ **To customize hover colors**

1. On the **View** menu, click **Internet Options**.
2. On the **General** tab, click **Colors**.
3. In the **Links** box, select **Use hover color**. The **Hover** button will be enabled with the default color.
4. Click the **Hover** button.
5. In the **Color** dialog box, click the color of your choice from the color palettes. (To create custom colors, see "Creating Custom Colors" next in this section.)
6. Click **OK**.

Creating Custom Colors

You can create custom colors to be used for fonts, text background, links, and hovered objects.

▶ **To create custom colors**

1. On the **View** menu, click **Internet Options**.
2. On the **General** tab, click **Colors**.
3. In the **Colors** dialog box, click either the **Text**, **Background**, **Visited**, or **Unvisited** button to bring up the **Color** dialog box, which includes the Basics and Custom color palettes.
4. In the **Color** dialog box, click **Define Custom Colors**. The dialog box will expand.
5. Select a custom color using either of two methods:
   - Enter the values of your choice in any of the Hue, Sat, Lum, Red, Green, or Blue boxes. The sample box changes color to reflect your choices.
   - Click in the color box to select a color and drag the slider arrow (on the right) up or down to select the luminance level. The sample box changes color to reflect your choices.
6. Select **Add to Custom Colors**.
7. Click **OK**.

Selecting the High Contrast Color Scheme

Rather than creating your own, customized color scheme, you can choose to view your Web pages using the special, High Contrast color scheme offered by Windows.

▶ **To display Web pages in the High Contrast color scheme**

1. On the **Start** menu, point to **Settings**, and select **Control Panel**.
2. Double-click the **Accessibility Options** icon, and then click the **Display** tab.
3. Click the check box to set the **High Contrast** option. (For more options, click the **Settings** button.)
4. Click **OK** to close the **Accessibility Options** dialog box.
5. In Control Panel, double-click the **Internet** icon.
6. On the **General** tab, click **Accessibility**, select **Ignore colors specified on Web pages**, and then click **OK**.
7. On the **General** tab, click **Colors**, select **Use Windows Colors**, and then click **OK**.
8. Restart Internet Explorer to make the changes take effect.

Understanding Font-Size Changes

This section explains how font-size changes are applied in Internet Explorer. Listed below are the various factors affecting font size, listed in the order in which they are applied when the browser displays a page:

1. The Internet Explorer display defaults (for example, P is size 3, H1 is size 6).
2. A user-specified style sheet—if one is provided and **Format documents using my style sheet** is selected in the **Accessibility** dialog box.
3. Style sheet information in the document—unless **Ignore font sizes specified on Web pages** is selected in the **Accessibility** dialog box.
4. <FONT> tags in the document—unless **Ignore font sizes specified on Web pages** is selected in the **Accessibility** dialog box.
5. A scaling factor determined by the fonts options accessible from the **View** menu—except in those cases where the font is specified in an absolute size, such as 12 point.

   The scaling factor used in step 5 can be set in either of two ways. Accessing the **Fonts** dialog box through the **Internet Options** dialog box on the **View** menu can change the default for current and future sessions, whereas accessing the **Fonts** menu directly from the **View** menu changes fonts for the current session only.

Font sizes can be specified in the <FONT> tag of an HTML page and in style sheets. Sizes can be specified three ways:

- As an index value (1–7)
- As a relative value (+1, +5)
- Using absolute size units (12pt, 32px)

Font sizes set using index values and relative values are affected by the **View** menu font options, while fonts set in absolute size units are not.

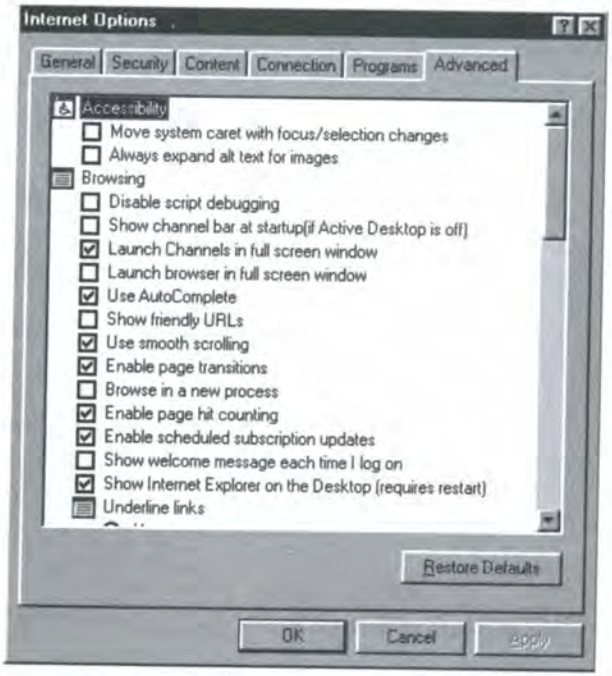
In order to have sizes in the user style sheet override those in the document, the **Ignore font sizes specified on Web pages** option must be selected in the **Accessibility** dialog box. The **Ignore font sizes specified on Web pages** option ignores all font sizes specified by <FONT> tags or style sheets, but it does not override relative sizes that are implied by structural tags. For example, a top-level heading (H1) will still be larger than body text, even when **Ignore Font Sizes** is turned on.

Configuring Advanced Internet Accessibility Options

Most accessibility features (other than customizing fonts and colors) are displayed in a checklist on the **Advanced** tab of the **Internet Options** dialog box.

1. On the **View** menu, click **Internet Options**.
2. Click the **Advanced** tab. You can either scroll through the checklist and make selections with your mouse, or:
   - Use the TAB key to move to the first option in the list.
   - Use the UP ARROW and DOWN ARROW keys to move through your selections.
   - Use the UP ARROW and DOWN ARROW keys to open or close groups of related options.
   - Use the SPACEBAR to select and clear the options you want.
3. Click **OK**.

Note Using the SPACEBAR to select and clear options causes a beep, as if you had entered an incorrect keystroke.



Useful Accessibility Options:

Move system caret with focus/selection changes

Specifies whether to move the system caret whenever the focus or selection changes. Some accessibility aids, such as screen readers or screen magnifiers, use the system caret to determine which area of the screen to read or magnify.

Always expand alt text for images

Specifies whether the image size should expand to fit all of the alternate text when the **Show Pictures** check box is cleared.

Useful Browsing Options:

Launch Channels in full screen window

Specifies whether to automatically display channels in full screen mode. This can be done more easily through the **View** menu. Use F11 to switch to full screen mode.

Launch browser in full screen window

Specifies whether to automatically display Web pages in a full screen whenever you start Internet Explorer. Full screen mode removes all toolbars and scroll bars from the screen to make more room for Web pages. This allows users with cognitive disabilities to have more information on the screen at one time or to remove distractions from peripheral controls. This mode is also useful if you are using large fonts or don't want to scroll as often. Use F11 to toggle out of full screen mode.

Use AutoComplete

Specifies whether you want Internet Explorer to automatically complete Internet addresses as you enter them in the Address bar. If you've visited the Web site before, the AutoComplete feature suggests a match as you type. Some users with cognitive disabilities may want to turn this off to avoid distractions, and some users of blind-access utilities may want to turn it off if their accessibility aid reads the suggestions as they appear, making typing difficult.

Show friendly URLs

Specifies whether you want Internet Explorer to show the full Internet address (URL) for a page on the status bar.

Use smooth scrolling

Specifies whether scrolling is used to gradually slide information up or down the screen when the user clicks on the scroll bar or presses navigation keys such as PAGE DOWN. Some users of blind-access utilities may want to turn this off if it causes timing problems. People with certain cognitive disabilities may want to turn it off because they find the motion distracting.

Underline links

Specifies how you want links on Web pages underlined. Select one of the following settings:

- **Always** to underline all links
- **Never** to not underline links
- **Hover** to underline links when your mouse pointer is over the link

  You may prefer to indicate whether or not a hovered link is indicated by a change in color (as explained earlier in this chapter). Older blind-access utilities rely on underlines to recognize links.

Useful Multimedia Options:

Show pictures

Specifies whether graphical images should be included when pages are displayed. Alt text (descriptive text) is displayed in place of the graphic if supplied by the page. When this check box is cleared, you can still display an individual image by right-clicking the icon that represents the graphic and then clicking **Show Picture**. (There is currently no keyboard equivalent for this.)

Turning off images will allow older blind-access utilities to read the textual description for these images aloud; however, newer utilities can use Microsoft Active Accessibility to identify and read these descriptions, even when the graphics are still displayed on the screen. Turning off images will speed up browser performance, although it may interfere with the functionality and effectiveness of some Web sites. If images are turned on or the textual description is cut off by space limitations, you can see the full description by moving the mouse over the image.

Play animations

Specifies whether animations can play when pages are displayed. Alt text is displayed in place of the graphic if supplied by the page. When this check box is cleared, you can still play an individual animation by right-clicking the icon that represents the animation and then clicking **Show Picture**. (There is currently no keyboard equivalent for this.)

As with users who are blind, users with seizure disorders may want to turn off animation (especially blinking). Users with cognitive disabilities may want to turn off animations or selectively download them to prevent distractions.

Play videos

Specifies whether video clips can play. When this check box is cleared, you can still play an individual video by right-clicking the icon that represents the animation and then clicking **Show Picture**. (There is currently no keyboard equivalent for this.)

As with users who are blind, users with seizure disorders may want to turn off video. Users with cognitive disabilities may want to turn off videos or selectively download them to prevent distractions.

Play sounds

If RealAudio is installed or if a movie is playing, sound might play, even if you clear this check box. As with users who are deaf or hard-of-hearing, users with seizure disorders may want to turn off sound. Users with cognitive disabilities may want to turn off sounds or selectively download them to prevent distractions. Users who are blind may want to turn off sounds or selectively download them so that they do not conflict with the screen reader when it is reading text aloud.

Useful Printer Options:

Print Background Colors and Images

Specifies that you want Internet Explorer to print background colors and images when you print a Web page. Users with low vision or those wanting to speed up print time may want to turn this off. You will also want to turn this off if you are preparing text to be scanned, for example, to provide it to a text reader.

Useful Toolbar Options:

Show font button

Specifies whether to display the **Font** button on the toolbar. You can use this button to immediately change the size of fonts displayed on a page you are currently viewing.

If the **Font** button does not appear on your toolbar when this setting is enabled, it may be off the right edge of the screen. The **Text Labels** option adds text labels to the toolbar buttons and makes the buttons larger, in some cases pushing some buttons off the screen. Without text labels, the toolbar buttons are smaller, and all fit on the toolbar. To hide the text labels, on the **View** menu, point to **Toolbars**, and then clear **Text Labels**.

Small icons

Specifies whether you want Internet Explorer to display the toolbar using Microsoft Office–style buttons. These buttons are smaller than the default buttons, and so users who prefer larger buttons should clear this option.

Using Accessibility Features in NetMeeting

Microsoft NetMeeting delivers a complete Internet conferencing solution that can greatly enhance accessibility for users with a wide range of disabilities. NetMeeting users can experience the benefits of real-time, multipoint communication that allows them to collaborate and share information with two or more conference participants at the same time.

Native application sharing allows you to share applications running on your computer with others in a conference. You can exchange graphics or draw diagrams with the electronic whiteboard. You can send messages or take meeting notes with the text-based chat program and send files to other conference participants with NetMeeting file transfer capability. Audio conferencing allows you to talk to friends, family, and business associates over the Internet or corporate intranet in real time. With a video capture card and camera, you can also send and receive video images for face-to-face communication. (You don't need a camera on your computer to see video that is sent by another user.) For complete information about NetMeeting, see Chapter 20, "NetMeeting," or visit **http://www.microsoft.com/netmeeting/**.

Using NetMeeting Keyboard Navigation and Shortcuts

You can use shortcuts to navigate in NetMeeting and to place calls.

To	Press
Place a call	CTRL+N
Send a file	CTRL+F
Start the Whiteboard	CTRL+W
Start Chat	CTRL+T
Toggle among the Directory, SpeedDial, Current Call, and History lists	CTRL+TAB
Refresh the Directory or SpeedDial list	F5
Stop loading the Directory list	CTRL+L
Open the folder list	CTRL+D
Toggle between the Audio toolbar and the main window, and, if open, the folder list	F6
Select check boxes (such as the **microphone** and **speaker** check boxes on the Audio toolbar)	SPACEBAR
Take control of a shared application	any key
Stop the collaboration of a person with whom you are sharing an application	ESC
When application sharing, toggle between open windows	ALT+TAB

PART 9

Deployment and Maintenance

The Microsoft® Internet Explorer Administration Kit (IEAK) provides tools that corporate administrators and information systems professionals can use to deploy custom versions of Internet Explorer 4 in their organizations. The IEAK also provides tools to centrally configure and maintain browser, application, desktop, and system settings on users' computers. Beginning with Internet Explorer 3, Microsoft has provided an IEAK to deploy and maintain the browser in organizations. With Internet Explorer 4, however, the deployment and maintenance capabilities of the IEAK have been greatly expanded. Organizations can now take advantage of the many new features of Internet Explorer 4 and the IEAK to exercise greater control over the deployment of Internet Explorer and over end-user desktop configurations.

Part 9 describes how to plan and implement successful deployments of Internet Explorer 4. It describes how to build and distribute custom versions of Internet Explorer to end users. It also describes how to centrally maintain end-user browser, application, and desktop configurations.

Chapter 34: Planning the Deployment

Planning is a key to successful deployment of Internet Explorer. Organizations need to: assign project teams; identify technical requirements, user needs, and migration issues; evaluate and choose deployment strategies; and then prepare project plans for the deployment.

Chapter 35: Validating the Deployment

To ensure a smooth deployment with minimum problems, organizations should test and refine their deployment plans in labs and in pilot programs before deployment to the whole organization. Feedback and lessons learned in the lab and during pilots provide valuable information for planning the final deployment.

Chapter 36: Implementing the Deployment

Organizations can use the enhanced features of the IEAK to build custom packages of Internet Explorer to distribute to user groups. These custom packages can be pre-configured with a wide range of browser, application, and desktop options and settings—giving corporate administrators a wide range of control over end users' browsers, applications, and desktops.

Chapter 37: Automatic Browser Configuration

Internet Explorer 4 provides enhanced capabilities for the automatic browser configuration feature introduced in Internet Explorer 3. Organizations can use the IEAK to deploy browsers that are set up for automatic browser configuration. System administrators can use the IEAK to centrally manage and maintain a wide range of browser, desktop, and system settings on users' computers.

Chapter 38: Software Distribution and Updates

Internet Explorer 4 introduces Active Channel™ technology, which can be used to automatically deliver new and updated Web content to users' computers. A software distribution channel is a special type of Active Channel that can be used to automate the distribution of new software and software updates to end users' computers.

Overview: The Deployment Process

The first three chapters of Part 9 contain information that network administrators and information systems professionals can use to plan and implement deployments of Internet Explorer in their organizations. To deploy Internet Explorer, you perform the following activities.

Develop the deployment plan

- Assemble project teams.
- Identify technical requirements for deployment.
- Identify your organization's client/server configurations and end-user needs.
- Identify migration issues and compatibility problems with previously existing systems.
- Specify preferred distribution strategies.
- Specify preferred custom-build configurations.
- Develop the deployment project plan.

See **Chapter 34, "Planning the Deployment"** for information on how to perform the planning tasks.

Validate the deployment plan

- Prepare the test plan and checklists.
- Test the deployment process in the lab.
- Plan the pilot program.
- Conduct the pilot program.
- Finalize the deployment project plan.

See **Chapter 35, "Validating the Deployment"** for information on how to perform the validation tasks.

Implement the deployment plan

- Announce the deployment to the organization.
- Provide user training and support.
- Complete the custom-build checklist.
- Build custom packages.
- Digitally sign custom package files.
- Configure Active Setup installation options.
- Implement a download site.
- Produce distribution media.
- Distribute Internet Explorer to users.
- Monitor and assist user installation of the Internet Explorer browser, as needed.

See **Chapter 36, "Implementing the Deployment"** for information on how to perform the implementation tasks.

See also **Appendix J, "Custom-Build Checklist"** for information on how to complete the custom-build checklist.

See also **Appendix L, "IExpress Configuration Wizard"** for information on how to build local packages that you can include with custom packages.

See also **Appendix K, "IEAK FAQs"** for more information about the IEAK.

CHAPTER 34

Planning the Deployment

In this chapter

Deployment Planning Overview 586
Assembling Project Teams 586
Identifying Technical Requirements for Deployment 587
Requirements for Internet Explorer 587
Requirements for Windows Operating Systems 587
Internet Explorer Suite Components 588
Requirements for the IEAK Configuration Wizard 588
Requirements for the IEAK Configuration Wizard 589
Identifying Client/Server Configurations and End-User Needs 590
Identifying Migration Issues 590
Migrating from Internet Explorer 3 591
Migrating from Netscape Navigator 3 591
Coexisting with Netscape Navigator 591
Using Previously Existing Browser Plug-Ins or Add-Ins 592
Using Previously Existing Internet E-Mail and News Programs 593
Dealing with Compatibility Problems 593
Specifying Distribution Strategies 594
Meeting End-User Needs 594
Reaching Your End Users 594
Assessing Size and Geographical Distribution of Your Organization 595
Assessing Resources Available to Your Organization 595
Assessing Network Performance and Bandwidth Issues 595
Assessing Network Security Issues 596

Specifying Custom Package Configurations 596
Choosing Deployment Roles 596
Deploying Language Versions 597
Selecting Available Media for Distribution 597
Selecting Version Synchronization Options 597
Determining Internet Explorer Setup Appearance Options 598
Specifying Component Installation Options 598
Specifying Browser Branding Options 598
Pre-Configuring Browser Settings 599
Specifying Automatic Browser Configuration Options 599
Setting Browser Security 599
Specifying Internet Mail and News Options 600
Setting System Policies and Restrictions 600
Developing the Deployment Project Plan 601

Deployment Planning Overview

This chapter describes how to plan the deployment of Microsoft Internet Explorer in your organization. To plan the deployment:

- Assemble project teams.
- Identify technical requirements for deployment.
- Identify your organization's client/server configurations and end-user needs.
- Identify migration issues and compatibility problems with previously existing systems.
- Specify preferred distribution strategies.
- Specify preferred custom-package configurations.
- Develop the deployment project plan.

Assembling Project Teams

Typically, a project manager oversees the deployment of Internet Explorer in an organization. That project manager assembles the necessary teams of system administrators and other information systems (IS) professionals to help plan, test, implement, and support the deployment. Project teams can include:

- Planning teams that help plan the deployment and develop the project plan.
- Installation teams that set up the test lab and use it to test the deployment.

- Training teams that develop training plans and train the organization for deployment.
- Support teams that develop support plans and support users during and after the deployment.

The size and number of required project teams will vary depending on the needs of your organization. For small organizations, only a few people who perform the roles of all the teams may be involved.

Identifying Technical Requirements for Deployment

The project teams should study the technical documentation for Internet Explorer to identify the requirements for deployment in their organization. Sources of technical information include:

- This deployment guide.
- The Internet Explorer Web site at **http://www.microsoft.com/ie/**.
- The Internet Explorer Customer Support Center at **http://www.microsoft.com/iesupport/**.
- Internet Explorer Help.
- The Internet Explorer Administration Kit (IEAK) Configuration Wizard Help.

The following sections describe the system requirements to install and run Internet Explorer and the IEAK Configuration Wizard.

Requirements for Internet Explorer

The following table lists the minimum hardware and software system requirements to deploy Internet Explorer 4 on Windows® 95 and Windows NT® operating systems. For information about system requirements for other systems, see the Internet Explorer Web site at **http://www.microsoft.com/ie/**.

Requirements for Windows Operating Systems

	Windows 95	Windows NT
Service Pack	All	Service Pack 3 required
Processor	486/66	486/66
Memory	8 MB (16 MB with Windows Desktop Update)	16 MB (24 MB with Windows Desktop Update)
Disk Space	39 MB Minimal installation 51 MB Standard installation 70 MB Full installation	39 MB Minimal installation 51 MB Standard installation 70 MB Full installation

Disk space requirements depend on the suite of components installed. Internet Explorer 4 Setup offers three standard installation suites: minimal, standard, and full.

Internet Explorer Suite Components

Option	Includes
Minimal Installation (39 MB)	Internet Explorer, Java support, Microsoft ActiveMovie™
Standard Installation (51 MB)	Internet Explorer, Java support, Microsoft ActiveMovie, Microsoft Internet Connection Wizard, Microsoft Outlook™ Express, Microsoft Interactive Music control, Microsoft Wallet
Full Installation (70 MB)	Internet Explorer, Java support, Microsoft ActiveMovie, Microsoft Internet Connection Wizard, Microsoft Outlook Express, Microsoft Interactive Music control, Microsoft Wallet, Microsoft FrontPage® Express, Intel Indeo5 Codec, Microsoft NetMeeting™ 2.0, Microsoft Chat 2.0, Microsoft Visual Basic® 5.01 Run Time, Microsoft NetShow™, RealPlayer by Progressive Networks, Microsoft Publishing Wizard

In addition, you can use the IEAK Configuration Wizard to build custom packages of Internet Explorer that include up to 10 other custom components. You'll need additional disk space for the custom components to be included in the installations.

Requirements for the IEAK Configuration Wizard

The following table lists the requirements to install and run the IEAK Configuration Wizard, which you can use to build custom packages of Internet Explorer to distribute to your end users.

Note You must install Internet Explorer before running the IEAK Configuration Wizard. If Internet Explorer is not installed, the wizard may appear to run, but it will not build your customized package correctly.

Requirements for the IEAK Configuration Wizard

Item	Requirements
Processor	486/66
Operating System	Windows 95 or Windows NT 4
Memory	8 MB Windows 95 16 MB Windows NT 4
Disk Space	40 MB to 60 MB to install 40 MB to 100 MB per custom package
Connection	Must be connected to the Internet to run the wizard the first time.

The disk space required in the C:\Program Files\Ieak folder varies considerably, depending on the number of Microsoft components you plan to include in custom packages; for example:

- 43 MB for a standard installation (includes Internet Explorer, Outlook Express, and ActiveMovie).
- 50 MB for an enhanced installation (includes Internet Explorer, Outlook Express, FrontPage Express, and ActiveMovie).
- 60 MB for a full installation (includes Internet Explorer, Outlook Express, NetMeeting, FrontPage Express, Microsoft Wallet, NetShow, and ActiveMovie).

The disk space required for custom packages varies depending on the Internet Explorer components and custom components you plan to install, as well as the distribution method you use. If you plan to distribute Internet Explorer on compact discs or floppy disks, the custom packages include the distribution files for the compact discs or floppy disks. Therefore, compact-disc and floppy-disk packages require about twice as much disk space as packages that do not use compact discs or floppy disks.

Note You can specify a local drive or a network drive on which to install the custom builds.

Identifying Client/Server Configurations and End-User Needs

Gather information to identify the existing client/server hardware and software configurations and end-user needs for all groups targeted to migrate to Internet Explorer. Based on this information, you can determine the preferred deployment strategies for the Internet Explorer custom-package configurations, which are described in Chapter 36, "Implementing the Deployment." Use this information to evaluate migration issues, including the need for hardware and software upgrades to support migration.

Gather information by surveying and interviewing the appropriate group managers, system administrators, and users for the groups to be migrated. However, the information-gathering process can be tedious and time-consuming, especially for large organizations. Therefore, it's recommended that you use network-asset survey software to identify and report the client/server configurations whenever feasible.

Identifying Migration Issues

It's important to identify and solve migration issues such as compatibility problems before you attempt to migrate from previously existing systems to Internet Explorer. To identify migration issues:

- Identify end-user hardware configurations.
- Identify end-user operating systems and applications.
- Research migration and compatibility problems.
- Test the migration process in a lab environment, using the actual user configurations to identify problems.
- Identify solutions such as upgrades of noncompatible, previously existing systems.
- Add solution implementations to the deployment plan.

For more information about testing the migration in the lab, see "Testing the Deployment Process," in Chapter 35, "Validating the Deployment."

The following sections discuss some of the general migration issues you should consider. For more information about migration issues:

- See the *Internet Explorer 4 Release Notes,* included with the Internet Explorer software.
- Visit the Microsoft Internet Explorer Support Center at **http://www.microsoft.com/iesupport/**.
- Contact the manufacturer of the conflicting software or hardware.

Migrating from Internet Explorer 3

Internet Explorer 4 Setup installs over an installed version of Internet Explorer 3 and imports proxy settings, favorites, and cookies from the previous version. However, you must reinstall any add-ons that you want to keep.

Note Users cannot have both Internet Explorer 3 and Internet Explorer 4 on the same machine unless they have created a dual-boot system, (a computer that can boot to either Windows 95 or Windows NT). With a dual-boot system, you can install Internet Explorer 3 under one operating system and Internet Explorer 4 under the other.

For more information, see Part 1, "Installing of Internet Explorer 4."

Migrating from Netscape Navigator 3

Internet Explorer 4 Setup imports proxy settings, bookmarks (called favorites in Internet Explorer), and cookies from Netscape Navigator 3. However, you must reinstall plug-ins. If you want helper applications to run when called by Internet Explorer, add the applications' Multipurpose Internet Mail Extension (MIME) types and file extensions to the list of Windows file-type extensions, and specify the program that opens files with those extensions. For more information on migrating e-mail information, see "Using Previously Existing Internet E-mail and News Programs," later in this section.

Coexisting with Netscape Navigator

Internet Explorer 4 can coexist safely with Netscape Navigator on the same machine. Since Netscape does not include support for ActiveX technology, the first thing Setup will do when upgrading Navigator is install ActiveX drivers on the system, so that Active Setup can run. If the Netscape ActiveX plug-in is installed, it makes no difference; it will not be used to support Active Setup.

If Netscape is installed when installing Internet Explorer, the Netscape plug-ins are copied to the Program Files\Internet Explorer\Plugins folder. The contents of this folder are loaded into memory each time the browser is launched.

Shdocvw.dll will call a plug-in to perform a rendering job if there is no native code for that task. However, at this time there is no Netscape plug-in that offers functionality beyond that offered by Internet Explorer's native code, so it is just a waste of memory to have them loaded. For this reason, a user may choose to delete files from the Plug-ins folder.

When installing Internet Explorer, Setup looks for an installed browser that is set to be the default browser. During Setup, the user-configurable settings, including proxy settings, dial-up connection, and favorites, are adopted from the current default browser. Some additional settings may also be adopted, if the corresponding optional components are installed, as indicated in the lists below.

Outlook Express Settings:

- SMTP server information.
- POP3 server settings (POP3 server name, POP3 user name).
- Identity information (name, e-mail address, reply address, organization, signature information).
- Personal address book.
- Internet telephone program, Web-based phone book.
- Send and post settings (8 bit chars. in headers, MIME compliance) if different from the Navigator default.
- Settings for check new message every *x* minutes if different from the Navigator default.

Web Publishing Wizard:

- Author name.
- Document template location.
- Publisher user name.
- Publisher password.

Using Previously Existing Browser Plug-Ins or Add-Ins

You can use most previously existing browser plug-ins and helper applications in conjunction with Internet Explorer 4 by including them as custom components when you build custom packages of Internet Explorer 4. For more information, see "Building Custom Packages" in Chapter 36, "Implementing the Deployment."

Keep in mind that some earlier plug-ins and add-ins may not be compatible with Internet Explorer 4. You may be able to obtain patches or updates to compatible versions from the software manufacturer.

Using Previously Existing Internet E-Mail and News Programs

You can configure Internet Explorer 4 to work with your previously existing e-mail and news applications in two ways. If the e-mail application is already on users' desktops, simply choose **Internet Options** from the **View** menu, and then click **Programs**. In the **Programs** tab, select the application you want to use for e-mail from the drop-down box. If you would like to introduce another e-mail or news application in conjunction with Internet Explorer, you can do so by including each application as a custom component when you build custom packages of Internet Explorer, and pre-configuring Internet Explorer to use each application. For more information, see "Building Custom Packages" in Chapter 36, "Implementing the Deployment."

You can also specify Outlook Express as your Internet e-mail and news program when you build custom packages of Internet Explorer. If Outlook Express is specified, Setup automatically imports folders from existing e-mail packages such as Netscape Mail, Eudora Light, and Eudora Pro into Outlook Express. Settings from Microsoft Exchange and Microsoft Outlook will also be imported into Outlook Express, if appropriate for your configuration.

Dealing with Compatibility Problems

Some previously existing software may not be compatible with Internet Explorer 4. In addition, Web pages that were developed for other Web browsers and for proprietary HTML or scripting extensions may not function the same way in Internet Explorer 4.

Compatibility problems with earlier software can often be corrected by obtaining upgrades or patches from the software manufacturer or by migrating previously existing applications to applications that are known to be compatible with Internet Explorer 4. To correct Web pages that do not function properly in Internet Explorer 4, however, you may need to redesign them to be compatible with Internet Explorer 4.

Test the Web pages on your intranet to see if there are any compatibility problems with Internet Explorer 4. For more information about third-party compatibility issues, see the *Internet Explorer 4 Release Notes,* included with the Internet Explorer software. For more information about scripting issues, see Part 6, Chapter 26, "Active Scripting."

Specifying Distribution Strategies

The IEAK Configuration Wizard is used to build custom packages of Internet Explorer 4 to distribute to end users. You can automate installations of Internet Explorer with preselected components and browser settings, so that no user action is required, or you can allow users to choose from up to 10 installation options during their installation.

You can distribute Internet Explorer from:

- Download sites on the Internet to end-user desktops.
- Download sites on your intranet to end-user desktops.
- Compact discs to end-user desktops.
- Floppy disks to end-user desktops.

The following sections discuss some of the factors to consider when you choose distribution strategies.

Meeting End-User Needs

Identify the needs of your end users. If your field personnel access your intranet through a remote-access modem pool at 28.8 Kbps, it can be time-consuming for them to download the Internet Explorer custom package from the Internet or their intranet. It also may unreliable due to poor phone connections. You can choose to distribute the custom package to field personnel on compact discs or floppy disks and distribute the custom package to the rest of your organization from download sites on your intranet.

Reaching Your End Users

Identify what's required to reach your end users. If some use stand-alone computers that are not connected to the network, you need either to distribute custom packages from the Internet or distribute custom packages on compact discs or floppy disks.

Assessing Size and Geographical Distribution of Your Organization

The size and geographical distribution of your organization will influence your distribution strategy. For example, a large organization may be able to produce compact discs at a volume discount and so can afford to distribute custom packages on compact discs. On the other hand, it may not be economical for a small organization to produce a small volume of compact discs; so that organization may decide to distribute custom packages over their intranet or the Internet. An organization with many offices worldwide may decide to distribute multiple-language versions of custom packages over the Internet.

Assessing Resources Available to Your Organization

The resources available to your organization will influence your distribution strategy. For example, if your organization doesn't have a wide-area network (WAN), you may decide to distribute custom packages to your worldwide user base over the Internet.

Assessing Network Performance and Bandwidth Issues

Your distribution strategies will affect network performance and the available bandwidth of your intranet. Choose distribution strategies that help optimize network performance and bandwidth. For example, if you distribute custom packages over the Internet to users on your intranet, it can cause excessive load on firewalls and proxy servers. If you distribute custom packages from only one download server in a large WAN, it can overload the server and cause traffic problems across the interconnecting routers and bridges of subnets and local area networks (LANs). You can usually achieve the best network performance by distributing custom packages from download servers that are located in multiple domains or subnets of your intranet.

Note You can specify up to 10 download sites that Internet Explorer Setup will automatically switch between during installations. This provides optimum download performance, as well as distribution of load across the intranet.

Assessing Network Security Issues

The distribution strategies available to you depend on the security configuration of your intranet, as well as the level of Internet access that you allow your users to have.

You can distribute custom packages from the Internet to users on the intranet if you configure firewalls and proxy servers to allow users to download the Internet Explorer components. Internet Explorer components are authenticated when downloaded from the Internet. However, distributing custom builds over your intranet still provides maximum security and does not require firewalls and proxy servers.

If your organization does not provide the required level of Internet access to users, you do not have the option to distribute custom packages over the Internet. However, you still need to provide Internet access to the administrators who run the IEAK Configuration Wizard to build the custom packages. The IEAK Configuration Wizard must access the Internet to download the most current components of Internet Explorer from the Microsoft Internet-download site.

Specifying Custom Package Configurations

When you use the IEAK Configuration Wizard to build custom packages of Internet Explorer, you can specify a wide variety of configuration options. For example, you can specify the media and the Setup options used to distribute the custom package to end users. You can also specify the URLs of download sites and pre-configure browser settings, such as the security and proxy settings.

The following sections briefly describe the major configuration options that are available for building custom packages. For more information to help you specify custom builds, see the checklist in Appendix J, "Custom-Build Checklist," and "Building Custom Packages" in Chapter 36, "Implementing the Deployment."

Choosing Deployment Roles

When you enter your 10-digit customization code for Corporate Administrators, the following roles are available in the IEAK Configuration Wizard:

- Content Provider/Developer
- Service Provider
- Corporate Administrator

For the purposes of this internal Internet Explorer deployment, you should select the **Corporate Administrator** option. For more information about the Content Provider/Developer and Service Provider roles, see the IEAK Configuration Wizard Help and the Internet Explorer Web site at **http://www.microsoft.com/ie/**.

Deploying Language Versions

You must create and distribute a separate Internet Explorer custom build for each language you want to deploy.

Selecting Available Media for Distribution

You can distribute the Internet Explorer custom package files from download sites on the Internet or your intranet. You can also select one of the following optional distribution media:

- CD-ROM
- Multiple floppy disks

When you select **CD-ROM** or **Multiple floppy disks,** the CD-ROM or floppy disk distribution files are added to the custom package. You can then copy the distribution files to the compact disc or floppy disks. In addition, when you select **CD-ROM,** you can use the IEAK Configuration Wizard to create and use a custom CD-ROM Autorun screen. This screen will automatically appear, to help users with their installation, when users insert their customized Internet Explorer compact disc.

Selecting Version Synchronization Options

When you start the IEAK Configuration Wizard, Automatic Version Synchronization (AVS) is turned on by default. With AVS turned on, you can use the IEAK Configuration Wizard to:

- Select the Microsoft download site from which to download the Internet Explorer components.
- Download the most current versions of Microsoft components for the custom package.

You use AVS to keep custom packages up-to-date with the most current Internet Explorer components. The first time you run the IEAK Configuration Wizard to build a custom package, AVS is turned on and cannot be turned off because you must download the Internet Explorer components used to build custom packages. Later, if you do not want the IEAK Configuration Wizard to compare your packages with the software on the Microsoft Web site, you can turn off AVS.

Determining Internet Explorer Setup Appearance Options

The IEAK Configuration Wizard creates a custom build of the Internet Explorer Setup that you distribute to users. Users then run Setup to install Internet Explorer on their systems. You can use the IEAK Configuration Wizard to:

- Customize the CD-ROM Autorun screen (when **CD-ROM** is selected).
- Brand the Setup Wizard to include your organization's logo and name.

Specifying Component Installation Options

You can specify the components to be installed with the custom build, and you can specify various installation options. You can use the IEAK Configuration Wizard to:

- Select a silent installation, which doesn't give users any opportunity to change your custom installation settings.
- Specify up to 10 custom components that you provide for installation.
- Specify URLs for up to 10 download sites from which to distribute the custom build.
- Specify up to 10 installation options from which users can choose during the installation.
- Specify any combination of standard or custom components to be included in each installation option.
- Specify the version number and configuration identifier for the custom package.
- Specify the folder where Internet Explorer will be installed on end-user systems.
- Specify whether to integrate the Windows Desktop Update in the custom package.

Specifying Browser Branding Options

You can brand several browser features. You can use the IEAK Configuration Wizard to:

- Specify title-bar text and a toolbar background bitmap.
- Specify a logo.

Pre-Configuring Browser Settings

You can pre-configure a variety of browser settings. You can use the IEAK Configuration Wizard to:

- Specify browser start and search pages.
- Specify an online browser support page.
- Specify a default set of favorites.
- Specify a custom Internet Explorer welcome page and desktop wallpaper.
- Specify Active Channels for installation.
- Specify custom HTML files for My Computer and Control Panel Web views.
- Specify a user agent string to be appended to the default Internet Explorer string.
- Specify proxy settings.

Specifying Automatic Browser Configuration Options

You can set up the browsers in your organization to be managed from centrally located files, using the Internet Explorer automatic browser configuration. If you enable automatic browser configuration, you can use the IEAK Profile Manager to administer Internet Explorer configurations. The IEAK Configuration Wizard can:

- Enable automatic browser configuration for end users. This will force Internet Explorer to look at an auto-configuration URL each time the browser is launched, to see if there is a new configuration that the browser must apply.
- Specify the URL containing user Internet settings (.ins files).
- Specify the URL containing auto-proxy (.js or .pac files).
- Specify a schedule for when automatic configuration occurs, if more often than only when the browser is started.

Setting Browser Security

You can control user access to Web sites and content through site certificates, Authenticode™, trusted publishers, security zones, and content ratings. You can use the IEAK Configuration Wizard to:

- Specify site certificate and Authenticode settings.
- Specify security zones and content ratings.

Specifying Internet Mail and News Options

You can specify various settings and options for Internet mail and news. You can use the IEAK Configuration Wizard to:

- Specify Internet mail servers, domain servers, and news servers.
- Specify Outlook Express as the default mail and news client.
- Specify Secure Password Authentication (SPA) to authenticate users when they log on.
- Specify the Lightweight Directory Access Protocol (LDAP) settings.
- Specify the Infopane and welcome message for Outlook Express.
- Specify default signature files for e-mail and news messages.

Setting System Policies and Restrictions

You can specify numerous desktop, shell, and security settings across your organization. You can customize settings, for example, to allow users to delete printers or to prevent them from adding items to the new Windows Desktop Update. Be sure to understand the impact of the security settings on your users, especially if you have roaming users who share computers with other users.

You can use the IEAK Configuration Wizard to set system policies and restrictions for users in the following areas:

- Microsoft NetMeeting
- Active Desktop™
- Internet Properties
- Outlook Express
- Shell
- Channels and Subscriptions
- Microsoft Chat
- Internet Explorer Advanced Settings
- Internet Code Download

You can control, or *lock down,* features and functions in these areas. For example, you can use the **Colors** and **Fonts** options under **Advanced Settings** in Internet Explorer to specify browser colors and fonts that users cannot change. More important, you can prevent users from adding or deleting channels that you have preset, or from rearranging or adding Active Desktop items. You can use the Shell options to prevent Windows 95 users from restarting their systems in MS-DOS® mode. All Policies and Restrictions you set in the IEAK Configuration Wizard can be changed later by the administrator, using the IEAK Profile Manager.

Developing the Deployment Project Plan

Develop a project plan for the deployment. To develop a project plan:

- Establish deployment goals.
- Identify critical success factors.
- Identify tasks, resources, and tools.
- Identify task and resource dependencies.
- Budget resources needed to meet deployment goals.
- Assign task responsibilities and timelines for completion.
- Identify significant risks, and develop contingency plans.

The project plan includes the deployment tasks described in: Chapter 34, "Planning the Deployment"; Chapter 35, "Validating the Deployment"; and Chapter 36, "Implementing the Deployment." You should update the project plan continuously throughout the project and use a project management tool, such as Microsoft Project, to help plan and manage the deployment.

CHAPTER 35

Validating the Deployment

In this chapter

Deployment Validation Overview 604
Preparing the Test Plan and Checklists 604
Testing the Deployment Process 605
  Preparing the Lab 605
  Conducting the Tests 605
Planning the Pilot Program 606
  Selecting Pilot Groups 606
  Documenting Resources and Tasks 606
  Developing the User-Support Plan 606
  Developing the User-Training Plan 607
Conducting the Pilot Program 607
  Preparing Pilot Groups 607
  Implementing the Pilot-Program Plan 607
    Preparing Custom Packages 608
    Deploying Custom Packages 608
    Monitoring and Supporting Users 608
Finalizing the Deployment Plan 609

Deployment Validation Overview

This chapter describes how to validate the deployment plan before you proceed to deploy Microsoft Internet Explorer to your entire organization. To validate the deployment, you need to:

- Prepare the test plan and checklists.
- Test the deployment process in the lab.
- Plan the pilot program.
- Conduct the pilot program.
- Finalize the deployment project plan.

Preparing the Test Plan and Checklists

Prepare a test plan and checklists for lab tests, and then use the test checklists to record satisfactory completion of tasks and note all problems with the process. Also, prepare a checklist to test each deployment and distribution strategy.

Test checklists tasks should include:

- Preparing custom packages for deployment:
  - Install and run the Internet Explorer Administration Kit (IEAK) Configuration Wizard.
  - Build custom packages containing the distribution files.
  - Configure browser auto-configuration (.ins, .js, .pac) files.
  - Configure download sites, and install the distribution files.
  - Copy distribution files to compact discs and floppy disks.
- Deploying custom packages to lab clients:
  - Run Internet Explorer Setup to install the custom package on each client.
  - Install, using each available user install option.
- Operating lab-client software after custom packages are installed:
  - Run Active Desktop to test all desktop features.
  - Run Internet Explorer to test all add-ins and features.
  - Run business applications to check for satisfactory operation.
- Restoring lab clients to their original state:
  - Uninstall Internet Explorer and add-ins.
  - Verify that Internet Explorer components have been removed.
  - Test the desktop and business applications.

Testing the Deployment Process

You should prepare a test lab and then test the proposed deployment strategies on lab computers that represent typical client/server configurations for your organization. If your organization is large or has groups with vastly different computing environments or needs, you may need to prepare multiple test labs and conduct tests at several different sites.

Preparing the Lab

Set aside a physical space for each lab, and acquire a mix of computers that accurately reflects your organization's hardware and software computing environment. If your organization uses portable computers that dial in from remote locations or you need to use additional servers or mainframe computers for business data, give the lab computers an analog phone line and appropriate access to the network.

Configure lab clients and servers to represent typical business and user configurations for your organization. Be sure to include all operating system and business-application configurations, as well as Internet and browser configurations. In addition, be sure to document the lab setup and maintain a record of any changes you make to the setup.

Conducting the Tests

To test the deployment in the lab:

- Perform all deployment tasks, using the test-plan checklists.
- Identify problems with the deployment process and migration issues.
- Revise the deployment plan based on test feedback.

Maintain a record of all issues and problems that you encounter. These records will help you design solutions to correct the problems you encounter. Be sure to follow the testing process described in this section when you test the solutions.

Planning the Pilot Program

Before you deploy Internet Explorer in your organization, plan a pilot program to further test and refine deployment strategies and configurations. The pilot program is a scaled-down version of the full deployment, using pilot groups that are representative of the users in your organization. To plan the pilot program:

- Select appropriate pilot groups.
- Document resources and tasks needed for the pilot program.
- Develop a user-support plan.
- Develop a user-training plan.

Selecting Pilot Groups

Identify and select pilot groups, and prepare them for the pilot program. If your organization is large or has groups with vastly different computing environments or needs, you may need to select several pilot groups. Locate groups that are representative of the users in your organization. Make sure participants have enough time in their schedules for the pilot and are willing to cooperate in the pilot program. Ask for volunteers for the pilot program—you don't want to ask people to participate who might be too busy meeting deadlines.

Documenting Resources and Tasks

Identify the tasks and resources you need to conduct the pilot, and add them to the project plan. Be sure to budget your resources to make sure those resources are available for the pilot program.

Developing the User-Support Plan

Develop a user-support plan that meets the needs of your users. Identify the support staff and resources necessary, and then budget to make sure those support staff and resources are available for the pilot program. User support may include providing online support for deployment through a Web page on your intranet, as well as providing support through your existing help desk.

This user-support plan is the basis for your final deployment user-support plan. You should revise the plan based on feedback from the pilot program and use it to support users during the final deployment.

Developing the User-Training Plan

Develop a training plan that meets the needs of your users. Identify the training staff and resources necessary, and then make sure the staff and resources are available for the pilot program. User training may include providing online Internet Explorer training through a Web page on your intranet, as well as presenting training information to groups to prepare them for the pilot.

This training plan is the basis for your final deployment user-training plan. You should revise the plan, based on feedback from the pilot program, and use it to train users for the final deployment.

Conducting the Pilot Program

You conduct the pilot program by preparing the pilot groups and then implementing the pilot-program plan.

Preparing Pilot Groups

Announce the start of the pilot program well in advance of the start date, and follow up your announcement with several reminders. Conduct meetings with the pilot group managers and with the entire group, to set their expectations and to answer any questions they have. Provide a deployment presentation that explains how users will install Internet Explorer. Explain any installation options that users may choose, and identify where users can go for support.

Conduct training on the new features of Internet Explorer 4. Encourage users to visit the Microsoft Internet Explorer Web site at **http://www.microsoft.com/ie/** for more information. If you implemented a Web page on your intranet for Internet Explorer training, use e-mail to broadcast the URL and a description of the training page to users. Be sure to explain how users can benefit from visiting your training page.

Implementing the Pilot-Program Plan

To implement the pilot-program plan:

- Prepare custom packages for deployment.
- Deploy custom packages to pilot users.
- Monitor and support users as they install Internet Explorer.

Preparing Custom Packages

Before you build custom packages, select a production computer that meets the system requirements for the IEAK Configuration Wizard. For more information, see "Requirements for the IEAK Configuration Wizard" in Chapter 34, "Planning the Deployment."

To prepare the custom packages:

- Install the IEAK on the production computer.
- Run the IEAK Configuration Wizard in the Corporate Administrator role.
- Build the required custom packages.
- Configure browser auto-configuration (.ins, .js, .pac) files.
- Configure download sites, and install the distribution files.
- Copy distribution files to compact discs and floppy disks (if necessary).

For more information on how to use the IEAK Configuration Wizard, as well as creating auto-configuration files and understanding the entire custom package preparation process, see Chapter 36, "Implementing the Deployment."

Deploying Custom Packages

Use the appropriate distribution methods to deploy the custom packages of Internet Explorer to pilot users. For example, you can send an e-mail message to users that directs them to the download site where they can follow instructions to download the custom package. Alternatively, you can include a batch file as an attachment in the e-mail message and instruct users to double-click the batch file to install the custom package. If you are using compact discs or floppy disks, you can distribute them to the users and provide e-mail instructions about how to install the custom package from the compact discs or floppy disks.

Monitoring and Supporting Users

The user support team can monitor the progress of the pilot program and provide user assistance, as necessary. Be sure to document all user trouble calls and problems, as well as the staff resources required to support users during the pilot. Use your experience during the pilot program to plan for the resources needed to support the final deployment.

Finalizing the Deployment Plan

Use the finalized deployment plan to deploy Internet Explorer in the rest of your organization. To finalize the deployment plan:

- Obtain feedback from all participants in the pilot, including end users.
- Document lessons learned during the pilot program.
- Incorporate lessons learned and participant feedback into the deployment project plan.

For information on how to conduct the final deployment, see Chapter 36, "Implementing the Deployment."

CHAPTER 36

Implementing the Deployment

In this chapter

Deployment Implementation Overview 611
Announcing the Deployment 612
Providing User Training and Support 612
  Setting Up User Training 613
  Setting Up User Support 613
Building Custom Packages 614
  Obtaining the Internet Explorer Administration Kit 614
  Using the Custom-Build Checklist 614
  Preparing to Build Custom Packages 614
    Preparing Distribution Servers 615
    Creating Any Custom Bitmaps You Want to Use 615
    Gathering the URLs for Start, Search, and Support Pages 616
    Including Other Applications with a Custom Package 617
  Using the IEAK Configuration Wizard 617
    Starting the IEAK Configuration Wizard 618
    Navigating in the IEAK Configuration Wizard 618
    Stage 1: Gathering Information 619
    Stage 2: Specifying Active Setup Parameters 622
    Stage 3: Customizing Active Setup 628
    Stage 4: Customizing the Browser 639
    Stage 5: Customizing Components 660
    Generating the Package 666
Signing Custom Package Files 666
Producing Distribution Media 667
  Designing Distribution 667
  Designing Other Distribution Media 668

Distributing Internet Explorer 668
Using Compact Discs and Floppy Discs 668
Using Distribution Sites on the Intranet or Internet 669
Running Active Setup 669
Troubleshooting Active Setup 669
Assisting Users During Installation 670

Deployment Implementation Overview

This chapter describes how corporate administrators can deploy custom versions of Internet Explorer packages to user groups in their organization. To deploy Internet Explorer:

- Announce the deployment to the organization.
- Provide user training and support.
- Configure Active Setup installation options.
- Build custom packages.
- Implement a download site.
- Produce distribution media.
- Distribute Internet Explorer to users.
- Monitor and assist user installation of the Internet Explorer browser, as needed.

Announcing the Deployment

After you finalize the deployment plan, inform your users about it. You may want to announce the plan through an e-mail memo or face-to-face meetings. Either way, it's important to communicate the benefits of using Internet Explorer 4, the details of the overall plan, and how the process will be implemented by each department or group.

Providing User Training and Support

Both user training and user support are critical to the success of deployment. Time and resources spent in training will decrease the demand for user support. In general, it's best to provide initial training before Internet Explorer is deployed and to make user support available at deployment.

Setting Up User Training

Tailor user training to the backgrounds and skills of each group in the organization. Consider separately the groups that need to be trained, the best presentation methods, and the amount of information appropriate to each.

Consider these groups of users:

- Average Internet Explorer users
- Power users
- User-support personnel
- New hires after deployment
- Others

Consider covering only the basics required by "average" Internet Explorer users before the deployment, and following up with a program tailored to the subject matter most needed by users (possibly based on support calls).

Setting Up User Support

Internet Explorer provides an **Online Support** option on the **Help** menu. By default, when users click **Online Support**, the Microsoft Support Web page, at **http://support.microsoft.com/support/**, is displayed in the browser window.

However, it's recommended that you create a Web page to provide online technical support for users in your organization. You can build custom packages of Internet Explorer that substitute the URL for your support page as the link used by **Online Support**.

Other resources available to users include:

- Internet Explorer Help.
- The Microsoft Internet Explorer Web site at **http://www.microsoft.com/ie/**.
- Microsoft Press® books on Internet Explorer 4. For more information, see Microsoft Press online at **http://mspress.microsoft.com/**. Books include:
  - *Microsoft Internet Explorer 4 Step by Step*
  - *The Official Microsoft Internet Explorer 4 Book*
  - *Microsoft Internet Explorer 4 At a Glance*

Building Custom Packages

You use the Internet Explorer Administration Kit (IEAK) Configuration Wizard to build custom packages of Internet Explorer that are tailored to meet the needs of user groups in your organization. You can specify all end-user setup options and control most browser features, Outlook Express features, the Active Desktop, Active Channels, security zones, and much more.

After you build custom packages, you distribute the packages to the appropriate user groups, and they install the customized versions of Internet Explorer on their desktops. Internet Explorer is installed with the settings and options you specified when building the custom package.

You can also use the IEAK Configuration Wizard to set up automatic browser configuration. Then, once Internet Explorer is installed on users' desktops, you can use the IEAK Profile Manager to manage Internet Explorer settings centrally, and automatically update the configuration of end users' computers. For more information, see Chapter 37, "Automatic Browser Configuration."

Obtaining the Internet Explorer Administration Kit

To obtain the IEAK, you must visit the Microsoft IEAK Web site at **http://www.microsoft.com/ie/ieak/** and register to download the IEAK. After registering and accepting the licensing agreement, you'll receive additional instructions on how to download the IEAK and your 10-digit customization key. You need the customization key to unlock the IEAK Configuration Wizard before you can build custom packages.

Using the Custom-Build Checklist

The Custom-Build Checklist is the tool you'll use to assemble everything you need to create the custom packages. The checklist saves you both planning and creation time because it helps you focus on decisions you need to make, items you need to create, and other information you need to gather before you begin to use the IEAK Configuration Wizard.

For more information, see Appendix J, "Custom-Build Checklist."

Preparing to Build Custom Packages

Decide how you will be distributing your custom package (compact discs, floppy disks, or download). After the IEAK builds your package, you will need to move the files to the selected media. If you build a downloadable package, you must move the package to the appropriate places on your distribution servers.

Preparing Distribution Servers

If you decide to distribute your browser packages from servers on your intranet or the Internet, gather the path to the servers and the URLs from which the files can be downloaded. Then, create a folder, such as "CIE," on each server to publish all the files and folders associated with your custom browser. For example, if you create server paths of C:\Webshare\Wwwroot\Cie and C:\Webshare\Ftproot\Cie on the hard disks of servers on your intranet, the corresponding URLs would be http://*computername*/cie and ftp://*computername*/cie.

Note When you are creating a browser package, the IE4 folder site will be appended to your URL.

Create the following directory structure:

Folder Name	Description
\Cie	Parent root directory for all files
\Cie\Bitmaps	Optional custom bitmap files that you plan to use

Creating Any Custom Bitmaps You Want to Use

You have the option to customize the following bitmaps in your browser. Place the bitmaps in the \Cie\Bitmaps folder before you run the IEAK Configuration Wizard.

- The custom icon used for the Active Setup Wizard that your users will run when they install the browser
- The custom-toolbar bitmap (that displays as a background for the buttons and menus)
- The custom-background bitmap for the CD-ROM Autorun screen (if you create a compact-disc package)
- The custom image for the CD-ROM buttons (if you create a compact-disc package)
- The custom Channel bar graphics and icons (if you create Active Channels)
- The custom icon used for the Lightweight Directory Access Protocol (LDAP) service (if you provide your own LDAP server)

For more information on how to create these graphics, see "Creating Customized Graphics" and "Create a Bitmap for the Autorun Splash Screen" in the IEAK Help.

The IEAK includes a number of sample graphics files you can use for custom packages. These files reside in the directory: \Ieak\Reskit\ Graphics\Samples after you install the IEAK.

In addition, you'll need to convert any 24-bit images to the 256-color palette. For information about how to do this, see "Editing Your Graphic" in the IEAK Help.

Note Custom backgrounds and buttons are displayed only on computers with 256-color (8-bit) display capabilities. On computers with 16-color (4-bit) display capabilities, a standard low-resolution background bitmap and button set is displayed.

Gathering the URLs for Start, Search, and Support Pages

The start page, also called the home page, appears when the user clicks the **Home** button. Internet Explorer can show a default home page, or you can specify another URL, such as your organization's internal Web home page.

When users click the **Search** button on the toolbar, a default Search page appears on the Search bar in the pane on the left side of the browser window. The Search bar enables the user to see the search query and search results at the same time. The default page that appears in the Search bar comes with a choice of search engines. You can specify another search page to appear in the Search bar if you want.

You can create a user-support page that is linked to **Online Support** on the **Help** menu for Internet Explorer. You will be prompted for the start, search, and support page URLs when you run the IEAK Configuration Wizard. If you do not specify these URLs, Internet Explorer will install with default URLs.

Including Other Applications with a Custom Package

If you would like to include custom components inside the Internet Explorer installation process, such as a custom FTP client or communication software, the IEAK includes a utility called IExpress. IExpress is a tool that creates custom self-installing, self-extracting packages (or .cab files) of applications.

You use the step-by-step IExpress Configuration Wizard to package applications so that they can be installed by Active Setup along with Internet Explorer. This can make the rollout of multiple applications much easier, as they can all be done at the same time with Active Setup. The IExpress program resides in the directory: C:\Program Files\Ieak\Tools\Iexpress. For more information on how to use the wizard, see Appendix L, "IExpress Configuration Wizard."

Using the IEAK Configuration Wizard

You use the IEAK Configuration Wizard to create custom packages that install customized versions of Internet Explorer for user groups. The IEAK Configuration Wizard is a step-by-step process organized into five stages.

Important You should allow one hour to configure the first package from start to finish. It's best to do this in one session; otherwise, you may have to respecify some options. Once you configure a package, each subsequent package will require less time, because you can reuse some of the values you specified for a previous package.

Depending on the options you choose, some pages may not appear; however, each stage requires you to complete at least four wizard pages.

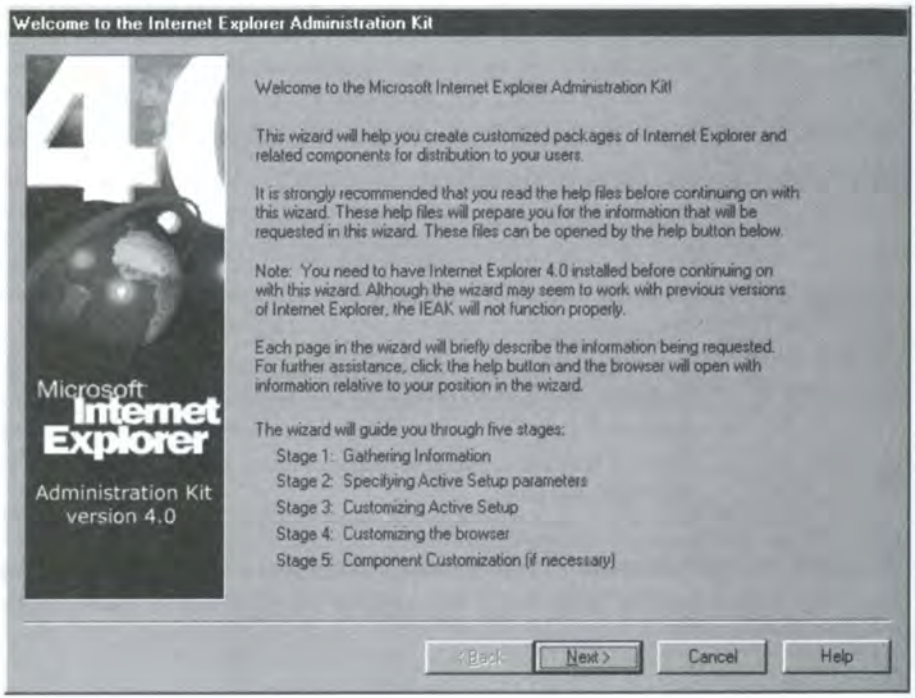
Starting the IEAK Configuration Wizard

▶ **To start the IEAK Configuration Wizard**

1. On the **Start** menu, click **Run**.

   The **Run** dialog box opens.

2. Type **ieakwiz.exe**.
3. Click **OK**.



Navigating in the IEAK Configuration Wizard

To	Click
Display the next page, and accept the values on the current page	**Next**
Display any previous page (You may have to reenter some of the values you've entered.)	**Back**
Exit this package	**Cancel**

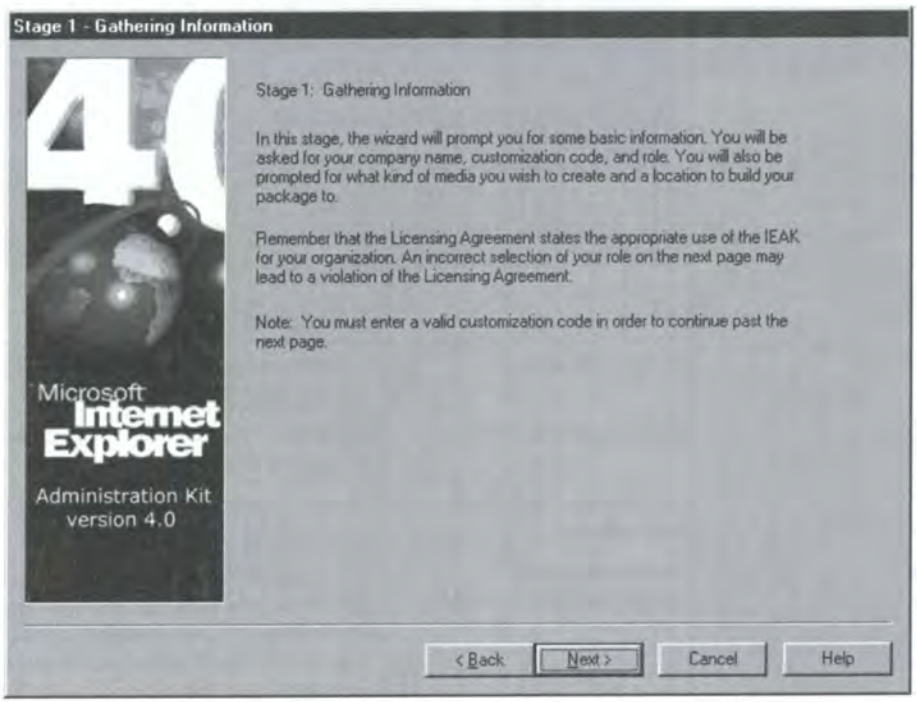
The following sections display all the wizard pages you can use to specify the custom package. Each page is followed by a table that describes the features and options available on that page.

Stage 1: Gathering Information

Before beginning to navigate the IEAK Configuration Wizard, be sure you have your completed Custom-Build Checklist available to speed up the configuration process. The checklist records all the information you need to supply as well as all the options you want to select. For more information, see Appendix J, "Custom-Build Checklist."

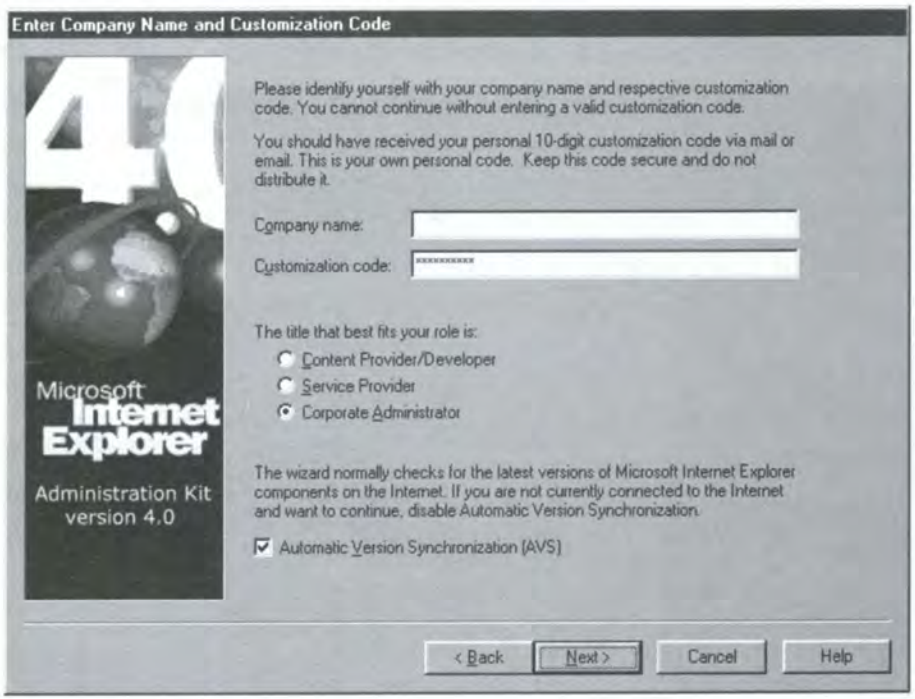
In Stage 1, you will:

- Provide your company name and 10-digit customization code. You received the customization code from Microsoft when you registered the IEAK.
- Select your role—Content Provider or Developer, Service Provider, or Corporate Administrator—based on your license agreement.
- Select the language of the browser package you are creating.
- Specify the destination folder for creating your browser package.
- Select any additional distribution methods you plan to use: compact disc, single floppy disk, or multiple floppy disks.

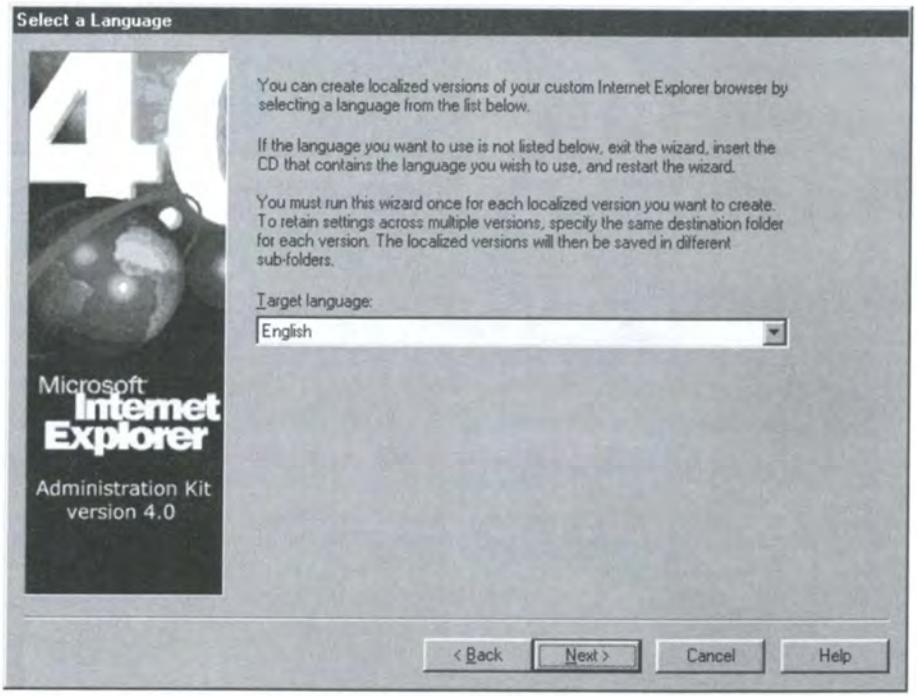


The IEAK Configuration Wizard pages in Stage 1 are:

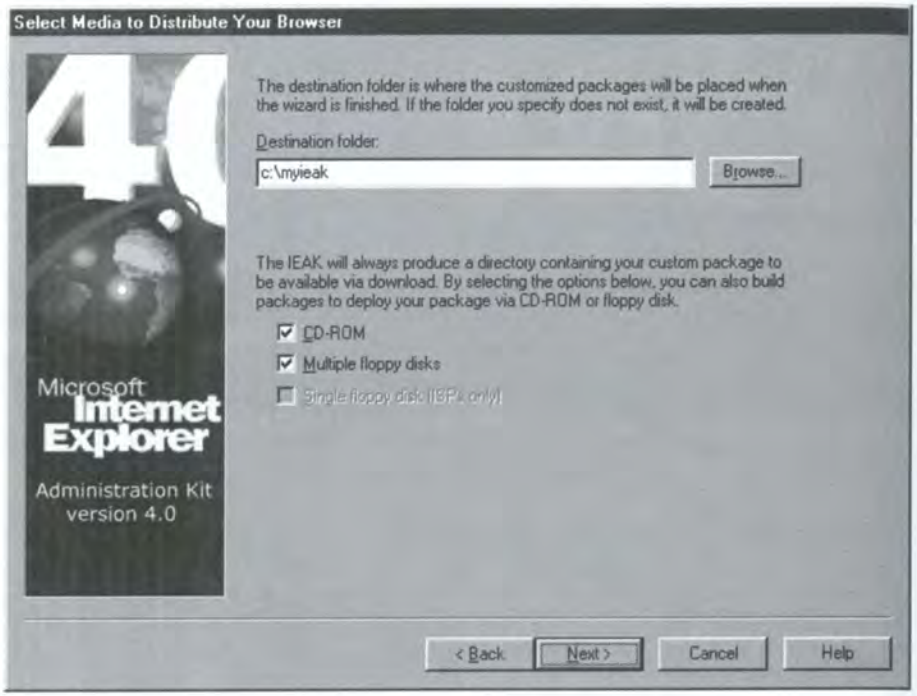
- Enter Company Name and Customization Code
- Select a Language
- Select Media to Distribute Your Browser



Option	Description
Company name	Type the name of your company. This information is put in the Registry for identification.
Customization code	Type the code you received from Microsoft when you registered your IEAK.
The title that best fits your role is	Select **Corporate Administrator**.
Automatic Version Synchronization (AVS)	This option is selected and shaded the first time you run the wizard to build a custom package, because you must download the components needed from the Internet. When you rebuild the custom package or build additional custom packages, you can clear this option if you don't want to connect to the Internet or update the components.



Option	Description
Target language	Type the name of the language for the Internet Explorer package you're creating. You need to run the wizard for each language you want to create.



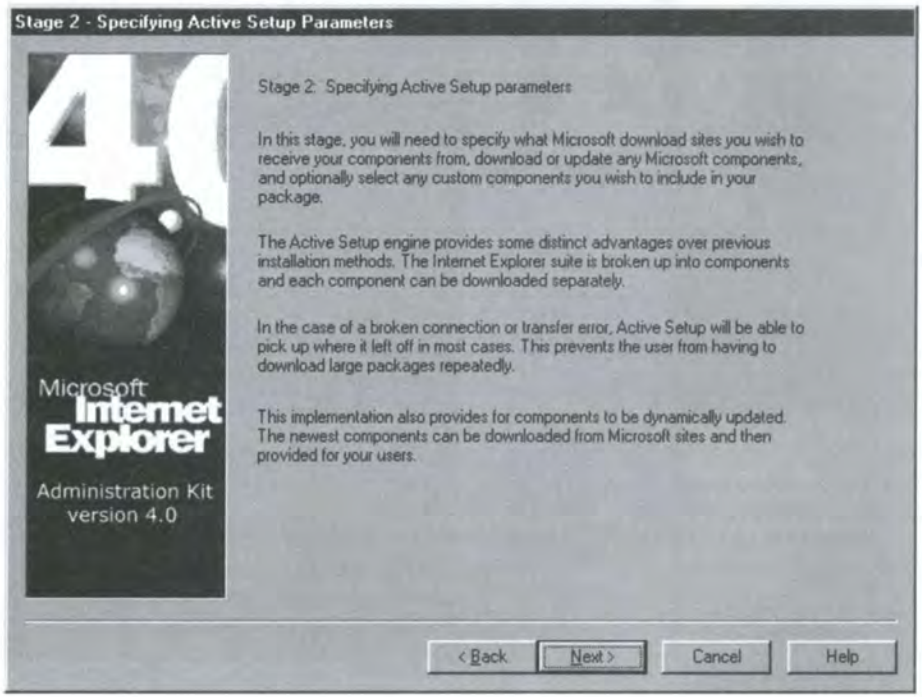
Option	Description
Destination folder	Type the name of the folder in which you want to place the customized package.
Deployment media	If you want to make the package available on compact disc and/or floppy disks, in addition to the destination folder, click one or both of these options.

Stage 2: Specifying Active Setup Parameters

Active Setup is a small, Web-based setup package that lets users install the latest Internet Explorer components directly from a Web site. It is small (about 400K), so it can be run from a single floppy disk or downloaded quickly over the Internet. Active Setup not only manages the entire installation process, but also can search to see what components are already installed, and alert users or administrators when there are newer versions available. When Active Setup downloads Internet Explorer 4, it breaks it up into several small segments. This makes it possible, in the event of a failure or dropped connection, to restart an installation from where it was interrupted, instead of having to start over from the beginning. For more information about Active Setup, see Chapter 2, "Phase 1: Active Setup."

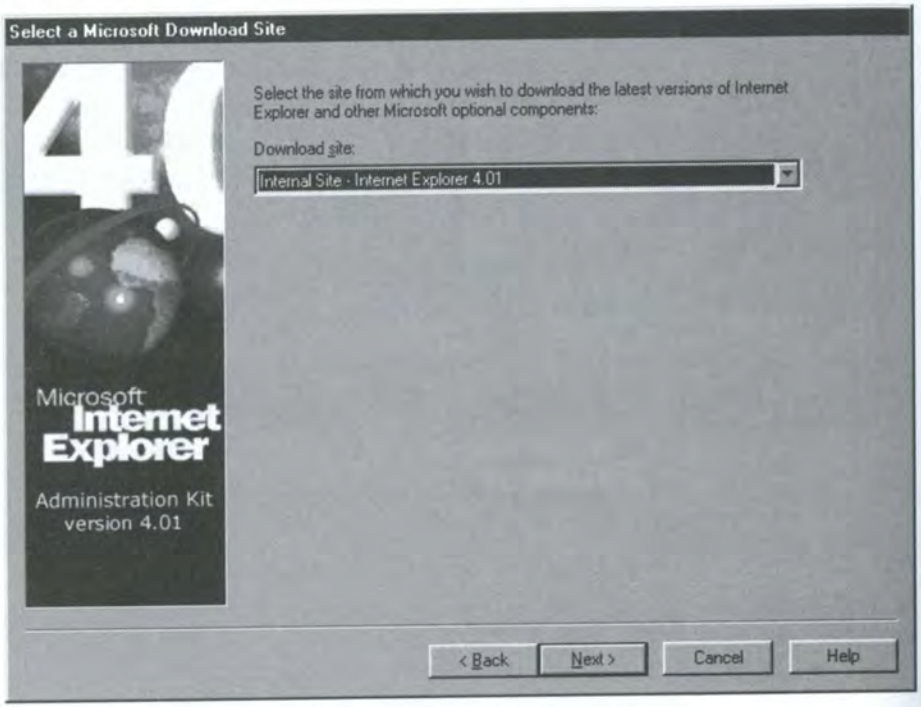
In Stage 2, you will:

- Select the Microsoft download sites from which you receive your components.
- Download or update Microsoft components used to build the package.
- Select any custom components you want to include.
- Select the trusted publisher that signs your custom browser package. (For more information about trusted publishers, see Part 7, "Security and Privacy.")



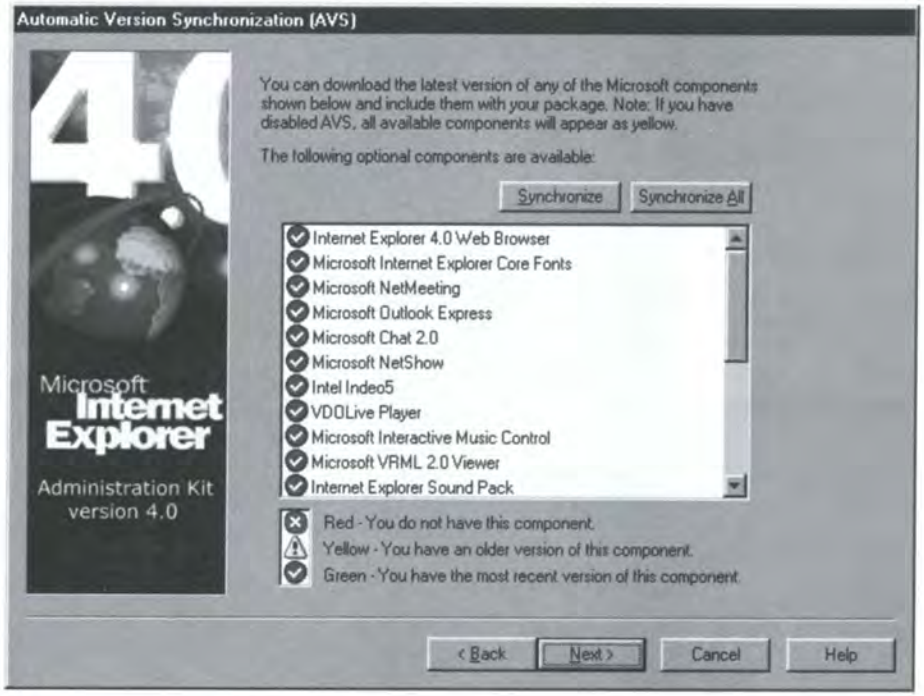
The IEAK Configuration Wizard pages in Stage 2 are:

- Select a Microsoft Download Site
- Automatic Version Synchronization (AVS)
- Specify Custom Active Setup Components
- Specify Trusted Publishers



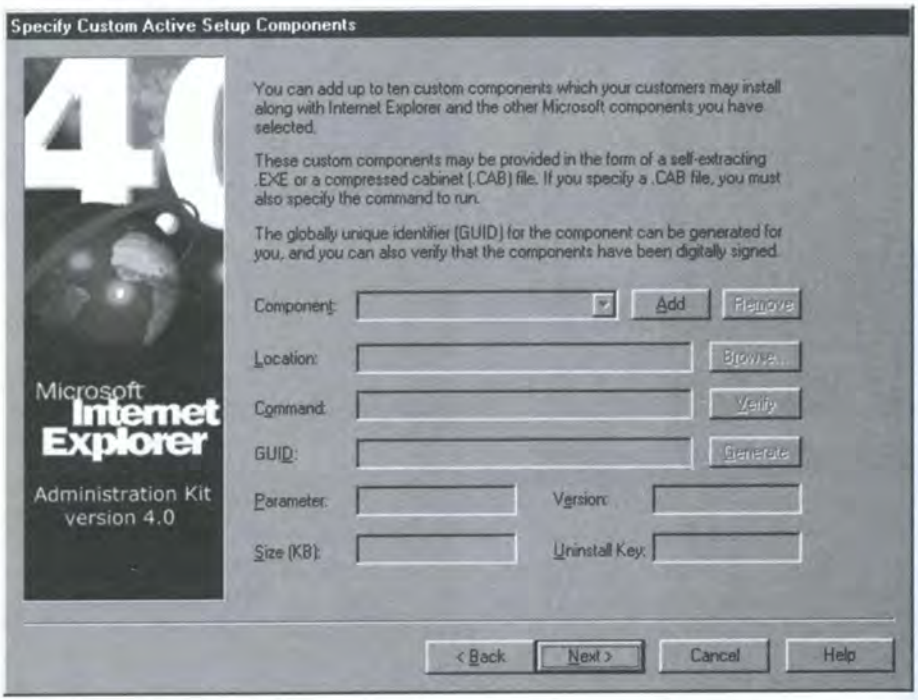
The IEAK automatically loads the list of sites from which you can choose.

Option	Description
Download site	Select the URL of the site—either HTTP or FTP—from which you will download the latest versions of Internet Explorer and other Internet Explorer components.



Option	Description
Synchronize	Select components, and click here to synchronize only the Internet Explorer components you want to update. The wizard downloads the latest versions of the selected components.
Synchronize All	Click to synchronize all the listed Internet Explorer components. The wizard downloads the latest version of all the Internet Explorer components.

With this wizard page, you can see quickly whether any updates have been posted for the Internet Explorer 4 components. A red signal means that you have not downloaded the component; a yellow signal means that a newer version is available; and a green signal means you already have the latest version.

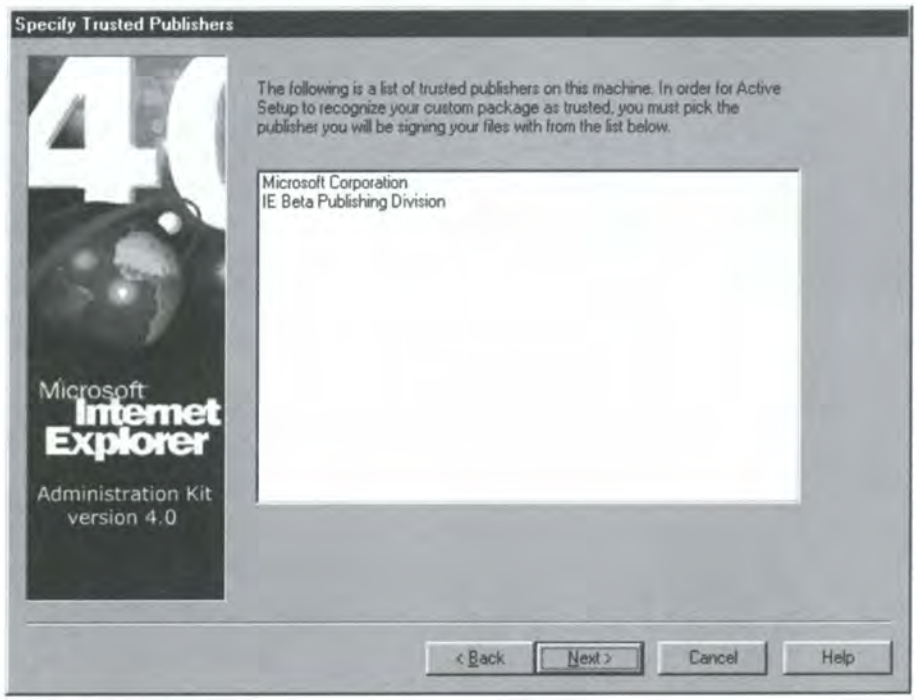


Here you can choose to add any custom components you may have built earlier with IExpress. You can add up to 10 custom components that your users can install at the same time they install the browser. These components can be self-extracting, executable (.exe) files or compressed cabinet (.cab) files.

It is recommended that you sign any custom code. Code-signing lets users know they can trust your code before they download it to their computers. The default settings in Internet Explorer will reject unsigned code.

Option	Description
Component	Type the name of your component in this box. This name will appear in the setup screen when users install your software.
Location	Click **Browse**, or type the path to the self-extracting .exe file or the .cab file for the component.
Command	*For .cab files only.* Type the command needed to run the .cab file.
GUID	If your program already has a globally unique identifier, or GUID, type it in this box. If your program doesn't have a GUID, then click **Generate** to assign a GUID. A GUID establishes a unique identity for programs, objects, and other items. For more information on GUIDs, see "What is a Globally Unique Identifier?" in the IEAK Help.

Option	Description
Parameter	*For .exe files only.* Type any command-line switches you want to run with the .exe file.
Size (KB)	Type the size of the program.
Version	Type a version number to help track versions of your program and to ensure that the latest version is installed.
Uninstall Key	If you want to allow users to uninstall this component, type the registry entry, including both the DISPLAYNAME and UNINSTALLSTRING values in **HKEY_LOCAL_COMPUTER/Software/Microsoft Windows/CurrentVersion/Uninstall/**.



Option	Description
Publisher list	Select the publisher you will use to sign your files. For information about how to add a trusted publisher, see Part 7, Chapter 28, "Digital Certificates." For information about signing files, see the "Signing Your Programs" section of the IEAK Configuration Wizard Help.

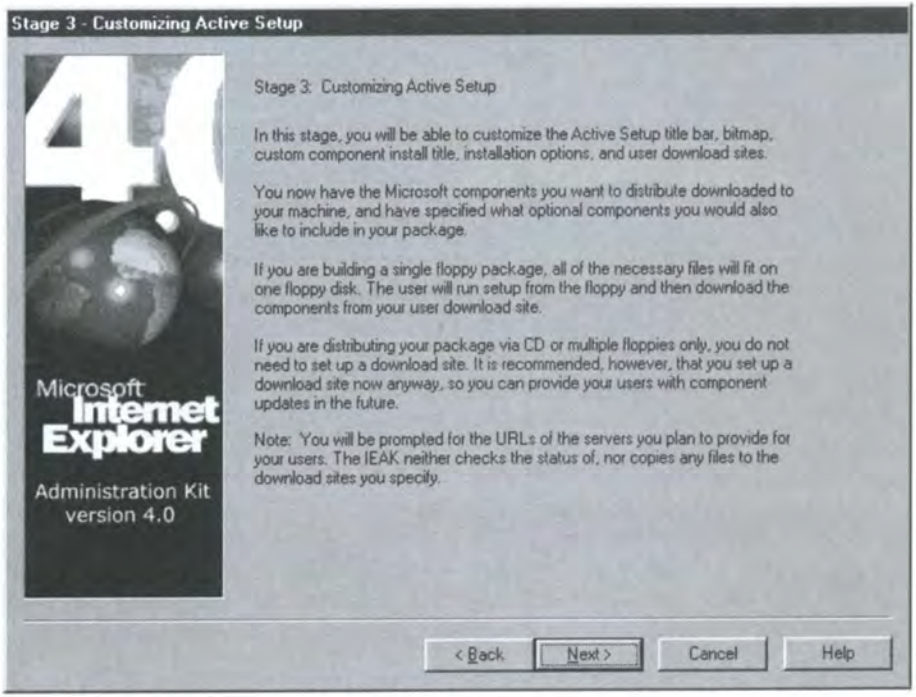
The IEAK Configuration Wizard will display the list of trusted publishers installed on your machine. In order for Active Setup to recognize your custom package as trusted, you must select the publisher that will sign your files.

Stage 3: Customizing Active Setup

In Stage 3, you will:

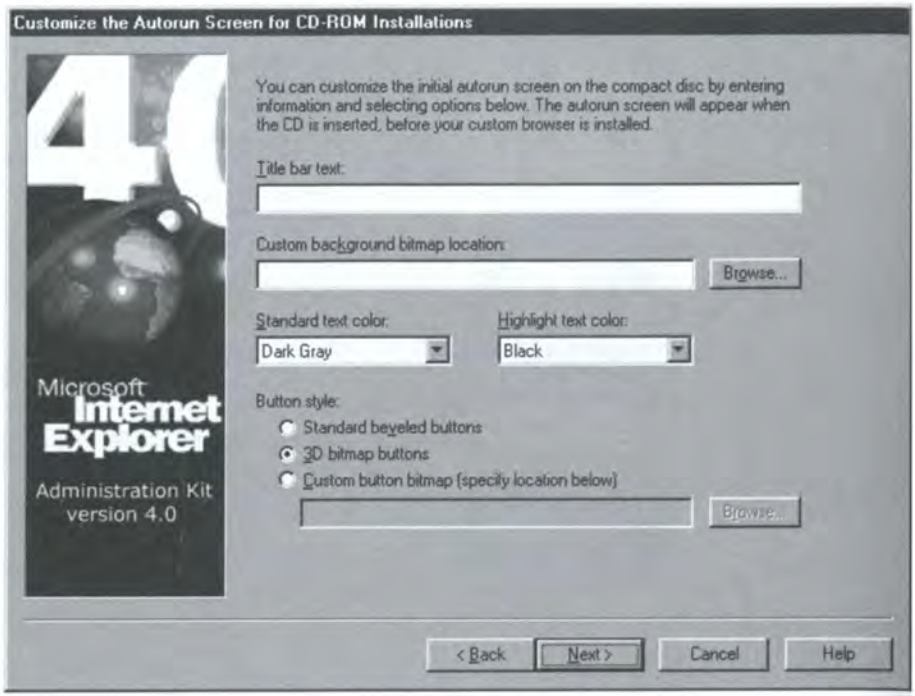
- Specify an optional custom CD-ROM Autorun screen, if you are creating a CD-ROM package.
- Specify optional custom Active Setup Wizard title bar text and bitmap. These settings affect how Setup appears to the user.
- Choose whether to install the package "silently," with few or no prompts to the user.
- Specify up to 10 unique installation options, and determine which components are included with each option.
- Specify up to 10 sites from which your package will be downloaded.
- Specify a unique version number for your browser customizations.
- Specify the directory in which you want Internet Explorer to be installed on your users' computers.
- Specify whether you want to allow the Windows Desktop Update to be installed to integrate Web browser functionality into users' desktops and folders.

(For more information about Active Setup, see Part 1, Chapter 2, "Phase 1: Active Setup.")



The IEAK Configuration Wizard pages in Stage 3 are:

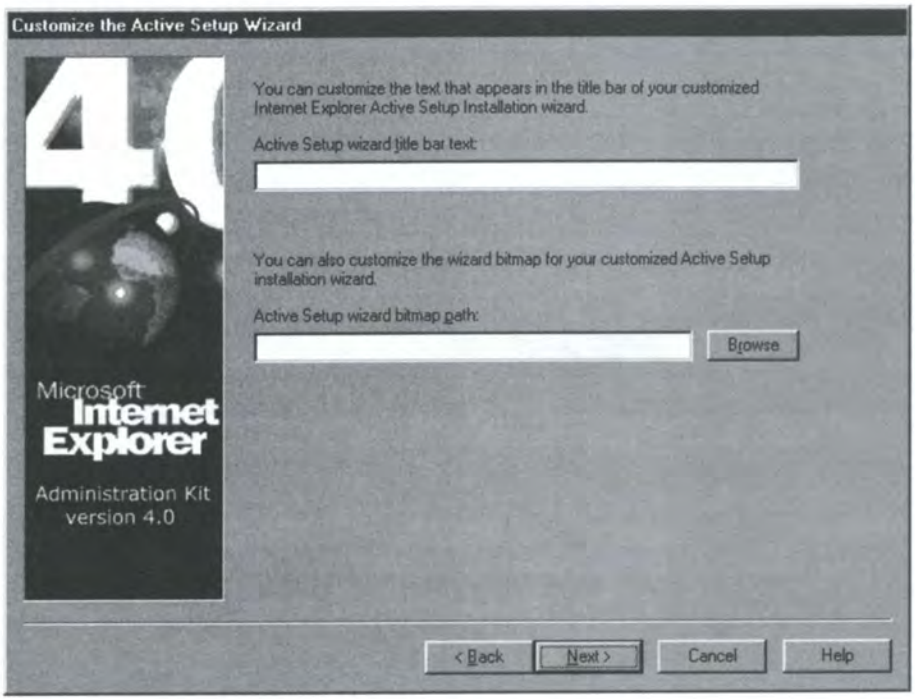
- Customize the Autorun Screen for CD-ROM Installations
- Customize the Active Setup Wizard
- Custom Components Install Section
- Select Silent Install
- Select Installation Options
- Specify Download URLs
- Select Version Number
- Specify Where You Want to Install Your Browser
- Integrating the Web Desktop Update



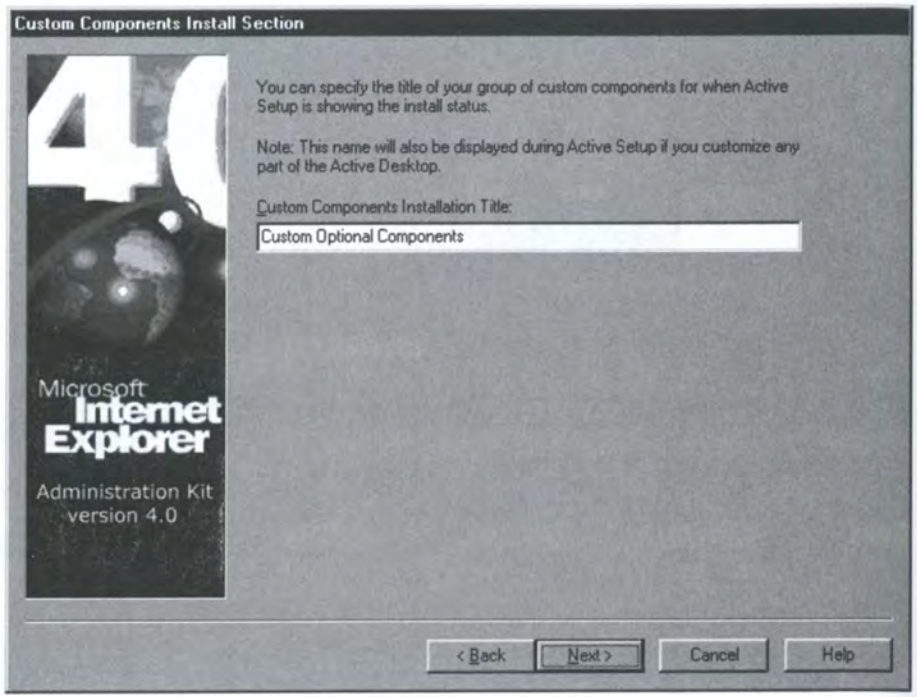
This wizard page displays only if you chose to distribute packages on compact disc (that is, you selected the **CD-ROM** check box in Stage 1 on the wizard page "Select Media to Distribute Your Browser").

Autorun is a technology that was introduced with Windows 95. The wizard creates an Autorun program and places it in the file system for the compact disc. Autorun will launch the appropriate startup screen when the user inserts the compact disc.

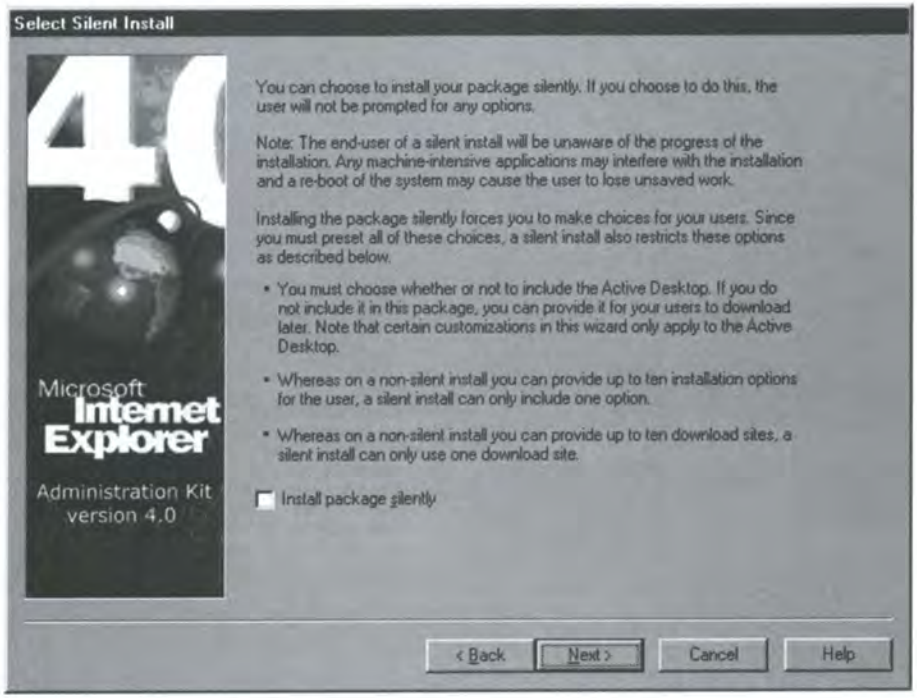
Option	Description
Title bar text	Type the text that you want to appear in the title bar of the user's Autorun page.
Custom background bitmap location	If you want a bitmap to appear behind the title bar text, type the path to its location here. Make sure that the background color doesn't conflict with the text color.
Standard text color	Select a color for text that isn't part of a link.
Highlight text color	Select a color for link text.
Button style	Click the button style to be used.
Custom button bitmap	*For Custom button bitmap only.* Click **Browse** to locate the path to the image.



Option	Description
Active Setup wizard title bar text	Type the text you want to appear in the title bar of the end user's Active Setup Wizard.
Active Setup wizard bitmap path	Type the path to a bitmap, or click **Browse** to locate the path to the image.



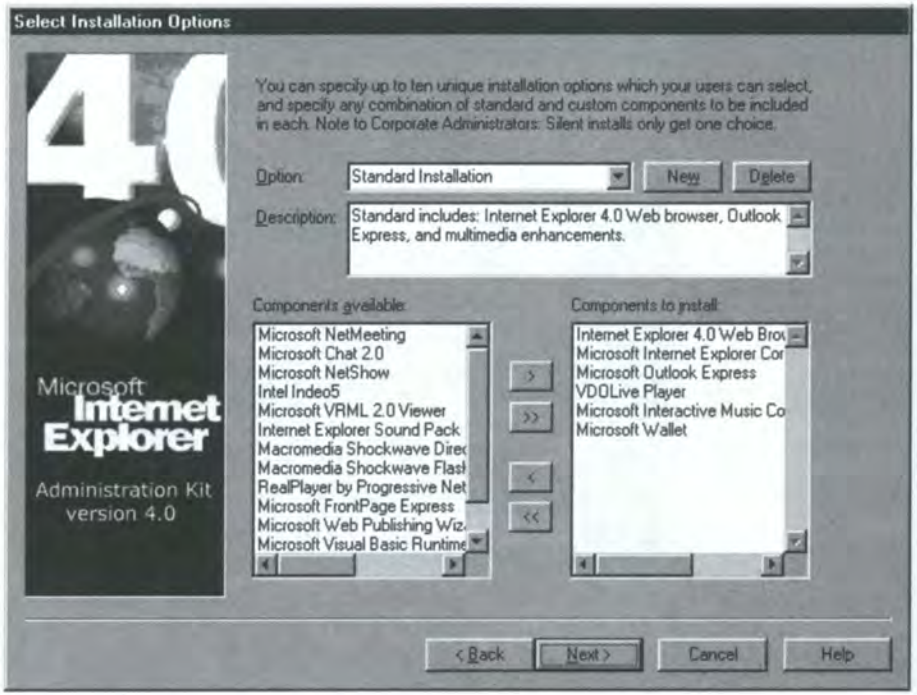
Option	Description
Custom Components Installation Title	Type the text you want to appear when Active Setup is installing your custom additions to the Internet Explorer package.



Option	Description
Install package silently	If you do not want end users to specify preferences during setup, select the check box. To allow end users to specify their preferences during setup, clear the check box.

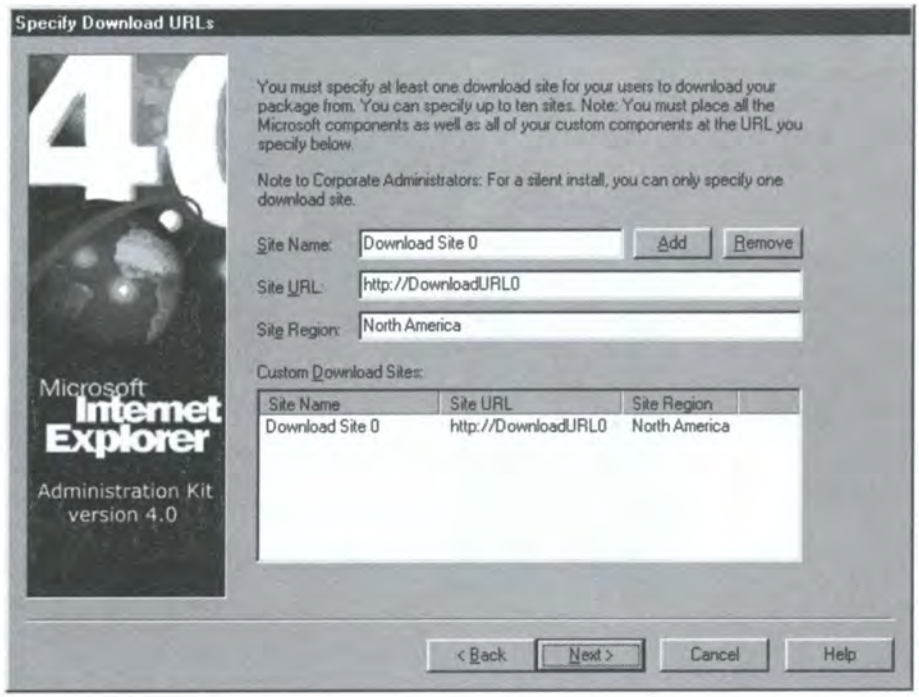
Installing the package silently forces you, as administrator, to make choices for your users. Because the user is not presented with any choices, you must pre-configure each of the Internet Explorer installation options. A silent installation also restricts the options outlined below. For a silent installation:

- You must choose whether or not to include the Windows Desktop Update or Active Desktop functionality. If you do not include it in this package, you can provide it for your users to download later.
- You can provide only one installation option. With a regular installation, you can provide up to 10 installation packages for your users.
- You have only one site available for downloads. With a regular installation, you can provide up to 10 download sites.



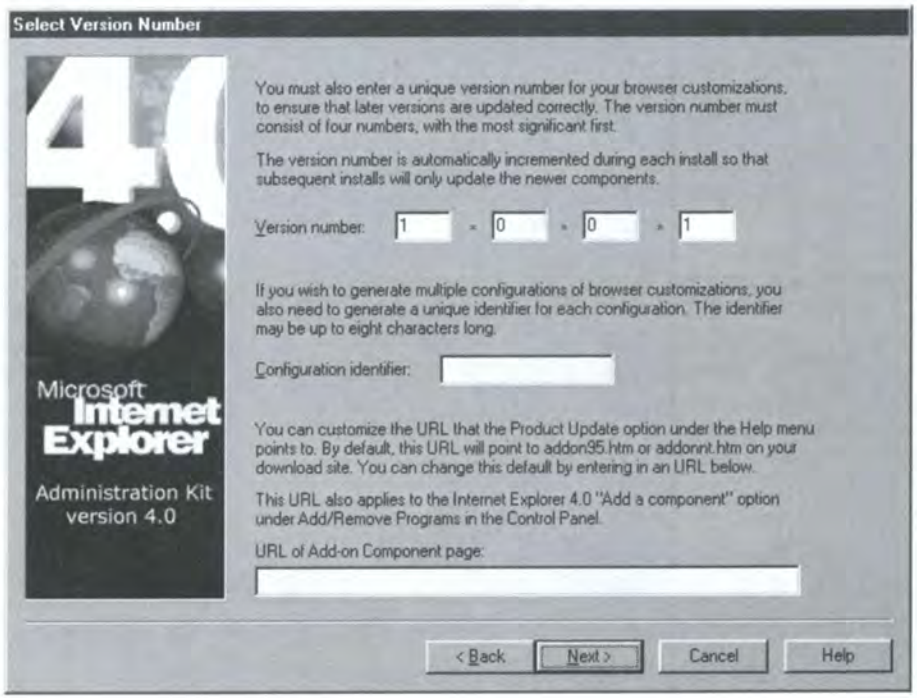
This wizard page enables you to do two things. First, you can customize the Minimal, Standard, and Full Installation packages to contain any components you want. Use the arrow keys to move the components back and forth to create customized packages. However, you aren't limited to just those three types of installations. You can create up to 10 installation packages that include whatever configuration you want, your name, and descriptions of those packages.

Option	Description
Option	Select the option you prefer, or click **New** to add a custom option.
Description	Type a description of this custom package that your end users will see when installing Internet Explorer. Provide enough information so that your users can make a decision about which software to install.
Components available	Lists the components that you made available on the Automatic Version Synchronization page. (To add additional components, click **Back** until you reach that page.)
Components to install	Lists the components to be included in this installation option.



You must complete this wizard page for each download URL.

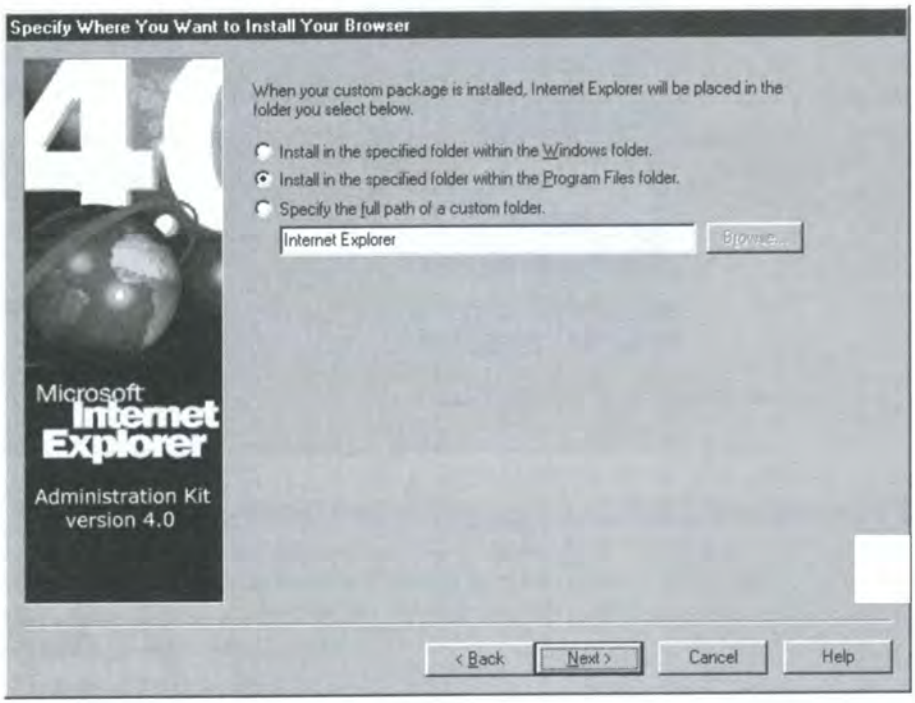
Option	Description
Site Name	Click **Add** to designate a download site. If you want, you can modify the name created by the wizard. Do not use commas in the name.
Site URL	Enter the URL for your HTTP or FTP server. IEAK appends the folder IE4site to the URL. Active Setup looks for this URL when installing Internet Explorer for this custom package.
Site Region	Enter the location of the site, such as the city, state, region, or country.
Custom Download Sites	Lists all the download sites.



These options ensure that the latest version of each customized component and feature is installed every time.

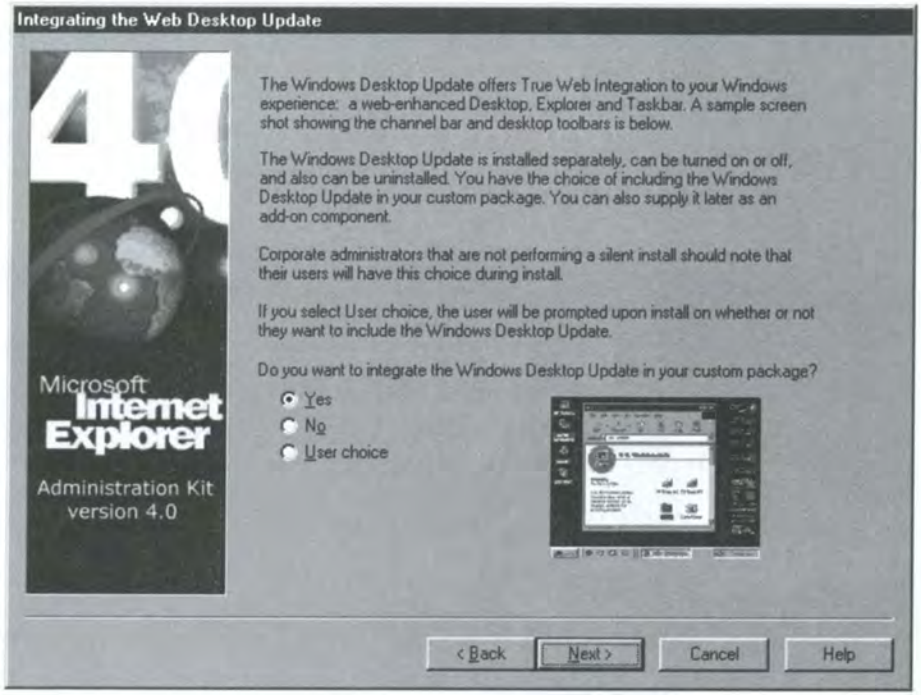
Option	Description
Version number	If you want, you can revise the version number. The wizard increments this number each time you run the wizard. The first digit is the most significant; for example, 2 0 0 0 is newer than 1 0 0 6.
Configuration identifier	Type a unique number for this version. The configuration identifier is an 8-digit code that identifies your customized version of the browser. Using this code can prevent the user from installing a previous version over a newer version of your customized browser. For the configuration identifier to prevent an earlier version from being installed, the company name for both browsers must be the same. You specified the company name in Stage 1 of the IEAK Configuration Wizard.
URL of Add-on Component page	If you want to allow end users to update Internet Explorer from the **Help** menu, type the URL of addon95.htm.

When new versions of Internet Explorer become available, users will be able to select **Product Updates** from the **Help** menu in Internet Explorer 4 to update their Internet Explorer. To reach this page, users can also click the **Add/Remove Programs** icon in the Control Panel, click **Microsoft Internet Explorer 4.0**, and then click **Add/Remove**. If you want users to obtain software updates from another location that you have customized, specify that URL in the **URL of Add-on Component page** box.



Option	Description
Install in the specified folder within the Windows folder	Click this option, and enter the name of the folder.
Install in the specified folder within the Program Files folder	Click this option, and enter the name of the folder or accept the default **Internet Explorer** option.
Specify the full path of a custom folder	Click and enter the path and folder name, or click **Browse** to locate it.

Active Setup installs Internet Explorer in the folder you specify on this wizard page. If the path you specify doesn't exist on the user's hard disk, Active Setup creates it.

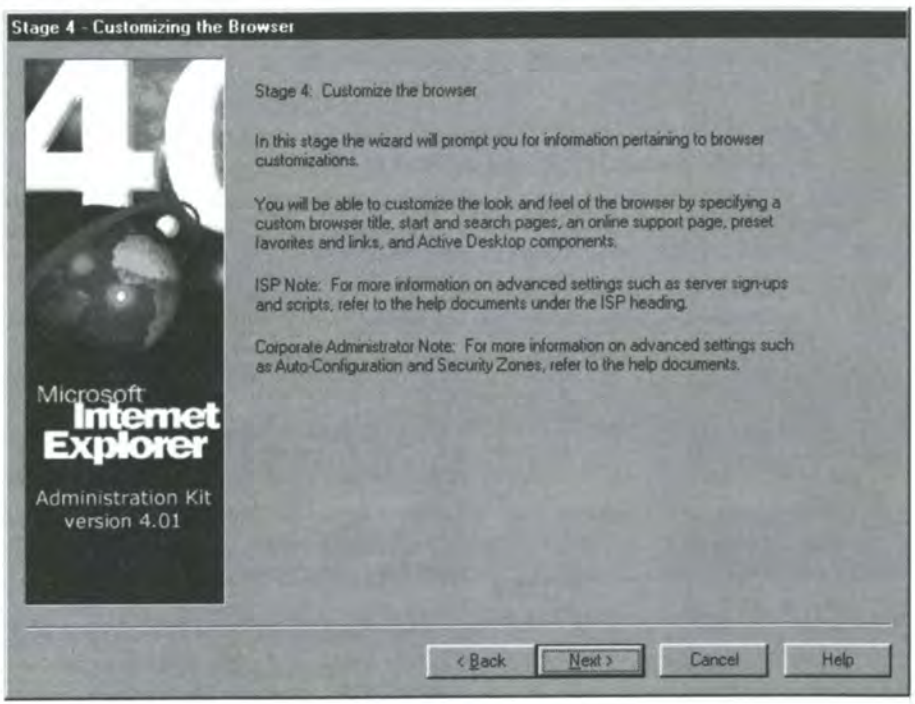


Option	Description
Yes	Click this option to install the Windows Desktop Update on users' computers.
No	Click this option if you don't want to install the Windows Desktop Update on users' computers.
User choice	Click this option to allow users to choose whether to install the Windows Desktop Update on their computers.

Stage 4: Customizing the Browser

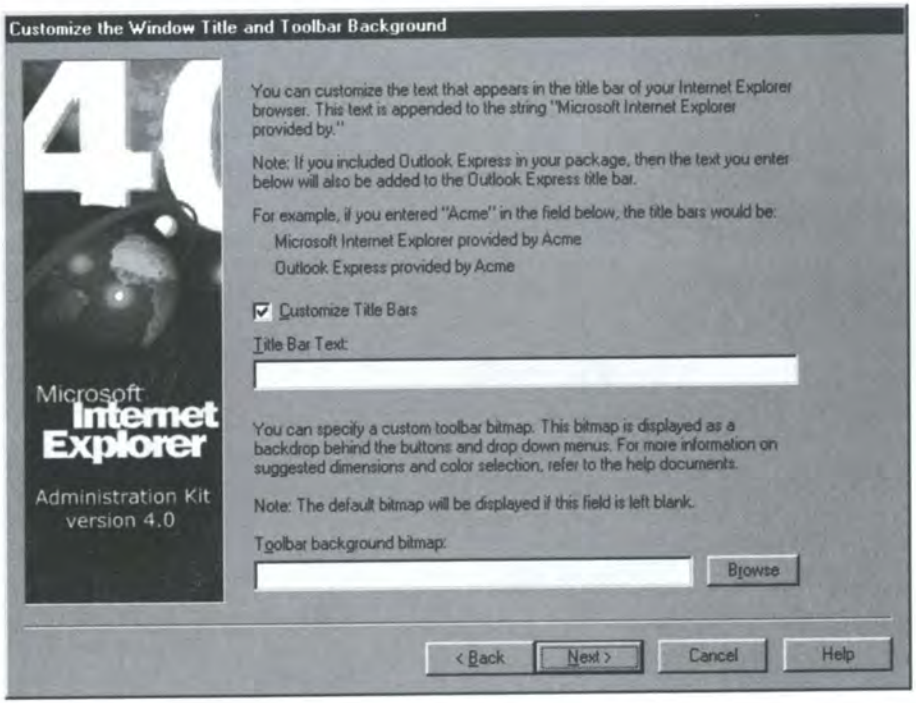
In Stage 4, you will:

- Specify browser title bar text and a toolbar background bitmap.
- Specify start, search, and online-support pages for the browser.
- Specify favorites, Favorites folders, and links for the Links bar.
- Specify welcome messages and desktop wallpaper.
- Specify the Active Channels that appear on users' desktops.
- Specify software distribution channels to update software on user's computers.
- Specify the Active Desktop items that appear on users' desktops.
- Specify the desktop toolbars that appear on users' desktops.
- Specify custom folders for My Computer and Control Panel.
- Specify a custom browser user agent string.
- Specify automatic browser configuration settings.
- Specify Internet Proxy settings.
- Specify custom settings for site certificates and Authenticode Security.
- Specify custom settings for security zones and content ratings.

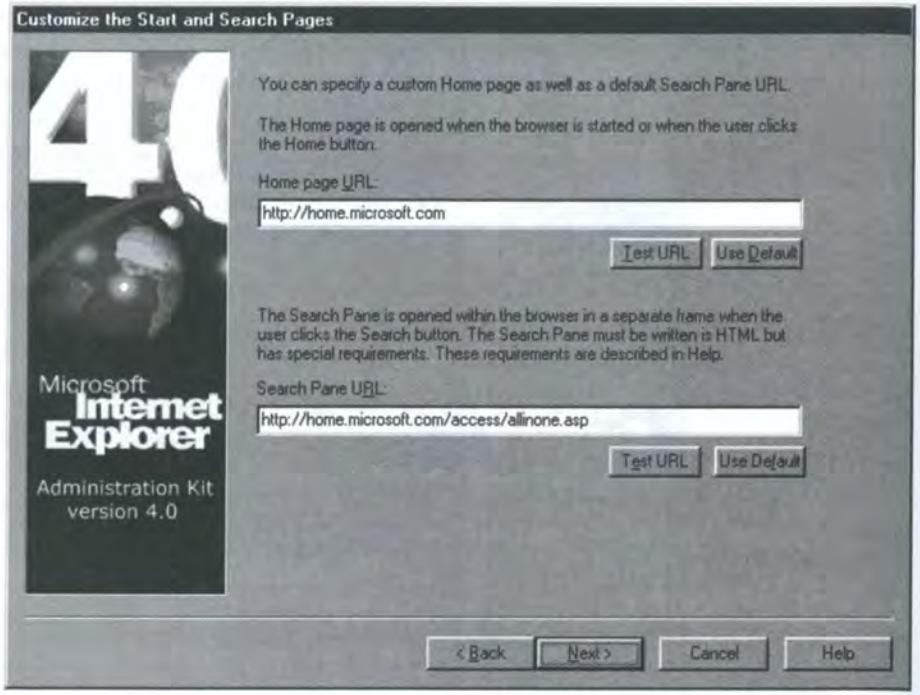


The IEAK Configuration Wizard pages in Stage 4 are:

- Customize the Window Title and Toolbar Background
- Customize the Start and Search Pages
- Specify an Online Support Page for Your Browser
- Favorites Folder and Links Customization
- Customize the Welcome Message and Desktop Wallpaper
- Customize the Active Channel bar
- Customize Software Update Channels
- Specify Active Desktop Components
- Customize Desktop Toolbars
- My Computer and Control Panel Webview Customization
- User Agent String Customization
- Automatic Browser Configuration
- Specify Proxy Settings
- Site Certificate and Authenticode Settings
- Security Zones and Content Ratings Customization



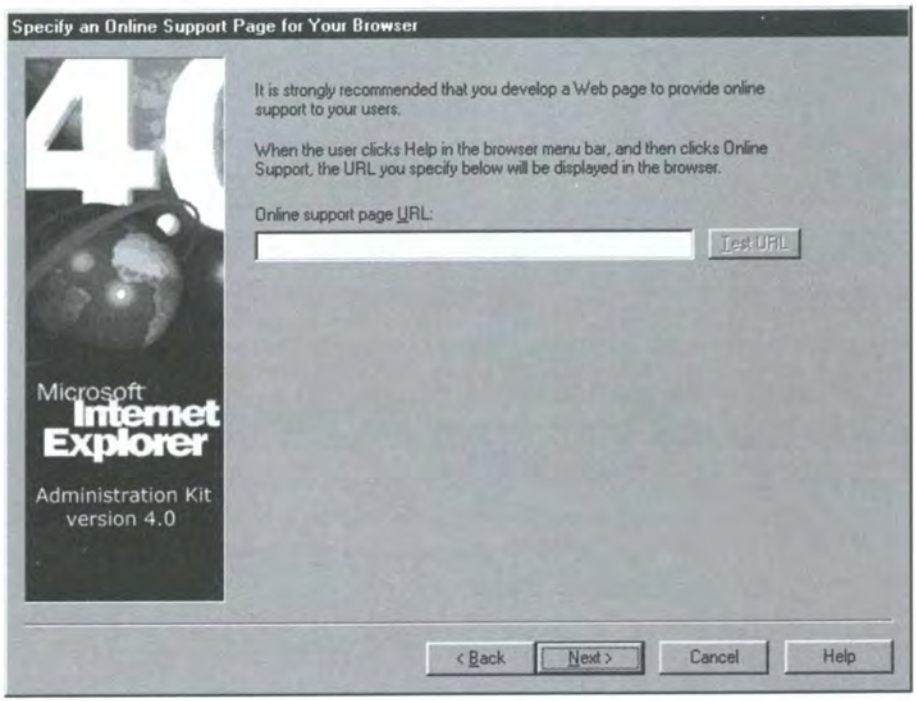
Option	Description
Customize Title Bars	Select this check box to customize the browser title bars (and Outlook Express, if included in the package).
Title Bar Text	Type the text that you want to follow the phrase: "Microsoft Internet Explorer provided by."
Toolbar background bitmap	Type the path and file name for the bitmap to be displayed in the background behind the Internet Explorer toolbar buttons, or click **Browse** to locate it.



Option	Description
Home page URL	To use the default Internet Explorer home page, click **Use Default**. To use another home page, type the URL of the home page, and then click **Test URL** to ensure that the URL is correct.
Search Pane URL	To use the default Internet Explorer Search Pane, click **Use Default**. To use another Search bar, type the URL of the Search bar, and then click **Test URL** to ensure that the URL is correct.

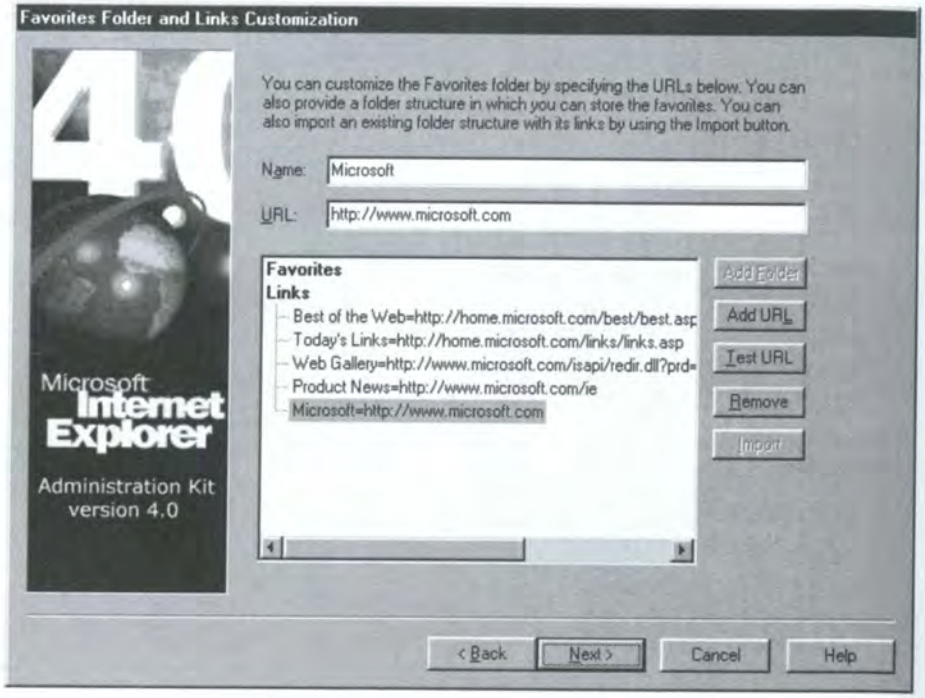
The Internet Explorer 3 Search-page functionality has been replaced with the Explorer Search bar—a pane that slides in on the left side of the screen. To load the Search bar, users simply click the **Search** button on the Internet Explorer 4 Standard toolbar. For more information about the Explorer Search bar, see "Explorer Bars" in Part 2, Chapter 9, "Browser Features and Functionality."

Important The Search bar lists search results in the Search bar pane, and when a user clicks a search-results link, the page is displayed in the main browser window, while the search-results list remains visible in the Search bar (until the **Search** button on the toolbar is clicked again). This functionality requires that special tags be included in the Search page. To learn more about creating a page for a custom Search bar, see "Explorer Bars" in Part 2, Chapter 9, "Browser Features and Functionality."



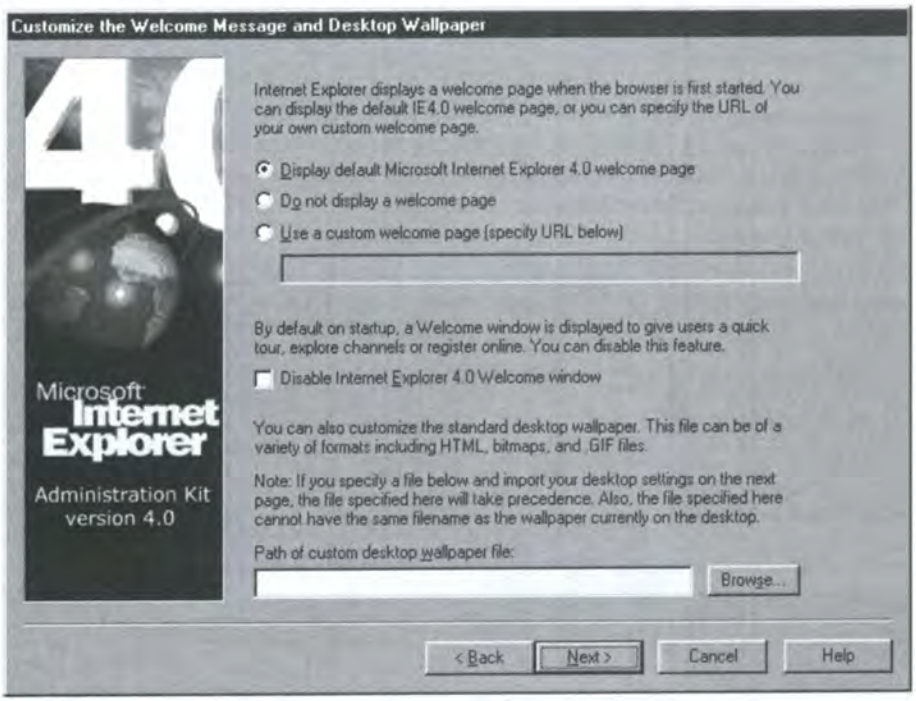
Option	Description
Online support page URL	Type the URL of the Web page that you created to offer technical support, and then click **Test URL** to ensure that the URL is correct.

This page will appear when your users click **Online Support** on the **Help** menu in Internet Explorer 4.



Option	Description
Name	Type a name for the Favorite or link.
URL	Type a URL for the Favorite or link.
Add Folder	To insert a hierarchical directory into the Favorites list, which can include more Favorites, click **Add Folder**.
Add URL	Select **Favorites** or **Links** or a folder, and then click **Add URL** to add its URL.
Test URL	You can click **Test URL** to ensure that the URL is correct.
Import	Select **Import** to point the IEAK to a link or a folder of links that you would like to import into the package.

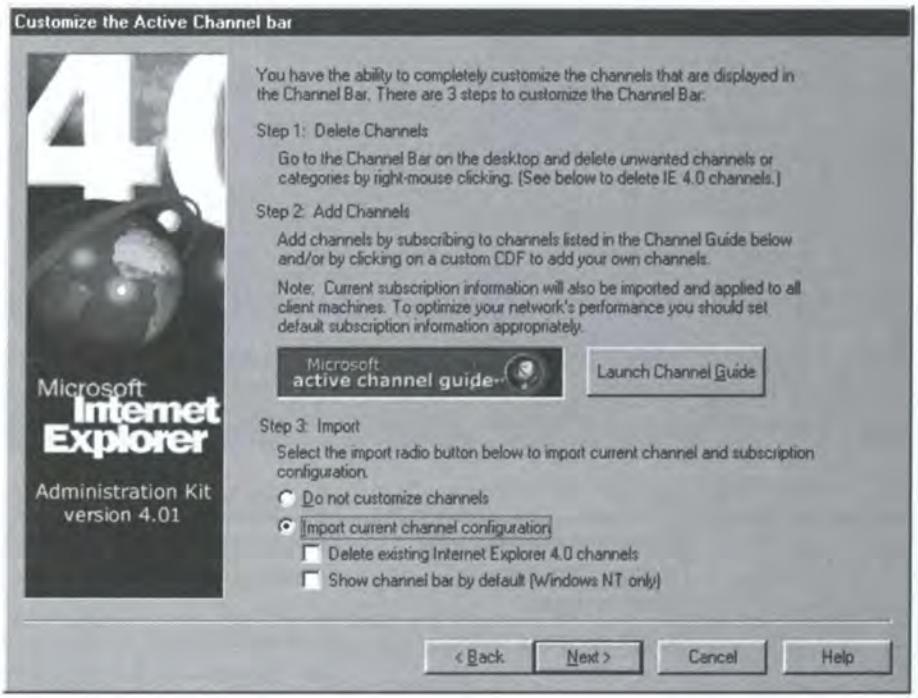
The favorites you specify on this wizard page appear in the Favorites folder of end users' computers. For example, you could add key URLs for your organization, such as the Help Desk and the Human Relations Web pages.



Option	Description
Display default Microsoft Internet Explorer 4.0 welcome page	Click here to choose the default Microsoft Internet Explorer 4 welcome page.
Do not display a welcome page	Click here if you don't want to display a welcome page. The first page that is displayed will be the home page.
Use a custom welcome page (specify URL below)	Click here, and type the URL for your custom welcome page.
Disable Internet Explorer 4.0 Welcome window	Click here to disable the Internet Explorer welcome window, which displays by default on the user's desktop when the Windows Desktop Update is installed.
Path of custom desktop wallpaper file	Type the URL for your custom desktop wallpaper, which can be a .bmp, .gif, or .htm file, or click **Browse** to locate the file.

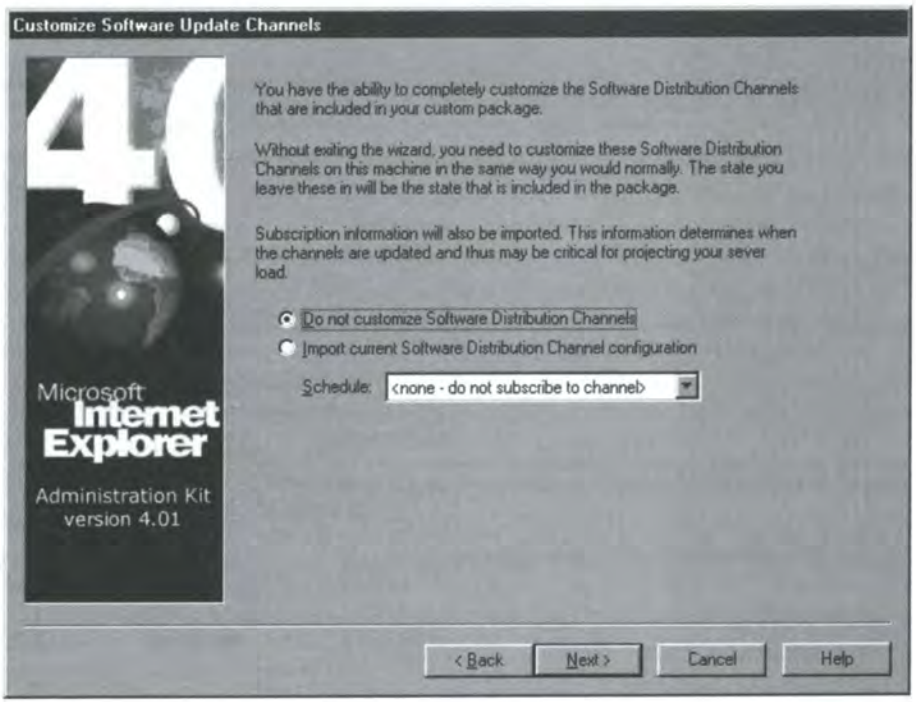
Internet Explorer displays a Welcome page the first time the browser is launched. You can display the default Internet Explorer Welcome window, or you can specify the URL of your own custom welcome page. The welcome page is not the same as the home page, which is the page that opens each time you start your browser (after the first time) and when the user clicks the **Home** button.

By default, an Internet Explorer Welcome window displays on the user's desktop when the Windows Desktop Update is installed. The Welcome window provides a link to a quick tour of the features of Internet Explorer, as well as a link to explore Active Channels. It's recommended that you allow the Welcome window to appear, so new users can learn about the new features of Internet Explorer 4. Users can easily turn off the welcome tutorial by clearing the check box for **Show this next time you log in** on the Welcome window.



In order to insert a customized set of Active Channels into your IEAK packages, you must set them up on your computer the way that you want them to be configured on your users' desktops. The IEAK will import your current settings and distribute them to your users. If you want to prevent users from changing, adding, or deleting these channels once Internet Explorer is installed, you can specify this in Stage 5 of the IEAK Configuration Wizard using the System Policies and Restrictions page. For more information about setting up channels, see Chapter 16, "Managed Webcasting," in Part 4, "Information Delivery: Webcasting."

Option	Description
Launch Channel Guide	This is simply a shortcut to the Microsoft Channel Guide on the Internet, where you can easily subscribe to the channels and configure how they will appear on your users' Channel bar. You can also add channels from your intranet without going to the Microsoft Channel Guide. For more information, see "Understanding Active Channels" and Desktop Items" in Chapter 16, "Managed Webcasting."
Do not customize channels	Select if you do not want to install channels on end users' computers.
Import current channel configuration	Select to import the channels you have set up on your computer.
Delete existing Internet Explorer 4.0 channels	Select to delete any existing Active Channels on end users' computers.
Show channel bar by default	*For Windows NT only.* Select to show the Channel bar in the browser window by default.



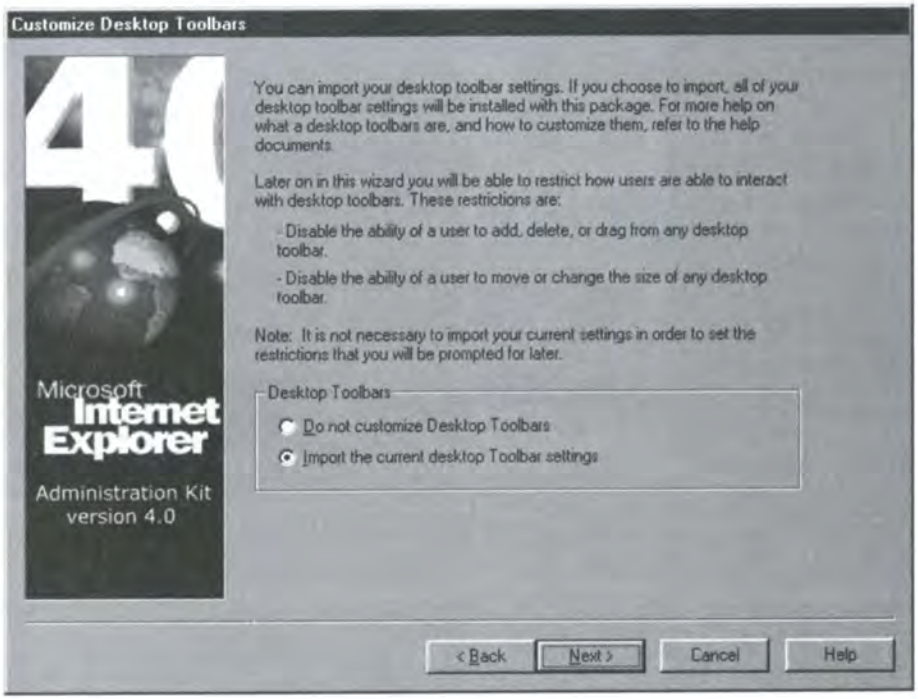
In order to insert a customized set of software distribution channels into your IEAK packages, you must set them up on your computer in the way that you want them to be configured on your users' desktops. The IEAK will import those settings and distribute them to your users. If you want to prevent users from changing their software distribution channel configuration once Internet Explorer is installed, you can specify this in Stage 5 of the IEAK Configuration Wizard, using the System Policies and Restrictions page. For more information about setting up software distribution channels, see Chapter 38, "Software Distribution and Updates."

Option	Description
Do not customize Software Distribution Channels	Select if you do not want to install software distribution channels on end users' computers.
Import current Software Distribution Channel configuration	Select to import the software distribution channels you have set up on your computer, and select a schedule option from the **Schedule** box.
Schedule Options	
<none – do not subscribe to channel>	Select to specify that all software distribution channels are imported, but not subscribed to, when the custom package is installed on users' computers. This is the default. Be careful you do not select this by mistake.
Auto	Select to specify that each software distribution channel uses the schedule information contained in the SCHEDULE section of its CDF file when the custom package is installed on users' computers
Daily	Select to specify that all software distribution channels are scheduled to be updated daily when the custom package is installed on users' computers.
Monthly	Select to specify that all software distribution channels are scheduled to be updated monthly when the custom package is installed on users' computers.
Weekly	Select to specify that all software distribution channels are scheduled to be updated weekly when the custom package is installed on users' computers.



In order to insert a customized set of Active Desktop items into your IEAK packages, you must set them up on your computer in the way that you want them to be configured on your users' desktops. The IEAK will import those settings and distribute them to your users. If you want to prevent users from changing their desktop configuration once Internet Explorer is installed, you can specify this in Stage 5 of the IEAK Configuration Wizard. For more information about setting up Active Desktop items, see Chapter 16, "Managed Webcasting," in Part 4, "Information Delivery: Webcasting."

Option	Description
Do not customize the Active Desktop	Select if you do not want to customize the Active Desktop.
Import the current Active Desktop components	Select to import the desktop items you have set up on your computer.
Modify Settings	Click to open the **Display Properties** dialog box. Use the Web tab to specify or change settings for desktop items.



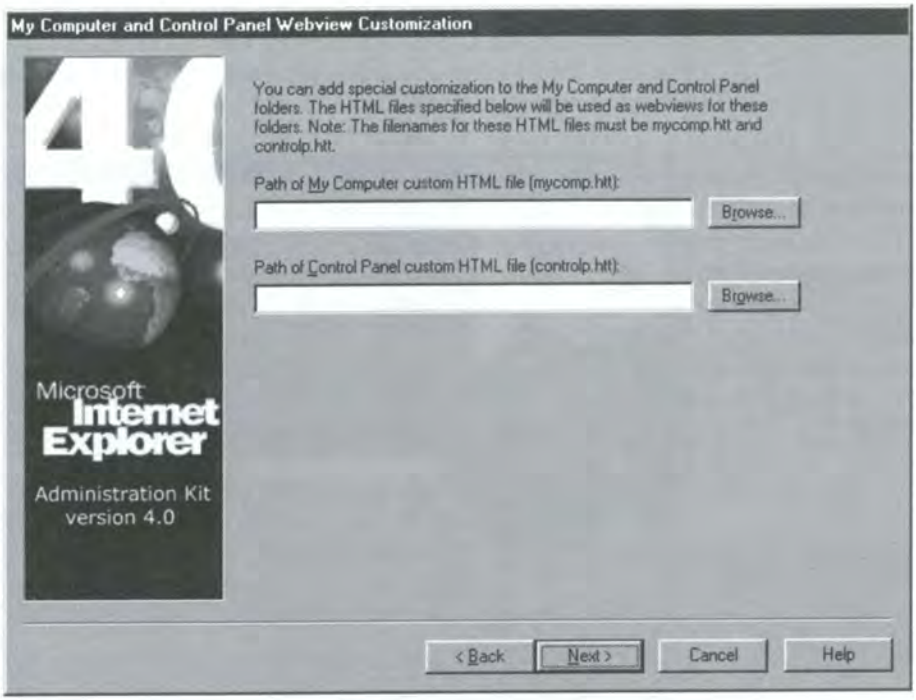
Option	Description
Desktop Toolbars	Click the option you want to use.

You can import your current settings by clicking **Import the current desktop Toolbar settings**. Click **Do not customize Desktop Toolbars** if you want users to have the default toolbar settings.

You can add the following four toolbars where you want them:

- The **Quick Launch** toolbar provides shortcuts to several often-used features of Internet Explorer 4: the desktop, the Web browser, Outlook Express, and channels.
- The **Address** toolbar enables you to enter a Web-page address (URL) without first opening the Internet Explorer browser.
- The **Links** toolbar provides shortcuts to important Web sites (for example, **http://www.microsoft.com/**) so that you can open them without first opening the browser.
- The **Desktop** toolbar contains all the shortcuts on your desktop and organizes them in one convenient location.
- In addition to the ready-made toolbars, you can create a toolbar from the contents of any folder.

For more information about these toolbars, see Part 3.



Option	Description
Path of My Computer custom HTML file (mycomp.htt)	Enter the path to the mycomp.htt file, or click **Browse** to locate it.
Path of Control Panel custom HTML file (controlp.htt)	Enter the path to the controlp.htt file, or click **Browse** to locate it.

You can customize how My Computer and Control Panel appear on your users' desktops by customizing the files that serve as templates for them: mycomp.htt (My Computer) and controlp.htt (Control Panel). If the user installs the Windows Desktop Update, My Computer and Control Panel can appear as Web pages in Web view. One reason to customize these folders is to provide your own instructions, a company logo, or links for support or corporate sites. For more information, see Part 3.

If you have installed the Windows Desktop Update on your computer, these files are located in the C:\Windows\Web or C:\Windows\NT folder. You can open them using a text editor, such as Notepad, or an HTML editor. It's recommended that you make a backup copy of these files before working with them, so you can restore them to their original state, if needed.

For more information about integrating Web views in the IEAK, see "Stage 4: My Computer and Control Panel Web View Customization," in the IEAK Help. For more information about development with **WebViewFolderContents** objects, see the *Internet Client SDK*.



Option	Description
Custom string to be appended to User Agent string	Enter the text you want to append to the user agent string for user-group browsers.

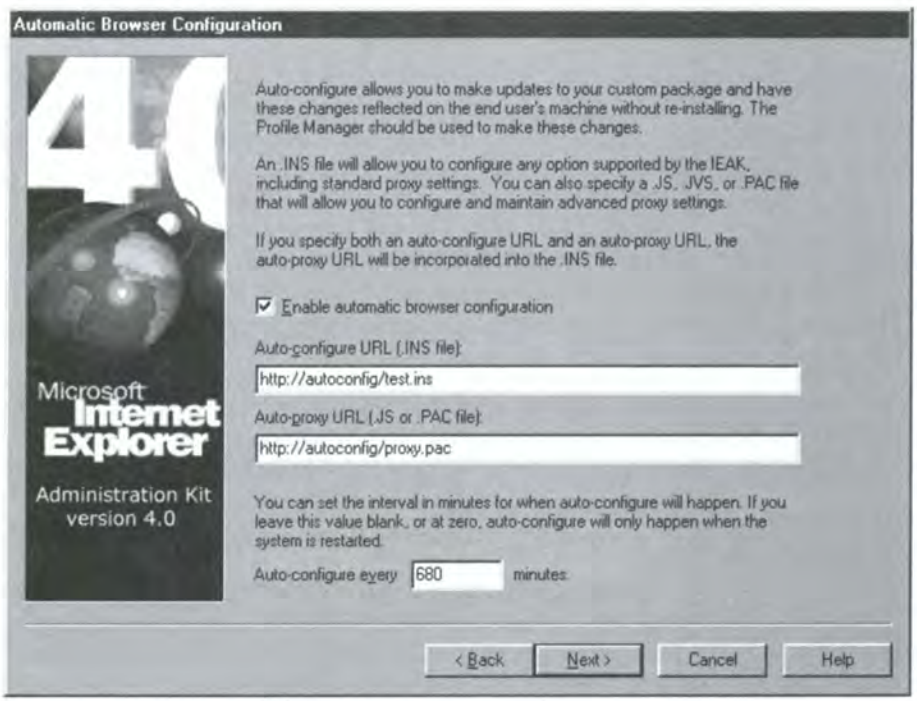
The user agent string is what a browser sends to Web servers to identify itself. Web servers use the information to identify the browser type and version, and typically record the information in server usage logs. Many organizations use the user agent string information to track statistics about browser usage on their Web sites. For example, organizations can identify what percentage of users access Web pages using Internet Explorer and Netscape Navigator. Based on a browser's user agent string, some Web sites download Web pages that are tailored to the capabilities of the browser type and version.

You only need to customize the user agent string if you want to do any of the following:

- Track the browser usage of specific user groups, and differentiate user group browser statistics from your intranet or Internet sites.
- Provide custom Web content to user groups based on the custom user agent string. For example, you might want to set up your Human Relations Web site to provide different Web pages for managers, with content appropriate only for managers. Therefore, you build separate custom packages for managers and non-managers, and include the appropriate custom user agent string.

Be aware that other organizations that track site statistics will see the custom user agent string. The following example shows how the IEAK appends a custom string *CustomUserAgentString* to the default user agent string:

```
Mozilla/4.0(compatible;MSIE 4.0b1;WindowsNT);CustomUserAgentString
```



Option	Description
Enable automatic browser configuration	Click if you want to turn on automatic browser configuration for this custom package.
Auto-configure URL (.INS file)	Type the URL for the auto-configuration (.ins) file. This URL points to the auto-configuration (.ins) file for this custom package. You can create a different file for each user group in your organization. Use a unique file name for each group managed—for example, sysadm.ins for system administrators and grpman.ins for group managers. The URL includes the file name in the following format: *http://path/file name*
Auto-proxy URL (.JS or .PAC file)	Enter the path to the .js or .pac file. The URL includes this file name in the following format: *http://path/file name*
Auto-configure every __ minutes	Enter an interval, in minutes, when automatic configuration occurs. After deployment, Internet Explorer updates the auto-configuration information at the specified interval. If you leave the space for this interval blank or type "0," auto-configuration occurs only when users manually refresh the browser's automatic configuration or when Internet Explorer is restarted.

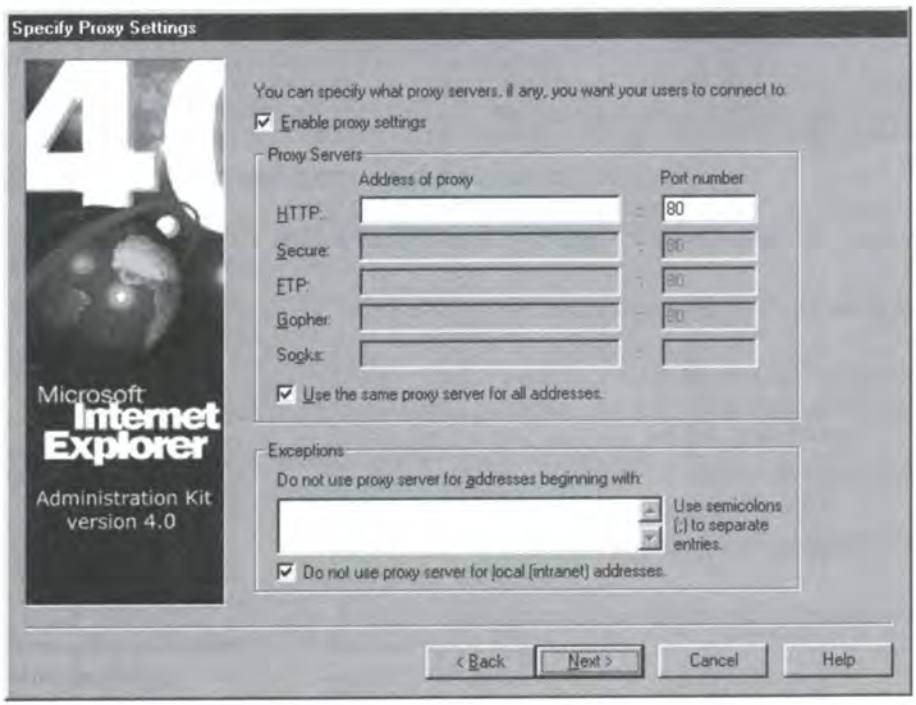
Automatic browser configuration is a feature of Internet Explorer 3 and Internet Explorer 4. You can set up Internet Explorer to periodically download auto-configuration files maintained on a central server. The contents of auto-configuration files are used to specify a wide variety of application, desktop, and shell settings for users. Internet Explorer 3 ignores any settings that apply only to Internet Explorer 4.

You typically create and maintain separate auto-configuration files for the different user groups in your organization. You can build custom packages configured to read auto-configuration files for each user group. You can then distribute the appropriate custom build to each user group. For more information, see Chapter 37, "Automatic Browser Configuration."

When the custom packages are deployed with automatic browser configuration enabled, Internet Explorer periodically downloads the auto-configuration files from the server. Each time the auto-configuration information is refreshed, the system checks to see if there are new changes and then updates user, application, desktop, and system settings, as necessary.

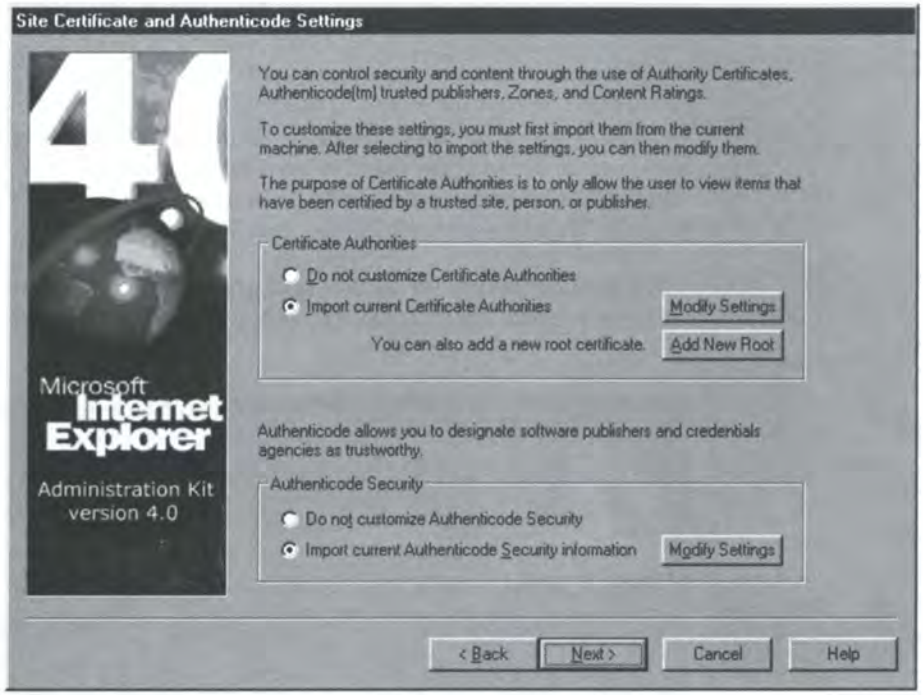
You can use automatic browser configuration to manage a wide range of settings for users' computers, including Internet Explorer settings, desktop settings, and system settings. You can use the IEAK Profile Manager to create and modify auto-configuration files to change most of the settings and options you specified using the IEAK Configuration Wizard. You can also use the Profile Manager to update and manage system policies and restrictions and to lock down settings to prevent your users from changing the settings you specify. For example, you can prevent users from changing automatic browser configuration settings in their **Internet Options** settings. For more information, see Chapter 37, "Automatic Browser Configuration."

You can use the auto-proxy (.js or .pac) files to configure proxy settings dynamically for user groups. Using auto-proxy files is optional. You may want to specify proxy settings for each user group, using the Specify Proxy Settings page, which displays next. For more information about creating auto-proxy files, see Chapter 37, "Automatic Browser Configuration," and "JavaScript or JScript Auto-Proxy Example Files" in the IEAK Help.



Option	Description
Enable proxy settings	If you do not use proxy servers, clear this check box. You should clear this check box if you use auto-proxy files.
HTTP	Type the URL of the proxy server for HTTP and its port number.
Secure	Type the URL of the secure proxy server and its port number.
FTP	Type the URL of the proxy server for FTP and its port number.
Gopher	Type the URL of the proxy server for Gopher and its port number.
Socks	Type the URL of the socks proxy server and its port number.
Use the same proxy server for all addresses	To use different proxy servers for different URLs, clear this check box.
Exceptions	Type the path(s) or domain(s) that do not require the use of proxy servers.
Do not use proxy server for local (intranet) addresses	To use proxy servers for local intranet URLs, clear this check box.

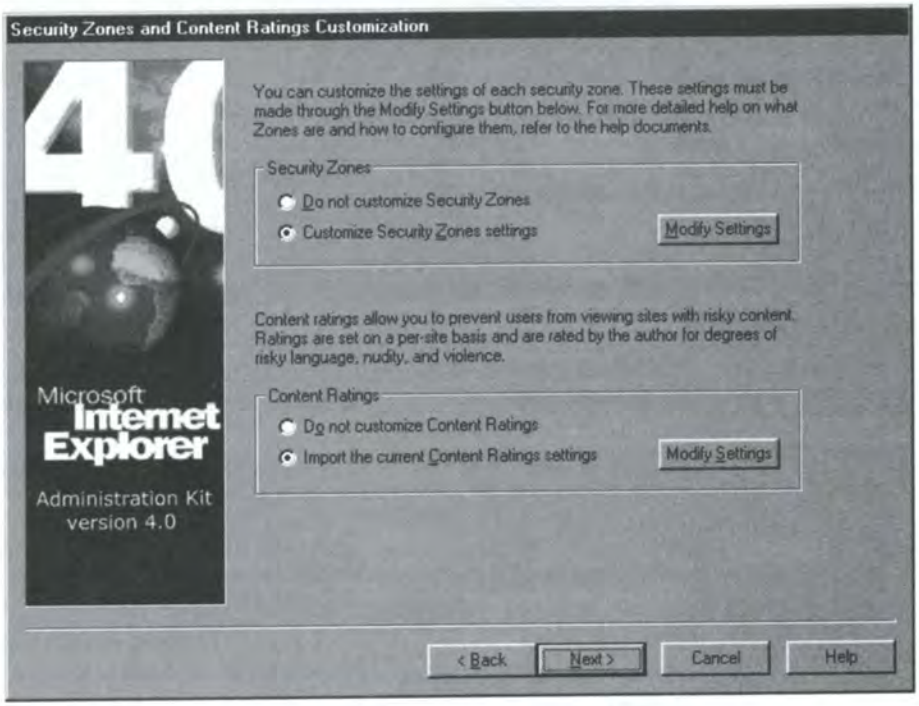
For more information about configuring proxy settings, see Chapter 8, "Configuring Connection Settings."



Option	Description
Do not customize Certificate Authorities	Select to accept the default Certificate Authorities settings.
Import current Certificate Authorities	Select to import the certificate settings you have set up on your computer.
Modify Settings	Click to modify Certificate Authority settings. Use the **Certificate Authorities** dialog box to remove certificates or to select trusted certificates for each **Issuer Type**.
Add New Root	Click to add a new root certificate. Use the **Browse** dialog box to add the *file name* of the root certificate file.
Do not customize Authenticode Security	Select to not install trusted publishers and authorities on your users' computers.
Import current Authenticode Security information	Select to import the trusted publishers and authorities you have set up on your computer.
Modify Settings	Click to remove trusted publishers and authorities. Use the **Authenticode Security Technology** dialog box to remove certificates for trusted publishers and authorities.

Internet Explorer 4 uses industry-standard digital certificates and Microsoft Authenticode technology to verify the identity of individuals and organizations on the Web and to ensure content integrity. Together with security zones, these can be used to control user access to online content based on the type, source, and location of the content. For example, you can use security zones in conjunction with certificates to allow users to have full access to Web content on your intranet, but limit the access to Web content from restricted sites located on the Internet. For more information, see Part 7, "Security and Privacy."

You can either accept the default certificate settings or customize the settings to meet your needs. For information on how to configure certificates, see Chapter 28, "Digital Certificates."



Option	Description
Do not customize Security Zones	Select to accept the default security zone settings.
Customize Security Zones settings	Select to import custom security zone settings you have set up on your computer.
Modify Settings	Click to customize security zone settings. Use the **Security** dialog box to specify the security levels assigned to the security zones.
Do not customize Content Ratings	Select to install browsers on users' computers with default settings and with content ratings disabled.
Import the current Content Ratings settings	Select to import custom content rating settings you have set up on your computer.
Modify Settings	Click to customize content rating settings. Use the **Content Advisor** dialog box to specify the custom content ratings.

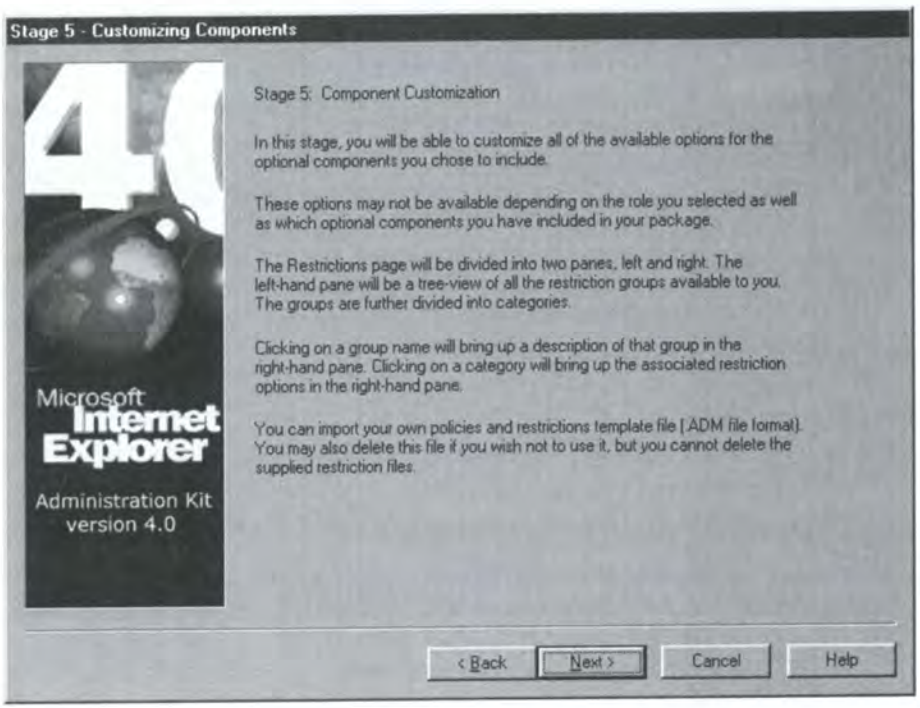
You can manage security zones and content ratings for your company and customize the settings for each security zone. For more information, see Chapter 27, "Security Zones." You can configure security zone settings to control how users can access Web content from sites located on the intranet, Internet, trusted sites, and restricted sites.

You can also control the types of content users can access on the Internet. You can adjust the content rating settings to reflect what you think is appropriate content in four areas: language, nudity, sex, and violence. For more information, see Chapter 30, "Content Advisor."

Stage 5: Customizing Components

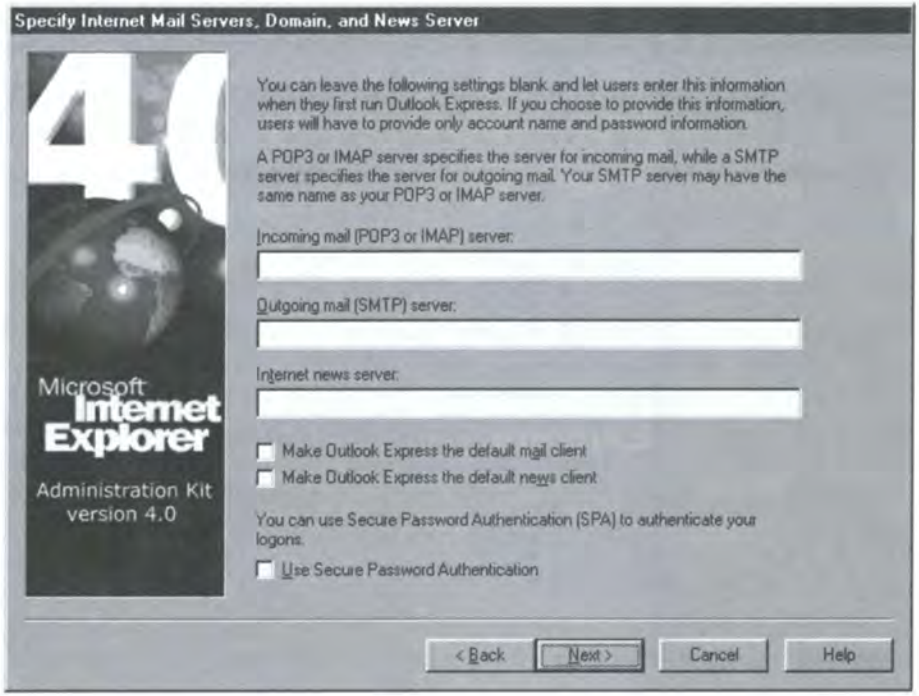
In Stage 5, you will:

- Specify your users' Outlook Express news and mail settings.
- Specify any LDAP server settings to provide Internet directory services to your users.
- Specify the Outlook Express welcome e-mail message to welcome users and customize the InfoPane that appears when users start the program.
- Specify default signatures to provide a corporate disclaimer or signature in Internet newsgroup or e-mail messages.
- Specify system policies and restrictions settings and lock down a wide range of browser, application, and system settings.



The IEAK Configuration Wizard pages in Stage 5 are:

- Specify Internet Mail Servers, Domain, and News Server
- Specify LDAP Server Settings
- Outlook Express Customizations
- Include a Signature
- System Policies and Restrictions



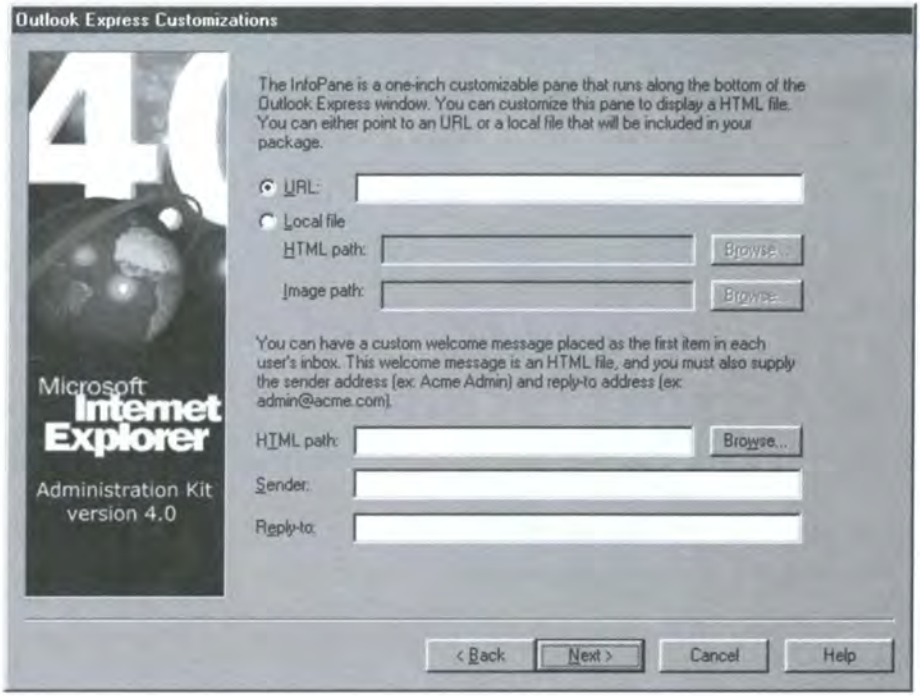
This wizard page appears only when you have chosen Outlook Express as an Internet Explorer component. It's optional because end users can provide this information when they run Outlook Express. This is a good way for administrators to pre-configure server settings that their users may not have.

Option	Description
Incoming mail (POP3 or IMAP) server	Type the server name, domain name, and subdomain for handling incoming mail.
Outgoing mail (SMTP) server	Type the server name, domain name, and subdomain for handling outgoing mail. This may be the same as the incoming mail server.
Internet news server	Type the server name of which Network News Transfer Protocol (NNTP) to use.
Make Outlook Express the default mail client	If you want Outlook Express to be the default mail client, select this check box.
Make Outlook Express the default news client	If you want Outlook Express to be the default news client, select this check box.
Use Secure Password Authentication	If you want Secure Password Authentication to authenticate users when they log on, select this check box.



Directory services are powerful search tools that help your users find people and businesses around the world. The Address Book supports LDAP for accessing directory services, and it comes with built-in access to several popular directory services. You can specify the LDAP services for your users.

Option	Description
Friendly Name	Type the name of the LDAP server.
Directory Service	Type the directory service.
Home Page	Type the URL of the home page that Internet Explorer displays when the end user requests the LDAP Web site.
Search Base	Type the root or scope for the hierarchical level at which to search the LDAP server: base, one, or sub.
Service Bitmap	Type the path to the location of the bitmap, or click **Browse** to locate it.
Check names against this server when sending mail	If you want Outlook Express to check names before sending mail, select this check box.
Authentication type	Select the authentication type: Anonymous, Secure Password, or Password.

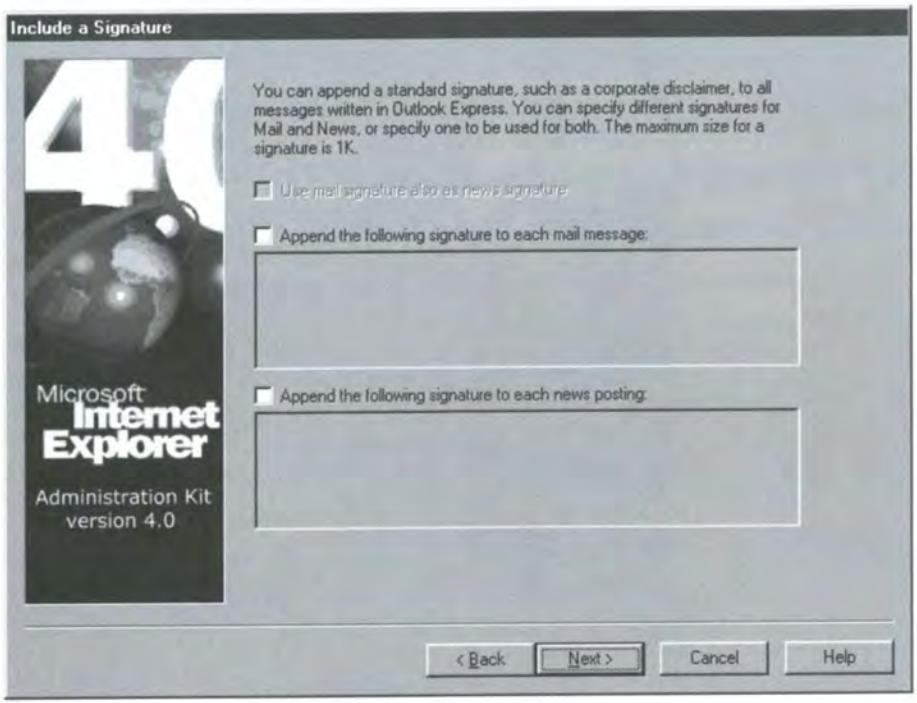


Option	Description
URL	Click to specify a URL for the Outlook Express InfoPane.
Local file	Click to use an HTML file for the Outlook Express InfoPane.
HTML path ***(InfoPane)***	Type the path to the InfoPane file, or click **Browse** to locate it.
HTML path ***(custom welcome message)***	Type the path to the custom welcome message file, or click **Browse** to locate it.
Sender	Type the user's name.
Reply-to	Type the user's e-mail address.

You can give Outlook Express a custom look and welcome new users with an e-mail message.

The Outlook Express InfoPane contains helpful information and links. You can customize this pane with support numbers, Frequently Asked Questions (FAQs), and information about your company.

The InfoPane appears as a window at the bottom of Outlook Express when you start the program. You can customize the InfoPane with an HTML file that is either a local file or an Internet address (URL).



Option	Description
Use mail signature also as news signature	To use the e-mail signature for posting news, select this check box.
Append the following signature to each mail message	Type the signature to append to each e-mail message.
Append the following signature to each news posting	Type the signature to append to each news posting.

You can include a default signature or disclaimer that will appear on Outlook Express newsgroup or e-mail messages. A disclaimer is often used to show that messages submitted by employees over the Internet do not represent official company policies. The maximum size of the signature is 1K. You can choose to append signatures to newsgroup messages only, to e-mail messages only, or to both types of messages.



Option	Description
Left pane	Select the subject for which you want to change policies and restrictions.
Right pane	Specify the policies and restrictions you want for the subject.

For more information on the System Policies and Restrictions page, see Chapter 37, "Automatic Browser Configuration." Also, for a complete list of all the options on this page, see Appendix J, "Custom-Build Checklist."

Generating the Package



After finishing Stage 5, the IEAK Configuration Wizard displays this page to give you a last chance to make changes. Once you click **Finish**, the wizard creates the package as you specified.

Signing Custom Package Files

Digital signatures identify the source of programs and guarantee that the code hasn't changed since it was signed. Depending on how users' browser security levels are configured, users could be warned not to download files that aren't signed, or could be prevented from downloading them. Therefore, you should digitally sign the .cab files created by the IEAK Configuration Wizard and any custom components you include.

Signing .cab files and custom programs requires two steps: obtaining a digital certificate—from a Certificate Authority (CA) such as VeriSign or GTE—and signing the code. For more information, see Chapter 28, "Digital Certificates," "Signing Your Programs" in the IEAK Help, and "Signing Code with Microsoft Authenticode Technology" in the *Internet Client SDK*.

Producing Distribution Media

This section covers the downloading and distributing of custom browser packages.

Designating Distribution

If you created the browser package on an Internet or intranet server, you need to set up your Web site so that users can download the files. For example, you can create a page where you post download information and a link to the install engine, IE4Setup.exe.

The IEAK Configuration Wizard places IE4Setup.exe in a directory at the URL you entered in the **Destination folder** box on the **Select Media to Distribute Your Browser** page during Stage 1. For example:

```
C:\Webshare\WWWroot\CIE\Download\Win95_NT\En\IE4setup.exe
```

Note The IEAK Configuration Wizard creates the directory structure using a convention that indicates the language version (English: En) and the platform (Windows 95 and Windows NT: Win95_NT) for the custom package.

If you created the browser package on your hard disk or network drive, you need to move the distribution files from the \IE4site folder on your hard disk or network drive to the \IE4site folder on the an Internet or intranet server at the URL you specified for your distribution servers.

The \IE4site folder contains the .cab files of the language version you are posting and the folder contents. For example, the English version is located in \IE4site\En. You need to move the \IE4site*Language version* folder and the files it contains to the URL you specified for download sites. For example, move files in C:\Cie\IE4site\En to C:\Webshare\Wwwroot\Cie\IE4site\En.

Active Setup uses the \IE4site\IE4sites.dat file to locate the files Active Setup needs to install the custom package on users' computer. You need to move the file \IE4site\IE4sites.dat to the URL for the download site (or sites) you specified when you ran the IEAK Configuration Wizard. For example, move IE4sites.dat from C:\IE4site\IE4sites.dat to C:\Webshare\Wwwroot\Cie\IE4site\IE4sites.dat.

Designating Other Distribution Media

For packages on compact discs or floppy disks, make sure to produce a sufficient volume of the chosen distribution media to meet end-user needs.

If you distribute your custom browser on compact discs for Windows 95 users, a splash-screen Autorun program appears when the user inserts the compact disc. This program offers users the choice to install your custom browser or view more information. If the current version of Internet Explorer is already installed, the Autorun program detects it. The browser appears in what is known as Kiosk mode, with the Start.htm file loaded.

The IEAK Configuration Wizard will also enable you to distribute your custom browser on multiple 1.44-MB floppy disks.

Distributing Internet Explorer

Depending on the media in which you distribute the custom packages, you can use one or more of the following methods to distribute Internet Explorer to end users:

- From download Web or FTP sites on the Internet
- From download Web or FTP sites on your intranet
- From compact discs
- From floppy disks

For each of these methods, end users run the Active Setup program, IE4setup.exe, to install the custom build of Internet Explorer.

Using Compact Discs and Floppy Disks

For distribution from compact discs and floppy disks, IE4Setup.exe is included on the distribution media. Users install Internet Explorer by running IE4Setup.exe from the AutoRun splash screen of the compact disc or from Disk 1 of the floppy disk set. Active Setup installs the appropriate files from the distribution media. You can provide written instructions to guide users through the installation process. You can include the instructions in an e-mail message to users or as hard-copy instructions packaged with the distribution media.

Using Distribution Sites on the Intranet or Internet

From distribution sites on the intranet or Internet, you can deliver IE4setup.exe directly to end users as an e-mail attachment, if your network bandwidth and load can support sending multiple copies of IE4Setup.exe, which is about 420K. You can also direct users where to go to download the IE4Setup.exe. For example, you could send an e-mail message with instructions and a link to a download Web page. The download Web page could provide instructions on how to download Internet Explorer.

Running Active Setup

When users run IE4.Setup.exe, Active Setup installs Internet Explorer from the distribution media as follows:

- IE4Setup.exe extracts the setup files into a temporary directory.
- IE4Setup.inf looks at the [String] section for the URL location of the IE4site.dat file.
- Active Setup goes to the file IE4site.dat, which points to the location of the download .cab files and then displays the download options to the end user.
- Active Setup downloads the .cab files, which are placed in the specified directory; for example, C:\Program Files\Internet Explorer.
- Active Setup extracts the .cab files.
- Active Setup installs Internet Explorer and each component for the specified installation package.

After Internet Explorer is installed, Active Setup prompts the user to restart the computer. After the computer restarts, Active Setup completes configuring the user's desktop and opens the Welcome splash screen to introduce the user to Internet Explorer 4.

Troubleshooting Active Setup

For troubleshooting Active Setup:

- Review the Active Setup Log.txt file in the Windows directory. Each installation creates a log file, which collects information about that particular installation. If an Active Setup Log.txt file exists when an installation is started, Active Setup renames the existing log as a .bak file and creates a new log file. (For more information about the Active Setup Log.txt file, see Part 1, "Installing Internet Explorer 4.")
- Make sure that the download URL in the file IE4Setup.inf is exact.
- Refer to Appendix B, "Troubleshooting Installation and Uninstallation."

Assisting Users During Installation

The user support team should monitor the progress of the pilot program and provide user assistance, as necessary. It's recommended that you provide an online support Web site that can provide users with help resources to solve common problems.

You should use your experience from pilot programs to provide the types of information and help your typical users need. As solutions are developed to solve users' problems during the deployment process, you should update the support Web site to provide solutions to problems.

You could integrate the online support site with your help desk and provide mechanisms to escalate unusual or difficult problems to user support specialists.

CHAPTER 37

Automatic Browser Configuration

In this chapter

Automatic Browser Configuration Overview 672
Understanding Automatic Browser Configuration 672
Setting Up Automatic Browser Configuration 673
- Setting Up Custom Packages 674
- Locking Down Automatic Browser Configuration 675
- Creating User Auto-Configuration Files 677
- Signing Auto-Configuration Cabinet Files Digitally 678
- Creating Auto-Proxy Files 678
- Configuring Central Auto-Configuration Servers 679
- Setting Up Auto-Configuration in Previously Deployed Browsers 679
- Updating Distribution Files 681

Using the IEAK Profile Manager 682
- Starting the IEAK Profile Manager 682
- Changing Wizard Settings 683
- Changing System Policies and Restrictions 685
- Using Custom Policy Templates 687
- Using Auto-Configuration File Templates 687
- Maintaining Auto-Configuration Files 688

Automatic Browser Configuration Overview

This chapter describes how to set up Internet Explorer and servers on the network to enable automatic browser configuration and how to use the automatic browser configuration feature of Microsoft Internet Explorer 4 to centrally manage desktop configurations. This chapter also explains how to use the Internet Explorer Administration Kit (IEAK) Profile Manager to create and manage separate configuration files for different user groups in your organization.

The information provided here will help you to:

- Understand the automatic browser configuration feature.
- Set up computing systems for automatic browser configuration.
- Use the IEAK Profile Manager to maintain configuration files.

Understanding Automatic Browser Configuration

Automatic browser configuration is a feature of Internet Explorer 3 and Internet Explorer 4. You can set up Internet Explorer to periodically download auto-configuration files maintained on a central server. The contents of auto-configuration files are used to specify a wide variety of application, desktop, and shell settings for users. Internet Explorer 3 ignores any settings that apply only to Internet Explorer 4.

You typically create and maintain separate auto-configuration files for the different user groups in your organization. You can build custom packages configured to read auto-configuration files for each user group. You can then distribute the appropriate custom build to each user group.

When the custom packages are deployed with automatic browser configuration enabled, Internet Explorer periodically downloads the auto-configuration files from the server. Each time the auto-configuration information is refreshed, the system checks to see if there are new changes, and then updates user, application, desktop, and system settings, as necessary.

Note Some auto-configuration changes require the system to be restarted before changes to the system registry can take effect.

You can use automatic browser configuration to manage a wide range of settings for users' computers, including Internet Explorer settings, desktop settings, and system settings. You can use the IEAK Profile Manager to create and modify auto-configuration files to change most of the settings and options you specified using the IEAK Configuration Wizard. You can also use the Profile Manager to update and manage system policies and restrictions, and to lock down settings to prevent your users from changing the settings you specify. For example, you can prevent users from changing automatic browser configuration settings in their **Internet Options** settings.

Setting Up Automatic Browser Configuration

You should set up automatic browser configuration when you deploy Internet Explorer. With automatic browser configuration enabled on all desktops in your organization, you can make configuration settings centrally, without having to touch the individual computers again. You can still set up automatic browser configuration after deployment, but then it requires some additional steps.

To set up automatic browser configuration before deployment:

- Set up custom packages for automatic browser configuration.
- Lock down automatic browser configuration.
- Create user-configuration files.
- Digitally sign auto-configuration cabinet files.
- Create optional auto-proxy files.
- Configure central auto-configuration servers.

To set up automatic browser configuration after deployment:

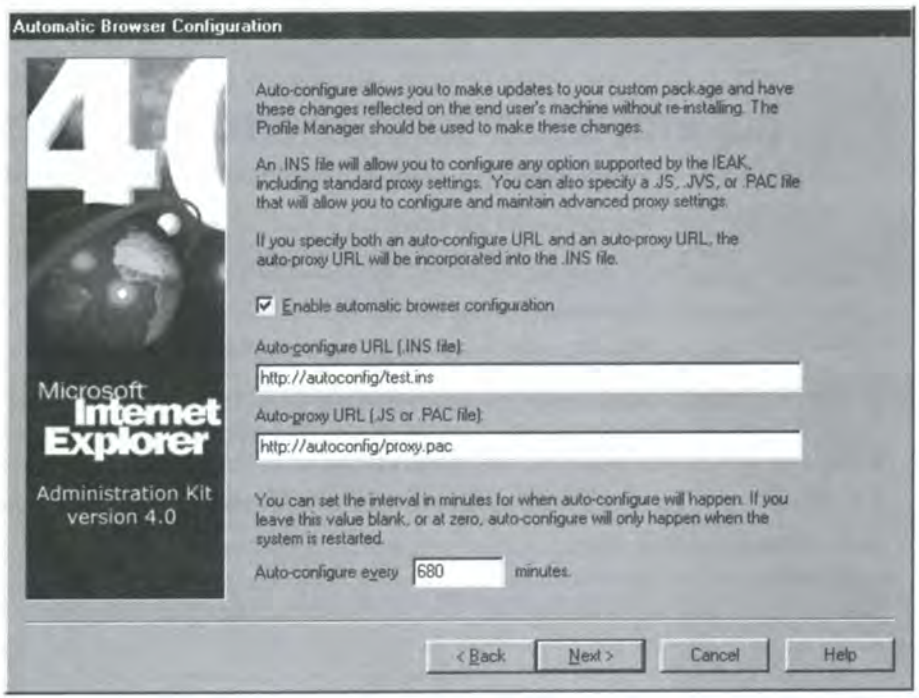
- Set up automatic browser configuration for deployed browsers.
- Update distribution files with the new custom-package files.

Setting Up Custom Packages

You use the IEAK Configuration Wizard to set up automatic browser configuration when you build custom packages. When the custom packages are deployed, Internet Explorer is installed with automatic browser configuration enabled.

To build custom packages, you need to run the IEAK Configuration Wizard and specify the custom package. For more information, see "Building Custom Packages" in Chapter 36, "Implementing the Deployment."

To set up automatic browser configuration, perform the following steps at the **Automatic Browser Configuration** page:



1. Select **Enable automatic browser configuration**.
2. Type the URL for the *user-configuration file* in the **Auto-configure URL (.INS file)** box.
3. Type the URL for the *auto-proxy file* in the **Auto-proxy URL (.JS or .PAC file)** box.
4. Type the *auto-configuration interval* in the **Auto-configure every _____ minutes** box.

The information you need is explained in the table below.

Information Needed	Explanation
URL for the user-configuration file	This URL points to the auto-configuration (.ins) file for this custom package. You can create a different file for each user group in your organization. Use a unique file name for each group managed—for example, sysadm.ins for system administrators and grpman.ins for group managers. The URL includes the file name in the following format: *http://path/file name*
URL for the auto-proxy file	You can use the auto-proxy (.js or .pac) file to configure proxy settings dynamically. The URL includes this file name in the following format: *http://path/file name*
auto-configuration interval	This interval is the time, in minutes, during which automatic configuration occurs. After deployment, Internet Explorer updates the auto-configuration information at the specified interval. If you leave the space for this interval blank or type "0," auto-configuration occurs only when users manually refresh the browser's automatic configuration or when Internet Explorer is restarted.

5. Finish building the custom package.

To specify automatic browser configuration, the IEAK Configuration Wizard places the following entries in the [URL] section of the install.ins file:

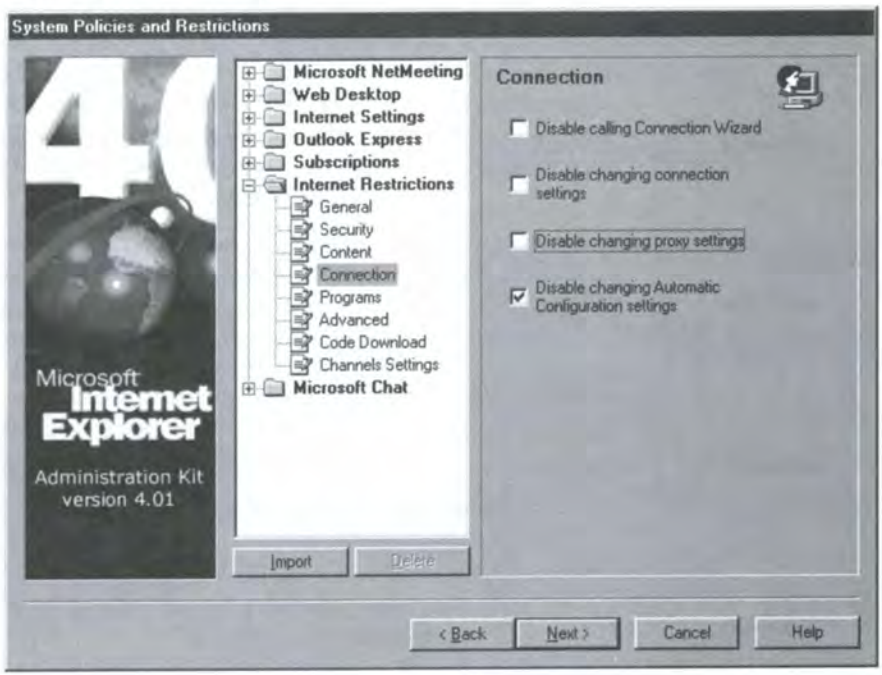
```
AutoConfig=1
AutoConfigURL=http://URL/user-configuration file name
AutoConfigJSURL=http://URL/auto-proxy file name
AutoConfigTime=auto-configuration interval
```

Locking Down Automatic Browser Configuration

You can use the IEAK Configuration Wizard to lock down automatic browser configuration and prevent users from changing automatic browser configuration in their **Internet Options** settings. After browsers are deployed, you can use the IEAK Profile Manager to lock down automatic browser configuration for user groups that have automatic browser configuration implemented.

▶ **To lock down automatic browser configuration**

1. Go to the **System Policies and Restrictions** page of the IEAK Configuration Wizard.
2. In the System Policies & Restrictions hierarchy, select **Internet Restrictions**, and then click **Connection**.



Note The IEAK Configuration Wizard is shown here, but the **System Policies and Restrictions** section of the IEAK Profile Manager works similarly.

3. In the right pane, click **Disable changing Automatic Configuration settings**.
4. Finish building the custom package.

When Internet Explorer is installed on end users' computers, the **Automatic Connection** option on the **Connections** tab of the **Internet Options** dialog box appears dimmed, preventing users from opening the **Automatic Configuration** dialog box to change settings.

Creating User Auto-Configuration Files

You use the IEAK Profile Manager to create and maintain user auto-configuration files. The Profile Manager generates the auto-configuration .ins file and companion .cab files that are needed to configure users' systems.

You can create user auto-configurations for each user group in your organization. You use the Profile Manager to specify the configurations and save them as *usergroup*.ins files, where *usergroup* is a unique name for each user group. The Profile Manager automatically generates the companion .cab files. For example, you could specify a user-group configuration for system administrators and save the configuration as sysadmin.ins. The Profile Manager would then generate the necessary companion .cab files.

A .cab file stores compressed files in a library. Cabinet files are used to organize installation files that are downloaded to users' systems. The cabinet files that the Profile Manager generates contain information (.inf) files that are automatically unpacked on users' systems.

The *usergroup*.ins file is used by Internet Explorer to change browser customization settings corresponding to the Wizard Settings section of the Profile Manager. For more information, see "Changing Wizard Settings" later in this chapter. Internet Explorer processes the contents of the *usergroup*.ins file and makes any changes specified. For example, if proxy settings have changed in *usergroup*.ins, Internet Explorer updates the user's Internet proxy settings. Internet Explorer also downloads and unpacks the companion .cab files for Windows to process. The unpacked auto-configuration .inf files are used by Windows to change system policies and restrictions corresponding to the System Policies and Restrictions section of the Profile Manager.

Each .inf file contains version information. When you modify user configurations, the Profile Manager changes the affected .inf files, updates the version information, and repackages the companion .cab files. When the auto-configuration .cab files are downloaded to a user's system and unpacked, the system checks the version of the .inf files and only updates system settings using new versions of the .inf files.

Signing Auto-Configuration Cabinet Files Digitally

Digital signatures identify the source of programs and guarantee that the code hasn't changed since it was signed. Depending on how users' browser security levels are configured, users could be prevented from downloading .cab files that aren't signed. Therefore, you should digitally sign the companion (.cab) files created by the IEAK Profile Manager.

Signing .cab files requires two steps: obtaining a digital certificate—from a Certificate Authority such as VeriSign or GTE—and signing the code. For more information, see Chapter 28, "Digital Certificates," "Signing Your Programs" in the IEAK Help, and "Signing Code with Microsoft Authenticode Technology" in the *Internet Client SDK*.

Creating Auto-Proxy Files

You can use a text editor to create auto-proxy (.js or .pac) files that dynamically assign browser proxy settings based on the location of hosts. Auto-proxy files are JScript files. When an auto-proxy file is specified, Internet Explorer uses the auto-proxy script to determine if it should connect directly to a host or use a proxy server. You can use auto-proxy files to configure users automatically to use different proxy servers for different domains.

The following example shows an auto-proxy function that checks to see whether the host name is a local host, and if it is, whether the connection is direct. If the host name is not a local host, the connection is through the proxy server, named proxy1.

```
function FindProxyForURL(url, host)
    {
        if (isPlainHostName(host))
            return "DIRECT";
        else
            return "PROXY proxy1:80";
    }
```

The ***isPlainHostName()*** function checks to see if there are any dots in the host name. If there are, it returns false; otherwise, the function returns true. For more examples of JScript auto-proxy files, see Help in the IEAK Configuration Wizard.

Note Using auto-proxy files is optional. You may want to specify proxy settings for each user group that uses the IEAK Configuration Wizard or the IEAK Profile Manager. You can also lock down the proxy-settings option. For more information, see "Using the IEAK Profile Manager" later in this chapter.

Configuring Central Auto-Configuration Servers

You need to configure servers on your intranet to support automatic browser configuration. To configure central management servers:

- Install Web-server software, such as Microsoft Internet Information Server.
- Install the auto-configuration and auto-proxy files on the server at the URLs necessary for automatic browser configuration.

The number of automatic browser configuration servers you need will vary depending on the size and demands of your organization. If your organization is large, you could configure automatic browser configuration servers for each domain. For example, you specify automatic browser configuration for user groups in domain 1:

- http://domain1_server/autoconfig/*usergroup*.ins
  http://domain1_server/autoconfig/proxy1.pac

You would install a Web server at http://domain1_server/ and install the *usergroup*.ins and *usergroup*.cab files and proxy1.pac on the server at http://domain1_server/autoconfig/. When users in domain 1 start Internet Explorer, it reads the appropriate auto-configuration files and the auto-proxy file residing at http://domain1_server/autoconfig/.

Setting Up Auto-Configuration in Previously Deployed Browsers

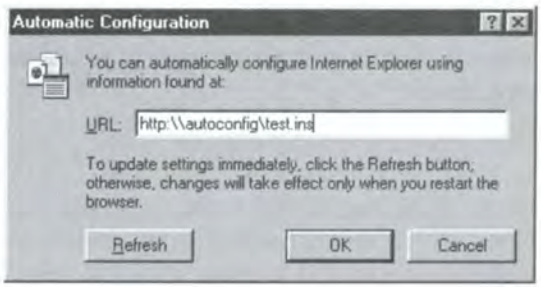
Clearly, it is advantageous to use the IEAK to customize Internet Explorer 4 so that automatic configuration is enabled before you deploy the browser. If that is not possible, users will have to perform a simple procedure to turn on automatic configuration. Once they have performed these steps, you can use the IEAK Profile Manager to lock down these settings, so your users will not be able to change these settings.

▶ **To set up Internet Explorer 4 for automatic configuration**

1. From the Internet Explorer window, on the **View** menu, choose **Internet Options**.
2. Select the **Connection** tab.



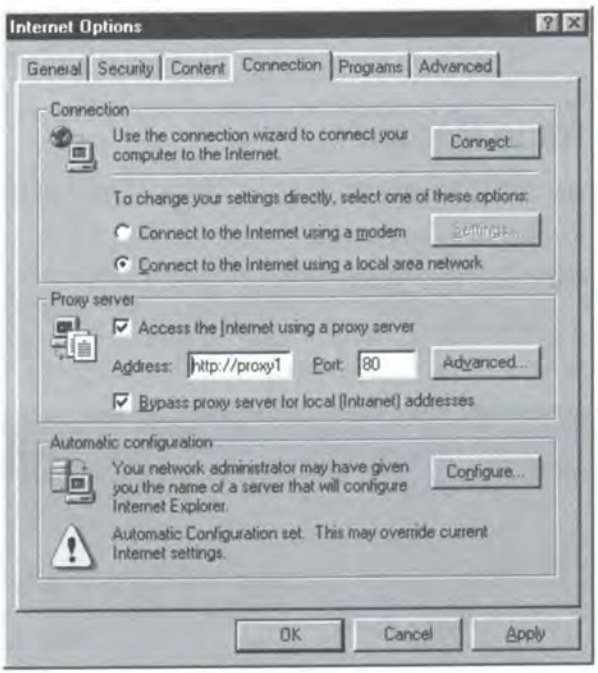
3. Select **Configure**.



4. Type the *URL/auto-configuration file name* in the URL box.
5. Select **Refresh** to refresh auto-configuration information.

Note Some auto-configuration changes require the system to be restarted before changes to the system registry will take effect.

When automatic browser configuration is turned on, the **Connection** tab displays a caution: "Automatic configuration set. This may override current Internet settings."



Updating Distribution Files

If you deployed Internet Explorer with automatic browser configuration disabled, you should update distribution files from new custom package builds that are enabled for automatic browser configuration. This ensures that new-user installations of Internet Explorer are enabled for automatic browser configuration.

Be sure to update all download sites. If you distribute custom packages using compact discs or floppy disks, you'll also need to produce new compact discs or floppy disks for distribution.

Using the IEAK Profile Manager

You can use the IEAK Profile Manager to create and maintain the auto-configuration files. With the Profile Manager you can specify a wide range of browser, user, desktop, and system settings and restrictions.

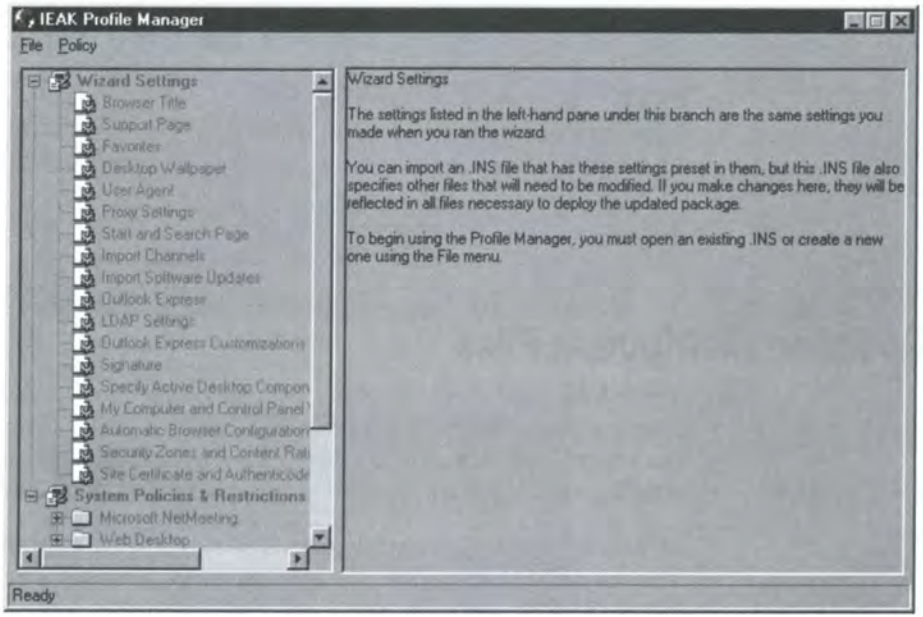
Starting the IEAK Profile Manager

▶ **To start the IEAK Profile Manager**

1. On the **Start** menu, click **Run**.

   The **Run** dialog box opens.

2. Type **profmgr.exe**.
3. Click **OK**.

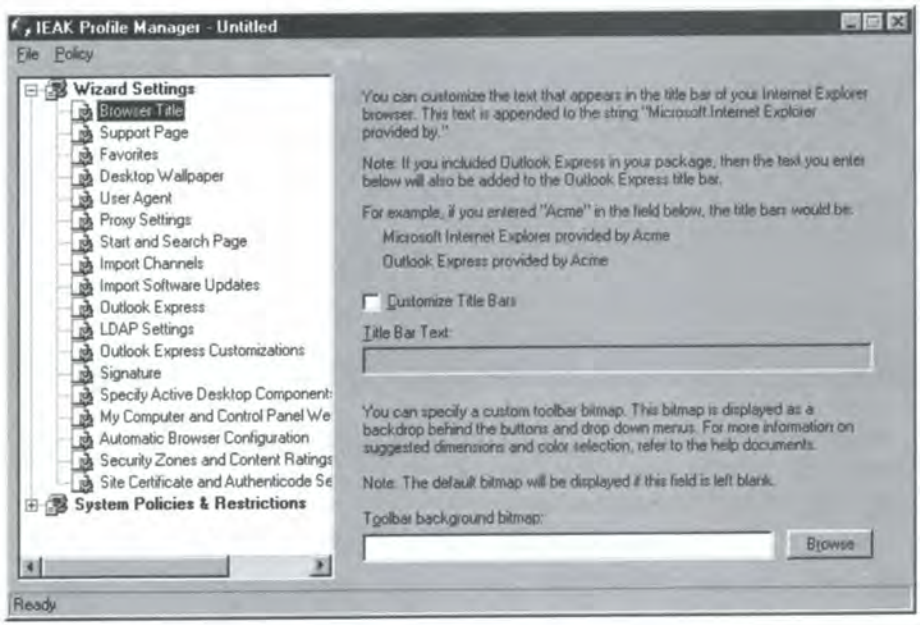


The Profile Manager is organized into a left pane showing a hierarchical tree of objects and a right pane showing the options. When you select an object in the tree in the left pane, the options and settings for that object appear in the right pane. You can change options or specify settings as necessary to manage automatic browser configurations.

The IEAK Profile Manager provides two categories of settings that you can specify: **Wizard Settings** and **System Policies & Restrictions**.

Changing Wizard Settings

In the left pane, the Wizard Settings object and its subobjects correspond to settings you can also specify using the IEAK Configuration Wizard. You can select an object and change the corresponding options and settings. For example, you can select the Browser Title object and change the **Browser Title Bar** and **Toolbar background bitmap** options.



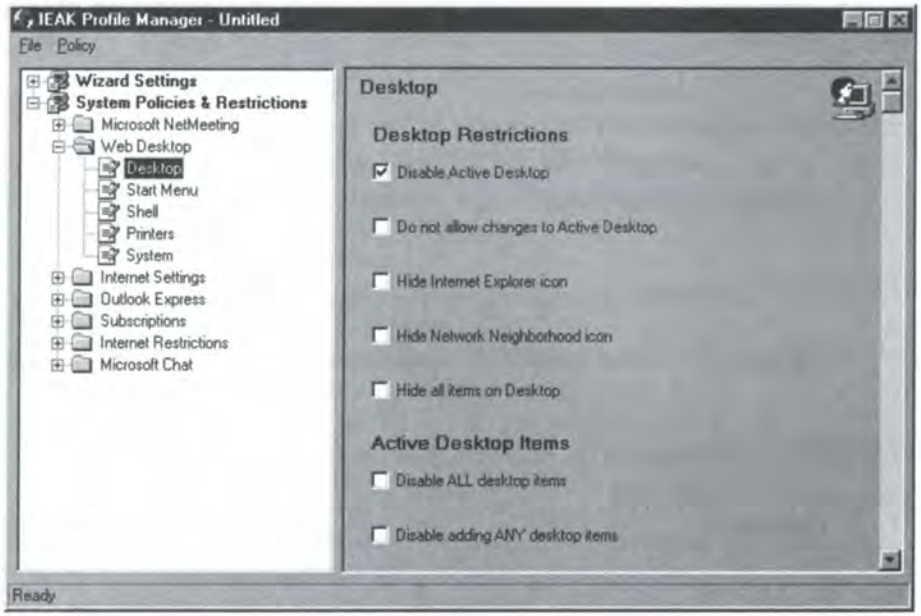
The following table briefly describes each subcategory of the **Wizard Settings** section of the IEAK Profile Manager.

Area	Description
Browser Title	Specifies the text that appears in the title bar of Internet Explorer and in a custom toolbar bitmap.
Support Page	Specifies the online-support page that appears when users select Online Support on the **Help** menu in Internet Explorer.
Favorites	Specifies the default favorites that appear on the **Favorites** menu in Internet Explorer.
Desktop Wallpaper	Specifies a custom wallpaper file to be used for the desktop background.
User Agent	Specifies a custom user agent string that will be appended to the default Internet Explorer string.
Proxy Settings	Specifies the proxy settings that Internet Explorer uses.
Start and Search Page	Specifies the start page that appears when users click **Home** and the search page that appears when users click **Search**.
Import Channels	Specifies custom Active Channels on users' desktops.
Import Software Updates	Specifies software distribution channels on users' desktops.
Outlook Express	Specifies Outlook Express Internet mail and news settings.
LDAP Settings	Specifies a Lightweight Directory Access Protocol (LDAP) server to provide Internet directory services to users.
Outlook Express Customizations	Specifies a custom InfoPane and welcome message for Outlook Express.
Signature	Specifies a standard signature line, such as a corporate disclaimer, to be appended to Outlook Express mail and news messages.
Specify Active Desktop Components	Specifies custom Active Channels on users' desktops.
My Computer and Control Panel Webview Customization	Specifies custom Web views for the My Computer and Control Panel folders.
Automatic Browser Configuration	Specifies automatic browser configuration settings.
Security Zones and Content Ratings Customization	Specifies security and content rating settings.
Site Certificate and Authenticode Settings	Specifies digital certificate and Authenticode trust settings.

For more information about specific Wizard Settings options, see "Building Custom Packages" in Chapter 36, "Implementing the Deployment."

Changing System Policies and Restrictions

In the left pane, the **Systems Policies & Restrictions** object and its subobjects correspond to the same settings available on the IEAK Configuration Wizard **System Policies and Restrictions** page. You can select an object and change the corresponding policies and restrictions. For example, you can expand the Web Desktop tree and select the **Desktop** object to specify Desktop options, such as **Disable Active Desktop**.



The IEAK uses a default set of Windows policy templates (.adm) files to define the rules for the wide range of policies and restrictions that appear in the **System Policies & Restrictions** hierarchy. You can also use your own custom .adm files to add policies and restrictions to the hierarchy.

Policies and restrictions that you specify using the IEAK are saved to information (.inf) files, which are packaged into the auto-configuration companion cabinet (.cab) files for download to user's systems. When unpacked, the .inf files are used to change policies and restrictions on users' systems.

The first time the IEAK Configuration Wizard is run, the policy template (.adm) files in the C:\Program Files\Ieak\Policies directory are created. The following table briefly describes each of the default areas for which you can specify system policies and restrictions.

Area	Description
Microsoft NetMeeting	Specifies policies to control user and computer-access privileges for your NetMeeting community.
Web Desktop	Restricts users from adding, accessing, modifying, or deleting various portions of the desktop.
Internet Settings	Specifies a variety of Internet settings for users.
Outlook Express	Specifies restrictions to help reduce Internet mail and news-support costs.
Subscriptions	Specifies restrictions for subscriptions.
Internet Restrictions	Specifies and locks down settings for Internet Explorer **Internet Options** settings, code download, and channel settings.
Microsoft Chat	Restricts access to Chat features and functions.

You can specify a wide variety of Internet Explorer, application, desktop, and operating system settings across your organization. You can customize settings, ranging from whether users can delete printers to whether or not they can add items to the new Windows Desktop Update.

You can lock down features and functions. For example, you could use the **System** options, under the **Web Desktop** category, to prevent Windows 95 users from restarting their systems in MS-DOS mode. You could also use the **Security** option under **Internet Restrictions** to prevent users from changing any of the security settings on the **Security** tab in Internet Explorer. When features are locked down, they either don't appear, or they appear dimmed on the user's desktop.

Before changing system policies and restrictions, you should understand the impact of the security settings on your users, especially if you have roaming users who share computers with other users. For example, what are the implications of removing icons from the desktop or not allowing users to change their security settings? Make sure that your users understand which features they have access to and which features need to be configured by your IT organization.

Using Custom Policy Templates

Those who are familiar with Windows policy template (.adm) files can create their own templates to define additional restrictions. Policies and restrictions and .adm files are standard in Windows 95 and Windows NT. For more information, see your Windows documentation.

You can choose **Import** on the **Policy** menu in order to import custom .adm files. You should choose **Check Duplicate Keys** on the **Policy** menu to check for duplicate registry keys in the templates, then delete any duplicates from your templates. Always test your templates thoroughly in the lab before using them to make changes to users' systems.

When you use custom policy templates, the IEAK Profile Manager generates an .inf file, using the file prefix for the imported custom template. For example, if you import custom.adm, a custom.inf file will be generated and added to the companion .cab files.

Using Auto-Configuration File Templates

You should use the install.ins file for each custom package as a template to create your auto-configuration files.

▶ **To use install.ins as a template**

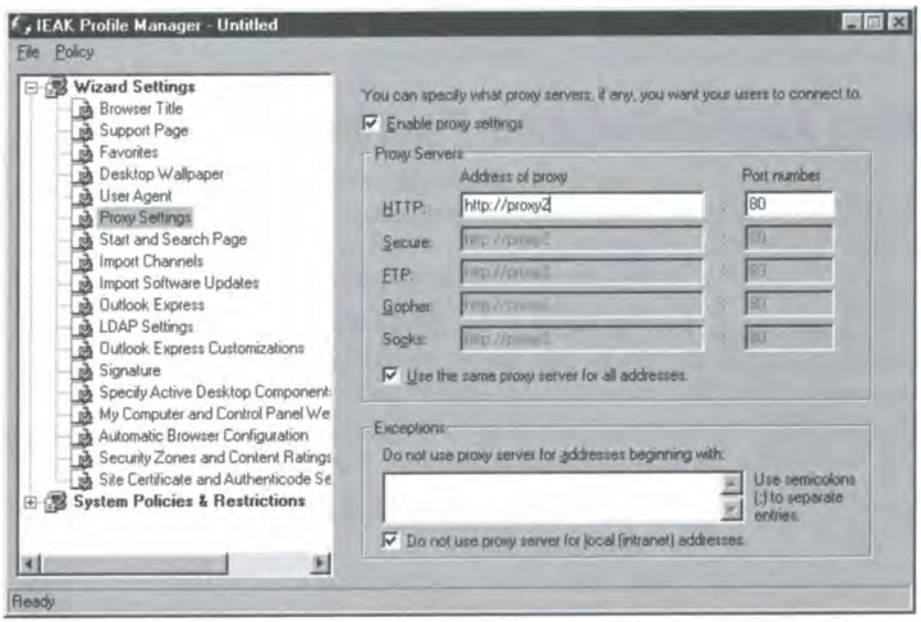
1. On the **File** menu, click **Open**, and then open the appropriate install.ins file.
2. On the **File** menu, choose **Save As,** and save the file as *usergroup*.ins (where *usergroup* is the name of the user group).
3. Change and save any new options or settings you want for the user group configurations.
4. Copy the file to the appropriate auto-configuration directory on the central management server.

When you first create the *usergroup*.ins file, the companion .inf files are generated and packaged as .cab files.

Maintaining Auto-Configuration Files

You maintain auto-configuration files by opening the *usergroup*.ins file in the Profile Manager, changing settings, and saving the *usergroup*.ins file. The Profile Manager keeps the companion files current, each time you save the *usergroup*.ins file.

For example, if you add more proxy servers to your network and you don't use auto-proxy files, you'll need to update users' settings by selecting the Proxy Settings object in the Wizard Settings hierarchy in the left pane of the IEAK Profile Manager. You would use the IEAK Profile Manager to modify the proxy settings for the affected user groups. Automatic browser configuration then updates the users' proxy settings at the specified auto-configuration interval or when Internet Explorer is restarted.



Caution You should not maintain files directly on the production server. You should copy *usergroup*.ins files and their companion files to a working directory, modify the files as necessary, and test auto-configuration in a lab to verify that auto-configuration changes work as intended. After changes have been validated, update the auto-configuration files on the production server.

CHAPTER 38

Software Distribution and Updates

In this chapter

Software Distribution Overview 690
Understanding Software Distribution Channels 690
Implementing Software Distribution Channels 691
Identifying Software Distribution Requirements 691
Selecting Software Distribution Strategies 692
Determining the Number of Distribution Sites 692
Determining the Types of Channels 692
Specifying Distribution Schedules 695
Choosing Installation Methods 695
Choosing Notification Methods 695
Configuring Software Distribution Channels 696
Creating Web Content 696
Creating the CDF Files 697
Creating OSD Files 699
Creating Software Distribution Packages 700
Signing Software Distribution Packages 701
Configuring Web Servers 702
Building Custom Packages With Pre-Configured Channels 702
Configuring the Current Computer 702
Importing the Software Distribution Channels 703
Locking Down Software Distribution Channels 704
Deploying the Custom Packages 704
Managing Software Distribution Channels 705

Software Distribution Overview

This chapter describes how to implement a software distribution system using Active Channels in Microsoft Internet Explorer 4. It describes how software distribution channels work. It also details how to configure software distribution channels and deploy custom packages of Internet Explorer, including the software distribution channels for your users.

This chapter provides information to help you:

- Understand software distribution channels.
- Implement software distribution channels.
- Manage software distribution channels.

Understanding Software Distribution Channels

Internet Explorer 4 users can subscribe to Active Channels, which are Web sites designed to deliver content from the Internet or intranet to subscribing computers. Subscribers receive updated information from Active Channels on demand or at scheduled intervals. You can turn any Web site into an Active Channel by creating a Channel Definition Format (CDF) file to define the channel. For more information on Active Channels, see Chapter 16, "Managed Webcasting" and the *Internet Client Software Development Kit (SDK).*

Software distribution channels are a special type of Active Channel. The CDF files for software distribution channels contain Open Software Distribution (OSD) elements that specify the software distribution settings and options. You can schedule a software distribution channel to update subscribers' computers at an interval of time such as daily, weekly, or monthly. Each time the channel is updated, the latest version of the CDF file is downloaded to subscribers' computers. When the OSD section of the CDF file indicates that a new version of the software is available, subscribers' computers can be instructed to do one of the following:

- Download the installation files to users' hard disks so that users can manually install the update.
- Install the update automatically.

You specify the update process to be used in the OSD section of the CDF file for the channel. You can also notify users and provide instructions for installation of the updates.

Implementing Software Distribution Channels

You can use software distribution channels to distribute software updates over your intranet or the Internet to end-user desktops. To implement software distribution channels:

- Identify software distribution requirements.
- Select software distribution strategies.
- Configure Web servers for software distribution channels.
- Build custom packages of Internet Explorer with pre-configured software distribution channels and automatic browser configuration enabled.
- Deploy the pre-configured custom packages to end users.

The following sections describe the process for implementing software distribution channels. Detailed technical information is provided in the following resources:

- For more information about the CDF and OSD specifications, see the Microsoft Site Builder Network specifications and standards page at **http://www.microsoft.com/standards/**.
- For detailed information about how to use CDF files and OSD files to create software distribution channels, see the *Internet Client SDK*. To obtain the Internet Client SDK, see **http://www.microsoft.com/msdn/sdk/inetsdk/asetup/**.
- For information on how to use sample CDF templates to set up software distribution channels for updating Internet Explorer 4, see the section named "Updates with Software Distribution Channels" in the Internet Explorer Administration Kit (IEAK) Help.

Identifying Software Distribution Requirements

Before selecting strategies for software distribution, identify the software distribution requirements for your organization. Begin by surveying the user groups in your organization and identifying the software packages they use. Be sure to note special requirements for each group, such as language requirements and any custom applications they use. For example, you would note that a graphics design group uses a suite of professional illustration applications that are not used by other groups in your organization.

After all user groups are surveyed:

- Identify the applications you want to support.
- Identify the user groups you want to provide with pre-configured software distribution channels.
- Group common applications into functional categories such as office-productivity applications and Internet applications.
- Group specialized applications by function or by the user groups that use them.

You'll use this information to help specify software distribution strategies for each user group that you want to support.

Selecting Software Distribution Strategies

The strategies you choose depend on various factors, including the size of your organization and the types of applications you need to distribute to your users. Select strategies for each of the following:

- Number of distribution sites
- Types of software distribution channels
- Software distribution channel-update schedule
- Installation methods
- Notification methods

Determining the Number of Distribution Sites

Small organizations may need only one distribution Web site. Large organizations may need to provide multiple, mirrored software distribution Web sites to distribute network load and to meet the needs of diverse groups of users. For example, an organization with large operations in North America, Europe, and Asia could implement mirrored distribution sites in each major region of North America, Europe, and Asia.

Determining the Types of Channels

The types of software distribution channels you include in custom packages of Internet Explorer will depend on the number and types of applications you plan to support, as well as the design limitations of CDF and OSD.

Depending on the contents of the CDF file, each software distribution channel can:

- Appear in the Channel bar or in the Software Updates folder on the **Favorites** menu in Internet Explorer.
- Include an unlimited number of software packages or SOFTPKG update items that specify software packages you can update.
- Define the installation of multiple languages, processors, and operating systems for each SOFTPKG update item.

Note Each user can configure Internet Explorer to enable e-mail notification. If a user has configured a channel to enable e-mail notifications, a notification page for each SOFTPKG update item can be automatically sent by e-mail to the user when the channel is updated.

When the channel appears in the Software Updates folder:

- Updates are indicated by a red gleam in the upper-left corner of the channel, and users can select the channel to view the notification Web page in the browser window. This Web page typically contains information briefly describing all available updates, and hyperlinks to pages providing more information on each update.
- Each channel can include an unlimited number of SOFTPKG update items, but only the top-level channel notification page will appear in the browser. Users are notified of individual updates only if they enable e-mail notification in Internet Explorer.
- Only the top-level channel can contain the SCHEDULE element, so all SOFTPKG update items will be updated on the subscribers' computers at the same time.

When the channel appears on the Channel bar:

- The top-level channel and all SOFTPKG update items appear as a hierarchical tree on the Channel bar.
- Updates are indicated by a red gleam in the upper-left corner of the top-level channel and users can select the top-level channel to view the notification Web page in the browser's right pane. This Web page typically contains information briefly describing all available updates, and hyperlinks to pages that provide more information on each update.

- Each SOFTPKG update item appears under the top-level channel without a red gleam. However, users can select each item to view the corresponding notification page in the browser's right pane. Users are notified of individual updates only if they enable e-mail notification in Internet Explorer.

  Note A SOFTPKG item with **USAGE VALUE="None"** does not appear in the channel hierarchy.

- Only the top-level channel can contain the SCHEDULE element, so all SOFTPKG update items will be updated on the subscribers' computers at the same time.

Since only the top-level channel shows the update gleam, you should use top-level notification pages to provide a summary of all available updates. The top-level notification page is the Web page users see when they click on the top-level Channel bar. By default, notification pages appear in the browser window and can also be sent to users via e-mail (when users enable e-mail notification). The summary page could provide a brief description of available updates and provide hyperlinks to the corresponding notification page for each update.

In addition, you can create an Active Desktop item that displays a summary page of available software components. An Active Desktop item is simply a Web page that displays in a floating, borderless frame on the user's desktop. Custom Active Desktop items require special CDF files. For more information, see Chapter 14, "Active Desktop," and Chapter 16, "Managed Webcasting."

When you deploy custom packages of Internet Explorer to end users, you should have enough pre-configured software distribution channels to meet your organization's needs. If automatic browser configuration is enabled for your user groups, however, you can use the IEAK Profile Manager to add or delete software distribution channels for deployed browsers.

You can also easily add SOFTPKG update items to CDF files for existing software distribution channels. Likewise, you can also easily delete SOFTPKG update items if an application is discontinued.

When you pre-configure custom packages for user groups, you should only provide the software distribution channels that each user group needs. For example, you could provide a software distribution channel for office-productivity applications to all user groups, but you wouldn't pre-configure the channels for users in the human resources department to include a software distribution channel for software-developers' applications.

Specifying Distribution Schedules

Specify the schedule for updates by using the SCHEDULE element in CDF files. You can specify daily, weekly, or monthly update frequencies as well as the time of day and the interval during which updates can occur. You can override the default CDF schedule, using the IEAK Configuration Wizard or the IEAK Profile Manager to specify different schedules for each custom package you build. Assigning user groups to different schedules, such as alternating days or weeks, can help distribute network load. All SOFTPKG update items use the same schedule as the top-level channel.

Schedule software downloads for times of low network load—especially for large software packages. To avoid heavy load on your distribution servers when all subscribers update the software distribution channel, you should randomize the time that Internet Explorer updates the channel. For example, you could schedule updates for a channel to occur between 1 A.M. and 5 A.M. one day a week. On the specified day, each subscribed Internet Explorer updates the download channel at a random time between 1 A.M. and 5 A.M.

Choosing Installation Methods

Use any of the following installation methods:

- Notify users by e-mail when new software updates are available. Provide instructions and hyperlinks so they can download the software manually.
- Download the installation files to users' hard disks, notify users, and provide instructions and hyperlinks so they can run the installation program manually.
- Install the updates on users' computers automatically, and notify users that the updates were made.

Use the installation methods that meet your needs, but be cautious about specifying large software packages to download or install automatically. Thoroughly test installation methods in the lab before implementing them as a production solution.

Choosing Notification Methods

Users do not receive e-mail notification on updates automatically. They can receive notification if they enable e-mail notification for each software distribution channel using the **Internet Explorer Software Distribution Channel Receive property** page. Also, even though Active Channels provide a top-level update gleam and you can provide a summary page to describe the available updates, users may not view the Internet Explorer Channel bar or the Software Updates folder on the **Favorites** menu for long periods of time—if ever. For this reason, consider multiple ways to notify your users, such as sending e-mail notices and instructions to all users for each new software update.

Configuring Software Distribution Channels

Software distribution channels are Web sites dedicated to software distribution. The content of the Web sites must support the software distribution strategies you select.

To configure software distribution channels:

- Create the Web content to support the channels.
- Create the CDF files to configure the channels.
- Create the OSD files for Microsoft Internet Component Download (MSICD) distributions.
- Create the software distribution packages.
- Sign the software distribution packages.
- Configure the Web servers to support the channels.

Creating Web Content

You can provide notification Web pages for each CDF file. You can also provide optional Channel bar graphics images for use by Internet Explorer.

The notification Web page is used to describe, briefly, all updates available and typically provides users with hyperlinks to the individual update-notification pages for more details. The summary page could be an HTML page or an Active Server page. The notification page is specified in the CDF file for the CHANNEL element HREF attribute—for example, HREF="http://webserver/*filename*.htm" where *filename* is the name of the summary page. When users select the channel on the Channel bar or in the **Favorites** menu, the summary page appears in the browser's right pane. If USAGE VALUE="E-mail", a notification page is sent via e-mail to users who have enabled e-mail notification.

You can create two optional graphics images in either .gif or .jpg format that are used by Internet Explorer to display in the desktop Channel bar and in the browser Channel bar. You can also create an optional .ico image for use in the browser window Channel bar hierarchy. The .ico image will appear to the left of each item in the Channel bar hierarchy. You can use a different icon for each SOFTPKG item in a CDF file.

- **Desktop Channel bar logo.** 32 pixels high by 80 pixels wide and a black background.

  CDF entry: <LOGO HREF="*filename*.gif" STYLE="Image">
- **Browser Channel bar logo.** 32 pixels high by 194 pixels wide and a color background.

  CDF entry: <LOGO HREF="*filename*.gif" STYLE="Image-Wide">

- **Browser Channel bar icon.** 16 pixels high by 16 pixels wide, with different images, colors, or shapes to indicate whether an item is a container for other items or is actual content.

  CDF entry: <LOGO HREF="*filename*.ico" STYLE="Icon">

You can use the Channel bar logo for the browser window logo, and the extra area will be filled in with the same color as the rightmost top pixel. Animated .gif files are not supported. Images are displayed with a fixed 256-color palette regardless of the monitor color depth. Therefore, you should use the Windows halftone palette.

Note The Channel bar provides users with a 14-pixels-high by 14-pixels-wide red gleam to indicate when channel content has been updated. The gleam is a triangular overlay applied to the upper-left corner of the Channel bar logos. When creating Channel bar logos, do not place critical text or visual elements in this area. A 7-pixels-high by 7-pixels-wide gleam is also applied to the upper-left corner of icons to indicate when item content has been updated.

Creating the CDF Files

Create a CDF file for each software distribution channel to be installed on users' desktops. An unlimited number of subchannels or SOFTPKG items can be nested in the CDF file, but they will all have the same schedule as the top-level channel.

This section describes the elements of CDF that are used to define software distribution channels. For more information about CDF files, see "Understanding CDF Files" in Chapter 16, "Managed Webcasting."

The following shows an example CDF file that, when subscribed to, appears on the **Favorites** menu in the Software Updates folder. This CDF file specifies the download of software package 1 to users' hard disks.

```
<?XML version="1.0"?>
<!DOCTYPE Channel SYSTEM "http://www.w3c.org/Channel.dtd">
<CHANNEL HREF="http://ie4support/softdist/product1_info.htm" >
    <TITLE>Software Distribution Channel 1</TITLE>
    <ABSTRACT>This is the abstract for the channel.</ABSTRACT>
    <USAGE VALUE="SoftwareUpdate" />
    <SCHEDULE>
        <INTERVALTIME DAY="7" />
        <EARLIESTTIME HOUR="1" />
        <LATESTTIME HOUR="5" />
    </SCHEDULE>
```

```
    <SOFTPKG NAME={D27CDB6E-AE6D-11CF-96B8-444553540000}"
        VERSION="2,33,608,0" AUTOINSTALL="No"
        STYLE=" " PRECACHE="Yes">
        <IMPLEMENTATION>
            <OS VALUE="win95" />
            <CODEBASE HREF="http/download/Pkg1_95.cab" />
        </IMPLEMENTATION>

        <IMPLEMENTATION>
            <OS VALUE="winnt" />
            <CODEBASE HREF="http/download/Pkg1_NT.cab" />
        </IMPLEMENTATION>
    </SOFTPKG>
</CHANNEL>
```

In this example:

- **CHANNEL HREF="http://ie4support/softdist/product1_info.htm"** provides the notification page for this channel.
- **<USAGE VALUE="SoftwareUpdate" />** specifies that this channel appears in the **Software Update** folder on the **Favorites** menu and not on the Channel bar.
- **INTERVALTIME DAY="7"** specifies the interval as weekly. Use "1" for daily or "28" for monthly (every four weeks).
- **EARLIESTTIME HOUR="1"** and **LATESTTIME HOUR="5"** specifies that subscribed Internet Explorer browsers refresh the channel at random times between 1 A.M. and 5 A.M. Use a 24-hour scale starting with Midnight = "0."
- **HREF="http://ie4support/softdist/package1.htm"** is the notification page that appears in the browser's right pane when users click this software update channel. You can provide installation instructions and hyperlinks on this page.
- **VERSION="2,33,608,0"** specifies the major, minor, build, and custom version numbers of the update. You change this for each new version and the system looks for update instructions.
- **AUTOINSTALL="No"** specifies that the software update is not automatically installed by the system. Use "Yes" to specify automatic installation of the update without user action. AUTOINSTALL overrides the PRECACHE element.
- **STYLE="MSICD"** specifies that the user's computer should use the MSICD to download the distribution package and look at the OSD file for processing instructions. Use "ActiveSetup" to specify that the user's computer should use Active Setup to install the package.

When STYLE="ActiveSetup," the CODEBASE HREF does not specify a .cab file and an OSD file is not used. Instead, Active Setup looks for the Internet Explorer update-distribution package by checking the IE4site.dat file. For example, the IMPLEMENTATION section for an Internet Explorer 4 update channel could specify the location of IE4site.dat as follows:

```
<IMPLEMENTATION>
    <OS VALUE="win95" />
    <CODEBASE HREF="http/ie4support/ie4site/ie4site.dat" />
</IMPLEMENTATION>
```

- **PRECACHE="Yes"** specifies that the software update is downloaded to the user's hard disk. Use "No" to specify that the update is not downloaded.
- **OS VALUE="win95"** and **CODEBASE HREF="http/download/Pkg1_95.cab"** specifies an implementation for Windows 95–based computers. Windows 95–based computers install this package.
- **OS VALUE="winnt"** and **CODEBASE HREF="http/download/Pkg1_NT.cab"** specifies an implementation for Windows NT–based computers. Windows NT–based computers install this package.

You can specify an OS VALUE element for each operating system you need to support. In addition, you can specify other attributes for the IMPLEMENTATION element, including the LANGUAGE and PROCESSOR attributes to further differentiate implementations. You can add IMPLEMENTATION sections that provide software packages for each of your platforms and operating systems.

Many other OSD elements and attributes can be used to specify software distribution channels. For example, you can use the DEPENDENCY element to specify a software component that needs to be present on the user's computer for the software distribution package to install successfully. For more guidelines on how to create CDF files for software distribution and a detailed reference on CDF and the OSD extensions, see the *Internet Client SDK*.

Creating OSD Files

The OSD file is similar to the OSD section of the CDF file. This file contains the information that users' computers need to download the MSICD distribution package from the server.

Note You do not create OSD files if you use Active Setup to install a software package.

The following example OSD file specifies a download location for the Windows 95 version of software package 1.

```
<?XML version="1.0" ?>
<!DOCTYPE SOFTPKG SYSTEM
"http://www.microsoft.com/standards/osd/osd.dtd" >
<?XML::namespace href="http://www.microsoft.com/standards/osd/msicd.dtd"
as="msicd"?>

<SOFTPKG NAME="{D27CDB6E-AE6D-11CF-96B8-444553540000}" VERSION="2,0,0,0"
STYLE="MSICD">
    <TITLE>Update for Product 1</TITLE>
    <ABSTRACT>This distribution contains package1.
    </ABSTRACT>

    <msicd::NATIVECODE>
        <CODE   NAME="diagnose.ocx"
                CLASSID="{D27CDB6E-AE6D-11CF-96B8-444553540000}"
                VERSION="2,33,608,0" >
            <IMPLEMENTATION>
                <OS VALUE="win95" />
                <CODEBASE HREF="http/download/Pkg1_95.cab" />
            </IMPLEMENTATION>
        </CODE>
    </msicd::NATIVECODE>
</SOFTPKG>
```

The OSD file is packaged in the Pkg1_95.cab file, and the system uses the OSD file information to properly install the distribution package. You create an OSD file for each implementation of the software package that you install. For more information, see the *Internet Client SDK*.

Creating Software Distribution Packages

Create the software distribution packages you need to support your software distribution channels. Active Setup distribution packages and MSICD software distribution packages contain files that are compressed using the .cab compression format. For more information on .cab, see the *CAB SDK,* which is provided as a self-extracting executable file (Cab-Sdk.exe) in the \bin directory of the *Internet Client SDK.*

For Active Setup, each .cab file contains an .inf file that specifies how the .cab file should be installed. To locate the .cab files for the update, Active Setup reads the information in the ie4site.dat file specified by the CODEBASE HREF="http/ie4support/ie4site/ie4site.dat" entry in the OSD section of the CDF file.

You can use Internet Express (IExpress) to create software packages that can be installed with Active Setup. IExpress is included in the IEAK 4. For more information, see Help for the IEAK.

For MSICD, the .cab files contain the OSD file that specifies how the .cab files should be installed. The MSICD CAB can be packaged three ways:

- Only the OSD file in the .cab file
- The OSD file and application files in the .cab file
- The OSD file and another .cab file in the .cab file

Having only the OSD file in your .cab file is the smallest distribution package possible. The OSD file would indicate the URL of the resource containing the software update in the CODEBASE HREF="http://download/*filename*.cab" element of the OSD file.

The simplest case is to package the OSD file with the application files into the .cab file. In this case, the OSD file does not need the CODEBASE element in it. When no CODEBASE element is given, the user's system automatically checks the same .cab file in which the OSD file was found to locate the application files.

When multiple program files are involved, and especially when the application files are separated into multiple subdirectories, it is easier to organize the distribution package by creating a .cab file that contains the OSD file and another .cab file that contains the application files.

Signing Software Distribution Packages

Digital signatures identify the source of programs and guarantee that the code hasn't changed since it was signed. Depending on how users' browser security levels are configured, users could be prevented from downloading .cab files that aren't signed. Therefore, you should digitally sign .cab, .exe., or .ocx files before distributing software to users' computers.

Signing software package files requires two steps: obtaining a digital certificate—from a Certificate Authority (CA) such as VeriSign or GTE—and signing the code. For more information, see Chapter 28, "Digital Certificates," "Signing Your Programs" in the IEAK Help, and "Signing Code with Microsoft Authenticode Technology" in the *Internet Client SDK*.

Configuring Web Servers

Configure enough Web servers to support your distribution channels, as well as the volume of software you distribute. You can include multiple channels on each Web server.

To configure Web servers:

- Install Web-server software, such as Microsoft Internet Information Server.
- Configure file systems for each software distribution channel.
- Add the notification pages, graphics files, and distribution packages.

Building Custom Packages With Pre-Configured Channels

Build custom packages with software distribution channels pre-configured for each user group in your organization. You should also enable automatic browser configuration, so you can add and manage software distribution channels after browsers are deployed.

When the IEAK Configuration Wizard adds software distribution channels to custom packages, it imports the Internet Explorer software distribution channel configurations from the computer running the wizard. You import the current software distribution channel configuration and specify schedule options.

You can also use the IEAK Configuration Wizard to lock down software distribution channels and prevent users from adding, deleting, or modifying the channels that you specify.

Configuring the Current Computer

Configure the current computer's Internet Explorer to incorporate your software distribution channels before running the IEAK Configuration Wizard. To configure the computer for software distribution channels, you subscribe to each of the software distribution channels you want to include for this user group.

▶ **To subscribe to a software distribution channel**

1. Run Internet Explorer 4.
2. On the **File** menu, click **Open**, and enter http://*server/path/filename*.cdf.

   Where *server/path/filename* is the Web server, path, and file name in which the CDF file is located.

   An **Add Active Channel** or an **Add Software Distribution Channel** dialog box appears.
3. At the dialog box, select **OK** to subscribe to the channel.

Repeat this process for each software distribution channel.

Importing the Software Distribution Channels

To import the software distribution channels, use the IEAK Configuration Wizard.

▶ To import the software distribution channels

1. Run the IEAK Configuration Wizard, and navigate to the **Customize Software Update Channels** page:



2. Select **Import current Software Distribution Channel configuration** to import the software distribution channel configurations.
3. Select one of the following options from the **Schedule** selection box.

Option	Description
<none – do not subscribe to channel>	Specifies that all software distribution channels are imported, but not subscribed to, when the custom package is installed on users' computers. This is the default. Be careful you do not select this by mistake.
Auto	Specifies that each software distribution channel uses the schedule information contained in the SCHEDULE section of its CDF file when the custom package is installed on users' computers.

Option	Description
Daily	Specifies that all software distribution channels are scheduled to be updated daily when the custom package is installed on users' computers.
Monthly	Specifies that all software distribution channels are scheduled to be updated monthly when the custom package is installed on users' computers.
Weekly	Specifies that all software distribution channels are scheduled to be updated weekly when the custom package is installed on users' computers.

4. Select **Next** to use the current channel configuration for the custom build.
5. Finish building the custom package.

Locking Down Software Distribution Channels

You can use the IEAK Configuration Wizard to lock down software distribution channels for the custom packages that you build. After browsers are deployed, you can use the IEAK Profile Manager to lock down software distribution channels through automatic browser configuration.

Software distribution channels use the same settings as Active Channels. For more information on how to lock down Active Channels, see "Locking Down Active Channels and Desktop Items" in Chapter 16, "Managed Webcasting."

Deploying the Custom Packages

Deploy custom packages to your user groups with the appropriate software distribution channels pre-configured. When custom packages are deployed and installed, you can manage software distribution and updates for each user group using the software distribution channels. For more information about how to deploy custom packages, see "Building Custom Packages" in Chapter 36, "Implementing the Deployment."

You could also add subscription links for the CDF files to your Web pages, so users who do not have pre-configured software distribution channels can visit your Web pages and click on the links to subscribe to the channels.

Managing Software Distribution Channels

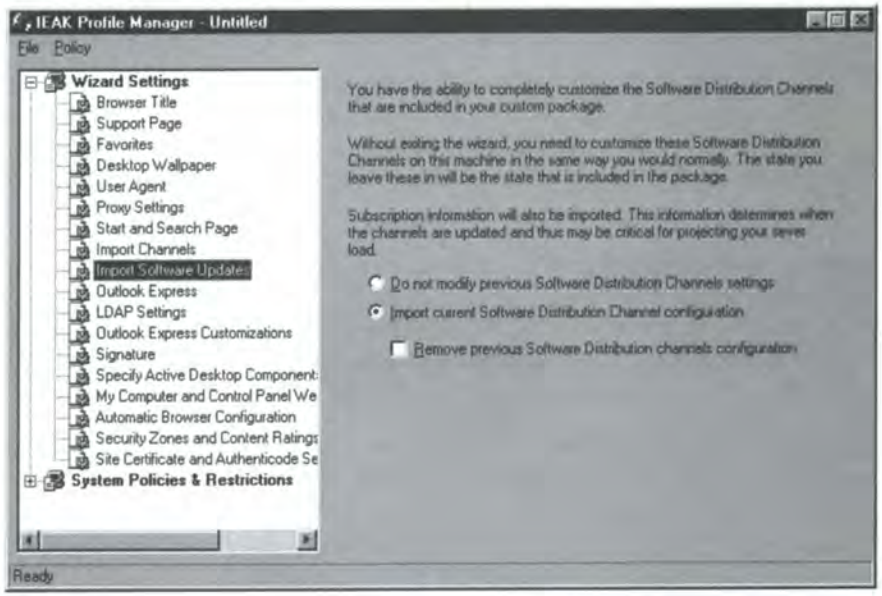
To manage software distribution channels for deployed browsers, you can use the IEAK Profile Manager in conjunction with automatic browser configuration. (For more information about automatic browser configuration, see Chapter 37, "Automatic Browser Configuration.")

To change software distribution channels for a group, you configure the channels on the machine running the IEAK Profile Manager and then use the Profile Manager to import the configurations and save the new configuration settings to the auto-configuration files for the user group.

When automatic browser configuration is refreshed at users' computers, users' desktops are configured with the new software distribution channel settings you specify. You can also optionally remove previous software distribution channel configurations from users' computers.

▶ To change software distribution channel configurations

1. Use Internet Explorer to configure software distribution channels for the current desktop.
2. Run the IEAK Profile Manager.
3. Open the auto-configuration (.ins) file for the user group.
4. In the left pane, select the **Wizard Settings** hierarchy, and select the **Import Software Updates** object.



5. In the right pane, select **Import current Software Distribution Channel configuration** to import the software distribution channel configurations.
6. If you want to remove previous channel configurations from users' computers, select **Remove previous Software Distribution channels configuration**.
7. On the **File** menu, click **Save**.

   Changes are made to users' configurations as scheduled by automatic browser configuration.

APPENDIX A

Switches, Keys, and Files in Internet Explorer 4 Setup

This appendix details the following switches, keys, and files for Internet Explorer Setup:

- WExtract command-line switches for IE4Setup.exe
- Other setup registry keys
- Command-line switches for Active Setup AutoUpdate
- Command-line switches for ACME Setup
- The sections of the SoftBoot.inf
- Files left in the system after uninstalling Internet Explorer

To learn more about Setup, see Chapters 2 and 3.

WExtract Command-Line Switches for IE4Setup.exe

The command-line switch **/c:*program command*** specifies the command to execute, which overrides the command defined in running WExtract at authoring time. If the command is blank, WExtract just extracts files to the defined temporary folder and leaves files there without executing a command or deleting any files.

If there is no blank **/c:** switch (user does not request to keep the extracted files), WExtract adds the RunOnce entry **wextract /d:*subfolder path*** before the RunCommand phase, in case the RunCommand phase never returns (failed install). This way, the next reboot will clean up the leftover files in the temp folder from the failed process.

If the RunCommand phase returns, WExtract will clean up the temp subfolder and delete the RunOnce entry entered earlier. Otherwise, if the RunCommand phase never returns to WExtract, RunOnce will call WExtract with the **/d** option at reboot time to clean up the process.

Switch	Purpose	Description
/q	Quiet mode	The difference between User and Admin quiet mode has to do with the amount of user-interface dialog boxes that are presented. User quiet mode will still present some user-interface dialog boxes, whereas Admin quiet mode will not show any user interface dialog boxes.
/qu -	User quiet mode	
/qa -	Admin quiet mode	
/t:*folder path*	Change target folder	Provides a target path. Failure to use a colon will return user to command help (**/?**). If the folder specified does not exist, WExtract will create it and remove it after using the files, if the **/c** switch is not also used. By default, without the **/t:** switch, WExtract will extract files to a unique, randomly created subfolder under C:\Temp or to the current folder if C:\Temp does not has enough space.
/c	Extract only	Prevents the execution of a Setup process after the extraction is complete.
/c:*path to exe*	Change Setup.exe	Specifies the path to .exe to run instead of the default .exe after file extraction.
/r:n	Never reboot	Never reboot.
/r:i	Reboot if necessary	Reboot if necessary.
/r:a	Always reboot	Always reboot.
/r:s	Silent reboot	Silent reboot.
/n:g	Do not run GrpConv	Do not run GrpConv.
/n:e	Do not extract files	Do not extract files.
/n:v	No version checking	No version checking. Enables you to install over anything.
/i:y	Integrated shell mode	Install integrated shell mode.
/i:n	Browser-only mode	Install browser-only mode.
/q	Batch mode	Install batch mode with no user interface dialog boxes.
/m:*mode*	Specify installation option	Used to select the installation option (**Full**, **Standard**, **Enhanced**), exact syntax not known.
/s:*installation path*	Target location	Chooses the location to install Internet Explorer.
/u:*download path*	Download location	Chooses the location to download the Internet Explorer files.

Other Setup Registry Keys

The following is a list of other registry keys—not mentioned in Chapter 2—that Setup uses before the download phase is complete:

HKEY_CURRENT_USER\Software\Microsoft\Active Setup\jobs

HKEY_CURRENT_USER\Software\Microsoft\Active Setup\jobs\job.IE4

HKEY_CURRENT_USER\Software\Microsoft\Active Setup\jobs\job.IE4\ Internet Explorer 4.0

HKEY_CURRENT_USER\Software\Microsoft\Active Setup\jobs\job.IE4\ Communication Components

HKEY_CURRENT_USER\Software\Microsoft\Active Setup\jobs\job.IE4\ Multimedia Components

HKEY_CURRENT_USER\Software\Microsoft\Active Setup\jobs\job.IE4\ Web Authoring Components

HKEY_CURRENT_USER\Software\Microsoft\Active Setup\jobs\job.IE4\ Additional ActiveX Controls

HKEY_CURRENT_USER\Software\Microsoft\Active Setup\jobs\job.IE4\ CustomOptionalComponents

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ Active Setup[VALDWORD]"TrustValueSet"="3"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\ Installed Components

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ Active Setup\Component Progress

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ Active Setup\Component Progress\IE4

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ Active Setup\InstallInfo

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ Active Setup\InstallInfo\"Setup option"="6"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ Internet Explorer\Security

**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Internet Explorer\Security\Basic**

**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Internet Explorer\Security\
Basic[VALSTR]"SecurityName"="Basic Authentication"**

**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Internet Explorer\Security\Basic[VALSTR]"DLLFile"="WININET.dll"**

**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Internet Explorer\Security\Basic[VALSTR]"SchemeList"="Basic"**

**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Internet Explorer\Security\Basic[VALBINARY]"Flags"="00000000"**

Command-Line Switches for Active Setup AutoUpdate

The following is based on Trigger.exe, now renamed to Actsetup.exe:

Switch	Description
/j:	Specifies "Job" branch to use under ActiveSetup for baseURL and .cif file name.
/u:	URL used to override job, no site switching.
/s:	URL of site list location.
/q	No user interface for any of the session.
/I:	GUID ID to install.
/c:	CIFCAB:.cif file name.

When a user runs Actsetup.exe with a job name, the .exe will look in the branch under the registry key

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Job

for the job name. Stored there will be the following values:

- SitelistURL
- Region
- baseURL
- alternate URLs
- .cif
- .cif .cab name

Then Actsetup.exe will look at the InstalledComponents branch and queue up all the items in the list by creating a temporary job. The job will then be passed to Jobexec.dll for processing. If the **/u:** is specified, only one URL will be used and will override the job settings. If **/s:** is used, Actsetup.exe will get the list and first try the URLs in the job list. If none are found, it will display to the user a list of sites similar to the user interface in the base Internet Explorer setup. The selected URLs should also be written back to the "job" branch under ActiveSetup, if possible.

If **/I:** is passed, only that GUID will be used for the update. Priorities for installed items will be based on entries in the CIF file. Priority = *x* (larger numbers being higher priority). Actsetup.exe will not set up any of the priorities in the job it creates. If not set in the .cif file, there will be no priorities for the session.

Command-Line Switches for ACME Setup

Switch	Purpose	Description
s/a	Administrator mode	Only available from original media (not from an image or flat).
/b *<digit>*	Always suppress AppMainDlg by preselecting one big button.	Always suppresses AppMainDlg by pre-selecting one big button. *<digit>* is the 1 based index into the button list in the data field of the AppMainDlg object. Invalid digit == noop.
/c *<COA>*	Specify OEM PID	Enters and validates the 20-character Product ID from the OEM Certificate of Authorization, replacing user dialog box. Example: /C 12345OEM123456712345 (OEM must be in caps.)
/f	No LFNs	Suppresses long file names and uses FAT compatible 8.3 names.
/g "*<path\file>*"	Generate logfile	Generates the log file that provides details of the install. Requires a fully qualified path. Note: When logging is turned on for Debug builds, any Assertion Failures will be sent directly to the log file without displaying a message box.
/g# "*<path\file>*"	Debug only	Debug only: dumps all error messages to log.
/gc "*<path\file>*"	Debug only, including all calls and returns from custom actions	Like **/g**, but includes all calls and returns from custom actions. This can get very big.

Switch	Purpose	Description
/g+ "*<path\file>*"	Append log entries to existing log file	Appends log entries to existing log file.
/g#c+ "*<path\file>*"		Can use any permutation or combination of **/g** parameters
/h		Reserved for BiDi Help file specification.
/i		Reserved for BiDi Help file UI interface choice.
/k "*<CD key>*"	Specify PID	Enters and validates the 10- or 11-digit key from the compact-disc sticker, replacing the user dialog box that would appear. Example: **/k** "1234567890" (key size depends on whether trigger is being used).
/l *<lst file>*	Specify Setup.lst file	Specifies the file that lists files bootstrapper copies to the temporary directory. Defaults to Setup.lst. Not seen by Acmsetup.exe.
/m [*#*]	Bypass anti-piracy limits	Bypasses anti-piracy limits. When used with a number, such as **/m50**, it specifies the additional licenses to be activated by an MLP purchaser.
/n ""		Uses Win.ini. Copies Disincentive Name if it exists; otherwise, prompts the user. Not useful with **/a**.
/n "*<name>*"		Uses Win.ini. Copies Disincentive Name if it exists; otherwise, uses the *<name>* value. Not useful with /A.
/o ""		Uses Win.ini. Copies Disincentive Org if it exists; otherwise, prompts the user.
/o "*<org>*"		Uses Win.ini. Copies Disincentive Org if it exists; otherwise, uses the *<org>* value.
/p *<script file>*	Debug only	Debug only: List of forced checkpoint failures.
/q[0|1|T]	Quiet install mode	Batch mode: no UI. Normally, the exit dialog box is still displayed (**/q** or **/q0**). /Q1 will suppress the exit dialog box, /QT will suppress all UI, including the background frame window and the copy gauge. Assert failures will still show up in debug mode, however. Note: An administrator can modify the check box State fields in the .stf file to generate a customized batch mode Setup. (See table.txt for more detail.)

Switch	Purpose	Description
/qn[1|t]	Quiet mode with reboot suppressed	Not valid with **/q0**. Warning: Chaining together several installs with suppressed reboots may have unpredictable results.
/r	Reinstall the application	
/s ***<src dir>***	Specify alternative source files	Specifies the location of source files to be installed. Overrides the default source (where ACME was launched from, or the source specified in the maintenance mode .stf file). Provided automatically by the bootstrapper if ACME is bootstrapped.
/t ***<table file>***	Specify alternative table files	Specifies table file to use (default is *<base>*.stf, where *<base>* is the "8" part of your .exe file's 8.3 file name).
/u [a]	Uninstall the application	Uninstalls the application. If **/q** is also specified, the user will not be prompted about removing shared components. **/u** will not remove shared components by default. **/ua** will always remove shared components without prompting the user.
/v	Don't bind executable files	Doesn't bind .exe files that are marked as bindable. This gives you a back door if binding turns out to be a problem.
/w ***<stf file>***	Specify alternative stf files	Used to indicate that the bootstrapper is running on a previously installed .stf file. Not seen by Acmsetup.exe.
/x "*<path\file>***"**	Create a network install log file.	Creates a network install log file for tracking the number of installs from an admin image. Overrides the value (if any) specified in the .stf file. See doc\table.txt for a description of Network Log Location.
/y	Do not copy files	Does not copy files. Useful when trying to track down problems that occur after the (time-consuming) step of copying the files.
/z		Optional UI hook .dll for replacement dialog boxes (consumer).
/#	Force reserialization of the PID	Forces reserialization of the Product ID. This is to be used in the rare case that two installations from the same original media have received the same generated PID.
/?	Usage message	
/##		## or other invalid parameter yields a better usage message.

Notes about command-line switches:

- The ACME command-line arguments are case insensitive.
- The **/a** and **/q** flags are mutually exclusive.
- The **/u** and **/r** flags are mutually exclusive and only make sense when running maintenance mode.

The Sections of the SoftBoot.inf

`[W95_NoKillProgs]`

SoftBoot will not close these programs/processes.

`[NT_NoKillProgs]`

SoftBoot will not close these programs/processes.

`[W95_SafeKillProgs]`

These programs will be terminated safely, i.e., a WM_ENDSESSION message will be sent to them.

`[NT_SafeKillProgs]`

These programs will be terminated safely, i.e., a WM_ENDSESSION message will be sent to them.

`[16BitDLLs]`

When programs/processes are terminated, their 16-bit DLLs are not freed up. This section specifies the 16-bit DLLs that need to be freed up explicitly.

`[KeepDLLs]`

Do not process the entry in the Wininit.ini that says to replace these files.

`[OkIfDelFileFails]`

During uninstall time, if SoftBoot cannot delete these files, don't flag this condition as requiring a hard reboot.

`[KnownApps]`

We do not care if these programs/processes are running. If these are running, the user will not be prompted to close programs.

Files Left in the System After Uninstalling Internet Explorer

Windows\Dooflop.exe
Windows\MSImgSiz.dat
Windows\FpXpress.ini
Windows\RaUninst.exe
Windows\MSMusCtl.ini
Windows\Active Setup Log.txt
Windows\IE4 Setup Log.txt
Windows\IE4 Uninstall Log.txt
Windows\JavaInst.log
Windows\Reg Restore Log.txt
Windows\Soft Boot Log.txt
Windows\Bind List Log.txt
Windows\RunOnceEx Log.txt
Windows\WpLog.txt
Windows\INF\IE4Setup.inf
Windows\INF\ICW95.inf
Windows\INF\INFD132.pnf
Windows\INF\INFD324.pnf
Windows\INF\CChat2.inf
Windows\INF\Setup.pnf
Windows\INF\MSImn.inf
Windows\INF\IR50_32.inf
Windows\INF\MSDXMIni.inf
Windows\INF\VdoLive.inf
Windows\INF\FPXpress.inf
Windows\INF\CabPayIE.inf
Windows\INF\ChlEn-US.pnf
Windows\INF\MSImn.pnf
Windows\INF\INFD0F1.pnf
Windows\System\IEJava.cab
Windows\System\ChatSock.dll
Windows\System\ILS.dll
Windows\System\MSSCMC32.dll
Windows\System\L3CodeCa.acm
Windows\System\WLDAP32.dll
Windows\System\ViVOG723.acm
Windows\System\IR50_32.dll
Windows\System\IR50_QC.dll

Windows\System\NSFile.ocx
Windows\System\IVVideo.dll
Windows\System\IR50_QCX.dll
Windows\System\HomePage.inf
Windows\System\IE4Files.inf
Windows\System\UniD192.tmp
Windows\System\IE4Uinit.exe
Windows\System\IE4Uinit.inf
Windows\System\MSVCRT.dll
Windows\System\AsycFilt.dll
Windows\System\CFGMgr32.dll
Windows\System\CkCNV.exe
Windows\System\MSAPSSPC.dll
Windows\System\IERnOnce.dll
Windows\System\LoadWC.exe
Windows\System\SetupAPI.dll
Windows\System\SoftBoot.exe
Windows\System\SoftBoot.inf
Windows\System\Cabinet.dll
Windows\System\VdK32119.acm
Windows\System\UniD1B4.tmp
Windows\System\UniD204.tmp
Windows\System\InetComm.dll
Windows\System\MSOEMAPI.dll
Windows\System\MSOERt.dll
Windows\System\MSOEAcct.dll
Windows\System\VdK3211W.dll
Windows\System\VdK32116.dll
Windows\System\VdoWave.drv
Windows\System\VdoDEC32.dll
Windows\System\DECVW_32.dll
Windows\System\ClrVidDD.dll
Windows\System\TR2032.dll
Windows\System\UNAXA.exe
Windows\System\IAC25_32.ax
Windows\System\IVFSrc.ax
Windows\System\SetDefEd.exe
Windows\System\MSDatSrc.tlb
Windows\System\MSR2C.dll
Windows\System\MSR2CENU.dll
Windows\System\MSVBVM50.dll
Windows\System\WLTUnins.exe

Windows\Help\MSMusCtl.hlp
Windows\Help\SignIn.hlp
Windows\Help\InetComm.hlp
Windows\Help\Conn_OE.hlp
Windows\Help\Conn_OE.cnt
Windows\SendTo\Mail Recipient.MAPIMail
Windows\Fonts\WebDings.ttf
Windows\Java\Security.txt
Windows\Cursors\Globe.ani
Windows\Temporary Internet Files\OAVI1SGX\Desktop.ini
Windows\Temporary Internet Files\ULCRMVYH\Desktop.ini
Windows\Temporary Internet Files\C1QL8AWK\Desktop.ini
Windows\Temporary Internet Files\4JDTB8SW\Desktop.ini
Windows\Recent\PreIE4US.txt.lnk
Windows\Recent\WithUS1712.2.txt.lnk
Windows\Application Data\Microsoft\Internet Explorer\Desktop.htt
Windows\Downloaded Program Files\Microsoft XML Parser for Java.osd
Windows\Downloaded Program Files\Internet Explorer Classes for Java.osd
Windows\Downloaded Program Files\DirectAnimation Java Classes.osd
Recycled\Desktop.ini
Program Files\Common Files\MSCreate.dir
Program Files\Common Files\Microsoft Shared\MSCreate.dir
Program Files\Common Files\Microsoft Shared\Stationery\Baby News.htm
Program Files\Common Files\Microsoft Shared\Stationery\
Balloon Party Invitation.htm
Program Files\Common Files\Microsoft Shared\Stationery\Chess.htm
Program Files\Common Files\Microsoft Shared\Stationery\Chicken Soup.htm
Program Files\Common Files\Microsoft Shared\Stationery\Formal Announcement.htm
Program Files\Common Files\Microsoft Shared\Stationery\For Sale.htm
Program Files\Common Files\Microsoft Shared\Stationery\Fun Bus.htm
Program Files\Common Files\Microsoft Shared\Stationery\Holiday Letter.htm
Program Files\Common Files\Microsoft Shared\Stationery\Mabel.htm
Program Files\Common Files\Microsoft Shared\Stationery\Running Birthday.htm
Program Files\Common Files\Microsoft Shared\Stationery\Story Book.htm
Program Files\Common Files\Microsoft Shared\Stationery\Tiki Lounge.htm
Program Files\Common Files\Microsoft Shared\Stationery\Ivy.htm
Program Files\Common Files\Microsoft Shared\Stationery\One Green Balloon.gif
Program Files\Common Files\Microsoft Shared\Stationery\Baby News Bkgrd.gif
Program Files\Common Files\Microsoft Shared\Stationery\Chess.gif
Program Files\Common Files\Microsoft Shared\Stationery\Chicken Soup Bkgrd.gif
Program Files\Common Files\Microsoft Shared\Stationery\
Formal Announcement Bkgrd.gif

Program Files\Common Files\Microsoft Shared\Stationery\For Sale Bkgrd.gif
Program Files\Common Files\Microsoft Shared\Stationery\FunBus.gif
Program Files\Common Files\Microsoft Shared\Stationery\Holiday Letter Bkgrd.gif
Program Files\Common Files\Microsoft Shared\Stationery\MabelT.gif
Program Files\Common Files\Microsoft Shared\Stationery\MabelB.gif
Program Files\Common Files\Microsoft Shared\Stationery\Running.gif
Program Files\Common Files\Microsoft Shared\Stationery\Santa Workshop.gif
Program Files\Common Files\Microsoft Shared\Stationery\Soup Bowl.gif
Program Files\Common Files\Microsoft Shared\Stationery\Squiggles.gif
Program Files\Common Files\Microsoft Shared\Stationery\StoryBook.gif
Program Files\Common Files\Microsoft Shared\Stationery\Tiki.gif
Program Files\Common Files\Microsoft Shared\Stationery\Christmas Trees.gif
Program Files\Common Files\Microsoft Shared\Stationery\Ivy.gif
Program Files\Common Files\Microsoft Shared\Stationery\
Balloon Party Invitation Bkgrd.jpg
Program Files\Common Files\Microsoft Shared\Stationery\Technical.htm
Program Files\Common Files\Microsoft Shared\Stationery\Tech.gif
Program Files\Common Files\System\MSAdC\MSAdCo.dll
Program Files\Common Files\System\MSAdC\MSAdCor.dll
Program Files\Common Files\System\MSAdC\MSAdCe.dll
Program Files\Common Files\System\MSAdC\MSAdCer.dll
Program Files\Common Files\System\AdO\MSAdEr15.dll
Program Files\Common Files\System\AdO\MSAdOr15.dll
Program Files\Common Files\System\OLE Db\MSDAdC.dll
Program Files\Common Files\System\OLE Db\MSDAPS.dll
Program Files\Common Files\Services\Bigfoot.bmp
Program Files\Common Files\Services\Four11.bmp
Program Files\Common Files\Services\WhoWhere.bmp
Program Files\Common Files\Services\InfoSpce.bmp
Program Files\Common Files\Services\SwtchBrd.bmp
Program Files\Common Files\Services\VeriSign.bmp
Program Files\Common Files\Services\InfoSpBz.bmp
Program Files\Internet Explorer\Setup\MSCreate.dir
Program Files\Internet Explorer\Signup\Install.ins
Program Files\Internet Explorer\Plugins\NpsMlVdo.dll
Program Files\Outlook Express_ISetup.exe
The entire contents of the Internet Explorer 4 Setup folder

APPENDIX B

Troubleshooting Installation and Uninstallation

This appendix reviews some of the issues related to Microsoft® Internet Explorer 4 installation and uninstallation that may require troubleshooting and explains procedures for solving installation and uninstallation problems. Topics include:

- Cannot install Internet Explorer 4 after download
- Windows Desktop Update not enabled after installing Internet Explorer
- Problems installing 128-bit server gated cryptography
- Problems reinstalling Windows® 95 with Internet Explorer 4
- Invalid page fault when installing additional components
- Problems installing Service Pack 3 after Internet Explorer
- Cannot uninstall Internet Explorer 4 using the Add/Remove Programs tool
- Cannot view Internet properties after uninstalling
- Problems returning to an earlier version of Internet Explorer
- Removing Internet Explorer 4 for Windows 95 using IERemove.exe
- Removing Internet Explorer for Windows NT® 4.0 using IERemove.exe

To learn more about these topics, see Part 1.

Important This section contains information about editing the registry. Before you edit the registry, you should first make a backup copy of the registry files (System.dat and User.dat). Both are hidden files in the Windows\System folder.

Warning Using Registry Editor incorrectly can cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk.

Troubleshooting Installation

There are a variety of problems you may encounter during or after installation of Internet Explorer 4.

Cannot Install Internet Explorer 4 After Download

During download of Internet Explorer 4, Active Setup determines the version of the operating system running and automatically downloads the files appropriate for that operating system. Because these files are unique to the operating system, you cannot download the Internet Explorer installation files using one operating system and then install it to another operating system.

If you attempt to install Internet Explorer from files that were downloaded using a different operating system than the one you are currently running, the following error message may display:

The Internet Explorer files on your computer are not the correct files for your operating system. To continue, you must download the correct files from the Internet. Do you want to continue?

If you click **No**, Active Setup quits. If you click **Yes**, Internet Explorer continues with Active Setup and attempts to download the appropriate files from the Internet.

Note You must be connected to the Internet for the download to continue.

▶ **To resolve this installation issue, use any of the following methods:**

- Download the installation files using the same operating system on which you intend to install Internet Explorer.
- Download the installation files for both operating systems in one session.

Windows Desktop Update Not Enabled After Installing Internet Explorer

After you install Internet Explorer with the Windows Desktop Update, the Windows Desktop Update (and Active Desktop™) may be disabled. This problem occurs when you are running different language versions of Internet Explorer and Windows 95 or Windows 95 OEM Service Release. For example, Windows Desktop Update would be disabled if you installed the English version of Internet Explorer 4 on a computer running a non-English version of Windows 95. As a result, Web sites and pictures are not displayed on your desktop, and the **Desktop** tab does not appear in the **Display Properties** dialog box.

To correct this problem, uninstall Internet Explorer, and then install the same language version of Internet Explorer as the version of Windows 95 or OEM Service Release installed on your computer. For more information about installing Internet Explorer 4, see Chapter 2, "Phase 1: Active Setup."

Problems Installing 128-Bit Server Gated Cryptography

If you install the English-language, exportable 128-bit Server Gated Cryptography (SGC) add-on for Internet Explorer 3 on a computer with Internet Explorer 4 installed, the following message may display:

Microsoft Internet Explorer SGC 128 update

Your computer already has a newer or 128-bit version of this product. Installation will exit.

▶ **To enable 128-bit strong encryption in Internet Explorer 4, use either of the following methods:**

- Install the 128-bit strong encryption version of Internet Explorer 3 before you upgrade to Internet Explorer 4.
- After you install Internet Explorer 4, download the 128-bit strong encryption upgrade for Internet Explorer 4 from the following Web site:

  http://www.microsoft.com/ie/download/?/ie/download/128bit.htm

To learn more about SGC, see Chapter 28, "Digital Certificates."

Problems Reinstalling Windows 95 with Internet Explorer 4

Before you reinstall any version of Windows 95, you should uninstall Internet Explorer 4. If you do not uninstall Internet Explorer 4 before reinstalling Windows 95, you may be unable to start Windows or run Internet Explorer or related components. To avoid these problems, uninstall Internet Explorer, reinstall Windows 95, and then reinstall Internet Explorer.

If you already reinstalled Windows 95 without uninstalling Internet Explorer 4 first and are having problems, read the following information, and select one of the methods explained below. To select the correct method for recovery, you must determine the version of Windows 95 you are running.

▶ To determine the version of Windows 95 you are running

1. In the Windows Control Panel, double-click the System icon.
2. On the **General** tab, locate the version number under the System heading, and then match that number to the version of Windows 95 in the following table:

Version number	Version of Windows 95
40.950	Windows 95
40.950A	Windows 95 plus the Service Pack 1 Update, or OEM Service Release 1
40.950B	OEM Service Release 2 (OSR2)

If you are running OEM Service Release version 2.1, you will see the version number 40.950B (the same as OSR2). To determine whether you are running OSR 2.1, check for "USB Supplement to OSR2" in the list of installed programs in the **Add/Remove Programs Properties** dialog box. Then, check for version 43.1212 of the Ntkern.vxd file in the Windows\System\Vmm32 folder.

Windows 95 may have been preinstalled on your computer. These installations are referred to as original equipment manufacturer (OEM) installations.

▶ To determine whether you have an OEM installation of Windows 95

1. In the Control Panel, double-click the **System** icon.
2. On the **General** tab, locate the Product ID number under the Registered To heading. This number typically contains 20 digits. If digits 7, 8, and 9 contain the letters "OEM," you have an OEM installation of Windows 95. For example:

   ```
   12345-OEM-6789098-76543
   ```

If you are using an OEM installation of Windows 95, you should contact your computer's manufacturer for Windows 95 support.

The methods outlined below are specific to the version of Windows 95 you are running and whether you selected **Yes** or **No** in all **Version Conflict** dialog boxes that displayed while you reinstalled Windows 95.

Version of Windows 95	Response to version conflicts	Use this method
Windows 95 or A	Yes	1
Windows 95 or A	No	2
Windows 95B	Yes	3
Windows 95B	No	4

Method 1

You do not need to make any changes to your current configuration. Reinstalling Windows 95 with Internet Explorer 4 installed and answering **Yes** to all file version conflicts does not cause any problems.

Method 2

Windows 95 works properly, but you may need to reinstall Internet Explorer to resolve browser problems. Reinstalling Internet Explorer 4 should resolve any file version conflicts resulting from reinstalling Windows 95.

Method 3

Windows 95 works properly, but you may experience problems running Internet Explorer 4, because Windows 95 reinstalls Internet Explorer 3. To resolve this problem, reinstall Internet Explorer 4.

Method 4

If you are using the Windows Desktop Update component, the following error messages may occur:

- When you start your computer:

  Error loading Explorer.Exe. You must reinstall Windows.

- When you click **OK**:

  Error Starting program: The Explorer.Exe File is Linked to Missing Export SHLWAPI.DLL:ShopenRegstreamA

In addition, the following may occur:

- Your computer stops responding (hangs) or shuts down.
- If you did not have the Windows Desktop Update installed, you may be able to start Windows 95, but you cannot run Internet Explorer, and your desktop icons cannot be moved.

▶ **To resolve these issues**

1. Restart your computer. When the "Starting Windows 95" message appears, press the F8 key; then choose **Command Prompt Only** from the **Startup** menu.
2. Type the following line, and press ENTER to change to the Uninstall folder:

   cd *uninstall folder* where ***uninstall folder*** is the location of the uninstall folder for Internet Explorer 4. For example:
   cd C:\Progra~1\Intern~1\Uninst~1.

3. Type the following line, and press ENTER to view the hidden files:
   attrib -s -h -r *.*
4. Type the following lines to restore the files necessary to start Windows 95:
   iextract integr~1.dat
5. Type the following lines to place the files in their proper folders:
   copy explorer.exe c:\windows
   copy shell32.dll c:\windows\system
6. Restart the computer.
7. Uninstall Internet Explorer 4, and then reinstall it.

Invalid Page Fault When Installing Additional Components

When you try to install additional components from the Internet Explorer Components Download page, an invalid page fault may occur in Kernel32.dll. As a result, you may not be able to properly restart your computer. This problem can occur if you do not have enough free hard disk space to install the selected components. To correct this problem, free some hard disk space, and try to install the additional components again.

Note The Components Download page does not indicate the amount of hard disk space needed to install the selected components. Instead, the Web page lists the total size of the components.

Problems Installing Service Pack 3 After Internet Explorer

When you try to reapply or uninstall Windows NT 4.0 Service Pack 3 after installing Internet Explorer 4, the following warning message may appear:

Update.exe

This program may not run correctly because of the new features in Internet Explorer 4. You may need to obtain an updated version of this program. For information about obtaining an updated version, click **Details**. If you want to try running this program, click **Details** to determine whether it will cause other problems. Then, if running this program will not cause other problems, click **Run Program**.

The warning dialog box includes a **Run Program** button (runs the program normally), a **Cancel** button (stops the program from running), and a **Details** button.

This warning occurs for the following reasons:

- Reapplying Service Pack 3 has rendered the Internet Explorer 4 shell (and other components) inoperable and invalidated your Service Pack 3 Uninstall folder.
- Uninstalling Service Pack 3 has rendered the Internet Explorer 4 shell (and other components) inoperable.

You can reapply Service Pack 3 by clicking **Run Program** on the warning dialog box and choosing the following options while you're reapplying Service Pack 3:

- Select **No, I do not want to create an Uninstall directory**.
- Select **No** whenever you are prompted to replace newer files.

If you're trying to uninstall Service Pack 3, click **Cancel** on the warning dialog box and uninstall Internet Explorer 4 before uninstalling Service Pack 3.

Windows NT 4 Service Pack 3 is required to run Internet Explorer 4. If you don't have Service Pack 3 installed when you install Internet Explorer 4, the following error message displays, and Setup cannot continue:

Windows NT 4 Service Pack 3 must be installed before Internet Explorer 4 installation can continue.

If you click **Details** on the warning dialog box, the following message appears:

Do not uninstall Windows 95 Service Pack 1. Doing so will render the Internet Explorer 4 shell inoperable.

This message should read as follows:

Do not uninstall Windows NT 4 Service Pack 3. Doing so will render the Internet Explorer 4 shell inoperable. If you are reapplying Service Pack 3, you can safely click Run Program if you choose the following while you are reapplying Service Pack 3:

Note To prevent the warning from being displayed when you run this program in the future, select the **Don't display this message in the future** check box.

Troubleshooting Uninstallation

There are a variety of problems you may encounter during or after uninstallation of Internet Explorer 4.

Cannot Uninstall Internet Explorer 4 Using the Add/Remove Programs Tool

If you cannot uninstall Internet Explorer 4 using the Add/Remove Programs tool in the Control Panel, it is probably because you have deleted the uninstall information by removing the necessary Setup files (IE4bak.dat, IE4bak.ini, Integrated Browser.dat, and Integrated Browser.ini). The Internet Explorer **Advanced Uninstall** dialog box offers the option to uninstall this backup information, but doing so will prevent you from uninstalling Internet Explorer in the future. (For more information, see "Deleting Uninstall Files" in Chapter 7.)

If you attempt to reinstall Internet Explorer after deleting these files, the following message will display:

You are upgrading a version of Internet Explorer 4 in which the uninstall feature has been disabled. If you choose to continue, Setup will update your PC with the newer version, but the uninstall feature will remain disabled.

Cannot View Internet Properties After Uninstalling

After you remove Internet Explorer 4, the following may occur because you have an incorrect version of the Inetcpl.cpl file installed on your computer:

- The **Internet** icon may not be present in the Control Panel.
- You may not be able to access the **Internet Properties** dialog box.
- When you are running Internet Explorer 3, and you select **Options** on the **View** menu, nothing happens.

▶ **To install the correct Inetcpl.cpl file**

1. Delete the Inetcpl.cpl file in the Windows\System folder.
2. Install (or reinstall) Internet Explorer 3. To download Internet Explorer 3, see **http://www.microsoft.com/ie/**.

Problems Returning to an Earlier Version of Internet Explorer

If you install Internet Explorer 4 and then decide that you want to return to an earlier version of Internet Explorer, you should uninstall Internet Explorer 4 before installing the earlier version.

If you attempt to install an earlier version of Internet Explorer on a computer with Internet Explorer 4 installed, the following error message appears:

Internet Explorer 3 cannot be installed on a system that has Internet Explorer 4 installed.

If you click **OK**, the following message appears:

There was an error during the Setup process. Either the user pressed Cancel or there was not enough disk space. Installation failed.

To correct this problem, install Internet Explorer 4 again, and then uninstall it. You can then safely install an older version of Internet Explorer. For information on how to reinstall Internet Explorer 4, see "Reinstalling Components" in Chapter 7. (The process for reinstalling Internet Explorer is the same as the process for reinstalling its components.)

Removing Internet Explorer 4 for Windows 95 Using IERemove.exe

This section describes how to remove Internet Explorer 4 for Windows 95 using the IERemove.exe tool and a registry (for example, System.1st) that was created before you installed Internet Explorer 4.

Use this procedure for the following situations:

- You tried to uninstall Internet Explorer 4, but were unsuccessful.
- With Internet Explorer 4 installed on your computer, you restored a registry that was created before you installed Internet Explorer 4.

Do *not* use this procedure for the following situations:

- You have not tried to uninstall Internet Explorer 4 by using the **Add/Remove Programs** applet in the Control Panel.
- You have removed the Internet Explorer 4 backup files. If you removed these files and are unable to uninstall Internet Explorer using the standard procedure (see Chapter 7), you cannot remove Internet Explorer without reinstalling Windows 95 to a different folder.

For more information about IERemove.exe, see "Understanding IERemove.exe," in Chapter 7.

Note IERemove.exe is a command-line executable file designed to remove Internet Explorer 4 and its components. IERemove.exe cannot remove Internet Explorer without using command line options. For information about the command-line options available for IERemove.exe, type **ieremove /?**.

▶ **To remove Internet Explorer 4 by using the IERemove.exe tool and a registry that was created before you installed Internet Explorer 4**

If you have not already done so, restore the registry that was created before you installed Internet Explorer 4.

Note During the Internet Explorer 4 installation, the original System.1st file is replaced with a copy of the registry. The original System.1st file is saved in the Integrated Browser.dat file (Integr~1.dat).

---

1. To extract the original System.1st file from the Integr~1.dat file, type the following command at a command prompt and press ENTER:

   cd *path*\uninst~1 where ***path*** is the path to the folder where Internet Explorer is installed.

2. Type the following line, and press ENTER:

   attrib integr~1.dat –h

3. Type the following line, and press ENTER:

   iextract /L *dir* integr~1.dat system.1st where ***dir*** is the folder in which the extracted file will be saved.

4. Restart the computer. When the "Starting Windows 95" message appears, press the F8 key, and then choose **Safe Mode Command Prompt Only** from the **Startup** menu.

5. Type the following commands, pressing ENTER after each command:

   cd *path*\uninst~1

   attrib integr~1.dat -h

   iextract integr~1.dat

   copy shell32.dll c:\windows\system

   copy explorer.exe c:\windows

   where ***path*** is the path to the folder where Internet Explorer is installed.

6. Restart the computer.
7. From the **Start** menu, select **Run**, and then type the following command in the **Open** box (with quotation marks):

   "*path1*\ieremove.exe" /i:"*path2*\integrated browser.dat"/n:"*path3*\ie4bak.dat"

   where ***path1*** is the full path to the IERemove.exe file, ***path2*** is the full path to the Integrated Browser.dat file, and ***path3*** is the full path to the IE4bak.dat file. For example, if the IERemove.exe file is in the C:\Windows\System folder, the Integrated Browser.dat file is in the C:\Program Files\Internet Explorer\Uninstall Information folder, and the IE4bak.dat file is in the C:\Windows folder, you would type the following command (with quotation marks):

   "c:\windows\system\ieremove.exe" /i:"c:\program files\internet explorer\uninstall information\integrated browser.dat"/n:"c:\windows\ie4bak.dat"
8. Click **OK**, click **Yes**, then restart your computer after the IERemove.exe tool is finished running.
9. Reinstall Internet Explorer 4, and then uninstall it. This step is necessary to ensure that the additional components included with Internet Explorer 4 are removed.

Removing Internet Explorer for Windows NT 4.0 Using IERemove.exe

This section describes how to remove Internet Explorer 4 for Microsoft Windows NT by using the IERemove.exe tool and the Emergency Repair Disk (ERD).

Use this procedure for the following situations:

- You tried to uninstall Internet Explorer 4, but were unsuccessful.
- You created an ERD before you installed Internet Explorer 4, and then you used the ERD while Internet Explorer 4 was installed on your computer.

Do *not* use this procedure for the following situations:

- You have not tried to uninstall Internet Explorer 4.
- You have removed the Internet Explorer 4 backup files. If you removed these files and are unable to uninstall Internet Explorer using the standard procedure (see Chapter 7), you cannot remove Internet Explorer without reinstalling Windows NT to a different folder.

For more information about IERemove.exe, see "Understanding IERemove.exe," in Chapter 7.

Note IERemove.exe is a command-line executable file designed to remove Internet Explorer 4 and its components. IERemove.exe cannot remove Internet Explorer without using command-line options. For information about the command-line options available for IERemove.exe, type **ieremove /?**.

Before proceeding, locate the "Integrated Browser NT.dat" and the IE4bak.dat files.

▶ **To locate the "Integrated Browser NT.dat" and IE4.bak files**

1. From the **Start** menu, select **Find** and then **Files Or Folders**.
2. In the **Named** box, type **"Integrated Browser NT.dat"** (with quotation marks), and then click **Find Now**.
3. Note the path for the "Integrated Browser NT.dat" file in the In Folder column.
4. Repeat steps 1 to 3 for the IE4bak.dat file.
5. From the **File** menu, select **Close**.

To remove Internet Explorer 4, use the IERemove.exe tool and an ERD that was created before you installed Internet Explorer 4. The following steps guide you through uninstalling the Windows Desktop Update component (if it has been installed) and Internet Explorer. You should uninstall the Windows Desktop Update component before you uninstall Internet Explorer 4.

▶ **To uninstall the Windows Desktop Update component using IERemove.exe**

1. Use the ERD that was created before you installed Internet Explorer 4 to repair your Windows NT installation.
2. Restart your computer and log on to Windows NT.
3. Press CTRL+ALT+DELETE to open the **Windows NT Security** dialog box, and then click **Task Manager**.

4. On the **File** menu, select **New Task (Run)**, and type the following command in the **Open** box (with quotation marks):

   "*path1*\ieremove" /i:"*path2*\integrated browser nt.dat" where ***path1*** is the full path to the IERemove.exe file and ***path2*** is the full path to the "Integrated Browser NT.dat" file.

   For example, if Windows NT is installed in the C:\Winnt folder, the IERemove.exe file will be in the C:\Winnt\System32 folder, and the "Integrated Browser NT.dat" file will be in the C:\Program Files\Plus!\Microsoft Internet\Uninstall Information folder. In this case, you would type the following command (with quotation marks):

   "c:\winnt\system32\ieremove" /i:"c:\program files\plus!\microsoft internet\uninstall information\integrated browser nt.dat"

5. Click **OK**.
6. Minimize the Task Manager window.
7. At the Internet Explorer 4 Uninstall prompt, click **OK**.
8. Click **Yes**, and then click **OK**.
9. Close Task Manager, and restart your computer.

▶ **Uninstall Internet Explorer using IERemove.exe**

1. From the **Start menu**, select **Run**.
2. In the **Open** box, type the following command (with quotation marks):

   "*path1*\ieremove" /n:"*path2*\ie4bak.dat" where ***path1*** is the full path to the IERemove.exe file and ***path2*** is the full path to the IE4bak.dat file.

   For example, if Windows NT is installed in the C:\Winnt folder, the IERemove.exe file will be in the C:\Winnt\System32 folder, and the IE4bak.dat file will be in the C:\Winnt folder. In this case, type the following command (with quotation marks):

   "c:\winnt\system32\ieremove" /n:"c:\winnt\ie4bak.dat"

3. Click **OK**, and then click **OK** again.

   After the IERemove.exe tool has uninstalled Internet Explorer 4, reinstall Internet Explorer 4, and then uninstall it normally. This step is necessary to ensure that the additional components included with Internet Explorer 4 are removed.

APPENDIX C

Troubleshooting the Browser

This appendix reviews some of the issues related to the Microsoft® Internet Explorer browser that may require troubleshooting and explains procedures for improving and configuring browser performance. Topics include:

- Font size change is not saved
- Determining your previous version of Internet Explorer
- Slow connections and inability to view non-Microsoft sites
- Restoring functionality to the downloaded program files folder
- Changing the download location for ActiveX files

To learn more about the browser, see Part 2.

Important This section contains information about editing the registry. Before you edit the registry, you should first make a backup copy of the registry files (System.dat and User.dat). Both are hidden files in the Windows folder.

Warning Using Registry Editor incorrectly can cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk.

Font Size Change is Not Saved

When you change the font size in Internet Explorer by using the **Fonts** command on the **View** menu or the **Fonts** button on the toolbar and then restart Internet Explorer, your change is lost.

Note This behavior is by design. The **Fonts** command on the **View** menu and **Fonts** button on the toolbar are designed to immediately change the font size for the current session only. The **Internet Options** dialog box enables you to change the default font size for future sessions.

▶ **To change the default font size for viewing Web pages**

1. On the **View** menu, click **Internet Options**.
2. On the **General** tab, click **Fonts**.
3. Select a font from the **Font Size** box.
4. Click **OK,** then **OK** again.

Because of the different ways Web pages can be formatted, some pages will not be affected by the above procedure. To change the appearance of such pages, you'll need to override the page formatting.

▶ **To override page formatting**

1. On the **View** menu, click **Internet Options.**
2. On the **General** tab, click **Accessibility.**
3. Select any of the following options:
   - Ignore Colors specified on Web pages
   - Ignore font styles specified on Web pages
   - Ignore font sizes specified on Web pages
   - Format documents using my style sheet
4. Click **OK**.

For more information, see "Customizing Display of Fonts, Colors, and Styles" in Chapter 33, "Accessibility Features and Functionality."

Determining Your Previous Version of Internet Explorer

To determine your previous version of Internet Explorer after installing Internet Explorer 4, view the PreviousIESysFile value under the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\IE4\Setup

The following table lists the possible values for the PreviousIESysFile registry value and the version of Internet Explorer that corresponds to each:

Value	Version
4.70.0.1155	3.0
4.70.0.1158	3.0
4.70.0.1215	3.01
4.70.0.1300	3.02
4.71.<xxxx>	4.0

Note The Internet Explorer 4 Uninstall feature returns your computer to a pre-Internet Explorer 4 browser. As a result, the PreviousIESysFile value cannot be used to determine if you upgraded to Internet Explorer 4 over an earlier, beta version of Internet Explorer 4.

The PreviousIESysFile value is used by the Internet Explorer 4 Uninstall program to determine which components should be removed when Internet Explorer 4 is removed. The registry contains a RequiredIESysFile value for each component. If the RequiredIESysFile value for a particular component is equal to or less than the PreviousIESysFile value, the component is not removed when you remove Internet Explorer 4. If the RequiredIESysFile value for a component is greater than the PreviousIESysFile value, the component is removed when you remove Internet Explorer 4.

Slow Connections and Inability to View Non-Microsoft Sites

When you use Internet Explorer version 3 or 4 with a proxy server and Novell NetWare 32-bit client software to browse the Internet, you may experience the following:

- Slow connections.
- Inconsistent downloads.
- An inability to view non-Microsoft sites.

To resolve these problems, verify that you are using the Novell NetWare 32-bit client and that you are connecting to the Internet using a proxy server.

▶ **To verify that you are using the Novell client**

1. On the **Start** menu, point to **Settings**, then click **Control Panel**.
2. Double-click the **Network** icon, and click the **Configuration** tab.
3. Verify that **Novell 32** appears in the box labeled **The following network components are installed.**

▶ **To verify that you are connecting using a proxy server**

1. On the **View** menu, click **Internet Options**, then click the **Connection** tab.
2. Verify that the **Access the Internet Using a Proxy Server** check box is checked and that the **Address** box contains entries. This indicates that Internet Explorer is set up to connect to the Internet through a proxy server.

▶ **To add DontUseDNSLoadBalancing to the Internet settings registry key**

If you are using the Novell NetWare 32-bit client and are connecting to the Internet using a proxy server, use the following information to add to the registry key:

1. Create a new binary value named:

   DontUseDNSLoadBalancing under the following registry key:

   HKEY_CURRENT_USER\Software\Microsoft\Windows\ CurrentVersion\Internet Settings
2. Set the value to:

   01 00 00 00
3. Restart your computer.

Note The Novell NetWare 32-bit client is not manufactured by Microsoft. Microsoft makes no warranty, implied or otherwise, regarding this product's performance or reliability.

For more information about configuring proxy server settings, see Chapter 8, "Configuring Connection Settings."

Restoring Functionality to the Downloaded Program Files Folder

The Download Program Files folder contains functionality that enables you to easily uninstall ActiveX controls. When this folder is deleted, a new Downloaded Program Files folder is created the next time Internet Explorer downloads new program files. However, the newly created folder does not contain the functionality to easily uninstall ActiveX controls. This section describes how to restore this functionality to the new folder.

▶ **To restore the ability to easily uninstall ActiveX controls**

1. From the **Start** menu, point to **Programs**, then click **MS-DOS Command Prompt**.
2. Type **cd**, and then press ENTER.
3. Type the following command, and then press ENTER:

   cd *windows*\system
   where ***windows*** is the folder in which Windows is installed.
4. Type the following command, and then press ENTER:

   regsvr32 /i occache.dll
5. Type **exit**, and then press ENTER.
6. From the **Start** menu, select **Shut Down**, click **Restart**, and then **OK**.

Controls that were deleted with the original folder are listed with a status of Damaged. These controls should be removed because the associated files have already been deleted.

Changing the Download Location for ActiveX Files

ActiveX .ocx and .inf files are installed in the Windows\Downloaded Program Files folder by default.

▶ **To change the location of ActiveX files**

1. Use Registry Editor to change the ActiveXCache value to the location you want in the following registry key:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings

2. Use Registry Editor to change the 0 value to the location you want in the following registry key:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ActiveXCache

Note The values you enter in steps 1 and 2 must match.

The new value can be a folder on a local hard disk, a Universal Naming Convention (UNC) name, or a mapped network drive. Storing ActiveX files on a network server may reduce Internet Explorer performance, because the ActiveX files must be delivered over the network.

APPENDIX D

Troubleshooting the Active Desktop

This appendix reviews some of the issues related to the Microsoft® Internet Explorer Active Desktop™ that may require troubleshooting and explains procedures for solving problems that may occur in this area. Topics include:

- Pointing to desktop icons causes text to disappear
- Changing to single-click mode using the registry
- Images copied to the desktop are saved as Active Desktop items
- **Find on the Internet** command appears twice on the Start menu
- Active Desktop items stop working when offline
- System properties do not show that Microsoft Plus! is installed
- Internet Explorer cannot find the Active Desktop
- Do not use Web pages with frames as your desktop wallpaper

To learn more about the Active Desktop, see Part 3.

Important This section contains information about editing the registry. Before you edit the registry, you should first make a backup copy of the registry files (System.dat and User.dat). Both are hidden files in the Windows folder.

Warning Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that problems resulting from the incorrect editing of the registry can be solved. Edit the registry at your own risk.

Pointing to Desktop Icons Causes Text to Disappear

If your computer is running Internet Explorer 4 and the Windows Desktop Update and you point to an icon on the desktop, the text under the icon may disappear. This behavior occurs when selected items and desktop are configured to use the same color in the **Display Properties** dialog box. To resolve this problem, either configure Windows® 95 so that selected items and the desktop are not configured to use the same color, or configure Windows 95 so that you must double-click to open an object.

▶ **To configure Windows 95 so that selected items and the desktop are not configured to use the same color**

1. From the **Start** menu, point to **Settings**, then click **Control Panel**.
2. Double-click the **Display** icon.
3. Click the **Appearance** tab, click **Selected Items** or **Desktop** in the list of items, then select a different color.
4. Click **OK**.

▶ **To configure Windows 95 so that you must double-click to open an object**

1. Double click the **My Computer** icon on the desktop, then click **Options** on the **View** menu.
2. Click the **View** tab, then click **Double-Click To Open Any Item**.
3. Click **OK**.

Changing to Single-Click Mode Using the Registry

If the Windows Desktop Update is installed, administrators can configure Internet Explorer so that instead of double-clicking to open an item, users single click, and rather than using a single-click to select an item, users point to select. Users can select this Web-style option for themselves (by selecting **Folders and Icons** from the **Settings** menu on the **Start** menu), but administrators may find it helpful to implement this option without user intervention. To do this, you must create a registry file.

▶ **TO create the .reg file**

1. Using any text editor, such as Notepad, create a file with the following content:

   regedit4[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer]"IconUnderline"=hex(0):03,00,00,00

[HKEY_USERS\.Default\Software\Microsoft\Windows\CurrentVersion\Explorer]"ShellState"=hex:1c,00,00,00,41,08,00,00,00,00,00,00,00,00,00,00,00,00,00,00,\00,00,00,00,09,00,00,00"IconUnderline"=hex(0):03,00,00,00

2. Save this file as Single.reg and place it on a server.

▶ **To run the .reg file**

- Add the following command to users' login scripts:

  regedit *path to file*\single.reg –s

  The **-s** switch makes the command run silently, so that no user intervention is required. After the command is carried out, restarting the computer or refreshing the screen activates the option to single-click to open an item (point to select).

Images Copied to the Desktop Are Saved as Active Desktop Items

When have the Windows Desktop Update installed and attempt to save an image file to the desktop by dragging the image from a Web page to the desktop, you may receive the following prompt:

Security Alert
Do you want to add a desktop item to your Active Desktop?

When you click **Yes**, the Subscription Wizard starts to set up a subscription for updating the image. When the wizard is finished, the image appears as an Active Desktop item, rather than as a file icon. This only occurs when you drag Web-based content to the desktop. You can drag items from My Computer or Windows Explorer to the desktop and the file is copied normally.

To work around the Active Desktop process, you can manually save the image.

▶ **To manually save the image**

1. Right-click the image to be copied, and then, on the pop-up menu, click **Save Picture As**.
2. Double-click your Desktop folder, then click **Save**. (By default, the Desktop folder is C:\Windows\Desktop in Windows 95 and C:\Winnt\Profiles*name*\Desktop in Windows NT®.)

You can also avoid this situation by uninstalling the Windows Desktop Update component. For the procedure to uninstall the Windows Desktop Update, see Chapter 6, "Adding and Removing Components after Setup."

"Find on the Internet" Command Appears Twice on the Start Menu

When you click **Start** and then point to **Find**, you may see two **On The Internet** commands, and one of the commands may not work correctly. This can occur when both Internet Explorer 4 and FindX PowerToy are installed on your computer.

Windows PowerToys are a suite of tools available for free download from the Microsoft Web site. Microsoft Technical Support does not support the installation or usage of PowerToys or any of their components. FindX is a Windows 95 PowerToy that you can use to add your own custom commands to the **Find** menu, including a built-in **On The Internet** command.

To resolve this issue, remove FindX PowerToy from your system.

▶ **To remove the FindX PowerToy**

1. Click **Start**, point to **Settings**, then click **Control Panel**.
2. Double-click the **Add/Remove Programs** icon.
3. On the **Install/Uninstall** tab, click **Find... Extensions** in the list of installed programs.
4. Click **Add/Remove** to remove FindX.

Active Desktop Items Stop Working When Offline

Active Desktop items that host Java programs may stop working when Internet Explorer 4 is offline. This can occur if the Java program is removed from the Temporary Internet Files folder. Also, if the Java program is not packaged into a .cab, .zip, or .jar file, it may not get cached at all.

Active Desktop items are retrieved from the cache when Internet Explorer 4 is offline. If the cache reaches its maximum size, Java programs may be automatically removed from the cache to make room for current downloads. If an Active Desktop item hosts a Java program that has been removed from the cache and Internet Explorer 4 is offline, the Active Desktop item stops working.

▶ **To activate Active Desktop items for offline use**

Empty the Temporary Internet Files folder or increase the amount of hard disk space it uses, by using the appropriate method:

- Empty the Temporary Internet Files folder by following these steps:
  1. In Internet Explorer, on the **View** menu, click **Internet Options**.

2. On the **General** tab, in the **Temporary Internet Files** box, click **Delete Files**.
3. Click **OK** when you are prompted to delete the files, and then click **OK** again.
4. Connect to the Internet.
5. Right-click an empty area on your desktop, point to **Active Desktop**, and then click **Update Now** to update the Active Desktop items.

- Increase the amount of hard disk space the Temporary Internet Files folder uses by following these steps:
  1. In Internet Explorer, on the **View** menu, click **Internet Options**.
  2. On the **General** tab, in the **Temporary Internet Files box,** click **Settings**.
  3. Move the **Amount of disk space to use** slider to the right.
  4. Click **OK**, then click **OK** again.
  5. Connect to the Internet.
  6. Right-click an empty area on the desktop, point to **Active Desktop**, then click **Update Now** to update the Active Desktop items.

System Properties Do Not Show That Microsoft Plus! Is Installed

If you install Microsoft Plus! and then install Internet Explorer 4, the **System Properties** dialog box may indicate that Microsoft Plus! isn't installed. The information line no longer shows:

Microsoft Plus! for Windows 95

Instead, this line reads:

IE 4.0 ***7-digit build number***

The opposite behavior may also occur. If you install Microsoft Plus! after installing Internet Explorer 4, the **System Properties** dialog box line no longer shows:

IE 4.0 ***7-digit build number***

Instead, this line reads:

Microsoft Plus! for Windows 95

This behavior is solely cosmetic; it does not affect your ability to run installed Microsoft Plus! or Internet Explorer.

Internet Explorer Cannot Find the Active Desktop

When you make changes to the Active Desktop, the following error message may occur:

Internet Explorer cannot find the Active Desktop HTML file. This file is needed for your Active Desktop. Click OK to turn off Active Desktop.

This occurs when the Windows\Web folder has been moved or renamed, because Internet Explorer needs to write to certain files stored within that folder.

To solve the problem, use Windows Explorer to create a new Windows\Web folder, or remove and reinstall Internet Explorer to re-create the folder. For the procedures to uninstall and reinstall Internet Explorer, see Chapter 7, "Uninstalling Internet Explorer" and Chapter 6, "Adding and Removing Components After Setup," respectively. (The process for reinstalling Internet Explorer is the same as the process for reinstalling its components.)

Do Not Use Web Pages with Frames as Your Desktop Wallpaper

If you use a Web page as your desktop wallpaper and it contains frames, some desktop items may stop working. For example, you may find that the Channel bar is removed from the desktop.

The Active Desktop cannot display desktop wallpaper with frames. Such pages are actually several separate pages tied together with links. If a frame set is copied to a computer, it is not usable as wallpaper, even if all related pages are copied.

APPENDIX E

Troubleshooting Webcasting

This appendix reviews some of the issues related to Webcasting in the Microsoft® Internet Explorer 4 that may require troubleshooting and explains procedures for solving problems with Web-site and channel subscriptions. Topics include:

- Unattended dial-up does not work without user intervention
- E-mail notification is not sent for updated web sites
- Red gleams do not appear on channel bar when site content updates
- Subscription images are downloaded even if images are disabled

Unattended Dial-Up Does Not Work Without User Intervention

If you configure an unattended dial-up connection in Internet Explorer 4 or Outlook™ Express, you may receive the following message when the modem attempts to connect:

You are currently using NetWare servers, which will be inaccessible if you establish this connection.

Click OK to continue dialing. Click Cancel if you do not want to dial at this time.

The unattended dial-up connection does not continue until you click **OK**. This can occur if the Microsoft Client for NetWare Networks™ is installed on your computer and the Inter-network Packet Exchange/Sequenced Packet Exchange (IPX/SPX)-compatible protocol is bound to the Dial-Up Adapter. To resolve this problem, disable the IPX/SPX protocol for the Dial-Up Adapter.

▶ **To disable the IPX/SPX protocol in the Dial-Up Adapter**

1. From the **Start** menu, point to **Programs**, point to **Accessories**, and then click **Dial-Up Networking**.
2. Right-click the connection you are using for the unattended dial-up, and then click **Properties**.
3. Click **Server Type**, and then click the **IPX/SPX Compatible** check box to clear it.
4. Click **OK**, and then click **OK** again.

You can use unattended dial-up in the following situations:

- You configure Internet Explorer to perform an unattended dial-up connection when it updates Web-site and channel subscriptions.
- You configure Outlook Express to automatically dial when it checks for new messages.

E-Mail Notification Is Not Sent for Updated Web Sites

Despite the fact that <USAGE VALUE="Email" /> has been specified for a parent ITEM element in a CDF file, the subscribed user may not receive e-mail notification when a content update occurs. This problem may occur for one of two reasons: when the user subscribed to the channel, he or she did not specifically ask to receive e-mail notifications for content update, or the SMTP server was not specified correctly.

For channel e-mail notifications to be sent, the following three conditions must be met:

1. <USAGE VALUE="Email" /> must be specified in the CDF file, as in this example:

```
<CHANNEL HREF="http://example.microsoft.com">
    <ITEM HREF="http://example.microsoft.com/emailthis.htm">
    <USAGE VALUE="Email" />
    </ITEM>
    </CHANNEL>
```

2. When subscribing to the channel, the user must select one of the two **Yes** options on the **Add Favorite** dialog box, then click the **Customize** button and select **Yes, send an e-mail notification to the following address** when asked if he or she wants to be notified in an e-mail message when the page has changed.
3. When prompted for an e-mail address, the user must click the **Change Address** button and specify the correct SMTP server name. If you do not know the correct server name, ask your Internet service provider (ISP) what server name to specify.

If all three conditions above are met, an e-mail notification is sent to the subscribed user in this format:

```
Subject:  Internet Explorer Notice: <web site title>
Message:  <site URL> Your subscription to <web site title> has been
updated. To view the subscription offline, click here: <site URL>
This message was sent by the Internet Explorer 4.0 Information Delivery
Agent.
```

If your e-mail client is HTML-aware, then the e-mail received is the actual Web page specified in the <ITEM> tag in the CDF file.

Red Gleams Do Not Appear on Channel Bar When Site Content Updates

When you subscribe to a channel Web site, a gleam may not appear on that channel's icon on the Channel bar, even though the contents of the subscribed Web site have changed.

When Internet Explorer checks a subscribed channel for updated information, it only checks the actual subscribed CDF file (that is, the specific type of information requested by the user during the subscription setup). If the subscribed file changes, a red gleam appears on that channel's icon. If the subscribed file does not change, no gleam appears on the subscription's icon. This is true whether or not any other content in the subscribed channel has changed.

Subscription Images Are Downloaded Even If Images Are Disabled

When you disable image downloading in an Active Desktop™ item's subscription properties, images may still be downloaded and displayed when the desktop item's subscription is updated. To prevent images from being downloaded when an Active Desktop item's subscription is updated, you must disable image downloading in both the subscription and in Internet Explorer.

▶ **To disable image downloading for desktop items**

1. In Internet Explorer, on the **Favorites** menu, click **Manage Subscriptions**.
2. In the **Subscriptions** dialog box, right-click the subscription for which you want to disable image downloading, and then click **Properties**.
3. Click the **Receiving** tab, then click **Advanced**.
4. In the **Items To Download** box, click the **Images** check box to clear it, then click **OK**, and click **OK** again.
5. On the **File** menu, click **Close** to close the Subscriptions window.
6. In Internet Explorer, on the **View** menu, click **Internet Options**, and then click the **Advanced** tab.
7. Under **Multimedia**, click the **Show Pictures** check box to clear it, and then click **OK**.

If image downloading is disabled in Internet Explorer 4 only, images are still downloaded when the desktop item's subscription is updated, but these images are not displayed in the desktop item.

APPENDIX F

Troubleshooting Outlook Express

This appendix discusses some of the issues related to Microsoft Outlook™ Express that may require troubleshooting and explains procedures for solving problems that may occur. Topics include:

- Problems changing the default mail client for Internet Explorer
- Cannot import address book in Outlook Express
- Preview pane does not display news messages when enabled
- Error message: **The command failed to execute.**
- Internet mail and news files renamed by Outlook Express

For more information about Outlook Express, see Chapter 18.

Problems Changing the Default Mail Client for Internet Explorer

▶ **To change the default mail client in Internet Explorer**

1. In Internet Explorer, on the **View** menu, click **Internet Options**.
2. Click the **Programs** tab.
3. In the **Mail** drop-down list and in the **News** drop-down list, click the programs you want.
4. Click **OK**.

In Internet Explorer, these changes modify the URL:MailToProtocol registered file type that is listed when you follow these steps:

1. In My Computer, on the **View** menu, click **Folder Options**, and then click **File Types**.
2. Click **URL:MailToProtocol**, click **Edit**, click **Open** in the **Actions** box, and then click **Edit**.

   The command line that controls the program that is used to open a MailTo Uniform Resource Locator (URL) appears in the **Application used to perform action** box.

Some programs may modify this setting without updating the list of programs available in Internet Explorer. For example, the Eudora Internet mail client changes the URL:MailToProtcol registered file type to the following:

C:\<EudoraFolder>\Eudora.exe /m

You can also change the default program back to **Internet Mail** or **Windows Messaging** in the **Mail** box on the **Programs** tab.

Selecting **Internet Mail** in the **Mail** box changes the URL:MailToProtcol registered file type to:

rundll32.exe C:\WINDOWS\SYSTEM\mailnews.dll,Mail_RunDLL

Selecting **Windows Messaging** in the **Mail** box changes the registered file type to:

rundll32.exe url.dll,MailToProtocolHandler %l

▶ **To specify Microsoft Outlook 97 as the program you want to open MailTo URL addresses**

1. In My Computer, on the **View** menu, click **Folder Options**, and then click **File Types**.
2. Click **URL:MailToProtocol**, click **Edit**, click **Open** in the **Actions** box, and then click **Edit**. Click the **Application used to perform action** box and press **DELETE** to delete the data in the box.
3. Type the following (including quotation marks) for the **Application used to perform action** box for the **Open** command:

   "C:\Program Files\Microsoft Office\ Office\Outlook.exe" -c IPM.Note /m "%1"
4. To save the changes, click **OK** until you return to My Computer.

▶ **To specify Microsoft Outlook Express as the program you want to open MailTo URL addresses**

1. In My Computer, click **Folder Options** on the **View** menu, and then click **File Types**.
2. Click **URL:MailToProtocol**, click **Edit**, click **Open** in the **Actions** box, and then click **Edit**. Click the **Application used to perform action** box, and press **DELETE** to delete the data in the box.
3. Type the following (including quotation marks) for the **Application used to perform action** box for the **Open** command:

   "C:\Program Files\Outlook Express\Msimn.exe" /mailurl:%1"
4. To save the changes, click **OK** until you return to My Computer.

Specifying Older Mail Programs

The list of mail programs that you can choose under the Internet Explorer options is made up of registry keys, which outline the behavior of the program you want to use. Modifications that need to be made to the registry are detailed and very specific. Most programs either self-register upon usage or have an option to become the default program. If these options are not available, please contact the manufacturer about how to make its program the default mail client.

Cannot Import Address Book in Outlook Express

When you attempt to import an address book in Outlook Express version 4, the address book may not be imported and you may not see an error message. This occurs when the Wabmig.exe file is missing or damaged.

If the Wabmig.exe file is damaged, rename the file, and then reinstall Outlook Express.

▶ **To rename the Wabmig.exe file**

1. From the **Start** menu, point to **Find**, and then click **Files Or Folders**.
2. In the **Named** box, type **Wabmig.exe**, and then click **Find Now**.
3. Right-click the file, and then click **Rename**.
4. Rename the file to Wabmig.*xxx*.
5. Reinstall Outlook Express.

Preview Pane Does Not Display News Messages When Enabled

While you are reading news messages in Outlook Express, you may receive the following message in the preview pane even though the preview pane is already enabled:

Press <Space> to display the selected message. You can also choose to automatically show messages in the preview pane from the Options command.

If you press SPACEBAR, the message reappears. If you double-click the news message to open it, you receive the following error message:

There was an error opening the message.

This occurs when there is not enough free space on your hard disk to open the news message. Increase the amount of free space on your hard disk by using one or more of the following methods:

- Remove any unnecessary files from the hard disk.
- Empty the Recycle Bin.
- Delete the Internet Explorer 4 Setup folder, or remove unnecessary files from the folder. Deleting this folder does not affect the performance of Internet Explorer, but it is important to note that without this folder, you will not be able to reinstall Internet Explorer or its components from the hard disk; you will have to download another copy from the Microsoft Web site.

Warning The Setup folder contains important backup files that are necessary for uninstalling Internet Explorer. IE4bak.dat and IE4bak.ini and, if Windows Desktop Update is installed, Integrated Browser.dat, and Integrated Browser.ini. are critical files. It is recommended that you not delete these files. (For more information, see "Deleting Uninstall Files" in Chapter 7.) If you need to make more disk space available, it is recommended that you leave these files and delete other files in the folder.

Error Message: The Command Failed to Execute

When you attempt to save a mail attachment to your hard disk in Outlook Express, you may receive the following error message:

The command failed to execute.

This occurs when there is not enough free disk space on your hard disk to save the attachment.

Increase the amount of free space on your hard disk by using one or more of the following methods:

- Remove any unnecessary files from the hard disk.
- Empty the Recycle Bin.
- Delete the Internet Explorer Setup folder. (Important: Note the warnings and information about removing the Setup folder, above.)

After you free some hard disk space, try to save the attachment again.

Internet Mail and News Files Renamed by Outlook Express

When you install Internet Explorer 4, the Windows®Address Book files used by Internet Mail and News 1 for Windows® 95 and Windows NT® 4.0 are renamed. This is because Outlook Express is installed as an upgrade to Internet Mail and News.

The following files in the Windows\System or Winnt\System32 folder are renamed:

File Name	Renamed To
Wab32.dll	Wab32.ie3
Wabfind.dll	Wabfind.ie3
Wabimp.dll	Wabimp.ie3

The following files in the Windows folder are renamed:

File name	Renamed to
Wab.exe	Wab.ie3
Wabmig.exe	Wabmig.ie3
***Username*.wab**	*path**Username*.wab.ie3

where *path* is one of the following paths:

- Windows\Profiles*Username*\Application Data\Microsoft\Address Book
- Program Files\Internet Explorer\Outlook Express*Username*\Address Book
- Program Files\Common Files\Microsoft Shared\Address Book

When the *Username*.wab file is moved and renamed, a new copy of the *Username*.wab file is used by Outlook Express. The Windows Address Book files are restored, however, if you uninstall Internet Explorer 4.

APPENDIX G

Troubleshooting HTML Authoring

This appendix reviews some of the issues related to Microsoft® Internet Explorer 4 HTML authoring that may require troubleshooting and explains procedures for resolving these authoring problems. Topics include:

- Text doesn't wrap in text boxes
- Background images are not displayed
- Internet Explorer browser is not automatically redirected
- Frames not displayed in web pages
- Permission denied when scripting across frames

For more information about HTML authoring for Internet Explorer 4, see Part 6.

Text Doesn't Wrap in Text Boxes

When you enter text in a text box created using the <TEXTAREA> tag on a Hypertext Markup Language (HTML) page, the text may not wrap correctly. In this case, the text continues to flow to the right side of the text box without breaking or wrapping. This is because the HTML page does not contain the parameters that activate text wrapping in a text box.

▶ **To wrap text in a text box, use one of the following methods:**

- Use the WRAP attribute of the <TEXTAREA> tag with either the Physical or Virtual value to enable word wrapping.

  The non-wrapping <TEXTAREA> tag might look like:

  ```
  <TEXTAREA NAME="Name" ROW99S=6 COL99S=40>
  </TEXTAREA>
  ```

- To enable wrapping, insert WRAP=Physical, as in the following example:

  ```
  <TEXTAREA NAME="Name" ROW99S=6 COL99S=40 WRAP=Physical>
  </TEXTAREA>
  ```

When you are typing in the text box, manually insert line breaks by pressing ENTER to wrap the text.

Background Images Are Not Displayed

Pages created with the Data Form Wizard by Visual InterDev™ may not display background images in Internet Explorer 4. If this occurs, it is likely due to the fact that Internet Explorer 4 adheres more closely to the HTML 3.2 specification than does Internet Explorer 3. In the Cascading Style Sheet (CSS) spec, CSS tags take precedence over HTML tags. Pages created using the Data Form Wizard reference a CSS; the CSS has a tag for the background image of Transparent, thus overriding any value in the body tag of the ASP file.

▶ **To display background images**

- Delete the "background: transparent" line from the BODY property of the CSS.

Internet Explorer Browser Is Not Automatically Redirected

When you load a Web page that contains the <meta http-equiv="refresh"...> HTML tag, the browser may not be automatically redirected to another Web page. This may occur for one of the following reasons:

- The author of the page did not place the <meta http-equiv="refresh"...> tag in the <HEAD> section of the HTML source code.
- The syntax of the <meta http-equiv="refresh"...> HTML tag is incorrect.

To resolve this issue, update the Web page using the appropriate method:

- If the <META> tag is not located in the <HEAD> section

  Modify the HTML source code to place the <META> tag in the <HEAD> section of the Web page. This may require adding the <HEAD> and </HEAD> tags to the Web page.

- If the syntax of the <META> tag is incorrect

  Modify the HTML source code to correct the syntax of the <META> tag. For example, a <META> tag might look like this:

  ```
  <meta http-equiv="refresh" content="n;url=http://www.domain.com/
      pagename.htm">
  ```

  where *n* is the number of seconds the browser program pauses before loading the new Web page.

For information about the HTML 3.2 Specification Reference, see **http://www.w3.org/TR/REC-html32.html**.

Frames Not Displayed in Web Pages

When you're using Internet Explorer 4 to view a Web page, a blank page may display instead of a defined set of frames. If you right-click an empty area of the Web page and then click **View Source**, or right-click an empty area of the Web page, click **Properties**, and then click **Analyze**, the following message may display:

This document might not display properly because there is a <FRAMESET> within the <BODY> of the document.

This behavior is by design and occurs when the Web author puts the <FRAMESET> tag after the <BODY> tag in the main or "framing" HTML document. All <FRAMESET> tags and underlying instructions should precede any <BODY> tags.

▶ **To resolve this problem**

1. Remove the <BODY> tag.
2. Remove any additional HTML code between the <HEAD> of the document and the <FRAMESET>.

The framing HTML document defines the frame regions that display in the browser and the documents or objects that initially appear in the frames. For information about the HTML syntax for frames, see **http://www.w3.org/pub/WWW/TR/WD-frames-970331.html**.

Permission Denied When Scripting Across Frames

Script code that attempts to access a script or an object in a different frame may result in the following script error message:

Permission denied: 'Parent.RemoteFrame.RemoteObject'

Internet Explorer 4 implements cross-frame security. A script or an object in one frame is not allowed to access scripts or objects in another frame when the documents referenced by the frames' SRC attribute specify Web servers in different second-level domains. This corresponds to the *domain-name.xxx* portion of the full server-name syntax *server.domain-name.xxx*.

The Internet Explorer Dynamic HTML object model allows a certain subset of safe actions to be scripted. For example, the *window.location* property of a remote server's frame can be set to allow navigation, but it cannot be read to prevent one frame from snooping on the contents of another frame.

For example, it is valid for a document retrieved from **http://test.microsoft.com/** to manipulate another document retrieved from **http://test.microsoft.com/**. It is not valid for a document retrieved from **http://*server1.some-domain-name.org/*** to manipulate a document retrieved from **http://*server2/*** or **http://*server3*.microsoft.com/**.

The intention of cross-frame security is to prevent a Web-page author from misusing or snooping on the trusted objects authored by another Web page author. Only pages hosted in the same domain can be trusted to safely script the contents of a particular page. Cross-frame security should also prevent unwanted communication between documents on opposite sides of a corporate firewall. Please refer to the *Microsoft Internet Client Software Development Kit (SDK)* for more information.

To allow two documents hosted on the same second-level domain to interact, both documents must set the *document.domain* property to their shared second-level domain. For example, one document on **http://*example.microsoft.com/*** could script and access another document on **http://*test.microsoft.com/*** if both documents used the following line of script code:

```
<SCRIPT LANGUAGE="VBScript">
document.domain = "microsoft.com"
</SCRIPT>
```

Given the following FRAMESET:

```
<FRAMESET COLS="50%, *" FRAMEBORDER=1>
<FRAME SRC="http://server1/server1.html" ID="Server1Frame">
<FRAME SRC="http://server2/server2.html" ID="Server2Frame">
</FRAMESET>
```

Script in the "Server1Frame" frame is not permitted to access script or objects in the "Server2Frame" frame, and vice versa.

The following example script code in server1.html causes the "Permission Denied" error, given that **RemoteTextBox** is an object created on the server2.html document:

```
<!-- From server1.html -->
<SCRIPT LANGUAGE="VBScript">
Sub CommandButtonLocal_Click()
Parent.Server2Frame.RemoteTextBox.Text = "Changed Text"
'Server2Frame has SRC on different server
end sub
</SCRIPT>
```

APPENDIX H

Frequently Asked Questions About Cabinet Files in Java

This appendix covers some of the Frequently Asked Questions (FAQs) about cabinet (.cab) files. For other Java-related FAQs visit: **http://www.microsoft.com/support/java/content/faq/default.htm**.

Where do I get the Code Sign Kit?

You can find the Code Sign Kit on the Visual J++™ CD-ROM, *Microsoft® ActiveX® Software Development Kit (SDK)*, or "Java Signing Tools" in the *Microsoft SDK for Java 2.0 Beta 2* or newer. The *Microsoft ActiveX SDK* is available at **http://www.microsoft.com/Intdev/sdk/**. The *Microsoft SDK for Java 2.0 Beta 2* is available at **http://www.microsoft.com/java/sdk/**.

Where can I get the *CAB Developers Kit* or the *CAB Resource Kit,* and what are they used for?

The *CAB Developers Kit* has been incorporated into the *Microsoft SDK for Java*, which is available at **http://www.microsoft.com/java/sdk/**. It's also available stand-alone at **http://www.microsoft.com/workshop/prog/cab/default.htm**. It will give you all of the tools you need to build cabinet files. The latest version includes cabarc.exe, a new tool that makes it easier to create cabinet files directly from the command line.

The *CAB Resource Kit* provides the information necessary to help the tool development community understand and work with cabinet files. It includes the compression and decompression application programming interfaces (APIs), documentation on their interfaces, and sample applications using these APIs. Soon, there will be more information on the cabinet file format. The updates provided on January 13, 1997, featured multithread and multicontext support and allow use in MFC-based applications.

When programmatically creating a .cab file from a Java application, can I reserve space in the .cab for signing?

The Java CAB API currently does not support the creation of reserved areas. The command-line tools, Cabarc.exe and Diamond.exe, support this functionality. The latest version of the Signcode.exe utility that is available in the *Microsoft SDK for Java 2.0 Beta 2* and newer does not require space to be reserved in the .cab file for a digital signature. It will automatically create space in the .cab when it is signed.

Can I sign a Java class file for use with Internet Explorer?

Although it is possible to digitally sign a Java class file and verify the signature using the trust check utility, Internet Explorer does not recognize the class as signed and does not present a certificate to the user at runtime. Furthermore, the class is not considered trusted by the Microsoft VM for Java. Presently, you need to place the classes within a .cab file, which can then be signed.

Will the Microsoft Virtual Machine for Java support the .jar file format?

Jar support is the same as .zip. .jar = .zip + manifest. So Microsoft will support uncompressed and compressed .jar files, but not signed .jar files. If you need Java security (beyond sandbox) in Internet Explorer 4, you need to use a signed .cab file. This applies to all fine-grained Java security (including running in a sandbox on the local machine using the Package Manager).

Can my applet that is inside a .cab file use class files from outside the .cab that are not installed in the local machine's CLASSPATH?

Class files from a Web server cannot be used by classes in a .cab file with the Microsoft VM for Java, build 1517 and earlier. With build 2057 of the VM, from the *Microsoft SDK for Java 2.0 Preview*, you can use classes from outside of the .cab file.

When I run signcode.exe on my .cab file, I get the following error:

Unable to sign the program <.cab file>. (80004005)

You did not reserve space in your .cab file. Recreate the .cab file using the **-s** 6144 option to Cabarc.exe. This space must be reserved in the .cab file to allow room for the digital signature. Note: it is not necessary to use the **-s** switch with the signing tools included with the *Microsoft SDK for Java 2.0 Beta 2* or newer. The Signcode.exe utility will now create the necessary space for the certificate at the time the .cab file is signed.

Unable to sign the program <.cab file>. (80030070)

You did not reserve enough space in your .cab file. Recreate the .cab file using the **-s** 6144 option to Cabarc.exe. Note: it is not necessary to use the **-s** switch with the signing tools included with the *Microsoft SDK for Java 2.0 Beta 2* or newer. The Signcode.exe utility will now create the necessary space for the certificate at the time the .cab file is signed.

Unable to sign the program <.cab file>. (80070005)

Your .cab file is marked read-only.

Unable to sign the program <.cab file>. (80070057)

Your .cab file is corrupt.

When do I use the -s option for Cabarc.exe?

The **-s** 6144 option reserves unnecessary space in most situations. With the 'test' certificate, you can typically get by with 1K of reserved space in the .cab. A good estimate of the space required is slightly larger than the size of the .spc file with which you are signing. Also note, it is possible that the certificate will require more than 6144 bytes. Note: it is not necessary to use the **-s** switch with the signing tools included with the *Microsoft SDK for Java 2.0 Beta 2* or newer. The Signcode.exe utility will now create the necessary space for the certificate at the time the .cab file is signed.

When do I use the -i option for Cabarc.exe?

The **-i** switch is used to insert a version number, SET ID, into a .cab file. The version number will be displayed when viewing a .cab file with the following command-line statement: **cabarc L <.cab file>.** Diamond.exe uses the ID number when spanning multiple .cab files.

How do I install a Java package on the user's machine?

You can use a setup information (.inf) file in a .cab to install Java libraries and packages on the local machine. The .inf file defines which files to extract from the .cab and where to place them on the user's system. There is an example .inf file called Master.inf included in the *Microsoft SDK for Java*. Place all the Java libraries and packages in a .cab file. In a second signed .cab file, place the unsigned .cab file and the .inf file. Reference the signed .cab file with an <OBJECT> tag in your HTML page.

For distributing trusted applets on my intranet, is there a more elegant solution than using a test certificate?

Currently, the only solution is to relax the security in Internet Explorer by placing the classes on the user's machine in the CLASSPATH or distributing the files in a signed .cab file. You can obtain a certificate for use within the company or use the test certificate and have the users run the Wvtston.reg file to enable test certificates on their machines.

Can I include .gif, .jpg, or .au files used by my applet in a .cab file?

Yes, the .cab file serves as a single, compressed repository for all .class, audio, and image files required by the applet. When creating the .cab file, be sure to use the **-r** and **-p** options to Cabarc.exe to recurse and preserve directory structure if any of the files in the .cab are in subdirectories. The **cabarc.exe -l** command can be used to confirm the directory structure was preserved.

Image and audio clips stored in the .cab can be retrieved by the applet code via the java.lang.applet.getImage and java.lang.applet.getAudioClip methods. Note that in order for Internet Explorer to find an image file or audio clip from within the .cab file, the URLs passed to these methods must be based upon the applet's codebase. For example, if the following code is found within an applet loaded from a .cab file, the image file picture1.gif and the audio clip sound1.au will be loaded from the .cab file (assuming that they are in the .cab). If an image or audio clip file is not within the .cab file, Internet Explorer will look for them on the server.

```
Image img = getImage(getCodeBase(),"picture1.gif");
AudioClip clip = getAudioClip(getCodeBase(),"sound1.au");
```

Why doesn't Internet Explorer display the certificate from a signed .cab file on some machines?

The two most common reasons for this behavior are the following:

If the .cab file was signed using a test certificate, you must enable test certificates for the local machine. Otherwise, the signature is not considered valid. You can do this by running the Wvtston.reg file included with the code signing kit.

You have accepted a software publisher as Always Trusted. To verify this, in Internet Explorer, on the **View** menu, click **Internet Options**. Click the **Content** tab, then click the **Publishers** button to ensure the publisher does not appear in the list box. If so, you can use this dialog box to remove it.

APPENDIX I

Internet Client SDK FAQs

This appendix covers some of the most Frequently Asked Questions (FAQs) about developing with the *Microsoft Internet Client Software Development Kit (SDK)* for Microsoft® Internet Explorer 4. These FAQs are also available on the Microsoft Web site at **http://www.microsoft.com/support/inetsdk/content/faq/**.

Setup

What are the system requirements for installing the SDK?

To download and use the *Microsoft Internet Client SDK*, you need the following:

- Internet Explorer 4.
- Windows NT® 4 or Windows® 95.

Active Channels

For more information about Active Channels™ and CDF files, see Part 4, "Information Delivery: Webcasting."

What MIME type do I specify in my dynamically generated CDF file?

A CDF file that is dynamically generated through Active Server Pages (ASP) should insert the following line at the top of the file (before any CDF lines):

```
<% Response.ContentType = "application/x-cdf" %>
```

This ensures that servers return the correct MIME (Multipurpose Internet Mail Extensions) /content type "application/x-cdf."

Problems with CDF files being displayed as HTML text inside the Internet Explorer browser, instead of invoking the Subscription Wizard, may be caused by the server returning the incorrect MIME type of "text/html" instead of the desired "application/x-cdf."

When dynamically generating a CDF file from an Active Server Pages (ASP) page, is the ASP file the one to which the user needs to subscribe?

Yes. Assuming that the correct CDF MIME type is specified in the ASP page, as illustrated in the FAQ above, double-clicking on a link to the ASP file should bring up the CDF Subscription Wizard appropriately.

I cannot use the ampersand character in my CDF file title. Do I have to specially treat certain characters when working with CDF files?

CDF supports encoding of ASCII characters with the format *&#nnn*. The ampersand character, therefore, could be encoded with its ASCII decimal value of 38 by using the string &#038.

To specify "Peaches & Cream," for example, your <TITLE> tag would look like this:

```
<TITLE>Peaches&#038;Cream</TITLE>
```

Is it necessary to specify the <!DOCTYPE> tag in my CDF file?

No. Internet Explorer 4 does not use the <!DOCTYPE> tag.

Is http://www.w3c.org/channel.dtd a valid URL for a <!DOCTYPE> tag?

No. This URL (Uniform Resource Locator) is only an example, does not actually exist, and is best not used in actual CDF files.

Is there a difference between the subscription cache and the regular cache that Internet Explorer maintains?

All subscription information goes into the same cache maintained by Internet Explorer. The subscription content in the cache, however, is specially marked so that it does not get deleted when a user clears the cache.

If the user is browsing a subscribed channel while connected to the Internet, is content pulled from the cache, or does Internet Explorer query the server again?

Internet Explorer looks at the Expires HTTP header returned by the server when the page was retrieved and checks to see if the cached page is still valid. If it is, content is pulled from the cache; otherwise, Internet Explorer queries the server again for the content. Note that with the latter, when Internet Explorer re-queries the server for content, in most cases, Internet Explorer will issue an HTTP GET request with an If_Modified_Since header, which helps reduce the server load.

Does the actual download of the HTML page occur upon subscription to the site or only during a subscription update?

Actual download occurs during subscription update. However, users can manually update a subscription any time they want.

From a CDF file, is there a way to specify items to be cached, without having the items appear in the Channel bar's item list? For example, can I specify a WAV file to be downloaded as part of the subscription update, so that it gets cached and is available when the user browses offline?

Yes, here's the correct way to do this:

```
<ITEM HREF="http://example.microsoft.com/sound.wav">
<USAGE VALUE="NONE"></USAGE>
</ITEM>
```

Note that in XML, an element that does not have child elements can be represented in a more compact format. For example, the above <USAGE> line could be written more compactly in the manner shown below. (Note the final / at the end of the tag.)

```
<USAGE VALUE="NONE" />
```

Also, when listing multiple items that are to be cached but not viewed in the Channel bar, instead of marking each one with a <USAGE VALUE="NONE" />, it is better to place them all in one subchannel that is marked with a usage tag, as illustrated in the example below:

```
<CHANNEL>
<USAGE VALUE="NONE" />
<ITEM HREF="http://example.microsoft.com/sound1.wav"/>
<ITEM HREF="http://example.microsoft.com/sound2.wav"/>
<ITEM HREF="http://example.microsoft.com/sound3.wav"/>
</CHANNEL>
```

Is it possible to specify multiple schedules for updates in one CDF file?

No. Only one schedule can be specified per CDF file in Internet Explorer. Also, a desktop item cannot be bundled with a channel in one CDF file. They have to be two separate CDF files to work correctly.

Is it possible to specify a global time for the <SCHEDULE> tag, so that my channel updates occur between certain times, regardless of the time zone?

Currently there is no way to specify local or global time in a CDF file. Information specified in the <EARLIESTTIME> and <LATESTTIME> tags is considered local and ignores any time zone information specified in the <STARTDATE> and <ENDDATE> tags.

How do I keep Internet Explorer from opening a new window when a user clicks on a link from a desktop item?

The way to do this is to specify a TARGET="_top" with the <A HREF> tag.

I haven't been able to get my desktop item to work unless I put it on a separate CDF file from the rest of my channel. Is this how it's designed to work?

Yes. Desktop items have to be in a separate CDF file from the rest of the channel.

HTML

For more information about HTML and Internet Explorer 4, see Part 6, "Authoring for Internet Explorer 4."

Why are my HTML pages with frames not showing up in Internet Explorer 4? They used to work fine in Internet Explorer 3.

Unlike Internet Explorer 3, Internet Explorer 4 does not support <FRAMESET> tags embedded within <BODY> tags. This was done in Internet Explorer 4 to ensure compatibility with Netscape Navigator. To work around the problem, move the <FRAMESET> outside the <BODY> tags.

In some cases, a <NOFRAMES> element is specified within the <FRAMESET> tags, as in the example below:

```
<BODY>
<FRAMESET>
<NOFRAMES>Sorry, your browser does not support frames! </NOFRAMES>
</FRAMESET>
</BODY>
```

Although Internet Explorer 4 supports frames, when the above HTML code is displayed in Internet Explorer, the content specified within the <NOFRAMES> tag is displayed. Moving the <FRAMESET> outside the <BODY> tags causes the page to display correctly.

Why doesn't Internet Explorer 4 close the <PLAINTEXT> container as Internet Explorer 3 did?

The <PLAINTEXT> tag is designed to render all of a Web page's subsequent text without parsing any tags, including its own </PLAINTEXT> tag. Internet Explorer 4 supports this tag as it is defined by the HTML DTD. This element is not recommended, as different browsers may not support it consistently. Instead, use the <PRE> tag, and display all reserved characters (such as brackets) with their corresponding HTML character entities.

Dynamic HTML

For more information about Dynamic HTML and Internet Explorer 4, see Part 6, "Authoring for Internet Explorer 4."

Is there a way to implement a custom ToolTip over anchors in Internet Explorer 4 (the same way you can use the ALT attribute in an <IMG> tag)?

By default, Internet Explorer renders the URL of the HREF attribute as a ToolTip, which may not always be the desired behavior. Yes, the way to do this is to specify the ToolTip in the TITLE attribute of the <A> tag, as in this example:

```
<a href="file.htm" TITLE="ToolTip goes here">some text</a>
```

How can I change the HTML or text associated with an element? I used to be able to do this using the rangeFromElement method, but now I keep getting the error "Object does not support this property or method." Have things changed?

Yes, the **rangeFromElement** method has been removed. Use innerHTML/outerHTML and innerText/outerText to manipulate text or HTML.

How do I determine the client width and height?

There are new properties on the body object, **clientWidth,** and **clientHeight,** which can be used for this purpose.

How do I change the current cursor being used as mouse pointer?

There is a cursor Cascading Style Sheet (CSS) attribute that can be used. Refer to the *Microsoft Internet Client SDK* documentation under the Dynamic HTML\HTML and CSS Reference section for more information.

Why do I get the error "Wrong number of arguments" in my event handlers?

Events do not have parameters (arguments). All information can be retrieved using the **window.event** object.

I'm finding that IFRAMES within a relatively positioned <DIV> tag causes Internet Explorer 4 to crash every time. This makes it difficult to relatively position IFRAMES. Is this a known problem, and is there a workaround?

Yes, the workaround is to put the positioning on the <IFRAME> directly.

WebBrowser Control

For more information about the WebBrowser Control, see Part 2, "Configuring the Browser."

In the Web browser documentation for developers of Visual Basic, the Navigate and Navigate2 methods look identical. Is there a difference?

The only difference is that the URL parameter is packaged as a VARIANT in Navigate2 instead of a BSTR. (You could verify this in the Web browser documentation for developers of C and Visual C++®.) Unlike a C++ application, a Visual Basic® application is not able to use the WebBrowser Control to navigate into special folders in the shell namespace like "My Computer." Currently, the shell does not expose an object that provides a PIDL, which a Visual Basic application can then use in a Navigate2 call.

I have an application that uses the WebBrowser Control. Is it possible to install just the WebBrowser Control without installing Internet Explorer 4?

No, there is no way to do this. The minimal installation will install the browser. Also, note that Internet Explorer 3 and 4 cannot coexist on the same machine. More information on redistributing Internet Explorer can be found on the IEAK page at **http://www.microsoft.com/ie/ieak/**.

Component Packaging

What version of the MFC .dll files will come with Internet Explorer 4? I'd like to know so I don't have to worry about packaging the MFC .dll files with my ActiveX® control.

Any component should be careful not to rely on the presence of any MFC .dll files with the currently installed browser, because Internet Explorer 4 and future versions of Internet Explorer may include alternative versions or may not include any MFC .dll files at all. A component that uses the MFC .dll files as dependencies should package the MFC .dll files accordingly.

I've written an ActiveX control that I've marked as Safe for Scripting, and I'm having trouble getting it to work when running off a page on a local hard disk. What am I doing wrong?

The problem may be due to any of the following reasons:

- A missing dependent .dll file
- Necessary security level set on the wrong zone
- A control that is not marked as "safe for scripting and initialization" will not be loaded if the page that references the control is being accessed from the local hard drive.

For more information on marking ActiveX controls as "safe for scripting and initialization," please refer to the *Microsoft Internet Client SDK* documents on "Safe Initialization and Scripting for ActiveX Controls" in the Component Development/ActiveX Controls section.

Control Development

How can I improve performance in my ActiveX control?

For better performance, make your control an apartment-model control. Internet Explorer 4 uses multiple threads and may host the control in a secondary thread. If the control is not created as apartment-model aware and marked as such, it is created and executed in the context of the calling application's primary thread, requiring calls on the control's methods to be marshaled between threads. This can cause a performance hit and can be very prominent if there are many non-apartment-model controls in an HTML page. To make a control apartment model, the control needs to be marked as such in the registry and has to be written so that it is apartment-model safe.

Scripting

How do I determine from a script if the Internet Explorer browser is running offline or not?

Currently, there is no way to determine this from a script. Although the IWebBrowser2 interface provides a get/put_Offline method that indicates whether the WebBrowser is reading from the cache, there is no way to get this information from the WebBrowser object model up to the script level. If desired, you could write an ActiveX control that gets this information from the WebBrowser object model and expose it as a property or method, which can then be accessed from a script.

Why do I get a Permission Denied error whenever I try to access a frame's document from a script written in another frame's document? The same code runs fine in Internet Explorer 3.

This is due to a cross-frame security feature that is implemented in Internet Explorer 4, but not in Internet Explorer 3. A frame running on one server is not able to access another frame's document running on another server. Similarly, with the introduction of security zones in Internet Explorer 4, a script cannot access pages across zones.

Why do I get a Permission Denied error whenever I try to access a frame on a different first-tier domain, but on the same second-tier domain?

This is another side effect of the Internet Explorer 4 cross-frame security feature described above. A frame running on example1.microsoft.com cannot access a frame on example2.microsoft.com.

The correct way to do this is to set the domain property on both pages to the common substring domain. In this case, set the domain to microsoft.com, as illustrated below:

```
<SCRIPT>
document.domain = "microsoft.com"
</SCRIPT>
```

From a client-side script, how do I check for the browser version so my application can degrade gracefully if the browser does not support the new Internet Explorer 4 features?

You can use the JScript™ function below, from a client-side script, to determine the version of the browser on which it is running. The function returns the major version number for any Microsoft Internet Explorer browser, and zero (0) for others. Use of this function ensures that the script is compatible with future versions of Internet Explorer.

```
// This function returns Internet Explorer's major version number,
// or 0 for others. It works by finding the "MSIE " string and
// extracting the version number following the space, up to the
// decimal point, ignoring the minor version number
<SCRIPT LANGUAGE="JavaSCRIPT">
function msieversion()
{
var ua = window.navigator.userAgent
var msie = uA:indexOf ( "MSIE " )

if ( msie > 0 ) // If IE, return version number
return parseInt (uA:substring (msie+5, uA:indexOf (".", msie )))
else    // If another browser, return 0
return 0
}
</SCRIPT>
```

Is there a way to detect the browser's support for the new Internet Explorer 4 features from a server-side script?

The Browser Capability component that comes with ASP provides your scripts with a description of the capabilities of the client's Web browser by comparing the User-Agent HTTP Header with the entries in the Browscap.ini file. In order for an ASP application to detect the browser's support for the new Internet Explorer features, copy the latest Browscap.ini from **http://www.microsoft.com/iis/usingiis/developing/updates.htm** to your \Windows\System32\Inetsrv\Asp\Cmpnts directory and execute a server-side script similar to the example described in article Q167820 in the Microsoft Knowledge Base.

Miscellaneous

Is it possible to have Internet Explorer 3 and Internet Explorer 4 coexist on the same machine?

No. There are no plans to support the coexistence of these two Internet Explorer versions at this time. Internet Explorer 3 and Internet Explorer 4 share system components that cannot exist in multiple copies on the same machine.

What is the difference between ADO and ADOR, and which should I be using on my Web pages?

The Active Data Object (ADO) components ship in two forms—one for a Web server and another for the client. The ADO component installed with Internet Explorer 4 is the ADO Recordset (ADOR). ADOR provides an object model for script access to data supplied by a data source object (DSO) embedded in a Web page. It does not, however, provide ADO Connection or Command objects. These are provided only as part of the server installation.

Included with the *Microsoft Internet Client SDK,* in self-extracting archives, is the full set of ADO components. When building applications using ADO for Internet Explorer, your client-side scripts should depend only on the availability of the **Recordset** object. The full ADO interfaces are intended for use with ASPs and custom business objects that run on a Web server. Refer to Mdac.txt in the Inetsdk\Bin folder for more details.

APPENDIX J

Custom-Build Checklist

The following tables are designed to help administrators prepare for the Microsoft® Internet Explorer Administration Kit (IEAK) Configuration Wizard. The information below outlines all the configuration options that will be presented in the IEAK. By preparing this information in advance, you can speed up your custom package generation. It is also recommended that you run through the IEAK Configuration Wizard yourself, in order to get acquainted with its features.

Stage 1—Gathering Information	
Enter Company Name and Customization Keycode	
Company Name	
IEAK Keycode	
Automatic Version Synchronization Support	Yes No
Select a Language	
Target Language	
Select Media to Distribute Your Browser	
Path of Destination Folder	
Select Media	
CD-ROM	Yes No
Multiple Floppy Disks	Yes No

Stage 2—Specifying Active Setup Parameters	
Select a Microsoft Download Site	
Download Site	
Automatic Version Synchronization (AVS)	
Microsoft Internet Explorer 4 Web Browser	
Microsoft Internet Explorer Core Fonts	
Microsoft NetMeeting™	
Microsoft Outlook™ Express	
Microsoft Chat 2.0	
Microsoft NetShow™	
Intel® Indeo™5	
VDOLive Player	
Microsoft Interactive Music Control	
Microsoft Internet Explorer Sound Pack	
Macromedia Shockwave Director	
Macromedia Shockwave Flash	
RealPlayer by Progressive Networks	
Microsoft FrontPage® Express	
Microsoft Web Publishing Wizard	
Microsoft Visual Basic® Run Time	
Microsoft Wallet	
Task Scheduler	
Microsoft Internet Explorer Supplemental Fonts	
Specify Custom Active Setup Components (up to 10)	
Components	
Locations	
Commands	
Global Universal Identifiers (GUIDs)	
Parameters	
Versions	
Sizes	
Uninstall Keys	
Specify Trusted Publishers	
Specify Trusted Publishers	

Stage 3—Customizing Active Setup	
Customize the Autorun Screen for CD-ROM Installations	
Title Bar Text	
Custom Background Bitmap Location	
Text Colors	
Button Styles	Standard 3-D Custom
Customize the Active Setup Wizard	
Active Setup Wizard Title Bar Text	
Active Setup Wizard Bitmap Path	
Custom Components Install Section	
Custom Components Installation Title	
Select Silent Install	Yes No
Select Installation Options (up to 10)	
Option Names	Minimal Standard Full Custom
Option Descriptions	
Component Combinations	
Specify Download URLs	
Site Names	
Site URLs	
Site Regions	
Select Version Number	
Version Number	
Configuration Identifier	
Product Update URL	
Specify Where You Want to Install the Browser	Windows Program Files Custom
Integrating the Web Desktop Update	Yes No User Choice

Stage 4—Customizing the Browser	
Customize the Window Title and Toolbar Background	
Title Bar Text	
Toolbar Background Bitmap Path	
Customize the Start and Search Pages	
Start Page URL	
Search Page URL	
Specify an Online Support Page for Your Browser	
Online Support Page URL	
Favorites Folder and Links Customization	
Add URLs	
Test URLs	
Import URLs	
Customize the Welcome Message and Desktop Wallpaper	
Display Welcome Page	Default Page No Page Custom Page
Disable Internet Explorer 4 Welcome Window	Yes No
Path of Custom Desktop Wallpaper File	
Customize the Active Channel Bar	
Delete Channels	
Add Channels	
Import Channels	
Do Not Customize Channels	
Import Current Channel Configuration	
Delete Existing Internet Explorer 4 Channels	Yes No
Show Channel Bar by default (Windows NT® only)	Yes No

Stage 4—Customizing the Browser *(continued)*	
Customize Software Update Channels	
Do Not Customize Software Distribution Channels	
Import the Current Software Distribution Channel Configuration	
Schedule	None Auto Daily Weekly Monthly
Specify Active Desktop Components	
Do Not Customize the Active Desktop™	
Import the Current Active Desktop Components	
Background HTML Settings	
Web (Desktop Item Settings)	
Customize Desktop Toolbars	
Don't Customize	
Import the Current Desktop Toolbar Settings	
My Computer and Control Panel Web View Customization	
Path of My Computer (Mycomp.htt)	
Path of Control Panel (Controlp.htt)	
User Agent String Customization	
Custom String to Be Appended to User Agent	
Automatic Browser Configuration	
Enable automatic browser configuration	Yes No
Auto-configure URL (.ins file)	
Auto-proxy URL (.js or .pac file)	
Auto-configure Every *n* Minutes	

Stage 4—Customizing the Browser *(continued)*	
Specify Proxy Settings	
Enable Proxy Settings	Yes No
HTTP	
Secure	
FTP	
Gopher	
Socks	
Use Same Proxy for All Addresses?	Yes No
Exceptions to Proxy Server	
Do Not Use Proxy Server for Local (intranet) Addresses	Yes No
Site Certificate and Authenticode Settings	
Import Certificate Authorities	
Import Authenticode™ Security	
Add New Root Certificate	
Security Zones and Content Ratings Customization	
Security Zone Modifications	
Zones	
Local Intranet Zone Setting	High Medium Low Custom
Trusted Sites Zone Setting	High Medium Low Custom Add Sites
Internet Zone Setting	High Medium Low Custom

Stage 4—Customizing the Browser *(continued)*	
Restricted Sites Zone Setting	High Medium Low Custom Add Sites
Settings	
High	
Medium	
Low	
Custom Security	
ActiveX® Controls and Plug-ins	
Java	
Scripting	
Downloads	
User Authentication	
Miscellaneous	
PICS Content Advisor	
Ratings	
Language	0 (none) to 4 (explicit)
Nudity	0 (none) to 4 (explicit)
Sex	0 (none) to 4 (explicit)
Violence	0 (none) to 4 (explicit)
General	
User Options	
Users Can See Sites That Have No Rating	Yes No
Supervisor Can Type a Password to Allow Users to View Restricted Content	Yes No
Supervisor Password	
Advanced	
Rating Systems	
Ratings Bureau	

Stage 5—Component Customization	
Specify Internet Mail Servers, Domain, and News Server	
Incoming (POP3 or IMAP) Server	
Outgoing Mail (SMTP) Server	
Internet News Server	
Make Outlook Express the Default Mail Client	Yes No
Make Outlook Express the Default News Client	Yes No
Use Secure Password Authentication	Yes No
Specify LDAP Server Settings	
Friendly Name	
Directory Service	
Home Page	
Search Base	
Service Bitmap	
Check Names Against This Server When Sending Mail	Yes No
Authentication Type	Anonymous Secure Password Password
Outlook Express Customizations	
Customize InfoPane	
URL	
Local File Path	
Custom Welcome Message	
HTML Path	
Sender	
Reply-to	
Include a Signature	
Append to Mail Messages	Yes No
Append to News Postings	Yes No

Stage 6—System Policies and Restrictions	
Microsoft NetMeeting Settings	
Restrict the Use of File Transfer	
Prevent the User from Sending Files	Yes No
Prevent the User from Receiving Files	Yes No
Restrict the Use of Application Sharing	
Disable All Application Sharing Features	Yes No
Prevent the User from Sharing the Clipboard	Yes No
Prevent the User from Sharing MS-DOS® windows	Yes No
Prevent the User from Sharing Explorer windows	Yes No
Prevent the User from Collaborating	Yes No
Restrict the Use of the Options Dialog	
Disable the General Options Page	Yes No
Disable the My Information Options Page	Yes No
Disable the Calling Options Page	Yes No
Disable the Audio Options Page	Yes No
Disable the Video Options Page	Yes No
Disable the Protocols Options Page	Yes No
Prevent the User from Answering Calls	Yes No
Prevent the User from Using Audio Features	Yes No

Stage 6—System Policies and Restrictions *(continued)*	
Restrict the Use of Video	
Prevent the User from Sending Video	Yes No
Prevent the User from Receiving Video	Yes No
Prevent the User from Using Directory Services	Yes No
Set the Default Directory Server	
Set Exchange Server Property for NetMeeting Address	
Preset User Information Category	
Microsoft NetMeeting Protocols	
Disable TCP/IP	Yes No
Disable null modem	Yes No
Web Desktop Settings	
Desktop	
Disable Active Desktop	Yes No
Do not allow changes to Active Desktop	Yes No
Hide Internet Explorer icon	Yes No
Hide Network Neighborhood icon	Yes No
Hide all items on Active Desktop	Yes No
Active Desktop Items	
Disable All Desktop Items	Yes No
Disable Adding Any Desktop Items	Yes No
Disable Deleting Any Desktop Items	Yes No
Disable Editing Any Desktop Items	Yes No
Disable Closing Any Desktop Items	Yes No

Stage 6—System Policies and Restrictions *(continued)*	
Desktop Wallpaper	
No HTML Wallpaper	Yes No
Disable Changing Wallpaper	Yes No
Desktop Toolbars Settings	
Disable Dragging, Dropping and Closing All Toolbars	Yes No
Disable Resizing All Toolbars	Yes No
Start Menu	
Remove Favorites from Start Menu	Yes No
Remove Find from Start Menu	Yes No
Remove Run from Start Menu	Yes No
Remove Documents from Start Menu	Yes No
Do Not Keep History of Recently Opened Documents	Yes No
Clear History of Recently Opened Documents	Yes No
Disable Logoff	Yes No
Disable Shut Down	Yes No
Disable Changes to Printers and Control Panel Settings	Yes No
Disable Changes to Taskbar and Start Menu Settings	Yes No
Disable Context Menu (right-click) for Taskbar	Yes No
Hide Custom Programs Folders	Yes No
Hide Common Program Groups in Start Menu (Windows NT only)	Yes No

Stage 6—System Policies and Restrictions *(continued)*	
Shell Settings	
Enable Classic Shell	Yes No
Disable File Menu in Shell Folders	Yes No
Do Not Allow Customization of Folders in Web View	Yes No
Disable Context Menu in Shell Folders	Yes No
Only Allow Approved Shell Extensions	Yes No
Do Not Track Shell Shortcuts During Roaming	Yes No
Hide Floppy Drives in My Computer	Yes No
Disable Net Connections/Disconnections	Yes No
Printer Settings	
Hide General and Details Tabs in Printer Properties	Yes No
Disable Deletion of Printers	Yes No
Disable Addition of Printers	Yes No
System	
Run only specified Windows applications	
Do not allow computer to restart in MS-DOS mode	Yes No
Internet Settings	
Colors	
General Colors	
Background Color (0,0,0 through 255,255,255)	
Text Color (0,0,0 through 255,255,255)	
Use Windows Colors	Yes No

Stage 6—System Policies and Restrictions *(continued)*	
Link Colors	
Link Color (0,0,0 through 255,255,255)	
Visited Link Color (0,0,0 through 255,255,255)	
Use Hover Color	Yes No
Hover Color (0,0,0 through 255,255,255)	
Fonts	
Font Size (0 smallest – 4 largest)	
Languages	
Choose the Default Language Preferences	
Modem Settings	
Dial-up Networking Connection	
Enable Autodialing	Yes No
Number of Times to Attempt Connection	
Number of Seconds to Wait Between Attempts	
Connect Without User Intervention	Yes No
Disconnect If Idle After Specified Number of Minutes	Yes No
Minutes to Wait Before Disconnecting	
Perform System Security Check Before Dialing	Yes No
Programs	
Program to use for Calendar	
Program to use for Contacts	
Program to use for Internet Call	
Browsing	
Disable Script Debugger	Yes No
Launch Channels in Full Screen Mode	Yes No
Launch Browser in Full Screen Mode	Yes No

Stage 6—System Policies and Restrictions *(continued)*	
Use Autocomplete	Yes No
Show Friendly URLs in Status Bar	Yes No
Enable Smooth Scrolling	Yes No
Enable Page Transitions	Yes No
Browse in a New Process	Yes No
Enable Page Hit Counting	Yes No
Enable Scheduled Subscription Updates	Yes No
Underline Links	Always Never Hover
Multimedia	
Show Pictures	Yes No
Play Animations	Yes No
Play Videos	Yes No
Play Sounds	Yes No
Smart Image Dithering	Yes No
Security	
Enable Profile Assistant	Yes No
Delete Saved Pages When Browser Is Closed	Yes No
Do Not Save Encrypted Pages to Disk	Yes No
Warn If Forms Submit is being Redirected	Yes No

Stage 6—System Policies and Restrictions *(continued)*	
Warn If Changing Between Secure and Insecure Mode	Yes No
Cookies	Always accept Prompt Disable
Java VM	
JIT Compiler Enabled	Yes No
Java Logging Enabled	Yes No
Printing	
Print Background Colors and Images	Yes No
Searching	
Autoscan Common Root Domains	Yes No
Search When URL Fails	Always Search Always Ask Never Search
Toolbars	
Show Font Button	Yes No
Small Icons	Yes No
HTTP 1.1 Settings	
Use HTTP 1.1	Yes No
Use HTTP 1.1 Through Proxy Connections	Yes No
Outlook Express Settings	
General Settings	
Mail and News Security Zones	
Put Mail and News in the Restricted Sites Zone (instead of the Internet Zone)	Yes No

Stage 6—System Policies and Restrictions *(continued)*	
HTML Mail and News Composition Settings	
Mail: Make Plain Text Message Composition the Default for Mail Messages (instead of HTML mail)	Yes No
News: Make HTML Message Composition the Default for News Posts (instead of plain text)	Yes No
View Customization	
Folder and Message Navigational Elements	
Turn On Outlook Bar	Yes No
Turn Off Folder List (tree view of folders)	Yes No
Turn On Folder Bar (horizontal line displaying folder names)	Yes No
Turn Off the Tip of the Day	Yes No
Channels and Subscriptions Settings	
Maximum KB of Site Subscriptions (zero disables restriction)	
Maximum KB of Channel Subscriptions (zero disables restriction)	
Maximum Number of Site Subscriptions That Can Be Installed (zero disables restriction)	
Minimum Number of Minutes Between Scheduled Subscription Updates (zero disables restriction)	
Beginning of Range in Which to Exclude Scheduled Subscription Updates. Minutes from Midnight (zero disables restriction)	
End of Range in Which to Exclude Scheduled Subscription Updates. Minutes from Midnight (zero disables restriction)	
Maximum Site Subscription Crawl Depth	
Internet Explorer Properties	
General Tab Settings	
Disable Changing Home Page Settings	Yes No
Disable Changing Cache Settings	Yes No
Disable Changing History Settings	Yes No

Stage 6—System Policies and Restrictions *(continued)*	
Disable Changing Color Settings	Yes No
Disable Changing Link Color Settings	Yes No
Disable Changing Font Settings	Yes No
Disable Changing Language Settings	Yes No
Disable Changing Accessiblity Settings	Yes No
Security Tab Settings	
Use Only Machine Settings for Security Zones	Yes No
Do Not Allow Users to Change Policies for Any Security Zone	Yes No
Do Not Allow Users to Add/Delete Sites from a Security Zone	Yes No
Content Tab Settings	
Disable Changing Ratings Settings	Yes No
Disable Changing Certificate Settings	Yes No
Disable Changing Profile Assistant Settings	Yes No
Disable Changing Microsoft Wallet Settings	Yes No
Connection Tab Settings	
Disable Calling Connection Wizard	Yes No
Disable Changing Connection Settings	Yes No
Disable Changing Proxy Settings	Yes No
Disable Changing Automatic Configuration Settings	Yes No

Stage 6—System Policies and Restrictions *(continued)*	
Programs Tab Settings	
Disable Changing Messaging Settings	Yes No
Disable Changing Calendar and Contact Settings	Yes No
Disable Changing Internet Explorer Default Browser Settings	Yes No
Advanced Tab Settings	
Disable Changing Settings on Advanced Tab	Yes No
Code Download	
Internet Search Path*	

* This is the CodeBaseSearchPath. The default is **CODEBASE; http://activex.microsoft.com/objects/ocget.dll**

When Internet Component Download is called to download code, it traverses the Internet Search Path to look for the desired component. This is a list of Object Store servers that will be queried every time components are downloaded using GoGetClassObjectFromURL. This way, even if an <OBJECT> tag in an HTML document does not specify a CODEBASE location to download code for an embedded OLE control, the Internet Component Download will still use the Internet Search Path to find the necessary code.

Stage 6—System Policies and Restrictions *(continued)*	
Channels Settings	
Disable Channel User Interface	Yes No
Disable Adding and Subscribing to Channels	Yes No
Disable Editing Channel Properties and Channel Subscriptions	Yes No
Disable Removing Channels and Subscriptions to Channels	Yes No
Disable Adding Site Subscriptions	Yes No
Disable Editing Site Subscriptions	Yes No
Disable Removing Site Subscriptions	Yes No

Stage 6—System Policies and Restrictions *(continued)*	
Disable Channel Logging	Yes No
Disable Update Now and Update All for Channels and Subscriptions	Yes No
Disable All Scheduled Channel and Site Subscriptions	Yes No
Disable Unattended Dialing by Subscriptions	Yes No
Disable password caching for all channel or site subscriptions	Yes No
Disable Downloading of Channel Subscription Content (change notification will still function)	Yes No
Disable Downloading of Site Subscription Content (change notification will still function)	Yes No
Disable Editing and Creating of Schedule Groups	Yes No
Microsoft Chat Settings	
Chat Server List (separated by semicolons)	
Default Chat Server	
Default Chat Room	
Default Character	
Default Backdrop	
User Profile String	
Show Only Registered Rooms in Room List	Yes No

APPENDIX K

Internet Explorer Administration Kit (IEAK) FAQs

This appendix covers some of the most Frequently Asked Questions (FAQs) about the Microsoft® Internet Explorer Administration Kit (IEAK) 4. For more information about using the IEAK, see Part 9.

What are some of the new features in the IEAK 4?

Brand the setup as well as the browser

The IEAK 4 now allows you to brand the entire user experience. With the IEAK 4, you can specify title elements and graphics to be used during the setup process. With the IEAK 3.2a, you could only brand the browser.

Create and/or delete channels in the Internet Explorer 4 Channel Guide

With the IEAK 4, you can add your own Active Channel™ to the Internet Explorer Channel bar. You can also use the IEAK 4 to delete competitors' channels. Please note that the IEAK 4 license agreement limits you to deleting only channels of competing Internet access providers.

Import Active Desktop items

The IEAK 4 enables you to specify which Active Desktop™ items appear on your end users' computers. You can add desktop views of Web pages, or you can display custom controls that link directly to your Web site.

Import Desktop toolbar settings

With the IEAK 4, you can import toolbar settings that will be applied when your end users install Internet Explorer 4. These settings are taken directly from the settings specified on the machine you used to build your Internet Explorer installation packages.

Specify more than five links on the Internet Explorer Links toolbar

Now you can specify more than five links to appear on the Internet Explorer 4 Links toolbar.

Create a package with up to 10 different installation options

With previous versions of the IEAK, you could only build a package with one installation option. Using the IEAK 4, you can build a package with up to 10 different installation options from which the user can choose.

Customize user agent string

Now you can customize the user agent string of your browser packages, so you can track the number of hits that are generated by your customized browser and distinguish between various distribution programs. Here's an example of a user agent string that would appear in your Web server log:

```
Mozilla/4.0 (compatible; MSInternet Explorer 4.0; Windows NT); your
    custom string
```

Create a custom welcome page

Present end users with your own custom page when they start up Internet Explorer for the first time.

Customize the Internet Explorer 4 Search bar

With IEAK 4, you can fully customize the new Internet Explorer Search bar.

Change toolbar background bitmap

Now you can customize the look of Internet Explorer by changing the background bitmap on the Internet Explorer toolbar. Use this feature with caution, however; using background bitmaps with dark colors can make the toolbar unreadable.

10 user-specified components

You can now build installation packages to include up to 10 user-specified components. The IEAK 3.2 allowed you to add just 2 user-specified components.

Specify up to 10 download sites

You can specify up to 10 download sites for each installation package you build with the IEAK 4.

Security zones and other security enhancements

Internet Explorer 4 adds a new security feature called security zones. Security zones break up the Internet and intranet sites to allow for greater manageability. Internet Explorer includes four default zones: Local Intranet, Trusted Sites, Internet, and Restricted Sites. As the system administrator, you can preset these settings. You can apply different security settings (high, medium, low, or custom) to each of these.

System policies and restrictions management

As the system administrator, you can manage system policies and restrictions with an easy-to-use interface in both the IEAK Configuration Wizard and the Profile Manager. Some of these restrictions include Active Desktop and shell feature lock-downs, as well as component settings (such as not allowing users to place calls from NetMeeting).

Improved Profile Manager

The improved Profile Manager (formerly known as the INS Editor) includes a tree-view pane that gives you easy access to all the options available in the IEAK Configuration Wizard. You can reach each option quickly, and the interface for making changes is as simple to use as the IEAK. The Profile Manager also has incorporated the System Policies and Restrictions management capabilities that are available at the end of the IEAK Configuration Wizard.

What optional components are available in the Internet Explorer 4 suite?

Here is a quick overview of the components included with the IEAK 4.

Microsoft Outlook™ Express

Outlook Express is a highly versatile tool for exchanging e-mail and newsgroup messages with individuals and groups. You can use the new HTML functionality to add graphics, animation, and even multimedia files to your e-mail messages.

Microsoft NetMeeting™

With NetMeeting, the Internet's premier conferencing tool, you can hold video and voice conversations and collaborate with groups of people in real time by sharing software applications, chatting, and sharing a whiteboard.

Microsoft Chat 2.0

Get online and communicate with others, using Microsoft Chat. This new kind of chat program lets you decide how to display your message—choose text only or a combination of text and graphical features.

Microsoft Web Publishing Wizard

This wizard steps you through the process of posting your Web site to almost any Web server available.

Microsoft FrontPage® Express

FrontPage Express makes it easy to create and edit Web pages that you can post on the Internet or intranet.

Microsoft Interactive Music Control

Internet Explorer 4 introduces the new Interactive Music control, an ActiveX® control that composes and plays music in response to a user's actions. The Interactive Music Control thus creates a soundtrack of the user's actions—for instance, in a computer game or guided tour of a Web site—all without using WAV or MIDI files that require time to download.

Microsoft Interactive Music Control with Synthesizer

The Microsoft Interactive Music Control with Synthesizer adds the Microsoft Synthesizer and support for DLS. DLS is an industry standard format for packaging instrument sounds in a way that can be recognized and used by hardware (like a soundcard) or software synthesizers.

Microsoft VRML 2.0 Viewer

With the Microsoft VRML 2.0 Viewer, Internet Explorer users can view engaging virtual 3-D worlds.

Microsoft Agent

Microsoft Agent is a set of software services that supports the presentation of software agents as interactive personalities within the Microsoft Windows interface. These agents can be developed to provide assistance to users by speaking to them as they use your applications of Web sites.

Macromedia Shockwave Director

With Director, you can create a variety of multimedia productions, including business presentations, Web content, interactive advertising pieces, kiosk productions, and CD-ROM titles.

Macromedia Shockwave Flash

Flash brings Web pages to life without the wait. Vector-based Flash movies offer compact, interactive Web interfaces, animations, buttons, advertising banners, logos, maps, cartoons, and more.

Microsoft Script Debugger

Microsoft Script Debugger for Internet Explorer is a debugging environment that extends Internet Explorer by allowing Web developers to browse, edit, and debug HTML pages that contain Visual Basic® Scripting Edition (VBScript) or JScript™ (the Microsoft implementation of JavaScript). The Microsoft Script Debugger is the first environment that allows users to debug scripted HTML. This tool gives developers a seamless way to combine HTML and script development.

Microsoft NetShow™

NetShow broadcasts high-impact, low-bandwidth video and more to computer desktops for entertainment, training, sales, event coverage, and more.

Microsoft Internet Explorer Supplemental Fonts

The IEAK provides a set of TrueType® fonts that can be used with Internet Explorer. If users install these, they will be able to read Web-page text that was designed to be viewed with the following TrueType fonts: Arial, Comic, Courier, Impact, and Times New Roman.

Microsoft Visual Basic Run Time

Microsoft Visual Basic Run Time makes it possible for you to distribute ActiveX controls with your Internet Explorer 4 installation packages.

Intel® Indeo™5

Indeo video is the Intel digital video capture, compression, and decompression codec—a software driver used to compress digital video data for storage and to decompress it for playback on a multimedia computer. The latest version of Indeo video, designed for Intel MMX technology, allows software-only playback of high-quality video on desktop multimedia computers.

VDOLive Player

The VDOLive Player takes advantage of streaming technology to deliver high audio and video quality over limited bandwidth.

Microsoft Internet Explorer Sound Pack

The Internet Explorer Sound Pack provides a collection of sounds for use with the Internet Explorer to help users know when pages have started and finished loading. It also alerts users when a site has been found.

RealPlayer by Progressive Networks

You can use RealPlayer to play different media types, including animation, audio, video, 3-D images, MIDI, presentations, and text.

Can an IEAK 3 .ins file be used in the IEAK 4?

The .ins files are backwards compatible. Sections and entries that existed in the IEAK 3 .ins files have not changed, but there are new sections and entries for the new features added to the IEAK 4. To take advantage of all the new features included in the IEAK 4, it's recommended that you create a new .ins file with the IEAK Configuration Wizard.

What are the requirements for running the IEAK Configuration Wizard?

Internet Explorer 4 must be installed on the build machine before the IEAK Wizard can be used. Before starting the wizard, calculate how much disk space is required for the components you want to install. If you plan to install all the components of the Internet Explorer suite, you will need approximately 50 MB in the Program Files folder and 50 MB on the destination drive.

What type of distribution media will the IEAK 4 support?

The IEAK 4 will support download from an intranet or the Internet, compact disc, and single and multiple floppy disks.

How can I offer a customized browser that takes advantage of 128-bit encryption?

U.S. regulations regarding encryption technology require a separate licensing process for users who wish to redistribute 128-bit encryption with Internet Explorer 4. According to federal regulations, licensees must be located in the U.S. or Canada only and must agree to distribution restrictions described in an addendum to the IEAK Licensing Agreement.

For more information, see the "Server Gated Cryptography" section of Chapter 28, "Digital Certificates," or see the Microsoft IEAK Licensing Agreement Web page at **www.microsoft.com/ie/ieak/license.htm**.

How can I uninstall components that were installed with Internet Explorer 3?

To remove the components installed with Internet Explorer 3, select the **Add/Remove Programs** icon in Control Panel, and then uninstall the appropriate component.

What are the bitmap dimensions for the Active Setup bitmap, and are there any sample bitmaps?

The dimensions for the Active Setup bitmap are 120 pixels wide by 239 pixels high. It needs to be a BMP file, and it must be 256 colors or fewer. No sample bitmaps are included with the IEAK.

What are the dimensions for the toolbar bitmap?

The toolbar bitmap can use any dimensions. It must be a BMP file, and it must be 256 colors or fewer. When creating a toolbar bitmap, however, be careful not to use colors that are too dark, or text will be difficult to read and graphics hard to see.

Is there a way to control the order of the channels in the IEAK?

There is no way to preset a custom channel order.

Can existing channels be removed?

Yes, you can remove channels in the IEAK. You can also use the Profile Manager to prevent users from adding or deleting the channels that you have pre-configured.

Are there any technical specs on how the Channel Definition Format (CDF) file is created and where it resides?

The CDF specification is located at **http://www.microsoft.com/standards/cdf.htm** and can also be found in the *Microsoft Internet Client SDK* at **http://www.microsoft.com/workshop/prog/inetsdk/**.

How does a CDF file get pushed to customers when they visit a Web site?

The CDF file itself does not get pushed to users who visit your Web site. The file resides on the server, and you must provide an HTML link to it. When the visitor clicks that link, it will activate the Channel Subscription Wizard that steps the user through the process of subscribing to a channel. Of course, you can pre-configure your own custom CDF files to be built into Internet Explorer using the IEAK. In that case, users won't have to do anything since the channels will already be present in their Channel bar. For more information about creating CDF files, see Chapter 16, "Managed Webcasting."

How do you configure Outlook Express to support multiple user scenarios?

Outlook Express uses Windows profiles to address the multiple user scenarios. Users can log into their respective profiles and access their mail. To switch from one user profile to another, users select the **Log Off** option from the **File** menu in Outlook Express or from the **Start** button on the Windows taskbar. Alternatively, they can restart Windows if they already have a profile set up. If users don't have a profile set up on their computer, the **Enable Multi-user Settings** dialog box will appear and guide users through the steps to set up a profile. Once the new profile is set up and new users log into Windows and then Outlook Express, they can set up their own account and use their own mail store. For more information about user profiles, see Chapter 5, "User Profiles."

What importing options does Outlook Express support?

Outlook Express ships with migration tools to convert mail messages, address books, and account settings from the following mail packages: Eudora Light and Eudora Pro, Netscape Mail, Communicator, Windows Messaging, Outlook, Exchange, and Internet Mail and News. In addition, Outlook Express offers conversion of LDIF-LDAP and comma-separated address books. For more information about Outlook Express, see Chapter 18.

Can I configure the Outlook Express AutoReply option with the IEAK?

By default, Outlook Express replies to messages in the format in which they were sent. For example, if a user sends you a message in plain text, you will respond in plain text, even though your default is HTML. This cannot be configured through the IEAK, but users have the option to turn it off. In addition, the IEAK does allow you to designate the default message format for users. You can write an .adm file that will turn this feature off by default in your users' version of Outlook Express. For more information about Outlook Express, see Chapter 18.

What is the "InfoPane" in Outlook Express?

You can use the IEAK to customize a 50-pixel-high HTML pane across the bottom of the Outlook Express screen. You have two options for customizing the InfoPane. First, you can download a local HTML file to your users' computers and have the InfoPane display this file. You can use this file to provide links to account information, support sites, training information, your home page, and other sites or images. The second option is to point the InfoPane to any URL on the Web. When users are online, they will see the contents of that site inside the InfoPane. When they are not online, the InfoPane will be blank. Note that users will always have an option to turn the InfoPane off.

Whichever option you choose, we suggest that you design your HTML content for 640 pixels wide by 50 pixels high.

Does the installer wait for custom components to finish?

Yes, Active Setup will not proceed until your custom components have finished installing. For more information about Active Setup, see Chapter 2.

Is there an installation option that allows users to select the individual components they want to install?

Yes, the IEAK does not offer a check box for each component, but there is an option for users to choose from 10 possible installation options. It is up to the IEAK administrator to create applicable packages. If you do not wish to include these components in your distribution package, you can provide them by a component add-on Web site.

Will there be a way to customize the Readme.txt?

No.

How do I create versions of Internet Explorer for Windows 3.1?

The IEAK 4 currently does not build packages for 16-bit platforms. Once Internet Explorer 4 for Windows 3.1 has been released, Microsoft will make available an IEAK that will generate packages for the 16-bit platform.

How do I import a collection of favorites arranged inside folders?

When you import a collection of favorites, the IEAK imports the contents of the folder but not the folder itself. To import an entire directory structure, select the top-level folder that contains all of the subdirectories you want to import. This will import all favorites and their folders.

Does the IEAK 4 support the creation of a single self-installing, executable (.exe) file (vs. the .cab files used by Active Setup)?

No.

What is Active Setup?

Active Setup is new in Internet Explorer 4. Active Setup is a small, Web-based setup package that enables your users to install the latest Internet Explorer components directly from your Web site or intranet. Active Setup can be run from a single floppy disk and over the Internet.

The Active Setup engine provides significant advantages in usability for both download and floppy-disk installations. For a download installation, it divides the download into several smaller segments, making it possible to restart in the event of a failure. For a floppy-disk installation, it enables Internet Service Providers (ISPs) to produce and distribute packages with a single floppy disk.

You can specify up to 10 download sites when you build your package(s), making it easy for your users to download and install Internet Explorer and its components.

Active Setup also detects which installed components need to be updated, so your users don't have to download an entirely new package just to update one of the components. For more information about Active Setup, see Chapter 2.

Are there any Setup switches for Internet Explorer 4?

There are two .exe files that actually run: IE4Setup.exe and IE4wzd.exe.

The IE4Setup.exe is just an application that wraps around Internet Express (IExpress), and most of the installation wizard code is in IE4wzd.exe. Since IE4Setup.exe is just the IExpress wrapper, typing **/?** does not reveal all the correct command-line switches. (For more information about IExpress, see Appendix L.)

This is the command line you can use to run IE4Setup.exe in batch mode (hands-free mode—so you don't need to click Next or press the ENTER key) to go to the next wizard page.

```
IE4Setup.exe /c:"ie4wzd.exe /q /u:""http://webserver/
    directory/cab"" /s:#e"
```

–Or–

```
IE4Setup.exe /c:"ie4wzd.exe /q /u:""file://\\netlocation\
    directory\cab"" /s:#e"
```

Other switches of interest in IE4wzd.exe are:

- /S:#e—Location of calling .exe (Usually will be IE4Setup.exe, not required but helps softboot work)
- /U—Location for installation .cab files (not used on CD-ROM)
- /M:1,2,3—0 = standard install(default), 1 = enhanced, 2 = full
- /I:Y,N—Whether you want integrated desktop or not. Default is "Y"
- /R:N—To disable hardboot/softboot

For more information about Active Setup and ACME Setup, see Chapters 2 and 3, respectively. For more information about Setup command-line switches, see Appendix A.

Where can I get more information about Internet Explorer 4?

For more information, see the following Web sites.

- For information about Internet Explorer 4:
  http://www.microsoft.com/ie/ie40/
- For information about the IEAK, including licensing:
  http://www.microsoft.com/ie/ieak/
- For Microsoft Internet Explorer Press (for news regarding Internet Explorer and the IEAK):
  http://www.microsoft.com/ie/press/
- For CDF specification:
  http://www.microsoft.com/standards/cdf.htm
- For information about developing content for Internet Explorer 4, such as Dynamic HTML and Active Channels:
  http://www.microsoft.com/workshop/

APPENDIX L

IExpress Configuration Wizard

If you want to include custom components inside the Internet Explorer installation process, such as a custom FTP client or communication software, the Microsoft® Internet Explorer Administration Kit (IEAK) includes a utility called Internet Express (IExpress) for this purpose. IExpress is a tool that creates custom, self-installing, self-extracting packages (or .cab files) of applications. The IExpress program resides in the directory C:\Program Files\ieak\tools\iexpress.

Using the IExpress Configuration Wizard

You can use the step-by-step IExpress Configuration Wizard to package applications so that they can be installed by Active Setup along with Internet Explorer. This can make the rollout of multiple applications much easier, as they can all be done at the same time.

Starting the IExpress Configuration Wizard

▶ **To start the IExpress Configuration Wizard**

1. On the **Start** menu, click **Run**.

   The **Run** dialog box opens.
2. Enter **IExpress.exe**.
3. Click **OK**.

Navigating in the IExpress Configuration Wizard

To	Click
Display the next page, and accept the values on the current page	**Next**
Display any previous page You may have to retype some of the values you've entered.	**Back**
Exit this package	**Cancel**

The following section displays all of the IExpress Configuration Wizard pages you need to navigate to specify packages. Each page is followed by a table that describes the features and options available on that wizard page.

Creating the Package



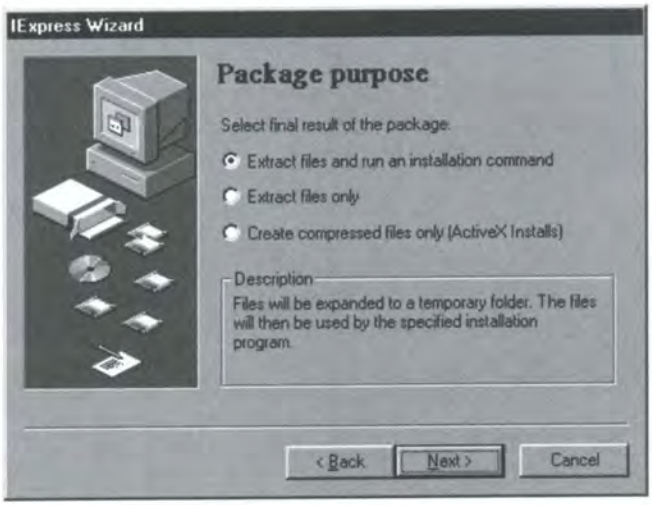
You can create a Self Extraction Directive (SED) file to store information about this application package.

Option	Description
Create new Self Extraction Directive file	To create a completely new SED file for an application, click this option.
Open existing Self Extraction Directive file	To modify an existing SED file or to use an SED file to create another, click this option. Then enter the path and file name, or click **Browse** to locate it.



This page appears only when you open an existing SED file from the Welcome page.

Option	Description
Create Package	Select this option to create a package, just as you would at the end of this process.
Modify Self Extraction Directive file	Select this option to modify the SED.



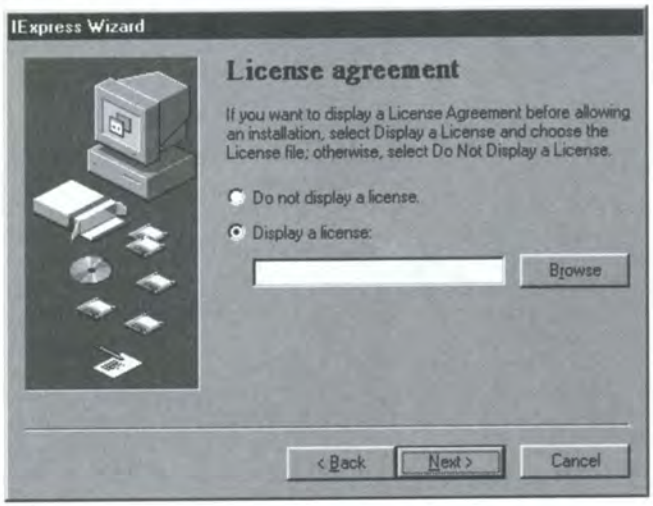
Option	Description
Extract files and run an installation command	Select this option if you want the package to consist of compressed files and an installation program.
Extract files only	Select this option if you want only files compressed.
Create compressed files only (ActiveX® installs)	Select this option if you want the files to be compressed into a .cab file.



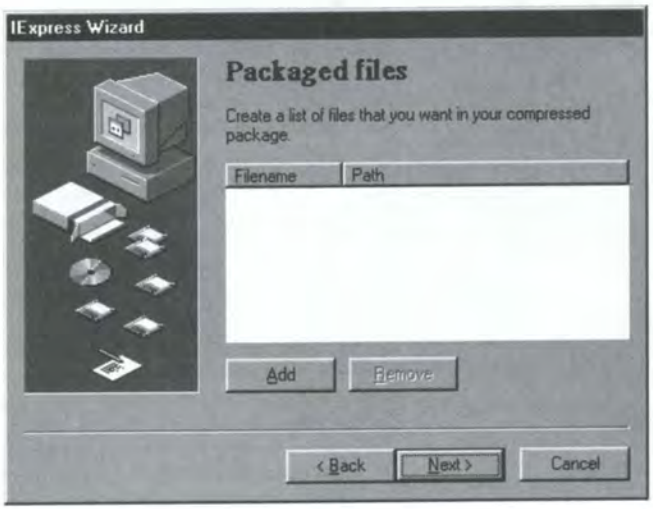
Option	Description
Type Package title	Type the title that you want to appear on all of the dialog boxes.



Option	Description
No prompt	Select this option when you do not want end users to see a confirmation prompt.
Prompt user with	Select this option to display a confirmation prompt, then enter the text you want the end user to see.



Option	Description
Do not display a license	If the software in this package does not need to be licensed to the end user, select this option.
Display a license	When the software in the package needs to be licensed to the end user, select this option. Then, enter the full path and file name for the license agreement, or click **Browse** to locate it.

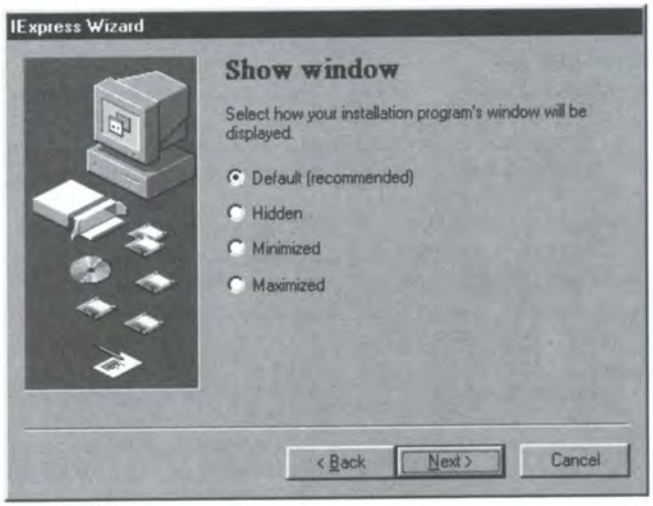


Option	Description
Enter filename and path	Click **Add**, then select the files you want in the package. To remove a file from the package, click **Remove**.



This page appears only if you have chosen **Extract files** and then run an installation command on the second screen of this wizard (**Package Purpose**).

Option	Description
Install Program	Select the program or .inf file that you want this package to launch.
Post Install Command	If you want to execute a command after this package's launch is complete, enter the command or select it.



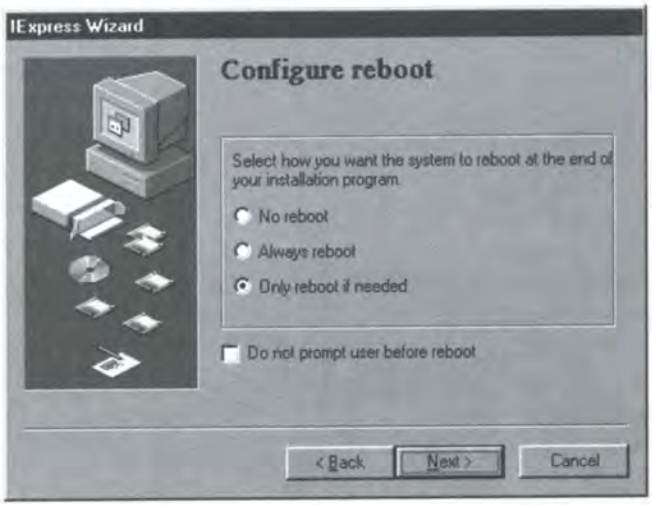
Option	Description
Default	Click this option to display the installation's window to the end user.
Hidden	Click this option to hide the installation's window from the end user.
Minimized	Click this option to display a minimized window to the end user.
Maximized	Click this option to display a maximized window to the end user.



Option	Description
No message	Click this option if you do not want to display a message that tells the end user that the installation is finished.
Display message	Enter a message that you want displayed to the end user after the installation is finished.



Option	Description
Enter target path and filename	Enter the path and file name of the file to which the application should be installed on the end-user's computer, or click **Browse** to locate the path and file.
Hide File Extracting Progress Animation from User	If you do not want to display progress indications to the end user, select this check box.
Store files using Long File Name inside Package	If you want to use long file names in this package, select this check box.



This page appears only if you have chosen **Extract files** and then run an installation command on the second screen of this wizard (**Package Purpose**).

Option	Description
No reboot	Click this option if you do not want the computer to be restarted after the installation.
Always reboot	Click this option if the computer must be restarted after the installation.
Only reboot if needed	Click this option if the computer may or may not need to be restarted after the installation.
Do not prompt user before reboot	Select this check box if you do not want to inform the user that the computer will be restarted. You should select this option whenever the end-user's installation is silent.



Option	Description
Save Self Extraction Directive (SED) file	To save the SED file, click this option. Then enter the full path and file name, or click **Browse** to locate it.
Don't save	To abandon this SED file, click this option.



The IExpress Configuration Wizard displays this page to give you a last chance to save the package you've created. Once you click **Next**, the IExpress Configuration Wizard creates the package files as you specified.

Signing Package Files

Digital signatures identify the source of programs and guarantee that the code hasn't changed since it was signed. Depending on how users' browser-security levels are configured, users could be warned not to download files that aren't signed, or could be prevented from downloading them. Therefore, you should digitally sign the .cab files created by the IEAK Configuration Wizard and any custom components you include.

Signing .cab files and custom programs requires two steps: obtaining a digital certificate—from a Certificate Authority (CA) such as VeriSign or GTE—and signing the code.

Now that you have created the package, you must sign it; otherwise, Active Setup will not install it. For more information about signing your files, please see the "Signing Your Programs" section of the IEAK Help.

Index

/# switch (ACME Setup) 713
/## switch (ACME Setup) 713
./? switch (ACME Setup) 713
+ operator (JScript 3.0) 437
== operator (JScript 3.0) 437
128-bit Server Gated Cryptography, installing 721, 798
304 (not modified) response 192
3-D borders, customizing (WebBrowser Control) 141
3-D effects, Dynamic HTML 405
8004004 error code (Active Setup) 15
800bxxxx error code (Active Setup) 15
800Cxxxx error code (Active Setup) 15
80100003 error code (Active Setup) 15

A

/a switch (ACME Setup) 714
<A> HTML tag 767
absolute positions, of HTML elements 405
Abstract Windows Toolkit (AWT) 423
<ABSTRACT> XML tag 217
Access to all network addresses (Java permission) 500
Access to all files (Java permission) 500
accessibility
  blind users 549–550
  cognitive impairments 553–554
  hearing impairments 551–552
  hearing impairments 578
  Internet Explorer 3 features 547
  Internet Explorer 4
    enhancements 546–547
    enhancements xvii
    upgrading to 548–549
    version 4.0 vs. version 4.01 544
  language impairments 553–554
  low-vision users 550–551
  Microsoft NetMeeting 579
  Microsoft Windows Keyboard Guide Web site 559
  physical impairments 552
  resources 554–556
  seizure disorders, users with 553
  system caret movement 576
Accessibility dialog box
  High Contrast color scheme, selecting 574
  style sheet usage, specifying 569
  style sheet usage, specifying 570
  Web-page formatting, overriding 567
Accessibility Options icon, Windows Control Panel 574
Accessibility Properties dialog box, Windows Control Panel 551–552
ACME Setup engine
  command-line switches 711–714
  core files, uninstalling 76–77
  Destination Folder dialog box 36
  IE4 Setup Log file 42–43
  installation, completing 40–41
  interrupted during OLE file update 39
  item installation phase 37–39
  launching 36
  maintenance mode uninstall 78
  signed .cab files 32
activatePrivilege method 493–495
Active Channel Properties dialog box 230–233
Active Channel Selection dialog box, Setup Wizard 22
Active Channels
  See also Active Desktop; CDF (Channel Definition Format) files; Channel bar; software distribution channels
  ActiveX controls 219, 223, 232
  channel screen savers 214, 225
  connection time, minimizing 228
  deleting from Channel bar 793
  design guidelines 221, 228–229
  download options 230–232
  downloadable file size, limiting 232, 236
  full screen display 576
  interface, disabling 237–238
  Internet Explorer 4, Software Updates channel 70–71
  language, selecting 22
  link-crawl architecture 215–216
  on deployed browsers
    locking down 235–238
    managing 239–240
    pre-configuring 234, 646–647
  overview 187–188, 210–211, 212–213
  personalized channels 225–229
  red gleam 213, 697
  Software Updates channel 70–71
  subscribing to 229
  support content 219, 223
  ToolTips 217
  updating
    e-mail updates 213, 219, 223, 746–747
    publisher's update schedule 217, 223–224, 233
    schedules, specifying in CDF files 217, 223, 765
    update notification 213, 746–747
  usage statistics 219

Active Data Object (ADO) components 772
Active Data Object Recordset (ADOR) components 772
Active Desktop
See also Active Channels; Windows Desktop Update
accessing from Start menu 151
Active Desktop gallery Web site 180
applications of 213–214
channel screen saver, adding 179
Custom-Build Checklist 782
design guidelines 182–185
expiration dates 184
historical background 174
items
adding to desktop 180
development process 182
disabling or deleting 181
in CDF files 185–186, 224
keyboard navigation 562
layered architecture 175–176
linked objects, caching 182, 185
making available to users 186
offline browsing 182–183
on deployed browsers
locking down 181
managing 239–240
pre-configuring 234–235
overview xxx–xxxi, 143–144, 174–175, 213–214
registry entry 175
relation to Webcasting 176–177
representation in Desktop.htm file 175
resetting using Safemode.htt file 170
security settings 458, 462
silent installation 633
subscribing to 180, 229–230
troubleshooting
during offline browsing 742–743
image downloads 748
images 741
not found by Internet Explorer 4 744
wallpaper 744
wallpaper
customizing 178
overview 174
samples on CD 178–179
troubleshooting 744
Active Desktop gallery Web site 180
Active Desktop item Subscription Wizard 186
Active Desktop Properties dialog box 178
Active Document servers 174
Active scripting (security option) 450, 460
Active Scripting xlii, 396
See also ECMAScript; Microsoft JScript 3.0; VBScript
Active Setup
See also ACME Setup engine; Active Setup log file; Active Setup Wizard
Add/Remove dialog box 62–63, 69, 74
Autorun screen, configuring 630, 775
custom components, adding 626–627, 774
custom packages 617, 634
customizing 628–638, 774–775
disk-space check 24, 28
download sites, configuring 624, 635, 775
installation folder, specifying 637
Internet Explorer 4 components, synchronizing 625
latest version, ensuring installation of 636
overview xviii–xix, 8–9
parameters, specifying 622–627, 774
running 669
running 5
silent installation, configuring 633
software distribution packages 700
specifying for software distribution channels 699
troubleshooting 669
Windows Desktop Update installation, configuring 638
Active Setup log file
Active Channel language entry 22
destination folder path entry 23
Download Options entry 18
error codes 15
installation option entry 20
selected download region entry 27
Windows Desktop Update installation entry 21
Active Setup Wizard
Active Channel Selection dialog box 22
.cab files downloaded 31–32
.cab files, downloading 30
.cab information file, downloading 28–29
command-line switches 16
custom icon 615
customizing 631, 775
Destination Folder dialog box 23–24
Download Options dialog box 18
Download Sites dialog box 26–27
errors
.cab files, downloading 31
download phase 28–29
insufficient disk space 24
proxy errors 25–26
trust errors 31
Installation Option dialog box 19–20
launching 10–11, 16–17
License agreement dialog box 17
manual installation 33
Setup folder, preparing 29–30
Smart Recovery 34
system configuration 40

Active Setup Wizard bitmap path
(Configuration Wizard setting) 631
Active Setup Wizard title bar text
(Configuration Wizard setting) 630
Active Stream Redirector *See* .asx files
ActiveX conferencing platform, NetMeeting 342
ActiveX controls
adding scriptlets to 412
adding to Web pages 378, 382, 416
apartment-model controls 415, 769
controlling downloads 198, 232
damaged controls 418
data source objects 408–409
dependencies 418
digital signatures 419, 458
in Active Channels 219, 223
in Active Desktop items 175, 224
informational Web site 183
Java Bean integration 423
location of 416
MFC .dll files 769
multimedia controls 419–420
NetMeeting control 369
NetShow file-transfer control (nsfile.ocx) 311
NetShow Player 288, 325–326
object safety 459
offline functionality 182–183
overview xli, 395, 414–415
performance 415, 769
properties, viewing 416–418
referencing in Web pages 416
removing 418
Safe for Scripting, troubleshooting 769
scriptlet security 412
security settings 449
signing 183
uninstalling 737
updating 418
version information, displaying 418
ActiveX Controls and Java applets
(site subscription setting) 196–198
ActiveX Data Objects (ADO) 386
ActiveX files
checked by Setup Wizard 17
download location, changing 738
Activity log, Personal Web Server 390
Actsetup.exe 710–711
Add Active Channel dialog box 229
Add Favorite dialog box 193
Add folder (Configuration Wizard setting) 644
Add New Root (Configuration Wizard setting) 657
Add URL (Configuration Wizard setting) 644
Add/Remove Programs applet, Control Panel 62–63
adding
channel screen savers 179
components from CD-ROM 66–67
components from the Internet 64–66
custom components 626, 774
Windows Desktop Update 69–70
Address (proxy server setting) 94
Address bar
accessibility benefits 547
adding to desktop 158
AutoComplete feature 100–102
AutoDomain Searching feature 102–103
displaying 559
implementing in custom browser 139
keyboard navigation 562
overview 153, 650
Address Book, Outlook Express
See also LDAP
adding digital IDs 277
importing data from other mail
applications 262–263, 751
LDAP directories, configuring and maintaining 264–266
overview 256, 260
Address Options dialog box, Microsoft Wallet 538–540
addresses *See* personal information, Address Book,
Outlook Express
.adm files 685, 686, 687
Admin quiet mode 708
ADO (Active Data Object) components 772
ADO (ActiveX Data Objects) 386
ADOR (Active Data Object Recordset) components 772
Advanced Add/Remove dialog box 74–75, 81
Advanced Data Connector (ADC) *See* Remote Data Service
Advanced Download Options dialog box 197–198, 231–232
advanced Java permissions editor dialog boxes 503–505
Advanced Options page, Personal Web Manager 389–391
Advanced tab
Content Advisor dialog box 525–527
Internet Options dialog box
accessibility settings 575, 576
advanced browser options 121–125
blind users, accessibility settings 550
cognitive and language impairments,
accessibility settings 554
Font button, displaying 568
HTTP 1.1, enabling 130
Java VM options, configuring 426
keyboard navigation 575
low-vision users, accessibility settings 551
physical impairments, accessibility settings 552
privacy security options, configuring 541–542
users with seizure disorders, accessibility
settings 553
advertising, using NetShow 292

Advpack.dll file 11, 14, 79
AFC (application foundation classes) 423
AFC Enterprise Libraries 423
AINF0000 files 76
AlignLeft/AlignRight parameters, FileList control 169
alt text (alternate text) display settings 576, 578
ALT+C (Help tool navigation) 562, 563
ALT+D (Help tool navigation) 565, 566
ALT+F4 (Help tool navigation) 564
ALT+I (Help tool navigation) 562, 563, 564, 565
ALT+K (Help tool navigation) 566
ALT+L (Help tool navigation) 565
ALT+LEFT ARROW (Internet Explorer 4 navigation) 558
ALT+S (Help tool navigation) 562, 565
ALT+T (Help tool navigation) 566
ALT+TAB (NetMeeting navigation) 580
Always accept cookies (privacy setting) 542
Always On Top (toolbar option) 154
ambient properties, WebBrowser control 137
Amount of disk space to use (cache setting) 133
animation 578
animations, browser performance 134
announcements, NetShow 300–301, 307, 309
anonymous logon, enabling 461
apartment-model controls 415, 769
<APPLET> tag 428
applets *See* Java applets
application foundation classes (AFC) 423
applications, adding scriptlets to 411–412
application sharing, NetMeeting
  keyboard shortcuts 580
  overview 331
  version 2.1 support 336
application testing, using Personal Web Server 392
application/x-cdf MIME/content type 225, 226
architecture
  Active Desktop interface 174–176
  browser architecture 136–138
  LDAP 351
  link-crawl architecture 191–192, 215–216
  NetMeeting 339–342
  Outlook Express 258
  security zones 450
  True Web Integration 145
  Web View 164
array handling (JScript) 432, 434
arrow keys 565
  See also DOWN ARROW key; LEFT ARROW key; RIGHT ARROW key; UP ARROW key
.asc files 303
ASCII characters, encoding in CDF files 764
.asd files 305
ASF (Active Streaming Format) 295, 303
  See also .asf files; ASF streams
ASFChop editor, NetShow 320
.asf files
  See also ASF (Active Streaming Format); NetShow Player
  ASF Editor tool 319–320, 321
  ASFChop editor 320
  bandwidth, selecting 317–318
  bit rates 295
  building 318
  generated by Real-Time Encoder 305–306
  HTTP streaming 311
  including script commands in 317
  including URLs in 317
  local, opening 324
  locating on NetShow Server 300
  making available to users 322
  Microsoft PowerPoint presentations 320
  playing 300
  remote, opening 324
  requesting using .asx files 300–301
  seekable files, creating 320
  streaming protocols 301–302, 311–313
ASF streams
  distribution servers 309–310
  generated by Real-Time Encoder 305
  live streams 304–307
  stored content, creating 315–322
  stored streams 306–309
ASP (Active Server Pages)
  Browser Capability component 771
  dynamically generated CDF files 225–228
  ILS customization 358
  redirect pages, Personal Web Server 390–391
  scriptlets 410
  subscribing to 764
assignments (JScript) 432
.asx files
  for distribution servers 310
  links in Web pages 300–301
  overview 300
  playing .asf files 322–324
  stored ASF streams 306–309
attachments, troubleshooting 752–753
.au files 762
audio conferencing, NetMeeting
  H.323 standards 348–349
  overview 330, 356
  restricting 365–366, 368
  through firewalls 360
audio content, NetShow
  ASF Editor tool 319, 321
  bandwidth 313–314, 317–318
  codecs 282, 293–294, 321–322
  data rate (bit rate) of files 293
  editing 318
  in .asf files 316

audio content, NetShow *(continued)*
including in .cab files 762
live content, multicasting 314
masking 296
Real-Time Encoder 290
WavToAsf tool 318–319, 321
Audio tab, Options dialog box 366
audio/video throughput limit, Average
(NetMeeting setting) 367
authentication
See also digital certificates
client/server communications 474
overview 441
Secure Password Authentication, configuring for deployed browsers 661
user authentication settings, security zones 450, 461, 532
Windows NT Challenge Response 461, 477
Authentication type (Configuration Wizard setting) 662
Authenticode
Authenticode 1.0 442
Authenticode 2.0 442, 473–474
configuring for deployed browsers 657
Java security 442–443
overview 471–473
Web site 12
Authenticode Security Technology dialog box 482, 484, 487
authorities, configuring for deployed browsers 657
Auto (software distribution channel schedule setting) 703
Auto-Add feature, Outlook Express 256
AutoArrange parameter, FileList control 169
AutoComplete feature
accessibility benefits 546
enabling 577
keyboard shortcuts 102, 560
overview xx–xxi, 100–102
auto-configuration files
creating 677
install.ins file, using as template 687
managing using Profile Manager 688
auto-configuration servers 679
Auto-configure every __ minutes
(Configuration Wizard setting) 654, 674–675
Auto-configure URL
(Configuration Wizard setting) 654, 674–675
AutoDomain Searching feature 102–103
AutoHide (toolbar option) 154
AUTOINSTALL element, CDF files 698
automated installation 46
automatic browser configuration
after browser deployment 673, 679–681
auto-configuration interval 654, 674, 675
auto-configuration servers 678–679
auto-proxy files 678
before browser deployment 673–679
automatic browser configuration *(continued)*
.cab files 676–677
custom packages 674–675
deployment planning 599
distribution files, updating 681
Favorites folder, editing 115
for deployed browsers 654–655
.inf files 677
.ins files 676–677
locking down 675–676, 686
overview 582, 672–673
software distribution channels 694, 705–706
Automatic Browser Configuration
(Wizard Settings option) 684
Automatic Browser Configuration page
(Configuration Wizard) 653–655, 777
Automatic Configuration URL 47–48
automatic logon, enabling 461
automatic setup option,
(Internet Connection Wizard) 89–92
Automatic Version Synchronization
(AVS) 597, 620, 624, 774
auto-proxy files, creating 678
Auto-proxy URL
(Configuration Wizard setting) 654, 674, 675
AutoReply option, Outlook Express 800
Autorun screen, customizing 597, 615, 629–630, 774
Autoscan common root domains (search setting) 125
AutoSize parameter, FileList control 169
AutoSizePercentage parameter, FileList control 169
Average audio/video throughput limit
(NetMeeting setting) 367
.avi files 315–316
AVS (Automatic Version Synchronization) 597, 620, 624, 774
AWT (Abstract Windows Toolkit) 423

B

/b switch, (ACME Setup) 711
Back button
Configuration Wizard 618
drop-down menus xxi, 103
backgrounds
bitmaps
Autorun screen 615, 630
toolbar background 615, 794, 798
color
formatting in style sheet 568
printing 579
selecting 571–572
custom, in deployed browsers 615–616, 630
images, troubleshooting 756

backup files
deleting, effect on Internet Explorer 4 uninstallation 75–77
required to run IERemove.exe 83
System.1st backup 39
bandwidth
ASF Editor tool 319–320
audio content 318
channel hierarchy design 221
distribution strategy planning 595
for .asf files, selecting 317
for NetMeeting, limiting 367, 368
Intranet bandwidth 317
multicasting 296–299
NetShow content, adjusting 320–322
overview 293
specialized networks 317–318
unicasting 296–297
BASE attribute, <CHANNEL> tag 217
base URLs, for channels and subchannels 217
basic Webcasting
See also Web site subscriptions
features 190
link-crawl architecture 191–192
overview xxxiii, 187–188
Behaviors control (DirectAnimation) 420
billing addresses, storing 535, 538–539
bind addresses (Java applet permission) 511
Bind List Log.text file 40
bitmaps, custom
Active Setup bitmap, dimensions 798
Autorun screen 615, 630
for custom packages 615–616
toolbar bitmap 794, 798
bit rate 293, 295
blend filters 406
blind-access utilities
alt text display settings 576, 577, 578
audio clips 578
browser options 577
system caret movement 575
Windows Desktop Update, interaction with 549
blind users 549–550
See also accessibility; low-vision users
.bmp files 316
See also bitmaps, custom
boolean values (JScript) 432
branding options, browsers 598, 793
bridges, NetMeeting compatibility 356
broadcasting 283–286, 296
See also multicasting, NetShow; unicasting, NetShow
Browse in a new process (browser setting) 123
Browser Capability component 771
Browser Channel bar icon, customizing 696–697
browser controls *See* WebBrowser Control, browsers
Browser Only (Setup Wizard installation option) 19
browsers
See also Active Desktop; Internet Explorer 4; WebBrowser Control
architecture 136–138
branding options 598, 793
capabilities, determining 771
custom, creating using WebBrowser control 139–140
customizing using Configuration Wizard 639–660, 776–780
full screen display 577
language conflicts with operating system 9, 720–721
optimizing 130–134
redirecting 756
version number, determining 771
Browser Title (Wizard Settings option) 684
Browsing options, Internet Options dialog box 122–123, 576–577
Business tab, Profile Assistant 538
buttons, custom 615–616
Button style color (Configuration Wizard setting) 630
Bypass proxy server for local (intranet) addresses (proxy setting) 95

C

/c switch
ACME Setup 711
Actsetup.exe 710
WExtract utility 13, 707, 708
Cabarc.exe 759, 760, 762
CAB Developers Kit (Web site) 759
.cab files
See also trust-based security, Java
adding components from the Internet 66–67
auto-configuration files, signing 496, 678
automatic browser configuration 677
certificate display, troubleshooting 762
compression and packaging 425
configuring for Active Setup 626
created by Configuration Wizard, signing 814
digital signatures 10, 760–761
for custom browser packages 666
Frequently Asked Questions (FAQs) 759–762
Internet Explorer 4 support for 422
missing, for local reinstallation 68
OSD files, packaging 701
overview 10
Package Manager 424
permission signing 492–493, 496
policies and restrictions settings 685
referencing in Web pages 428
reinstalling components 67–68
trust-based security 428

.cab files *(continued)*
used in Setup process
corrupted, troubleshooting 6
downloaded for Windows Desktop Update 21
downloading during Active Setup 30–32
IE4Setup.exe, files extracted from 10–11
version number, inserting 761
WExtract utility 10
Cabinet files *See* .cab files
.cab information file, downloading 30–31
CAB Resource Kit 759
Cache Container Tool 120
cached resources
Active Desktop items 742–743
cache settings 132–133
CD caching 120
file history 116
Java applets, pre-caching 182
manually updating 133
not visible in Channel bar 765
storage of 120
subscription content 764
updating during online sessions 764
calendar program, selecting default 126
call stack, Java permission scoping 494
call windows, NetMeeting 333
Calling tab, Options dialog box 365
Cancel button (Configuration Wizard) 618
CANRESIZE attribute, <USAGE> tag 224
capability signing 443
CAs (Certificate Authorities)
See also certificate servers; digital certificates
Certification Practices Statement (CPS) 470
configuring for deployed browsers 657–658
issuer types 480
overview 468
root certificates, configuring 479–480, 484, 487
selection of 470
services provided 469
trusted CAs
designating 481, 484, 487
removing 482, 484, 487
types of certificates 469
cascaded topology *See* topologies
Cascading Style Sheets
background images, troubleshooting 755–756
.css files 569
cursor attribute 767
external style sheets 402
font embedding 403–405
overview 401–402
STYLE attribute 402
STYLE blocks 402
cdcache.exe 120
CD Caching utility 120
CDF (Channel Definition Format) files
See also Active Channels
Active Desktop items 185, 224
ASCII character encoding 764
channel hierarchy 212
channel screen savers, designating 225
creating 216–229
desktop items 766
dynamically generated 225–228
e-mail notification, specifying 746
examples of 186, 220–222
expiration date, defining 184–185
format of 215
generating using ASP 226–228
items, pointing to 218
logo for channel 218
MIME type 763
MIME/content type 225
personalized channels 225–228
referencing from Web pages 186
software distribution channels 690, 697–699
statistics, logging 219, 238
subchannels, creating 216
ToolTip text 217
update schedules 217, 223, 765
updating content not visible in Channel bar 765
URLs, referencing 218
usage types, specifying 219, 221, 223
user access to 799
CDF link-crawl architecture 215–216
CDF specification, Web site 691, 799, 802
Cdfview.dll 216
CD-ROM installation, custom packages
Autorun screen, customizing 629–630, 774
Autorun screen, customizing
custom buttons 615
distribution files 668
distribution strategy planning 594–596, 597
installation options 19–20, 36–40
installation process 36
CD-ROM, Internet Explorer 4 Resource Kit
HTML wallpaper samples 178–179
Web View sample applications 163
Certificate Authorities *See* CAs (Certificate Authorities)
certificate servers 471
Certification Practices Statement (CPS) 469
Change Supervisor Password dialog box 525
Channel bar
custom graphics and icons 615
deployed browsers, configuring 118
icons, customizing 696–697
keyboard navigation 562
offline browsing 121
overview 118

Channel bar *(continued)*
software distribution channels 693–694
<USAGE> tag 222
Channel Definition Format files *See* CDF (Channel Definition Format) files
Channel Guide 22
Channel Manager, NetShow Administrator 300–304
channel screen savers
adding to Active Desktop 179
designating in CDF files 225
overview 214
support content, downloading 225
Channel Settings object
Active Channel subscription options, locking down 236–238
subscription options, locking down 203–206
<CHANNEL> tag 185, 216–217, 221, 698
channels
See also Active Channels; Channel bar; NetShow channels; software distribution channels
base URLs 217
e-mail delivery 254
hierarchy 212
order of 798
removing 798
secure channels 474–477
Channels and Subscriptions Settings (Custom-Build Checklist) 788
Channels folder, Favorites bar 113
channels.htm resource, IE4tour.dll 138
channels, NetShow *See* NetShow channels
Channels Settings (Custom-Build Checklist) 790
Chat feature, NetMeeting 332, 580
Check for certificate revocation (security setting) 124, 542
Check names against this server... (Configuration Wizard setting) 662
checklists
Custom-Build Checklist 614, 773–791
deployment testing 604
CheckSum, installing .cab files 38
CLASSID (ActiveX controls) 416, 417
class libraries *See* Package Manager, Java
Client Authentication dialog box 480–481
client certificates, importing 480–481
clientHeight property 767
client programs 126–128
client/server communications
CryptoAPI 2.0 477
firewall support 477
overview 474
secure channels 474
Server Gated Cryptography (SGC) 475–477, 721
Windows NT Server Challenge Response 477
client/server configurations, deployment planning 590
client services (Java applet permissions) 512–513
Client Services tab, Edit Custom Permissions dialog box 511–513
Client storage settings (Java permissions) 512
clientWidth property 767
Clipboard, Windows
applet access to 513
sharing, in NetMeeting 332
clock synchronization 192
CLSID (ActiveX controls) 416, 417
CODEBASE attribute, Nsplayer.ocx control 326
CODEBASE element, packaging OSD files 701
codecs
adjusting content for bandwidth 320–322
codec independence 294
included with NetShow 282–283, 294
informational Web site 294, 322
overview 293
code signing
See also Authenticode
auto-configuration files 677
.cab files 10, 759, 760–761
CryptoAPI 2.0 477
custom packages 626, 813–814
software distribution packages 701
Code Sign Kit, obtaining 759
cognitive impairments
accessibility settings 553–554
Browsing options 576, 577
multimedia settings 552
collaboration, using NetMeeting 337, 371–372
See also Microsoft NetMeeting
color blindness *See* vision impairments
Color dialog box 572, 573
color palettes, Active Desktop items 184
colors
custom colors, creating 573
formatting in style sheet 568–570
high-contrast color scheme, selecting 573–574
hover color, selecting 573
hyperlinks, selecting 572
overriding Web-page formatting 567
text and background colors, selecting 571–572
Colors dialog box 571–574
Colors options, Internet Options dialog box
cognitive and language impairments, settings for 554
low-vision users, accessibility settings 551
COM (component object model)
and ActiveX controls 414
and Java 414
Internet Explorer 4 support for 422
Java integration of 425
Command (Configuration Wizard setting) 626
comments (JScript) 432
commercial CAs 469–470
communications, corporate, using NetShow 292

Compact Disc *See* Internet Explorer 4 Resource Kit CD
Company name (Configuration Wizard setting) 620
compatibility issues
  deployment planning 591, 593
  Web pages 593
Completions option (Address bar shortcut menu) 100–102
Component (Configuration Wizard setting) 626
component installation options 588, 598, 775, 800
components
  See also components, Internet Explorer 4
  ADO components 772
  custom
    adding to Active Setup installation 625–627, 774
    allowing uninstallation 627
    including in custom packages 617
    MFC .dll files 768
  installed with Internet Explorer 3, uninstalling 798
  installing during ACME Setup 37–39
  Personal Web Server, optional components 386–387
  WebBot components 381–382
Components Download page 65–66
components, Internet Explorer 4
  See also components
  adding 64–66, 66–67
  configuring for deployed browsers 660–665
  extracting using IExtract.exe 69
  included in standard installation suites 588
  installation options 588, 598, 775, 800
  not included in installation options 65–66
  optional components 795–797
  reinstalling 67–68
  removing 63
  troubleshooting
    installation of 38–39, 724
    reinstallation of 68
  uninstalling 74–75
  updating 70–72, 624
  version requirements 75, 735
  Windows Desktop Update, adding and removing 69–70
Components to install (Configuration Wizard setting) 634
compression/decompression algorithms *See* codecs
conditional compilation (JScript) 434
conferencing *See* Microsoft NetMeeting
conferencing servers, NetMeeting compatibility 355–356
conferencing standards, NetMeeting
  H.323 standard 348–349
  LDAP 350–353
  overview 335, 343
  standards organizations 344
  T.120 standard 344–347
configuration, automatic
  See also automatic browser configuration
  Active Channels, managing 239–240
  Active Desktop items, managing 239–240
  deployment planning 599
Configuration identifier (Configuration Wizard setting) 636
Configuration Wizard *See* IEAK Configuration Wizard
Configure reboot page (IExpress Wizard) 812
Confirmation prompt page (IExpress Wizard) 807
connect addresses (Java permission) 511
Connection object, Profile Manager 676
connections *See* Internet connections
Connection tab
  Internet Options dialog box
    automatic browser configuration settings, locked down 676
    Automatic Configuration URL, selecting manually 48
    Internet Connection Wizard, launching 87
    proxy bypass settings 95–96
    proxy servers, configuring 93–95
    setting up browser for automatic configuration 679–681
  Options dialog box 452
constants (JScript) 432
content *See* Webcasting; support content
Content Advisor
  See also rating systems
  content rating systems 520–521
  enabling and disabling 522–523
  in deployed browsers
    locking down settings 528
    pre-configuring 526–527
    updating settings 529–530
  overview 520
  PICS rating standards 520, 521
  rating systems, importing 525–526, 527
  ratings categories, configuring 523
  restricted content, configuring access to 522, 524–525
  restricted content, configuring access to
  RSACi content rating system 520–521
  supervisor password 522, 524–525
  unrated sites, configuring access to 524
Content Advisor dialog box
  Advanced tab 525–526, 527
  General tab 524–525, 527
  Ratings tab 523, 527
content, NetShow
  adjusting for bandwidth 320–322
  .asf files, building 318
  audio content, creating 316
  bandwidth selection 317–318
  content-creation tools 318–320
  distributed delivery 286
  images, creating 316
  overview 315
  script commands 317
  URLs 316
  video content, creating 315–316

Content object, System Policies and Restrictions hierarchy 528
content pane 108
content rating tags 184
content ratings xliv, 440
See also Content Advisor
Content tab, Internet Options dialog box
Certificate Authorities dialog box 479–480
Client Authentication dialog box 480–481
Content Advisor 522–523
digital certificates, configuring 478
Microsoft Wallet, configuring 538–541
Profile Assistant, configuring 537–538
trusted publishers and CAs, removing 482, 484, 487
Content.inf file 11
Contents list, Help tool 563–564
context menus, customizing in WebBrowser Control 141
contrast sensitivity impairment *See* vision impairments
control flow (JScript) 432, 434
Control Panel
Accessibility Properties dialog box 551
Add/Remove Programs applet 63
Services dialog box 312
sound events 107
Sounds Properties dialog box 550, 551
Users icon 55–57
Web View, configuring for deployed browsers 651
Control Panel folder, customizing 170–171
controlled information delivery
See also Microsoft NetShow
managed Webcasting 210–211
true Webcasting 241
vs. Web site subscriptions 207
Controlp.htt file 164, 170, 651
controls *See* ActiveX controls
cookies 124, 225, 532–533, 542
cookies (security settings) 124, 542
copy and paste activities (security settings) 450, 462
Corporate Administrator role 596
corporate communications, using NetShow 292
corporate information delivery, using NetMeeting 372–373
CPS (Certification Practices Statement) 469
crawl depth 197, 204, 206
credit card information, storing 536, 540
Cryptographic Service Provider (CSP) 477
.css files 569
See also Cascading Style Sheets
CTRL key (AutoComplete feature) 560
CTRL+D (NetMeeting navigation) 580
CTRL+ENTER (AutoComplete feature) 102, 560
CTRL+F (NetMeeting navigation) 580
CTRL+F10 (Help tool navigation) 564, 565, 566
CTRL+L (NetMeeting navigation) 580
CTRL+LEFT ARROW (AutoComplete feature) 102
CTRL+N (Internet Explorer 4 navigation) 559
CTRL+N (NetMeeting navigation) 580
CTRL+P (Internet Explorer 4 navigation) 559
CTRL+Q (Internet Explorer 4 navigation) 558
CTRL+RIGHT ARROW (AutoComplete feature) 102
CTRL+S (Internet Explorer 4 navigation) 559
CTRL+SPACEBAR (desktop icon navigation) 562
CTRL+T (NetMeeting navigation) 580
CTRL+TAB (Internet Explorer 4 navigation) 558
CTRL+TAB (NetMeeting navigation) 580
CTRL+W (NetMeeting navigation) 580
Current Call list, NetMeeting 580
current record binding (data presentation) 409
cursor attribute, Dynamic HTML 767
Custom background bitmap location (Configuration Wizard setting) 630
Custom-Build Checklist 614, 773–791
Custom button bitmap (Configuration Wizard setting) 630
custom colors, creating 573
Custom Component Install page (Configuration Wizard) 632, 775
Custom Components Installation Title (Configuration Wizard setting) 631
Custom Java Security dialog box 459, 498, 499–501
custom packages
See also automatic browser configuration; deployed browsers; IEAK Configuration Wizard
automatic browser configuration, setting up 673–675
Automatic Version Synchronization (AVS) 593, 620, 624, 774
bitmaps, custom 615–616, 798
building 608, 614–617
configuration 596–601
Configuration Wizard 617–637
custom components, including in 616
deploying 608
distributing 614–615
distribution files 667–668
distribution servers 615
generating 666
installation packages, configuring 633–634
Online Support option (Help menu), default Web page 613
signing package files 666, 813–814
software distribution channels 702–704
custom permissions, Java applets 517
Custom Security Settings dialog box 404
Custom string to be appended to user agent string (Configuration Wizard setting) 652, 794
Custom tab, Edit Custom Permissions dialog box 516–517
custom templates
See also template files
FrontPage Express 381
stationery templates 255, 271–274

custom toolbars
background bitmaps 615, 794, 798
creating 158–159
design guidelines 157, 794
keyboard navigation 562
New Toolbar command 154
pre-configuring in deployed browsers 159–160
customer service, using NetMeeting 337
Customization code (Configuration Wizard setting) 620
customization key, IEAK 614
Customize Desktop Toolbars page (Configuration Wizard) 159, 650, 777
Customize Software Update Channels page (Configuration Wizard) 648, 703, 777
Customize the Active Channel bar page (Configuration Wizard) 234, 646–647, 776
Customize the Active Setup Wizard page (Configuration Wizard) 630, 775
Customize the Autorun Screen for CD-ROM Installations page (Configuration Wizard) 629–630, 775
Customize the Start and Search Pages page (Configuration Wizard) 642, 776
Customize the Welcome Message and Desktop Wallpaper page (Configuration Wizard) 645–646, 776
Customize the Window Title and Toolbar Background page (Configuration Wizard) 641, 776
Customize Title Bars (Configuration Wizard setting) 640
Customizing the Browser (Configuration Wizard) 639–660, 776–779

D

/d switch (WExtract utility) 707
Daily (software distribution channel schedule setting) 704
daily updates to subscribed sites 201
daisy-chain topology *See* topologies
damaged controls 417
.dat files, Outlook Express 259
Data Access Components, Microsoft 386
databases
data binding, Dynamic HTML 407–409
LDAP databases 351
data binding 407, 409
data conferencing 343–350, 355–357, 360
See also Microsoft NetMeeting
Data Form Wizard, troubleshooting 755–756
data rate 293
See also bit rate
Data Source Object Gallery 408
data source objects 407–409
date handling (JScript) 432, 434, 436–437
DCOM (Distributed COM) 422
deaf users, accessibility settings 551–552
debug install 47
declarations (JScript) 433
Declared member reflection (Java permissions) 516
decompression *See* codecs
Delete access (Java applets) 508–510
Delete existing Internet Explorer 4.0 channels (Configuration Wizard setting) 647
delete operator (JScript) 437
Delete saved pages when browser closed (security setting) 124, 542
delimited text files, data source 408
demographic information, Profile Assistant 533–535, 536–538
DEPENDENCY element, CDF files 699
Dependency Tab, Properties dialog box 418
deployed browsers
See also automatic browser configuration; custom packages
Active Channels
locking down 235–238
managing 238–240
pre-configuring 233–234
Active Desktop
locking down 181
managing 239–240
pre-configuring 234–235
automatic browser configuration 653–655
browser title bar, configuring 640
Content Advisor
locking down 527–528
pre-configuring 526–527
updating 528–530
custom toolbars, pre-configuring 159–160
digital certificates
locking down 485
pre-configuring 483–487
updating 486–487
Favorites, configuring 644
Java permissions, customizing 502–517
LDAP, configuring 662
Online Support option, customizing 616, 643
Outlook Express, configuring 661, 663, 664
proxy settings, configuring 655–656
root certificates, configuring 657
Search page, customizing 616
Search Pane, configuring 642
Secure Password Authentication, configuring 661
security zones, pre-configuring 463–466
signatures, configuring 664
software distribution channels
configuring 647–648
locking down 704
start page, customizing 616
technical support during installation 670
trust-based security for Java, customizing 502–517
user agent string, customizing 652–653, 794

deployed browsers *(continued)*
Web site subscription options, locking down 203–206
Welcome page, configuring 645–646
Deployed browsers, SMTP server, configuring 661
deployment planning
See also validating deployment
announcing deployment 612
branding options 598, 793
browser security 599
browser settings, pre-configuring 599
client/server configurations 590
compatibility issues 591–593
component installation options 588, 598, 775, 800
custom package configuration 596–600
distribution media 597, 622, 773, 798
distribution strategies 594–596
e-mail and news programs, configuring 593
e-mail options 600
finalizing 609
migration issues 590–592
news options 600
overview xviii, 581–583, 586
pilot programs 607–608
plug-ins and add-ins 592
project plan, developing 601
project teams 586–587
roles 596–597
security issues 599
setup appearance 598
system policies and restrictions 600
technical requirements 587–588
testing deployment 604–605
user needs 590
user support and training 606–607
validating deployment 604–609
version synchronization 597, 620, 624
Description (Configuration Wizard setting) 634
design guidelines
Active Channels 228–229
Active Desktop 182–185
custom toolbars 157, 794
folder display, Web View 168–169
taskbar 157
Deskmovr.htt file 164
Desktop bar 153
Desktop Channel bar logo, customizing 696–697
Desktop folder, optimizing roaming profiles 52
Desktop.htm file 175
desktop icon layer, Active Desktop interface 175
desktop icons, keyboard navigation 562
Desktop.ini file 165
Desktop object, custom toolbar options, locking down 159–160
desktop settings, (Custom-Build Checklist) 782–784
Desktop toolbar
configuring for deployed browsers 650
customizing 158, 793
keyboard navigation 561–562
overview 650
Desktop Wallpaper (Wizard Settings option) 684
See also wallpaper, Active Desktop
Destination folder (Configuration Wizard setting) 622
Destination Folder dialog box 23–26, 36
Dialogs (Java permission) 500, 501
dial-up connections
for site and channel updates, disabling 205, 238
unattended, troubleshooting 745–746
.dib files 316
digital cash *See* Microsoft Wallet
digital certificates
Authenticode 471–474
Certificate Authorities 468–470
client certificates, importing 480–481
client/server communications 474–477
configuring 478
contents of 468
lifetime of 473
overview xliii, 439, 441–442, 468–469
pre-configuring in deployed browsers 483–487
privacy security settings 541–542
root certificates, configuring 478–480, 484, 486–487
server certificates, SGC 476
Server Gated Cryptography (SGC) 475–477
SGC certificates 477
test certificates 762
uses of 468–469
validity, verifying 472–473
digital IDs, Outlook Express
associating with e-mail accounts 275
encrypted mail, sending and receiving 276–277
Microsoft Internet Explorer Digital ID Web site 275
obtaining 275
overview 274
signed mail, sending and receiving 276
storing in Address Book 276–277
trust status 277
digital signatures
See also code signing; digital IDs, Outlook Express
ActiveX controls 419, 458
Authenticode 471–474
.cab files 10, 760–761
custom packages 814
for custom browser packages 666
in .jar files 422
overview 441
software distribution packages 701
verifying 471–472
DirectAnimation multimedia controls 419–420

directories
See also directory services; folders
created during installation 42
installed with Personal Web Server 387
directory browsing, Personal Web Server 390
Directory list, NetMeeting 580
Directory Server (NetMeeting setting) 366
directory servers, ILS compatibility 357
Directory Service (Configuration Wizard setting) 662
directory services
See also LDAP (Lightweight Directory Access Protocol)
configuring in Outlook Express 264–265
ILS (Internet Locator Service) 332–333, 353
ports required 361
profiles installed with Outlook Express 264
registry data 266
updating 266
Directory Services Order dialog box 265
Directory Services tab, Internet Accounts dialog box 266
DirectX
DirectSound, NetMeeting support 336
multimedia class libraries 423
Disable all cookie use (privacy setting) 542
Disable Internet Explorer 4.0 Welcome window (Configuration Wizard setting) 645
disablePrivilege method 493
Disable script debugging (browser setting) 122
Disables... (site subscription settings, locking down) 205–206
disclaimers, in Outlook Express messages 270
discussion groups, using NetMeeting 373
diskless workstations, Internet Explorer 4 installation 5
disk-space checks, Active Setup 23, 24, 28
Display default...welcome page (Configuration Wizard setting) 645
Display tab, Accessibility Options dialog box 573–574
distance learning, using NetMeeting 338
distribution of custom packages
See also custom packages; software distribution channels
automatic browser configuration 681
deployment planning 594–596
distribution files 667–668
distribution media 597, 621–622, 773, 798
distribution methods 589, 668–669
preparation for 614–615
distribution servers 309–310
DIV element 405
.dll registration problems, troubleshooting 44
DNS names 452
Do not customize channels (Configuration Wizard setting) 647
Do not customize Software Distribution Channels (Configuration Wizard setting) 648
Do not display a welcome page (Configuration Wizard setting) 645
Do not save encrypted pages... (security setting) 124, 542
Do not use proxy server for local (intranet) addresses (Configuration Wizard setting) 656
<!DOCTYPE> tag 764
document collaboration, NetMeeting 337
Document Object Model
ActiveX controls 415
dynamic content in Web pages 406
dynamic styles 403
Java exposure 423
overview 400
scriptlets 410–411
W3C Document Object Model Web page 400
documents, keyboard navigation 558
Documents menu, optimizing roaming profiles 52
Don't update this subscription when I'm using my computer (site subscription setting) 202
DontUseDNSLoadBalancing entry, adding to registry 736
DOWN ARROW key
Advanced tab, Internet Options dialog box 575
AutoComplete feature 102, 560
Contents list (Help tool) navigation 563
Internet Explorer 4 navigation 558
Search tab (Help tool) navigation 565–566
Downloaded Web page folder 53
Download linked pages within a depth of __ (site subscription setting) 197
download options
Active Channel subscriptions 230–232
Web site subscriptions 196–198
Download Options dialog box, Setup Wizard 18
Download Program Files folder 737–738
Download signed ActiveX controls (security option) 449, 458
Download site (Configuration Wizard setting) 624
download sites
Active Setup, configuring 624, 634, 775
Internet Explorer 4 Web site 544
registry entries 27
silent installation 633
Download Sites dialog box, Setup Wizard 24–27
downloads, security settings 450, 459–460
Download unsigned ActiveX controls (security option) 449, 458
Draft folder, Outlook Express 256
Drag and drop or copy and paste files (security option) 450, 462
dual-boot computers 5, 591
DVMRP (Distance Vector Multicast Routing Protocol) 298
dynamically generated CDF files 225–228
dynamic content, in Web pages 403, 406–407
See also Dynamic HTML
dynamic directory services 350
See also ILS (Internet Locator Service)

Dynamic HTML
See also DirectAnimation multimedia controls; HTML (Hypertext Markup Language)
cross-frame security 757–758, 770
cursor attribute 767
data binding 407–409
Document Object Model 400, 415
dynamic content 403, 406–407
dynamic styles 401–403
event handlers, troubleshooting 768
filters 406
Frequently Asked Questions (FAQs) 767–768
graceful degradation 400, 771
HTML standards 399–400
in Active Desktop items 182
overview xli, 395, 398
positioning HTML elements 405
reflowing pages for offline browsing 228
resources 398–399, 401
scriptlets 409–412
text associated with elements, changing 767
TextRange objects 407
ToolTips over anchors, customizing 767
transitions 405–406
Web site 178
Dynamic HTML Object Model 141
dynamic objects, ILS 352
dynamic styles
and Document Object Model 403
Cascading Style Sheets 401–402
font embedding 403–404
inline script events 403
overview 401
STYLE attribute 402
STYLE blocks 402

E

<EARLIESTTIME> XML tag 217, 698
ECMA-262 specification *See* ECMAScript
ECMAScript
ECMA-262 specification 431, 432–433
Internet Explorer 4 vs. Netscape Navigator 4 support 436–437
overview 431
Public_Description object 411
Edit Custom Permissions dialog box 505–507
Client Services tab 512–513
Custom tab 517
File tab 508–509
Network tab 510–511
Reflection tab 516
Registry tab 509–510
System tab 514–515
Edit Permissions tab, Custom Java Security dialog box 499–501
editable setting, embedded fonts 404
Effects control, DirectAnimation 420
electronic checks *See* Microsoft Wallet
elements, HTML *See* HTML elements
e-mail accounts 256
E-mail address (site subscription setting) 198
e-mail delivery of site subscriptions 254
e-mail messages, importing from other mail applications 264
e-mail messaging, NetMeeting 334
e-mail notification
for Active Channels 219, 223
setting e-mail address 198
software distribution channels 695
troubleshooting 746–747
e-mail programs, in deployment planning 593
E-mail server name (SMTP) (site subscription setting) 198
e-mail servers, configuring for deployed browsers 661
Email UsageType value 219, 223
Emergency Repair Disk (ERD), Windows NT 41, 77
Enable automatic browser configuration (Configuration Wizard setting) 654
enabled permissions 493
Enable page hit counting (browser setting) 123
Enable page transitions (browser setting) 123
Enable Profile Assistant (security setting) 124, 542
Enable proxy settings (Configuration Wizard setting) 655–656
Enable scheduled subscription updates (browser setting) 123
encrypted .asx files 300
encrypted mail, sending and receiving 276–277
encrypted Web content, saving to disk 542
encryption 474, 721
encryption check (IE4Setup.exe) 14
END key
Contents list (Help tool) navigation 563
Index tab (Help tool) navigation 564
Internet Explorer 4 navigation 558
Search tab (Help tool) navigation 565
End of range ... (site subscription setting) 204
End-User License agreement dialog box, Setup Wizard 17
enhanced installation 589
Enter Company Name and Customization Code page (Configuration Wizard) 620
ENTER key
Active Desktop items navigation 562
Channel bar navigation 562
Contents list (Help tool) navigation 563, 564
desktop icon navigation 562
Help tool navigation 562, 563
hyperlink navigation 562
Index tab (Help tool) navigation 565
Internet Explorer 4 navigation 558
QuickLaunch toolbar navigation 561

ENTER key *(continued)*
Search tab (Help tool) navigation 565, 566
taskbar navigation 561
Web page navigation 559
entertainment, using NetShow 292
Enumeration (JScript) 434
error codes
Active Setup error codes 15
HResult error codes (Active Setup log file) 15
error correction
ASF packets 296
multicast file transfer 310
error messages
in Active Desktop items 184
Permission Denied 770
shdocvw.dll 138, 140–141
The command failed to execute 753
Unable to sign the program <.cab file> 760–761
Wrong number of arguments 768
errors
See also troubleshooting
item installation, ACME Setup engine 38–39
Setup Wizard
.cab files, downloading 31
download phase 28–29
insufficient disk space 24
proxy errors 25–26
trust errors 31
SoftBoot 44
uninstalling Internet Explorer 4 79
ESC key
animation, turning off 553
Internet Explorer 4 navigation 558
NetMeeting navigation 580
European Computer Manufacturers Association
See ECMAScript
Eval method (JScript) 437
event handlers, Dynamic HTML 768
Every time you start Internet Explorer (cache setting) 133
Every visit to the page (cache setting) 133
Exceptions (Configuration Wizard setting) 656
Exceptions section, Proxy Settings dialog box 95–96
Exchange mail clients, and NetMeeting mail extension 334
Exchange Server Property (NetMeeting setting) 367
.exe files 627, 801
See also names of specific .exe files
Execute (Java permission) 500, 501
Execution access (Java permissions) 515
expiration dates, Active Desktop items 184
Explorer bars
accessibility benefits 546
Channel bar 118
displaying 559
Favorites bar 113–115
History bar 116–118
Explorer bars *(continued)*
new, creating 119
overview xxii, 104, 108
Search bar 108–112
Explorer.exe
troubleshooting Explorer uninstallation 79
updated version, Windows Desktop Update installation 145
Explorer toolbar, Search button 108
Extensible Markup Language *See* XML
extraction, installing .cab files 38

F

/f switch (ACME Setup) 711
F5 key
Internet Explorer 4 navigation 558
NetMeeting navigation 580
F6 key, NetMeeting navigation 580
fail-over, intelligent (NetShow) 285
Favorites (Wizard Settings option) 684
Favorites bar
default contents 113
editing using Profile Manager 114–115
Organize Favorites dialog box 114
Favorites folder
adding folders 115
configuring for deployed browsers 644
folder location, registry entry 155
importing folders 801
roaming profiles, optimizing 53
Favorites Folder and Links Customization page (Configuration Wizard) 644, 776
Favorites menu
customizing 155
editing contents of 156
item arrangement information, registry entry 156
overview 105–106
reordering items on 156
Start menu integration 148–149
file access (Java permissions) 508–509
file dialog boxes (Java permissions) 513
File download (security option) 450, 460
file names
in user profile registry entries 59
Web View, customizing 168
file properties, left folder pane display 167
file sharing, and Internet connections 88–90
file size, limiting downloads 198, 204, 232, 236
File tab, Edit Custom Permissions dialog box 508–509
file transfer, NetMeeting 332
file transfer streams 284, 310–313
file URLs, allowing applet access to 509, 511
FileList control 169

files
See also names of specific file types
backup files 39, 76–77, 83
distribution files, custom packages 667–668
IE4bak.dat file, extracting from 69
IE4Setup.exe
copied to system folder 14
extracted from 10–11
loaded into memory 14
left in system after uninstallation 714–718
making accessible using Personal Web Server 390
Outlook Express, used by 258, 753–754
replaced during Windows Desktop Update installation 145
required for ACME Setup uninstall 76
required for uninstallation 79–80
Web Publishing Wizard, publishing using 393–394
Web View Wizard, created by 165
filters
Dynamic HTML 406
NetMeeting directory entries 333
financial transactions, Microsoft Wallet 535
Find command, Start menu 150–742
Find People dialog box
updating directory services 266
Windows Address Book 260
FindResource function 142
FindX PowerToy 742
Finished message page, IExpress Wizard 810–811
firewalls
HTTP streaming 311
NetMeeting 360–362
NetShow 287
overview 359
security zones, configuring 452
socks protocol 477
flat file directory, Outlook Express 258–259
floating frames 175
floppy disk installation, custom packages
distribution files 668
distribution strategy planning 594, 597
Folder bar, Outlook Express, configuring 270
Folder.htt file
customizing 167–168
overview 165
replacing with custom HTML file 168–169
Web View functionality 164
Folder list
NetMeeting 580
Outlook Express 270
Folder Options dialog box 151
Folder Properties dialog box 171
folders
See also Web View
adding to Favorites folder 115
folders *(continued)*
applying InBox Assistant rules to 267–268
custom toolbars, creating 158
customizing using Web View Wizard 166
displaying contents of 169
Folder.htt file 167–169
header graphics, customizing 168
installation folder, specifying 637
left pane display, customizing 167
My Documents folder, customizing 168
per-user folders 59–60
roaming folders 59–60
Thumbnail view, selecting 171–172
user profile settings 60
virtual folders, customizing 170
Follow links outside of this page's Web site (site subscription setting) 197
Font button, displaying 568, 579
Font download (security option) 450, 460
font embedding
font download, controlling 404, 450, 460
levels of embedding 404
Open Type Font Embedding technology, Microsoft 403
overview 403
STYLE blocks 404
WEFT (Web Embedding Fonts Tool, Microsoft) 405
<FONT FACE=> tag 403
font sizes
changing default size 567, 571, 574–575
changing in current session 568, 574–575, 734
factors affecting 574–575
overriding Web-page formatting 567–568, 571, 734
scaling factor 574–575
specifying in <FONT> tag 575
font styles, overriding Web-page formatting 567–568, 571, 734
formatting of Web pages, overriding 567–568, 571, 734
forms
creating using FrontPage Express 377
publishing using Personal Web Server 392
redirection warning 542
security settings 450, 461
forms, HTML
in offline browsing 191
personalized Active Channels 226–228
using stationery templates 271–273
Forward button xxi, 103
frames
cross-frame security 757–758, 770
HTML syntax, Web site 757
in desktop wallpaper 744
keyboard navigation 558
troubleshooting 757–758, 766, 770
<FRAMESET> tag 757, 766

Friendly Name (Configuration Wizard setting) 662
friendly names, third-party clients 128
FrontPage Express *See* Microsoft FrontPage Express
FTP (Configuration Wizard setting) 656
Full installation option
components included 588
customizing 634
IEAK Configuration Wizard requirements 589
NetShow Player 288–289
Setup Wizard 19
system requirements 587
Full Screen mode 105
full screen window 576–577
Function Creation (JScript) 433, 434
FX libraries 423

G

/g switch (ACME Setup) 711–712
gatekeepers, H.323 protocol 349, 357
gateways, H.323 protocol 349, 357
General tab
Content Advisor dialog box 524–525, 527
Internet Options dialog box
Accessibility options 549
blind users, settings for 549
cache settings 132–133
cognitive and language impairments, settings for 553
colors, selecting 571–572
custom colors, creating 573
default fonts, changing 569–570
History list, setting item lifetime 117
hover color, setting 573
low-vision users 550, 551
page formatting, overriding 734
physical impairments 552
Web page formatting options 566–567
Options dialog box 365
Properties dialog box 417–418
GET method 192
.gif files
Channel bar logos, customizing 696–697
including in .cab files 762
using as NetShow content 316
Global Methods (JScript) 433
Global Ports (Java applet permission) 511
Globe.ani file 11
Go menu, NetMeeting 334
Gopher (Configuration Wizard setting) 656
graceful degradation, Dynamic HTML 400, 771
granted permissions 493
graphics
See also images
browser performance 134
graphics *(continued)*
folder header graphic, customizing 168
sample graphics files, IEAK 616
group collaboration, using NetMeeting 371–372
Grplist.dat file, Outlook Express 259
GUI libraries 423
GUID (Configuration Wizard setting) 626

H

/h switch (ACME Setup) 712
H.323 protocol
audio conferencing, NetMeeting 330
compatible products and services 356–357
gatekeepers 349
gateways 349
in NetMeeting 341, 349
interaction with T.120 protocol 349
interoperability 349, 355
NetMeeting support 335, 336
overview 348
ports required 361
video conferencing, NetMeeting 330–331
hard drive, increasing amount of free space 752
hard-of-hearing users, accessibility settings
See hearing impairments
hearing impairments
overview 551–552
HEIGHT attribute, <USAGE> tag 224
height of HTML client, determining 767
help *See* technical support
help desk, using NetMeeting 370
helper applications 591, 592
Help tool
Contents list, keyboard navigation 563–564
Index tab, keyboard navigation 564–565
keyword searching, keyboard navigation 565–566
left pane, hiding and showing 563
help topics, displaying shortcut menus 564, 565
Hexadecimal Constants (JScript) 436
high-contrast display 568–570, 573–574
Highlight links when clicked (browser setting) 123
Highlight text color (Configuration Wizard setting) 630
High Safety, default capabilities 492
High security level
changing 456
default settings 449–450
Restricted Sites zone 448, 454
users with Authenticode 1.0 473
History bar
clearing contents of 117
configuring 117–118
offline browsing 121
overview 116–117

History folder
AutoComplete feature 100, 102, 560
Back and Forward buttons 103
registry entry 117
History list (NetMeeting) 580
hive synchronization 51
HKEY_CURRENT_CONFIG hive 50
HKEY_CURRENT_USER hive 50, 58–59
HKEY_LOCAL_MACHINE hive 50
home directories, roaming profiles 53
HOME key
Contents list (Help tool) navigation 564
Index tab (Help tool) navigation 565
Internet Explorer 4 navigation 558
Search tab (Help tool) navigation 566
Home Page (Configuration Wizard setting) 662
home page, configuring for deployed browsers 616
Homepage.inf file 11
Home Pages, Active Channels 232
Home page URL (Configuration Wizard setting) 642
Home Page Wizard 385
Home tab, Profile Assistant 537–538
Host Meeting option (Call menu, NetMeeting) 346
hosts, allowing applet access to 511
Hot spot control, DirectAnimation 420
hourly updates to subscribed sites 202
hover color, selecting 573
HREF attribute
<CHANNEL> tag 217, 221
in custom Web View HTML files 169
<ITEM> XML tag 218, 221
HResult error codes 15
HTML (Hypertext Markup Language)
See also Dynamic HTML
Frequently Asked Questions (FAQs) 766
variable substitution strings 168
HTML 4 standards
accessibility benefits 546
Dynamic HTML 399–400
HTML authoring, troubleshooting 755–758
HTML Data Source Objects 408
HTML editor, default, setting 380
HTML elements
See also names of specific elements
binding data to 408–409
changing text associated with 767
innerHTML, innerText properties 406, 767
outerHTML, outerText properties 406, 767
positioning 405
HTML Help, customizing display 566
See also Help tool
HTML layer, Active Desktop interface 175–176
HTML mail
See also e-mail
formatting tags, adding to 272
HTML mail *(continued)*
Outlook Express support 251
overview 248
security zones 278
source code, visibility of 259
stationery templates, Outlook Express 255, 271–273
HTML pages
See also Web pages
and zone security 450
replacing Folder.htt file 168–169
scriptlets 410
setting as Active Desktop wallpaper 178
stationery files 272
HTML path (Configuration Wizard settings) 663
HTML resources
adding to WebBrowser Control 141–142
IE4tour.dll information tour resources 138
overview 138
Shdocvw.dll error messages 138
HTML tags, adding to HTML mail 272
See also individual tag names
HTML wallpaper, Active Desktop 178–179, 744
HTTP (Configuration Wizard setting) 656
HTTP 1.1 130
HTTP 1.1 settings, Internet Options dialog box 125
HTTP cookies
overview 533
personalized Webcasts 225
security settings 542
HTTPS (Hypertext Transport Protocol Secure)
proxy settings 95
server verification 454, 455
HTTP servers, MIME types, setting 313
HTTP streaming
enabling 311–312
MIME types, setting 312–313
overview 311
registry setting 312
Hummingbird Communications 477
hyperlinks
See also links
adding to left folder pane 167
colors, selecting 572
in Help tool, keyboard navigation 562
in user profile registry entries 59
in-place hyperlinking 136
shortcut menus, displaying 558, 559

I

/i switch (Cabarc.exe) 761
ACME Setup 712
IE4Setup.exe 46

/i switch (Cabarc.exe) 761 *(continued)*
IERemove.exe 83
WExtract utility 708
/I switch
Actsetup.exe 710, 711
IE4wzd.exe 710, 711
WExtract utility 16
I/O, user-directed (Java applet permissions) 513
Icmp.dll 191, 215
icons
customizing 615–616, 696–697
disappearing, troubleshooting 740
.idx files, Outlook Express 259
IE4bak.dat file
deleted, effect on Explorer reinstallation 81
extracting files from 69
required for ACME Setup uninstall 76
required to run IERemove.exe 82–83
uninstalling Internet Explorer 4 79
IE4bak.ini file
uninstalling Internet Explorer 4 79
IE4data.cab file 80
IE4data.inf file 80
IE4.dll file 79
IE4.inf file 79
IE4Setup.exe
ACME Setup engine, launching 36
command-line switches 801–802
debug install 47
distributing Internet Explorer 668–669
downloading 9, 12–13
extracting 9
files
copied to system folder 14
extracted from 10–11
loaded into memory 14
maintenance mode 67
network installation 46
quiet mode 46, 708
reinstalling components 67–68
Setup Wizard, launching 16–17
silent installation 46
system checks 13–14
target folder, specifying 708
Web site 12
WExtract utility 10, 707–708
Windows Desktop Update installation 20–21
IE4Setup.hlp file 11
IE4Setup.inf file 11
IE4 Setup Log.txt file 42–43
IE4shell.cab file 79
IE4shell.inf file 80
IE4Sites.dat file 25
IE4tour.dll 138
IE4 Uninstall Log.txt file 82
IE4wzd.exe 11, 802
IEAK (Internet Explorer Administration Kit)
See also IEAK Configuration Wizard; IEAK Profile Manager
Configuration Wizard, system requirements 797
distribution media supported 798
license agreement limits 793
new features 793–795
obtaining 614
on 16-bit platforms 800
optional components 795–797
overview xvi–xviii, 581
self-installing .exe file 801
using IEAK 3 .ins files 797
Web site 802
IEAK (Internet Explorer Administration Kit), overview 581
IEAK Configuration Wizard
See also names of specific pages
Active Channels
locking down settings 235–238
pre-configuring 230–233
Active Desktop items
locking down settings 181
pre-configuring 230–233
Active Setup
customizing 628–638
customizing 775
parameters, specifying 622–627
advanced Java permissions editor dialog boxes 502–504
automatic browser configuration, locking down 675–676
Automatic Version Synchronization 597, 620, 624
browser, customizing 639–659, 776–779
components, customizing 660–666
Content Advisor
locking down settings 527–528
pre-configuring 526–527
custom toolbars, pre-configuring 159
Custom-Build Checklist 773–791
customization key, IEAK 614
.inf files 677
Java permissions, customizing 502–517
navigating 618
Outlook Express settings, pre-configuring 262
overview 617
publisher's update schedule, locking down 223–224
security options, locking down 464–465
silent installation, configuring 633
software distribution channels
importing 703–704
locking down 704
Stage 1 619–622, 773
Stage 2 622–627, 774
Stage 3 628–638, 775
Stage 4 639–659, 776–779
Stage 5 660–666, 780

IEAK Configuration Wizard *(continued)*
Stage 6 781–791
starting 218
system requirements 588–589, 797
Web site subscription options, locking down 203–206
Wizard Settings, changing in
Profile Manager 683–684, 705
IEAK Profile Manager
See also names of specific pages
Active Channels
managing 239–240
subscription options, locking down 118, 236–238
Active Desktop items
locking down 181
managing 239–240
advanced Java permissions editor
dialog boxes 502, 503–504
auto-configuration files, managing 672, 688
automatic browser configuration, locking down 675–676
Channel bar, customizing 118
Content Advisor
locking down settings 528
pre-configuring 526–527
updating settings 529–530
custom toolbars, pre-configuring 160
Java permissions, customizing 502–517
locking down features in deployed browsers 686
NetMeeting settings, customizing 364–368
Outlook Express settings, pre-configuring 261
overview 682–683, 795
publisher's update schedule, locking down 223
Search bar page, customizing 110
security options, locking down 464–465
Security Zones, customizing 465–466
software distribution channels 694, 704
System Policies and Restrictions object 685–686
Web site subscription options, locking down 203–206
Wizard Settings object 683–684
IERemove utility
emergency uninstall 82–83
Internet Explorer 4
removing from Windows 95 system 727–729
removing from Windows NT system 729–731
Windows Desktop Update, uninstalling 730–731
IETF (Internet Engineering Task Force) 344
IETF protocols
LDAP 335
RTP/RTCP protocol 330, 335, 347
Iexplore.exe
IE4Setup.exe system check 13–14
in browser architecture 136–138
True Web Integration architecture 145
IExpress Configuration Wizard
navigating 804
overview 617
IExpress Configuration Wizard *(continued)*
Self Extraction Directive (SED) file, creating 804
starting 803
IExpress Wizard
Configure reboot page 812
Confirmation prompt page 807
Create package page 813
Finished message page 810–811
Installation Program to page 809
License agreement page 808
Modify or create page 805
Package Name and Options page 811
Package purpose page 806
Package title page 807
Packaged files page 808
Save Self Extraction Directive page 813
Show window page 810
IExtract.exe 69
If_Modified_Since header 192
IFRAME options 450, 461–462
<IFRAME> HTML tag 175
IFRAMES, relative positioning, troubleshooting 768
IIS (Internet Information Server) 312
iissamples directory 387
ILS (Internet Locator Service)
administration 358
conferencing servers 357
customization 358
directory servers 357
entry lifetime, NetMeeting 352
non-NetMeeting client access 358
overview 332, 358–359
Web site 332, 359
image masking, NetShow 296
images
adjusting file size 321
alternate text (alt text) display settings 576, 578
ASF Editor tool 319, 321
background, troubleshooting 756
codecs, associating with source files 321
copied to desktop, troubleshooting 741
downloads, controlling 197, 232
in Active Desktop items, troubleshooting 748
including in .cab files 762
people with disabilities, settings for 576–578
using as NetShow content 316
Images (site subscription setting) 197
IMAP server, configuring 661
IMAP4 (Internet Mail Access Protocol) 251
<IMG> HTML tag 175
IMPLEMENTATION element, CDF files 699
Import (Configuration Wizard setting) 644
Import Channels (Wizard Settings option) 684
Import current channel configuration
(Configuration Wizard setting) 647

Import current Software Distribution Channel configuration (Configuration Wizard setting) 648
Import option (File menu) 262–264, 751
Import Software Updates (Wizard Settings option) 684, 705
IMTC (International Multimedia Teleconferencing Consortium) 344
InBox Assistant dialog box 267
InBox Assistant, Outlook Express
applying rules to folders 267–268
overview 253, 267
registry entry 268
rules, adding 267–268
Include a Signature page (Configuration Wizard) 270, 663, 780
Include WebBot component 381
Incoming mail (POP3 or IMAP) server (Configuration Wizard setting) 661
Index tab (Help tool navigation) 564–565
Inetcomm.dll file, Outlook Express 258
Inetcpl.cpl file, incorrect version, troubleshooting 726
.inf files
automatic browser configuration 677
Content.inf file 11
Homepage.inf file 11
IE4data.inf file 80
IE4.inf file 79
IE4Setup.inf file 11
IE4shell.inf file 80
policies and restrictions settings 685
softBoot.inf file 714
using custom policy templates 687
InfoPane, Outlook Express
configuring for deployed browsers 663
customizing 269
overview 268, 800
registry entry 269
information delivery
See also Microsoft NetShow
managed Webcasting 210–211
true Webcasting 241
information exchange, using Personal Web Server 392
Initialize and script ActiveX controls... (security option) 449, 458–459
inline script events 403
innerHTML property, HTML elements 406, 767
innerText property, HTML elements 406, 767
Inseng.dll file 11, 14
insertAdjacentHTML method 406
insertAdjacentText method 406
.ins files
automatic browser configuration 676–677
configuring for deployed browsers 654
using as template 687
using IEAK 3 .ins files 797
Install in the specified folder... (Configuration Wizard settings) 637
Install package silently (Configuration Wizard setting) 633
Installation of desktop items (security option) 450, 462
Installation Option dialog box, Setup Wizard 19–20
installation options
See also Full installation option; Minimal installation option; Standard installation option
components available for reinstallation 67
in custom packages 800
software distribution channels 695
specifying in IE4Setup.exe 708
standard installation suites 588
installation packages
configuring 633–634
silent installation 633
Installation Program to page, IExpress Wizard 809
installing
See also ACME Setup engine; Active Setup; IE4Setup.exe; uninstalling
128-bit Server Gated Cryptography 721, 798
Internet Explorer 3 after running IERemove.exe 83
Internet Explorer 4
debug install 46–47
from network share using IE4Setup.exe 46
manual installation 33, 36
Stepping Mode 47
troubleshooting 720–725
Java packages on user's machine 761
Windows Desktop Update 21, 39–44, 720
Integrated Browser *See* Windows Desktop Update
Integrated Browser.dat file
removing Windows Desktop Update 70
required to run IERemove.exe 83
uninstalling Internet Explorer 4 79–79
Integrated Browser.ini file
deleted, effect on Explorer reinstallation 80
removing Windows Desktop Update 70
uninstalling Internet Explorer 4 78–79
Integrated Shell 21
See also Windows Desktop Update
integrated shell mode, specifying in IE4Setup.exe 708
Integrating the Web Desktop Update page (Configuration Wizard) 638, 775
Intel Indeo 5 797
intelligent fail-over, NetShow 285
International Telecommunications Union *See* ITU (International Telecommunications Union)
internationalization 424
Internet Accounts dialog box 265, 266
Internet bandwidth 317
Internet call program, selecting default 126

Internet Client SDK
Frequently Asked Questions (FAQs) 763–772
system requirements 763
Web site 398, 691
Internet connections
See also Internet Connection Wizard
dial-up connections 205, 238, 745–746
proxy bypass settings 95–96
proxy servers 93–95
Internet Connection Services for Remote Access Systems 387
Internet Connection Wizard
automatic setup option 89–92
ensuring installation of 20
ISP selection 92
launching 86
Location Information dialog box 91
manual setup option 88–89
registry setting 86
Setup Options dialog box 87
Internet Explorer 3
accessibility features 547
coexisting with Internet Explorer 4 5, 591, 727, 772
installing after running IERemove.exe 82–83
migrating from 591
returning to, after Internet Explorer 4 installation 727
using Internet Explorer 4 roaming profile 53
Internet Explorer 4
See also browsers
actions requiring previous uninstallation of Internet Explorer 77
coexisting with Internet Explorer 3 5, 591, 727, 771
coexisting with Netscape browsers 5, 591
core, removing with IERemove.exe 82–83
installation
debug install 46–47
from network share using IE4Setup.exe 46
installation issues 5–6, 76–77
manual installation 33, 36
Stepping mode 47
troubleshooting 719–725
integration with Windows Explorer 144
Microsoft Plus!, troubleshooting 743
multiple installations of 5
new features xvi–xviii
Outlook Express integration 257
reinstalling Windows 95 721–724
returning to earlier version 727
system requirements 4, 587–588
tour, loading 138
uninstallation
Add/Remove Programs, troubleshooting 726
after backup files removed 77
core files, removing 74–75
emergency uninstall 82–83
Internet Explorer 4 *(continued)*
uninstallation *(continued)*
errors 79
files left in system 714
files required 76
maintenance mode, ACME Setup 78
manual uninstall 77
registry entries 76, 80
situations not supported 77
system state following uninstall 77
troubleshooting 726–731
uninstall log 82
using IERemove.exe 727–731
updating 70–71, 637
Web sites xv, 802
Internet Explorer 4 Resource Kit CD-ROM
HTML wallpaper samples 178–179
Web View sample applications 162–163
Internet Explorer 4.01, Java security 496, 502
Internet Explorer Administration Kit *See* IEAK (Internet Explorer Administration Kit)
Internet Explorer Properties (Custom-Build Checklist) 788
Internet Explorer Software Distribution Channel Receive property page 695
Internet Explorer Sound Pack component 66, 107
Internet Explorer toolbar 103, 104
Internet Information Server (IIS) 312
Internet Mail, setting default mail program 750
Internet news server (Configuration Wizard setting) 661
Internet Options dialog box
Accessibility options
blind users, settings for 549–550
cognitive and language impairments, settings 553
deaf or hard-of-hearing users, settings for 551–552
low-vision users, settings for 550–551
physical impairments, settings 552
Advanced tab
advanced browser options 121–125
HTTP 1.1, enabling 130
Java options, configuring 425–426
privacy security options, configuring 541–542
Browsing options 121–125
Colors options 553–554
Connection tab
automatic browser configuration settings, locked down 675–676
Automatic Configuration URL, selecting 47–48
Internet Connection Wizard, launching 86
setting up browser for automatic configuration 680
Content tab
Content Advisor, configuring 522–523
digital certificates, configuring 478
Microsoft Wallet, configuring 538–540
Profile Assistant, configuring 536–538

Internet Options dialog box *(continued)*
General tab
Accessibility options 549
cache settings 132–133
History list, setting item lifetime 117
low-vision users, settings for 550–551
overriding Web-page formatting 567
page formatting, overriding 734
physical impairments, settings 552
HTTP 1.1 settings 125
Java Virtual Machine (VM) options 125
Multimedia options 123
Searching options 125
Security options 124
Security tab
font downloads, controlling 404
Java permissions, customizing 496–507
security zones, setting up 451, 457
Toolbar options 125
Internet Restrictions folder, System Policies and Restrictions hierarchy
Active Channel subscription options, locking down 236–238
Web site subscription options, locking down 203–206
Internet Settings
Custom-Build Checklist 784–787
Internet virtual white pages 149
Internet zone 448
interoperability
H.323 protocol 348
LDAP 351
overview 335, 353–354
T.120 protocol 345
interoperability of communications products
directory servers 357
H.323-based products 356–357
ILS-based products 358–359
in NetMeeting 354–355
LDAP-based products 357
overview 353–354
T.120-based products 355–356
<INTERVALTIME> XML tag 217, 698
Intranets
See also Local Intranet zone
bandwidth 317
NetMeeting 368–369, 370–373
proxy bypass settings 95–96
proxy servers, configuring 92–95
trusted applets, distributing 762
invalid page fault, troubleshooting during component installation 724
IP (Internet Protocol), multicast support 241
IP addresses, configuring security zones 452
IP multicast *See* multicasting, NetShow
IP ports, required for NetMeeting connections 361
IPX/SPX protocol, troubleshooting 745
ISDN modems 317
IShellView interface 163
ISPs (Internet Service Providers)
selecting in Internet Connection Wizard 91–92
software, installing and configuring 92
supported by Web Publishing Wizard 393
<ITEM> XML tag
Active Desktop items 185, 224
Active Desktop items 185
usage and attributes 218, 221
within <CHANNEL> tag 221
within <CHANNEL> tag 216
items
displayed in Channel bar 222–223
downloads of, controlling 231
in channel hierarchy 212
specifying in CDF files 218
ITU (International Telecommunications Union)
H.323 protocol 335, 336, 341
overview 344
T.120 protocol 335, 341
T.126, T.127, T.128 standards 347
Ixp000.tmp folder 10–11

J

/j switch (Actsetup.exe) 710
J/Direct 422, 427
.jar (Java Archive) files 422
Java
See also Java applets
accessing Win32 API 427
Authenticode 2.0 security 442–443
capability signing 443
development environment 424–425
Internet Explorer 4 support for 422–424
Java Virtual Machine (JVM) 131, 137, 425
JIT (Just In Time compiler) 130, 425–426
logging, enabling 426
Microsoft Java Technologies Web page 422
overview xlii, 422–423
security 428, 449, 459–460
trust-based security
High Safety, default capabilities 492
Internet Explorer 4.0 vs. Internet Explorer 4.01 496, 502
Low Safety, default capabilities 492–493
Medium Safety, default capabilities 492
overview 424, 428, 439, 490
Package Manager 495
permission model 491–492
permissions 496
permission scoping 493–495

Java *(continued)*
trust-based security *(continued)*
permission signing 492–493, 496
security zones, permission options 491
Trust User Interface 492, 496
Java applets
client services permissions 512–513
controlling downloads of 198, 232
custom permissions 517
data source objects 407–409
file access permissions 508–509
in Active Channels 219, 223
in Active Desktop items 224
in Web pages, using FrontPage Express 378
network connection permissions 510–511
performance 130
pre-caching for offline functionality 182
referencing in Web pages 428
Reflection API permissions 516
registry key permissions 509–510
scripting, security settings 460
signing 182
system permissions 514–515
system properties, readable by default 515
trusted, distributing in intranets 762
Web site 183
Java Beans 423, 495
Java Data Base Connectivity (JDBC) data source objects 408
Java JIT compiler enabled (Java setting) 125
Java Just In Time (JIT) compiler 130–131, 425–426
Java logging enabled (Java setting) 125
Java Native Interface (JNI) 422
Java permissions
client services 512–513
custom 517
customizing 496–501
file access 508–509
network connection 510–511
Reflection API 516
registry key 509–510
system 514–515
Java permissions (security option) 449, 459–460
Java programs, offline browsing 742–743
Java Virtual Machine (VM)
browser architecture 136–137
Just In Time (JIT) compiler 130–131, 425–426
Microsoft Virtual Machine 425
True Web Integration architecture 145
Java Virtual Machine (VM) options,
Internet Options dialog box 122
java.lang.security classes 513
JavaScript 1.2, compared to JScript 3.0 435–437
JavaScript, in Web pages 378
JDBC Data Source Object 408
JDK (Java Development Kit) 422
JDK security classes 513
JIT (Just In Time) Java compiler 130–131, 425–426
Jobexec.dll file 11, 14, 21
.jpg files
including in .cab files 762
using as NetShow content 316
.js files 654
JScript 3.0 *See* Microsoft JScript 3.0
JVM (Java Virtual Machine) *See* Java Virtual Machine (VM)

K

/k switch (ACME Setup) 712
keyboard focus 548, 569
keyboard navigation
Active Desktop items 562
Channel bar 562
Contents list, Help tool 563–564
desktop icons 562
Help tool 548, 562–566
Index tab, Help tool 564–565
Microsoft Windows Keyboard Guide Web site 559
Quick Launch toolbar 561
taskbar 561
Web pages 559–560
Windows Desktop Update 560–562
keyboard shortcuts
See also individual keys
AutoComplete feature 560
Internet Explorer 4 558–559
Microsoft NetMeeting 580
keycode *See* Customization code
keyword searching (Help tool) 565–566

L

-l switch (Cabarc.exe) 762
/l switch
ACME Setup 712
IExtract.exe utility 69
lab testing of deployment process 605
language impairments, accessibility settings 553–554
Language ratings category (RSACi)
configuring acceptable content level 523
content allowed, by level 521
default setting 521
languages
building custom packages for several 597
for Active Channels, selecting 22
Multi Language Support component 66
selecting for custom packages 621
LASTMOD attribute, <ITEM> XML tag 218, 221
<LATESTTIME> XML tag 217, 697–698
Launch browser in full screen window (browser setting) 122

Launch Channel Guide (Configuration Wizard setting) 647
Launch Channels in full screen window (browser setting) 122
Launching applications...from an IFrame
(security option) 450, 462
LDAP (Lightweight Directory Access Protocol)
access to ILS 358
additional services, specifying 266
architecture 351
conferencing servers 357
configuring for deployed browsers 662
custom icon 615
directory services 264–265
dynamic directory services 350
in NetMeeting 333, 341, 349–353
in Outlook Express 250, 251, 264–266
interoperability 351, 357
LDAP servers 351
overview 250, 349–350
registry data 266
topologies 351
version 2 vs. version 3 350
Web site 351
LDAP Settings (Wizard Settings option) 684
LDAP Settings page (Profile Manager) 266
LEFT ARROW key (AutoComplete feature) 560
left folder pane display, customizing 167
left pane, Help tool, hiding and showing 563
LEVEL attribute
<CHANNEL> tag 217
<ITEM> tag 218, 221
libraries *See* Package Manager, Java
License agreement dialog box, Setup Wizard 17
License agreement page, IExpress Wizard 808
License.txt file 11
<LINK> tag, Cascading Style Sheets 402
link-crawl architecture 191–192, 215–216
links
See also hyperlinks
.asx files 301
downloads from subscribed sites, controlling 197
following on subscribed sites 197
from Search page to main browser window,
implementing 112
keyboard navigation 558, 559–560
underlining, specifying 577
Links bar 106–107, 559–560
See also QuickLinks
Links folder, Favorites bar 113
Links toolbar 650
See also QuickLinks toolbar
LoadResource function 142
Local file (Configuration Wizard setting) 663
Local Intranet zone 448, 452
Local Intranet zone dialog box 452–454
Local Machine zone 449
local path, user profile registry entries 59
Location (Configuration Wizard setting) 626
Location Information dialog box,
Internet Connection Wizard 91
Location parameter, FileList control 169
lock icon, status bar 532
log files
Active Setup Log.txt file 15, 669
Activity log, Personal Web Server 390
IE4 Setup Log file 42–43
IE4 Uninstall Log file 81
Monitor Events Log file, NetShow 287
registry entries 80
Server Event Log file, NetShow 287
SoftBoot Log file 40
system configuration, Setup Wizard 40
uninstall log 82
<LOG> tag 219
logging, Active Channel user activity 219, 238
Login Options dialog box 199
<LOGO> tag 218
Logon (security option) 450, 461
<LOGTARGET> XML tag 219
Low Safety, default capabilities 492–493
Low security level 449–450, 454, 456
low-vision users, settings for 550–551, 568–570, 573–575
luring attacks, preventing 494

M

/m switch
ACME Setup 712
IE4Setup.exe 46
WExtract utility 16, 708
/M switch (IE4wzd.exe) 802
Macromedia Shockwave Director component 65
Macromedia Shockwave Flash component 66
mail attachments, troubleshooting 752–753
mail clients, default, changing 749–750
Mail data directory, Outlook Express 259
Mail Options dialog box 198
mail program
default, selecting 126
registry keys 127–128
mail server, configuring in Outlook Express 261
MailTo URLs
selecting program to open 750–751
third-party clients, registry entries 128
Main window, Personal Web Manager 388
managed Webcasting
See also Active Channels
applications of 210–211
link-crawl architecture 215–216
overview xxxiv, 187–188, 210–211

Manage Subscriptions dialog box 230, 233
manual setup option, Internet Connection Wizard 87–89
manual updates to subscribed sites 202, 205
masking ASF packets 295–296
Math.atan2 method (JScript) 437
Math methods (JScript) 433
Maximum KB of site subscription
(site subscription setting) 204
Maximum number of minutes ...
(site subscription setting) 204
Maximum number of site subscriptions ...
(site subscription setting) 204
Maximum site subscription crawl depth
(site subscription setting) 204
MBONE-compatible applications, NetShow support for 285
.mbx files 259
MCUs (Multipoint Conferencing Units) 336
MCUs (multipoint control units) 356
media, selecting for package distribution 597, 622, 773, 798
Medium Safety, default capabilities 492
Medium security level
changing level 456
default settings 449–450
Internet zone 448
Local Intranet zone 448
users with Authenticode 1.0 473
MeetingPlace object, ILS 352
Menu bar 106
Message Queue Server, Microsoft 386
<META> tag, troubleshooting 756
MFC .dll files, packaging with components 768
MHTML (MIME HTML), Outlook Express support 251
Microsoft ActiveX SDK, Web site 759
Microsoft Agent 65, 796
Microsoft Chat Settings, Custom-Build Checklist 791
Microsoft Chat 686, 795
Microsoft Client for NetWare Networks 745
Microsoft Data Access Components 386
Microsoft Developer Network Web site 414
Microsoft Fast SGC key usage extension 476
Microsoft Font Properties ExtensionWeb site 405
Microsoft FrontPage Express
ActiveX controls, adding to pages 382
existing pages, editing 379–380
features 376–378
new page, creating 379
overview xl, 245, 795
saving pages 380
scripts, adding to pages 382
templates, creating 381
WebBots, adding to pages 381–382
Microsoft Interactive Music Control 796
Microsoft Internet Explorer Digital ID Web site 275
Microsoft Internet Explorer Press Web site 802
Microsoft Internet Explorer Sound Pack 797
Microsoft Internet Explorer Supplemental Fonts 797
Microsoft Java Technologies Web page 422
Microsoft JScript 3.0
availability 435
ECMA-262-compliant features 431–433
features not included in ECMA-262 434
JavaScript 1.2 compared to 435–437
licensing 435
Web site 435
Microsoft Knowledge Base Web site 6
Microsoft Message Queue Server 386
Microsoft NetMeeting
See also audio conferencing, NetMeeting; video conferencing, NetMeeting
accessibility features 579–580
ActiveX control 369
adding to intranet Web pages 368–369
application sharing 331
architecture 339–343
calling options 334
call windows 333
chat feature 332
client/server architecture 352
Clipboard, sharing 332
conferencing standards
H.323 standard 348–349
LDAP 350–353
overview 343
standards organizations 344
T.120 standard 344–347
conferencing topologies 345–347
data conferencing 343–347, 360
directory entries, filtering 333
e-mail messaging 334
file transfer 332
firewalls 359–362
Go menu 334
H.323 gateway calling option 334
H.323 protocol 335, 336, 341, 348–349
home page URL, setting 367
ILS (Internet Locator Service) 332, 352–353, 357–359
intelligent stream control 331
interoperability 336, 345, 347, 351, 353–359
IP port requirements 361
LDAP (Lightweight Directory Access Protocol) 332, 341, 349–353
limitations across firewalls 362
mail extension 334
multipoint data conferencing 331–332
Outlook bar integration 336
overview xxxviii, 245, 795
protocols (Configuration Wizard) 782
protocols supported 335
security and firewalls 362
settings (Configuration Wizard) 780

Microsoft NetMeeting *(continued)*
server compatibility 353
system policies and restrictions 333, 363–368, 686
T.120 protocol 335, 341, 344–347, 355–356
toolbars 334
top provider 346
user information category, presetting 367
user interface features 333–334
uses for 337–338, 369–373
version 2.1 features 336
Web site 355, 579
whiteboard feature 332
Windows NT Workstation support 333
Microsoft NetShow
See also .asx files; ASF (Active Streaming Format); content, NetShow; individual NetShow components
access control 289
announcement files 300–301, 306–307
ASFChop editor 320
ASF Editor tool 319, 321
ASF streams
multicasting 303–307
unicasting 303, 307, 308
bandwidth 296–297, 317–318, 320–322
broadcasting 283, 284, 296
channels 302–303
Client SDK 290
codec independence 294, 314
codecs 282–283, 293–294, 321–322
content-creation tools 289–290, 305, 318–320
content types 315–317
distributed streams 286, 303
error correction 296
fault tolerance 285
features 282
file transfer streams 284, 304, 310–311
firewalls 287, 302
HTTP streaming 311–313
live content, developing 314–315
logging events 287
masking 296
Microsoft PowerPoint presentations 320
monitoring events 287
multimedia content, multicasting 296–297
NetShow Content-Creation Authoring Guide 290
NetShow How-To Web page 313
network transport protocols 285
overview xxxix, 244, 281–282, 796
Real-Time Encoder SDK 290
RTP Live Audio 304
RTP WAV Audio 304
scalability 286
SDKs 290
stored content, developing 315–322
streaming content 282, 283, 293, 300–313
Microsoft NetShow *(continued)*
streaming technologies supported 283
streams vs. programs 303
stream types 303–304
true Webcasting 241, 291–292
VidToAsf tool 319, 321
WavToAsf tool 318, 321
Web site 241
Windows NT Server integration 285
Microsoft Open Type Font Embedding 403
Microsoft Outlook 97 750
Microsoft Outlook Express
Address Book 256, 260, 262–263
architecture 258
Auto-Add feature 256
AutoReply option 800
configuration options 261
configuring for deployed browsers 661–664
Custom-Build Checklist 787–788
digital IDs 275
Draft folder 256
encrypted mail 276–277
encryption 532
features 248
files used by 258, 753–754
flat file directory structure 258–259
HTML integration 249
HTML mail 251
IMAP4 support 251
importing
address information 262–263
existing e-mail folders 593
messages from other applications 264
options 799
InBox Assistant 253, 267–268
InfoPane 268–269, 663, 800
Internet Explorer 4 integration 257
Internet standards support 251
LDAP (Lightweight Directory Access Protocol) 250, 264–266
Mail data directory 259
mail server, configuring 261
MHTML (MIME HTML) support 251
multiple users 799
newsgroup filters 254
news server, configuring 261–262
NNTP support 251
online accounts, multiple 256
POP3 support 251
preview pane, troubleshooting 752
productivity features 256
saving mail attachments, troubleshooting 753
security 250, 274–278, 532
security zone settings 278
settings adopted by Internet Explorer 4 Setup 592

Microsoft Outlook Express *(continued)*
setup 249
signature, default 270, 664
signed mail 276
site subscriptions, e-mail delivery 254
Smart Reply feature 254
S/MIME support 251
SMTP support 251
specifying to open MailTo URLs 751
stationery templates 255, 270–273
System Policies and Restrictions object, Profile Manager 685–686
toolbars, customizing 270
troubleshooting 749–754
welcome message, creating 270
word processor-like features 256
Microsoft Personal Web Server xxxviii, 380
Microsoft Plus! 743
Microsoft Press Web site 613
Microsoft Referral Server 91–92
Microsoft Remote Data Service (RDS) 386
Microsoft Sales Information Center 554, 555
Microsoft Script Debugger 66, 796
Microsoft Security Advisor Web page 428
Microsoft Shockwave Director 796
Microsoft Shockwave Flash 796
Microsoft Site Builder Network (SBN) 398
Microsoft Specifications and Standards Web site 400
Microsoft Support Web page 613
Microsoft Transaction Server (MTS) 386
Microsoft Virtual Machine (VM)
J/Direct 427
JIT (Just In Time compiler) 425–426
overview 425
Microsoft Visual Basic Run time 797
Microsoft VRML 2.0 Viewer 796
Microsoft Wallet
addresses, configuring 538–539
overview 535–536
payment methods, configuring 540
Microsoft Web Embedding Fonts Tool (WEFT) 404
Microsoft Web Publishing Wizard 795
Microsoft Windows Keyboard Guide Web site 559
migration issues, deployment planning 590–592
migration tools, Outlook Express 799
MIME/content types
application/x-cdf type 225
for dynamically generated CDF files 225–226
MIME types
CDF files 763
setting 312–313
Minimal installation option
CD-ROM installation option 19–20
components included 588
Minimal installation option *(continued)*
customizing 634
system requirements 587–588
Mixer control, DirectAnimation 420
MMS streaming protocol 301
modal dialog boxes 183
modems 317
modification dates 192, 218, 221
Modify or create page, IExpress Wizard 805
Modify Settings (Configuration Wizard setting) 649
Monthly (software distribution channel schedule setting) 704
monthly updates to subscribed sites 201–202
MOSPF (Multicast Open Shortest Path First) protocol 298
mouse-over ToolTips
in channel items 217
over HTML anchors, customizing 767
site summary, Search bar 109
.mov files 315–316
MPEG video streams 291
MS PowerPoint, synchronizing presentations into ASF streams 320
Mshtml.dll file
basic link-crawl architecture 191–192
browser architecture 137
in Outlook Express architecture 258
style sheets and 569
True Web Integration architecture 145
MSICD 698, 701
Msimn.exe file 258
Msimnimp.dll file 258
Msimnui.dll file 258
Msml.dll file 215
Msoeacct.dll file 258
Msoemapi.dll file 258
Msoert.dll file 258
MTS (Microsoft Transaction Server) 386
multicast connections (Java permission) 511
multicasting, NetShow
See also broadcasting
announcing with .asx files 300–301, 306–307
ASF streams 303
bidirectional communication 299
delivery paths 299
file transfer streams 284, 304, 310–311
live ASF streams 304–305
NetShow channels 302–303
overview 283, 296–299
routing protocols 298
RTP Live Audio 303
RTP WAV Audio 304
stored ASF streams 306–307
Multi Language Support component 66
multimedia content, NetShow
ASF (Active Streaming Format) 295
bandwidth, controlling 313

multimedia content, NetShow *(continued)*
H.323 standards 348
multicasting 296
multimedia objects 295
performance 134
streaming media 293
true Webcasting 291–292
multimedia libraries 423, 513
Multimedia options, Internet Options dialog box 122–123, 578
multiple users, Outlook Express 799
Multipoint Conferencing Units (MCUs) 336
multipoint control units (MCUs) 356
multipoint data conferencing 331–332
See also Microsoft NetMeeting
mycomp.htt file 164, 170, 651
My Computer and Control Panel Webview Customization (Wizard Settings option) 684
My Computer and Control Panel Webview Customization page (Configuration Wizard) 651, 777
My Computer folder, customizing 170, 651
My Documents folder
customizing 168
Favorites bar 113
roaming profiles, optimizing 53
My Information tab, Options dialog box 365

N

/n switch
ACME Setup 712
IERemove.exe 82–83
WExtract utility 708
Name (Configuration Wizard setting) 644
NaN dates (JScript) 436
National Information System 556
navcancl.htm resource, Shdocvw.dll 138
Navigate method, WebBrowser Control 768
Navigate2 method, WebBrowser Control 768
navigation controls 183
navigation history xxi, 103
navigation pane 108
.nch files, Outlook Express 259
Negative Zero (JScript) 436
nested <CHANNEL> tags 185, 216
NetMeeting 2.1 SDK
See also Microsoft NetMeeting
overview 335, 368–369
Web site 335, 369
NetMeeting *See* Microsoft NetMeeting
Netscape Navigator 3
coexisting with Internet Explorer 4 5, 591–592
migrating from 591–592
Netscape Navigator 4, ECMAScript support 435–437
Netscape, Sever Gated Cryptography (SGC) implementation 476–477
NetShow Administrator
See also Microsoft NetShow
Channel Manager 300, 302, 303, 304
overview 286–287, 289
Program Manager 307, 311
NetShow channels
See also Microsoft NetShow
ASF streams 303
distribution servers 309–310
file transfer streams 304
overview 302–303
RTP Live Audio 304
RTP WAV Audio 304
stored ASF streams, multicasting 306–307
NetShow Client SDK 290
NetShow Content-Creation Authoring Guide 290
NetShow Encoder with Real Video 290
NetShow Player
ActiveX control, Web site 325
embedding in Web page 325–326
launching from Web page 324
opening 323–324
overview 288–289, 323
platforms supported 284
Stand-Alone player 323–324
NetShow Presenter 320
NetShow Real-Time Encoder
live ASF streams, multicasting 304–305
live content, developing 314–315
overview 290
Real-Time Encoder SDK 290
NetShow Server 289, 302, 309–310
NetShow Server SDK 290
NetShow Theater Server 291
NetShow *See* Microsoft NetShow
NetWare servers, troubleshooting 745–746
network bandwidth 293, 317
network connections (Java permissions) 510–511
network installation, custom packages
distribution files 667
distribution servers 614–615
distribution strategy planning 594–596
running IE4Setup.exe 46
Network tab, Edit Custom Permissions dialog box 510–511
network transport protocols, NetShow 284–285
Never (cache setting) 133
Never download more than __ Kb per update (site subscription setting) 198
New operator (JScript) 437
New Toolbar command 154
news
URLs, third-party clients 128

news accounts, multiple 256
news messages in Outlook Express, troubleshooting 752
news programs
  default, selecting 126
  deployment planning 592
  registry keys 127–128
news server
  configuring for deployed browsers 661
  configuring in Outlook Express 261–262
Next button (Configuration Wizard) 618
NNTP (Network News Transfer Protocol) 251
NoClientEdge parameter, FileList control 169
no-embedding (embedded fonts setting) 404
<NOFRAMES> tag 766
nonencrypted .asx files 300
None UsageType value 219, 221, 223
non-file URLs, allowing applet access to 511
Notify me of updates and download the page for offline viewing (site subscription setting) 195
.nsc files 306–307, 309
nsfile.ocx control 311
.nsp files 303
nsplay.ocx control (NetShow Player) 324–326
NTLM authentication 477
Nudity ratings category (RSACi)
  configuring acceptable content level 523
  content allowed, by level 521
  default setting 521
Number formatting (JScript) 437
Numbers (JScript) 433

O

/o switch (ACME Setup) 712
Object Creation (JScript) 433
OBJECT element 325–326
Object numbers, uninstall log 82
object safety, enforcing 458–459
<OBJECT> tag
  adding ActiveX controls to Web pages 416
  adding scriptlets to Web pages 411–412
  data source object, specifying 409
  DirectAnimation controls, adding to Web pages 420
  Java packages, installing on user's machine 761
  referencing .cab files 428
Objects (JScript) 433, 434
OC96 specification 415
Octal constants (JScript) 436
.ocx controls *See* ActiveX controls
ODBC (Open Database Connectivity)-compliant databases 408
OEM installation, Windows 95 720–724
offcancl.htm resource, Shdocvw.dll 138
offline browsing
  See also cached resources; Web site subscriptions
  Active Desktop items 182, 742–743
  ActiveX controls 182–183
  CD caching 120
  Channel bar 121
  Dynamic HTML, reflowing pages 228
  enabling 121
  History bar 121
  HTML forms 191
  Java programs 183, 742–743
  noncached resources 138, 191, 228
  opening sites while offline 121
  overview xxiii, 119
  recognizing from scripts 770
  secure content 542
  usage statistics, Active Channels 219
  viewing list of available sites 121
  Web content, saving to hard disk 120
OLE check (IE4Setup.exe) 13
OLE Controls 1996 specification 415
OLE controls *See* ActiveX controls
OLE files
  mismatch, troubleshooting 69
  update interrupted during browser installation 39
on-demand NetShow content *See* stored ASF streams
On the Internet option (Find menu)
  appearing twice, troubleshooting 742
  overview 150
  Search page, customizing 111
online accounts, multiple 256
online banking *See* SGC (Server Gated Cryptography)
online purchases
  credit card information, storing 535, 540–541
  shipping and billing addresses, storing 535, 538–539
Online Support option (Help menu)
  customizing in deployed browsers 616, 643
  default Web page 613
Online support page URL (Configuration Wizard setting) 643
Only tell me when this page is updated (site subscription setting) 195
operating system check (IE4Setup.exe) 13
operating system resources, allowing applets access to 514–515
Operators (JScript) 433, 434
optimization
  cache settings 131–133
  HTTP 1.1 130
  Java JIT compiler 130
  multimedia settings 133–134
Option dialog box, NetMeeting 365–366
Options option (View menu), troubleshooting 726
Organize Favorites dialog box 113–114
OS VALUE element, CDF files 699

OSD (Open Software Distribution)
creating files 699–700
packaging files 701
specifications, Web site 691
OSR2
reinstalling over Internet Explorer 4 6
System.1st backup 39
Other tab, Profile Assistant 538
outerHTML property, HTML elements 406–407
outerText property, HTML elements 406–407
Outgoing mail (SMTP) server
(Configuration Wizard setting) 661
Outlook bar, Outlook Express
configuring 270
NetMeeting integration 336
overview 252
Outlook Express (Wizard Settings option) 684
Outlook Express Customization page
(Profile Manager) 269, 663, 780
Outlook Express Customizations page
(Configuration Wizard) 269
Outlook Express Customizations
(Wizard Settings option) 684
Outlook Express page (Profile Manager) 261
Outlook Express Settings (Custom-Build Checklist) 787–788
Outlook Express *See* Microsoft Outlook Express
Outlook mail clients, and NetMeeting mail extension 334

P

-p switch (Cabarc.exe) 762
/p switch (ACME Setup) 712
P3 (Platform for Privacy Preferences) model 533
.pac files 654
Package Manager, Java 424, 443, 495
Package Name and Options page, IExpress Wizard 811
Package purpose page, IExpress Wizard 806
Package title page, IExpress Wizard 807
Packaged files page, IExpress Wizard 808
packets, ASF 295
PAGE DOWN key 558
PAGE UP key 558
PARAM elements, <OBJECT> tag 416
<PARAM> tag 458
Parameter (Configuration Wizard setting) 627
parameters
Active Setup 622–627, 774
custom Java permissions, specifying 517
FileList control 169
password caching 198–199, 206, 238
passwords
credit card information, storing 540
Secure Password Authentication, configuring 661
security zones 532
passwords *(continued)*
storing for subscribed sites 198–199
supervisor password, Content Advisor 522, 525
Passwords Properties dialog box, User Profiles tab 54
Path control, DirectAnimation 420
Path of Control Panel custom HTML file
(Configuration Wizard setting) 651
Path of custom desktop wallpaper file
(Configuration Wizard setting) 645
Path of My Computer custom HTML file
(Configuration Wizard setting) 651
paths, in user profile registry entries 58–59
Pattern Matching (JScript) 434
Payment Options dialog box, Microsoft Wallet 540
PCT (Private Communications Technology) 474, 532
PCT 1.0 (security setting) 124, 542
People option, Find command 150
people with disabilities
accessibility resources 554–556
accessibility settings
blind users 549–550
cognitive impairments 553–554
hearing impairments 551–552, 578
language impairments 553–554
low-vision users 550–551, 573–574
physical impairments 552
seizure disorders, users with 553
Microsoft customer service 554
Microsoft Press books, downloading 555, 613
Microsoft Technical Support 554–555
National Information System 556
Recordings for the Blind and Dyslexic 555
Trace R&D Center 556
upgrading to Internet Explorer 4 548–549
performance
See also bandwidth
ActiveX controls 416, 769
cache settings 132–133
distribution strategy planning 595
download times, minimizing 228
HTTP 1.1 130
Java applets 131
Java JIT compiler 131
multimedia settings 133–134
personalized channels 226–228
roaming profiles 52–53
Permission Denied (error message) 770
permission model, trust-based security 491–492
permissions, Java
client services permissions 512–513
custom permissions 517
file access permissions 508–509
for security zones, customizing 496–501
in deployed browsers, customizing 502–517
network connection permissions 511

permissions, Java *(continued)*
overview 459–460
reflection API permissions 516
registry key permissions 510
security zones 490–491
system permissions 514–515
permission scoping 493–495
permission signing 492–493
PersistMoniker line, Desktop.ini file 165, 168
personal information 533–535, 536–538
Personal tab, Profile Assistant 538
Personal Web Manager 385, 388–391
Personal Web Server
Activity log 390
administration 388–390
applications of 391–392
application-testing scenario 392
ASP redirect pages 390–391
default documents, setting 390
directory browsing 390
document-sharing scenario 391
files and directories installed 387
files, adding 390
Home Page Wizard 385
information-exchange scenario 392
Internet Connection Services for Remote Access Systems 387
Microsoft Data Access Components 386
Microsoft Message Queue Server 386
Microsoft Transaction Server (MTS) 386
optional components 386
overview 245, 384
Personal Web Manager 385, 388–391
Publishing Wizard 385, 390
security 385
standards supported 386
virtual directories 389
Web pages, adding 390
Windows 95 integration 384–385
personalized channels
MIME/content type, CDF files 225–226
overview 225
performance 228
Personalized Item Settings dialog box 52–53, 57
per-user folders 59–60
physical impairments, accessibility settings 552
PICS (Platform for Internet Content Selection) 520–521
pilot program, for deployment planning 606–608
PIM (Protocol-Independent Multicast) 298
<PLAINTEXT> tag 767
Platform for Privacy Preferences (P3) model 533
Play animations (browser setting) 123
Play sounds (browser setting) 123
Play videos (browser setting) 123
plug-ins, deployment planning 591, 592
policy template (.adm) files 685, 686
POP3 (Post Office Protocol 3) 251
POP3 server, configuring for deployed browsers 661
ports
allowing applet access to 511
proxy server setting 93
required for NetMeeting connections 360–361
Port setting, proxy server configuration 93
positioning HTML elements 405
PowerToys add-on utilities
accessibility benefits 546
troubleshooting 742
<PRE> tag 767
PRECACHE attribute, <ITEM> tag
content, downloading 218, 221, 223
software distribution channels 699
support content, channel screen savers 225
preview pane, Outlook Express 752
PreviousIESysFile registry value 735
print and preview (embedded fonts setting) 404
Print background colors and images (browser setting) 125
printer sharing, and Internet connections 90
Printers folder, customizing Web View 170
Printers.htt file
customizing 170
Web View functionality 164
printing
background colors and images 579
frames 559
Internet Explorer 4 enhancements 107
Web pages 559
Printing (Java permission) 500, 501
printing services, allowing applets access to 513
privacy
See also security
client/server communications 474
cookies 124, 225, 532–533, 542
information requested by Web sites 535
Microsoft Wallet 535, 536, 538–540
overview xvii, xliv, 532
personal information, making available 533–535, 536–538
privacy security options, configuring 541–542
Profile Assistant 533–535, 536–538
secure communications 532
Private Communications Technology (PCT) 474
private keys *See* digital IDs, Outlook Express
Product Update option (Help menu) 65, 72, 636
Profile Assistant 533–535, 537–538
Profile Assistant dialog box 534–535
Profile Manager *See* IEAK Profile Manager
profile supervisor, specifying 58
Program folders, optimizing roaming profiles 52
Program Manager, NetShow Administrator 307, 311
programmed pull *See* managed Webcasting

Programs menu
customizing 154–155
editing contents of 156
Internet Explorer 4 extensions 148
item arrangement information, registry entry 156
reordering items on 156
programs, NetShow 303–304
See also Microsoft NetShow
Programs tab, Internet Options dialog box 592
Progressive Networks (RealPlayer) 797
project plan, for deployment 601
project teams, assembling 586–587
Prompt before accepting cookies (privacy setting) 542
Properties dialog box, ActiveX controls 417–418
Property access (Java permissions) 514–515
Protected scratch space (Java permission) 500, 501
Protocols tab, Options dialog box 366
protocol types, proxy configuration 95
proxy names 95
proxy servers
configuring 93–95
errors 96
HTTP 1.1, enabling 130
overview 93
proxy bypass settings 95–96
security zones, configuring 452–453
troubleshooting 96
using directory services 266
proxy settings
auto-proxy files 678
configuring for deployed browsers 655–656
errors during Active Setup 25–26
Proxy Settings (Wizard Settings option) 684
Proxy Settings dialog box 94–96, 452
Public_Description object, ECMAScript 411
public keys *See* root certificates; digital IDs, Outlook Express
Public member reflection (Java permissions) 516
public_ prefix, exposing scriptlet names 411
Publisher list (Configuration Wizard setting) 627
publisher's update schedule, locking down 223
Publishing Wizard 385, 390

Q

/q switch
ACME Setup 712–713, 714
Actsetup.exe 710
IE4Setup.exe 46
QI Dance 415
Quick Activation, ActiveX controls 415
Quick Launch toolbar
customizing 157, 158
design guidelines 157
Quick Launch toolbar *(continued)*
keyboard navigation 561
overview 153, 650
QuickLinks 106
See also QuickLinks toolbar
QuickLinks toolbar 153, 158, 546, 562
quiet mode 46–47, 708, 812
See also silent installation
QuietUninstall registry key 80

R

-r switch (Cabarc.exe) 762
/r switch
ACME Setup 713, 714
IE4Setup.exe 46
WExtract utility 16
/R switch (IE4wzd.exe) 802
rangeFromElement method 767
range-request header 192
ratings categories
acceptable content level, configuring 523
default settings 523
unrated Web sites, configuring access to 524
rating systems
overview 520
PICS ratings 520, 521
RSACi content rating system 520–521
Raw Native Interface (RNI) 422
RDS (Remote Data Service) 386
Read access (Java applets)
file permissions 508–509
registry keys 509–510
user-directed I/O permissions 513
Readme.txt, customizing 800
RealAudio 96, 578
RealPlayer (Progressive Networks) 797
Real-Time Encoder SDK, NetShow 290
Real-Time Encoder *See* Microsoft NetShow Real-Time Encoder
reboot options, specifying
in IE4Setup.exe 708
in IExpress Wizard 812
reboot, simulating with SoftBoot 43–44
Receiving tab
Active Channel Properties dialog box 230–232
Properties dialog box 196–199
Recordings for the Blind and Dyslexic 555
red gleam
channel update notification 213
software distribution channel notification 693
troubleshooting 747
with customized Channel bar logos 697
redirect pages, Personal Web Server 390–391

redirection
of forms, warning 542
Web pages, troubleshooting 756
redistributing components in custom applications 142, 768
Referral Server, Microsoft 91–92
Reflection API (Java permissions) 516
Reflection tab, Edit Custom Properties dialog box 516
RegCloseKey() function 58
RegDeleteValue() function 58
.reg file, creating 740–741
registry
DontUseDNSLoadBalancing entry, adding 736
hive synchronization 51
information required for ACME Setup uninstall 76
MIME types, setting 312–313
removing Internet Explorer 4 using IERemove.exe 728–729
Search bar page, customizing 111
setting Exchange attribute 367
Shdocvw.dll error messages, changing 140–141
single-click mode, configuring 740–741
updating using SoftBoot 43–44
registry (Java permissions) 509–510
Registry Editor, incorrect use of 110, 140
registry entries
Active Desktop items 175
ActiveX support files 17
ActiveXCache value, changing 738
auto-configuration changes 672
Automatic Configuration URL 47
backup file locations 83
backup registry information 80
component installation information 75
Control Panel folder, Web View 170
debug install, initiating 47
default HTML editor 379
digital signature of installation files 18
directory services data 266
duplicate entries 687
History folder 117
home directories, roaming profiles 53
HTTP streaming, enabling 311–312
HTTP streaming setting 312–313
hyperlinks 59
IE4Bak.dat information 80
IE4Sites.dat file location 25
IE4tour.dll information tour resources 138
InBox Assistant rules data 268
installation folder 37
Integrated Browser information 80
Internet Connection Wizard setting 86
job name, Actsetup.exe 710
log file information 80
mail program, default 127–128
*.map keys 80
registry entries *(continued)*
MIME types 313
My Computer folder, Web View 170–171
news program, default 127–128
Outlook Express data 259
Package Manager, Java 424
per-user base paths 59
previous browser information 80, 735
profile supervisor 58
proxy server settings 94
proxy settings 25
QuietUninstall keys 80
relative paths 59
Search bar page 111
Search page, Windows Find menu 111
Setup folder 23
setup phase data 34
Shdocvw.dll error messages 138
Start menu folder location 155
Stepping mode, initiating 46
suffixes for AutoDomain searching 103
System.1st backup 39
third-party client programs 127
trust check, disabling 6
Trust files 17
uninstalling components 627
uninstalling using maintenance mode, ACME Setup 78
URLs of add-on pages 64
used by Setup during download phase 709–710
used by uninstall 80
user profile entries 50–51
Web site subscriptions 192
Windows Desktop Update installation entry 21
Windows NT SP3 installation 4
zone security settings 449–450
registry keys, in .adm files 687
Registry tab, Edit Custom Permissions dialog box 510
RegOpenKeyEx() function 58
RegQueryValueEx() function 58
Regular Expressions (JScript) 434
relative paths, in user profile registry entries 59
relative positions
of HTML elements 405
of IFRAMES 768
relative URLs, in CDF files 217
Remote Data Service (RDS), Microsoft 386, 408
Remote Method Invocation (RMI) 422
removing
See also uninstalling
Internet Explorer 4 components 63
Windows Desktop Update 6, 69–70
repeated tables data presentation 409
reset object 170
Reset Sharing button, Content tab 535
Restrict the use of ... (NetMeeting settings) 365–366

Restricted Sites zone 448, 454–455
result pages 112
retailing
  using NetMeeting 372–373
  using NetShow 292
reveal filters 406
revertPrivilege method 493–494
RIGHT ARROW key
  AutoComplete feature 102, 560
  Quick Launch toolbar navigation 561
  taskbar navigation 561
.rle files 316
roaming files 512
roaming folders 52, 53, 59–60
roaming profiles
  home directories 53
  local paths and per-user folders 59–60
  optimizing 52–53
  overview 50
  platform dependence 53
roles (Configuration Wizard setting) 620
root certificates 479–480, 484, 486–487, 657
routers, multicast delivery paths 299
routing protocols, multicasting 298
roving profiles *See* roaming profiles
RSAC (Recreational Software Advisory Council) 520–521
RTCP (real-time control protocol) 330, 348
RTP (real-time protocol) 330, 348
RTP Live Audio 303
rules, InBox Assistant 267–268
Run ActiveX controls and plugins (security option) 449, 458
run command line, using Address bar as 153
RunOnceEx Log.text file 40
Run Signed Content (Java permission) 500
Run Unsigned Content (Java permission) 499

S

-s switch (Cabarc.exe) 761
/s switch
  ACME Setup 713
  Actsetup.exe 710, 711
  IE4Setup.exe 46
/S switch (IE4wzd.exe) 802
S/MIME (Secure MIME), Outlook Express support 251
Safe for Scripting ActiveX controls, troubleshooting 769
safe-for-initialization controls 459
Safemode.htt file 164, 170
sales, using NetMeeting 372–373
Save Self Extraction Directive page, IExpress Wizard 813
Savepack folder 12
SBindHost service, ActiveX controls 415
SBN Workshop 399, 407, 409
scalability, NetShow 286
scaling factor, font sizes 574–575
Schannel.dll file
  128-bit vs. 40-bit encryption 14
  Server Gated Cryptography 475
scheduled updates
  for software distribution channels 694
  independent of time zone 766
  limited usefulness of 207
  randomizing 223–224, 694
  specifying in CDF files 217, 223–224
  to subscribed sites 201–202
  to subscribed sites, disabling 206
schedule groups, disabling creation of 206
Schedule Options (software distribution channel settings) 648
Schedule tab
  Active Channel Properties dialog box 233
  Properties dialog box 199–202
<SCHEDULE> tag 184–185, 217, 693, 694, 766
Scheduling Agent 192
scheduling NetShow broadcasts 284
scope *See* permission scoping
scratch space (Java settings) 512
screen readers
  audio clips and 578
  system caret movement 576
ScreenSaver UsageType value 219, 225
Script ActiveX controls... (security option) 449, 458
script commands, including in .asf files 317
Script Debugger, Microsoft 66
scripting
  cross-frame security 757–758, 770
  in Outlook Express messages 271
  security settings 449–450, 460
  within .asf files 315
Scripting of Java applets (security option) 450, 460
scriptlet container object control 412
scriptlets
  adding to applications 411–412
  creating 410–411
  interface, defining 411
  overview 409–410
  security 412
scripts
  adding to Web pages using FrontPage Express 382
  ASF Editor tool 319–321
  browser information, determining 770, 771
  Document Object Model 400
  inline script events 403
  offline mode, recognizing 769
scripts directory 387
scrolling menus 548
SDK for Java 2.0 Beta 759
SDKs (Software Development Kits)
  Client SDK 290
  Microsoft NetMeeting 2.1 SDK, overview 335, 368–369

SDKs (Software Development Kits) *(continued)*
Real-Time Encoder SDK 290
SDK for Java 2.0 Beta 759
Server SDK 290
Search bar
customizing 112
navigation controls 112
overview 108–109, 642
Search site, configuring 109–111
Search Base (Configuration Wizard setting) 662
search engine, launching from start menu 150
Search page
custom, creating 111–112
customizing in deployed browsers 616
links to main browser window, implementing 112
specifying using Profile Manager 109–110
specifying using Registry 110–111
Search Pane, configuring for deployed browsers 642
Search Pane URL (Configuration Wizard setting) 642
Search tab (Help tool) 565–566
Search WebBot component 382
Search when URL fails: (search settings) 125
Searching options, Internet Options dialog box 125
Secure (Configuration Wizard setting) 656
Secure (proxy server setting) 95
secure channels 474
secure containers 412
Secure Password Authentication, configuring for deployed browsers 661
Secure Sockets Layer *See* SSL (Secure Sockets Layer protocol)
secure Web content, saving to disk 542
security
See also privacy; trust-based security, Java
authentication 441
Authenticode 471–474
class libraries, Java 495
client/server communications 474–477
cross-frame security 757–758, 770
deployment planning 599
digital certificates 441–442
digital signature 441
distribution strategy planning 596
font downloading 404, 450, 460
Internet Explorer 3.0 settings 451
Internet Explorer 4 enhancements xvii
Java 427–428, 442–443
Microsoft Security Advisor Web page 428
NetShow, access control 289
Outlook Express 250, 274–278
Personal Web Server 385
scriptlets 412
secure channels 474–477
secure communications 532
security *(continued)*
trust management 440–441
Web content issues 443–445
security classes, allowing applets access to 513
Security dialog box 466
security levels
changing for security zones 456
default settings 449–450
Security object 464
Security options, Internet Options dialog box 124
Security Settings dialog box 466, 497
security settings, overriding in WebBrowser Control 141
Security tab
font downloads, controlling 404, 450, 460
Internet Options dialog box
security zones, setting up 451, 457
Java permissions, customizing 496
Local Intranet zone, adding sites to 452–454
mail account Properties dialog box 275
Restricted Sites zone, adding sites to 455
security options, customizing 457–462
Trusted Sites zone, adding sites to 454–455
Security Warning dialog box 481, 484, 487
security zones
architecture 450
assigning Web sites to 452–455
changing security levels 456
customizing security settings 456–462, 463, 465–466
deployed browsers, configuring 463–466, 659
for Outlook Express 278
Internet zone 448
Java permissions
client services permissions 512–513
custom permissions 517
customizing 496–501
file access permissions 508–509
network connection permissions 511
Reflection API permissions 516
registry key permissions 509–510
system permissions 514–515
Local Intranet zone 448, 452–454
Local Machine 448
overview xliii, 439, 444–445, 448–450
password protection 532
permission options, Java applets 490–491
predefined zones 448
Restricted Sites zone 448, 454–455
scripts, accessing pages across zones 770
Trusted Sites zone 448, 454–455
user authentication settings 461
Security Zones and Content Ratings Customization (Wizard Settings option) 684

Security Zones and Content Ratings Customization page (Configuration Wizard) 658–659, 778–779
advanced Java permissions editor dialog boxes 503–505
security zones, pre-configuring 463
Security Zones and Content Ratings Customization page (Profile Manager)
advanced Java permissions editor dialog boxes 503–504
Content Advisor, updating settings in deployed browsers 529–530
SED (Self Extraction Directive) file, creating 804
seekable .asf files, creating 320
seizure disorders, users with
accessibility settings 553
multimedia settings 553
Select a Language page (Configuration Wizard) 621
Select a Microsoft Download Site page (Configuration Wizard) 624, 774
Select Installation Options page (Configuration Wizard) 634, 775
Select Media to Distribute Your Browser page (Configuration Wizard) 622, 773
Select Payment Methods dialog box, Microsoft Wallet 540
Select Silent Install page (Configuration Wizard) 633, 775
Select Version Number page (Configuration Wizard) 636–637, 775
SELF attribute, <CHANNEL> tag 217
Self Extraction Directive (SED) file, creating 804
self-installing .exe file 801
Sequencer control, DirectAnimation 420
server certificates, SGC 476
Server Gated Cryptography *See* SGC (Server Gated Cryptography)
Service Bitmap (Configuration Wizard setting) 662
Services dialog box, Control Panel 312
SET (Secure Electronic Transaction) protocol 535
Settings command, Start menu 151–152
setup appearance, deployment planning 598, 793
Setup folder
hard drive, increasing amount of free space 753
network installation 46
preparing 29–30
removing 63
Setup Options dialog box, Internet Connection Wizard 87
Setup program 591–592
Setup Wizard *See* Active Setup Wizard
Setup.exe 78, 79
Setup.stf file 79
Setupapi.dll file 79
Setupwbv.dll file 79
Sex ratings category (RSACi) 521, 523
SGC (Server Gated Cryptography)
128-bit encryption, installing 721, 798
enabling 475
Microsoft's implementation 476
Netscape's implementation 476
SGC (Server Gated Cryptography) *(continued)*
overview 475
Schannel.dll support 14
sglobal object (JScript) 437
Shadocvw.dll 14
shared applications *See* application sharing
Shdocvw.dll
See also WebBrowser Control
basic link-crawl architecture 191–192
CDF link-crawl architecture 215–216
error messages 138, 140–141
IE4Setup.exe system check 13–14
in browser architecture 136–138
including in custom applications 139–140
location of 145
True Web Integration architecture 145
Shell check (IE4Setup.exe) 13
shell files 69, 82–83
Shell32.dll
troubleshooting Explorer uninstallation 79–80
updated version, Windows Desktop Update installation 145
SHIFT+CTRL+TAB key 558
SHIFT+F10 key
desktop icon navigation 562
Internet Explorer 4 navigation 558
Quick Launch toolbar navigation 561
taskbar navigation 561
Web page navigation 559
SHIFT+SPACEBAR key, Internet Explorer 4 navigation 558
SHIFT+TAB key
Channel bar navigation 562
Internet Explorer 4 navigation 558
Web page navigation 560
Windows Desktop Update navigation 561
shipping addresses, storing 535, 538–539
Shlwapi.dll 58, 79
Show channel bar by default (Configuration Wizard setting) 647
Show Desktop button 153
Show font button (toolbar setting) 125
Show friendly URLs (browser setting) 123
ShowHTMLDialog function 141
Show Internet Explorer on the Desktop setting 122
Show pictures (browser setting) 123
ShowSounds setting 552
Show window page, IExpress Wizard 810
SHRegCloseUSKey() function 58
SHRegDeleteUSValue() function 58
SHRegGetUSValue() function 58
SHRegOpenUSKey() function 58
SHRegQueryUSValue() function 58
Signature (Wizard Settings option) 684
Signature page (Profile Manager) 270

signatures
See also digital signatures; signed files
configuring for deployed browsers 270, 664, 780
default, Outlook Express 270, 664
Signcode.exe utility 760
signed applets
See also Trusted Signed Permissions; Untrusted Signed Permissions
customizing permissions 500–501
resetting permissions 501
viewing permissions 498
zone security, customizing 506, 507–517
signed files
See also .cab files; digital signatures
Authenticode 471
.cab files, in ACME Setup 31–32
custom browser packages 666, 814
signed mail, sending and receiving 276
silent installation
configuring for Active Setup 633
configuring in IExpress Wizard 812
running from IE4Setup.exe 46, 708
single-click mode, configuring 740–741
Single Explorer xxiv, 144
Site Builder Magazine 399
Site Certificate and Authenticode Settings page (Configuration Wizard) 483–484, 657, 778
Site Certificates and Authenticode Settings (Wizard Settings option) 684
Site Certificates and Authenticode Settings object 486
Site Certificates dialog box, trusted certificates, customizing 484, 487
Site Name (Configuration Wizard setting) 635
Site Properties dialog box
editing site subscriptions, disabling 205
Receiving tab 196–199
Schedule tab 199–202
Site Region (Configuration Wizard setting) 635
site subscriptions *See* Web site subscriptions
Site URL (Configuration Wizard setting) 635
sitecrawler 192, 206–207
Size (KB) (Configuration Wizard setting) 627
size guidelines, Active Desktop items 183
Small Icons (toolbar setting) 125
small icons, displaying 579
Smart image dithering (browser setting) 123
Smart Recovery 34
Smart Recovery check (IE4Setup.exe) 14
Smart Reply feature, Outlook Express 254
smooth scrolling, enabling 577
SMTP (Simple Mail Transfer Protocol) 251
SMTP server, configuring for deployed browsers 661
snews: (secure news) URLs 128
Socks (Configuration Wizard setting) 656
socks protocol 477
SoftBoot 43–44
softBoot.inf file 714
SoftBoot Log file 40
SOFTPKG items
icons, specifying in CDF files 696–697
in CDF files 697
in Channel bar 693–694
in Software Updates folder 693
Software channel permissions (security option) 450, 462
software distribution channels
CDF files, creating 697–699
configuration 696
current computer, configuring 702
custom packages, pre-configuring 702–704
distribution schedules 695
distribution strategy 692
implementing 691–692
importing 703–704
installation methods 695
managing with automatic browser configuration 705–706
notification methods 695
number of sites 692
on deployed browsers 648, 704
OSD files, creating 699–700
overview 582, 690
requirements, identifying 691–692
security settings 450, 462
software distribution packages 700–701
subscribing to 702
summary pages 694
types of channels 692–694
version number, specifying 698
Web servers, configuring 702
software distribution packages 700–701
Software Update Available dialog box 71
Software Updates folder, Favorites bar 113
Software Updates folder, Favorites menu 693
SoftwareUpdate UsageType value 219, 698
Sound and video (site subscription setting) 198
sound events, Control Panel
accessibility benefits 547
Start Navigation and Complete Navigation 107, 547
sound files, controlling downloads of 198, 232
Sound Pack component, Internet Explorer 65–66
sounds
See also audio content, NetShow
browser performance 134
settings for people with disabilities 578
Sounds Properties dialog box, Control Panel 550, 552
SoundSentry 551
SPACEBAR key
Advanced tab, Internet Options dialog box 575
Internet Explorer 4 navigation 558
NetMeeting navigation 580

Specify Active Desktop Components
(Wizard Settings option) 684
Specify Active Desktop Components page
(Configuration Wizard) 235, 649, 777
Specify an Online Support Page for Your Browser page
(Configuration Wizard) 643, 776
Specify Custom Active Setup Components page
(Configuration Wizard) 626–627, 774
Specify Download URLs page
(Configuration Wizard) 635, 775
Specify Internet Mail Servers, Domain, and News
Server page (Configuration Wizard) 261, 661, 780
Specify LDAP Server Settings page
(Configuration Wizard) 266, 662, 780
Specify Proxy Settings page
(Configuration Wizard) 655–656, 778
Specify the full path of a custom folder
(Configuration Wizard setting) 637
Specify Trusted Publishers page
(Configuration Wizard) 627, 774
Specify Where You Want to Install Your Browser page
(Configuration Wizard) 637, 775
SpeedDial list, NetMeeting 580
Sprite Buttons control, DirectAnimation 420
Sprite control, DirectAnimation 420
SSL (Secure Sockets Layer protocol)
Internet Explorer 4 support 532
Microsoft Wallet support 535
troubleshooting 96
SSL 2.0 (security setting) 124, 542
SSL 3.0 (security setting) 124, 542
Stage 1, Configuration Wizard 619–622, 773
Stage 2, Configuration Wizard 622–627, 774
Stage 3, Configuration Wizard 627–638, 775
Stage 4, Configuration Wizard 639–660, 776–779
Stage 5, Configuration Wizard 660–666, 780
Stage 6, Configuration Wizard 781–791
Standard installation option
components included 588
customizing 633–634
IEAK Configuration Wizard requirements 588–589
Setup Wizard 19–20
system requirements 588
standard installation suites
components included 588
system requirements 587
Standard text color (Configuration Wizard setting) 630
standards
See also LDAP (Lightweight Directory Access Protocol)
H.323 protocols 348–349
Personal Web Server support 385
T.120 protocol 344–347
standards organizations 344
star topology *See* topologies
Start and Search Page (Wizard Settings option) 684
Start and Search Page object, (Profile Manager) 110
Start menu
customizing 155
editing contents of 155–156
Find command 150
folder location, registry entry 155
Internet Explorer 4 extensions xxiv–xxv, 144, 148–151
roaming profiles, optimizing 52–53
Settings command 151–152
Start Navigation sound event 107
start page, customizing in deployed browsers 616
stationery templates, Outlook Express 271–273
statistics
Active Channels usage 219
tracking with user agent string 653, 794
Status bar 107, 577
Stepping mode 47
stored ASF streams
content, creating 315–322
multicasting 307–309
streaming
See also Microsoft NetMeeting; Microsoft NetShow
distributed streams 302
HTTP streaming 311–313
intelligent stream control 331
NetShow 303
overview 282–283, 293
streaming protocols 301, 311–313
technologies supported by NetShow 283
Strings (JScript) 433, 434
Structured Graphics control, DirectAnimation 420
STYLE attribute
dynamic styles 402
positioning HTML elements 405
software distribution channels 698
STYLE blocks
dynamic styles 402
embedded fonts 404
style sheets
See also Cascading Style Sheets
customizing Web page display 566
file name extension 569
font sizes, specifying 574–575
for high-visibility display 568–570
in Outlook Express messages 271
overriding Web-page formatting 567
testing 570
Style Tag button, Outlook Express toolbar 272
subchannels
in channel hierarchy 212
nested <CHANNEL> tags 185, 216
subfolders, adding to Favorites folder 115
Sublist.dat file, Outlook Express 259
Submit nonencrypted form data (security option) 450, 461
Subscribe Favorite dialog box 195

subscribing
to Active Channels 229
to Active Desktop items 230
to software distribution channels 702
to Web sites 193–202
subscription options
Active Channel subscriptions 229
Add Favorite dialog box 193
Subscribe Favorite dialog box 195
Subscription tab, Press Properties dialog box 194
Subscription Wizard
Active Channel subscriptions 229–230
Active Desktop items 186, 230
subscriptions
See also Active Channels; Web site subscriptions
e-mail delivery 254
e-mail notification, troubleshooting 746–747
Subscriptions object 203–204
substitution strings, HTML variables 168
supervisor password, Content Advisor
options, configuring 524–525
overview 522
Supplemental Web Fonts component 66
support content
for Active Channels 219, 223
for Active Desktop items 224
for channel screen savers 225
Support Page (Wizard Settings option) 684
support *See* technical support
synchronization
clock synchronization 192
hive synchronization 51
version synchronization 597, 620, 624
Synchronize (Configuration Wizard setting) 625
Synchronize All (Configuration Wizard setting) 625
system caret, movement of 576
system checks, IE4Setup.exe 13–14
System.getProperty method 515
System information (Java permission) 500, 501
System.1st backup 39, 70
system permissions, Java applets 514–515
system policies and restrictions
deployment planning 600
NetMeeting 333
System Policies and Restrictions page (Configuration Wizard)
Active Channel subscription options, locking down 236
Active Desktop items, locking down 181
automatic browser configuration, locking down 676
Content Advisor settings, locking down 528
custom toolbars, pre-configuring 159
Custom-Build Checklist 781–790
digital certificate options, locking down 485
NetMeeting settings, customizing 365–368
System Policies and Restrictions page (Configuration Wizard) *(continued)*
Outlook Express toolbars, customizing 270
security options, locking down 464–465
Web site subscription options, locking down 203–206
System Policies and Restrictions page (Profile Manager)
Active Channels subscription options, locking down 236–238
custom toolbars, pre-configuring 159–160
Outlook Express toolbars, customizing 270
overview 685–686
system properties, allowing applet access to 514–515
system requirements
custom package distribution methods 589
IEAK Configuration Wizard 588–589, 797
Internet Client SDK 763
Internet Explorer 4 4, 587–588
standard installation suites 587
system state, after running IERemove.exe 82
System stream redirection access 515
System tab, Edit Custom Properties dialog box 514–515

T

/t switch
ACME Setup 713
T.120 protocol
compatible products and services 355–356
in NetMeeting 335, 341, 347, 367
interaction with H.323 protocol 349
interoperability 345, 354–355
overview 344–345
topologies 345–347
T.126 standard 347
T.127 standard 347
T.128 standard 347
TAB key
Active Desktop items navigation 562
Advanced tab, Internet Options dialog box 575
Channel bar navigation 562
Help tool navigation 562
hyperlink navigation 562
Internet Explorer 4 navigation 558
Internet Explorer 4 vs. Internet Explorer 3 548
keyboard focus, losing 548
Web page navigation 559
Windows Desktop Update navigation 561
Table of Contents, Active Channels 232
tables, using FrontPage Express 377
Tabular Data Control 408
Target language (Configuration Wizard setting) 621
taskbar
customizing 157
design guidelines 157

taskbar *(continued)*
Internet Explorer 4 integration 153–154
keyboard navigation 561
Taskbar Properties dialog box, Start Menu Programs tab 156
Task Scheduler component 66
TCP, in NetMeeting architecture 340
technical requirements, deployment planning 587–588
technical support
during browser deployment 606, 613
for users of Internet Explorer 613
text telephone (TTD) support
Microsoft 554, 555
National Information System 556
using NetMeeting 338, 370
telecommuting, using NetMeeting 338
Telephon.ini file 43
template files
install.ins files 687
policy template (.adm) files 686
%TEMPLATEDIR% substitution string 168
templates
for Web pages 378, 381
stationery templates 271–273
Temporary Internet Files folder
cached resource storage 120
roaming profiles, optimizing 52–53
'test' certificates 761
Test URL (Configuration Wizard setting) 644
testing deployment
lab testing 605
pilot programs 606–608
test plan 604
text, associated with HTML elements, changing 767
text color
formatting in style sheet 568
selecting 571–572
Text Labels, displaying 579
TextRange objects 407
text reader, preparing text for 578
text telephone (TTD) support
Microsoft 554, 555
National Information System 556
text wrapping, troubleshooting 755
<TEXTAREA> tag, troubleshooting 755
The command failed to execute (error message) 753
third-party programs 126–128
This.txt file 11
%THISDIRNAME% substitution string 168
%THISDIRPATH% substitution string 168
Thread access (Java permissions) 514
Thumbnail view 171–172
time handling (JScript) 432, 434, 436, 437
Time Stamp WebBot component 382
Tip of the Day, Outlook Express 270
TITLE attribute, <A> tag 767
Title bar text (Configuration Wizard setting) 630, 641
title bar, configuring for deployed browsers 641
<TITLE> XML tag 217
Toolbar background bitmap
(Configuration Wizard setting) 641, 794, 798
Toolbar options, Internet Options dialog box 126
toolbars
desktop toolbars 158, 562, 650, 795
Internet Explorer toolbar 104
NetMeeting 334
Outlook Express, customizing 270
overview 148–154
Toolbar options, Internet Options dialog box 125
ToolTips
in channel items 217
over HTML anchors, customizing 767
site summary, Search bar 109
top provider, NetMeeting 346
top level windows (Java permissions) 513
topologies
LDAP 351
T.120 protocol 345–347
tour.htm resource, IE4tour.dll 138
Trace R&D Center 556
training
deployment implementation 613
deployment planning 607
using NetShow 291–292
Transitions control, DirectAnimation 420
transitions, Dynamic HTML 406
transport layer, NetMeeting architecture 340
transport protocols, supported by NetShow 285
Trigger.exe *See* Actsetup.exe
troubleshooting
See also errors
128-bit Server Gated Cryptography, installing 721
Active Desktop 742–743, 744, 748
Active Setup 669
ActiveX controls 769
address book, importing 751
ASCII characters, encoding in CDF files 764
background images 756
browser redirection 756
browser version, determining 770
.cab files 760–761, 762
component installation errors 38–39
cross-frame security 770
Data Form Wizard 756
desktop icons, disappearing 740
desktop wallpaper 744
.dll registration problems 44
downloads, inconsistent 737
e-mail notification 746–747
event handlers, Dynamic HTML 767
font size changes, saving 734

troubleshooting *(continued)*
frames 757–758, 766, 770
<FRAMESET> tag 757
HTML authoring 755–758
IFRAMES, relative positioning 768
image downloads, Active Desktop items 748
images copied to desktop 741
Internet Explorer 4
browser installation 720–725
components, installation 724
uninstallation using Add/Remove Programs 726
Internet Properties dialog box access 726
mail attachments, saving 752–753
<META> tag 756
Microsoft Plus! 743
MIME types, CDF files 763
news display in Outlook Express 752
no-boot situation 82
non-Microsoft sites, unviewable 736–737
Novell NetWare 32-bit client 736–737
OLE files, mismatch 69
On The Internet option (Find menu) 742
Outlook Express 749–754
<PLAINTEXT> tag 767
PowerToys 742
proxy servers 95– 96
RealAudio 96
red gleam 747
reinstalling Windows 95 after Internet Explorer 4 installation 721–724
returning to earlier version of Internet Explorer 4 727
Secure Sockets Layer (SSL) 96
Service Pack 3 installation, Windows NT 724–725
Setup and installation, trust check failure 6
shell files, mismatch 69
slow connections 736–737
SoftBoot 44
<TEXTAREA> tag 755
ToolTips over HTML anchors 767
unattended dial-up 745–746
uninstallation 81–83
WebBrowser Control 768
Webcasting 745–748
Windows Desktop Update installation 720–721
true Webcasting xxxvi, 188, 241, 291–292
See also Microsoft NetShow
True Web Integration xxiv, 143, 145
TrueType fonts *See* font embedding
trust-based security, Java
enabled permissions 493–494
granted permissions 493–494
High Safety, default capabilities 492
Internet Explorer 4.0 vs. Internet Explorer 4.01 496, 502
Low Safety, default capabilities 492–493
Medium Safety, default capabilities 492
trust-based security, Java *(continued)*
overview xliv, 424, 428, 439, 490
Package Manager 495
permission model 491
permission scoping 493–495
permission signing 492–493, 496
permissions, customizing 496–501, 502–517
security zones, permission options 491
Trust User Interface 492, 496
trust check
.cab files, installing 38
failed during installation 6
trusted CAs
designating 481, 484, 487
removing 482, 484, 487
trusted certificates, customizing 484, 487
trusted publishers
configuring for Active Setup 627
configuring for deployed browsers 657
designating 481, 484, 487
removing 482, 484, 487
Trusted Signed Permissions 502, 506, 507–517
See also signed applets
Trusted Sites zone 448, 455
trust files, checked by Setup Wizard 18
trust management 440–441
See also security
trust status, of digital IDs 277
Trust User Interface 492, 496
TTD *See* text telephone (TTD) support

U

/u switch
ACME Setup 713, 714
Actsetup.exe 710
/U switch (IE4wzd.exe) 802
UDP (user datagram protocol) 340
ULS (User Location Service) 357
See also ILS (Internet Locator Service)
Unable to sign the program <.cab file> (error message) 760–761
unattended dial-up, troubleshooting 745–746
uncached resources, links to, cursor indicator 120
Underline links (browser settings) 123
unicasting, NetShow
See also broadcasting
announcing with .asx files 300–301, 307, 309
ASF streams 303
live ASF streams 307
NetShow channels 302–303
overview 283, 296
stored ASF streams 307–309
unicode characters (JScript) 436

uninstall files, deleted,
effect on Explorer reinstallation 81
uninstall information, deleting,
effect on reinstallation 75, 77
uninstalling
See also removing
ActiveX controls 737
Internet Explorer 4
Add/Remove Programs, troubleshooting 726
after backup files removed 78
core files, removing 74–75
emergency uninstall 82–83
errors 79
files left in system 714
files required 76
maintenance mode, ACME Setup 78
manual uninstall 78
registry entries required 80
registry information 76
situations not supported 77
system state following uninstall 77
troubleshooting 726–731
uninstall log 82
Windows Desktop Update 69–70, 730–731
Uninstall Key (Configuration Wizard setting) 627
uninstall log 82
Universal Naming Convention (UNC) paths 453
unplugged controls 418
unsigned applets
See also Unsigned Permissions
customizing permissions 499–500
resetting permissions 501
viewing permissions 498
zone security, customizing 506, 507–517
Unsigned Permissions
See also unsigned applets
Edit Custom Permissions dialog box 505–506, 507–517
overview 502
Untrusted Signed Permissions 502–503, 506, 507–517
See also signed applets
UP ARROW key
Advanced tab, Internet Options dialog box 575
AutoComplete feature 560
Contents list (Help tool) navigation 563
Internet Explorer 4 navigation 558
Search tab (Help tool) navigation 566
Update All option, disabling 205, 238
Update Now option, disabling 205, 238
update schedules
in CDF files 217, 223, 765
publisher's update schedule 217, 223–224, 233
randomizing, for Active Channels 223
Web site subscriptions 201–202, 204
updates *See* Web site subscriptions
updating subscribed sites
during online sessions 765
manual updates 202
scheduling 201–202
Upgrade All button, Components Download page 65
URL (Configuration Wizard setting) 644, 663
URL of Add-on Component page
(Configuration Wizard setting) 636
URL:MailToProtocol registered file type,
changing 750–751
Urlmon.dll file 11, 14
browser architecture 137
extracted during setup 14
proxy settings used by 25
True Web Integration architecture 145
URLs
See also Web sites
AutoComplete feature 560
editing in Favorites folder 115
including in .asf files 316
partial, suggested completions 100–102
Personal Web Server 387
prefix and suffix
adding automatically 101–102
AutoDomain searching 102–103
referencing, in CDF files 216–218
relative, in CDF files 217
<USAGE> tag 218, 219, 221–223
Active Desktop items 185, 224
channel screen savers 225
default value 223
e-mail notification 746
software distribution channels 698
usage types 219
UsageType values 219, 221, 222–223
Use a custom welcome page
(Configuration Wizard setting) 645
Use AutoComplete (browser setting) 122
Use HTTP 1.1 (HTTP setting) 125
Use HTTP 1.1 through proxy connections
(HTTP setting) 125, 130
Use Secure Password Authentication
(Configuration Wizard setting) 661
Use smooth scrolling (browser setting) 123
Use the same proxy server for all addresses
(Configuration Wizard setting) 656
User Agent (Wizard Settings option) 684, 794
User Agent String Customization page
(Configuration Wizard) 652–653, 777, 794
user agent string, customizing for
deployed browsers 652–653, 794
User Authentication - Logon (security option) 450, 460–461
user authentication, security settings 450, 460–461
user feedback, in Status bar 107

user information
making available to Web sites 533–535
Profile Assistant, configuring 537–538
user interface (Java permissions) 513
user interface, NetMeeting 334
user needs
See also technical support
deployment planning 590
distribution strategy, custom packages 594
support and training 606–607, 612–613, 670
User object, ILS 352
user privacy *See* privacy
User Profile Wizard
profile supervisor, specifying 58
user profiles, creating 54–57
user profiles
See also Profile Assistant
advanced functionality 58–60
creating 53–57
folder settings 60
hive synchronization 51
Links folder, default path 107
overview 50–51
per-user settings 59–60
profile structure 52
profile supervisor, specifying 58
registry entries 51, 58–59
roaming profiles 52–53, 59–60
uninstalling Internet Explorer 4 78
User.dat file 50–51
User Profiles feature
Address Book files, location of 260
Outlook Express files, location of 258
User Profiles tab, Passwords Properties dialog box 54
User quiet mode 708
User.dat file 50–51
User-directed I/O (Java permissions) 513
Username.wab file 754
User-selected file access (Java permission) 500, 501
Users icon, Control Panel 55

V

/v switch
ACME Setup 713
WExtract utility 16
validating deployment 581, 583, 604–609
variable substitution strings, HTML 168
VBScript 226, 378
See also ECMAScript; Microsoft JScript 3.0
VBScript.dll 145
VDOLive Player 797
verification *See* Authenticode
VeriSign CA, SGC certificates 477
Version (Configuration Wizard setting) 627
version check (IE4Setup.exe) 13, 14
version number
of ActiveX controls 416, 418
specifying for software distribution channels 698
Version number (Configuration Wizard setting) 636
version of Windows 95, determining 722
version synchronization 597, 620, 624, 774
Version Tab, controls Properties dialog box 418
video clips, settings for people with disabilities 578
video conferencing, NetMeeting
See also Microsoft NetMeeting
H.323 standards 348–349
NetMeeting compatibility 356
overview 330–331
restricting 366
through firewalls 360
video content, NetShow
adjusting image or video file size 321
bandwidth, controlling 313
codecs 282–283, 293–294, 321–322
converting to .asf format 315–316
data rate (bit rate) of files 293
masking 296
MPEG video streams 291
Real-Time Encoder, NetShow 290
VidToAsf tool 319, 321
video files, controlling downloads of 197, 232
Video tab, Options dialog box 366
videos, and browser performance 134
VidToAsf tool, NetShow 319, 321
View Customization object
(Configuration Wizard) 270
View Permissions tab,
Custom Java Security dialog box 498
ViewMode parameter, FileList control 169
Violence ratings category (RSACi) 521, 523
virtual directories, in Personal Web Server 389
virtual folders, customizing 170
Virtual Machine (VM) *See* Microsoft Virtual Machine,
Java Virtual Machine
virtual meetings, using NetMeeting 337, 371
virtual white pages, Internet 150
vision impairments
accessibility options 575, 576
blind users 549–550
Browsing options 576, 577
larger buttons, displaying 579
low-vision users 550–551, 568–570, 574
multimedia options 578
Visual Basic 5 139–140
VM (Virtual Machine) *See* Microsoft Virtual Machine
VRML component 65

W

/w switch
  ACME Setup 713
  IExtract.exe utility 69
W3C (World Wide Web Consortium)
  Document Object Model Web page 400
  Dynamic HTML, and HTML 4.0 standards 399–400
  P3 (Platform for Privacy Preferences) model 533
  Web Style Sheets site 401
W95inf16.dll file 11, 14
W95inf32.dll file 11, 14
Wab32.dll 258, 753
Wab.exe 258, 754
Wab.exe program 260
Wabfind.dll 258, 265, 753
.wab files 260
Wabimp.dll 258, 753
Wabmig.exe 258, 751, 754
wallpaper, Active Desktop 174, 178–179, 744
Warn about invalid site certificates (security setting) 124, 542
Warn if changing between secure and insecure mode (security setting) 124, 542
Warn if forms submit is being redirected (security setting) 124, 542
WavToAsf tool, NetShow 318, 321
Web content
  See also audio content, NetShow; video content, NetShow
  Active Channels 212–213
  Active Desktop items 213–214
  CDF-based channels 215
  channel screen savers 214
  controlling downloads in WebBrowser Control 141
  customizing based on user agent string 652–653, 794
  <ITEM> XML tags 218
  secure content, saving to disk 542
  security issues 443–445
  software distribution channels
    notification pages 696–698
Web crawls
  disabled by Web sites 190, 207
  link-crawling process 191–192
  on subscribed sites 191
Web pages
  See also HTML pages; style sheets
  adding scriptlets to 412
  .asx links 300–301
  compatibility issues 593
  creating using FrontPage Express 376–382
  custom toolbars, creating 159
  formatting, overriding 567–570
  keyboard navigation
    between pages 558
    SHIFT+TAB key 558, 559–560
Web pages *(continued)*
  keyboard navigation *(continued)*
    TAB key 558–559
    through pages 558
  making accessible using Personal Web Server 390
  NetMeeting, adding to 368–369
  NetShow Player 324–326
  posting using Web Publishing Wizard 393–394
  printing 559
  publishing xli
  redirection, troubleshooting 756
  referencing Java applets 428
  saving 559
  software distribution channels
    notification pages 696–697, 698
Web Publishing Wizard 380, 393–394, 592
Web Review (Style Sheets Reference Guide Web site) 401
Web site subscriptions
  See also Active Channels
  ActiveX controls, downloading 198
  controlled information delivery 206–207
  crawl depth 197, 204
  daily updates 201
  disabling 205
  download options, customizing 196–198
  file size, limiting downloads 198, 204
  hit-or-miss nature of 207
  Java applets, downloading 198
  links, following and downloading 197
  login options, customizing 199
  mail address options, customizing 198
  manual updates 202, 205, 764
  monthly updates 201–202
  number of subscriptions, restricting 204
  on deployed browsers, locking down 191, 203–206
  overview 190–191
  password caching 198–199, 206
  registry key 192
  scheduled updates 201–202
  scheduled updates, disabling 204–205
  scheduling options, customizing 199–202
  subscribing 193–195
  unsubscribing 195
  usefulness, limitations to 206–207
  Web crawls, disabled by Web sites 190, 207
  weekly updates 201
Web sites
  See also URLs
  personal information requested by 533–535
  security zones, specifying 451–456
Web sites (URLs)
  128-bit Server Gated Cryptography 721, 798
  Active Channel content development 802
  Active Desktop gallery 180
  Active Streaming Format (ASF) white paper 295

Web sites (URLs) *(continued)*
ActiveX controls 183
Authenticode 2.0 download 12
Browser Capability component 771
CAB Developers Kit 759
CAs supporting Microsoft products 469
CDF specification 691, 799, 802
Data Source Object Gallery 408
DirectSound component, DirectX 5 336
Dynamic HTML 178, 802
ECMA-262 specification 431
firewalls, NetShow integration 287
frames, HTML syntax 757
HTML 3.2 Specification Reference 756
IE4Setup.exe download 12
IEAK (Internet Explorer Administration Kit) 614
IEAK information 802
IETF (Internet Engineering Task Force) 344
ILS 332, 359
IMTC (International Multimedia Teleconferencing Consortium) 344
Inside Dynamic HTML 398
Internet Client SDK 398, 412, 691
Internet Explorer 4
add-on pages 64
content development 802
download site 544
information 802
Internet Explorer Customer Support Center 587
Internet Explorer Digital ID Web site 275
ITU (International Telecommunications Union) 344
Java applets 183
JScript 3.0 432, 435
LDAP architecture 351
Microsoft ActiveX SDK 759
Microsoft Developer Network 414
Microsoft Font Properties Extension 405
Microsoft Internet Explorer Press 802
Microsoft Internet Explorer Support Center 591
Microsoft Internet Explorer Web site xv, 613
Microsoft Java Technologies Web page 422
Microsoft Knowledge Base 6
Microsoft Message Queue Server 386
Microsoft NetMeeting 2.1 SDK 335, 369
Microsoft NetMeeting 355, 579
Microsoft NetShow 241
Microsoft NetShow codec information 294, 322
Microsoft NetShow How-To Web page 313
Microsoft NetShow Player ActiveX control 325
Microsoft Press 613
Microsoft products, accessibility 554
Microsoft Remote Data Service (RDS) 386
Microsoft Security Advisor 428
Microsoft Site Builder Network (SBN) 398
Web sites (URLs) *(continued)*
Microsoft Specifications and Standards page 400
Microsoft Support Web page 613
Microsoft Transaction Server (MTS) 386
Microsoft WEFT (Web Embedding Fonts Tool) 404
Microsoft Windows Keyboard Guide 559
OSF specifications 691
PICS (Platform for Internet Content Selection) 520
Recordings for the Blind and Dyslexic 555
SBN Workshop 399, 412
SDK for Java 2.0 Beta 759
Site Builder Magazine 399
Trace R&D Center 556
W3C Document Object Model Web page 400
W3C Web Style Sheets site 401
Web Review Style Sheets Reference Guide 401
WebPost Provider .dll file, distributing 393
Web tab, Active Desktop Properties dialog box 178
Web View
See also Web View Wizard
and Thumbnail view 172
architecture 164
Control Panel folder, customizing 170
Desktop.ini file 165
FileList control 169
Folder.htt file 165, 166–169
folders, customizing 165–169
header graphic, customizing 168
HTML file, replacing Folder.htt file 168–169
left folder pane, customizing 167
My Computer folder, customizing 170–171
My Documents folder, customizing 168
overview xxvii–xxviii, 144, 162
Printers.htt folder, customizing 169, 170
Safemode.htt file, customizing 170
sample applications 163
Web View Wizard
changing default Web View 166
customizing folders 165–166
files created by 164, 165
overview xxix
removing customization 166
WebBot components 381–382
WebBrowser Control
See also Shdocvw.dll
customizing functionality 141
distributing in custom applications 142, 768
error messages, changing 140–141
Explorer bars 108
Frequently Asked Questions (FAQs) 768
HTML resources 138, 141–142
overview 136–137
reusing 139–140
vs. Mshtml.dll 137

Webcasting
accessibility benefits 547
basic Webcasting xxxiii, 190, 191–192, 206–207
managed Webcasting xxxiv–xxxv, 188, 210–211, 215
overview xxxii–xxxvi, 187–188
personalized Webcasts 225–229
relation to Active Desktop items 176–177
troubleshooting 745–748
true Webcasting xxxvi, 241
Webcheck.dll 191, 215
WebPost Provider .dll 393
Webpub directory 387
Weekly (software distribution channel schedule setting) 704
weekly updates to subscribed sites 201
WEFT (Web Embedding Fonts Tool, Microsoft) 403, 404
welcome.htm resource, IE4tour.dll 138
welcome message, Outlook Express 270
Welcome page, configuring for deployed browsers 645
Welcome screen 41
whisper feature, NetMeeting chat 332
whiteboard feature, NetMeeting 332, 580
WIDTH attribute, <USAGE> tag 224
width of HTML client, determining 767
wildcard characters
AutoDomain searching 103
Proxy Settings dialog box 96
Win32 API, accessing from Java code 427
Win32 platform 424
windowless controls 415
Windows 3.1, using IEAK 800
Windows 95
See also Windows NT
Internet Explorer 4
removing using IERemove.exe 727–729
system requirements 587
OEM installation, determining 722
Personal Web Server integration 384
reinstalling after Internet Explorer 4 installation 6, 77, 721–724
roaming profiles 53
System.1st backup 39
version, determining 722
Windows Address Book
See Address Book, Outlook Express
Windows Desktop Update
See also Active Desktop
accessibility benefits 547
Active Setup installation, configuring 638
adding 69–70
adding 6
blind-access utilities, interaction with 549
copying images to desktop, troubleshooting 741
disappearing icons, troubleshooting 740
files replaced during installation 145
Windows Desktop Update *(continued)*
installing
from Setup Wizard 20–21
registry backup 39
separately from browser 21
SoftBoot process 43–44
troubleshooting 720
keyboard navigation 560–566
language conflicts with operating system 9, 720
overview 143
registry information, Integrated Browser 80
removing 69–70
removing 6
scrolling menus 548
single-click mode, changing to 740–741
uninstalling from Windows NT using IERemove.exe 730–731
User.dat file, updating 50–51
Windows 95 reinstallation, troubleshooting 723
Windows Explorer integration 145
Windows Messaging, setting default mail program 750
Windows NT
See also Windows 95
Emergency Repair Disk (ERD) 41, 77
Internet Explorer 4
installation, completing 40–41
removing using IERemove.exe 729–731
system requirements 4, 587
NetMeeting support 333
NetShow, NT Server integration 285
reinstalling operating system 77
roaming profiles 53
Service Pack 3 installation, troubleshooting 724–725
Windows NT Challenge Response 461, 477
Wininet.dll 11, 14, 137, 145
Wininit.ini 43
Winsock 340
wizards *See* names of individual wizards
Wizard Settings object (Profile Manager) 683–684, 705
Wldap32.dll file, Outlook Express 258
working offline *See* offline browsing
Work Offline option (File menu) 121
World Wide Web Consortium *See* W3C
WRAP attribute, <TEXTAREA> tag 755
Write access (Java applets)
file permissions 509
registry keys 509–510
user-directed I/O permissions 513
Wrong number of arguments (error message) 768
Wwwroot directory 387

X

/x switch (ACME Setup) 713
XML (Extensible Markup Language)
  Data Source Objects 408
XML tags *See* individual tag names
<XML VERSION=> tag 216

Y

/y switch (ACME Setup) 713
Yes, but only tell me when this page is updated
  (site subscription setting) 193
Yes, notify me of updates and download the page for
  offline viewing (site subscription setting) 193

Z

/z switch (ACME Setup) 713
z-index property 405
zones *See* security zones
zone security *See* security zones